

CONFIGURATION D'UNE INFRASTRUCTURE WIFI D'ENTREPRISE SÉCURISÉE



Sommaire

Introduction	3
Schéma	4
VLAN	5
Routeur :	5
Création VLAN :	5
Switch :	7
Configuration VLAN :	7
Vérification	10
Les Cas	11
Contrôleur Wifi	13
Mise en place du contrôleur :	13
Configuration Wifi :	18
Création SSID Invites :	20
Mise en place portail Invites :	22
Mise en place serveur Radius :	25
Création SSID Entreprise_Secure :	28
Sécurité	30
Filtrage inter-VLAN :	30
Journalisation :	33
Supervision	37
Clients connectés :	37
Topologie :	38
Trafic :	39
Appareils :	39

Introduction

Le contrôleur wifi permet de gérer de manière centralisée les bornes WiFi et d'appliquer de manière homogène les mêmes politiques de qualité de service, de sécurité, de filtrage, d'historisation des logs et de noms de SSID. Il est relié au switch afin qu'il accède à la configuration du réseau ainsi qu'à la borne wifi.

Le VLAN est une technologie réseau permettant de créer plusieurs réseaux logiques indépendants sur une même infrastructure physique. Il faudra, dans un premier temps, créer les interfaces VLAN sur le routeur puis les configurer avec les ports sur le switch. Segmenter un réseau est important car il permet d'améliorer la surveillance de l'environnement, d'augmenter les performances, de détecter les problèmes techniques et de renforcer la sécurité.

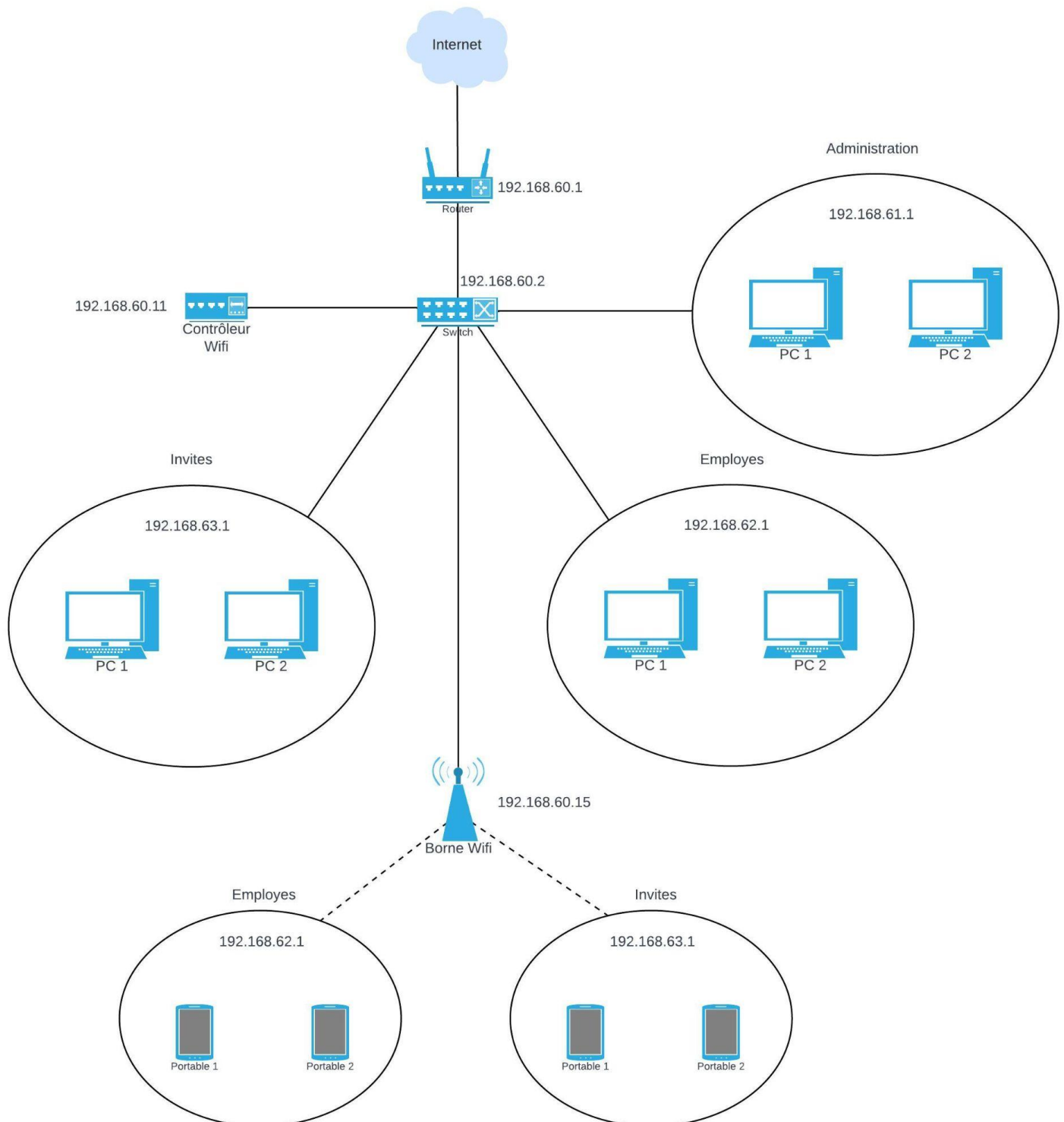
Dans un deuxième temps, il faudra mettre en place le contrôleur wifi avec la création d'un compte administrateur ainsi que la mise à jour du firmware. Ensuite configurer le wifi avec la création de SSID en sélectionnant la sécurité voulue.

Enfin, pour finaliser le tout, il faudra s'occuper de la sécurité de l'infrastructure en changeant les mots de passe, en isolant les clients, en filtrant les VLAN, etc. Cette partie est très importante car elle permet d'éviter de potentielles intrusions et attaques dans le réseau.

Equipements utilisé pour ce guide :

- Switch : Tp-link Omada SG2428P
- Routeur : Tp-link Omada ER605
- Contrôleur : Tp-link Omada controller OC200
- Borne Wifi : Tp-link Omada EAP225-Outdoor
- PC Administrateur

Schéma



VLAN

Routeur :

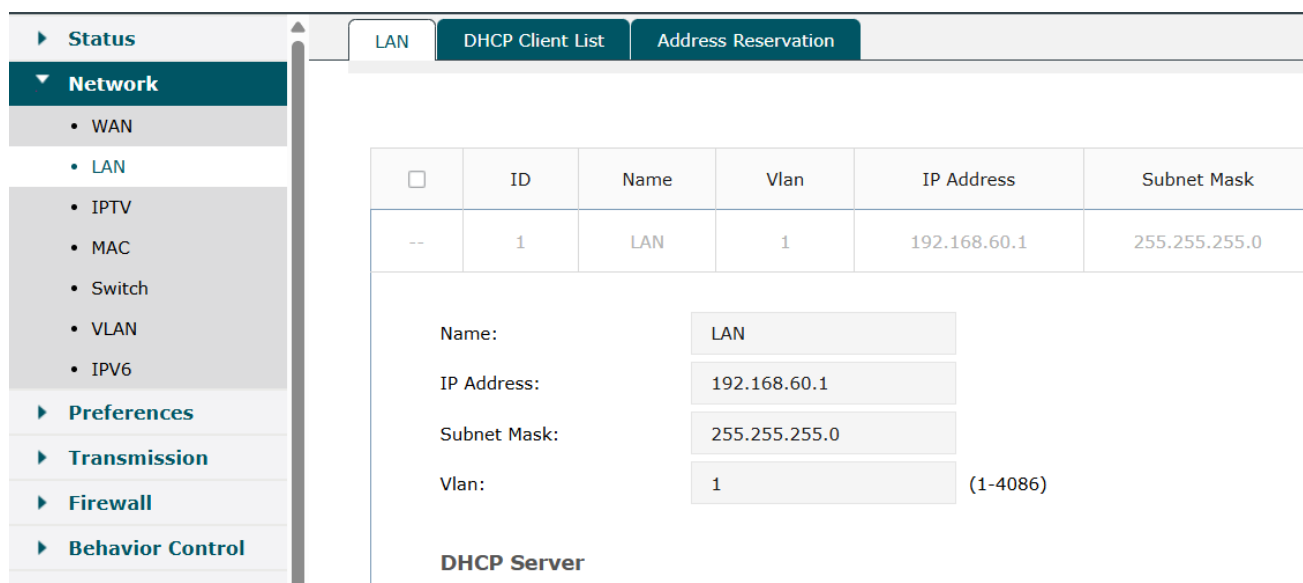
Création VLAN :

Connectez-vous avec un ordinateur au port LAN du routeur avec un câble RJ45 puis rentrez dans le routeur en entrant l'adresse par défaut **192.168.0.1** du routeur dans la barre de recherche. Créer ensuite un nom d'utilisateur et un mot de passe pour vous connecter à l'interface du routeur.



The image shows the TP-Link login page. At the top is the TP-Link logo. Below it, there are two input fields: 'Username' and 'Password'. Underneath these fields are two buttons: 'Log In' and 'Clear'.

Dans l'interface du routeur, allez dans *Network > LAN* puis modifiez l'adresse IP du routeur par **192.168.60.1**.



The image shows the TP-Link router's web interface. On the left is a sidebar menu with options: Status, Network (selected), WAN, LAN, IPTV, MAC, Switch, VLAN, IPV6, Preferences, Transmission, Firewall, Behavior Control, and VPN. The main area has tabs for LAN, DHCP Client List, and Address Reservation. The LAN tab is active, showing a table with one entry:

☐	ID	Name	Vlan	IP Address	Subnet Mask
--	1	LAN	1	192.168.60.1	255.255.255.0

Below the table, there are configuration fields for the selected LAN entry:

- Name: LAN
- IP Address: 192.168.60.1
- Subnet Mask: 255.255.255.0
- Vlan: 1 (1-4086)

At the bottom, there is a section for 'DHCP Server'.

Reconnectez vous en entrant l'adresse IP *192.168.60.1* dans le navigateur puis, toujours dans LAN, ajoutez le VLAN 10 Administration en cliquant sur *add* et entrez les informations renseignées sur l'image. Répété la même manipulation en suivant ces infos :

- **VLAN 20** : Nom : Employes
 Adresse IP = 192.168.62.1
 Plage adresse = 62.10 à 62.30
- **VLAN 30** : Nom : Invites
 Adresse IP = 192.168.63.1
 Plage adresse = 63.10 à 63.30

 **Pour la plage d'adresse IP, entrée toujours une plage IP réduite pour la sécurité et les performances.**

Status

Network

- WAN
- LAN
- IPTV
- MAC
- Switch
- VLAN
- IPv6

Preferences

Transmission

Firewall

Behavior Control

VPN

Authentication

Services

System Tools

Logout

Copyright © 2021

LAN

DHCP Client List

Address Reservation

+ Add

☐	ID	Name	Vlan	IP Address	Subnet Mask	DHCP Server	Operation
☐	1	Administration	10	192.168.61.1	255.255.255.0	Enabled	---

Name:

Administration

IP Address:

192.168.61.1

Subnet Mask:

255.255.255.0

Vlan:

10

(1-4086)

DHCP Server

Status:

☒ Enable

Starting IP Address:

192.168.61.10

Ending IP Address:

192.168.61.30

Lease Time:

120

minutes (1-2880. The default value is 120)

Default Gateway:

(Optional)

Default Domain:

(Optional)

Primary DNS:

(Optional)

Secondary DNS:

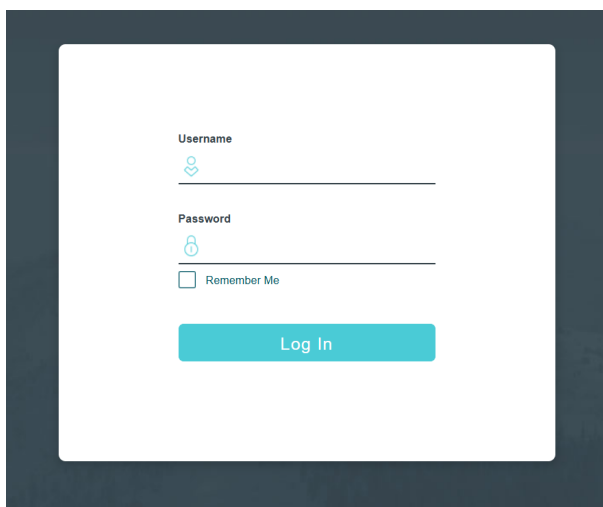
(Optional)

