Mode Opératoire

Gestion des VLANs sur switches Aruba Instant On 1930

Code :	MO-NET-003
Version :	1.2
Date :	10 septembre 2026
Auteur :	Cédric LEGRAND
Classification :	USAGE INTERNE — Équipe BTS SIO

Historique des révisions

Version	Date	Modifications
1.0	06/05/2026	Création initiale
1.1	26/06/2026	Harmonisation de la présentation des étapes et des encadrés.
1.2	10/09/2026	Application de la procédure aux VLANs 240/241 du Wi-Fi pédagogique : création des VLANs sur les six commutateurs Aruba et le cœur HP 1920G, marquage *tagged* des trunks bornes → pare-feu. Détail des ports et de l'architecture résultante dans le MO-NET-008.

1 Objet

Ce mode opératoire décrit la procédure de création, de configuration et d'affectation des VLANs sur les switches Aruba Instant On 1930 de l'infrastructure BTS SIO du lycée Jean Lurçat. Il couvre l'accès à l'interface web d'administration, la création d'un VLAN, l'affectation des ports en mode *access* ou *trunk*, ainsi que la configuration des liaisons inter-switches et vers le pare-feu OPNsense.

L'état initial du parc est le suivant : les six switches sont configurés avec un seul VLAN (VLAN 1, *Default*), l'ensemble des ports étant en mode *untagged* sur ce VLAN. La segmentation du réseau en VLANs constitue un préalable au routage inter-VLAN documenté dans le MO-NET-004.

2 Champ d'application

Public concerné	Administrateurs de l'infrastructure BTS SIO
Équipements	6 switches Aruba Instant On 1930 (24 ports)
Protocole	HTTPS (serveur web GoAhead intégré)
Authentification	Compte `admin` local (gestionnaire de mots de passe)
Durée estimée	20–30 minutes par switch

Modèle	Référence	Adresse IP	Firmware
1930 24G PoE 195W	JL683B	`10.0.112.221`	2.8.0.0
1930 24G	JL682A	`10.0.112.222`	2.8.0.0
1930 24G	JL682A	`10.0.112.223`	2.6.0.0
1930 24G PoE 195W	JL683B	`10.0.112.224`	2.8.0.0
1930 24G PoE 195W	JL683B	`10.0.112.225`	2.8.0.0
1930 24G	JL682A	`10.0.112.226`	2.9.0.0

3 Prérequis

Prérequis

— **Accès réseau au switch cible : `https://10.0.112.22x` (RJ45 sur site ou VPN WireGuard)**
— **Identifiants du compte `admin` local (gestionnaire de mots de passe de l'équipe)**
— **Plan d'adressage VLAN validé : identifiant numérique, nom, ports concernés**
— **Savoir quel port physique est relié au pare-feu OPNsense et lesquels assurent les liaisons inter-switches**
— **Navigateur web récent (le certificat auto-signé devra être accepté)**

Risque de perte d'accès

Une erreur de configuration VLAN peut entraîner la perte immédiate de l'accès réseau au switch. Avant toute modification, identifier le port par lequel on est connecté et s'assurer qu'il restera sur le VLAN de gestion (VLAN 1). En cas de perte d'accès, un *reset* physique du switch sera nécessaire.

4 Procédure

4.1 Connexion à l'interface d'administration

1 Se connecter à l'interface web du switch

Ouvrir un navigateur et accéder à l'adresse du switch cible :

```
https://10.0.112.221
```

Le navigateur affiche un avertissement de certificat (certificat auto-signé GoAhead). Accepter l'exception de sécurité pour poursuivre.
Sur la page de connexion, saisir :
— ***Username*** **:** `admin`

— ***Password*** **: le mot de passe stocké dans le gestionnaire de mots de passe**

Cliquer sur Log In. Le tableau de bord (*Dashboard*) s'affiche après authentification.

