Guide de déploiement du réseau Omada

Chapitres

Contenu

1 À propos d'Omada SDN

Mise à niveau de la solution Omada actuelle, Omada SDN est une solution complète de réseautage défini par logiciel (SDN) qui intègre les points d'accès, les commutateurs, les passerelles, et plus encore. Il permet à un intégrateur system (SI) de créer efficacement des réseaux de toute taille, de petite à grande, avec une grande évolutivité.

Membres Omada SDN

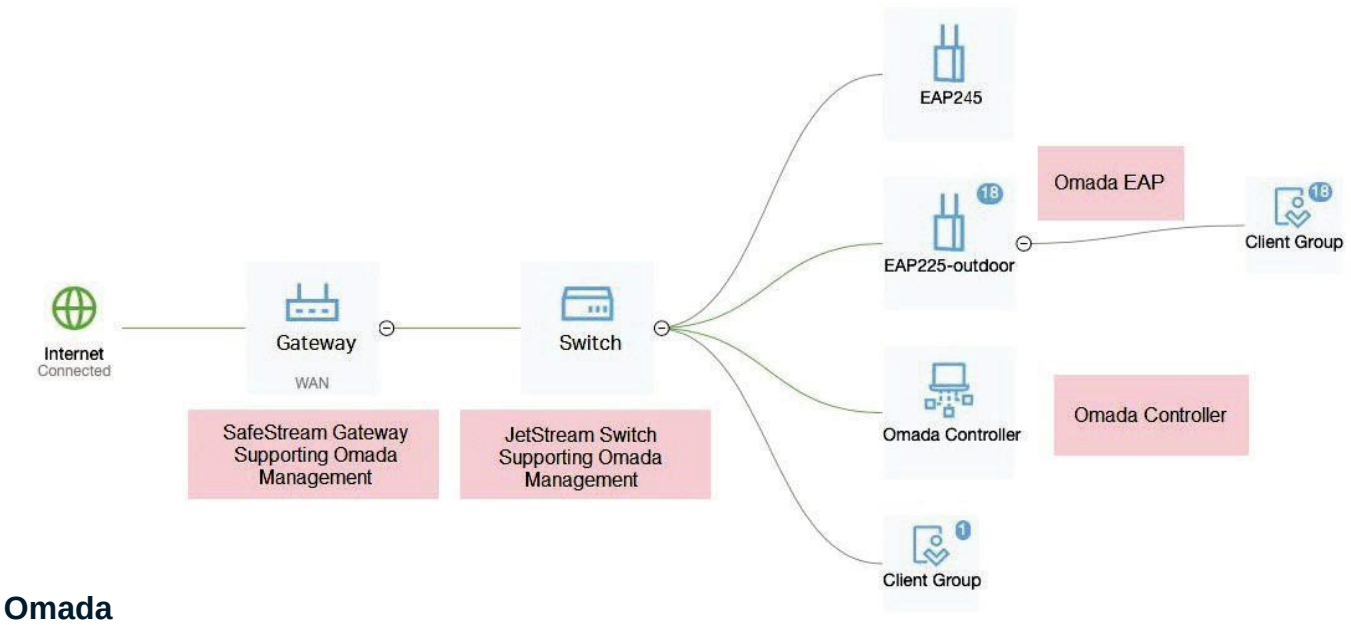
Comme le montre le chiffre suivant, Omada SDN inclut les membres suivants :

Les contrôleurs Omada

Les PAE d'Omada

SafeStream Gateways avec la version firmware qui prend en charge la gestion Omada

JetStream Switches avec la version firmware qui prend en charge la gestion Omada



Contrôleurs Omada

Parmi tous les membres, les contrôleurs Omada sont au cœur de la solution Omada SDN. Vous pouvez configurer tous les périphériques membres Omada et surveiller l'ensemble du réseau simplement via l'interface utilisateur du contrôleur. TP-Link fournit plusieurs types de contrôleurs Omada, vous permettant de choisir le plus approprié pour votre situatisur.

Type de contrôleur	Description
Contrôleur matériel (OC200/OC300)	Doit être acheté en plus Il faut un petit espace pour se déployer avec un corps mince Supportez l'accès au cloud
Contrôleur logiciel	Gratuit pour installer et mettre à niveau, mais besoin d'un ordinateur réservé pour continuer à fonctionner si vous utilisez des fonctionnalités avancées comme Portal Soutient l'accès au cloud
Cloud-Based Contrôleur	Déployé sur Omada Cloud, fournit un service payant avec des prix à plusieurs niveaux Service personnalisé professionnel pour les réseaux de plus de 500 appareils

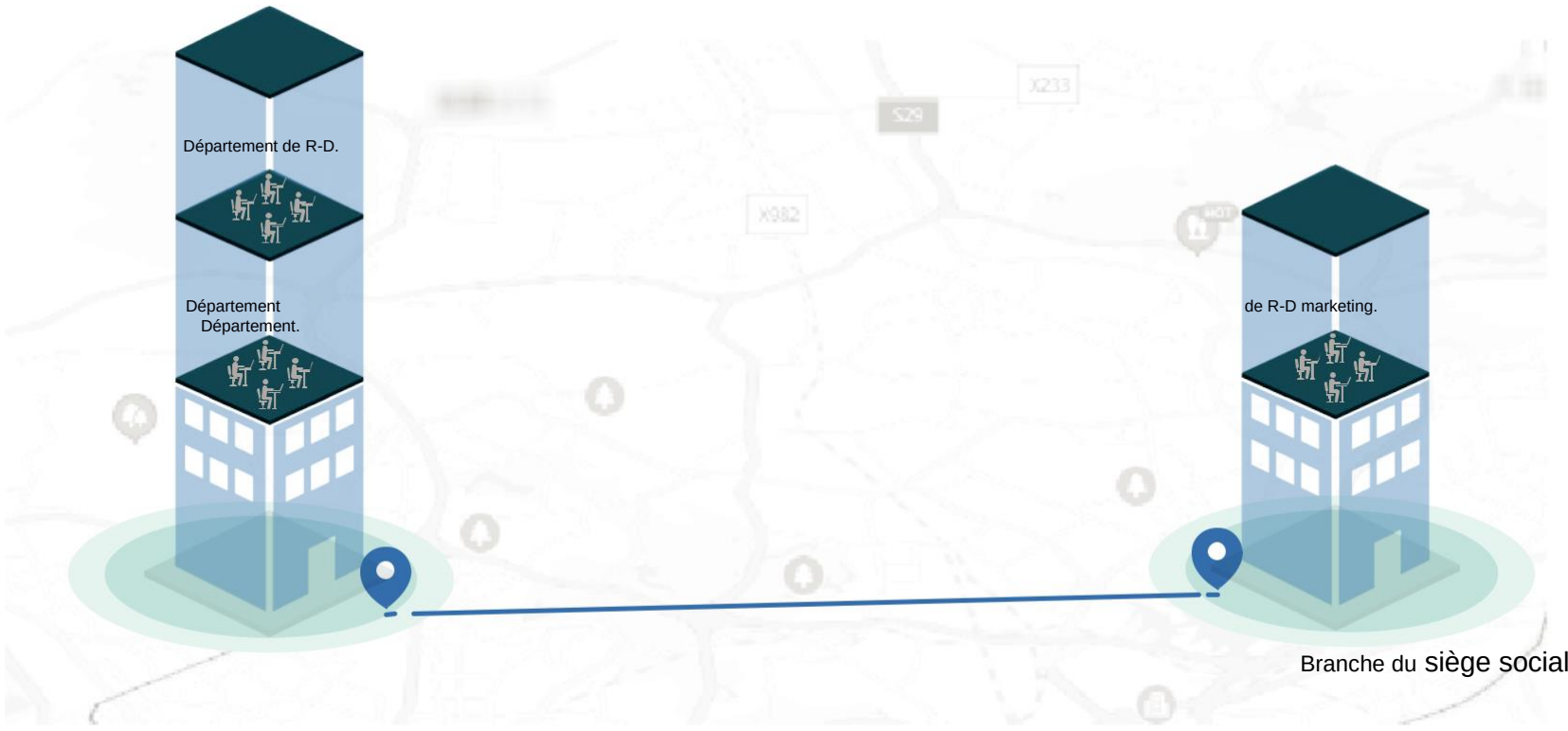
2 Mise en place d’un réseau de base

La solution Omada SDN est conçue pour construire des réseaux évolutifs. Les configurations varient selon les situations réelles. Ce chapitre introduit comment configurer un réseau de base à travers une application typique.

2.1 Exigences réseau

Un intégrateur de système est la planification d’un réseau pour son client, une entreprise avec deux bâtiments. Comme le montre le chiffre suivant, le département du marketing est au siège social, tandis que le Département de la R-D a deux bureaux, l’un au siège social et l’autre dans la succursale.

Figure 2-1 Bâtiments de la Société



Il est nécessaire que:

Le réseau doit contenir des réseaux câblés et sans fil pour permettre l’accès à divers appareils.

Pour améliorer l’efficacité du réseau et améliorer la sécurité, le même département devrait être dans le même réseau et différents ministères devraient être dans différents réseaux.

Les deux départements ont besoin d’un serveur FTP pour transmettre des fichiers entre eux.

Pour une meilleure gestion, l’administrateur du réseau doit surveiller et contrôler le réseau de façon centralitaire à tout moment, de n’importe où.

2.2 Schéma de configuration

La solution Omada SDN peut répondre à toutes les exigences ci-dessus. Avec les passerelles, les commutateurs et les PAE Omada, vous pouvez configurer les réseaux câblés et sans fil. Tous les appareils peuvent être gérés via Omada SDN Controller, permettant de surveiller et de contrôler à partir d’une seule interface. Construisez le réseau selon les directives de topologie et de configuration ci-dessous.

Pour libérer les configurations sur place, vous pouvez choisir Omada Cloud-Based Controller pour déployer et configurer à distance les réseaux pour le client. Toutes les configurations peuvent être acheminées et envoyées aux appareils via Omada Cloud.

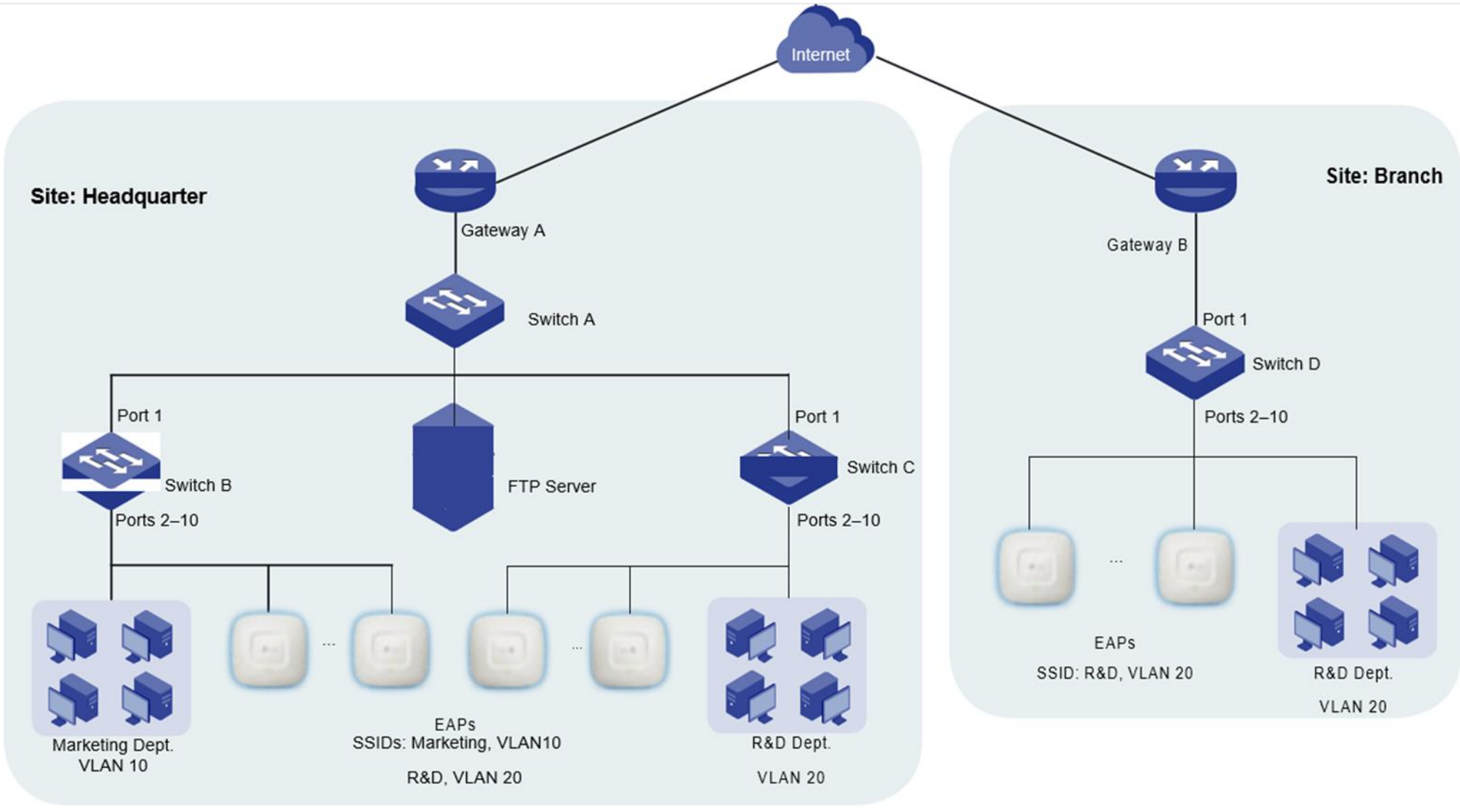
Pour faciliter la gestion, créez deux sites pour le réseau, l’un pour le siège social et l’autre pour la succursale. Omada SDN Controller gère des réseaux basés sur des sites. Le site est la plus grande unité pour la gestion des réseaux.