Switch :

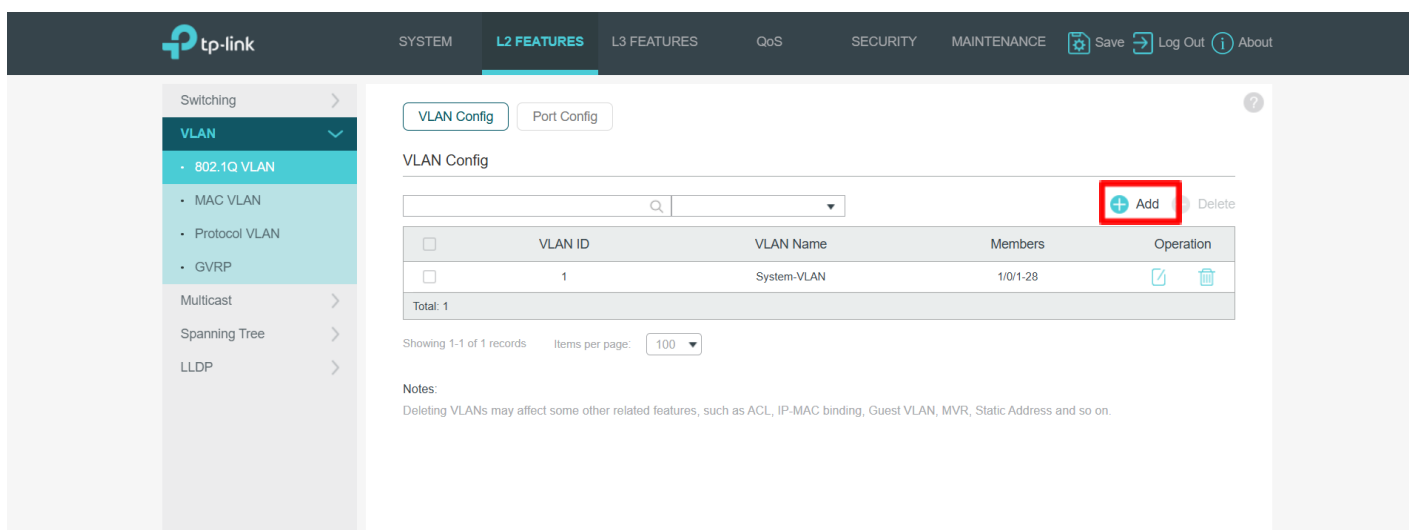
Configuration VLAN :

Pour entrer dans l'interface du switch, il faut se mettre en IP static avec l'adresse *192.168.0.x* (x compris entre 2 et 254) et entrer l'adresse ip *192.168.0.1* dans le navigateur.

Les identifiants pour se connecter sont *admin/admin*.



Dans l'interface du switch, se rendre dans *L2 FEATURES > VLAN > 802.1Q VLAN > VLAN CONFIG* puis cliquer sur *add* pour ajouter le VLAN 10.



Configurer le VLAN 10 en renseignant les infos ci-dessous (sélectionner les ports que vous souhaitez intégrer au VLAN).

The screenshot shows the 'VLAN Config' window. At the top, 'VLAN ID' is set to 10 and 'VLAN Name' is 'Administration'. Under 'Untagged Ports', the 'Port' field contains '1/0/7-12'. Below this is a grid of 28 port icons arranged in two rows of 14. The first row is labeled 'UNIT1' and the second 'LAGS'. Ports 7, 8, 9, 10, 11, and 12 are highlighted in blue, indicating they are selected. A 'Select All' checkbox is on the left. A legend at the bottom shows a blue icon for 'Selected', a white icon for 'Unselected', and a grey icon for 'Not Available'. At the bottom right are 'Cancel' and 'Save' buttons.

 **Et surtout n'oubliez pas de tagué le port qui est câblé au routeur pour chaque Vlan (ici le port 3). Très important car tout le trafic passe par ce port.**

This screenshot shows the 'VLAN Config' window with the 'Tagged Ports' section active. The 'Port' field now contains '1/0/3'. The port grid is the same as in the previous image, but now only port 3 in the first row is highlighted in blue. The 'Select All' checkbox and the legend are still present. The 'Cancel' and 'Save' buttons are at the bottom right.

Répété cette manip pour les 2 autres VLAN en changeant l'ID, le nom et les ports que vous désirez imprégner aux Vlan.

Ensuite, allez dans *Port Config*, sélectionnez les ports du VLAN 10 et modifiez le PVID en ajoutant 10. Cliquez ensuite sur *Apply* pour confirmer les modifications. Faites de même pour le VLAN 20 et 30.

The screenshot shows the 'Port Config' page in the TP-Link web interface. The left sidebar has 'Switching' > 'VLAN' > '802.1Q VLAN' selected. The main area has 'VLAN Config' and 'Port Config' tabs, with 'Port Config' active. Below the tabs, there are 'UNIT1' and 'LAGS' sections. The 'UNIT1' section contains a table with columns: Port, PVID, Ingress Checking, Acceptable Frame Types, LAG, and Details. The table lists ports 1/0/4 through 1/0/13. Ports 1/0/7 through 1/0/12 are selected (checked) and have their PVID set to 10. The 'Apply' button at the bottom right is highlighted with a red box.

Port	PVID	Ingress Checking	Acceptable Frame Types	LAG	Details
1/0/4	1	Enabled	Admit All	---	Details
1/0/5	1	Enabled	Admit All	---	Details
1/0/6	1	Enabled	Admit All	---	Details
1/0/7	10	Enabled	Admit All	---	Details
1/0/8	10	Enabled	Admit All	---	Details
1/0/9	10	Enabled	Admit All	---	Details
1/0/10	10	Enabled	Admit All	---	Details
1/0/11	10	Enabled	Admit All	---	Details
1/0/12	10	Enabled	Admit All	---	Details
1/0/13	20	Enabled	Admit All	---	Details

Total: 28 6 entries selected. Cancel Apply

 **Pour n'importe quelle configuration du switch Tp-link, quand vous avez fini de configurer, pensez toujours à sauvegarder en cliquant sur le bouton Save en haut à droite.**

Vérification

Pour vérifier si tout fonctionne, il est important de faire un *ipconfig* sur chaque post pour voir si le switch a bien attribué la bonne adresse IP au bon VLAN sur chaque poste.

Comme exemple, j'ai mon PC qui est câblé sur le port 9 qui est dans le Vlan 10 (Pour rappel l'adresse IP du Vlan 10 est 192.168.61.1). Je fais une ipconfig et je vérifie si l'adresse IP est bien en 192.168.61.x. Si ce n'est pas le cas, alors je cherche l'erreur que j'ai pu faire dans la configuration des Vlan. Sur l'image, on peut voir que je suis en 192.168.61.10 donc ma config est correcte.

```
C:\Users\Administrateur>ipconfig

Configuration IP de Windows

Carte inconnue OpenVPN Wintun :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::e21f:e5fc:7eb7:c7df%19
    Adresse IPv4. . . . . : 192.168.61.10
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.61.1
```

Aussi, faites des *ping* entre les PC appartenant à un même Vlan et à un Vlan différent pour contrôler la connectivité entre chaque poste.

```
C:\Users\Administrateur>ping 192.168.62.1

Envoi d'une requête 'Ping' 192.168.62.1 avec 32 octets de données :
Réponse de 192.168.62.1 : octets=32 temps<1ms TTL=63
Réponse de 192.168.62.1 : octets=32 temps<1ms TTL=63
Réponse de 192.168.62.1 : octets=32 temps<1ms TTL=63
Réponse de 192.168.62.1 : octets=32 temps<1ms TTL=63

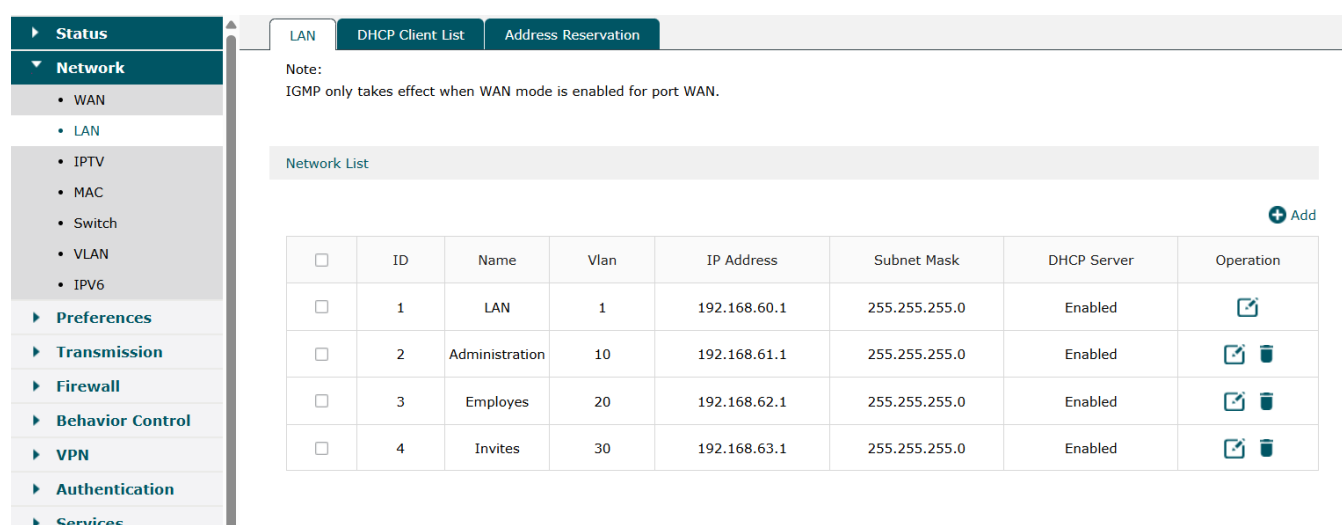
Statistiques Ping pour 192.168.62.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Les Cas

Vous ne pingez aucun poste, ni le routeur, ni le switch ? Pour résoudre ce problème, voici les différents cas possibles avec la solution pour régler le soucis.

1^{er} Cas : Vous avez mal configuré les interfaces Vlan sur le routeur.

Solution : Repasser dans la configuration de chaque interfaces VLAN et essayer de trouver le problème en vous aidant du guide (voir page 6).



The screenshot shows a network configuration interface. On the left is a sidebar menu with categories: Status, Network, Preferences, Transmission, Firewall, Behavior Control, VPN, Authentication, and Services. Under the 'Network' category, there are sub-items: WAN, LAN, IPTV, MAC, Switch, VLAN, and IPV6. The 'LAN' sub-item is selected. The main content area has tabs for 'LAN', 'DHCP Client List', and 'Address Reservation'. The 'LAN' tab is active. Below the tabs, there is a note: 'Note: IGMP only takes effect when WAN mode is enabled for port WAN.' Below the note is a 'Network List' table. The table has columns: ID, Name, Vlan, IP Address, Subnet Mask, DHCP Server, and Operation. There are four rows of data. Each row has a checkbox in the first column. The 'Operation' column contains icons for edit and delete.

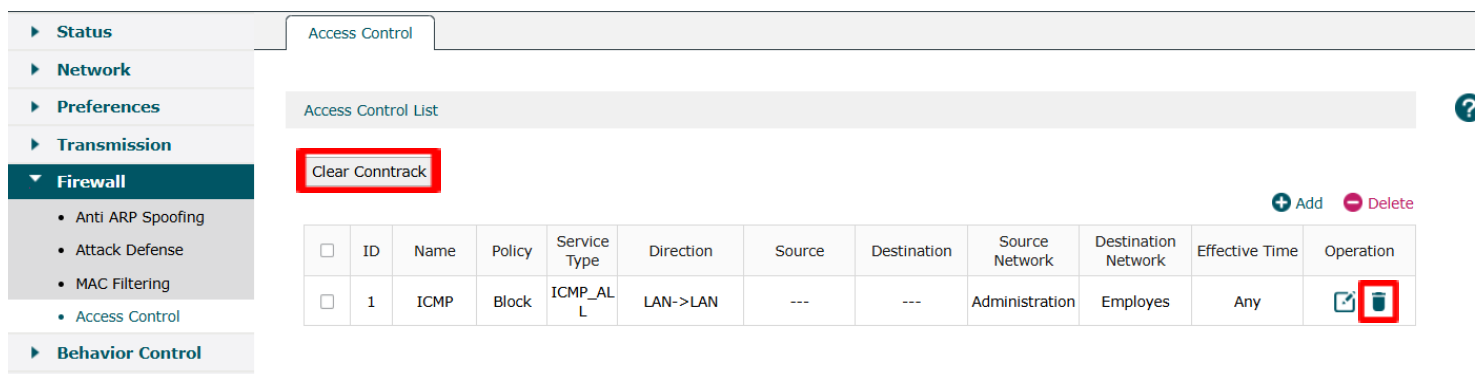
☐	ID	Name	Vlan	IP Address	Subnet Mask	DHCP Server	Operation
☐	1	LAN	1	192.168.60.1	255.255.255.0	Enabled	
☐	2	Administration	10	192.168.61.1	255.255.255.0	Enabled	
☐	3	Employes	20	192.168.62.1	255.255.255.0	Enabled	
☐	4	Invites	30	192.168.63.1	255.255.255.0	Enabled	

2^{eme} Cas : Le câble RJ45 du routeur relié aux switch est défectueux ou mal branché.

Solution : Remettre correctement le câble ou le changer par un autre câble en bon état.

3^{ème} Cas : Une règle ACL bloquant l'ICMP existe peut être entre 2 Vlan.
ICMP (Internet Control Message Protocol) est un protocole de la couche réseau utilisé par les appareils du réseau pour diagnostiquer les problèmes de communication du réseau. C'est grâce à lui que l'on peut ping.

Solution : Supprimer la règle ACL qui bloque l'ICMP. Ici pour un switch tp-link, il suffit de la supprimer et ensuite cliquer sur *Clear Conntrack*.



The screenshot shows the TP-Link web interface. On the left, the 'Firewall' menu is expanded, showing 'Access Control' as the selected option. In the main area, under 'Access Control List', the 'Clear Conntrack' button is highlighted with a red rectangle. Below this, there is a table with columns: ID, Name, Policy, Service Type, Direction, Source, Destination, Source Network, Destination Network, Effective Time, and Operation. The table contains one entry with ID 1, Name ICMP, Policy Block, Service Type ICMP_AL L, Direction LAN->LAN, Source ---, Destination ---, Source Network Administration, Destination Network Employes, Effective Time Any, and Operation with a red trash icon.

ID	Name	Policy	Service Type	Direction	Source	Destination	Source Network	Destination Network	Effective Time	Operation
1	ICMP	Block	ICMP_AL L	LAN->LAN	---	---	Administration	Employes	Any	[Trash Icon]

Exemple du ping du PC admin en 192.168.61.10 vers le PC employes 192.168.62.10 :

