# 802.11d & 802.11h 在 WLAN 中的应用

fox210317@sina.com
lifz@cvanguard.com
2024-06-17

# 1. 概念及功能

## 1.1. 802.11d

IEEE 802.11d-2001 是对 IEEE 802.11 规范的一项修正，它增加了对“additional regulatory domains（额外的监管领域）”的支持。该支持包括向 beacon frame（信标）、Probe requests（探测请求）和 Probe responses（探测响应）中添加国家信息元素。国家信息元素简化了创建符合世界各地不同规定的 802.11 无线接入点和客户设备的过程。该修正已被纳入发布的 IEEE 802.11-2012 标准中，后续在 802.11-2016 修订标准有更详细的关于 802.11d 的描述。

- beacon frame、probe response frame 字段中包含了国家信息

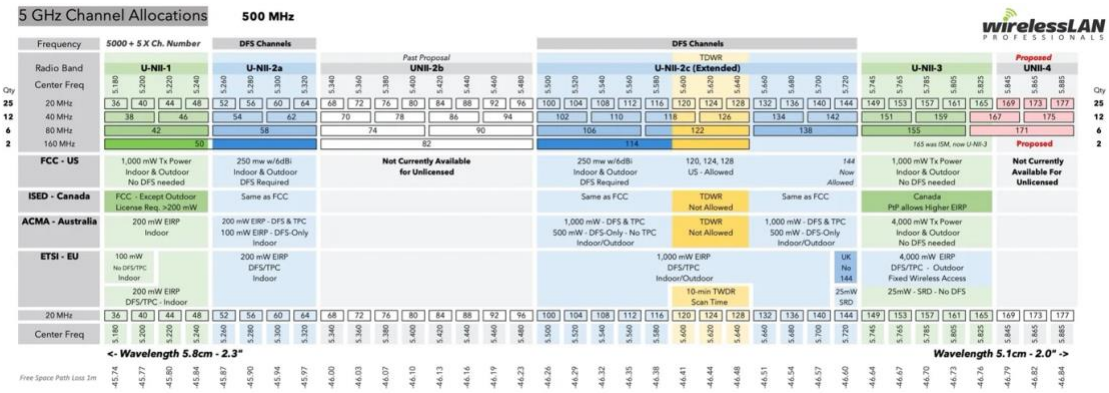
  说明：在 Wikipedia 中描述的 Probe request 中也会有 country information。实际在使用 iphone12 测试中，抓取了 Probe Request Frame 中并未发现包含该信息。同时也不排除一些其他使用场景，如 AP 的网桥互联方式。

## 1.2. 802.11h

IEEE 802.11h-2003，简称 802.11h，指的是 2003 年添加到 IEEE 802.11 标准中的用于频谱和发射功率管理扩展的修正案。它解决了与卫星和雷达在相同的 5 GHz 频段上发生干扰的问题。该标准为 802.11a 物理层提供了动态频率选择（DFS: Dynamic Frequency Selection）和发射功率控制（TPC: Transmit Power Control）。如果检测到这些信号，网络会自动切换到另一个信道。它后来已经被整合到完整的 IEEE 802.11-2007 标准中。同样在 802.11-2016 也有一部分描述。

- 发射功率控制（TPC）会降低每个网络发送器的无线频率（RF）输出功率，以最大程度地减少干扰风险。
- 802.11h 提供了检测、避免对 5GHz 卫星、雷达系统的干扰。
- 802.11h 修正案还定义了一个新的频段提供 802.11 无线接口传输信息使用，即 U-NII-2 扩展（UNII-2 Extended；ch100-144）
- DFS 信道：U-NII-2: ch52-64、U-NII-2c：ch100-144

Tips: 美国与欧洲规定，使用 U-NII-2、U-NII-2 Extended 频段传输信息时，**必须部署**雷达探测与回避技术。频段、信道信息如下图所示：