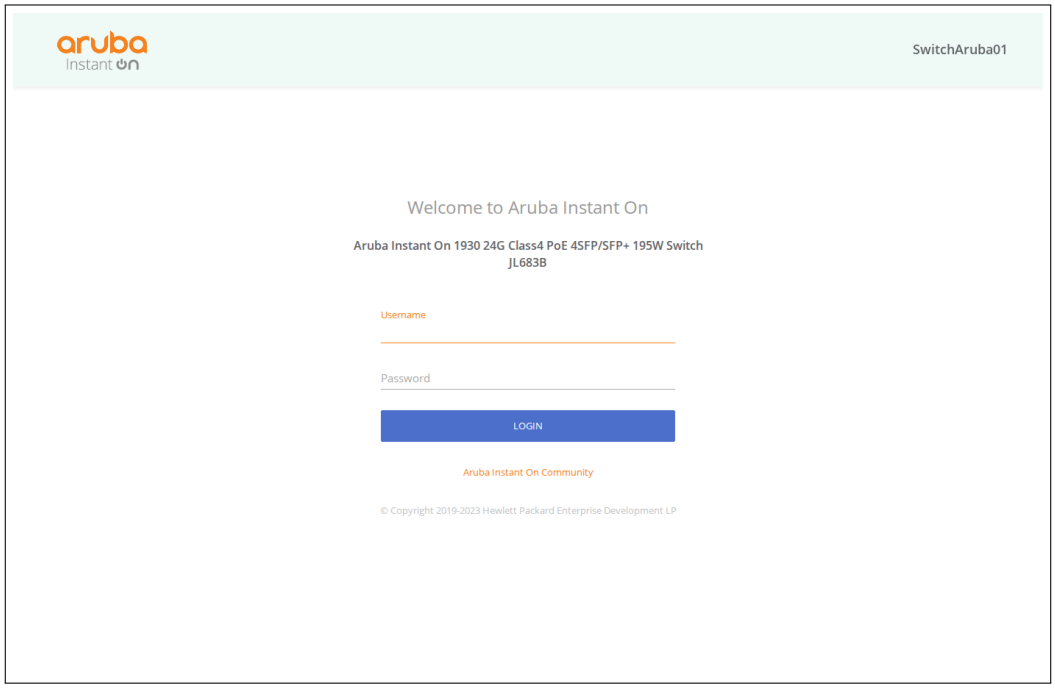


Figure 1 : Page de connexion de l'interface web Aruba Instant On 1930 (GoAhead-Webs, HTTPS).

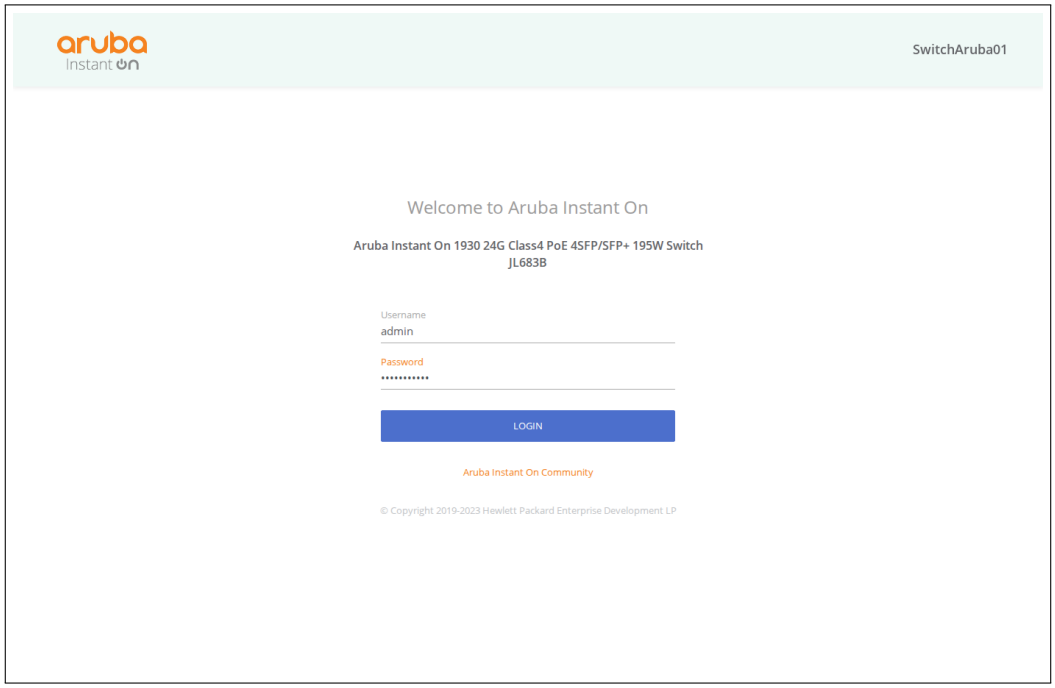


Figure 2 : Formulaire de connexion rempli avec le compte `admin` : modèle JL683B (24G PoE 195W), hostname *SwitchAruba01*.