```
C:\Users\Administrateur>ping 192.168.62.10

Envoi d'une requête 'Ping' 192.168.62.10 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.62.10:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

4^{ème} Cas : Dans la configuration des Vlan, il y a peut être un port qui est non tagué suite à un oubli.

Solution : Regarder dans l'interface du switch dans quel VLAN le port est censé être non tagué. Sélectionner le port dans le bon VLAN et sauvegarder (voir page 8).

Contrôleur Wifi

Mise en place du contrôleur :

Pour entrer dans l'interface du contrôleur, il faut entrer son adresse IP dans le navigateur, qui est attribué par le switch. Pour le connaître, il suffit de *ping* les adresses IP qui sont dans le VLAN 1 et qui sont compris entre 60.10 et 60.30. Ici, l'adresse du PC est 192.168.60.10 et celle du contrôleur est 192.168.60.11.

Il vous mènera à cette page où il faudra créer un compte administrateur. Vous pourrez lier votre compte Tp-link pour un accès en cloud.



Controller Access

Create an administrator name and password for local login to Omada Controller.

Controller Main Administrator

Administrator Name	
Password	
Confirm Password	
Email	

To enjoy Omada Cloud Service, you can log in and bind your TP-Link ID to your controller.

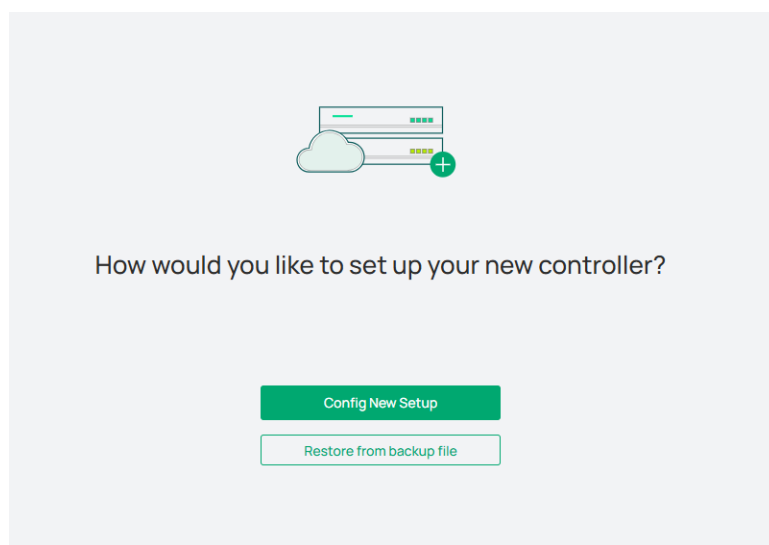
Cloud Access	☒
TP-Link ID	
Password	

No TP-Link ID? [Register now.](#)

Terms

☐ I accept the [Terms of Use](#) and confirm that I have fully read and understood the [Privacy Policy](#).

Ensuite cliquer sur *Config New Setup*.



Ici, vous pourrez modifier le nom du contrôleur ainsi que le pays et l'heure.

1 Omada Setup Wizard — 2 Create Site — 3 Configure Devices — 4 Configure WAN Settings Overrides — 5 Configure Wi-Fi — 6 Summary

Omada Setup Wizard

Controller Name

Controller Country/Region

Controller Time Zone

Controller Update Notification ☒ ⓘ

Join User Experience Improvement Program ☐

By joining this program, you have fully read and understood our [User Experience Improvement Program Policy](#). You can opt out of the program at any time.

Back Next

Crée le site en choisissant le nom, le pays et l'heure et entrer un compte pour l'appareil. Dans *Application Scenario*, choisissez *Office*.

The screenshot shows the 'Create Site' step of the Omada Setup Wizard. The progress bar at the top indicates the current step is 2, 'Create Site', with previous steps marked as complete and subsequent steps as pending.

Create Site

Site Setup

Site Name:

Site Country/Region: France

Site Time Zone: (UTC) Coordinated Universal Time

Switch Series: ☐ Agile (Easy Managed) ☒ Access Series/ Aggregation/ Campus (Smart / L2+ / L3)

Choose your switch series, and the system will adjust switch-related configuration pages accordingly. [Check Switch Categories](#)

Device Account

Username:

Password:

Application Scenario

Select the application scenario depending on your needs. We will guide you configure and optimize the parameters of your network according to your scenario.

☐ Hotel ☐ Restaurant ☒ Office ☐ Factory

Buttons: Back, Skip, Next

Ajouter la borne wifi qui apparaît dans la colonne et cliquer sur next puis sur skip jusqu'à finir la configuration.

The screenshot shows the 'Configure Devices' step of the Omada Setup Wizard. The progress bar at the top indicates the current step is 3, 'Configure Devices', with previous steps marked as complete and subsequent steps as pending.

Configure Devices

Please select the devices you would like to configure.

☐	DEVICE NAME	MODEL	IP ADDRESS	UPTIME
<i>No device to adopt. Please refresh the page.</i>				

Buttons: Back, Skip, Next

Après avoir terminé la configuration de base, connectez-vous avec les identifiants du compte admin ou de votre compte Tp-link.

Contrôleur Omada

 Nom d'utilisateur / ID TP-Link

 Mot de passe 

☐ Se souvenir de moi

Connexion

[Mot de passe oublié ?](#)

Ensuite, vérifier que le contrôleur possède bien la dernière mise à jour. Allez dans *Paramétrage > Les paramètres du système > Mises à jour Contrôleur > Vérifier les mises à jour*.

Omada Controller_F1EB4D

Omada
by tp-link

Vue Globale

Tableau de bord

Modèle de site BETA

Appareils

Journaux

firmware

Comptes

Paramétrages

Adresse MAC

82-E9-3A-71-05-7F

Heure système

Jan 15, 2026 02:54:05 pm

Disponibilité

4h 22m 12s

Mises à jour Contrôleur

Rejoignez le programme d'accès anticipé

☐

Canal de sortie

Écurie

Version Contrôleur

6.0.0.25

Vérifier les mises à jour

Notification de mise à jour de Contrôleur

☒

Certificat HTTPS

Sauvegarder

Annuler

Cliquez sur **Vérifier les mises à jour** pour vérifier et enregistrer les informations du canal de publication.

Vérifier aussi que la borne wifi possède la dernière version du firmware.

Le firmware aide le système d'exploitation (OS) à communiquer avec le matériel et à fournir des instructions pour lui permettre d'effectuer des tâches, il est donc important qu'il possède bien la dernière version sortie.

Allez dans *firmware* > *Mise à niveau unique* et sélectionnez la borne wifi puis mettez la à jour. Si elle possède sa dernière version, dans *Etat du firmware*, il y aura écrit *À jour*.

Vue Globale

Tableau de bord

Modèle de site BETA

Appareils

Journaux

firmware

Aperçu

Mise à niveau unique

Mise à niveau périodique

Télécharger le micrologiciel pour la mise à niveau

Modèle de recherche

Définir la règle de mise à niveau

	MAQUETTE	VERSION ACTUELLE	ÉTAT DU FIRMWARE	ACTION
☐	EAP225-Outdoor(EU) v3.0	5.111 Build 20250401 Rel. 50587	● À jour	

Sélectionnez 0 of 1 items [Tout sélectionner](#)

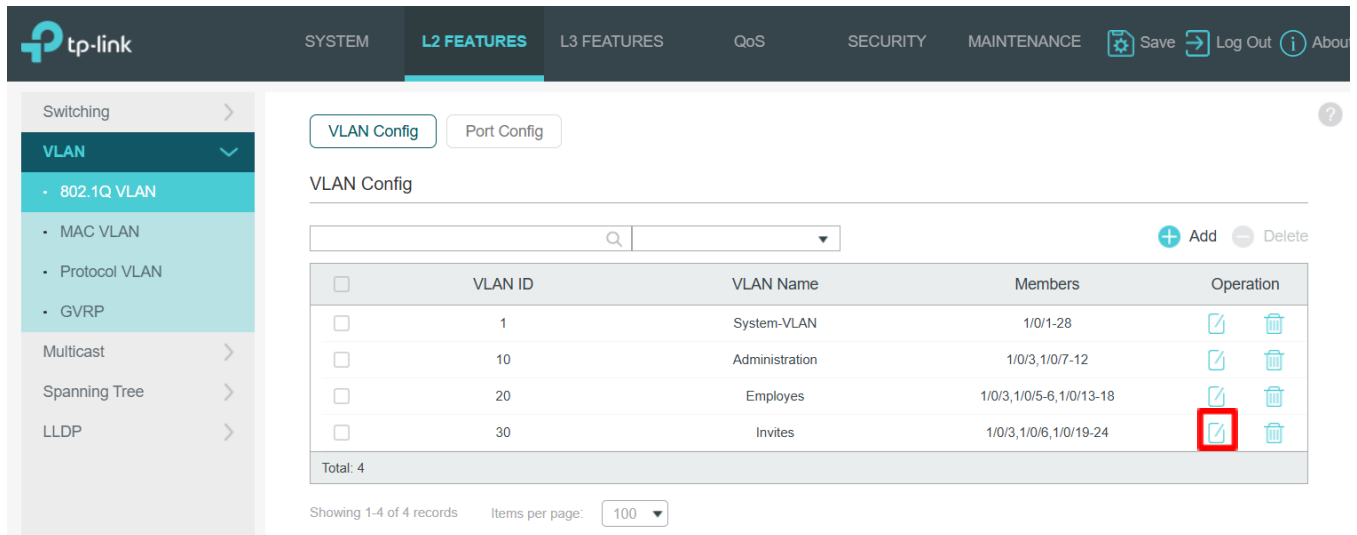
Affichage de 1-1 enregistrements sur 1

< 1 >

10 /page

Configuration Wifi :

