MAISON DE LA LIGUE
SAINT-ASPAIS

Configuration Borne Wi-Fi DD-WRT

VLANs • Bridging • DHCP • Sécurité

Mars 2026 — v1.0

Objectif du document

Ce document décrit la procédure complète de configuration d'une borne Wi-Fi sous firmware DD-WRT dans le cadre du projet réseau de la Maison de la Ligue Saint-Aspais. La borne est connectée au switch SF-500 et gère deux réseaux sans fil séparés (INVITE et PERMANENT) via des VLANs distincts.

1. Prérequis & Topologie

1.1 Prérequis réseau

Avant de commencer la configuration de la borne DD-WRT, les éléments suivants doivent être en place :

- VLANs 10 à 14 et 99 configurés sur le switch SF-500
- Routes inter-VLAN opérationnelles
- Port du SF-500 connecté à la borne configuré en trunk
- Adresse IP 10.10.30.2 / 255.255.255.248 assignée au port du SF-500

> ⚠ **Note :** *Réinitialiser la borne Wi-Fi (appui 30 sec sur Reset) avant de commencer la configuration.*

1.2 Configuration SF-500 (côté port borne)

Extrait de la configuration de l'interface fastethernet1/2/12 du SF-500 :

```
interface fastethernet1/2/12
  ip address 10.10.30.1 255.255.255.248
  switchport trunk allowed vlan add 10-14,99
```

1.3 Plan d'adressage

Réseau / Interface	Adresse IP	Masque	Rôle
Borne (LAN)	10.10.30.2	255.255.255.248	Adresse locale de la borne
SF-500 (trunk)	10.10.30.1	255.255.255.248	Passerelle de la borne
Passerelle par défaut	10.10.30.1	—	Gateway vers le réseau
Serveur DHCP/DNS	172.16.2.245	—	DHCP Forwarder cible
VLAN 13 (INVITE)	Bridge br13	—	Réseau invités Wi-Fi
VLAN 14 (PERMANENT)	Bridge br14	—	Réseau permanent Wi-Fi

2. Configuration Initiale de la Borne

2.1 Accès à l'interface d'administration

Se connecter via navigateur à l'adresse par défaut de la borne :

Paramètre	Valeur
URL d'accès	http://192.168.1.1
Login	root
Mot de passe	admin

2.2 Configuration WAN

La borne n'étant pas directement connectée à Internet, il faut :

1. Aller dans **Setup → Basic Setup**
2. Mettre **WAN Connection Type** sur **Disabled**
3. Cocher **Assign WAN Port to Switch** dans la section WAN Port

> ⚠ **Note :** *Cette option intègre le port WAN dans le switch, permettant d'utiliser tous les ports physiques pour le réseau local.*

2.3 Adressage IP de la borne

Dans Setup → Basic Setup, section Network Setup :

Paramètre	Valeur à saisir
Local IP Address	10.10.30.2
Subnet Mask	255.255.255.248
Gateway	10.10.30.1
Local DNS	0.0.0.0
Router Name	Wireless Ligue

2.4 Mode de fonctionnement

La borne doit fonctionner en mode Routeur (et non Gateway) :

- Aller dans Setup → Advanced Routing
- Changer Operating Mode de Gateway vers Routeur
- Interface : Désactiver

> ⚠ **Note :** *La borne n'est pas la passerelle finale du réseau — le SF-500 joue ce rôle.*

3. Configuration Sans Fil (SSID)

3.1 Interface physique wl0

Dans Wireless → Basic Settings, configurer l'interface physique :

Paramètre	Valeur
Wireless Mode	AP
Wireless Network Mode	Mixed
SSID (physique)	dd-wrt
Wireless Channel	6 - 2.437 GHz
Wireless SSID Broadcast	Disable (désactivé)
Network Configuration	Bridged

> ⚠ **Note :** *Le SSID physique doit être désactivé. Seules les interfaces virtuelles seront visibles des utilisateurs.*

3.2 Interfaces virtuelles

Créer deux interfaces virtuelles en cliquant sur Add Virtual AP :

Interface	SSID	Broadcast	AP Isolation	Network Config
wl0.1	INVITE_Vlan	Enable	Disable	Bridged
wl0.2	PERMANENT_Vlan	Enable	Disable	Bridged

3.3 Sécurité Wi-Fi

Dans Wireless → Wireless Security, configurer chaque interface :

Interface	Security Mode	WPA Algorithms	Key Renewal (s)
wl0 (physique)	Disabled	—	—
wl0.1 (INVITE)	WPA2-PSK	TKIP	3600
wl0.2 (PERMANENT)	WPA2-PSK	TKIP	3600

> ⚠ **Note :** *Définir le WPA Shared Key pour chaque interface virtuelle. Utiliser des mots de passe différents pour INVITE et PERMANENT.*

4. Configuration des VLANs

4.1 Accès à la configuration VLAN

Dans Setup → VLANs, associer les VLANs aux interfaces physiques :

4.2 Tableau de configuration VLAN

VLAN	Port W	Port 1	Port 2	Port 3	Port 4	Bridge
0	—	✓	✓	✓	✓	LAN
1	✓	—	—	—	—	LAN
13	✓	✓	—	—	—	None
14	✓	✓	—	—	—	None
Tagged	✓	✓	—	—	—	—

