Omada Network Deployment Guide

CHAPTERS

CONTENTS

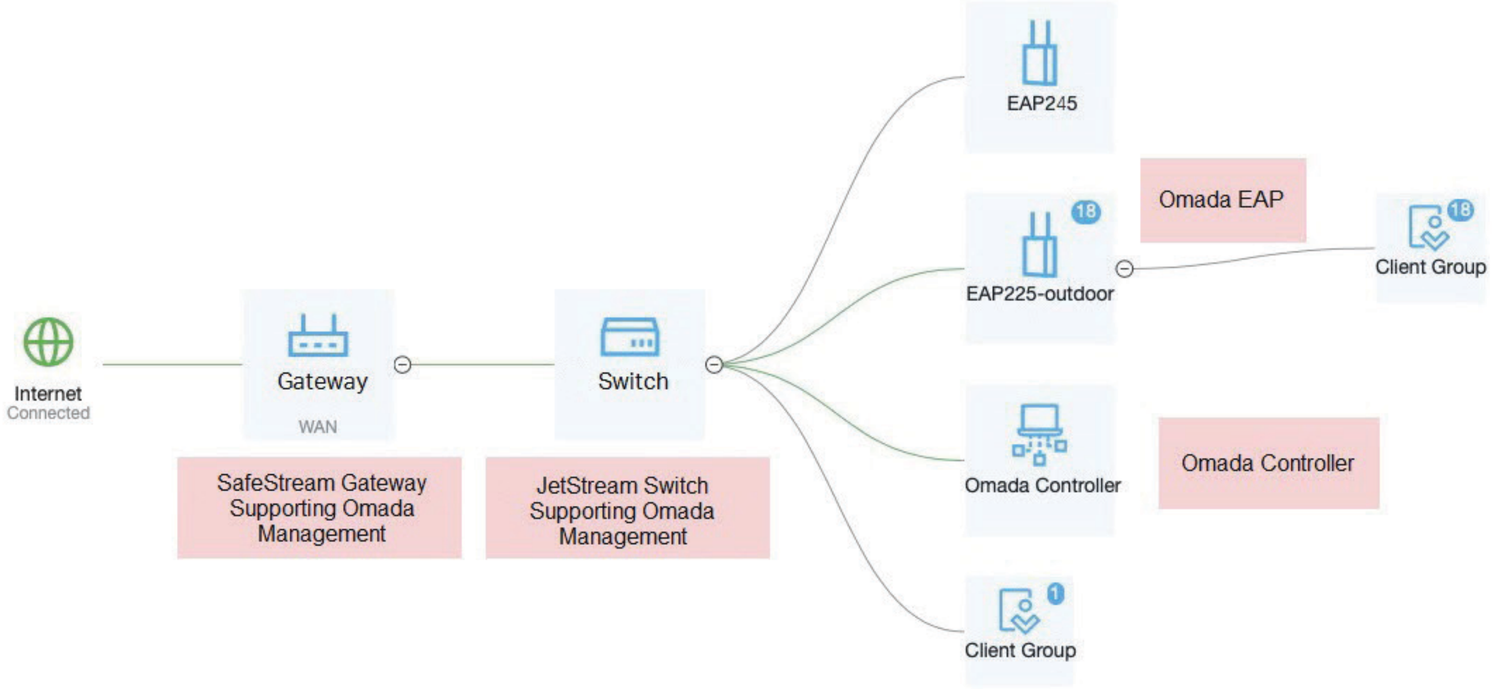
1 About Omada SDN

Upgrading from the current Omada solution, Omada SDN is a full Software Defined Networking (SDN) solution that integrates access points, switches, gateways, and more. It enables a system integrator (SI) to efficiently create networks of any size, from small to large, with high scalability.

Omada SDN Members

As the following figure shows, Omada SDN includes the following members:

- Omada Controllers
- Omada EAPs
- SafeStream Gateways with the firmware version that supports Omada management
- JetStream Switches with the firmware version that supports Omada management



Omada Controllers

Among all members, Omada Controllers are the core of Omada SDN solution. You can configure all Omada member devices and monitor the entire network simply via the controller's user interface. TP-Link provides multiple types of Omada Controllers, allowing you to choose the most appropriate one for your situation.

Controller Type	Description
Hardware Controller (OC200/OC300)	● Needs to be purchased additionally ● Takes small space to deploy with slim body ● Support cloud access
Software Controller	● Free to install and upgrade, but need a reserved computer to keep running if you use advanced features like Portal ● Supports cloud access
Cloud-Based Controller	● Deployed on Omada Cloud, provides paid service with tiered pricing ● Professional personalized service for networks with more than 500 devices

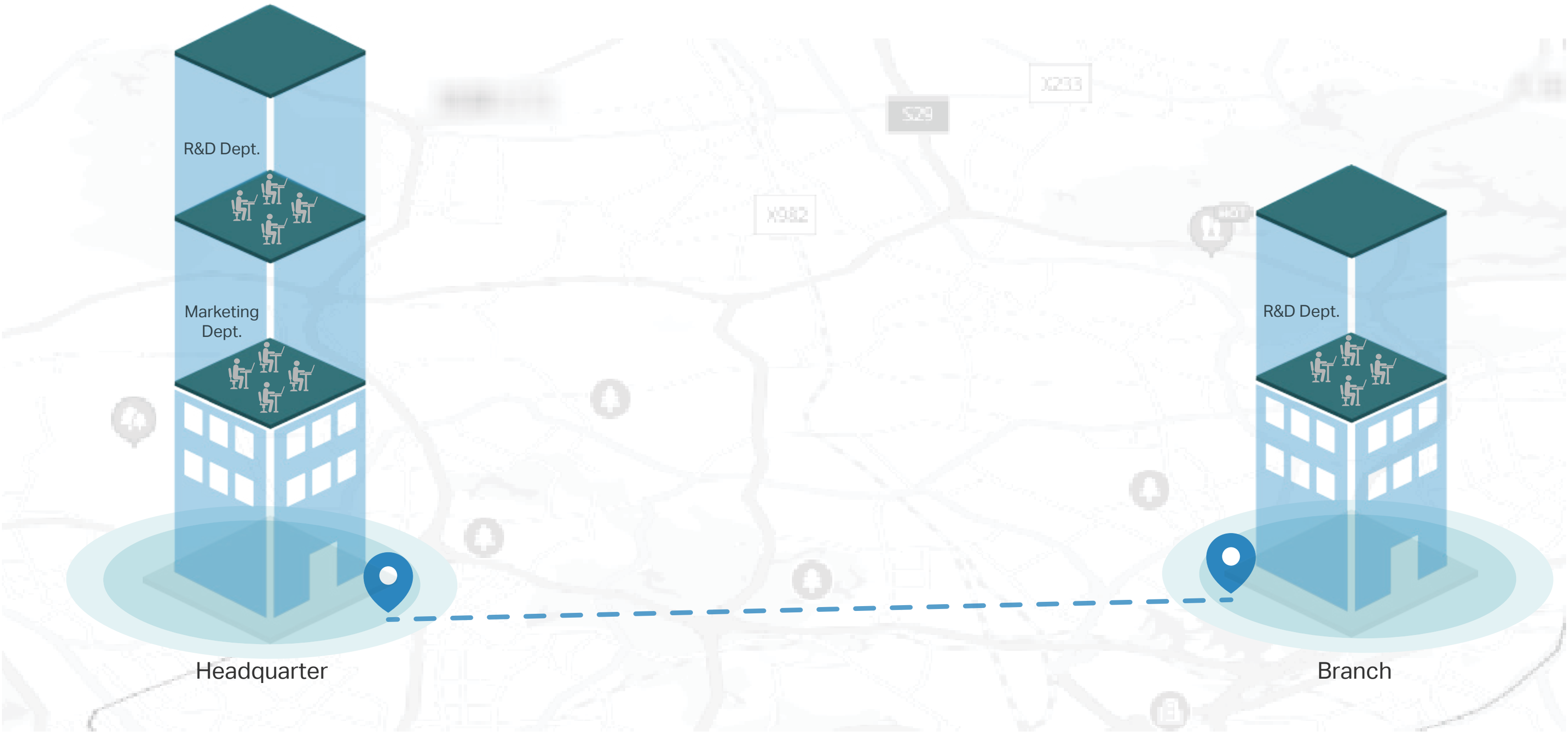
2 Setting Up a Basic Network

Omada SDN solution is designed to build scalable networks. Configurations vary according to actual situations. This chapter introduces how to set up a basic network through a typical application.