Pour diviser différents départements à différents réseaux, créez deux réseaux LAN (VLAN) — l’un pour le département Marketing et l’autre pour le département de recherche et développement. Par conséquent, créez deux réseaux sans filpour les deuxministères. Les réseaux câblés et sans fil d’un département devraient être dans le même VLAN.

Conseil: Les ports de commutation sans paramètres spéciaux seront ajoutés automatiquement à tous les VLAN. Pour les ports de commutation qui sont connectés à des périphériques ayant un accès accordé aux deux départements, comme le serveur FTP et les passerelles, il suffit de conserver les paramètres par défaut.

Pour s’assurer que les employés de la succursale peuvent accéder aux ressources (comme le serveur FTP) au siège social, construisez un tunnel VPN entre les deux sites.

Topologie réseau Figure 2-2



2.3 Procédure de configuration

Préparations

Avant l’expédition :

Notez les numéros de série de tous les appareils. Les numéros de série sont requis lors de l’ajout d’appareils au contrôleur basé sur le cloud.

Configurer les passerelles. Omada Cloud -Based Controller fournit des fichiers de configuration à tous les appareils via Omada Cloud. Pour recevoir avec succès les configurations, la passerelle de chaque site doit être préconfigurée et accéder à Internet une fois alimentée. on.

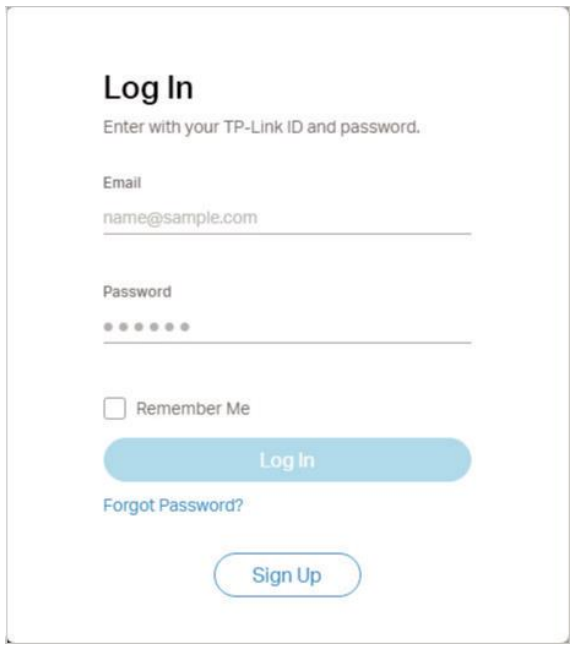
Après que le client avait reçu tous les appareils :

Assurez-vous que tous les appareils sont connectés selon la topologie du réseau et alimentés.

1. Abonnez-vous à un contrôleur cloud d’Omada.

a. Allez https://omada.tplinkcloud.com et connectez-vous au Cloud Omada avec votre ID TP-Link. Si vous n’avez pas d’ID TP-Link, enregistrez-en un.

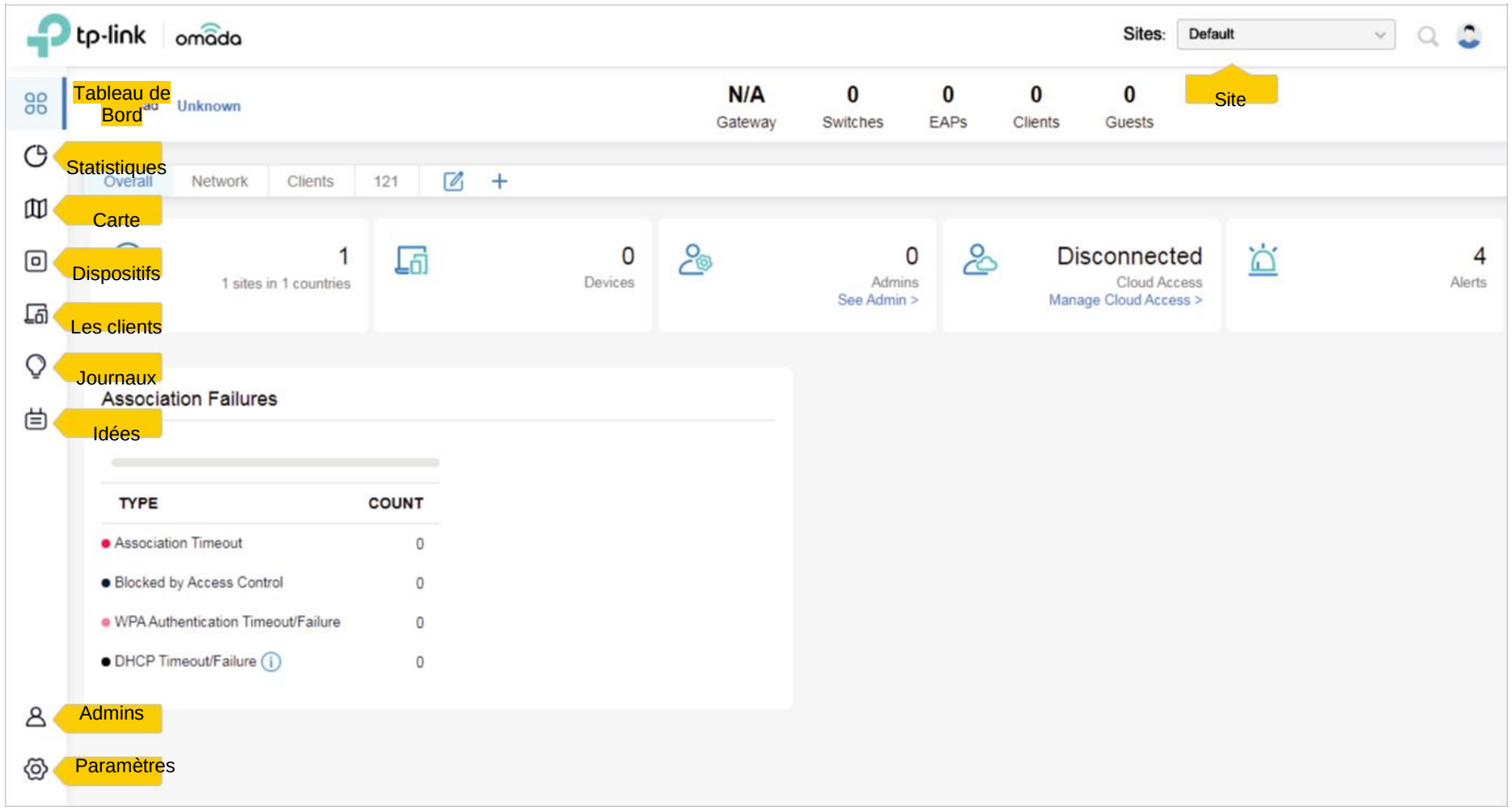
Figure 2-3 Se connectant dans le nuage d’Omada



b. Cliquez + Add Controller en bas de la page et suivez les instructions pour vous abonner à un contrôleur basé sur le cloud pour le client.

c. Le contrôleur basé sur le cloud sera affiché dans la liste des contrôleurs après le paiement. Cliquez pour entrer la page de gestion du contrôleur.

Figure 2-4 Page de gestion du contrôleur



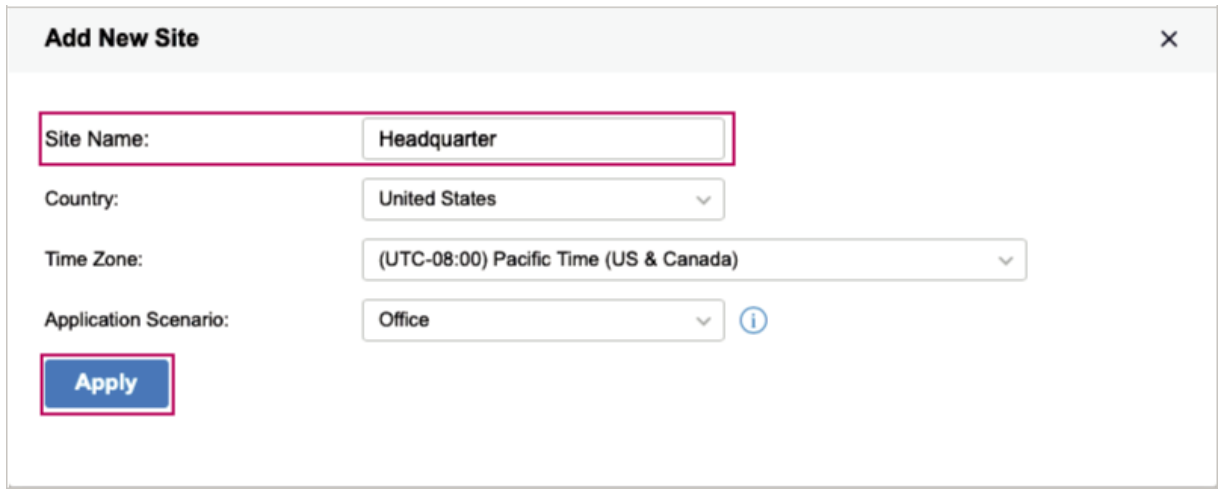
2. Créez deux sites pour le client.

a. Cliquez sur le nom actuel du site en haut de la page, puis cliquez sur **le site d’ajouter**un nouveau site.

Figure 2-5 Comité de gestion du site

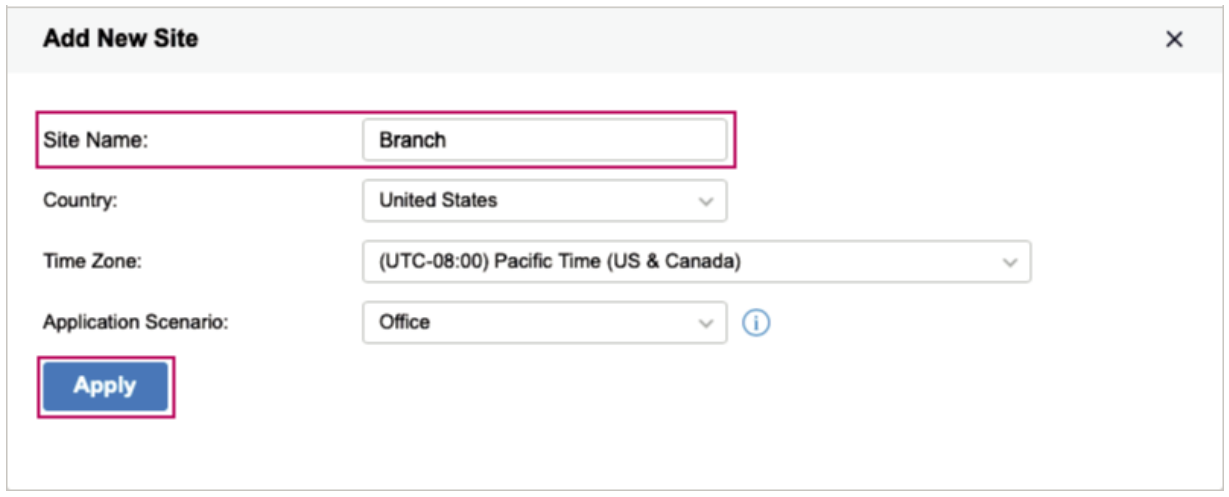
b. La page Add New Site apparaîtra. Créez un site nommé Siège et configurez les paramètres en fonction de votre situation.