### 1.2.1. DFS 服务的功能：

- 接入点根据支持的信道，允许客户端进行关联。如果客户端成为接入点所在无线网络的成员，则称二者建立关联。
- 接入点可以将信道“禁声”以测试是否存在雷达传输。
- 在使用信道之前，接入点可以测试信道是否存在雷达传输（我们常常可以在 ARUBA 控制器的日志中看到，AP 在工作前，都会检测雷达信道）。
- 接入点可以检测当前信道和其他信道是否存在雷达传输。
- 如果检测到雷达传输，接入点将停止操作以避免干扰。
- 检测到干扰时，接入点可以选择不同的信道进行传输。并通知所有关联到自己的客户端。

### 1.2.2. 接入点的 DFS 功能如何工作的?

- 每当接入点首次启动 DFS 信道时，无线接口必须监听 60 秒后才能使用该信道传输数据；
- 如果检测到雷达脉冲，接入点无法使用该信道，必须尝试其他信道；
- 如果在最初的 60 秒监听期内没有检测到雷达传输，则接入点可以在该信道发送 beacon；

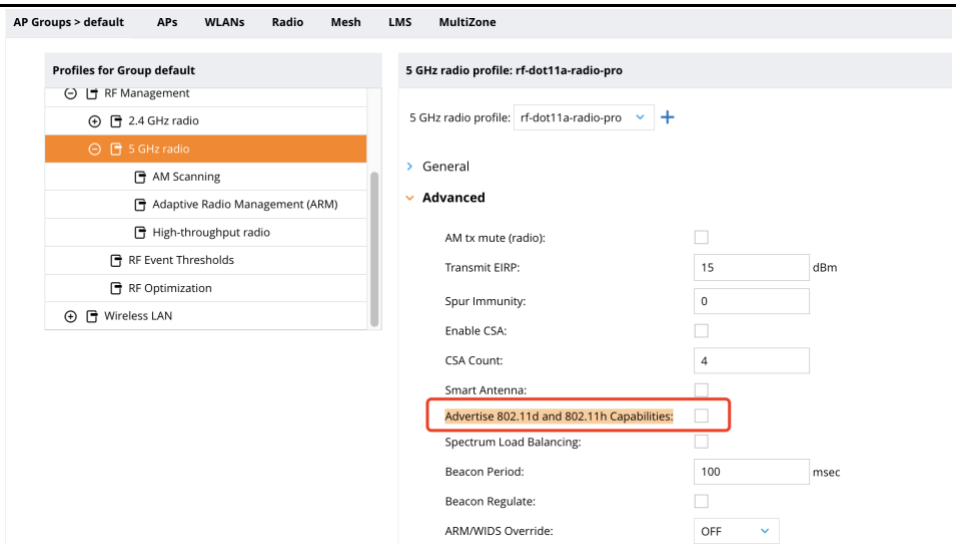
TIPS：在欧洲国家针对 ch120、124、128 更为严格，接入点必须监听 10 分钟。该三个信道为 TDWR（多普勒天气雷达）

## ARUBA 的 DFS 功能

开启 dot11h，AP 会通告 802.11d、802.11h（包含 TPC）的能力。

| | | | |
|---|---|---|---|
| dot11h | Enable advertisement of 802.11d (Country Information) and 802.11h (TPC or Transmit Power Control) capabilities. This parameter is disabled by default. | — | disabled |