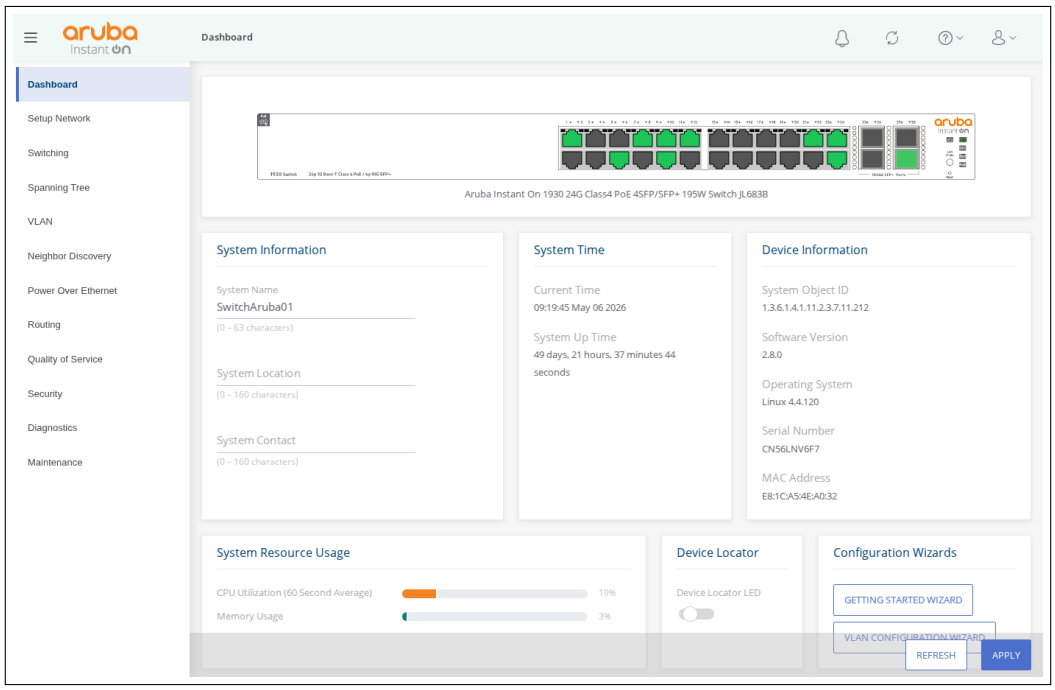


Figure 3 : Tableau de bord après connexion : informations système, état des ports et statistiques générales.

Mode d'administration local

Les switches sont configurés en mode local (*not cloud-managed*). Toute la gestion se fait via l'interface web intégrée. Il n'est pas nécessaire de disposer d'un compte Aruba Central.

4.2 Accéder à la page de configuration VLAN

2 Naviguer vers la configuration VLAN

Dans le menu latéral gauche, déplier la section VLAN puis cliquer sur VLAN Configuration.

La page affiche :

- **La liste des VLANs existants (par défaut, seul le VLAN 1 *Default* est présent)**
- **Le tableau d'appartenance des ports (*VLAN Membership*) : pour chaque port, l'état *Tagged*, *Untagged* ou *Excluded***