Figure 2-6 Ajout d’un site pour le siège social



c. Répéter l’étape a et b pour créer un autre site nommé Branch.

Figure 2-7 Ajout d’un site pour la Direction



Une fois les sites créés, vous pouvez adopter des périphériques et configurer les réseaux de chaque site séparément. Les étapes suivantes prennent des configurations pour le siège du site à titre d’exemple. Les configurations pour la branche du site sont illustrées par des conseils dans les étapes 4-6.

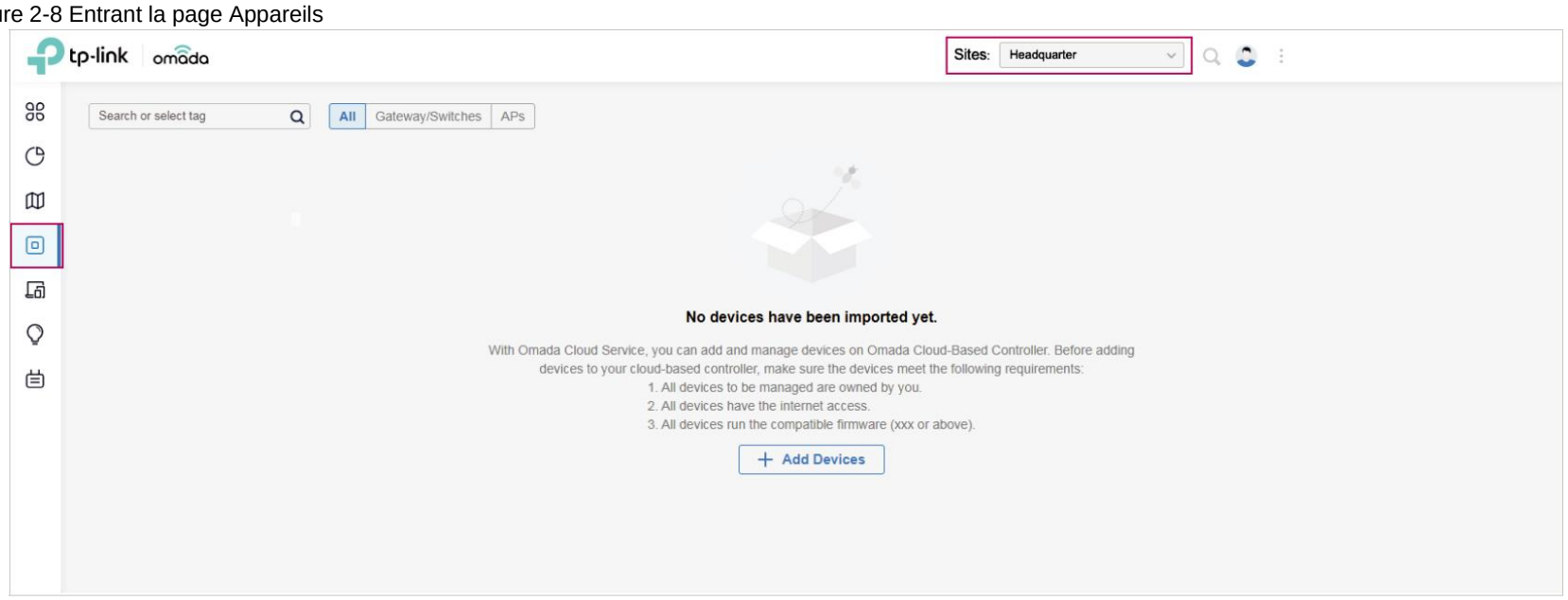
4. Adopter des dispositifs pour le site.

Conseil: De même, vous pouvez adopter des appareils pour la branche du site.

a. Sélectionnez le site actuel en tant que siège social et cliquez sur la barre latérale pour entrer la page **Appareils.**

b. Cliquez et la fenêtre suivante apparaîtra

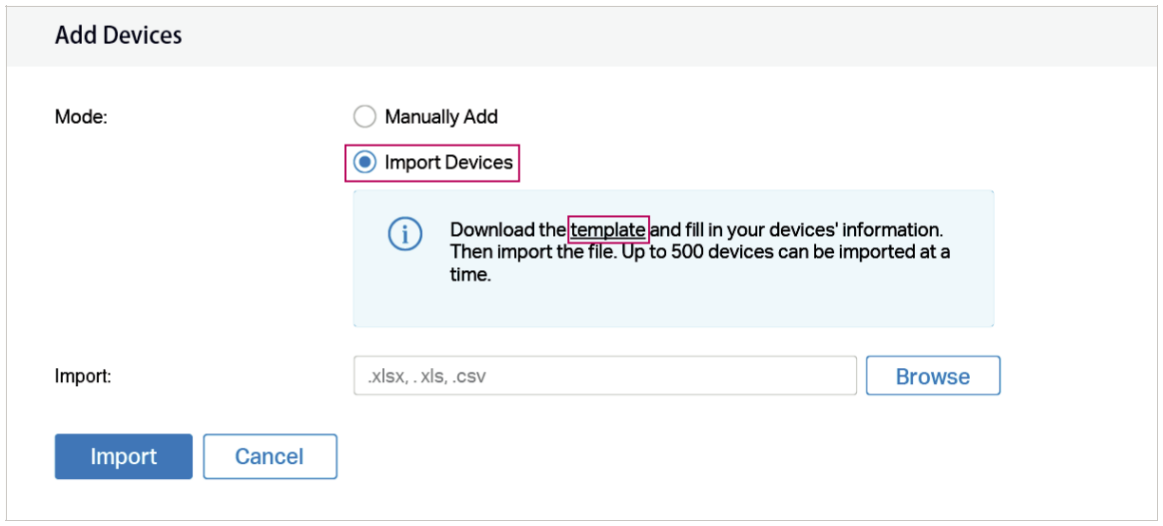
Figure 2-8 Entrant la page Appareils



Add Devices

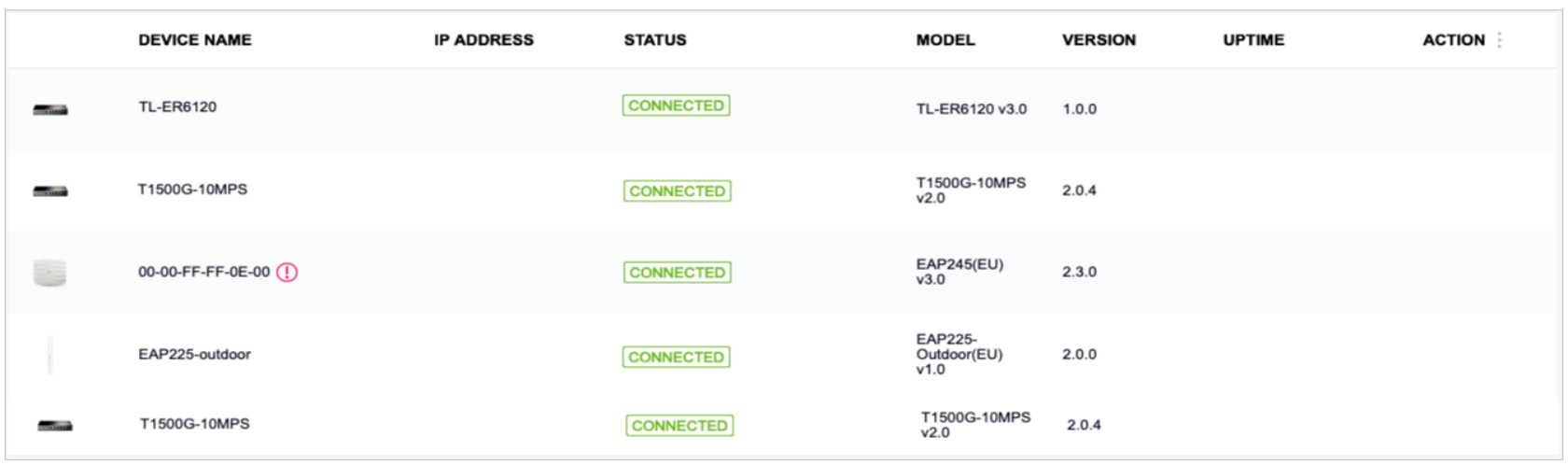
Pour ajouter des périphériques en lots, spécifiez le mode comme périphériques d’importation et téléchargez le modèle pour remplir les numéros de série des appareils pour le siège.

Figure 2-9 Télécharger le modèle



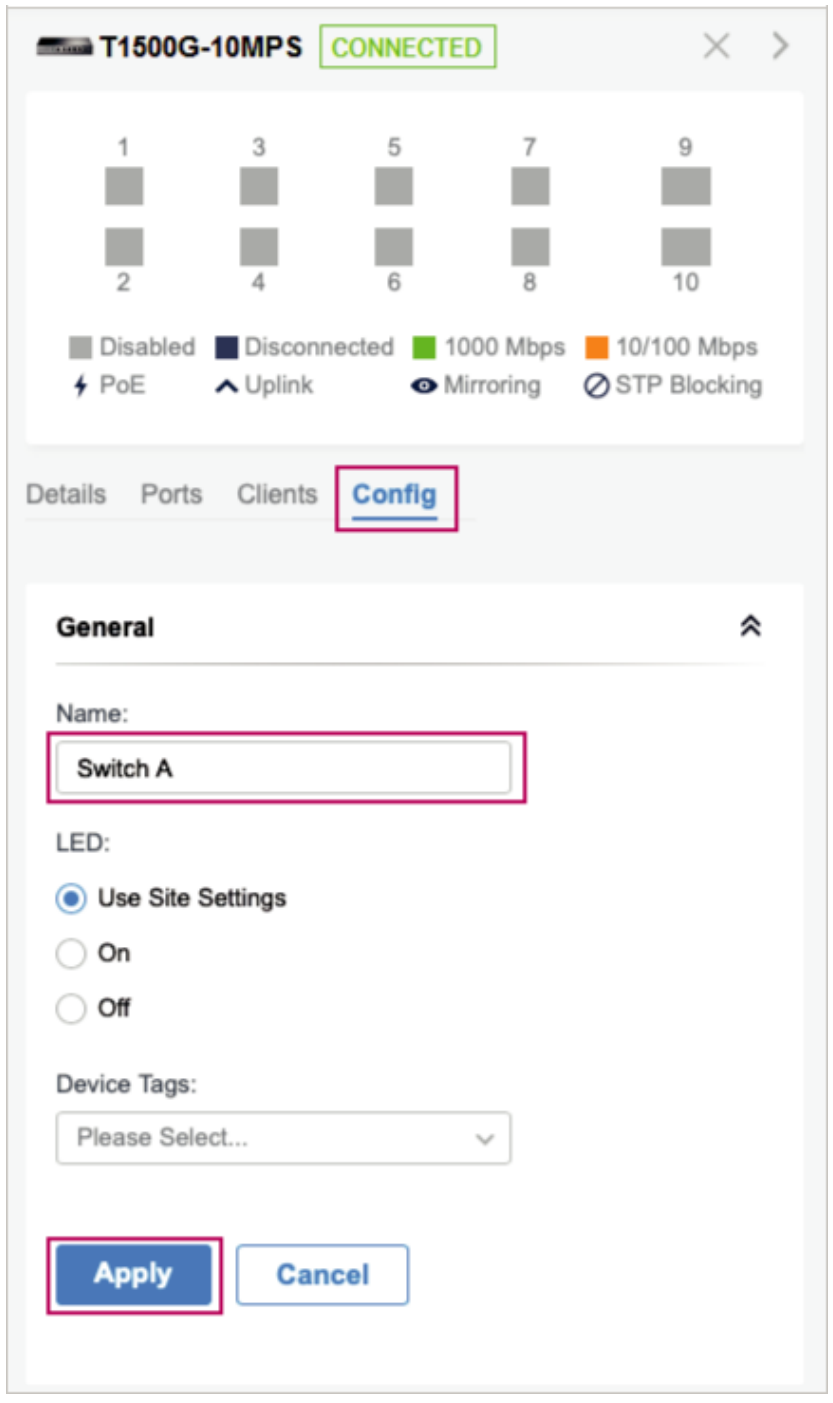
c. L’importation du fichier et des périphériques (avec les paramètres par défaut de l’usine) sera automatiquement adoptée par le contrôleur. Vous pouvez afficher les périphériques sur la page **Appareils.** page.

Figure 2-10 Liste des appareils



d. Cliquez sur un appareil dans la liste, et la fenêtre Propriétés de l’appareil sera affichée sur le côté droit. Vous pouvez donner un nom reconnaissable pour l’appareil sur sa page **Config.** page.