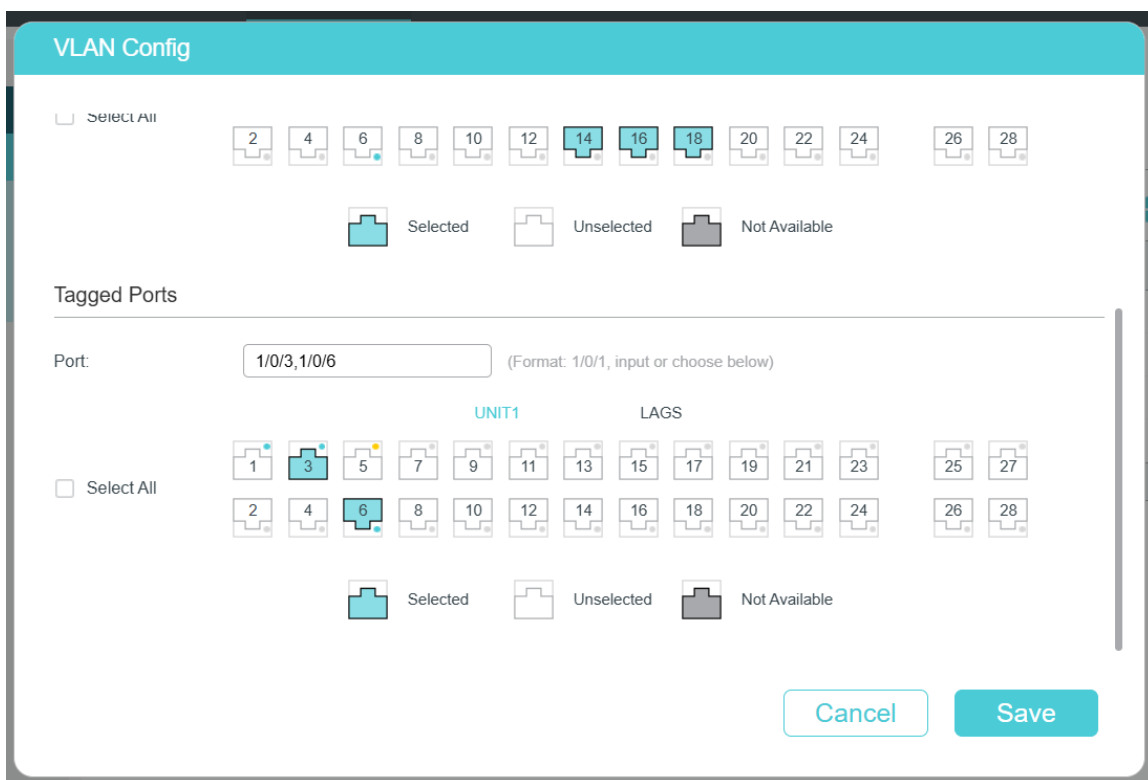
Revenez sur le switch pour taguer le port qui est relié à la borne wifi.
Rendez-vous dans **L2 FEATURES > VLAN > 802.1Q VLAN > VLAN CONFIG** et cliquer sur le logo encadré en rouge sur l'image pour modifier le VLAN 20.



The screenshot shows the TP-Link web interface. The top navigation bar includes 'SYSTEM', 'L2 FEATURES', 'L3 FEATURES', 'QoS', 'SECURITY', and 'MAINTENANCE'. The 'L2 FEATURES' tab is active, and the 'VLAN' sub-tab is selected. The left sidebar shows the 'VLAN' menu with '802.1Q VLAN' selected. The main area displays the 'VLAN Config' page with a table of VLANs. The table has columns for 'VLAN ID', 'VLAN Name', 'Members', and 'Operation'. The 'VLAN 20' row is highlighted with a red box around the edit icon.

VLAN ID	VLAN Name	Members	Operation
1	System-VLAN	1/0/1-28	
10	Administration	1/0/3, 1/0/7-12	
20	Employees	1/0/3, 1/0/5-6, 1/0/13-18	
30	Invites	1/0/3, 1/0/6, 1/0/19-24	

Sélectionner le port qui est relié à la borne wifi dans la catégorie *Tagged Ports* puis sauvegarder. (Ici c'est le port 6)



The screenshot shows the 'VLAN Config' page with the 'Tagged Ports' section. The 'Port' field is set to '1/0/3, 1/0/6'. The 'Tagged Ports' section shows a grid of ports. Port 6 is selected.

Port: (Format: 1/0/1, input or choose below)

UNIT1 LAGS

UNIT1	LAGS
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	10
11	11
12	12
13	13
14	14
15	15
16	16
17	17
18	18
19	19
20	20
21	21
22	22
23	23
24	24
25	25
26	26
27	27
28	28

De retour dans l'interface du contrôleur, changer de site (case rouge) en sélectionnant celui que vous avez créé précédemment puis modifier l'adresse IP de la borne pour la mettre en statique.

Allez dans *Appareils* > *liste d'appareils* et cliquez sur la borne wifi puis, dans la fenêtre qui s'ouvre à droite, cliquez sur *Gérer l'appareil*.

Omada Controller_F1EB4D

liste d'appareils

Rechercher le nom, le SN, le MAC, l'IPv4, le Q

NOM DE L'APPAREIL	ADRESSE IP	STATUT	MAQUETTE
54-AF-97-C6-F9-07	192.168.60.1	EN ATTENDANT	ER7206 v1.0
40-AE-30-34-F9-9D	192.168.60.2	EN ATTENDANT	SG2428P v5.30
98-03-8E-2F-5F-2A	192.168.60.15	CONNECTÉ	EAP225-Outdoor(EI

98-03-8E-2F-5F-2A

CONNECTÉ 5h 50m 50s

Gérer l'appareil

Processeur 1% Mémoire 55%

Aller dans *Configuration* > *Paramètres IP* et sélectionnez comme mode *Statique*. Saisissez les adresses IP renseignées ci-dessous.

98-03-8E-2F-5F-2A

Aperçu Statistiques Journaux Outils Configuration

Général

WiFi

Prestations de service

Paramètres IP

Mode ☐ DHCP ☒ Statique

Adresse IP 192 . 168 . 60 . 15

Masque IP 255 . 255 . 255 . 0

Passerelle 192 . 168 . 60 . 1

Serveur DNS primaire 1 . 1 . 1 . 1

Serveur DNS secondaire 1 . 0 . 0 . 1

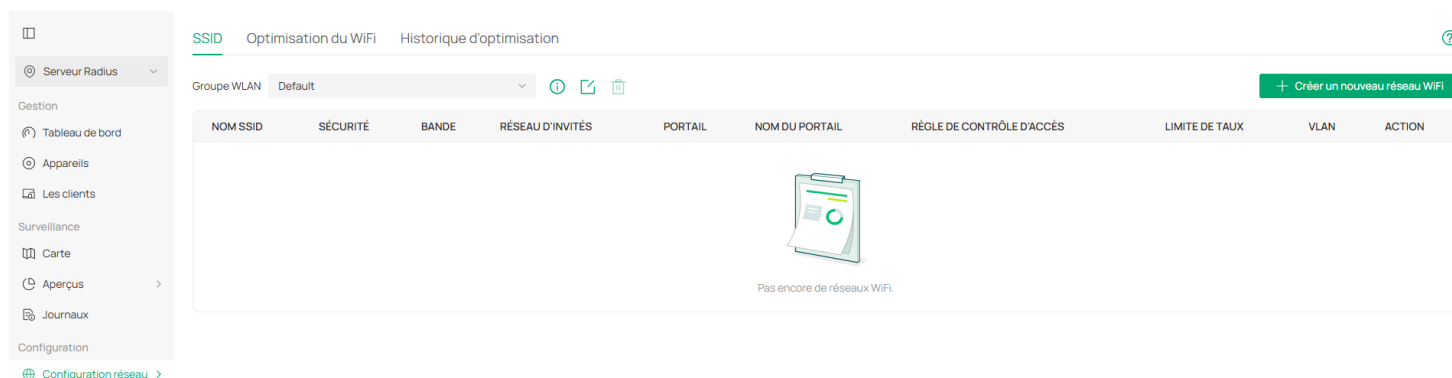
Sauvegarder Annuler

Création SSID Invites :

Le SSID (Service Set Identifier) est le nom d'un réseau WiFi, composé au maximum de 32 caractères alphanumériques. Il permet donc d'identifier le réseau sur lequel vous voulez vous connecter.

Vous allez commencer par configurer le SSID du wifi *Invites*.

Rendez-vous dans *Configuration réseau > Wifi > SSID > Créer un nouveau réseau Wifi*.



Entrer les informations renseignées sur les 2 captures suivantes.

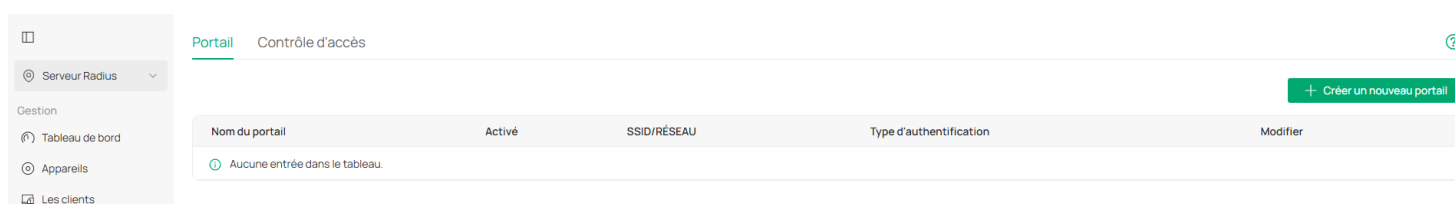
- **Très important d'activer le réseau invités car il empêche les clients sans fil de communiquer entre eux.**
- **Vous allez créer un portail d'authentification juste après, donc pas besoin de mettre de sécurité. Interdire le partage wifi pour augmenter la sécurité.**
- **Limiter aussi le téléchargement et l'upload pour éviter la saturation de la connexion par les clients.**

Mise en place portail *Invites* :