2.1 Network Requirements

A system integrator is planning a network for its customer, a company with two buildings. As the following figure shows, the Marketing Department is at the headquarter, while the R&D Department has two offices—one at the headquarter and the other in the branch.

Figure 2-1 Buildings of the Company



It is required that:

- The network should contain both wired and wireless networks to allow the access of various devices.
- To improve network efficiency and enhance security, the same department should be in the same network and different departments should be in different networks.
- The two departments need an FTP server for transmitting files with each other.
- For better management, the network administrator needs to centrally monitor and control the network at any time, from anywhere.

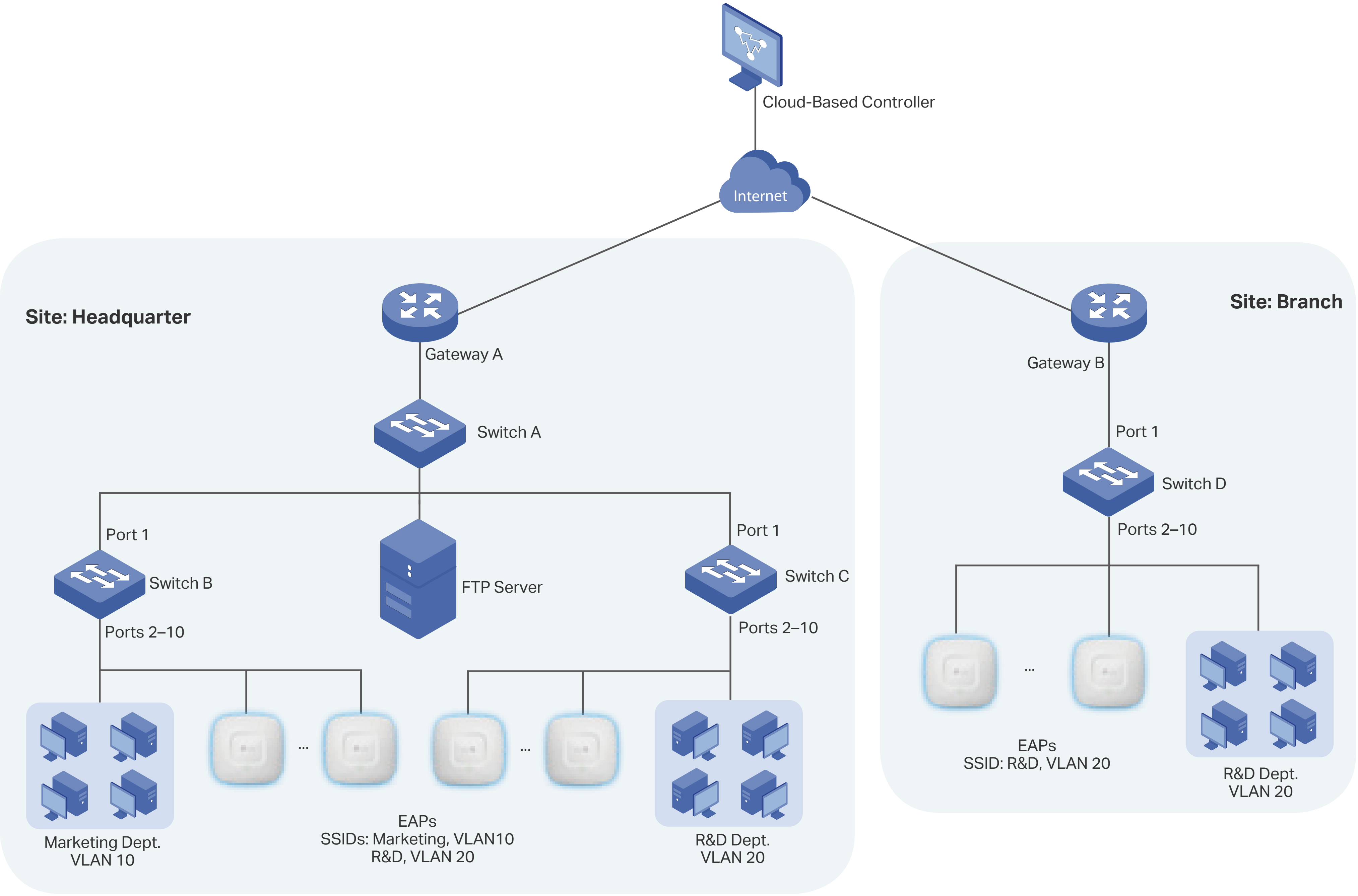
2.2 Configuration Scheme

Omada SDN solution can meet all the above requirements. With Omada gateways, switches, and EAPs, you can set up both the wired and wireless networks. All the devices can be managed via Omada SDN Controller, making it possible to monitor and control from a single interface. Build the network according to the topology and configuration guidelines below.

- To free the on-site configurations, you can choose Omada Cloud-Based Controller to remotely deploy and configure networks for the customer. All configurations can be provisioned and sent to the devices via Omada Cloud.
- For ease of management, create two sites for the network—one for the headquarter and the other for the branch. Omada SDN Controller manages networks based on sites. The site is the largest unit for managing networks.
- To divide different departments to different networks, create two LAN networks (VLANs)—one for the Marketing department and the other for the R&D department. Accordingly, create two wireless networks for the two departments. The wired and wireless networks for a department should be in the same VLAN.

  Tip: Switch ports without special settings will be added to all VLANs automatically. For the switch ports which are connected to devices with granted access to the both departments, like the FTP server and the gateways, just keep the default settings.
- To ensure employees in the branch can access the resources (like the FTP server) in the headquarter, build a VPN tunnel between the two sites.

Figure 2-2 Network Topology



2.3 Configuration Procedure

Preparations

Before Shipment:

- Note down the serial numbers of all devices. The serial numbers are required when adding devices to the cloud-based controller.
- Configure the gateways. Omada Cloud-Based Controller delivers configuration files to all devices via Omada Cloud. To successfully receive the configurations, the gateway at each site should be pre-configured and can access the internet once powered on.

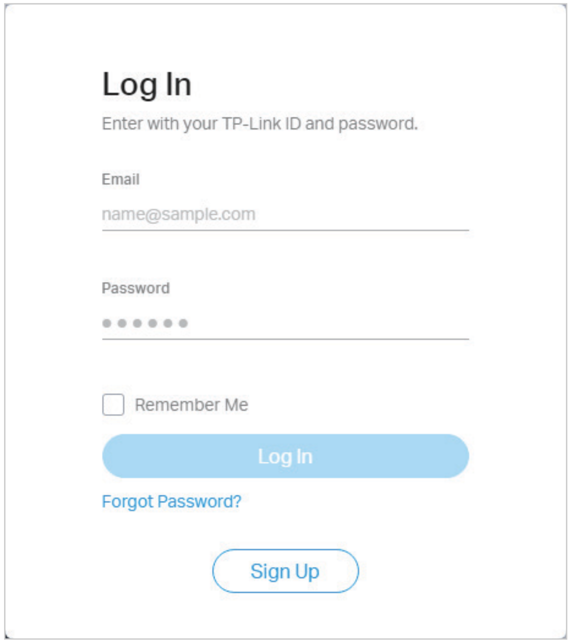
After the Customer Had Received All Devices:

- Make sure all devices are connected according to the network topology and powered on.