> ⚠ **Note :** *Cocher 'Tagged' sur les ports W et 1 pour que les requêtes soient taguées avec les numéros de VLAN.*

5. Configuration du Bridging

5.1 Création des bridges

Dans Setup → Networking, section Create Bridge :

Bridge	Nom interne	STP	MTU	Rôle
br0	Bridge 0	Off	1500	Bridge principal (LAN)
br13	Bridge 13	STP On	1500	Réseau INVITE (VLAN 13)
br14	Bridge 14	STP On	1500	Réseau PERMANENT (VLAN 14)

> ⚠ **Note :** *Le nom affiché 'br1' dans l'interface peut correspondre au Bridge 0 selon les versions de DD-WRT. Vérifier dans Current Bridging Table.*

5.2 Assignation interfaces → bridges

Dans Setup → Networking, section Assign to Bridge :

Assignment	Bridge	Interface	Priorité
Assignment 0	br13	wl0.1	128
Assignment 1	br14	wl0.2	128
Assignment 2	br13	vlan13	128
Assignment 3	br14	vlan14	128

> ⚠ **Note :** *Conserver impérativement les assignements wl0.1 et wl0.2. Les associer également aux VLANs respectifs (vlan13 et vlan14) avec une priorité de 63.*

5.3 Vérification — Current Bridging Table

Bridge Name	STP	Interfaces
br0	no	vlan0 eth1 vlan1
br13	yes	wl0.1 vlan13
br14	yes	wl0.2 vlan14

6. Configuration DHCP

6.1 Paramètres DHCP Forwarder

Dans Setup → Basic Setup, section Network Address Server Settings (DHCP) :

Paramètre	Valeur
DHCP Type	DHCP Forwarder
DHCP Server (adresse du relais)	172.16.2.245

> ⚠ **Note :** *En mode DHCP Forwarder, la borne ne distribue pas elle-même les adresses IP — elle redirige les requêtes DHCP vers le serveur centralisé à 172.16.2.245.*

7. Configuration du Pare-feu

7.1 Règles iptables

Dans Administration → Commands (ou Firewall Scripts), ajouter les règles suivantes :

Ces règles permettent de :

- Rediriger les requêtes des clients Wi-Fi des sous-interfaces vers l'interface physique (POSTROUTING SNAT)
- Autoriser les requêtes DHCP (UDP port 67) sur les bridges br1 et br2
- Autoriser les requêtes DNS (UDP/TCP port 53) sur les bridges br1 et br2

```
iptables -t nat -I POSTROUTING -o 'get_wanface' -j SNAT --to 'nvram get
wan_ipaddr'
iptables -I INPUT -i br1 -p udp --dport 67 -j ACCEPT
iptables -I INPUT -i br2 -p udp --dport 67 -j ACCEPT
iptables -I INPUT -i br1 -p udp --dport 53 -j ACCEPT
iptables -I INPUT -i br1 -p tcp --dport 53 -j ACCEPT
iptables -I INPUT -i br2 -p udp --dport 53 -j ACCEPT
iptables -I INPUT -i br2 -p tcp --dport 53 -j ACCEPT
```

8. Dépannage

8.1 Perte d'accès HTTP

En cas de perte de l'interface web, se connecter via Telnet :

```
nvram set httpd_enable=1
nvram set http_enable=1
nvram commit
httpd -p 80
reboot
```

8.2 Tableau de dépannage rapide

Symptôme	Cause probable	Solution
Borne inaccessible (192.168.1.1)	IP changée ou config corrompue	Reset 30 sec + recommencer depuis 2.1
Pas de DHCP sur Wi-Fi	Bridge ou assignment manquant	Vérifier Section 5.2 + règles firewall 7.1
VLAN non taggé	Case 'Tagged' non cochée	Revoir Section 4.2 (cocher Tagged port W et 1)
Pas de route inter-VLAN	SF-500 non configuré	Vérifier trunk + adresse 10.10.30.2
SSID INVITE invisible	wl0.1 broadcast désactivé	Vérifier Section 3.2 (Enable broadcast)

8.3 Ressources complémentaires

Documentation officielle DD-WRT Multiple WLANs :

```
https://wiki.dd-wrt.com/wiki/index.php/Multiple_WLANs
```

9. Checklist de Vérification Finale

Étape	Action	Statut
1	SF-500 : port trunk configuré + IP 10.10.30.2	☐
2	Borne réinitialisée (reset 30s)	☐
3	WAN Connection Type : Disabled	☐
4	WAN Port : Assign WAN Port to Switch coché	☐
5	IP borne : 10.10.30.1 / 255.255.255.248	☐

6	Gateway : 10.10.30.2	☐
7	Mode fonctionnement : Routeur (non Gateway)	☐
8	SSID physique wl0 désactivé	☐
9	SSID INVITE_Vlan créé (wl0.1)	☐
10	SSID PERMANENT_Vlan créé (wl0.2)	☐
11	WPA2-PSK configuré sur wl0.1 et wl0.2	☐
12	VLAN 13 et 14 : port W+1 cochés + Tagged	☐
13	Bridges br13 et br14 créés	☐
14	Assignments : wl0.1→br13, wl0.2→br14, vlan13→br13, vlan14→br14	☐
15	DHCP Forwarder pointant sur 172.16.2.245	☐
16	Règles iptables firewall appliquées	☐
17	Test de connectivité Wi-Fi INVITE et PERMANENT	☐