配置路径：



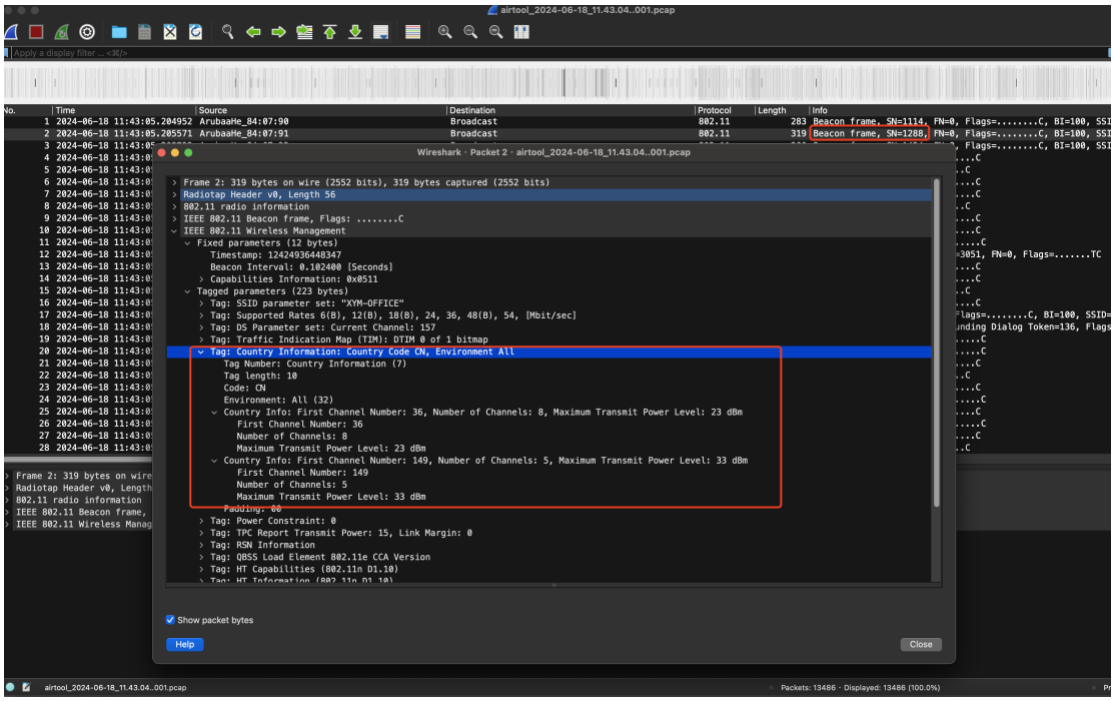

解释：启用 802.11d（国家信息）和 802.11h（TPC 或传输功率控制）功能的通告。默认情况下禁用此参数。

该项参数开启时仅在 AP 面向客户端的 802.11 管理帧中存在，而 AP 面向空口的 DFS 功能是无法被关闭的，这是因为“监管域”的强制性要求。

**空口抓包的信息：**

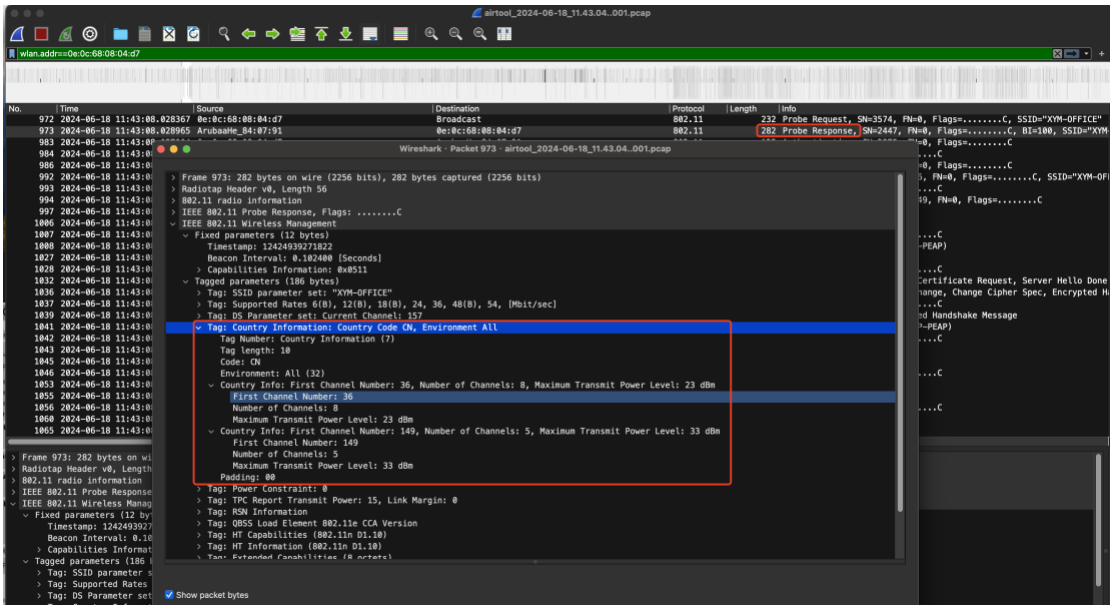
1) 开启 dot11h 时抓取的 beacon:

在 IEEE 802.11 Wireless Management -Tagged parameters 字段中有对应的字段填充国籍信息、信道数量、最大发射功率、TPC 等参数



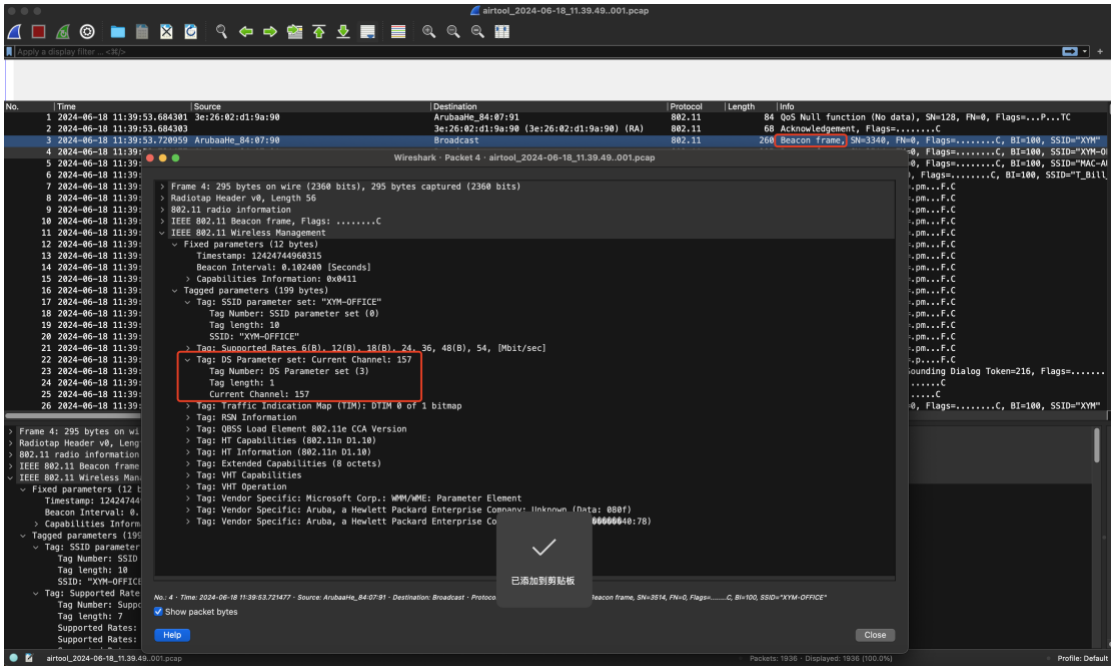
2) 开启 dot11h 时抓取的 probe response

在 IEEE 802.11 Wireless Management -Tagged parameters 字段中有对应的字段填充国籍信息、信道数量、最大发射功率、TPC 等参数