Figure 2-11 Changement de nom des périphériques



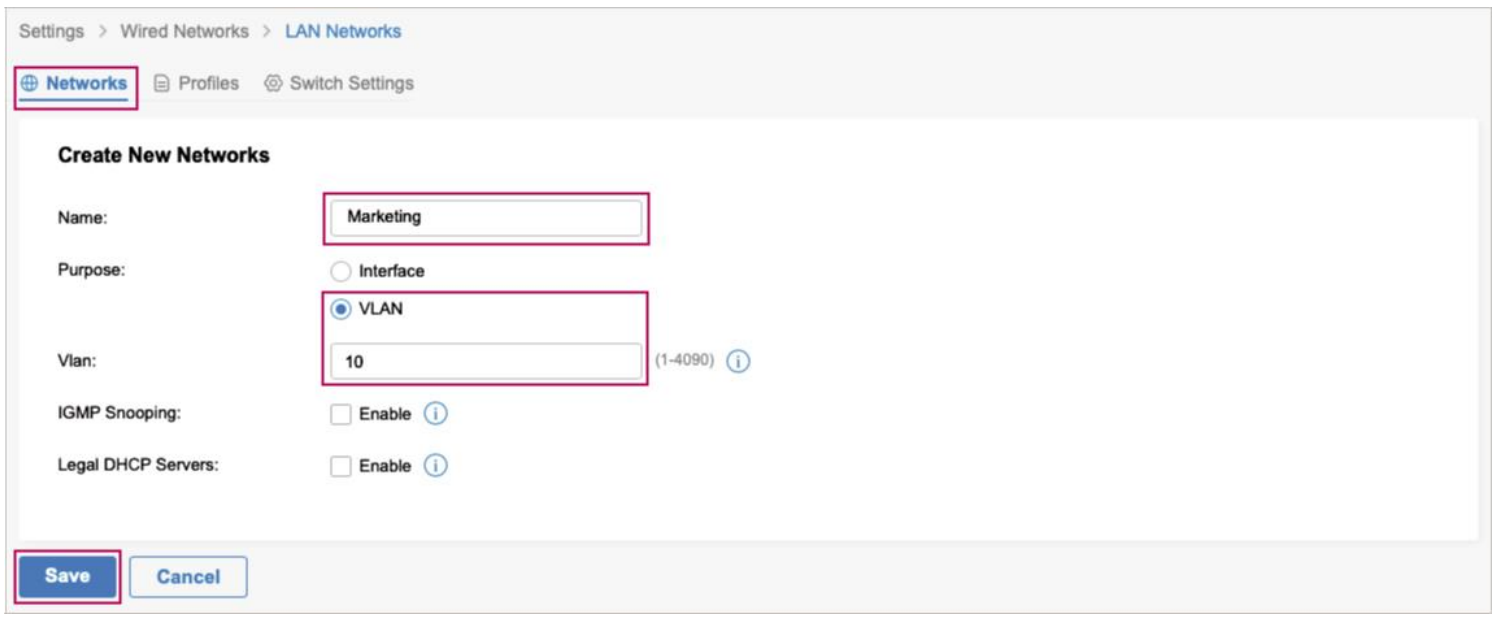
5. Configurer les réseaux LAN.

Conseil: Pour la Direction générale du site, suivez les étapes pour créer un réseau LAN et un profil portuaire pour le département de recherche et développement. Les configurations du réseau LAN et du profil portuaire sont les mêmes que celles du siège social du site et sont appliquées aux ports 2 à 10 sur le commutateur D.

a. Aller à **Paramètres >Wired Networks >LAN Networks.**

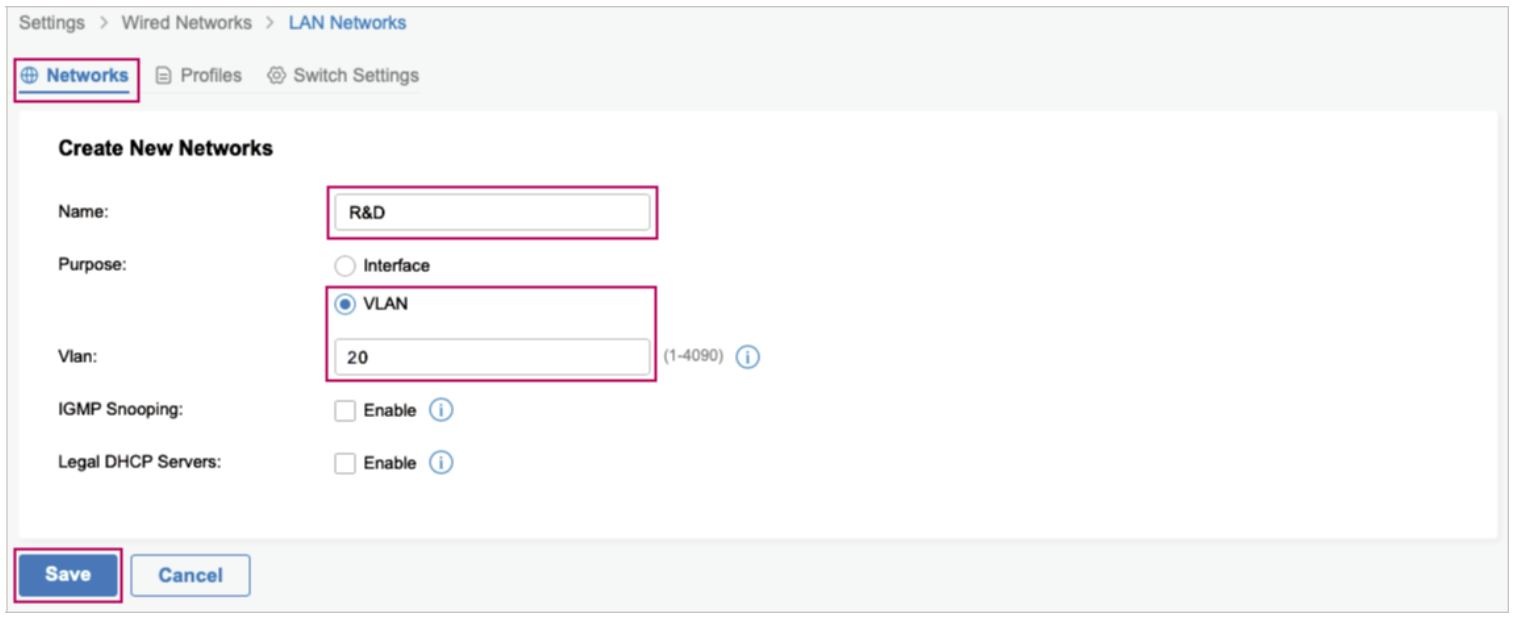
b. Sur l'onglet **Réseaux,** cliquez pour créer un réseau LAN pour le service Marketing. Configurez le But comme VLAN et le VLAN ID comme 10.

Figure 2-12 Création d'un réseau pour le département marketing



c. De même, créez un réseau LAN avec le VLAN ID 20 pour le département de recherche et développement.

Figure 2-13 Création d'un réseau pour le Département de la recherche et du développement



d. Sur l'onglet **Profils,** cliquez sur + Create New Port Profile pour créer des profils portuaires pour les deux réseaux avec les paramètres suivants :

Tableau 2-1 Profils portuaires pour les réseaux

Nom	Réseau autochtone	Réseaux Tagged	Réseaux non étiquetés
Marketing	Marketing	/	LAN, Marketing
R-D	R-D	/	LAN, R-D

Figure 2-2 Création de profils portuaires pour le réseau de marketing

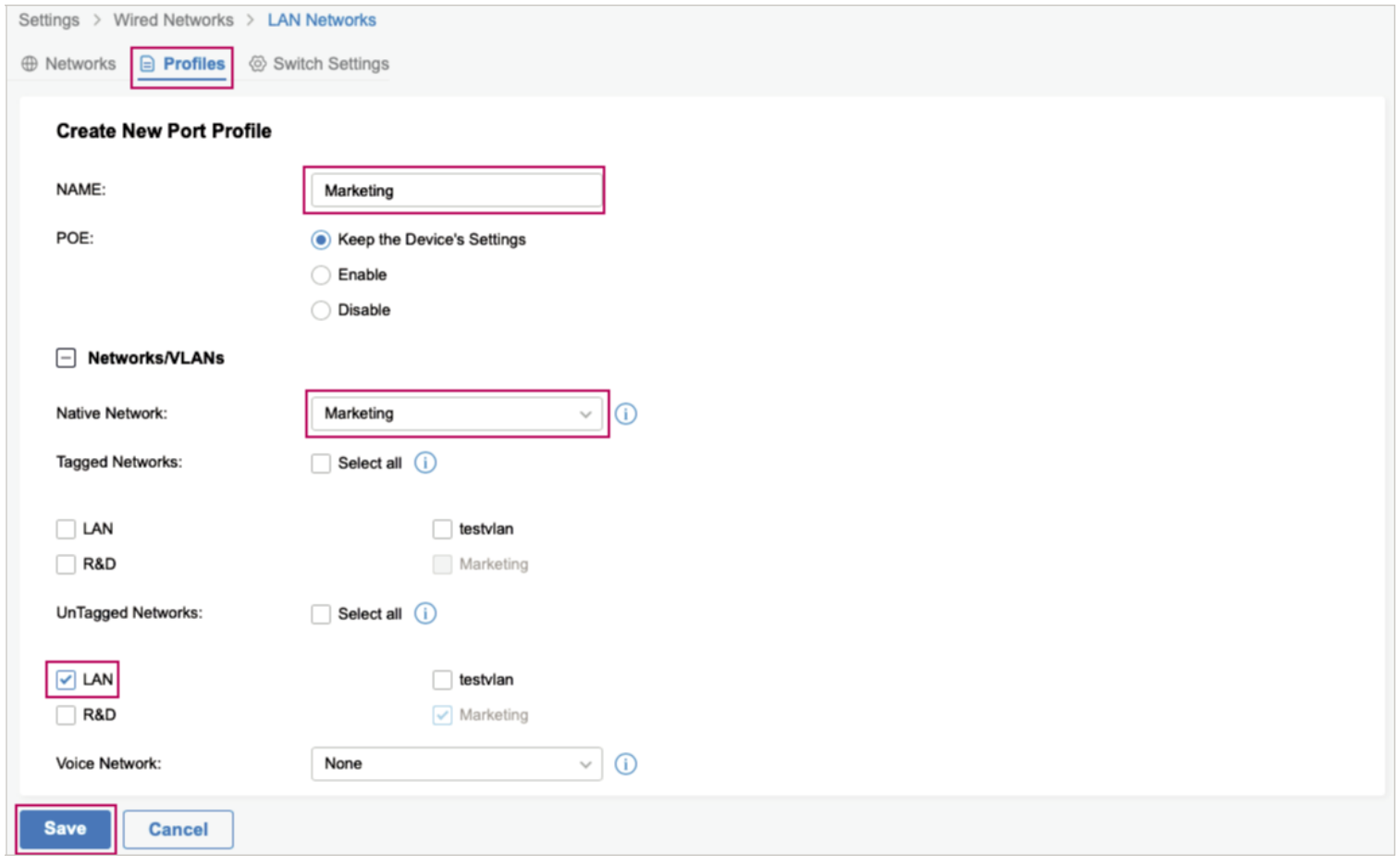
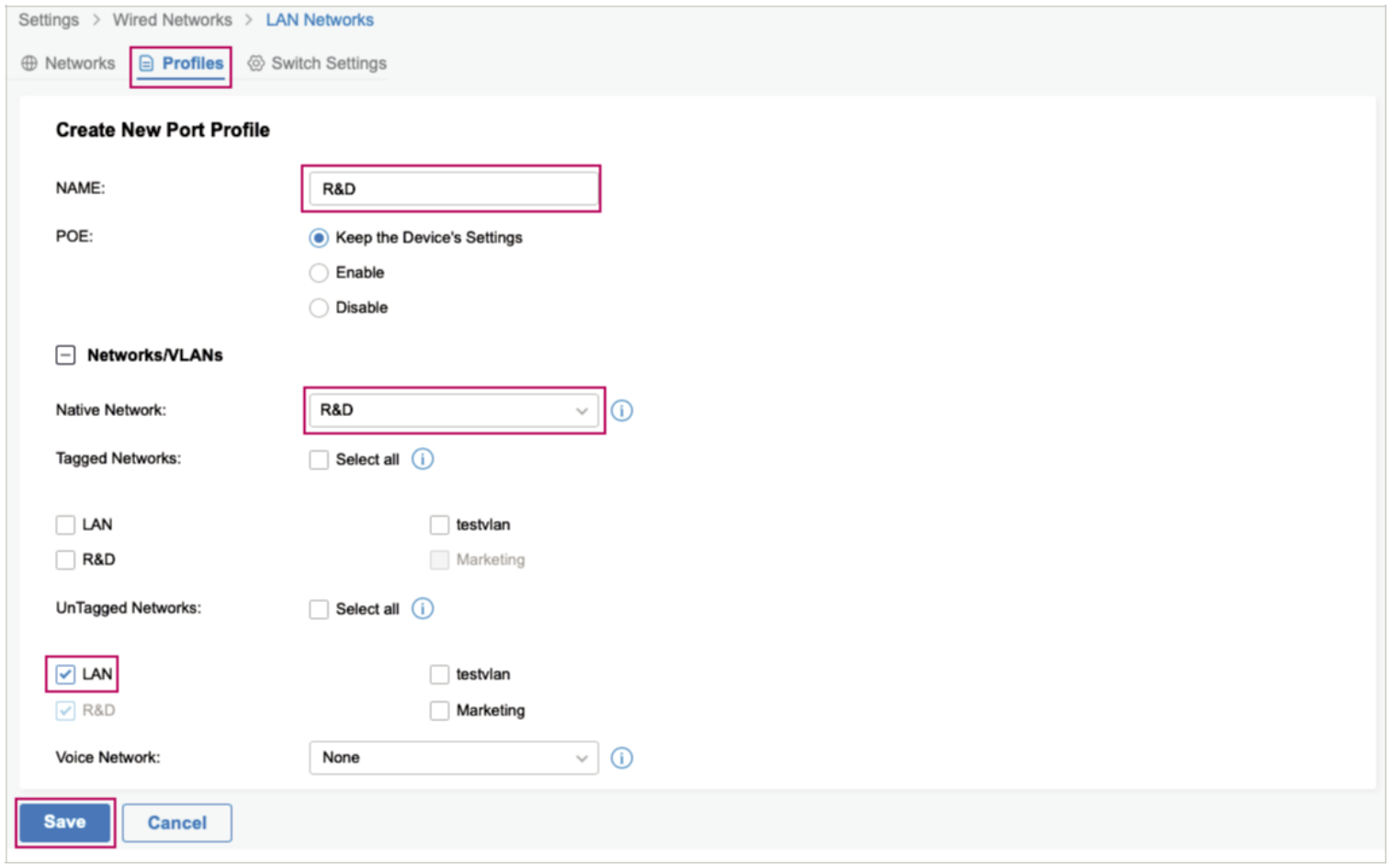