1) Subscribe to an Omada Cloud-Based Controller.

a. Go to https://omada.tplinkcloud.com and log into the Omada Cloud with your TP-Link ID. If you don't have a TP-Link ID, register one.

Figure 2-3 Logging Into Omada Cloud



Log In

Enter with your TP-Link ID and password.

Email

name@sample.com

Password

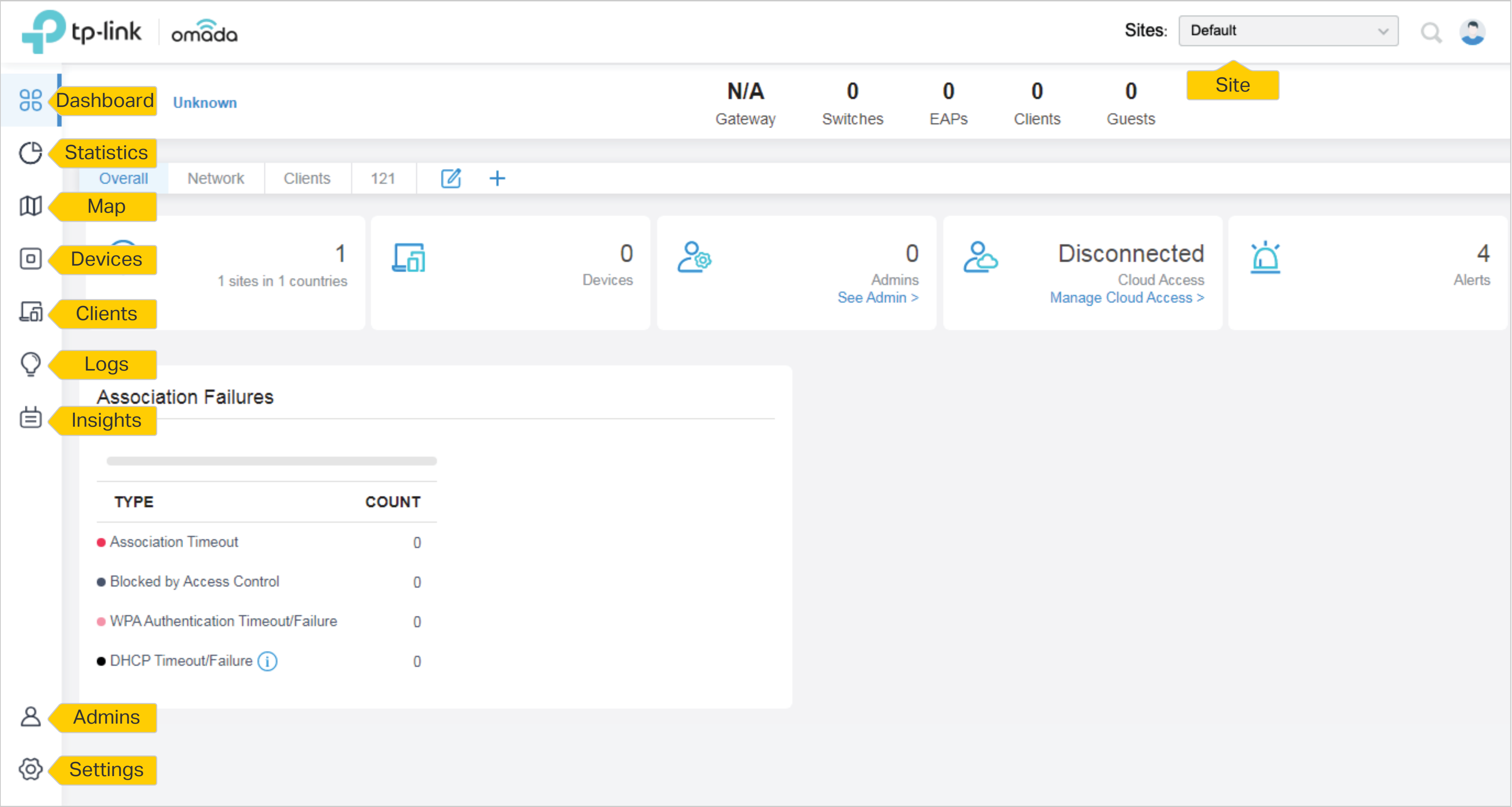
●●●●●●

□ Remember Me

b. Click [+ Add Controller] at the bottom of the page and follow the instructions to subscribe a cloud-based controller for the customer.

c. The cloud-based controller will be shown in the controller list after the payment. Click ⌂ to enter the management page of the controller.

Figure 2-4 Management Page of the Controller



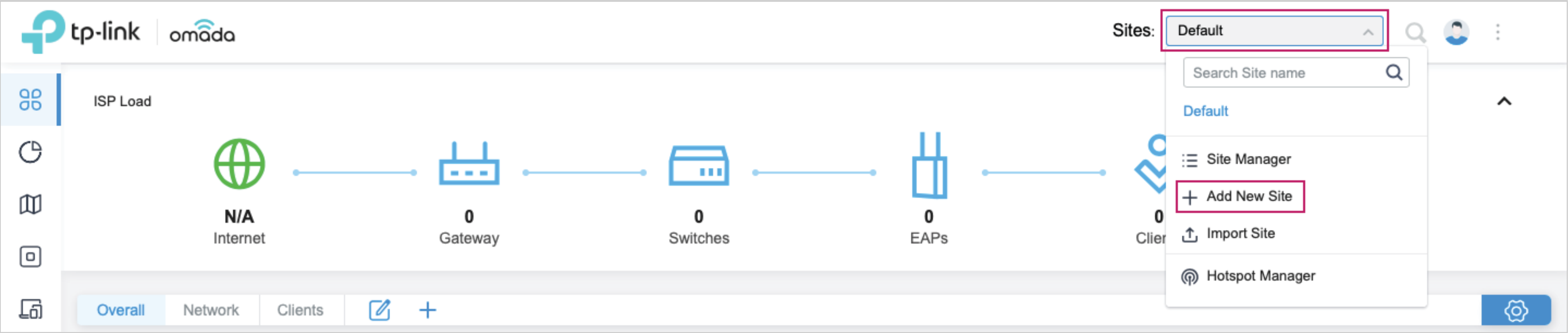
Association Failures

TYPE	COUNT
● Association Timeout	0
● Blocked by Access Control	0
● WPA Authentication Timeout/Failure	0
● DHCP Timeout/Failure ⓘ	0

2) Create two sites for the customer.