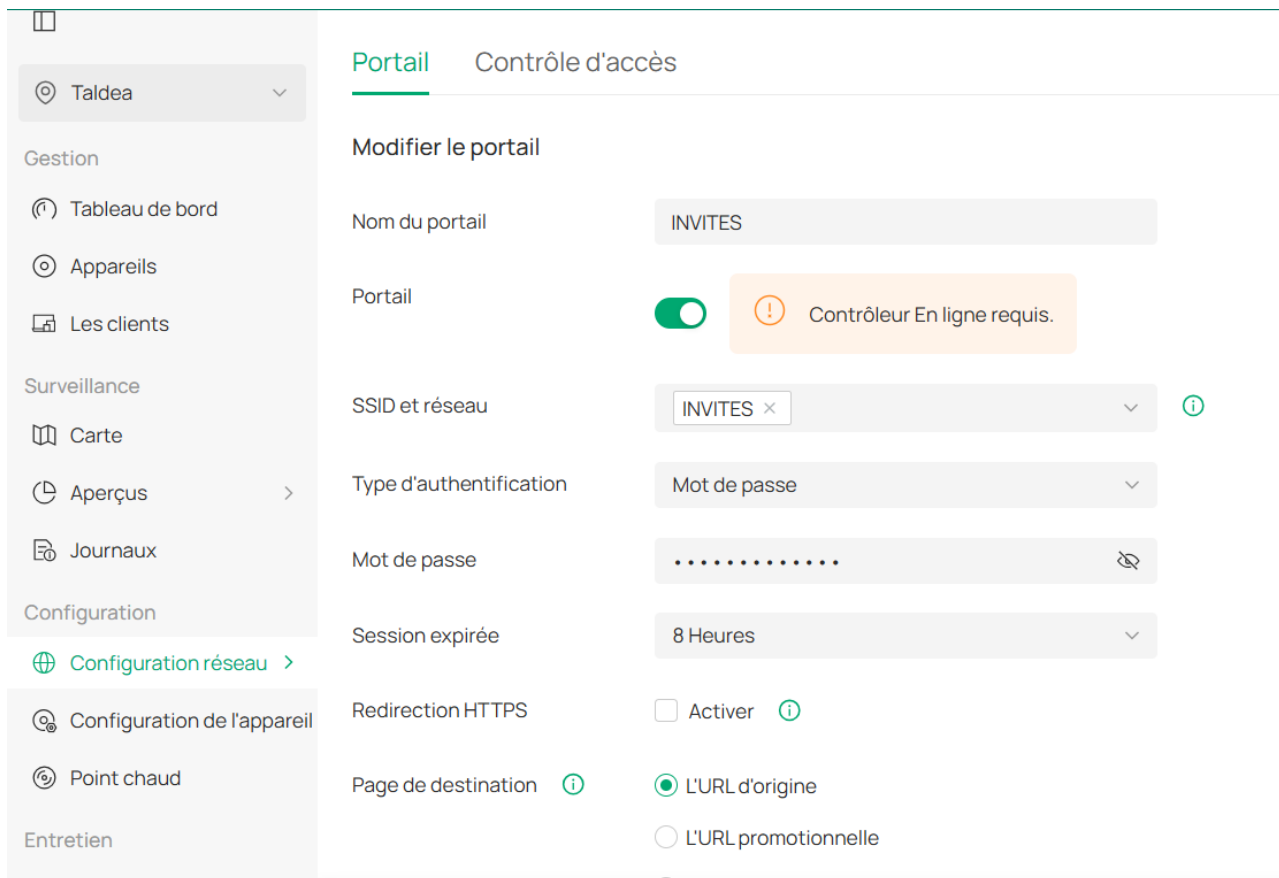
L'authentification du portail fournit un service d'authentification aux clients qui n'ont besoin que d'un accès temporaire au réseau, tels que les clients d'un restaurant ou d'un supermarché. Pour accéder au réseau, ces clients doivent accéder à la page de connexion d'authentification et utiliser les informations de connexion correctes pour réussir l'authentification.

C'est donc un système adapté pour le réseau *Invites*.

Dans *Configuration réseau > Portail*, cliquez sur *Créer un nouveau portail*.



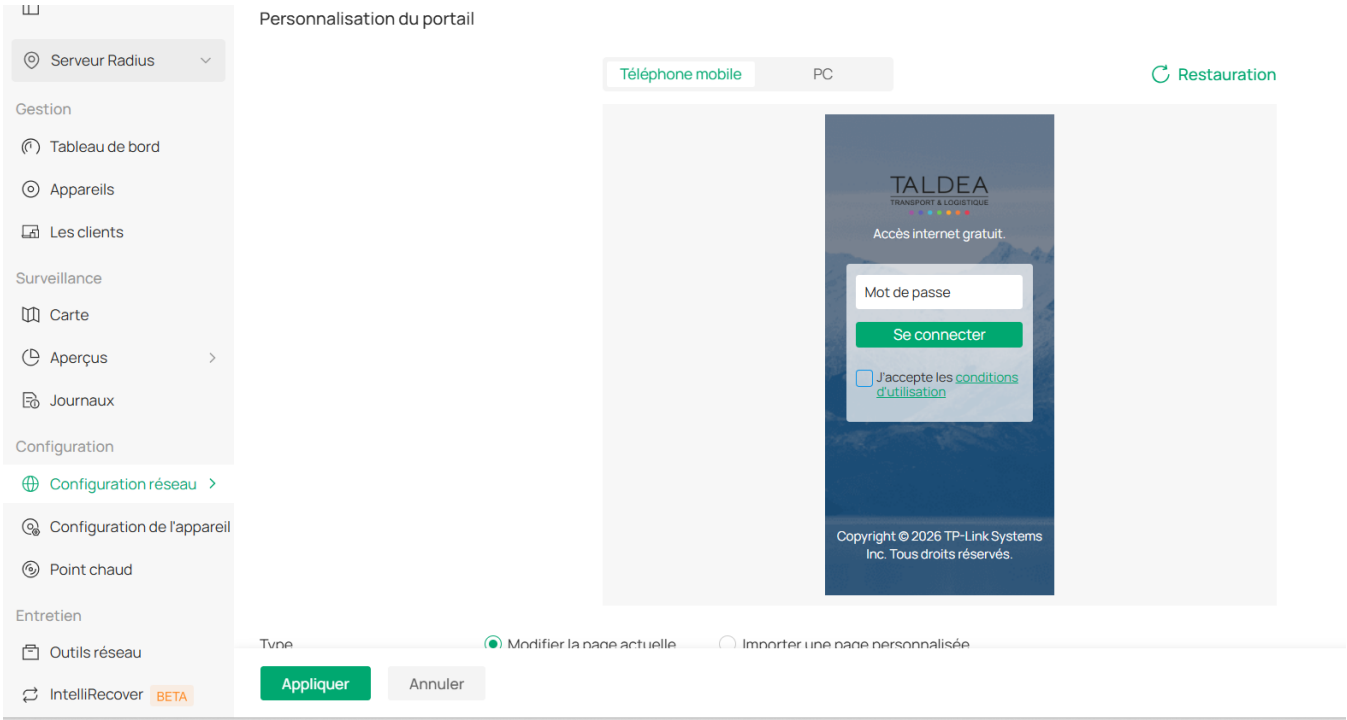
Configurer le portail avec les informations ci-dessous. Vous pouvez modifier l'heure de la *Session expirée* comme bon vous semble.



Vous pourrez éditer la page web où sera emmené le client pour se connecter avec le code au wifi.

 **Pour la conformité au RGPD, pensez à mettre une case à cocher pour les conditions d'utilisation.**

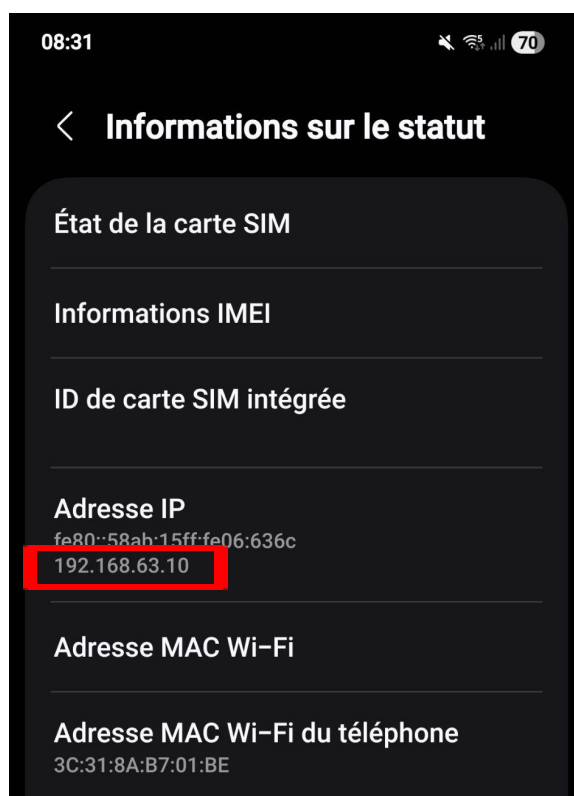
Voici un exemple d'une page web pour l'accès internet gratuit de l'entreprise Taldea :



The screenshot displays the 'Personnalisation du portail' (Portal Personalization) interface. On the left is a sidebar menu with categories: Gestion (Dashboard, Devices, Clients), Surveillance (Map, Overview, Logs), Configuration (Network, Device, Hotspot), and Entretien (Network Tools, IntelliRecover BETA). The main area shows a preview for a 'Téléphone mobile' (Mobile phone) with a 'PC' tab also available. A 'Restauration' (Restore) link is in the top right. The preview shows a login page for 'TALDEA TRANSPORT & LOGISTIQUE' with 'Accès internet gratuit.' (Free internet access.), a password field, a 'Se connecter' (Connect) button, and a checkbox for 'J'accepte les conditions d'utilisation' (I accept the terms of use). The footer of the preview mentions 'Copyright © 2026 TP-Link Systems Inc. Tous droits réservés.' (All rights reserved.). At the bottom of the configuration area, there are radio buttons for 'Modifier la page actuelle' (Modify current page) and 'Importer une page personnalisée' (Import custom page), along with 'Appliquer' (Apply) and 'Annuler' (Cancel) buttons.

Pour confirmer la fonctionnalité du portail et du SSID, vérifiez avec votre téléphone portable si vous apercevez, dans un premier temps, la connexion et après vous être connecté, si ça vous emmène vers la page web de connexion. Entrez le mot de passe, confirmez tout et faites une recherche pour tester la connectivité.

Vérifier, sur l'appareil auquel vous vous êtes connecté, l'adresse IP pour confirmer qu'il est bien dans le VLAN 30. Il doit avoir une adresse IP comprise entre 192.168.63.10 et 192.168.63.30. Voici un exemple sur un Samsung S24 :



Mise en place serveur Radius :

Avant de configurer le SSID *Entreprise_Secure*, il faut mettre en place un serveur Radius.

Le serveur Radius sert à établir des connexions entre les ordinateurs et fournir l'authentification, l'autorisation et la comptabilité. C'est un outil important pour gérer l'accès au réseau, car il peut empêcher les utilisateurs non autorisés et les attaquants d'infiltrer votre réseau. Ce sera donc important et utile pour le wifi *Entreprise_Secure* dont seul les employés auront accès.

Pour ce faire, allez dans *Paramétrages* > *Paramètres du serveur* > *Serveur RADIUS* et activer le *RAYON intégré*. Mettez l'adresse en *Manuelle* et entrez comme IP *192.168.60.11*. Dans *Secret*, entrez un mot de passe et cliquez sur *Appliquer*.

Vue Globale

Tableau de bord

Modèle de site **BETA**

Appareils

Journaux

firmware

Comptes

Paramétrages

Serveur RADIUS

RAYON intégré

RAYON intégré ☒

Etat ☒ Fonctionnement

Type d'adresse du serveur ☒ Manuelle ☐ Auto

Adresse IP 192 . 168 . 60 . 11

Secret  

Port d'authentification 1812 (1-65535)

Activer la réponse en tunnel ☐ Activer

Certificat de serveur

Format de fichier JKS

Appliquer Annuler

Ensuite, il faut créer un profil RADIUS qui est liée au SSID *Entreprise_Secure*.

