

无线配置

无线UCI配置位于 `/etc/config/wireless` 中。

如果设备有以太网端口，无线是关闭默认情况下。您可以通过将禁用的 `1` 更改为禁用 `0` 来在 `/etc/config/wireless` 中打开它

第

典型的无线配置文件包含至少一个 **WiFi** 设备，其指定通道，驱动程序类型和 `txpower` 等一般无线电属性，以及在无线电设备顶部定义无线网络的一个 `wifi` 接口。

Wifi设备

该 **WiFi** 的设备是指在系统上存在的物理无线电设备。本节中提供的选项说明了该无线电接口上所有无线网络中通用的属性，如通道或天线选择。

一个最小的 `wifi` 设备声明可能看起来像下面的例子。请注意，不同的芯片组类型或驱动程序的标识符和选项可能会有所不同。

```
config 'wifi-device' 'wl0'
    option 'type' 'broadcom'
    option 'channel' '6'
```

- `wl0` 是无线适配器的内部标识符
- `broadcom` 指定芯片组/驱动程序类型
- `6` 是设备操作的无线通道

下表列出了设备部分的可能选项。请注意，并非所有选项都用于所有芯片组/驱动程序类型，有关详细信息，请参阅注释。

常用选项

名称	类型	需要	默认	描述
类型	串	是	(自动检测)	在初始无线电设备检测期间，该类型是在 <code>firstboot</code> 上不需要更改它。使用的值是博通在 <code>brcm47xx</code> ，或 <code>me</code> 其他平台
<i>PHY</i>	串	无/有	(自动检测)	指定与此部分相关联的无线电系统。如果存在，它推测的，不应该更改。
<i>MACADDR</i>	MAC	是/	(自动检测)	指定与此部分关联的无线电话适配器，它不用于更改该

	地址	否		是标识底层接口。
IFNAME	串	没有	(驱动程序默认)	指定WiFi接口的自定义名称，否则将自动命名。
残	布尔	没有	0	如果设置为1，则禁用无线电适配器。删除此选项或将启用适配器
渠道	整数或“自动”	是	汽车	指定要使用的无线频道。“auto”默认为最低可用频道
HWMODE	串	没有	(驱动程序默认)	选择要使用的无线协议，可能的值为11b, 11g和11e
htmode	串	没有	(驱动程序默认)	指定802.11n和802.11ac模式下的通道宽度，可能的有：HT20, HT40-, HT40+, HT40, NONE或VHT20, VHT40, VHT80, VHT160
chanbw	整数	没有	20	指定在窄通道宽度兆赫 (Megahertz)，可能的值为：
ht_capab	串	没有	(驱动程序默认)	指定收音机的可用功能。这些值是自动检测的。看到(http://hostap.epitest.fi/cgi/hostap/tree/hostapd/ho 选项
TXPOWER	整数	没有	(驱动程序默认)	指定发送功率 (dBm)
多样	布尔	没有	1	启用或禁用驱动程序自动选择天线
rxantenna	整数	没有	(驱动程序默认)	指定用于接收的天线，该值可能是驱动程序特定的，第一个天线是1，对于第二个天线通常是2。指定0可序自动选择。如果启用了分集，则此选项不起作用
txantenna	整数	没有	(驱动程序默认)	指定用于发送的天线，值与rxantenna 相同
国家	变化	没有	(驱动程序默认)	指定国家代码，影响可用频道和传输功率。对于类型使用两个字母的国家代码 (EN或DE)。该Madwifi的 数字代码。
country_ie	布尔	没有	1如果国家设置，否则为0	在信标和探测响应帧中启用IEEE 802.11d国家IE (Int Explorer) (信息元素) 广告。该IE (Internet Explore 码和频道/权力图。需要的国家。
距离	整数	没有	(驱动程序默认)	ap和最远客户之间的距离以米为单位。
beacon_int	整数	没有	100 (hostapd默认)	设置信标间隔。这是以1.024 ms为单位测量的信标中 间隔。hostapd允许将其设置在15到65535之间。此 ad hoc wifi-ifaces有影响
basic_rate	名单	没有	(hostapd /	设置支持的基木费率 每个basic_rate以kb / s为单位