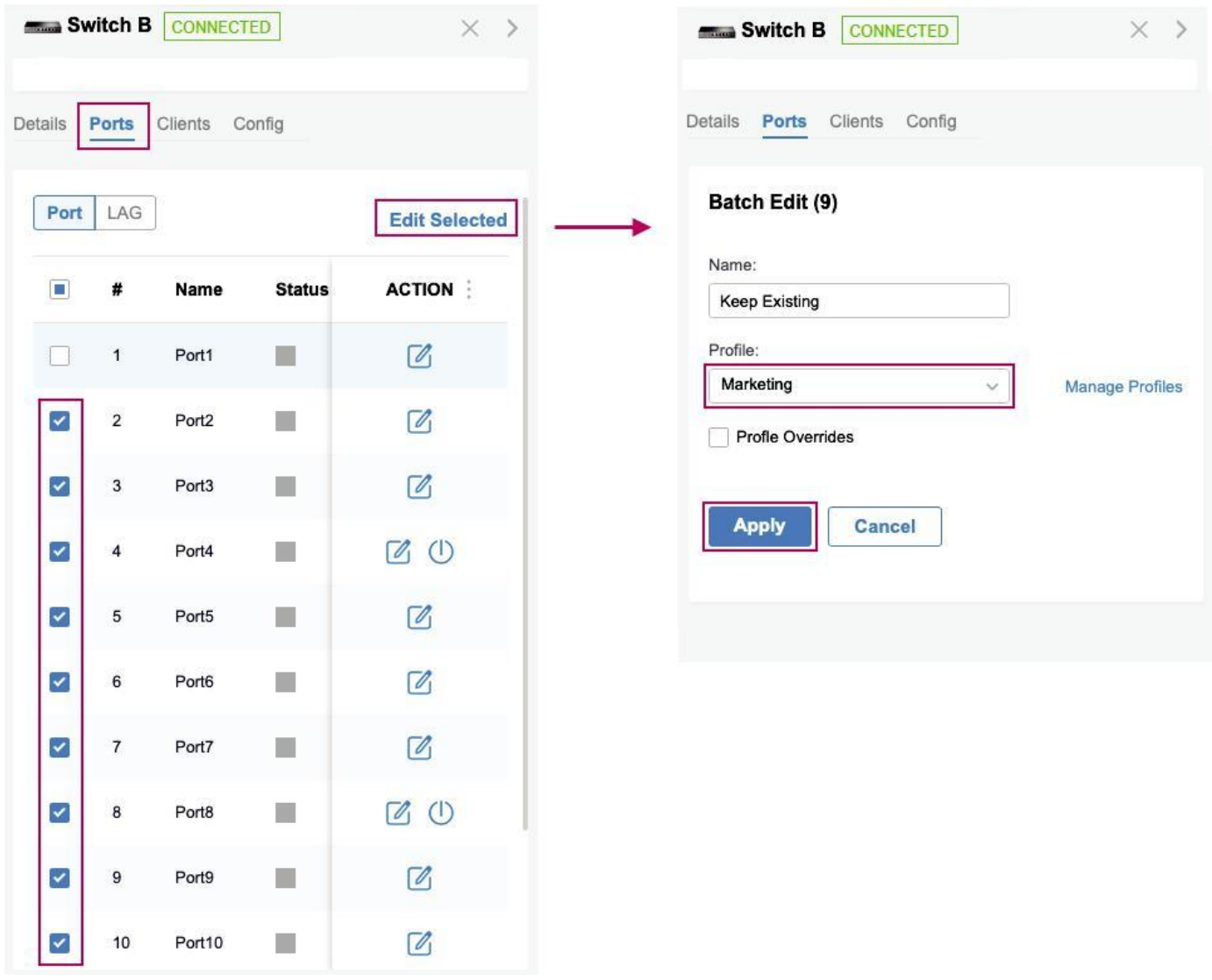
Figure 2-3 Création de profils portuaires pour le réseau de R-D



e. Sur l'onglet **Paramètres d'interrupteur,** cliquezà côté du commutateur B pour révéler sa fenêtre Propriétés. Sur l'onglet **Ports,** sélectionnez les ports 2 à 10 et cliquez sur Edit **Selected**.

Vous entrerez le mode d'édition par lots. Sélectionnez le profil sous forme de Marketing et cliquez sur **Appliquer**.

Figure 2-4 Appliquer les profils portuaires aux ports de Switch B



f. De même, appliquez le profil R-D aux ports 2-10 sur le commutateur C.

6. Configurer les réseaux sans fil.

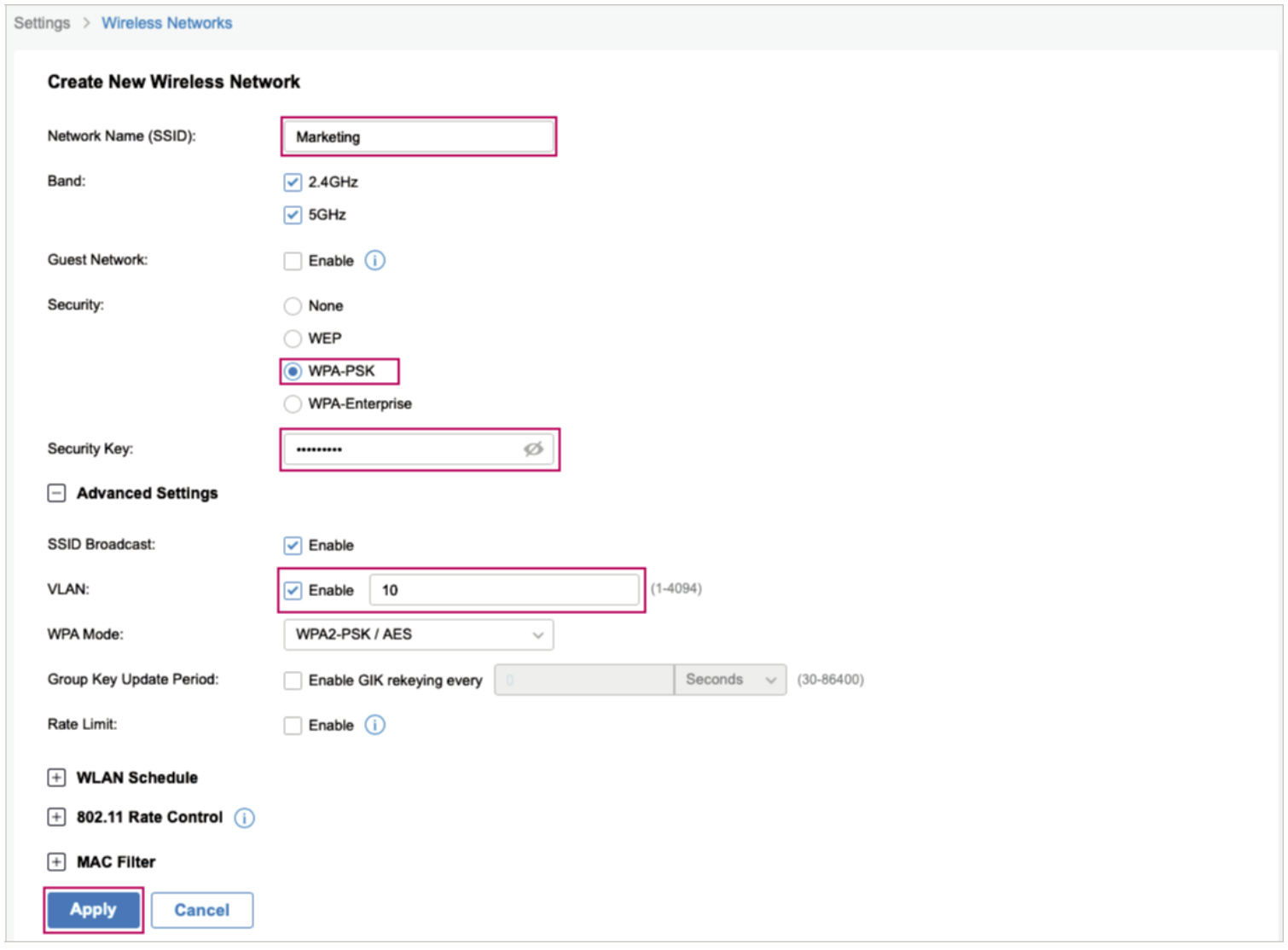
Les réseaux sans fil entreront en vigueur sur tous les PAE sur le site.

Conseil: Pour la direction du site, créez uniquement un réseau sans fil avec le VLAN ID 20 pour le département de recherche et développement.

a. Aller à **Paramètres> Réseaux sans fil**.