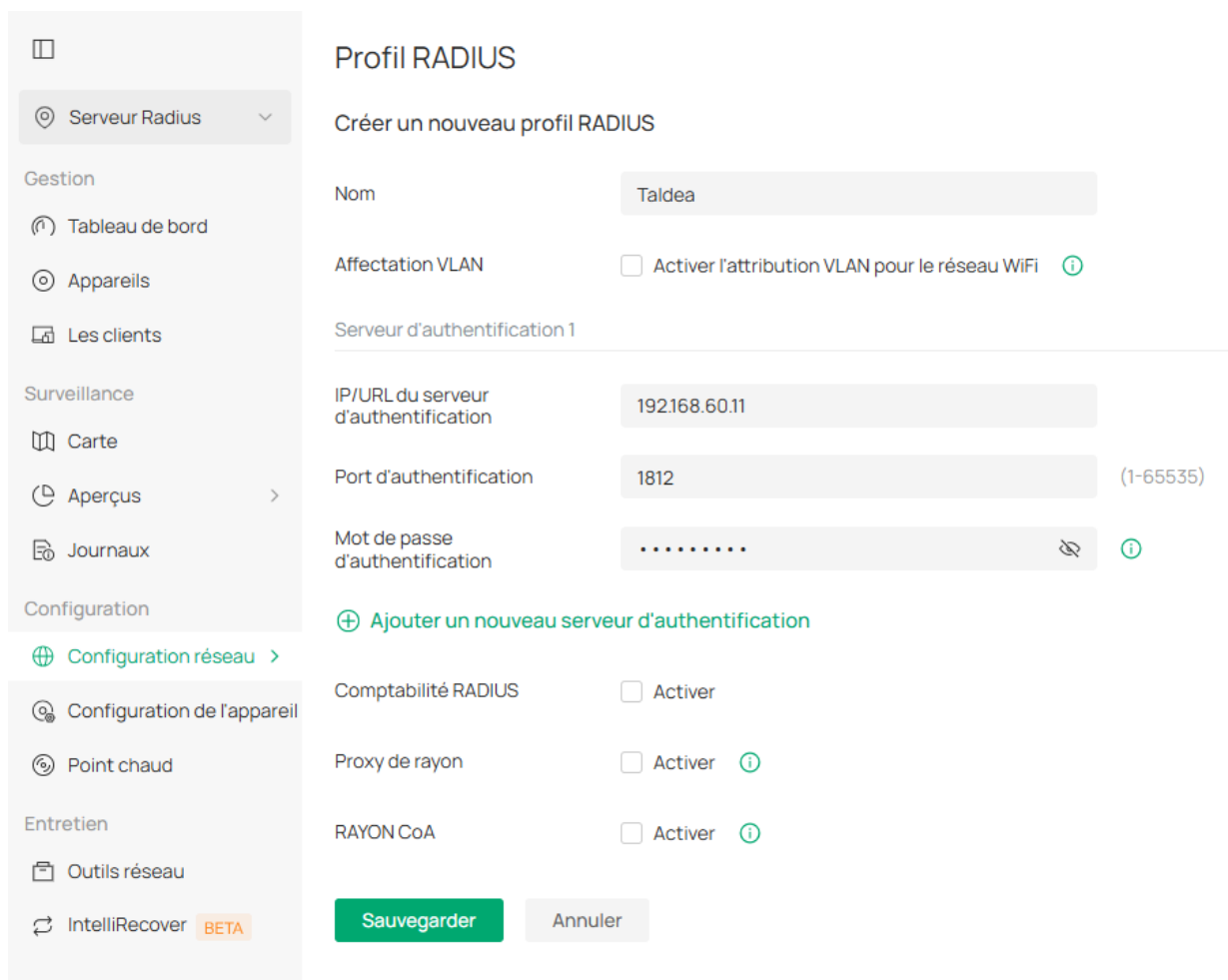
Un profil RADIUS enregistre les paramètres personnalisés d'un serveur RADIUS. Il permet d'appliquer ces paramètres à plusieurs stratégies d'authentification ce qui évite de saisir à plusieurs reprises les mêmes informations.

Allez dans *Configuration réseau > Profil RADIUS > Créer un nouveau profil RADIUS*.



NOM	SERVEUR RADIUS	PORT RADIUS	ASSIGNATION VLAN (WIFI)	COMPTABILITÉ ACTIVÉE	RADIUS PROXY	RADIUS COA ACTIVÉ	ACTION
Built-in Radius Profile	-	1812	-	-	-	-	

Choisissez un nom, mettez l'adresse IP *192.168.60.11* (adresse IP du contrôleur wifi) et créez un mot de passe.



Profil RADIUS

Créer un nouveau profil RADIUS

Nom

Affectation VLAN ☐ Activer l'attribution VLAN pour le réseau WIFI ⓘ

Serveur d'authentification 1

IP/URL du serveur d'authentification

Port d'authentification (1-65535)

Mot de passe d'authentification ⓘ

[+ Ajouter un nouveau serveur d'authentification](#)

Comptabilité RADIUS ☐ Activer

Proxy de rayon ☐ Activer ⓘ

RAYON CoA ☐ Activer ⓘ

[Sauvegarder](#) [Annuler](#)

Il faut ensuite créer les utilisateurs qui auront leur propres comptes pour se connecter au wifi.

Rester dans *Profil RADIUS* et cliquer sur modifier (encadrer en rouge) du profil *Built-in Radius Profile*.

Profil RADIUS

+ Créer un nouveau profil RADIUS

NOM	SERVEUR RADIUS	PORT RADIUS	ASSIGNATION VLAN (WIFI)	COMPTABILITÉ ACTIVÉE	RADIUS PROXY	RADIUS COA ACTIVÉ	ACTION
Built-in Radius Profile	-	1812	-	-	-	-	
Taldea	192.168.60.10	1812	✓	-	-	-	

Cliquez sur *Ajouter un nouvel utilisateur RADIUS*.

Utilisateurs RADIUS

+ Ajouter un nouvel utilisateur RADIUS

Importer Exporter

NOM	VLAN	EXPIRATION DE LA SESSION	LIMITE DE TAUX	TRAFFIC	ACTION
Pas de données.					

Enfin, créer vos utilisateurs en fonction de vos besoins.

Créer un nouvel utilisateur RADIUS

Type d'authentification ☒ Authentification d'utilisateur ☐ Authentification MAC

Nom

Mot de passe

ID VLAN

(Facultatif, 1-4094)

Expiration de la session Secondes

(Optionnel)

Limite de débit ☐

Limite de trafic ☐

Appliquer Annuler

Création SSID Entreprise_Secure :

Même étape que pour le SSID *Invites*, allez dans *Configuration réseau > Wifi > SSID > Créer un nouveau réseau Wifi*. Entrer les informations des 2 captures suivantes.

La sécurité choisie est WPA2-Entreprise. Cette sécurité est conçue pour les entreprises : chaque utilisateur a un identifiant unique et l'accès est contrôlé via un serveur RADIUS, ce qui permet de sécuriser le réseau et de révoquer l'accès d'une personne sans affecter les autres. C'est donc une sécurité adaptée pour ce réseau.

Sélectionner le profil RADIUS créé précédemment.

The screenshot shows the 'SSID' configuration page in the TP-Link Omada web interface. The left sidebar has a menu with 'Configuration réseau' selected. The main content area is titled 'Modifier le réseau WiFi' and contains the following fields:

- Nom de réseau (SSID):** ENTREPRISE_SECURE
- Type d'appareil:** ☒ EAP, ☐ Passerelle
- Bande:** ☒ 2,4 GHz, ☒ 5 GHz, ☐ 6 GHz
- Réseau invités:** ☐ Activer
- Sécurité:** WPA-Entreprise
- Profil RADIUS:** Taldea
- ID NAS:** ☒ Par défaut (TP-Link : adresse MAC), ☐ Suivre le nom de l'appareil, ☐ Personnalisé

- Menu
- Serveur Radius
- Gestion
 - Tableau de bord
 - Appareils
 - Les clients
- Surveillance
 - Carte
 - Aperçus
 - Journaux
- Configuration
 - Configuration réseau**
 - Configuration de l'appareil
 - Point chaud
- Entretien
 - Outils réseau

Réglages avancés

Le tunnel eogre ☐ Activer [Aller à Le tunnel eogre](#) ⓘ

transmission SSID ☒ Activer

Interdire le partage Wi-Fi ☐ Activer ⓘ

VLAN ☐ Par défaut ☒ Personnalisé

Ajouter un VLAN ☐ Par réseau ☒ Par ID de VLAN

(1-4094, jusqu'à 256 ID pour un SSID)

Mode WPA

MLO ☐ Activer ⓘ

PMF ☐ Obligatoire ☐ Capable ☒ Désactiver

Intervalle de génération ☐ Activer la ressaisie GIK tous les Secon... (30-86400)

802.11r ☐ Activer ⓘ

Profil de limite de débit client ⓘ

Tester sur un téléphone portable ou sur un PC si vous apercevez le wifi et si c'est le cas, connectez-vous avec un de vos utilisateurs RADIUS créé et vérifiez si vous accédez bien à internet. Contrôler si vous êtes bien dans le VLAN 20 en ayant une adresse IP comprise entre *192.168.62.10* et *192.168.62.30*.

Sécurité

Pour la sécurité du réseau, il faut faire un filtrage inter-VLAN et une journalisation.

Filtrage *inter-VLAN* :

Le filtrage inter-VLAN est un mécanisme de sécurité réseau qui permet de contrôler, autoriser ou bloquer les communications entre différents VLAN à l'aide de règles définies sur un routeur, un switch de couche 3 ou un pare-feu. C'est donc nécessaire pour que les appareils du VLAN 20 et 30 puissent communiquer avec les appareils du même VLAN qu'eux mais ne pas pouvoir communiquer ou accéder aux appareils attribuer aux autres VLAN.

Dans le routeur, vous allez créer une règle ACL pour le VLAN 20 afin d'interdire la communication et l'accès avec les appareils des autres VLAN.

Une règle ACL (Access Control List) est une règle de filtrage réseau qui permet d'autoriser ou refuser le passage de paquets en fonction de critères comme l'adresse IP source ou destination, le protocole ou le port utilisé.

Commencez par créer une liste d'adresse IP avec la plage d'adresse IP 192.168.62.10 à 192.168.62.30. Allez dans *Preferences > IP Group > IP Address* puis cliquez sur *Add* et renseignez le nom et la plage d'adresse.

IP Address List

[+ Add](#) [- Delete](#)

☐	ID	Name	IP Address Type	IP Address Range	IP Address/Mask	Description	Operation
--	1	IP_LAN	IP Address/Mask	192.168.60.0/24,192.168.61.0/24,192.168.62.0/24,192.168.63.0/24	192.168.60.0/24,192.168.61.0/24,192.168.62.0/24,192.168.63.0/24	IP_LAN	---
--	2	Employees	IP Address Range	192.168.62.10-192.168.62.30	---	---	---

Name:

IP Address Type: ☒ IP Address Range ☐ IP Address/Mask

-

Description: (Optional)

Dans *IP Group*, faites *Add* et dans *Address Name* sélectionné *Employees*.

Group List

[+ Add](#) [- Delete](#)

☐	ID	Group Name	Address Name	Description	Operation
--	1	IPGROUP_ANY	---	IPGROUP_ANY	---
--	2	IPGROUP_LAN	IP_LAN	IPGROUP_LAN	---
--	3	Employees	Employees	---	---

Group Name:

Address Name:

Description: ☐ IP_LAN ☒ Employees (Optional)

Rendez-vous dans *Firewall > Access Control* et cliquez sur *Add* puis reproduisez la capture ci-dessous. Dans *Destination*, choisissez *IPGROUP_LAN* car il réunit tous les réseau existant dont les VLAN.

The screenshot shows the 'Access Control' configuration page. On the left is a sidebar with navigation options: Status, Network, Preferences, Transmission, Firewall (selected), Behavior Control, VPN, Authentication, Services, System Tools, and Logout. The main area has a 'Clear Contrack' button and a table of rules. Below the table is a form to add a new rule.

ID	Name	Policy	Service Type	Direction	Source	Destination	Source Network	Destination Network	Effective Time	Operation
1	Employees	Block	ALL	ALL	Employees	IPGROUP_LAN	---	---	Any	---

Form fields for adding a new rule:

- Name: Employees (1-50 characters)
- Policy: Block
- Service Type: ALL
- Direction: ALL
- Source: Employees
- Destination: IPGROUP_LAN
- Effective Time: Any
- States: New
- ID: (Optional)

Buttons: OK, Cancel

Cliquez sur *OK* puis sur *Clear Contrack* pour lancer la règle.

Vérifier que la règle a bien fonctionné en faisant des pings entre les PC d'un même et différent VLAN. Les PC d'un même VLAN doivent se ping tandis que les PC d'un VLAN différent ne doivent pas se ping.