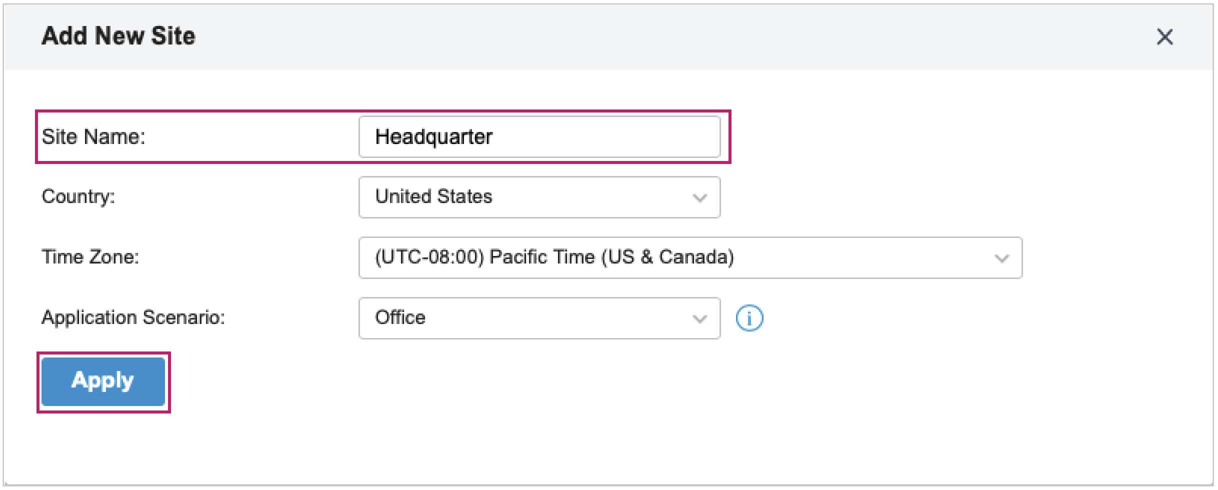
a. Click the current site name at the right top of the page, and then click **+ Add New Site**.

Figure 2-5 Site Management Panel



b. The Add New Site page will pop up. Create a site named Headquarter and configure the parameters according to your situation.

Figure 2-6 Adding Site for the Headquarter



Add New Site

Site Name: Headquarter

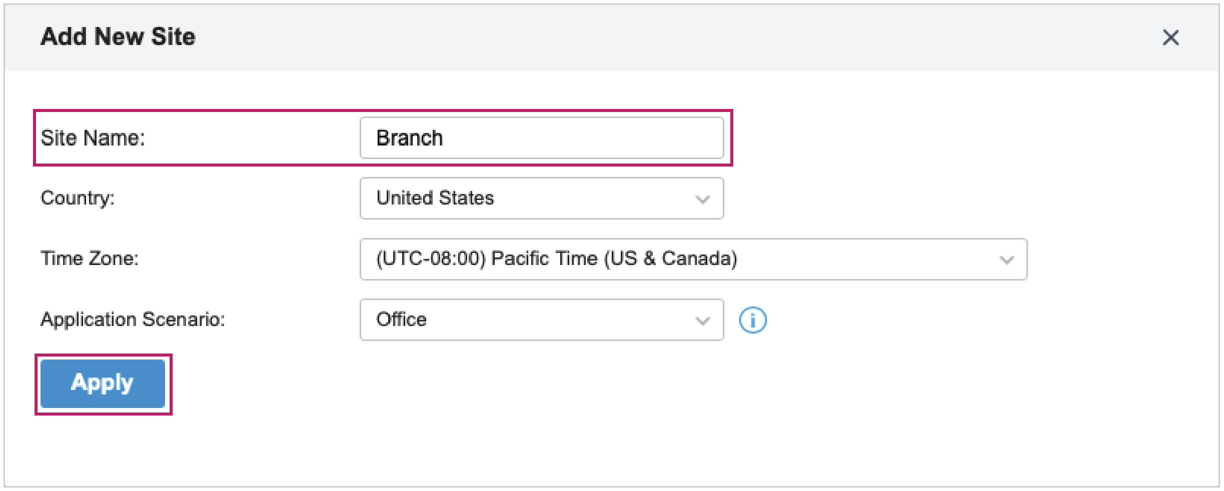
Country: United States

Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Application Scenario: Office

c. Repeat Step a and b to create another site named Branch.

Figure 2-7 Adding Site for the Branch



Add New Site

Site Name: Branch

Country: United States

Time Zone: (UTC-08:00) Pacific Time (US & Canada)

Application Scenario: Office

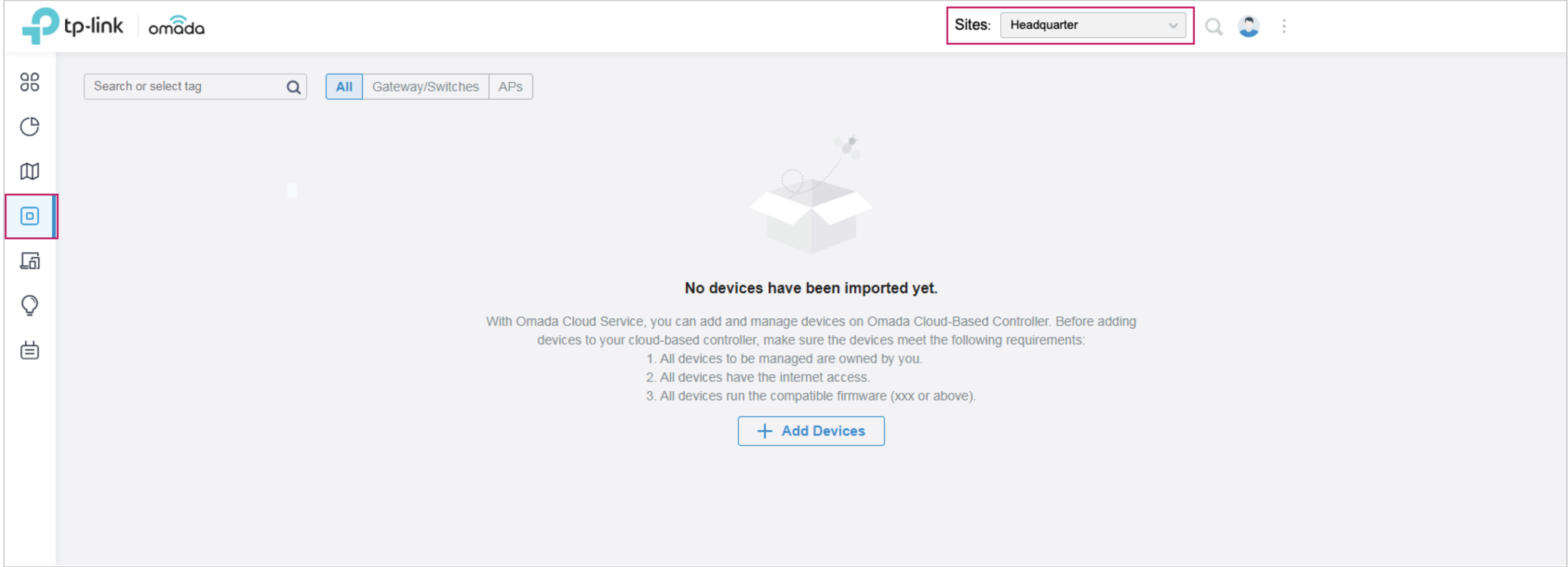
After the sites are created, you can adopt devices and configure the networks for each site separately. The following steps take configurations for site Headquarter as an example. Configurations for site Branch are illustrated via tips in steps 4–6.

3) Adopt devices for the site.

Tip: Similarly, you can adopt devices for the site Branch.

a. Select the current site as Headquarter and click ⊡ in the sidebar to enter the **Devices** page.