<code>basic_rate</code>	字符串	没有	(<code>hostapd / driver</code> 默认)	设置支持的速率。每个支持的速率以kb / s为单位。对 ap 和 adhoc wifi-ifaces 有影响。
<code>supported_rates</code>	列表	没有	(<code>hostapd / driver</code> 默认)	设置支持的数据速率。每个支持的速率以kb / s为单位。对 ap 和 adhoc wifi-ifaces 有影响。必须是 basic_rate 支持的。Basic_rate应该是最低的数据速率。
<code>require_mode</code>	字符串	没有	没有	(AP模式) 设置连接客户端需要支持以允许连接的模式。支持的值: <code>g = 802.11g</code> , <code>n = 802.11n</code> , <code>ac = 802.11ac</code>
<code>LOG_LEVEL</code>	整数	没有	2	设置log_level。支持的级别为: 0 =详细调试, 1 =调试消息, 3 =通知, 4 =警告

Broadcom选项

警告 以下选项仅由专有的Broadcom驱动程序 (`broadcom`) 使用。

名称	类型	需要	默认	描述
<code>frameburst</code>	布尔	没有	0	支持Broadcom帧突发
<code>maxassoc</code>	整数	没有	(驱动程序默认)	限制关联客户端的最大允许数量
<code>slottime</code>	整数	没有	(驱动程序默认)	插槽时间 (毫秒)

Ubiquiti Nanostation选项

警告 以下选项仅供Ubiquiti Nanostation系列器件使用

名称	类型	需要	默认	描述
天线	字符串	没有	(驱动程序默认)	选择天线, 可能的值是垂直于内部垂直极化, 水平为内部水平偏振或外部使用外部天线连接器

Wifi网络

完整的无线配置每个适配器至少包含一个**wifi-iface**部分, 以在硬件之上定义无线网络。一些驱动程序支持每个设备的多个无线网络:

- 如果核心修订版本大于或等于9, 请参阅**broadcom** (参见 `dmesg | grep corerev`)
- `mac80211`

以下给出了**wifi-iface**声明的一个最小例子。

```

config'wifi-iface'
    选项'device''wlo'
    选项'network''lan'
    选项'mode''ap'
    选项'ssid''MyWifiAP'
    选项'加密''psk2'
    选项'key''secret passphrase'

```

- *wlo*是底层无线电硬件的标识符
- *lan*指定wifi连接到的网络接口。
- *ap*在这个例子中是opetion模式，*Access Point*
- *MyWifiAP*是广播的SSID
- *psk2*指定无线加密方法，WPA2 PSK在这里
- 秘密密码是秘密的WPA密码

常用选项

以下列出了 *wifi-iface* 部分的常见配置选项。

名称	类型	需要	默认	描述
设备	串	是	(第一个设备 ID)	指定使用的无线适配器，必须参考定义
模式	串	是	美联社	选择无线网络接口控制器的工作模式。是 <i>ap</i> , <i>sta</i> , <i>adhoc</i> , <i>wds</i> , <i>monitor</i> , <i>mesh</i>
残	布尔	没有	0	当设置为1时，无线网络被禁用。
SSID	串	是	勒德”	广播的无线网络的SSID和用于被管理的SSID
BSSID	BSSID地址	没有	(驱动程序默认)	覆盖网络的BSSID，仅适用于 <i>adhoc</i> 或指定用于创建WDS的另一个AP的BSSID
mesh_id	网格ID	没有	没有	IEEE 802.11s中定义的网格ID。如果添加此网状网络。如果没有，则必须在 <i>mesh join <mesh_id></i> 来连接网格。
隐	布尔	没有	0	如果设置为1，则关闭SSID广播
隔离	布尔	没有	0	将无线客户端彼此隔离，仅适用于 <i>ap</i> 和 <i>sta</i>
岂	布尔	没有	0	支持802.11h。
WMM	布尔	没有	1	支持WMM (802.11e)。需要802.11r
网络	串	是	兰	指定要将无线连接到的网络接口。