Exemple d'un ping d'un PC dans le VLAN 10 vers un PC du VLAN 20.

```
C:\Users\Administrateur>ping 192.168.62.10

Envoi d'une requête 'Ping' 192.168.62.10 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.62.10:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

Journalisation :

La journalisation désigne l'enregistrement chronologique et horodaté des événements produits par un système ou une application. Chaque action (ouverture de session, consultation, modification ou suppression d'un fichier) est inscrite dans un journal technique, sorte de mémoire fidèle de l'activité. C'est donc très utile pour repérer de potentielles intrusions ou attaques mais aussi pour être informé des appareils qui se sont connectés ou déconnectés, etc...

Pour recevoir les alertes, il faut lier le contrôleur à un e-mail. Si vous êtes sur Gmail, il faut activer la validation en deux étapes puis créer un mot de passe des applications qui sera utilisé pour la configuration du serveur de courrier du contrôleur wifi.

← Mots de passe des applications

Les mots de passe d'application vous permettent de vous connecter à votre compte Google sur des applis et des services plus anciens, non compatibles avec les normes de sécurité les plus récentes.

Les mots de passe d'application sont moins sécurisés que les applis et services à jour qui utilisent les normes de sécurité les plus récentes. Avant de créer un mot de passe d'application, vous devez vérifier si votre appli en a besoin pour établir la connexion.

[En savoir plus](#)

Vos mots de passe d'application

Omada Controller

Date de création : 09:03, dernière utilisation : 14:52



Pour créer un mot de passe spécifique à une appli, indiquez son nom ci-dessous.

Nom de l'appli

Créer

Dans le contrôleur wifi, sélectionnez le site *Vue Globale* et allez dans *Paramétrages > Paramètres du serveur > Serveur de courrier* et renseigner les informations suivantes. Le mot de passe des applications est à mettre dans *Code d'autorisation*.

Faites un test d'envoi pour confirmer le fonctionnement du serveur.

Paramètres du serveur

Serveur de courrier ☒

Avec le serveur de messagerie, le contrôleur peut envoyer des e-mails pour réinitialiser votre mot de passe. configurer soigneusement le serveur de messagerie.

SMTP: smtp.gmail.com

Port: 465 (1-65535)

SSL: ☒ Activer

Authentification: ☒ Activer

Nom d'utilisateur: taldea974@gmail.com

Code d'autorisation:

E-mail de l'expéditeur: taldea974@gmail.com

Test d'envoi

Appliquer Annuler

Ensuite, vous pouvez soit activer les alertes sur votre compte principale que vous avez créé à votre première connexion (voir page 13) soit créer un nouvel utilisateur qui sera bénéficiaire des alertes.

Compte principale :

Pour activer les alertes sur votre compte principale, rendez-vous dans *Comptes > Utilisateur* et cliquez sur modifier (encadré en rouge) puis entrer votre mot de passe.

	NOM D'UTILISATEUR	TYPE D'UTILISATEUR	STATUT	E-MAIL	2FA	RÔLE	PÉRIODE DE VALIDITÉ	PRIVILÈGES DU SITE	ACTION
☐	errotaberea.thomas@taldea.com	Utilisateur du nuage	Vérifié	errotaberea.thomas@taldea.com	-	Owner	Permanent	Tous les sites	
☐	Taldea	Utilisateur local	Vérifié	-	-	Owner	Permanent	Tous les sites	

Entrer votre adresse mail et activer l'e-mail d'alertes comme sur la capture puis sauvegarder.

Vue Globale

Tableau de bord

Modèle de site

BETA

Appareils

Journaux

firmware

Comptes

Paramétrages

Utilisateur

Rôle

Utilisateur SAML

Groupe d'utilisateurs SAML

Informations de base

Rôle

Owner

Transfert d'autorisation

Privilèges du site

Tous les sites

Modifier l'utilisateur

Nom d'utilisateur

Taldea

Modifier le mot de passe

☐ Activer

Email

taldea974@gmail.com

E-mails d'alerte/événement

☒ Activer

Authentification à deux facteurs (2FA)

☐

Avec l'authentification à deux facteurs (2FA) activée, vous aurez besoin d'un mot de passe de connexion beaucoup plus élevé.

Remarque: Veuillez d'abord télécharger l'application d'authentification sur votre téléphone.

Sauvegarder

Annuler

Compte secondaire :

Pour activer les alertes sur votre compte secondaire, rendez-vous dans *Comptes > Utilisateur > Ajouter un nouvel utilisateur*.

Vue Globale

Tableau de bord

Modèle de site

BETA

Appareils

Journaux

Utilisateur

Rôle

Utilisateur SAML

Groupe d'utilisateurs SAML

Rechercher un nom d'utilisateur ou un e-mail

+ Ajouter un nouvel utilisateur

	NOM D'UTILISATEUR	TYPE D'UTILISATEUR	STATUT	E-MAIL	2FA	RÔLE	PÉRIODE DE VALIDITÉ	PRIVILÈGES DU SITE	ACTION
☐	errotaberea.thomas64@gmail.com	Utilisateur du nuage	Vérifié	errotaberea.thomas64@gmail.com	-	Owner	Permanent	Tous les sites	
☐	Taldea	Utilisateur local	Vérifié	-	-	Owner	Permanent	Tous les sites	

Configurer l'utilisateur comme sur la capture ci-dessous.
 Pour la section *Privilèges du site*, choisissez *Sites spécifiques* et sélectionnez le site auquel vous voulez recevoir les alertes pour éviter qu'elles se mélangent toutes dans une même adresse e-mail.
 Utiliser une adresse e-mail adéquate pour recevoir les alertes.

The screenshot shows the 'Ajouter un nouvel utilisateur' form. The left sidebar contains navigation links: 'Vue Globale', 'Tableau de bord', 'Modèle de site BETA', 'Appareils', 'Journaux', 'firmware', 'Comptes', and 'Paramétrages'. The main form has tabs for 'Utilisateur', 'Rôle', 'Utilisateur SAML', and 'Groupe d'utilisateurs SAML'. The 'Utilisateur' tab is active. The form fields are as follows:

- Type d'administrateur:** ☒ Utilisateur local, ☐ Utilisateur du nuage
- Période de validité:** ☒ Permanent, ☐ Temporaire
- Nom d'utilisateur:** Alerte
- Mot de passe:** [Masked]
- Rôle:** Viewer (with a 'Gérer le rôle' link)
- Privilèges du site:** ☐ Tous les sites (y compris les sites nouvellement créés), ☒ Sites spécifiques
- Choisissez des sites:** Serveur Radius (selected)