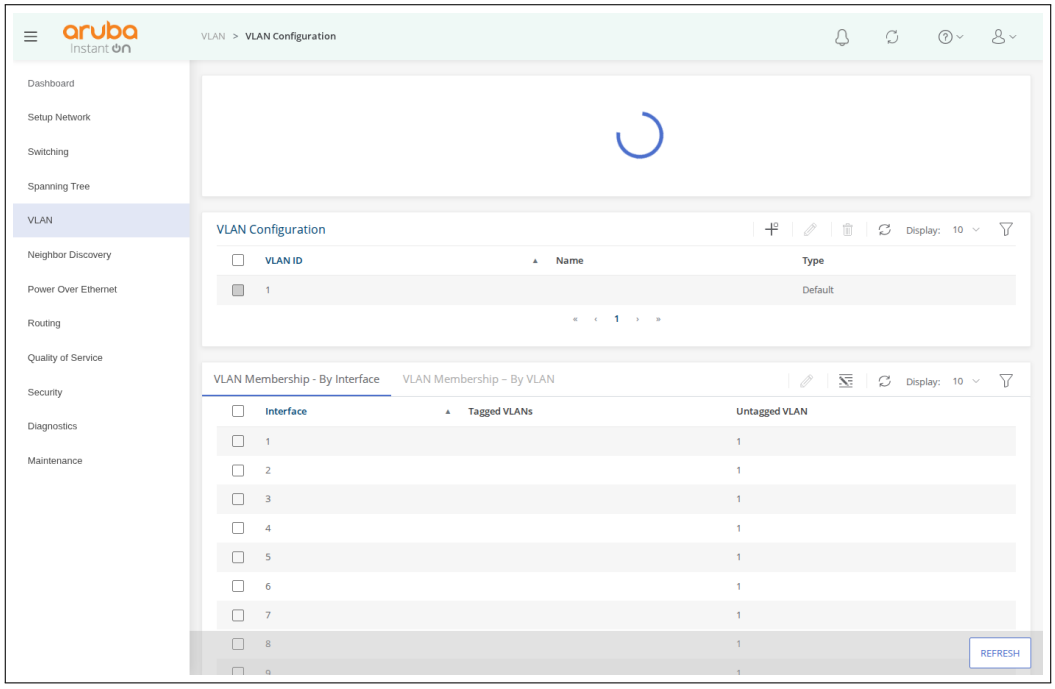


Figure 4 : Page **VLAN → VLAN Configuration** : le VLAN 1 (*Default*) est le seul VLAN configuré. Tous les ports sont en mode *Untagged*.

4.3 Créer un VLAN

3 Ajouter un nouveau VLAN

Depuis la page VLAN Configuration :

1. **Cliquer sur le bouton + (Add) situé au-dessus de la liste des VLANs**
2. **Dans la boîte de dialogue qui apparaît, renseigner :**
   - ***VLAN ID* : l'identifiant numérique du VLAN (ex. `100`)**
   - ***VLAN Name* : un nom descriptif (ex. `Serveurs`)**
3. **Cliquer sur Apply pour valider la création**

Le nouveau VLAN apparaît dans la liste. Par défaut, aucun port ne lui est affecté : tous les ports restent sur le VLAN 1.