加密	串	没有	没有	无线加密方式。可能的值是： <i>none</i> ， <i>v</i> WEP站模式，默认为“开放系统”认证。开， <i>wep +</i> 混合以集中一个特定的模式
键	整数或字符串	没有	(没有)	在任何 WPA-PSK 模式下，这是一个字中预先共享的密钥。如果提供了一个6串，它将直接用作预共享密钥。在 WE 数，指定要使用的密钥索引 (<i>key1</i> ， <i>k</i> 者，它可以是直接指定密码或密钥的守任何 WPA-Enterprise AP 模式下，此
<i>KEY1</i>	串	没有	(没有)	WEP 密码或密钥#1 (由密钥中的索引密码短语，从中导出 WEP 密钥。如果控制字符串，则将直接用作 WEP 密钥。
<i>KEY2</i>	串	没有	(没有)	WEP 密码或密钥#2 (由密钥中的索引
<i>KEY3</i>	串	没有	(没有)	WEP 密码或密钥#3 (由密钥中的索引
<i>KEY4</i>	串	没有	(没有)	WEP 密码或密钥#4 (由密钥中的索引
<i>macfilter</i>	串	没有	禁用	指定 mac 过滤器策略，禁用以禁用过滤或拒绝将其视为黑名单。
<i>maclist</i>	MAC地址列表	没有	(没有)	MAC地址列表 (除以空格) 放入 mac 这
<i>iapp_interface</i>	串	没有	(没有)	指定要用于 802.11f (IAPP) 的网络接
<i>rsn_preauth</i>	布尔	没有	0	允许对 WPA2-EAP 网络进行预认证 (并宣传)。只有指定的网络接口是桥接才
<i>ieee80211w</i>	整数	没有	0	启用 MFP (802.11w) 支持 (0 =禁用，有驱动程序不支持
<i>ieee80211w_max_timeout</i>	整数	没有	(<i>hostapd</i> 默认)	指定 802.11w 关联 SA 查询最大超时。
<i>ieee80211w_retry_timeout</i>	整数	没有	(<i>hostapd</i> 默认)	指定 802.11w 关联 SA 查询重试超时。
<i>maxassoc</i>	整数	没有	(<i>hostapd / driver</i> 默认)	指定要连接的最大客户端数。
<i>MACADDR</i>	MAC地址	没有	(<i>hostapd / driver</i> 默认)	覆盖用于 WiFi 接口的 MAC 地址。
<i>dtim_period</i>	整数	没有	2 (<i>hostapd</i> 默认)	设置 DTIM (发送交通信息消息) 期间个 DTIM 。这可以设置在1到255之间。有影响。

<i>short_preamble</i>	布尔	没有	1	设置可选使用短前导码
<i>max_listen_int</i>	整数	没有	65535 (<i>hostapd</i> 默认)	设置最大允许STA (客户端) 监听间隔值的监听间隔关联, 则关联将被拒绝。 <i>ifaces</i> 有影响。
<i>mcast_rate</i>	整数	没有	(驱动程序默认)	设置固定的组播速率, 以kb / s为单位。
<i>WDS</i>	布尔	没有	0	这设置4地址模式 (http://wireless.kernel.org/en/users/Daddress_for_ap_and_client_mode)

WPA模式

除了WPA模式, 加密选项还指定要使用的组和对等体密码。要覆盖的密码, 的值加密必须在形式给出模式+密码。有关可能的组合, 请参阅下面的列表。如果接口的*hwmode*设置为*ng*或*na*, 则CCMP密码总是添加到列表中。