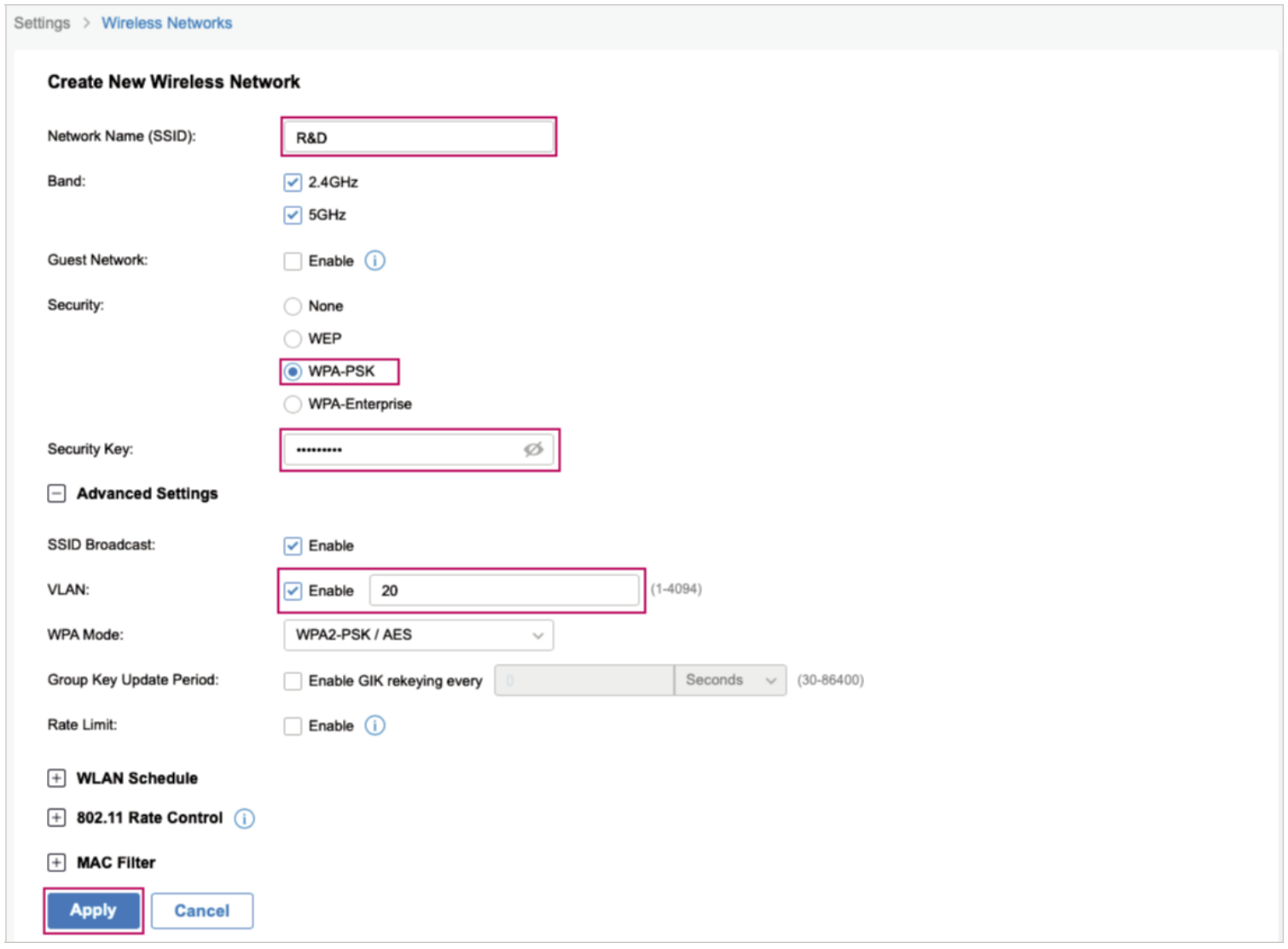
b. Cliquez pour créer un réseau sans fil pour le service Marketing. Configurez le nom du réseau sous le nom de Marketing, le mode de sécurité WPA-PSK, et configurez une clé de sécurité pour le réseau sans fil. Dans la section **Paramètres avancés,** activez VLAN et configurez l’ID VLAN comme 10.

Figure 2-5 Création d’un réseau sans fil pour le service marketing



c. De même, créez un réseau sans fil pour le département de recherche et développement. Configurer le nom du réseau comme R-D et le VLAN ID comme 20.

Figure 2-6 Création d’un réseau sans fil pour le département de recherche et développement

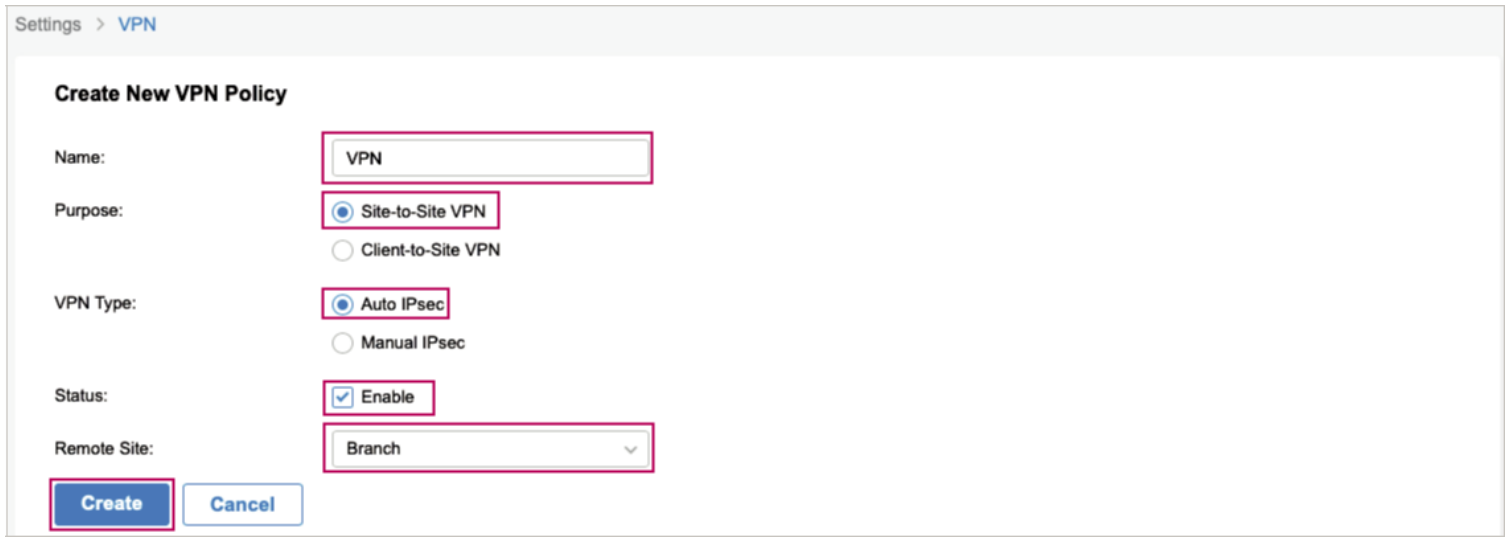


6) Construire un tunnel VPN pour les deux sites.

a. Aller à **Paramètres >VPN** et cliquez sur

b. Configurez le but en tant que VPN site-à-site, le type VPN comme Auto IPsec, l’état comme Active, et spécifiez le site distant en tant que branche. Cliquez ensuite sur Créer. Un tunnel VPN sera automatiquement mis en place entre le site actuel (siège social) et le site à distance spécifié (Branch)..

Figure 2-7 Création d’une politique VPN



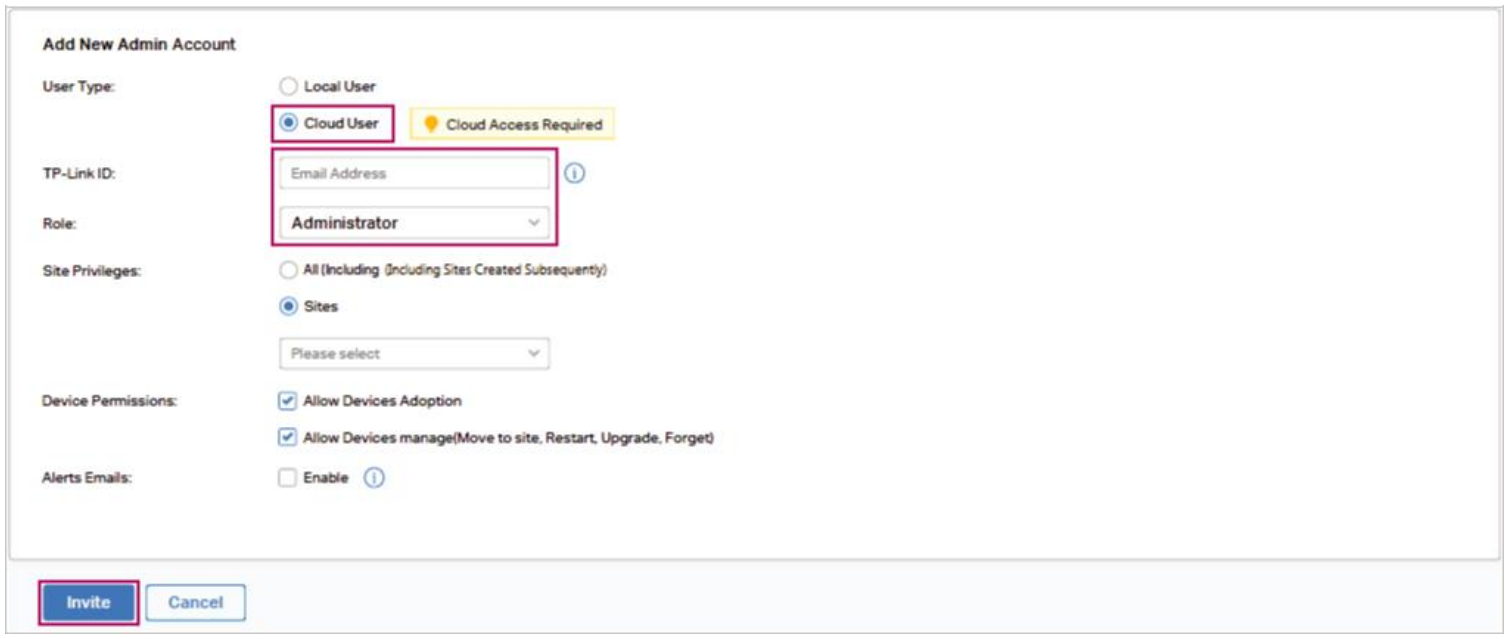
Jusqu’à présent, vous avez terminé les configurations. Tous les appareils obtiendront automatiquement les fichiers de configuration d’Omada Cloud et développeront un réseau Omada.

2.4 Autoriser le client à gérer le réseau

Pour permettre au client de surveiller et de gérer le réseau, suivez les étapes ci-dessous pour créer un compte Admin. Ensuite, fournissez le compte Admin et l’adresse IP du contrôleur basé sur le cloud au client.

1) Cliquez sur la barre latérale pour aller à la page **Admins.**
2) Cliquez + Add New Admin Account pour créer un compte.

Figure 2-8 Création de compte d’administrateur pour le client



a. Sélectionnez le type d’utilisateur en tant qu’utilisateur Cloud et entrez l’adresse e-mail du client. Le contrôleur enverra un courriel d’invitation à l’adresse e-mail. Si l’adresse e-mail est déjà enregistrée avec un ID TP-Link, elle deviendra un compte utilisateur cloud valide après avoir accepté l’invitation. Si ce n’est pas le cas, il sera invité à l’inscription et deviendra automatiquement un compte utilisateur cloud valide après avoir terminé l’enregistrement.
b. Configurer le rôle d’administrateur, unnd assigner des privilèges de site pour le compte. Si le contrôleur basé sur le cloud n’est utilisé que par le client, sélectionnez **Tous (y compris les sites créés par la suite)**; s’il est partagé par d’autres clients, sélectionnez des **sites** et assignez uniquement les sites Siège et Branche à l’unccount.
c. Spécifier les autorisations de l’appareil et cliquez sur **Inviter**.

Le client pourra accéder à la page de gestion du contrôleur après avoir accepté l’invitation. Omada SDN Controller fournit un tableau de bord facile à utiliser, permettant au client de surveiller facilement l’état du réseau en temps réel, de vérifier l’utilisation du réseau et la distribution du trafic, ou même de suivre les données clés des clients pour de meilleurs résultats d’affaires.

En outre, le contrôleur prend en charge la connexion muti-compte. Le client peut créer d’autres comptes Admin avec différents rôles (Administrateur ou Viewer) en fonction des besoins réels.

3 Configuration des fonctionnalités avancées

Le réseau Omada SDN offre des fonctionnalités riches pour assurer des performances élevées et une excellente expérience utilisateur. Ce chapitre répertorie les fonctionnalités les plus utilisées. Accordez le réseau avec les fonctionnalités en fonction des besoins réels de votre client.

3.1 Optimisation de l’utilisation et contrôle de la bande passante

Qu’est-ce que le contrôle de la bande passante?

Le contrôle de bande passante vous permet de distribuer la bande passante réseau en fonction des utilisateurs, des réseaux ou des groupes IP. En configurant les règles de contrôle de bande passante, vous pouvez limiter la quantité de bande passantequ’un ser u ou les utilisateurs dans des réseaux spécifiques ou des groupes IP peuvent utiliser.