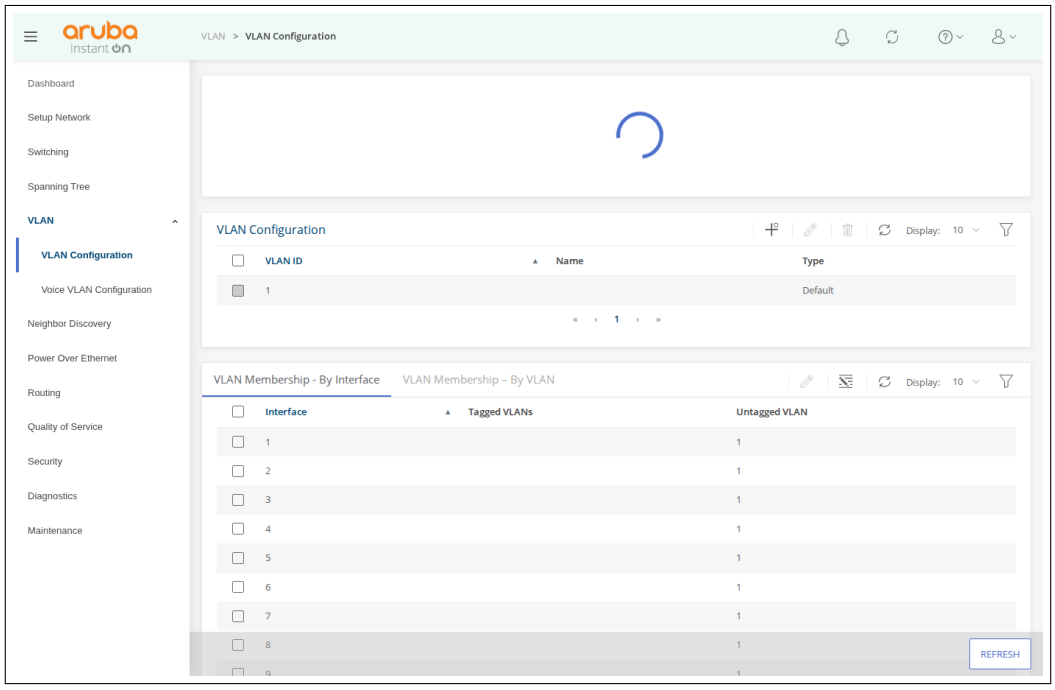


Figure 5 : Boîte de dialogue d'ajout de VLAN : saisir l'identifiant numérique et le nom du VLAN.

Plage d'identifiants VLAN

Les identifiants VLAN valides vont de 2 à 4094. Le VLAN 1 est réservé (*Default*) et ne peut être supprimé. Privilégier un schéma cohérent : par exemple, 100 pour les serveurs, 200 pour les postes pédagogiques, 300 pour l'administration.

4.4 Affecter les ports au VLAN

4

Configurer les ports en mode *access* (accès)

Un port en mode *access* appartient à un seul VLAN et transporte le trafic sans marquage 802.1Q. C'est le mode utilisé pour connecter les postes de travail, les serveurs ou tout équipement terminal. Depuis la page VLAN Configuration, dans la section VLAN Membership :

1. **Sélectionner le VLAN cible dans la liste (ex. VLAN 100 *Serveurs*)**
2. **Pour chaque port à affecter :**
   - **Cliquer sur le port pour faire défiler les états : *Tagged* → *Untagged* → *Excluded***
   - **Sélectionner Untagged (U) pour placer le port dans ce VLAN**
3. **Cliquer sur Apply**

Le port est automatiquement retiré du VLAN 1 en tant qu'*Untagged* : un port ne peut être *Untagged* que sur un seul VLAN à la fois.

Port de gestion

Ne pas retirer du VLAN 1 le port par lequel la connexion d'administration est établie. Si ce port est basculé sur un autre VLAN en *Untagged*, l'accès à l'interface web sera immédiatement perdu. Conserver au moins un port sur le VLAN 1 pour l'administration.

5 Configurer les ports en mode *trunk*

Un port *trunk* transporte plusieurs VLANs simultanément grâce au marquage 802.1Q. C'est le mode requis pour les liaisons inter-switches et pour la connexion vers le pare-feu OPNsense.

Depuis la page VLAN Configuration :

1. **Pour le port trunk, s'assurer que le VLAN 1 reste en Untagged (U) : c'est le VLAN natif (*PVID*)**
2. **Pour chaque VLAN supplémentaire (ex. VLAN 100) :**
   - **Sélectionner le VLAN dans la liste**
   - **Régler le port trunk sur Tagged (T)**
3. **Répéter pour tous les VLANs qui doivent traverser cette liaison**
4. **Cliquer sur Apply**

Le port transporte désormais le VLAN 1 en natif (trames non marquées) et les VLANs ajoutés en *tagged* (trames marquées 802.1Q).