Figure 2-8 Entering the Devices Page



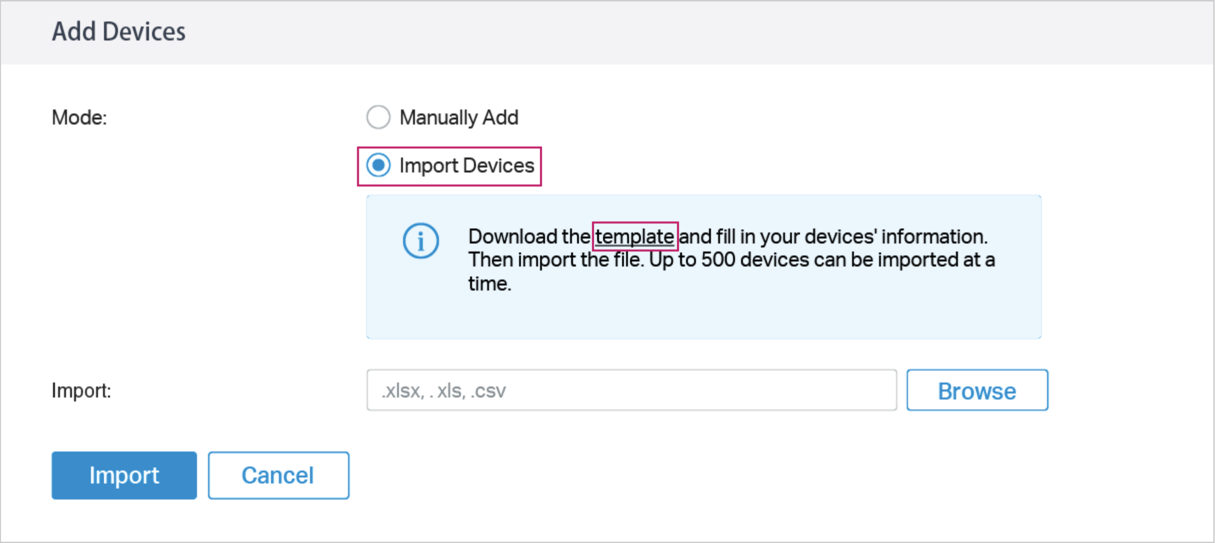
No devices have been imported yet.

With Omada Cloud Service, you can add and manage devices on Omada Cloud-Based Controller. Before adding devices to your cloud-based controller, make sure the devices meet the following requirements:

1. All devices to be managed are owned by you.
2. All devices have the internet access.
3. All devices run the compatible firmware (xxx or above).

b. Click + Add Devices and the following window will pop up. To add devices in batch, specify the mode as Import Devices and download the template to fill in the serial numbers of the devices for the headquarter.

Figure 2-9 Downloading the Template



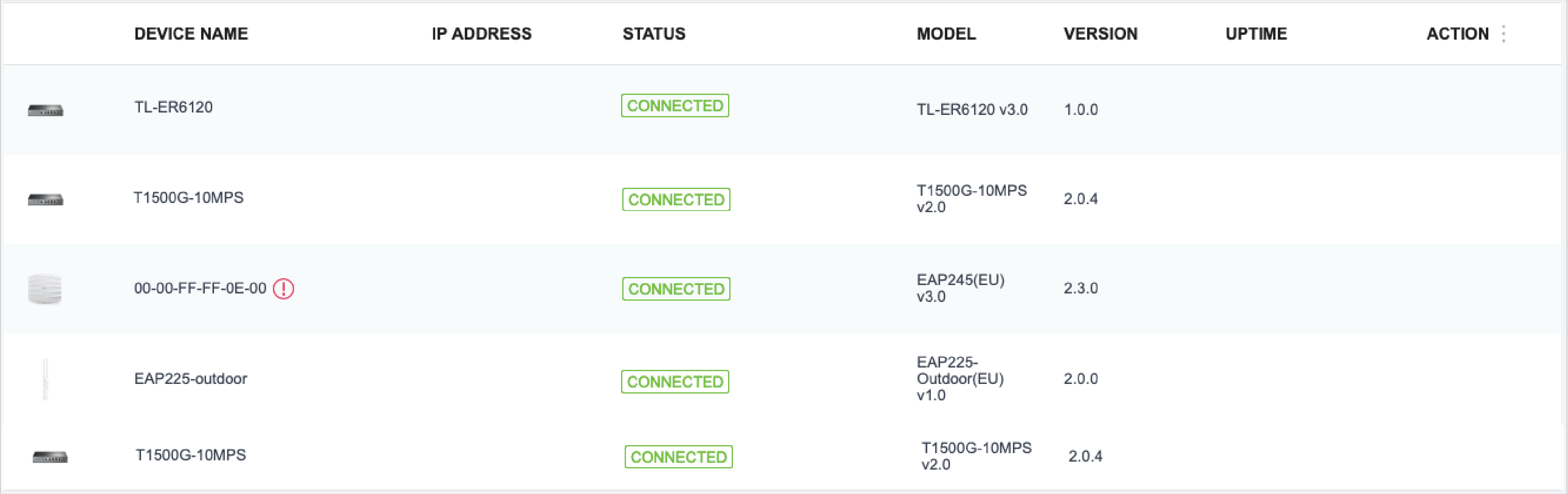
Mode: ○ Manually Add ● Import Devices

Download the template and fill in your devices' information. Then import the file. Up to 500 devices can be imported at a time.

Import: .xlsx, .xls, .csv

c. Import the file and the devices (with the factory default settings) will be automatically adopted by the controller. You can view the devices on the **Devices** page.