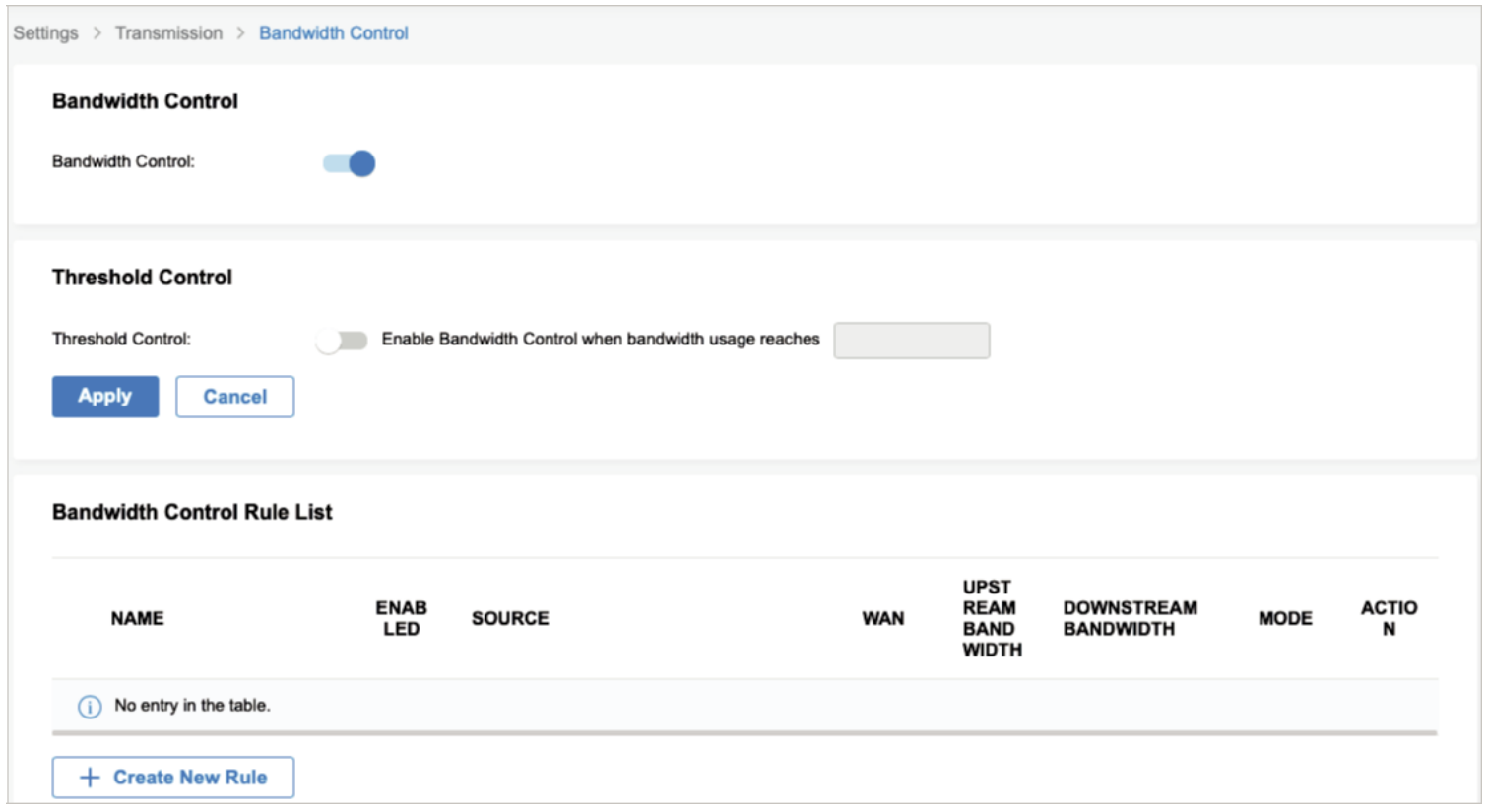
Le contrôle de la bande passante est important pour éviter le trafic réseau "goulots d’étranglement". Normalement, la bande passante du FAI est partagée par tous les terminaux sous la passerelle. Lorsque l’un des terminaux utilise une bande passante élevée, unepplication comme les programmes torrent, les autres peuvent connaître un ralentissement des activités réseau normales comme le transfert de fichiers entre ordinateurs ou tout simplement naviguer sur le Web.

Avec Le contrôle de la bande passante, vous pouvez minimiser l’impact causé par la congestion du réseau. En fixant des limites pour chaque utilisateur, réseau ou groupe IP, la bande passante réseau peut être raisonnablement distribuée et utilisée.

Comment le configurer ?

Aller à **Paramètres 'gt; Transmission 'gt; Contrôle de bande passante** pour charger la page suivante.

Figure 3-1 Contrôle de la bande passante configuration



Pour configurer le contrôle de la bande passante, suivez les étapes ci-dessous :

1) Activez le contrôle de la bande passante. Il est activé par défaut.
2) Activez le contrôle des seuils et configurez le seuil. Le contrôle de la bande passante n'entre en vigueur que lorsque l'utilisation totale de la bande passante atteint le seuil.
3) Cliquez + Create New Rule pour créer des règles de contrôle de bande passante.

3.2 Blocage d'utilisateurs non autorisés avec 802.1X Authentification

Qu'est-ce que l'authentification 802.1X?

802.1X fournit un service d'authentification portuaire pour empêcher les clients non autorisés d'accéder au réseau par l'intermédiaire de ports de commutation accessibles au public. Un port compatible 802.1X n'autorise que les messages d'authentification et interdit un trafic normal jusqu'à ce que le client passe l'authentification.

Le commutateur fournit également deux fonctionnalités qui sont basées sur l'authentification 802.1X:

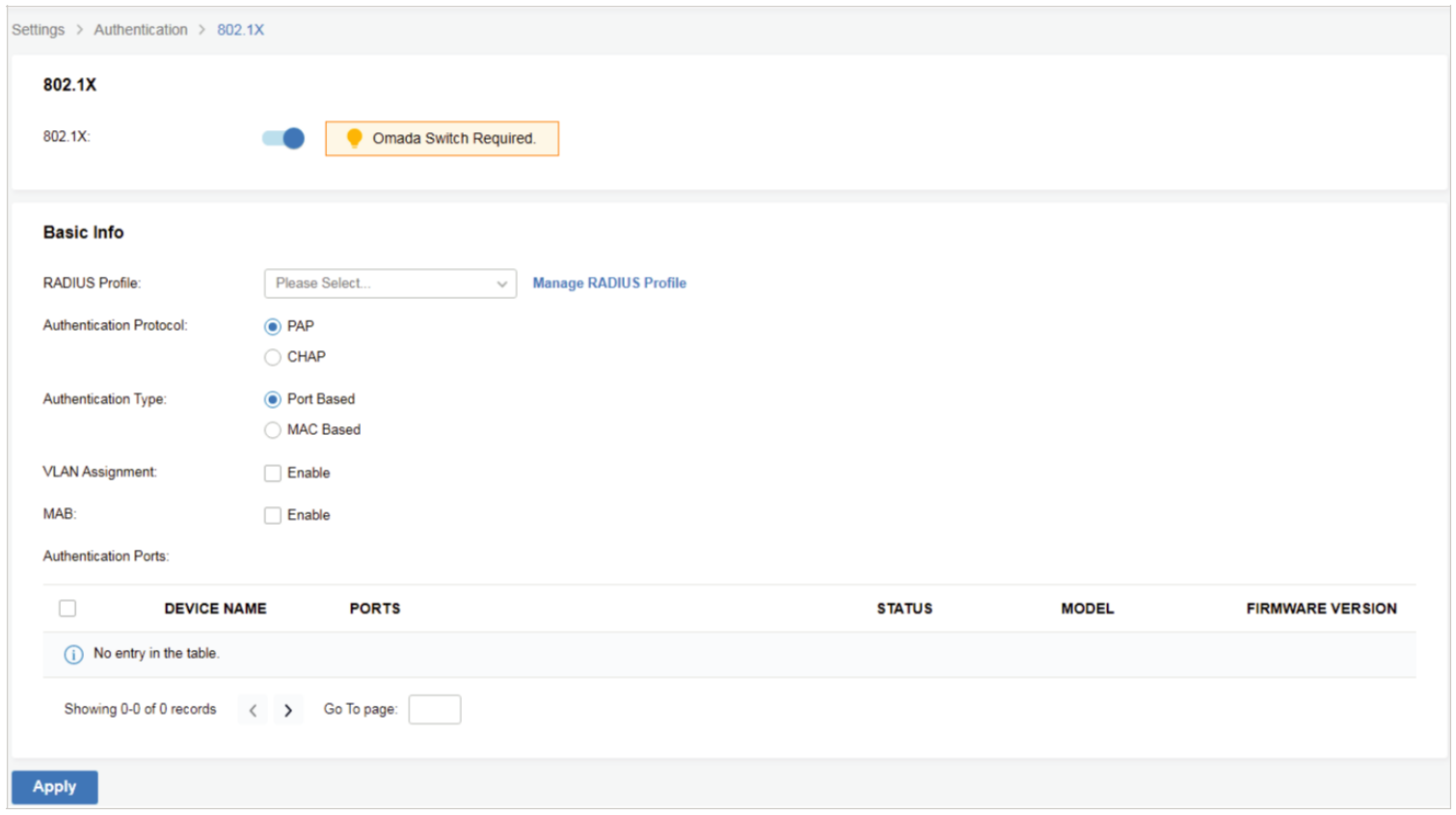
- Affectation VLAN : assigne dynamiquement les ports authentifiés aux VLAN. Les cartes nom d'utilisateur-VLAN doivent déjà être stockées dans la base de données du serveur RADIUS.

MAB (MAC Authentication Bypass) : permet aux clients d'être authentifiés sans aucun logiciel client installé. MAB est utile pour lesappareils authenticatin g sans capacité 802.1X comme les téléphones IP.

Comment le configurer ?

Aller à **Paramètres 'gt; Authentication 'gt; 802.1X** pour charger la page suivante.

Figure 3-2 Configuring 802.1X Authentification



Pour configurer l’authentification 802.1X, suivez les étapes ci-dessous :

1. Activez le 802.1X.
2. Sélectionnez le profil RADIUS que vous avez créé et configurez d’autres paramètres. Le profil RADIUS comprend les informations du serveur RADIUS qui agit comme serveur d’authentification lors de l’authentification 802.1X.
3. Sélectionnez les ports sur lesquels 802.1X Authentification entrera en vigueur.

3.3 Fournir un accès temporaire aux visiteurs avec l’authentification du portail

Qu’est-ce que Portal Authentication ?

L’authentification du portail offre un service d’authentification aux clients qui n’ont besoin que d’un accès temporaire au réseau, comme les visiteurs d’un bureau ou les clients d’un restaurant. Pour accéder au réseau, ces clients doivent entrer la page de connexion d’authentification et utiliser les informations de connexion correctes pour passer l’authentification. Vous pouvez annoncer votre entreprise en personnalisant la page de connexion d’authentification.
Pour permettre auxclients non-tiers d’accéder aux ressources réseau spécifiques, vous pouvez configurer les stratégies de pré-authentification.