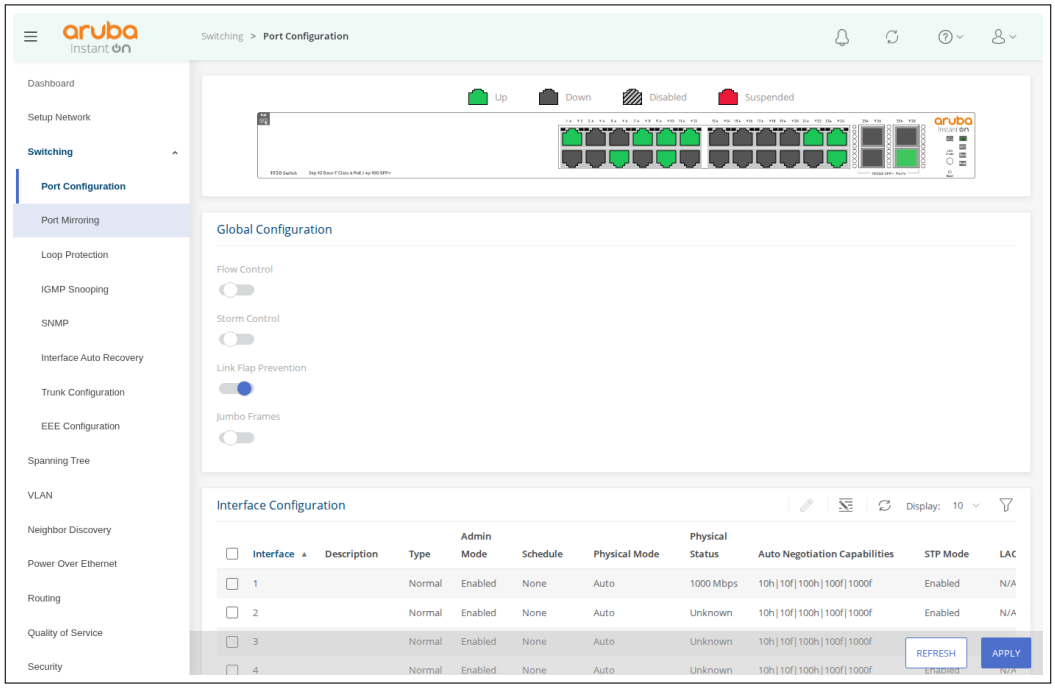


Figure 6 : Page **Port Configuration** : vue d'ensemble des ports avec leur état, vitesse et description.

4.5 Configurer le trunk vers le pare-feu OPNsense

6 Configurer le port uplink vers OPNsense

Le port connecté au pare-feu OPNsense doit transporter l'ensemble des VLANs pour permettre le routage inter-VLAN. La configuration de l'interface OPNsense correspondante est décrite dans le MO-NET-004.

1. **Identifier le numéro du port physique relié au pare-feu**
2. **Sur ce port :**
   - **VLAN 1 : Untagged (PVID, trafic de gestion)**
   - **Chaque VLAN créé (100, 200, 300, . . .) : Tagged**
3. **Cliquer sur Apply**

Vérification rapide

Depuis l'interface OPNsense, naviguer vers Interfaces → VLANs. Les sous-interfaces VLAN créées sur le port physique connecté au switch doivent recevoir du trafic. En cas de problème, capturer le trafic sur l'interface parente avec `tcpdump` pour vérifier la présence des tags 802.1Q.

4.6 Configurer les trunks inter-switches

7 Configurer les liaisons entre switches

Les ports reliant les switches entre eux doivent transporter tous les VLANs pour assurer la connectivité de bout en bout. La configuration doit être identique à chaque extrémité de la liaison. Sur chaque port inter-switch :

1. **VLAN 1 : Untagged (PVID)**
2. **Tous les VLANs créés : Tagged**

Répéter cette opération sur les deux switches à chaque extrémité du câble, puis cliquer sur Apply sur chaque switch.