值	WPA版本	密码
<i>PSK2 + TKIP + CCMP</i>	WPA2个人 (PSK)	TKIP, CCMP
<i>PSK2 + TKIP + AES</i>	WPA2个人 (PSK)	TKIP, AES
<i>PSK2 + TKIP</i>	WPA2个人 (PSK)	TKIP
<i>PSK2 + CCMP</i>	WPA2个人 (PSK)	CCMP
<i>PSK2 + AES</i>	WPA2个人 (PSK)	AES
<i>PSK2</i>	WPA2个人 (PSK)	
<i>PSK TKIP + + CCMP</i>	WPA个人 (PSK)	TKIP, CCMP
<i>PSK TKIP + AES +</i>	WPA个人 (PSK)	TKIP, AES
<i>PSK TKIP +</i>	WPA个人 (PSK)	TKIP
<i>PSK + CCMP</i>	WPA个人 (PSK)	CCMP
<i>PSK AES +</i>	WPA个人 (PSK)	AES
<i>PSK</i>	WPA个人 (PSK)	
<i>PSK混合+ TKIP + CCMP</i>	WPA / WPA2个人 (PSK) 混合模式	TKIP, CCMP
<i>PSK混合+ TKIP + AES</i>	WPA / WPA2个人 (PSK) 混合模式	TKIP, AES
<i>PSK混合+ TKIP</i>	WPA / WPA2个人 (PSK) 混合模式	TKIP
<i>PSK混合+ CCMP</i>	WPA / WPA2个人 (PSK) 混合模式	CCMP
<i>PSK混合+ AES</i>	WPA / WPA2个人 (PSK) 混合模式	AES

<i>PSK</i> 混合	WPA / WPA2个人 (PSK) 混合模式	
<i>WPA2 TKIP + + CCMP</i>	WPA2企业	TKIP, CCMP
<i>WPA2 TKIP + AES +</i>	WPA2企业	TKIP, AES
<i>WPA2 + CCMP</i>	WPA2企业	CCMP
<i>wpa2 + aes</i> '	WPA2企业	AES
<i>WPA2</i>	WPA2企业	
<i>WPA2 TKIP +</i>	WPA2企业	TKIP
<i>WPA TKIP + + CCMP</i>	WPA企业	TKIP, CCMP
<i>WPA TKIP + AES +</i>	WPA企业	TKIP, AES
<i>WPA + CCMP</i>	WPA企业	CCMP
<i>WPA + AES</i>	WPA企业	ES
<i>WPA TKIP +</i>	WPA企业	TKIP
<i>WPA</i>	WPA企业	
<i>WPA-混合+ TKIP + CCMP</i>	WPA / WPA2企业混合模式	TKIP, CCMP
<i>WPA-混合+ TKIP + AES</i>	WPA / WPA2企业混合模式	TKIP, AES
<i>WPA-混合+ TKIP</i>	WPA / WPA2企业混合模式	TKIP
<i>WPA-混合+ CCMP</i>	WPA / WPA2企业混合模式	CCMP
<i>WPA-混合+ AES</i>	WPA / WPA2企业混合模式	AES
<i>WPA-混合</i>	WPA / WPA2企业混合模式	

WPA企业 (接入点)

WPA Enterprise的接入点相关选项列表。

名称	默认	描述
服务器	(没有)	RADIUS服务器来处理客户端认证
港口	1812	RADIUS端口
键	(没有)	共享RADIUS密钥
<i>wpa_group_rekey</i>	600	WPA组密码重新密钥间隔 (秒)
<i>auth_server</i>	(没有)	RADIUS认证服务器来处理客户端认证
<i>auth_port</i>	1812	RADIUS认证端口

<i>auth_secret</i>	(没有)	共享认证RADIUS秘密
<i>auth_cache</i>	0	禁用或启用PMKSA和机会密钥缓存
<i>acct_server</i>	(没有)	RADIUS计费服务器处理客户端认证
<i>acct_port</i>	1813	RADIUS计费端口
<i>acct_secret</i>	(没有)	共享会计RADIUS秘密
<i>NASID</i>	(没有)	用于RADIUS身份验证请求的NAS ID
<i>ownip</i>	(没有)	用于RADIUS认证请求的NAS IP地址
<i>dae_client</i>	(没有)	动态授权扩展客户端。该客户端可以发送“Disconnect-Request”或“CoA-Request”数据包强制断开客户端或更改连接参数。
<i>dae_port</i>	3799	端口动态授权扩展服务器侦听。
<i>dae_secret</i>	(没有)	共享DAE秘密。
<i>dynamic_vlan</i>	0	动态VLAN分配
<i>vlan_naming</i>	1	VLAN命名
<i>vlan_tagged_interface</i>	(没有)	VLAN标签接口
<i>vlan_bridge</i>	(没有)	VLAN Bridge命名方案 - 添加到 https://dev.openwrt.org/changeset/43473/ (https://dev.openwrt.org/changeset/43473/)