- Email:** taldea974@gmail.com (Optionnel)
- E-mails d'alerte/événement:** ☒ Activer

Buttons at the bottom: 'Créer' (green) and 'Annuler' (grey).

Après avoir configuré l'un des 2 comptes, allez dans *Journaux > Réglage > Événement > Paramètres de contenu* et configurer en fonction des alertes que vous voulez recevoir.

The screenshot shows the 'Paramètres des journaux' page. The left sidebar is the same as the previous screenshot. The main section is titled 'Paramètres des journaux' and 'Paramètres de contenu'. There are two tabs: 'Système (14)' and 'Appareil (1)'. The 'Système (14)' tab is active. Below the tabs is a table with columns for event names, 'ACTIVER', 'NOTIFICATION PAR E-MAIL', and 'NOTIFICATION WEBH'.

	ACTIVER	NOTIFICATION PAR E-MAIL	NOTIFICATION WEBH
TAPER	☒	☒	☐
Backup Schedule Executed	☒	☒	☐
Backup Schedule Failed	☒	☒	☐
Email Limit Reached	☒	☒	☐
Controller Access Port Changed	☒	☒	☐
Portal Port Changed	☒	☒	☐
Device List Schedule Mail Failed	☒	☒	☐
Device List Schedule Executed	☒	☒	☐
Global Logs Mailed Automatically	☒	-	☐
Automatic Global Logs Mail Failed	☒	-	☐
Global Logs Sent to Log Server	☒	-	☐

Buttons at the bottom: 'Sauvegarder' (green) and 'Annuler' (grey).

Changez de site et refaites la même manipulation en configurant la section *Événement* mais aussi la section *Alertes* de votre site.

☐

📶 Serveur Radius

Gestion

📊 Tableau de bord

📶 Appareils

👤 Les clients

Surveillance

📍 Carte

🕒 Aperçus

📅 Journaux

Configuration

🌐 Configuration réseau

🔧 Configuration de l'appareil

← Paramètres des journaux

Webhook ☐

Paramètres de contenu

Système (5)

Appareil (53)

🔄 Réinitialiser par défaut

TAPER	☒ ACTIVER	NIVEAU	☒ NOTIFICATION PAR E-MAIL	☐ NOTIFICATION WEBHook
DST configuration error.	☒ Activer	❌ Erreur	☒ Activer	☐ Activer
IntelliRecover - Reboot Recovery Initiated	☒ Activer	ℹ Info	☒ Activer	☐ Activer
IntelliRecover - Reboot Recovery Failed	☒ Activer	❌ Erreur	☒ Activer	☐ Activer
IntelliRecover - Retry Limit Exceeded	☒ Activer	❌ Erreur	☒ Activer	☐ Activer
Gateway's LAN segment is modified	☒ Activer	⚠ Avertissement	☒ Activer	☐ Activer

Pour tester la fonctionnalité des alertes, débranchez par exemple la borne wifi et vérifiez si vous avez reçu une alerte dans l'adresse e-mail. Voici un aperçu du mail reçu :

← 📧 ⌚ 🗑 📧 📧 ⋮

Omada Controller_F1EB4D-Serveur Radius Log - 2026-01-13

Boîte de réception x

T

taldea974@gmail.com

À moi ▼

Omada Controller_F1EB4D-Serveur Radius Log - 2026-01-13
Time: 2026-01-13
Controller version: 6.0.0.25
Controller Name: Omada Controller_F1EB4D
Site: Serveur Radius
#####

2026-01-13 09:24:12 AM DEVICE ERROR [ap:98-03-8E-2F-5F-2A:98-03-8E-2F-5F-2A] was disconnected.
2026-01-13 09:24:12 AM DEVICE ERROR [ap:98-03-8E-2F-5F-2A:98-03-8E-2F-5F-2A] was disconnected.

Supervision

Maintenant que toute la configuration de l'infrastructure est terminée, voici quelques aperçus d'outils disponibles dans le contrôleur qui vont vous être utiles pour la supervision du réseau.

Clients connectés :

Vous avez accès aux clients qui sont connectés au réseau en allant dans la section *Les clients*. Vous pouvez voir leur adresse IP, le SSID auquel ils sont connectés, leur retirer la permission pour le wifi, les bloquer, etc... (vous pouvez activer les alertes concernant la connexion et la déconnexion pour recevoir un mail de chaque client et employés qui se connecte au wifi)

NOM DU CLIENT	ADRESSE IP	TYPE D'IDENTIFICATION	STATUT	SSID	RÉSEAU	PA/PORT	TÉLÉCHARGÉ	ACTION
Client	192.168.63.10	Mot de passe	AUTORISÉ	INVITES	-	98-03-8E-2F-5F-2A	4.43 M	[Icons for actions]

Aperçu de l'alerte de connexion par e-mail.

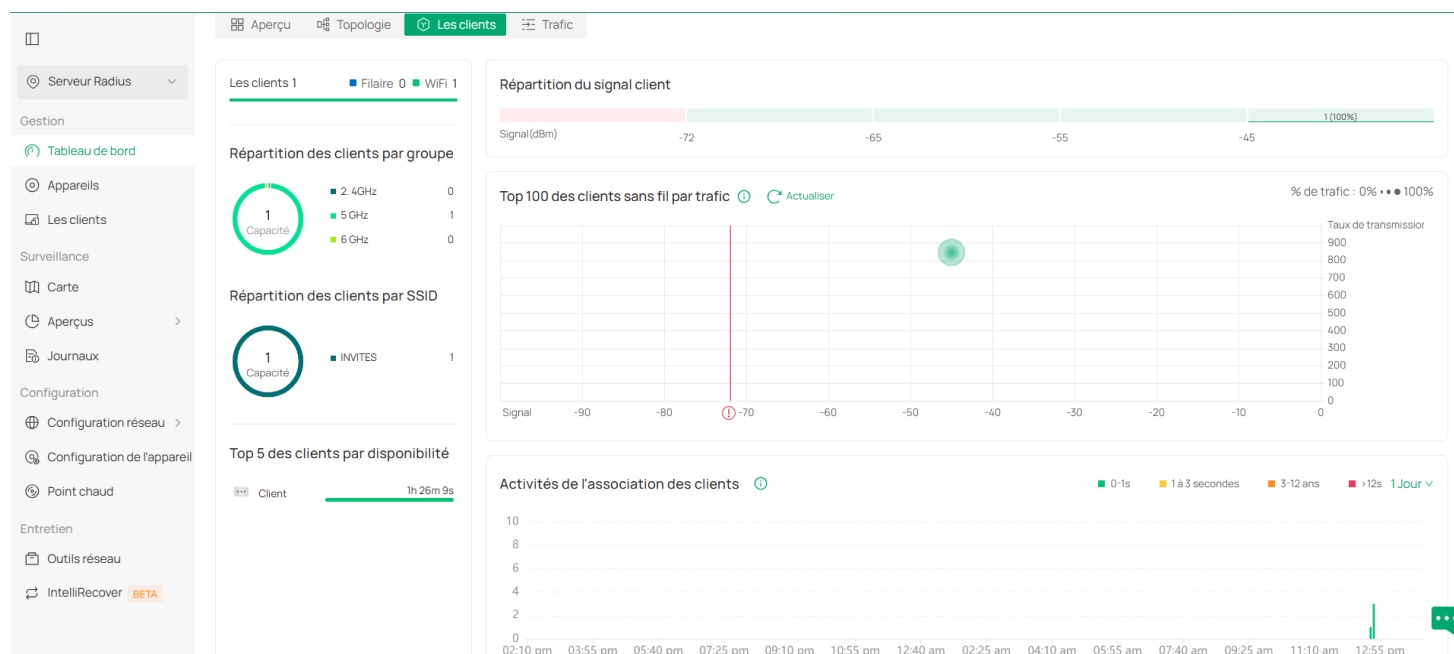
Omada Controller_F1EB4D-Serveur Radius Log - 2026-01-21 Boîte de réception x

T taldea974@gmail.com
À moi ▾

Omada Controller_F1EB4D-Serveur Radius Log - 2026-01-21
Time: 2026-01-21
Controller version: 6.0.0.25
Controller Name: Omada Controller_F1EB4D
Site: Serveur Radius
#####

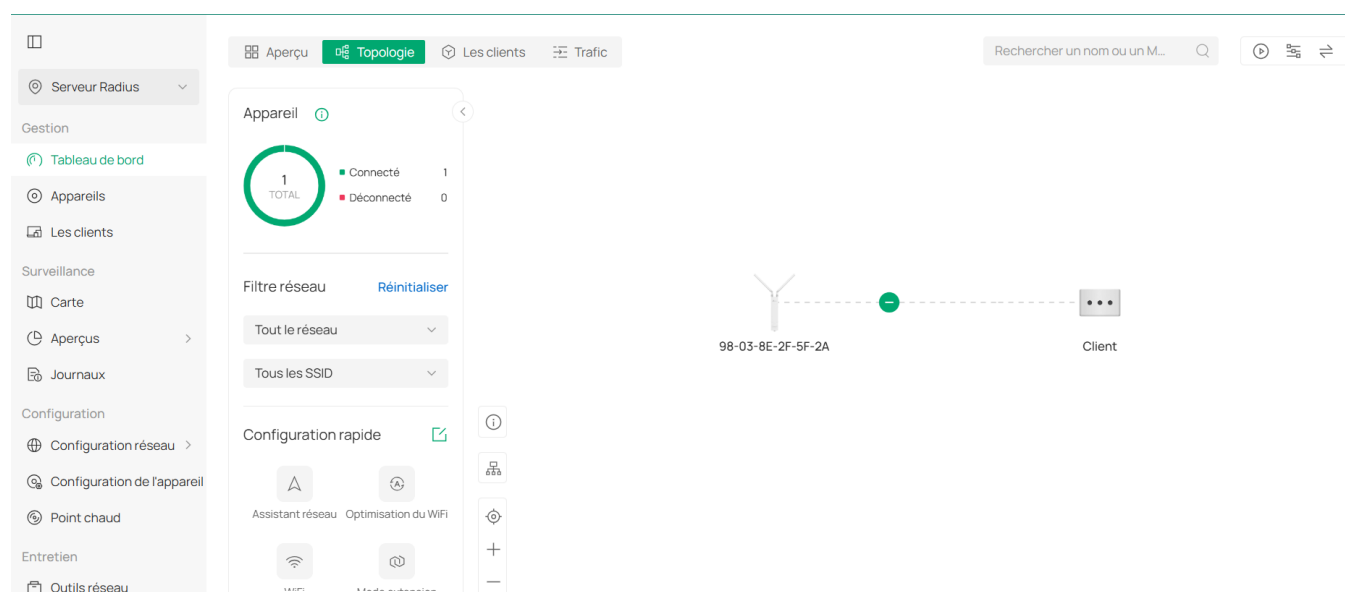
2026-01-21 12:41:44 PM CLIENT [client:Client:5A-AB-15-06-63-6C] (IP: 192.168.63.10) went online on [ap:98-03-8E-2F-5F-2A:98-03-8E-2F-5F-2A] with SSID "INVITES" on channel 44.

Dans *Tableau de bord*, vous avez accès à l'activité de tous les clients. Vous pouvez consulter le trafic, la répartition du signal, des clients, etc...



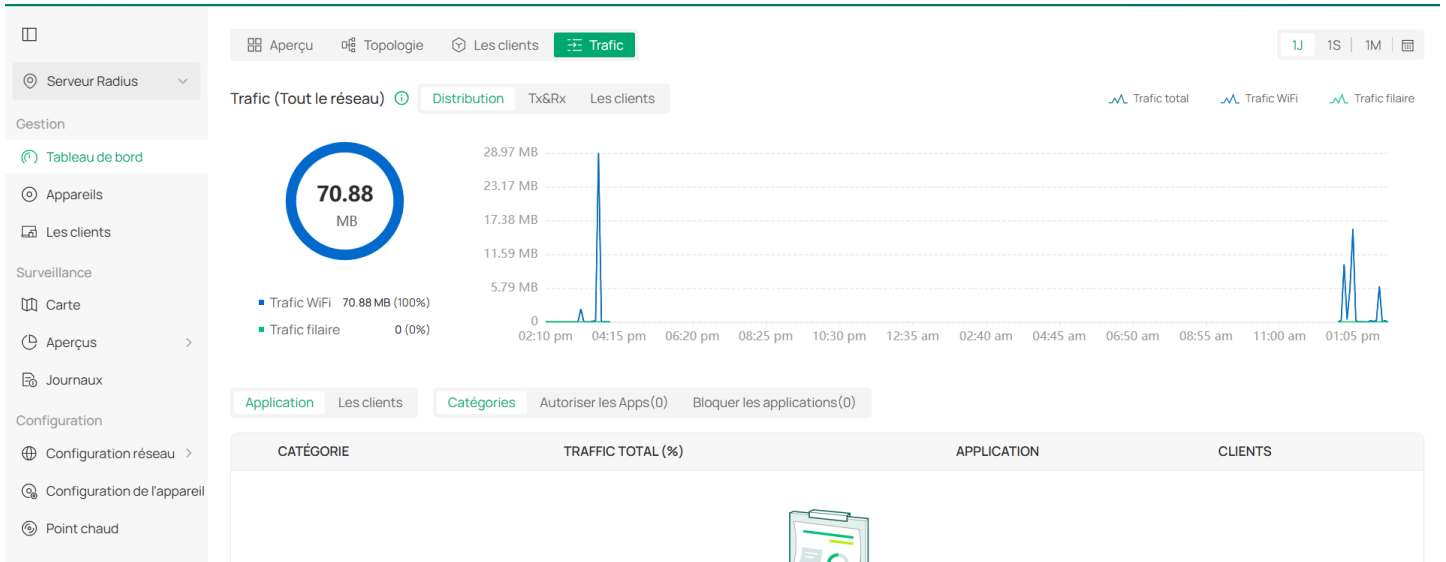
Topologie :

Avec la *Topologie*, vous avez accès à un schéma avec tous les appareils connectés à la borne wifi.



Traffic :

Vous pouvez apercevoir tout le trafic du réseau comme les applications consultées, les clients, le wifi, etc...



Appareils :

Vous avez accès à l'ensemble des appareils de l'infrastructure du réseau qui soit connecté ou non au contrôleur.

Vous pouvez décider de connecter les appareils non liée au contrôleur mais attention car l'interface web de ces derniers ne sera plus disponible, ils seront configurables seulement avec le contrôleur.

Serveur Radius

Gestion

- Tableau de bord
- Appareils
- Les clients

Surveillance

- Carte
- Aperçus

liste d'appareils

Groupe d'appareils

Résultat de la configuration

Rechercher le nom, le SN, le MAC, l'IPv4, le Q

Tout (3)Passerelle/switchs (2)OLT (0)AP (1)

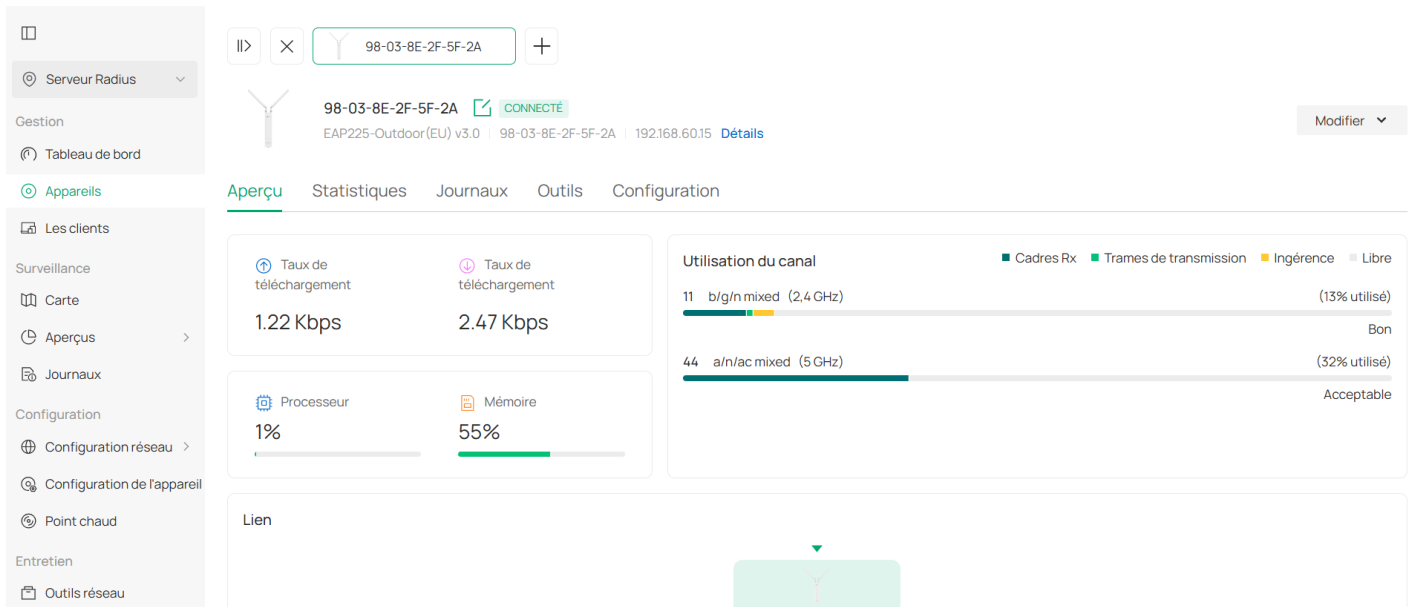
ExporterAction par lots

+ Ajouter des appareils

NOM DE L'APPAREIL	ADRESSE IP	STATUT	MAQUETTE	VERSION	ACTION
 54-AF-97-C6-F9-07	192.168.60.1	● EN ATTENDANT	ER7206 v1.0	1.2.3	
 40-AE-30-34-F9-9D	192.168.60.2	● EN ATTENDANT	SG242BP v5.30	5.30.0	
 98-03-8E-2F-5F-2A	192.168.60.15	● CONNECTÉ	EAP225-Outdoor (EU) v3.0	5.111	 

Affichage de 1-3 du 3 d'enregistrements < 1 > 10 /page

Aperçu de l'interface de configuration du wifi :



Vous avez accès à plusieurs informations et paramètres comme le taux de téléchargement, les statistiques, les journaux, la configuration, etc...