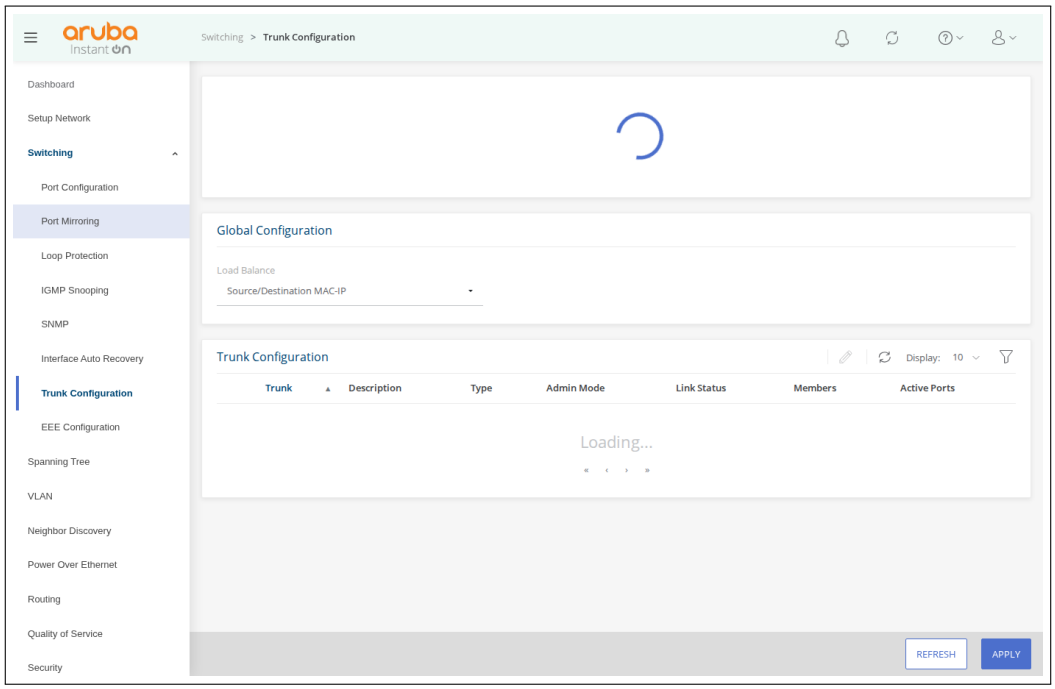


Figure 7 : Page **Trunk Configuration** : regroupement de ports physiques en agrégat (LAG). À ne pas confondre avec le mode trunk 802.1Q — ici il s'agit d'agrégation de liens.

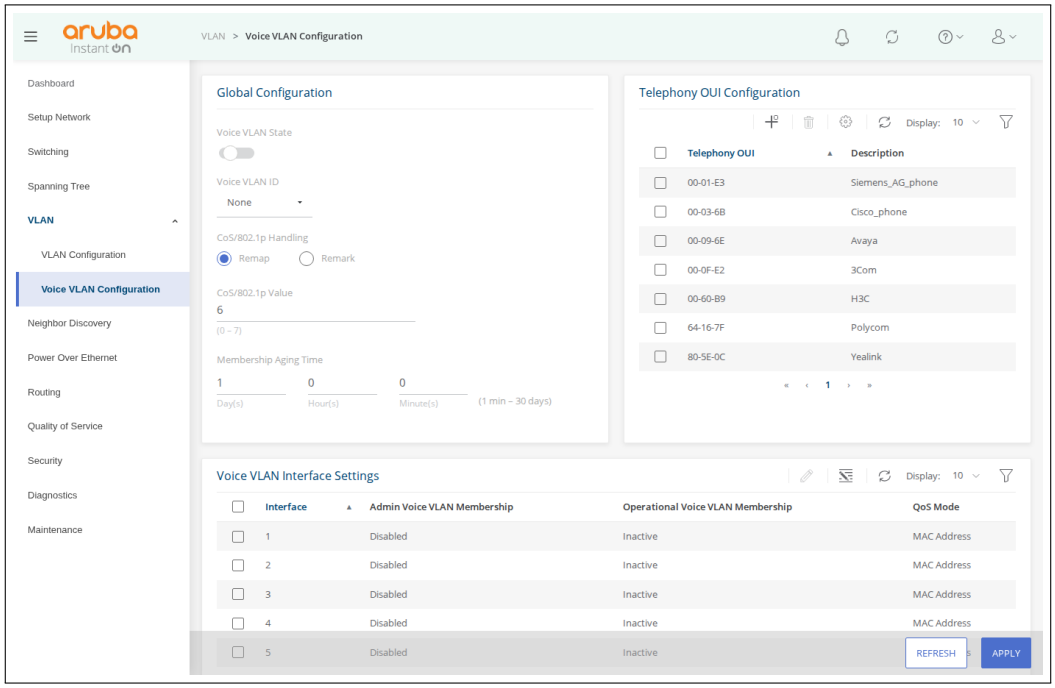


Figure 8 : Page **Voice VLAN Configuration** : configuration du VLAN voix avec détection OUI des téléphones IP (Siemens, Cisco, Avaya, Polycom, Yealink). Fonctionnalité non utilisée dans l'infrastructure actuelle.

Trunk 802.1Q versus agrégation LAG

L'interface Aruba utilise le terme *Trunk* dans deux contextes distincts :

- **VLAN trunk (802.1Q) : un port qui transporte plusieurs VLANs avec marquage. Se configure dans VLAN Configuration via les états *Tagged* / *Untagged*.**
- **Link Aggregation (LAG) : regroupement de ports physiques pour augmenter le débit ou la redondance. Se configure dans Trunk Configuration.**

Ne pas confondre ces deux notions. La présente procédure traite du trunk 802.1Q.