WPA企业（客户端）

WPA Enterprise客户端相关选项列表。

名称	默认	描述
<i>eap_type</i>	(没有)	定义要使用的EAP协议，可能的值为EAP-TLS的 <i>tls</i> 和EAP-PEAP的 <i>peap</i> 或 <i>ttls</i>
<i>AUTH</i>	<i>MSCHAPV2</i>	“auth = PAP”/ PAP / MSCHAPV2 - 定义要使用的第2阶段（内部）身份验证方法，仅适用于 <i>eap_type</i> 为 <i>peap</i> 或 <i>ttls</i>
身分	(没有)	认证过程中要发送的EAP身份
密码	(没有)	在EAP认证期间发送的密码
<i>ca_cert</i>	(没有)	指定用于认证的CA证书的路径

<code>client_cert</code> 这	(没有)	指定用于身份验证的客户端证书
<code>priv_key</code>	(没有)	指定用于认证的私钥文件的路径，仅在 <code>eap_type</code> 设置为 <code>tls</code> 时适用
<code>priv_key_pwd</code>	(没有)	解密私钥文件的密码只能与 <code>priv_key</code> 配合使用

警告	当使用WPA Enterprise类型PEAP与Active Directory服务器时，“auth”选项必须设置为“auth = MSCHAPV2”或“auth = PAP”
----	--

选项`auth'auth = MSCHAPV2'`

要么

选项`auth'auth = PAP'`

WPS选项

Wi-Fi保护设置 (http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup)相关选项 列表。

警告	支持WPS由 <code>wpad</code> 和 <code>hostapd-utils</code> 软件包提供。默认包 <code>wpad-mini</code> 还不够。
----	---

警告	只有选择加密PSK / PSK2时，WPS才有可能。
----	----------------------------

名称	类型	需要	默认	描述
<code>wps_config</code>	名单	没有	(没有)	配置方法列表。当前支持的方法是: <code>push_button</code> 。
<code>wps_device_name</code>	串	没有	<i>LEDE AP</i>	用户友好的设备描述; 最多32个字节以UTF-8编码。
<code>wps_device_type</code>	串	没有	6-0050F204-1	主要设备类型。示例: 1-0050F204-1 (计算机/PC), 1-0050F204-2 (计算机/服务器), 5-0050F204-1 (存储/ NAS), 6-0050F204-1 (网络基础设施/ AP)
<code>wps_label</code>	布尔	没有	0	启用标签配置方法。
<code>wps_manufacturer</code>	串	没有	<i>lede-project.org</i>	设备的制造商 (最多64个ASCII (American Standard Code for Information Interchange)字符)。
<code>wps_pushbutton</code>	布尔	没有	0	启用按钮配置方法。
<code>WPS_PIN</code>	串	没有	没有	与WPS-PIN一起使用的PIN (仅在外部注册器模式?)

获取WPS运行所需的最小步骤:

- 将wps_pushbutton'1'添加到配置为/etc / config / wireless中的WPA2-PSK 的配置wifi-iface部分
- opkg更新
- opkg删除wpa2-mini
- opkg安装wpa2 hostapd-utils
- 重启

重新启动后, 您可以手动启动WPS按钮, 而不是按下WPS按钮 (如果它同时作为复位按钮, 则可以比使用该按钮更安全):

```
hostapd_cli wps_pbc
```

使用WPS-PIN时:

- 将配置wps_label'1'添加到配置为/etc / config / wireless中的WPA2-PSK 的配置wifi-iface部分
- opkg更新
- opkg删除wpa2-mini
- opkg安装wpa2 hostapd-utils
- 重启

在重新启动后, 每次站尝试连接时, 都需要向hostapd发送WPS PIN。PIN可能不被多次使用, 因为主动攻击者可以在每次尝试期间恢复一半。“any”关键字可以由hostapd日志中打印的特定站EUIID替换。

```
hostapd_cli wps_pin任何$ PIN码
```