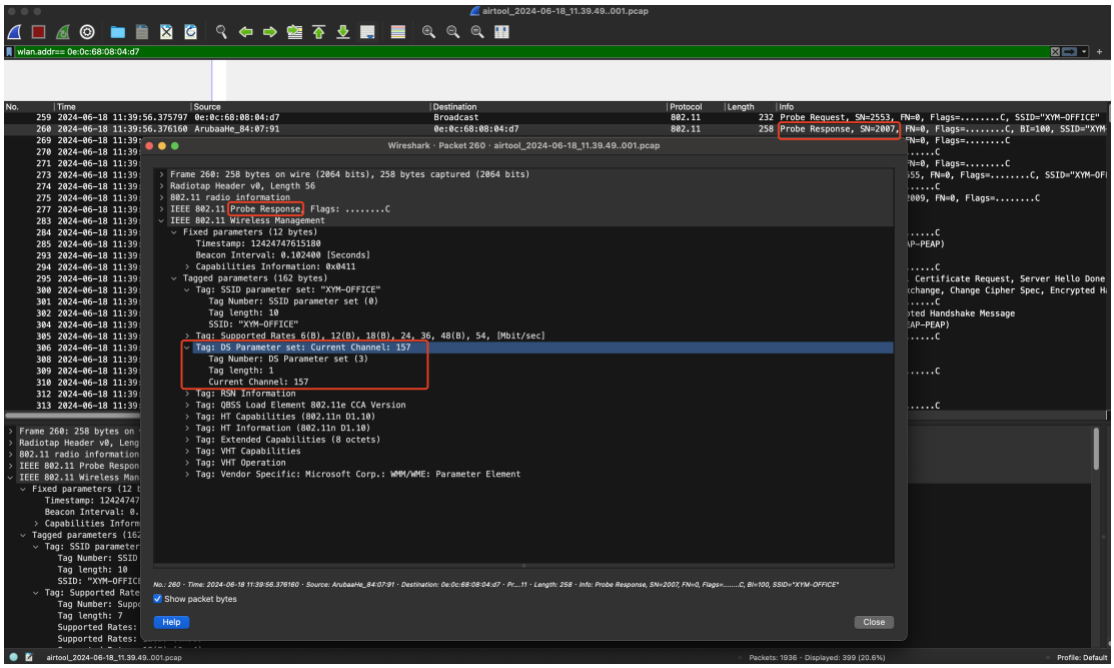

3) 未开启 802.11h 时抓取的 beacon

在 IEEE 802.11 Wireless Management -Tagged parameters 字段中没有国籍信息，仅有工作信道以及其他相同的 tagged 字段



4) 未开启 802.11h 时抓取的 probe response

同样，在 tag 字段无国籍信息




## 1.2.3. 客户端的 DFS 功能如何工作的?

- 802.11 客户端无线接口同样必须遵守雷达避让的规定，因此客户端一般不会首先通过任何 DFS 信道发送 probe request。
- 客户端扫描 DFS 信道时，如果侦听到接入点使用该 DFS 信道发送 beacon frame，就会假定该 DFS 信道不存在雷达传输。因此可以完成关联交换、身份验证的过程。

## 1.2.4. 接入点、客户端二者的 DFS 协同工作的 CSA 机制

如果接入点和客户端正在使用 DFS 信道，当检测到雷达脉冲时，接入点以及客户端必须离开信道。如果在当前的 DFS 频率检测到雷达传输，接入点向所有关联的客户端发送信道切换通告（CSA：Channel Switch Announcement）帧，通知它们切换另一个信道。接入点和客户端需要在 10 秒内离开 DFS 信道。接入点可能会发送多个 CSA 帧，确保所有客户端离开当前信道。一般接入点会切换至非 DFS ch36。后续也新增了很多 DFS 信道的等待时间优化、多个信道的选择机制。

| |
|---|
| 雷达脉冲测试中，使用的是 DFS Radar Signal Generator 软件；<br>发射标准 FCC 06-96<br>Radar Type 1 -Short Pulse Stream. Fixed<br>Radar Type 2 -Short Pulse Stream. 1-5 us pulse width |

| |
|---|
| Radar Type 3 -Short Pulse Stream. 6-10 us pulse width |
| Radar Type 4 -Short Pulse Stream. 11-20 us pulse width |
| Radar Type 5 -Long Pulse Stream. with FM chip |
| Radar Type 6 -Long Pulse Stream. including frequency hopping |
| Radar Type 7 -Bin 1-Weather radar now under proposal -Generates 30 waveforms. |

## ARUBA 的 CSA 功能

| Parameter | Description | Range | Default |
|---|---|---|---|
| csa | Channel Switch Announcement (CSA), as defined by IEEE 802.11h, allows an AP to announce that it is switching to a new channel before it begins transmitting on that channel. Clients must support CSA in order to track the channel change without experiencing disruption. | — | disabled |
| csa-count | Number of CSA announcements that are sent before the AP begins transmitting on the new channel. | 1-16 | 4 |