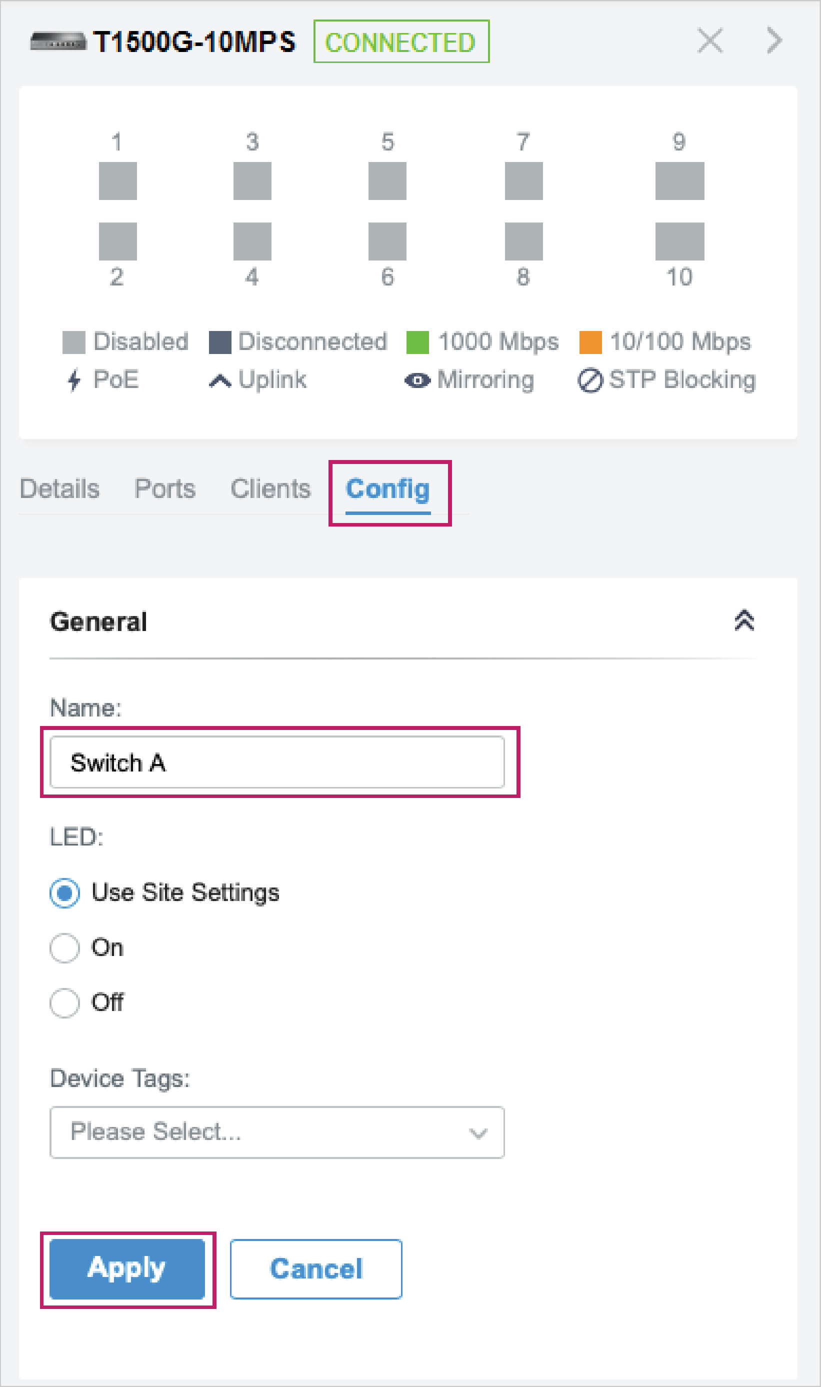
Figure 2-10 Device List



	DEVICE NAME	IP ADDRESS	STATUS	MODEL	VERSION	UPTIME	ACTION
	TL-ER6120		CONNECTED	TL-ER6120 v3.0	1.0.0		
	T1500G-10MPS		CONNECTED	T1500G-10MPS v2.0	2.0.4		
	00-00-FF-FF-0E-00 ⓘ		CONNECTED	EAP245(EU) v3.0	2.3.0		
	EAP225-outdoor		CONNECTED	EAP225-Outdoor(EU) v1.0	2.0.0		
	T1500G-10MPS		CONNECTED	T1500G-10MPS v2.0	2.0.4		

d. Click a device in the list, and the device's Properties window will be shown on the right side. You can give a recognizable name for the device on its **Config** page.

Figure 2-11 Changing Devices' Name



General

Name: Switch A

LED:

● Use Site Settings

○ On

○ Off

Device Tags: Please Select...

Apply Cancel

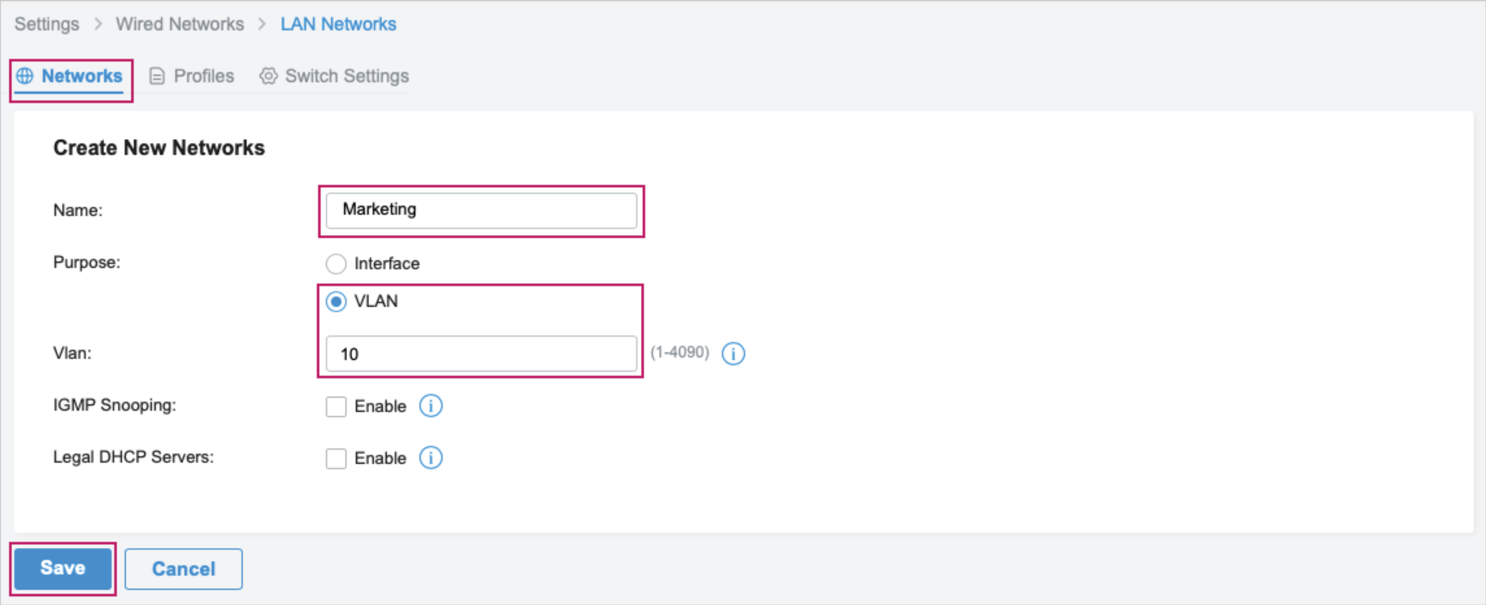
4) Configure the LAN networks.

Tip: For site Branch, follow the steps to create a LAN network and port profile for the R&D department. The configurations for the LAN network and port profile are the same with those in site Headquarter, and are applied to ports 2–10 on Switch D.

a. Go to **Settings > Wired Networks > LAN Networks.**

b. On the **Networks** tab, click + Create New LAN to create a LAN network for the Marketing department. Configure the Purpose as VLAN and the VLAN ID as 10.

Figure 2-12 Creating Network for Marketing Department



Settings > Wired Networks > LAN Networks

Networks | Profiles | Switch Settings

Create New Networks

Name: Marketing

Purpose: ○ Interface ● VLAN

Vlan: 10 (1-4090)

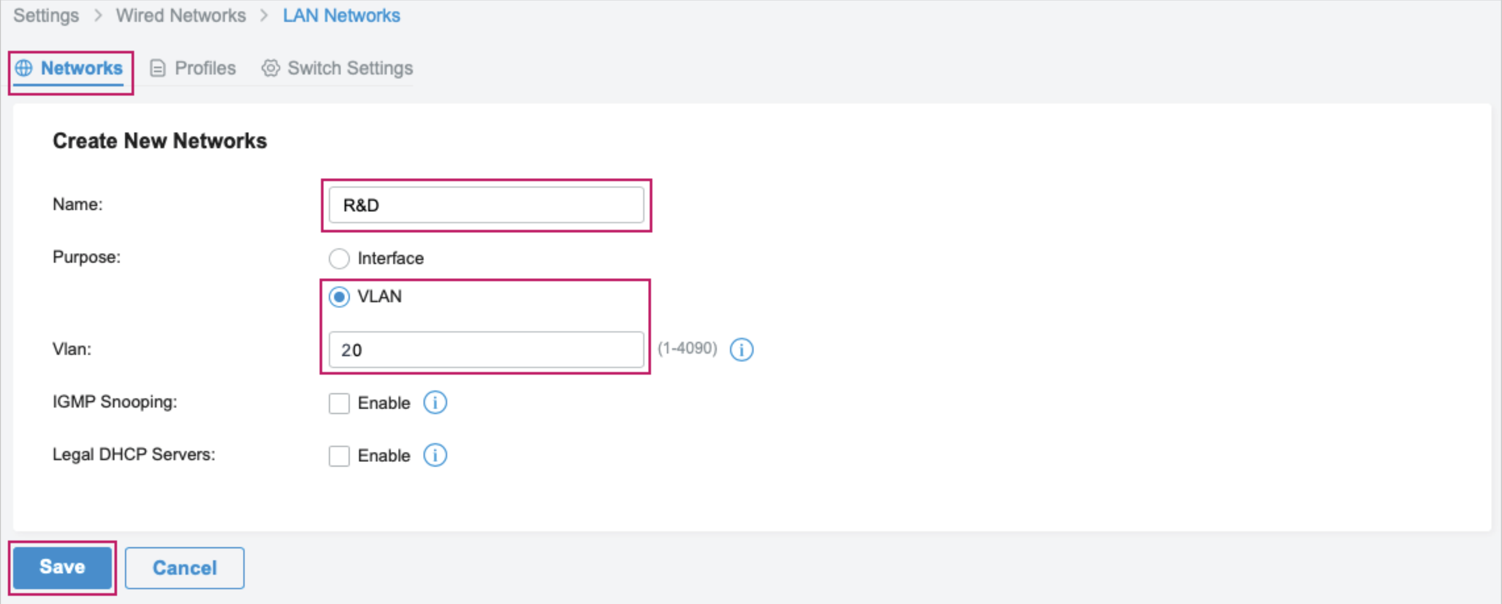
IGMP Snooping: □ Enable

Legal DHCP Servers: □ Enable

Save | Cancel

c. Similarly, create a LAN network with the VLAN ID 20 for the R&D department.