/etc / config / wireless示例需要更好的理解, 如下所示

```
root @ XYZ: ~# cat / etc / config / wireless
...
配置wifi-iface
  选项设备'radio0'
  选项模式'ap'
  选项ssid'My-WiFi-Home'
  选项网络'lan'
  选项加密'psk2'
  选项键“WiFipassword”
  选项ieee80211w'0'
  选项wps_pushbutton'1'
根@ XYZ: ~#
```

快速BSS过渡选项

名称	类型	需要	默认	描述
ieee80211r	布尔	没有	0	启用快速BSS过渡 (802.11r) 支持。
NASID	串	是	(没有)	PMK-R0键盘标识符

				(dot11FTR0KeyHolderID)。1到48个字节标识符。
<i>mobility_domain</i>	串	没有	4f57	移动域标识符 (dot11FTMobilityDomainID, MDID)。MDID用于指示一组AP (在ESS内, 即共享相同的SSID), STA可以在其间使用快速BSS过渡。2字节标识符作为十六进制字符串。
<i>r0_key_lifetime</i>	整数	没有	10000	PMK-RO的默认生命周期 (分钟) [1-65535]。
<i>r1_key_holder</i>	串	没有	00004f577274	PMK-R1键盘标识符 (dot11FTR1KeyHolderID)。六位字节标识符作为十六进制字符串。
<i>reassociation_deadline</i>	整数	没有	1000年	时间单位的关联期限 (TU / 1.024 ms, 1000-65535)
<i>r0kh</i>	串	没有	(没有)	同一移动域中的R0KH列表。有效格式: <MAC地址>, <NAS标识符>, <128位密钥为十六进制字符串>该列表用于将R0KH-ID (NAS标识符) 映射到目标MAC地址, 当从R0KH请求PMK-R1密钥时, 在初始移动域协会期间使用STA。
<i>r1kh</i>	串	没有	(没有)	相同移动域中的R1KH列表。有效格式: <MAC地址>, <R1KH-ID>, <128位密钥作为十六进制字符串>此列表用于在从R0KH发送PMK-R1密钥时将R1KH-ID映射到目标MAC地址。这也是可以请求PMK-R1键的MD中授权的R1KH的列表。
<i>pmk_r1_push</i>	布尔	没有	0	是否在R0KH使能PMK-R1推动。

不活动超时选项

名称	类型	需要	默认	描述
<i>disassoc_low_ack</i>	布尔	没有	1	基于过度传输故障或其他连接丢失指示来拆除站点。这取决于驱动程序的功能, 可能并不适用于所有驱动程序。
<i>max_inactivity</i>	整数	没有	300	站不活动限制 (以秒为单位): 如果站在 ap_max_inactivity 秒内没有发送任何内容, 则会向其发送一个空数据帧, 以便验证它是否仍在范围内。如果此帧未被确认, 则该站将被解除关联然后被去认证。
<i>skip_inactivity_poll</i>	布尔	没有	0	可以禁用不活动轮询以基于不活动超时来断开站, 使得空闲站更可能被断开, 即使它们仍然在AP的范围内。

<code>max_listen_interval</code>	整数	没有	65535	最大允许侦听间隔（允许多少个信标周期STA保持睡眠）。
----------------------------------	----	----	-------	-----------------------------

开始/停止无线

无线接口通过 `wifi` 命令进行升降。要重新启动配置更改后的无线网络，请使用 `wifi`，禁用无线网络，运行无线网络。如果您的平台携带多个无线设备，可以通过将 `wifi` 命令跟随设备名称作为第二个参数来单独启动或运行每个无线设备。注意：`wifi` 命令有一个可选的第一个参数，默认为 `up`，即启动设备。为了使第二个参数确实是第二个参数，必须给出一个第一个参数，它可以是除了 `down` 之外的任何东西。例如启动界面 `wlan2` 问题：`wifi up wlan2`；停止界面：`wifi down wlan2`。如果平台还有 `wlan0` 和 `wlan1`，则这些不会被选择性地停止或启动 `wlan2` 所触及。

重新配置

要重建配置文件，例如安装新的无线驱动程序后，请删除现有的无线配置（如果有），并使用 `wifi config` 命令：

```
rm -f / etc / config / wireless
wifi配置
```