解释:

**CSA:** IEEE 802.11h 定义的信道切换公告 (CSA) 允许 AP 在开始在该信道上传输之前宣布它正在切换到新信道。

客户必须支持 CSA，以便在不中断的情况下跟踪渠道变化;

该功能的使用需要开启 802.11h

**CSA-COUNT:** AP 开始在新信道上传输之前发送的 CSA 公告数。

该功能的使用需要开启 802.11h、csa

### 1.2.5. TPC 服务的功能：

- 客户端可以根据发射功率与接入点建立关联
- 如果法规允许，接入点和客户端遵守信道的最大发射功率电平
- 接入点可以指定某个或所有关联到自己的客户端使用的发射功率
- 接入点可以根据实际的射频环境参数（如路径损耗）调整客户端的传输功率。

TIPS: 客户端与接入点之间通过管理帧交换 DFS 和 TPC 的使用信息。

管理帧如下表:

| Type value (bits 3–2) | Type description | Subtype value (bits 7–4) | Subtype description |
|---|---|---|---|
| 00 | Management | 0000 | Association Request |
| 00 | Management | 0001 | Association Response |
| 00 | Management | 0010 | Reassociation Request |
| 00 | Management | 0011 | Reassociation Response |
| 00 | Management | 0100 | Probe Request |
| 00 | Management | 0101 | **Probe Response** |
| 00 | Management | 0110 | Timing Advertisement |
| 00 | Management | 0111 | Reserved |
| 00 | Management | 1000 | **Beacon** |
| 00 | Management | 1001 | ATIM |
| 00 | Management | 1010 | Disassociation |
| 00 | Management | 1011 | Authentication |
| 00 | Management | 1100 | Deauthentication |
| 00 | Management | 1101 | Action |
| 00 | Management | 1110 | Action No Ack (NACK) |
| 00 | Management | 1111 | Reserved |

控制帧如下表:

| Type value (bits 3–2) | Type description | Subtype value (bits 7–4) | Subtype description |
|---|---|---|---|
| 01 | Control | 0000–0001 | Reserved |
| 01 | Control | 0010 | Trigger |
| 01 | Control | 0011 | TACK |
| 01 | Control | 0100 | Beamforming Report Poll |
| 01 | Control | 0101 | VHT/HE NDP Announcement |
| 01 | Control | 0110 | Control Frame Extension |
| 01 | Control | 0111 | Control Wrapper |
| 01 | Control | 1000 | Block Ack Request (BAR) |
| 01 | Control | 1001 | Block Ack (BA) |
| 01 | Control | 1010 | PS-Poll |
| 01 | Control | 1011 | RTS |
| 01 | Control | 1100 | CTS |
| 01 | Control | 1101 | ACK |
| 01 | Control | 1110 | CF-End |
| 01 | Control | 1111 | CF-End + CF-ACK |

# 2. 802.11d、802.11h 在 WLAN 中的应用

## 2.1. 中国可用信道

在中国 5GHz 可用的 20MHz 信道如下（未展示信道捆绑），共 13 个 20MHz 信道：

| Seq | PHY Type | Allowed Channels | Frequency Range (MHz) |
|---|---|---|---|
| 1. | 802.11a | 36（U-NII-1） | 5170-5190 |
| 2. | 802.11a | 40（U-NII-1） | 5190-5210 |
| 3. | 802.11a | 44（U-NII-1） | 5210-5230 |
| 4. | 802.11a | 48（U-NII-1） | 5230-5250 |
| 5. | 802.11a | 52（U-NII-2a） | 5250-5270 |
| 6. | 802.11a | 56（U-NII-2a） | 5270-5290 |
| 7. | 802.11a | 60（U-NII-2a） | 5290-5310 |
| 8. | 802.11a | 64（U-NII-2a） | 5310-5330 |
| 9. | 802.11a | 149（U-NII-3） | 5735-5755 |
| 10. | 802.11a | 153（U-NII-3） | 5755-5775 |
| 11. | 802.11a | 157（U-NII-3） | 5775-5795 |
| 12. | 802.11a | 161（U-NII-3） | 5795-5815 |
| 13. | 802.11a | 165（U-NII-3） | 5815-5835 |