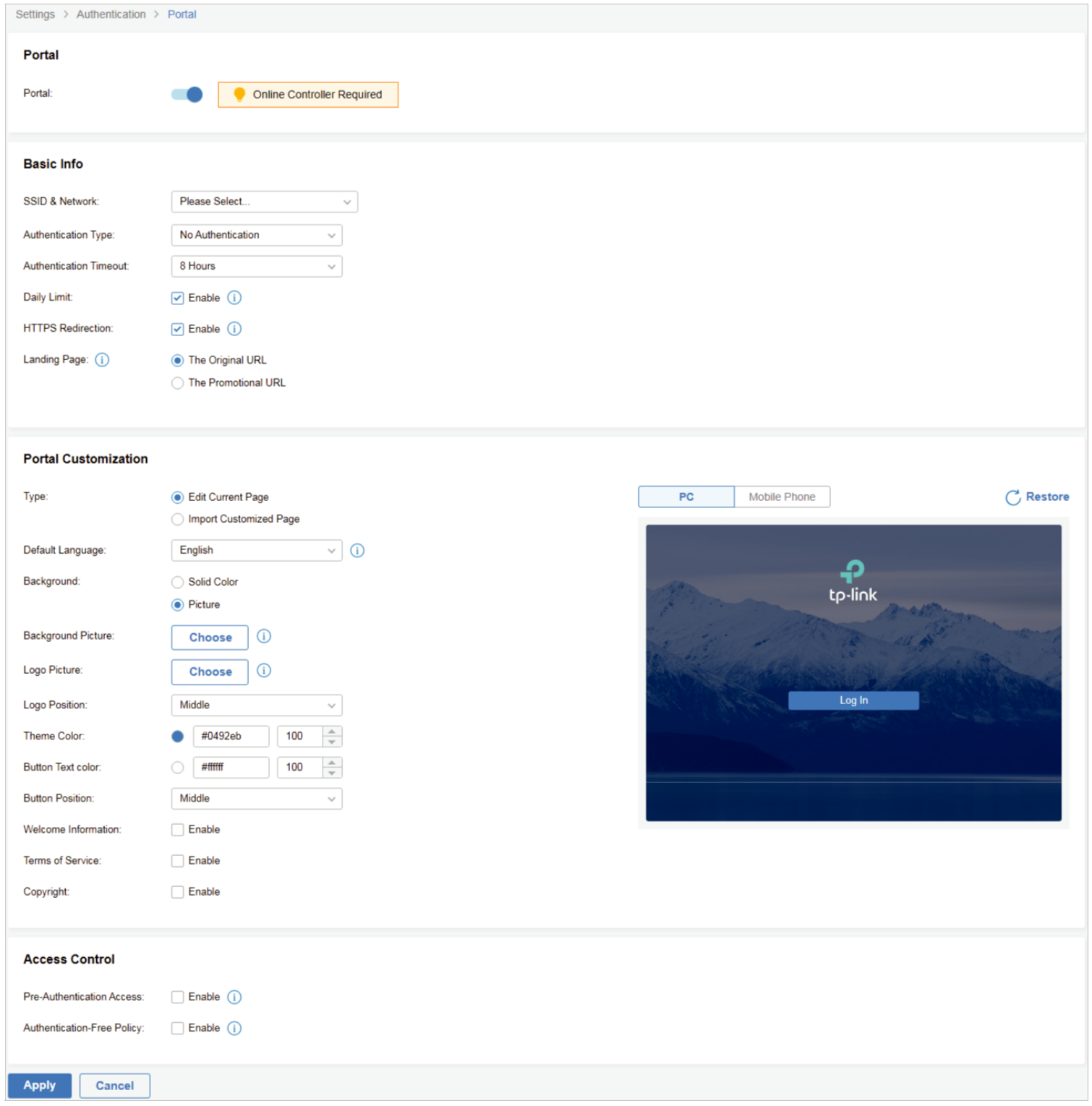
Pour permettre aux clients spécifiques comme les employés d’accéder au réseau sans authentification, vous pouvez configurer les stratégies Authentication-Free.

L’authentification du portail prend effet sur les SSID et les réseaux LAN. Les PAE authentifient les clients sans fil qui se connectent au SSID avec Portal configuré, et la passerelle authentifie les clients câblés qui se connectent au réseau avec Portal configuré. Pour rendre l’entication Portal authdisponible pour les clients câblés et sans fil, assurez-vous que la passerelle et les PAE sont connectés et fonctionnent correctement.

Comment le configurer ?

Aller à **Paramètres > Authentication > Portal** pour charger la page suivante.

Figure 3-3 Configuring Portal Authenticaiton



Pour configurer l’authentification du Portail, suivez les étapes ci-dessous :

1) Activez Portal.
2) Sélectionnez les SSID et les réseaux LAN pour que le portail entre en vigueur et configure d’autres paramètres de base.
3) Personnalisez la page Portal, y compris l’image de fond, l’image du logo et ainsi de suite.
4) Configurez les règles de contrôle d’accès, y compris l’accès préalable à l’authentification et la politique sans authentification si nécessaire.

3.4 Construire une connexion Wi-Fi transparente avec Mesh et Fast Roaming

Qu’est-ce que Mesh et Fast Roaming?

Dans un réseau domestique traditionnel, un point d’accès (AP) se connecte à Internet et diffuse des signaux Wi-Fi, qui ne peuvent généralement pas couvrir tous les coins du site. Parfois, vous pouvez utiliser plusieurs AP pour étendre la couverture Wi-Fi. Cependant, chaque AP forme un réseau séparé avec différents paramètres Wi-Fi. Lorsque vous errez d’un AP à l’autre, votre expérience Internet souffrira de longs temps de chargement et de décalage. Comment conserver une connexion Internet constante ? Vous avez deux choix : construire un réseau de maillage ou permettre Fast Roaming.

Mesh Mesh

Dans un réseau Wi-Fi en maille, plusieurs AP se connectent pour former un réseau unique et unifié qui partage les mêmes paramètres Wi-Fi. Ces paramètres comprennent le nom du réseau, le mot de passe, les paramètres de contrôle d’accès, et plus encore. Ce système Wi-Fi unifié offre à votre site une couverture Wi-Fi. Pour construire le système Wi-Fi unifié, tous les PAE devraient prendre en charge Omada Mesh.

L’itinérance rapide

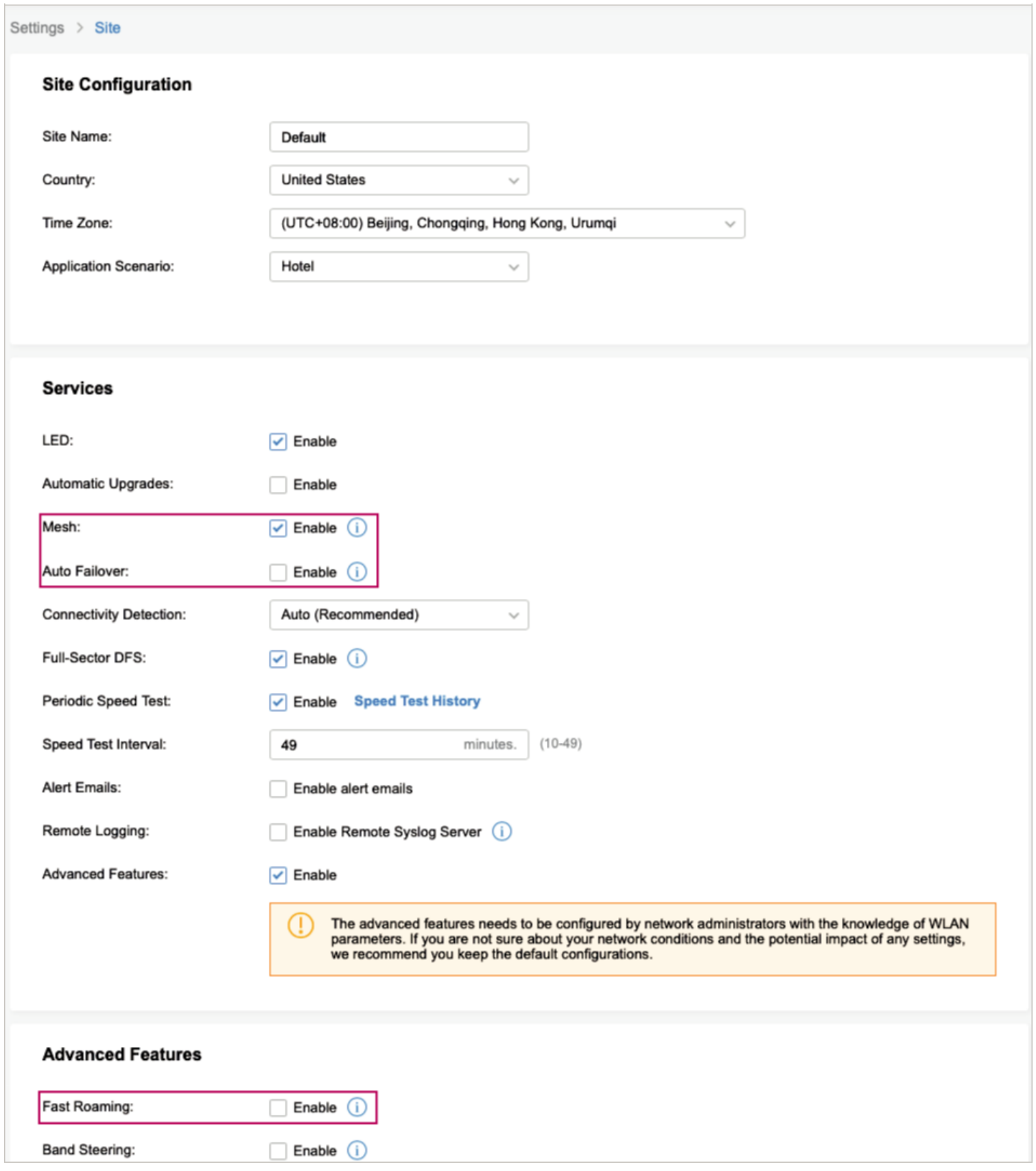
Fast Roaming améliorer l’expérience d’itinérance en raccourcissant le temps qu’il faut à un client sans fil pour passer d’un AP à l’autre. Du point de vue de l’utilisateur, l’interruption du signal lors de l’utilisation d’un téléphone, d’une tablette ou d’un ordinateur portable sera imperceptible parce que Fast Roaming rend la transition si rapide.

Comment rendre l’itinérance plus rapide? L’IEEE propose trois solutions : IEEE 802.11k, 802.11v et 802.11r. TP-Link combine les avantages de 802.11k et 802.11v pour développer sa technologie Fast Roam. Pour profiter de l’itinérance rapide, les clients ont besoin de to support IEEE 802.11k/v.

Comment les configurer ?

Accédez à **Paramètres et site** pour charger la page suivante.

Figure 3-4 Permettant Mesh et Fast Roaming



Pour construire un réseau de maillage, activez Mesh dans la section **Services.** Tous les PAE qui prennent en charge Mesh sur le site construiront automatiquement un réseau de maillage. En outre, pour assurer la stabilité du réseau de maillage, activez Auto Failover. Lorsqu'un lien dans le réseau de maillage échoue, le contrôleur établit automatiquement un autre lien pour s'assurer que tous les PAE sont toujours dans le réseau de maillage.

Pour faire l'expérience de l'itinérance rapide, activez l'itinérance rapide dans la section **Fonctions avancées.** 802.1k/v clients peuvent errer de façon transparente parmi les PAE.

3.5 Contrôle des droits d'accès avec ACL

Qu'est-ce que ACL (Liste de contrôle d'accès)?

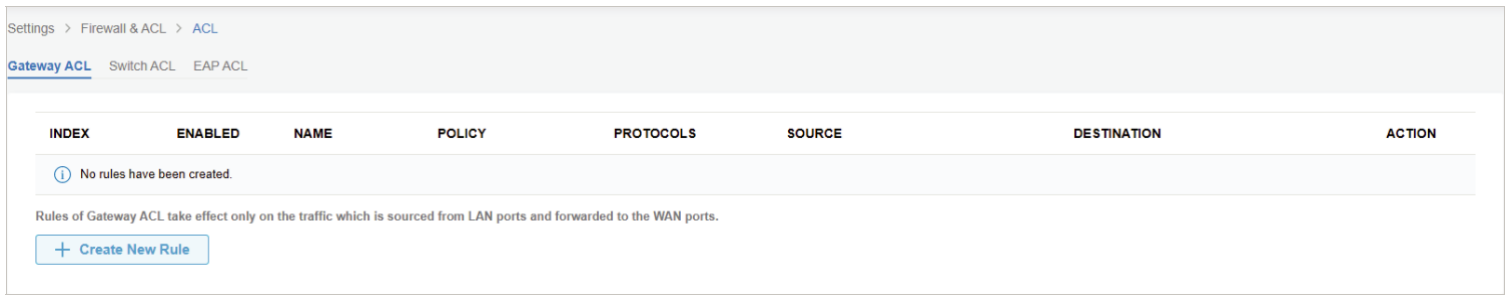
ACL (Access Control List) permet à un administrateur réseau de créer des règles pour restreindre l'accès aux ressources réseau. Les règles ACL filtrent le trafic en fonction de critères spécifiques tels que les adresses IP source, les adresses IP de destination et les numéros de port, et déterminent s'il faut transmettre les paquets appariés. Ces règles peuvent être appliquées à des clients ou des groupes spécifiques dont le trafic passe par l'eway gat,les commutateurs et les PAE.

Le système filtre le trafic contre les règles de la liste de façon séquentielle. Le premier match détermine si le paquet est accepté ou abandonné, et d'autres règles ne sont pas vérifiées après le premier match. Par conséquent, l'ordre des règles est essentiel. Par défaut, les règles sont priorisées par leur temps créé. La règle créée plus tôt est vérifiée pour un match avec une priorité plus élevée. Pour réorganiser les règles, sélectionnez une règle et faites-la glisser vers une nouvelle position. Si aucune règle ne correspond, l'appareil transmet le packet en raison d'une clause implicite De tous les permis.

Comment le configurer ?

Aller à **Paramètres et pare-feu et ACL >ACL** pour charger la page suivante. Trois types d'ACL sont pris en charge : Gateway ACL, Switch ACL et EAP ACL.

Figure 3-5 Configurer ACL



1) Cliquez sur l'onglet pour choisir le type désiré.
2) Créez un LCA avec le type désiré et configurez les critères de filtrage des paquets pour la règle.