仅802.11n设备的40 MHz信道宽度（高达300 Mbps）

默认最大通道宽度为20MHz，最大速度为150Mbps。将其增加到40MHz将最大理论速度提高到300Mbps。捕获的是，在拥有大量WiFi流量的地区（以及共享相同无线电频率的蓝牙等），40MHz可能会降低您的整体速度。器件在使用40MHz时应检测干扰，并回到20MHz。编辑文件 `/ etc / config / wireless` 中的 `htmode` 选项，然后重新启动WiFi AP以测试各种通道宽度。请注意，选项 `htmode` 应设置为 `HT40 +`（通道1-7）或 `HT40-`（通道5-11）或简称 `HT40`。

DFS /雷达检测

在许多国家，在5GHz频段的部分或所有频道上运行WiFi设备需要雷达检测和DFS（说明）（<http://wifi-insider.com/wlan/dfs.htm>）。如果您根据国家规定在无线配置中定义了需要DFS的通道，那么5GHz无线设备将无法启动，除非固件映像能够提供DFS支持（即包括并启用）。有关Linux实现的更多技术细节可以在这里（<http://wireless.kernel.org/en/developers/DFS>）找到。DFS在Linux中

的工作原理如下：驱动程序检测雷达脉冲并将其报告给nl80211处理信息。如果一系列脉冲与定义的雷达图案中的一个匹配，则将向用户空间应用程序（例如，hostapd）报告，然后通过切换到另一个信道来进行响应。

以下配置选择需要DFS支持的通道104，默认地用国家代码DE表示：

```
配置wifi-device radio0
  选项类型mac80211
  选项通道104
  选项hwmode 11a
  选项路径'pci0000: 00/0000: 00: 00.0'
  选项htmode HT20
  选项国'DE'

配置wifi-iface
  选项设备radio0
  选项网络
  选项模式
  选项ssid lede
  选项加密无
```

您可以检查您的WiFi卡认为必须符合的国家（监管域名）

我会得到

如果有疑问，请仔细检查您的hostapd-phy.conf以确保它包含以下值，并将您的国家/地区代码设置为：

```
COUNTRY_CODE = DE
ieee80211n = 1
ieee80211d = 1
ieee80211h = 1
hw_mode =
```

如果雷达检测工作正常，则DFS频道将显示如下（对于比利时，iw phy1信息输出修整）：

```
频率：
* 5220 MHz [44] (17.0 dBm)
* 5240 MHz [48] (17.0 dBm)
* 5260 MHz [52] (20.0 dBm) (雷达检测)
DFS状态：可用 (2155257秒)
DFS CAC时间：60000 ms
* 5280MHz [56] (20.0dBm) (雷达检测)
DFS状态：可用 (2155257秒)
DFS CAC时间：60000 ms
```


警告	当DFS打开时，在启用接口之前会有延迟（例如在重启后）。在此期间（通常为60秒，由本地注册确定），luci将报告该接口被禁用。该时间段用于检测信道上其他信号的存在（信道可用性检查时间）。可以通过以下方式监视此过程：
----	---

```
logread -f
```

如果您选择需要在您所在国家/地区使用DFS的通道，并启用HT40，则可能会导致**DFS start_dfs_cac**（）失败错误（与logread一起显示）：

```
配置文件: /var/run/hostapd-phy1.conf
wlan1: 接口状态UNINITIALIZED-> COUNTRY_UPDATE
wlan1: 接口状态COUNTRY_UPDATE-> HT_SCAN
wlan1: 接口状态HT_SCAN-> DFS
wlan1: DFS-CAC-START freq = 5680 chan = 136 sec_chan = -1, width = 0, seg0 = 0, seg
1 = 0, cac_time = 60s
DFS start_dfs_cac（）失败, -1
接口初始化失败
wlan1: 接口状态DFS-> DISABLED
wlan1: AP-DISABLED
hostapd_free_hapd_data: 接口wlan1未启动
```

将配置更改为HT20应该解决这个问题。

 最后修改: 2017/03/25 05:32 由kdm6389

除非另有说明，本维基的内容将根据以下许可证获得许可：CC Attribution-Share Alike 4.0 International
(<http://creativecommons.org/licenses/by-sa/4.0/>)