在现阶段高密的职场部署 WLAN 有如下特点：

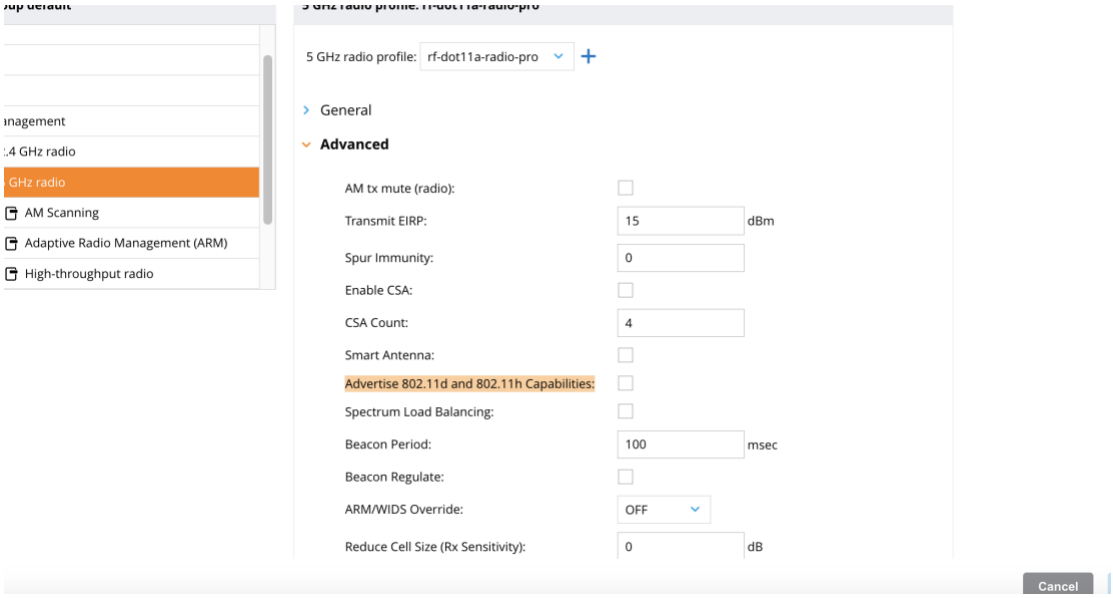
- 单颗 AP 普遍接入终端数量在 40-60 个左右；
- 特殊区域的 ch52-64 不定时避让，造成网络中断；
- AP 的 5GHz 工作频宽 20-40MHz 不等；
- AP 部署密集，漫游体验差；

## 2.2. 802.11h 的使用建议

使用前提：

- 确保终端设备支持 U-NII-2a 信道（中国区 ch52、56、60、64），如终端普遍支持其他监管域的信道，经过测试后建议使用；
- 确认周围无 U-NII-2a 的雷达使用时，关闭 802.11h（与客户端不协商）； 但 AP 面向空口仍然使用 DFS 功能；

《Enterprise-WLAN-Optimization-ChecklistAruba 无线网络优化项-v7》中建议开启此功能


nagement
.4 GHz radio
GHz radio
AM Scanning
Adaptive Radio Management (ARM)
High-throughput radio
5 GHz radio profile: rf-dot11a-radio-pro
General
Advanced
AM tx mute (radio):
Transmit EIRP: 15 dBm
Spur Immunity: 0
Enable CSA:
CSA Count: 4
Smart Antenna:
Advertise 802.11d and 802.11h Capabilities:
Spectrum Load Balancing:
Beacon Period: 100 msec
Beacon Regulate:
ARM/WIDS Override: OFF
Reduce Cell Size (Rx Sensitivity): 0 dB
Cancel