Figure 2-13 Creating Network for R&D Department



Settings > Wired Networks > LAN Networks

Networks | Profiles | Switch Settings

Create New Networks

Name: R&D

Purpose: ○ Interface ● VLAN

Vlan: 20 (1-4090)

IGMP Snooping: □ Enable

Legal DHCP Servers: □ Enable

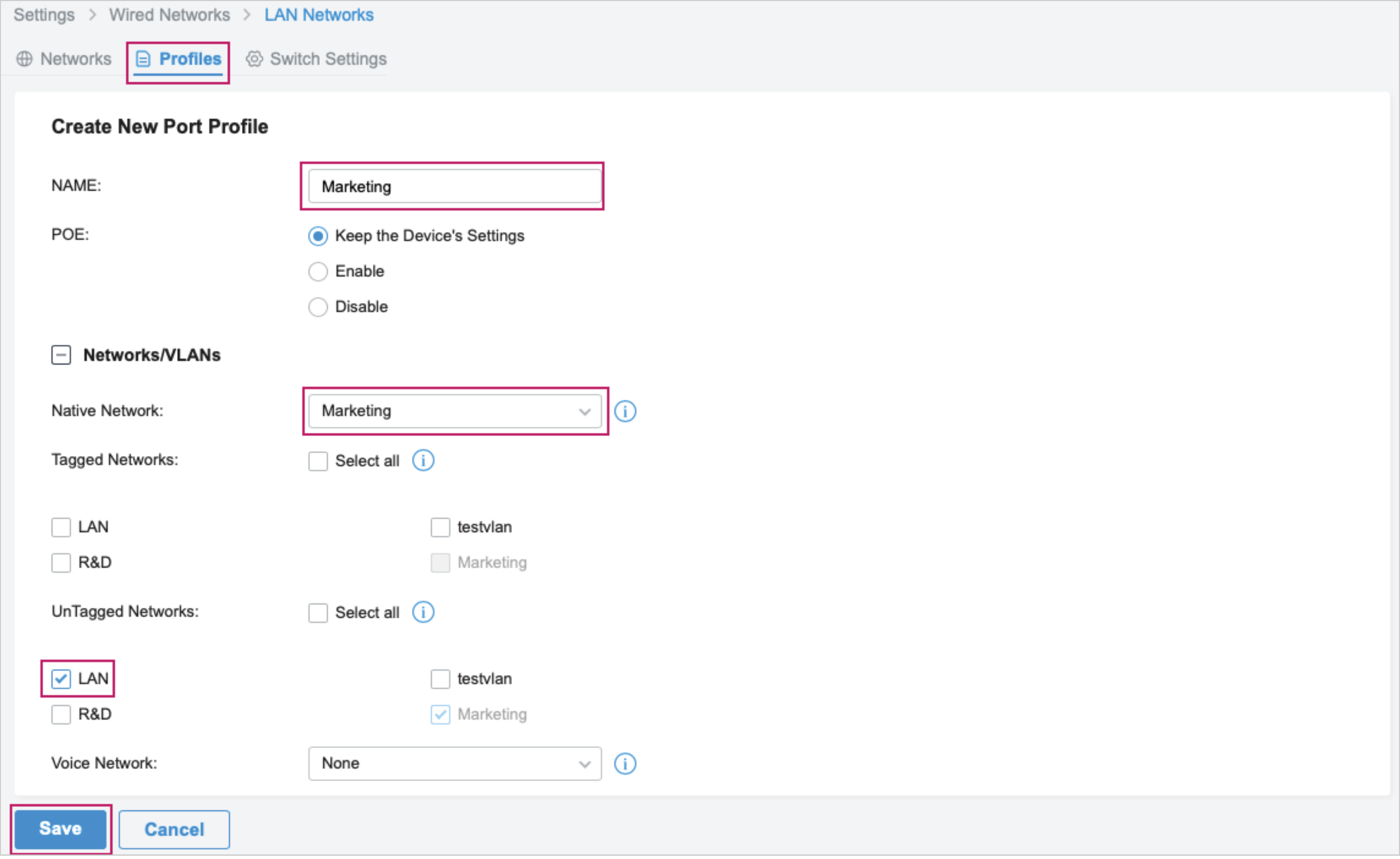
Save | Cancel

d. On the **Profiles** tab, click + Create New Port Profile to create port profiles for the both networks with the following settings:

Table 2-1 Port Profiles for the Networks

Name	Native Network	Tagged networks	Untagged Networks
Marketing	Marketing	/	LAN, Marketing
R&D	R&D	/	LAN, R&D