4.7 Sauvegarder la configuration

8 **Sauvegarder la configuration en mémoire persistante**

Après chaque modification, une bannière de notification apparaît en haut de l'interface pour signaler que la configuration en cours d'exécution (*running-config*) diffère de la configuration sauvegardée (*startup-config*).

1. **Cliquer sur le bouton Save Configuration dans la bannière de notification**
2. **Attendre la confirmation : le message de notification disparaît une fois la sauvegarde terminée**

Sauvegarde obligatoire

Sans sauvegarde explicite, les modifications seront perdues au prochain redémarrage du switch. Après un redémarrage involontaire (coupure de courant, par exemple), le switch reviendra à la dernière configuration sauvegardée. Vérifier systématiquement que la bannière de notification a disparu avant de passer au switch suivant.

5 Vérification

Vérification

Après la configuration de chaque switch, valider les points suivants :

VLANs créés

- ☐ **Les VLANs apparaissent dans la liste VLAN Configuration avec le bon identifiant et le bon nom**
- ☐ **Le VLAN 1 (*Default*) est toujours présent et non modifié**

Ports *access*

- ☐ **Les ports terminaux sont *Untagged* sur le VLAN cible et *Excluded* des autres VLANs**
- ☐ **Un équipement connecté à un port *access* obtient une adresse IP dans le bon sous-réseau (si DHCP configuré)**

Ports *trunk*

- ☐ **Le port vers OPNsense est *Untagged* sur VLAN 1 et *Tagged* sur tous les autres VLANs**
- ☐ **Les ports inter-switches sont configurés de manière identique aux deux extrémités**
- ☐ **Le trafic *tagged* arrive correctement sur le pare-feu (vérifiable via `tcpdump` côté OPNsense)**

Accès de gestion

- ☐ **L'interface web de chaque switch reste accessible après les modifications**
- ☐ **Au moins un port par switch est *Untagged* sur le VLAN 1 (gestion)**

Cohérence du parc

- ☐ **Les six switches ont la même liste de VLANs créés**
- ☐ **La configuration a été sauvegardée (*startup-config*) sur chaque switch**

6 Dépannage

Problème	**Solution**
Perte d'accès à l'interface web après modification VLAN	Le port d'administration a été retiré du VLAN 1. Se reconnecter physiquement sur un port encore en VLAN 1. Si aucun port n'est accessible, maintenir le bouton *Reset* du switch pendant 5 secondes pour rétablir la configuration usine.
Un poste ne communique pas malgré le bon VLAN	Vérifier que le port est bien en *Untagged* (et non *Tagged*) sur le VLAN du poste. Un poste de travail standard n'interprète pas les tags 802.1Q.
Le trafic ne traverse pas la liaison inter-switches	Vérifier que le VLAN est *Tagged* sur le port trunk à **chaque extrémité** de la liaison. Un oubli sur un seul côté suffit à bloquer le trafic pour ce VLAN.
OPNsense ne voit pas le trafic d'un VLAN	Vérifier que le VLAN est *Tagged* sur le port uplink du switch. Côté OPNsense, vérifier que la sous-interface VLAN existe et est assignée (**Interfaces** → **Assignments**).
Interface légèrement différente sur le switch `.223`	Ce switch utilise un firmware plus ancien (2.6.0.0 contre 2.8.0.0 ou 2.9.0.0 pour les autres). Les fonctionnalités VLAN sont identiques, mais l'agencement des menus ou le libellé de certains boutons peuvent varier. Privilégier une mise à jour du firmware pour homogénéiser le parc.
Session expirée pendant la configuration	La session web a une durée de vie limitée. Se reconnecter et vérifier l'état de la dernière modification avant de poursuivre. Les changements appliqués (**Apply**) sont conservés en *running-config* même après expiration de la session.

7 Voir aussi

— **MO-NET-001** — Vérification post-hardening du pare-feu OPNsense (contrôle des règles de filtrage après création de VLANs)
— **MO-NET-002** — Mise à jour du firmware OPNsense
— **MO-NET-004** — Routage inter-VLAN sur OPNsense (complément indispensable : la configuration des sous-interfaces VLAN et du filtrage côté pare-feu pour chaque VLAN créé sur les switches)
— **MO-PLT-017** — Inventaire réseau Netbox (référencement des VLANs et affectation des ports)