Figure 2-2 Creating Port Profiles for the Marketing Network



Settings > Wired Networks > LAN Networks

Networks | **Profiles** | Switch Settings

Create New Port Profile

NAME: Marketing

POE: ● Keep the Device's Settings ○ Enable ○ Disable

Networks/VLANs

Native Network: Marketing

Tagged Networks: ☐ Select all

☐ LAN ☐ testvlan
☐ R&D ☐ Marketing

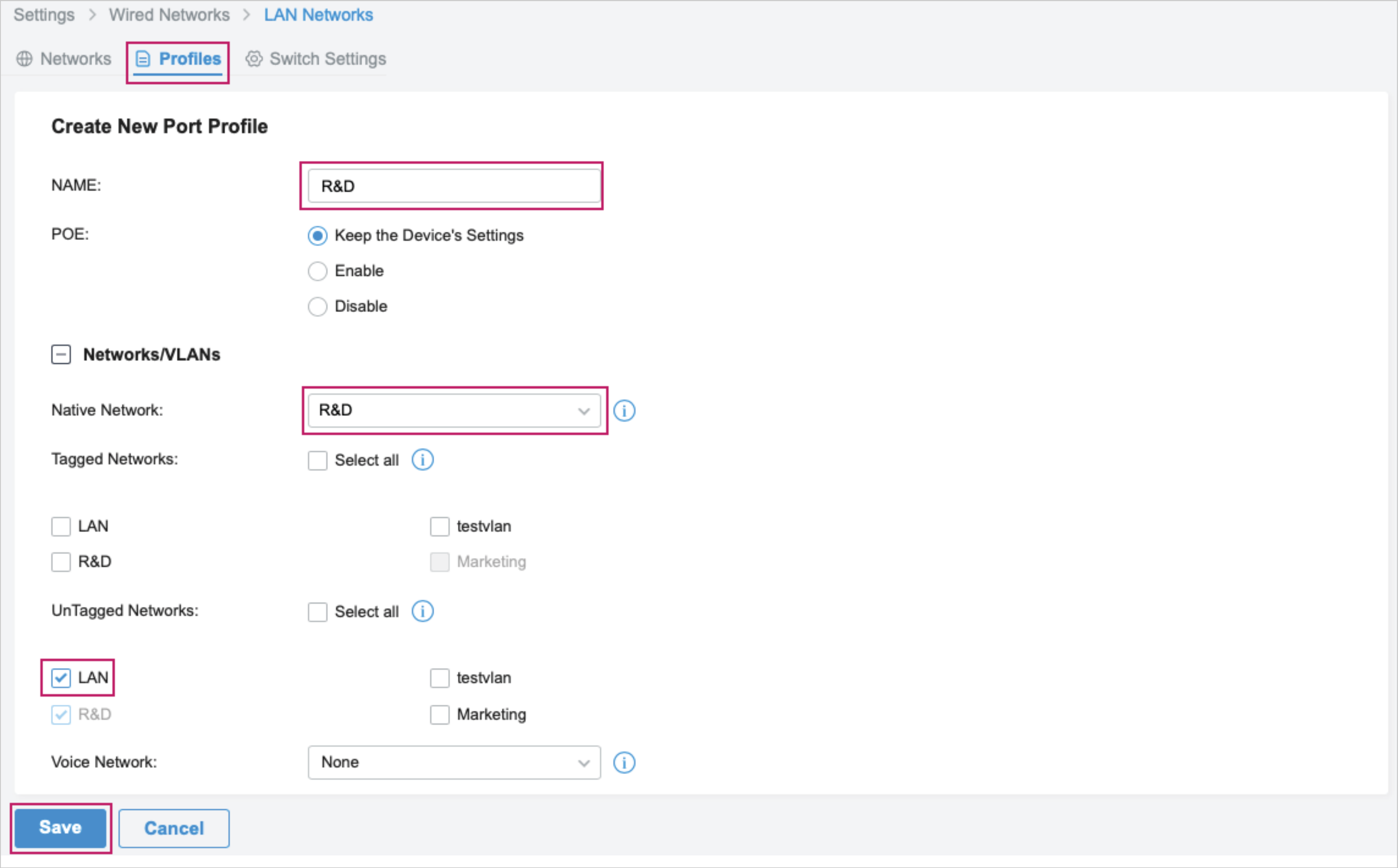
UnTagged Networks: ☐ Select all

☑ LAN ☐ testvlan
☐ R&D ☑ Marketing

Voice Network: None

Save Cancel

Figure 2-3 Creating Port Profiles for the R&D Network



Settings > Wired Networks > LAN Networks

Networks | **Profiles** | Switch Settings

Create New Port Profile

NAME: R&D

POE: ● Keep the Device's Settings ○ Enable ○ Disable

Networks/VLANs

Native Network: R&D

Tagged Networks: ☐ Select all

☐ LAN ☐ testvlan
☐ R&D ☐ Marketing

UnTagged Networks: ☐ Select all

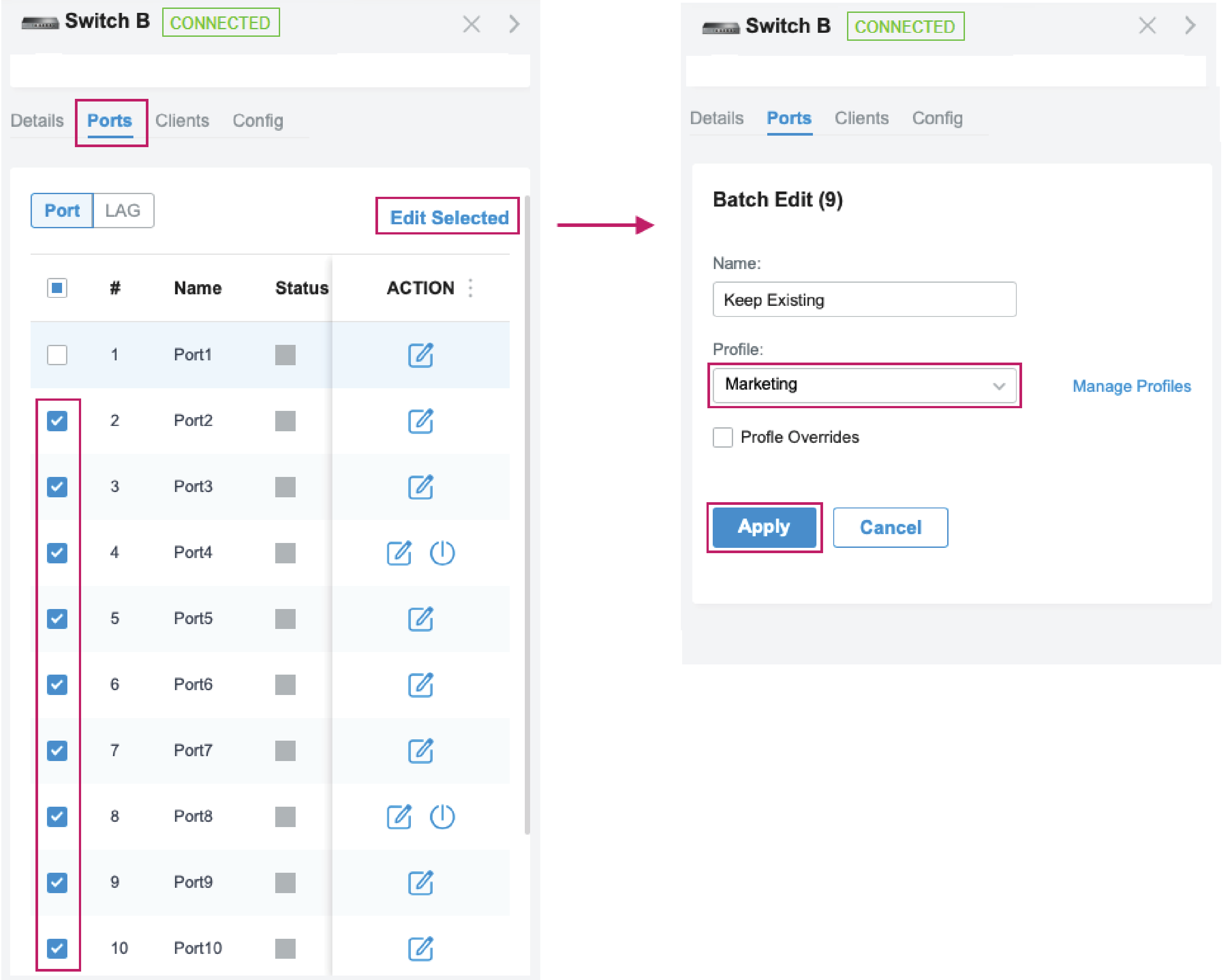
☑ LAN ☐ testvlan
☑ R&D ☐ Marketing

Voice Network: None

Save Cancel

e. On the **Switch Settings** tab, click ✎ beside Switch B to reveal its Properties window. On the **Ports** tab, select ports 2–10 and click **Edit Selected**. You will enter the batch editing mode. Select the profile as Marketing and click **Apply**.

Figure 2-4 Applying Port Profiles to the Ports on Switch B



Switch B CONNECTED

Details | **Ports** | Clients | Config

Port | LAG — Edit Selected

■	#	Name	Status	ACTION
□	1	Port1	■	✎
☑	2	Port2	■	✎
☑	3	Port3	■	✎
☑	4	Port4	■	✎ ⏻
☑	5	Port5	■	✎
☑	6	Port6	■	✎
☑	7	Port7	■	✎
☑	8	Port8	■	✎ ⏻
☑	9	Port9	■	✎
☑	10	Port10	■	✎

Switch B CONNECTED

Details | **Ports** | Clients | Config

Batch Edit (9)

Name: Keep Existing

Profile: Marketing — Manage Profiles

□ Profle Overrides

Apply | Cancel

f. Similarly, apply the profile R&D to ports 2–10 on Switch C.

5) Configure the wireless networks.

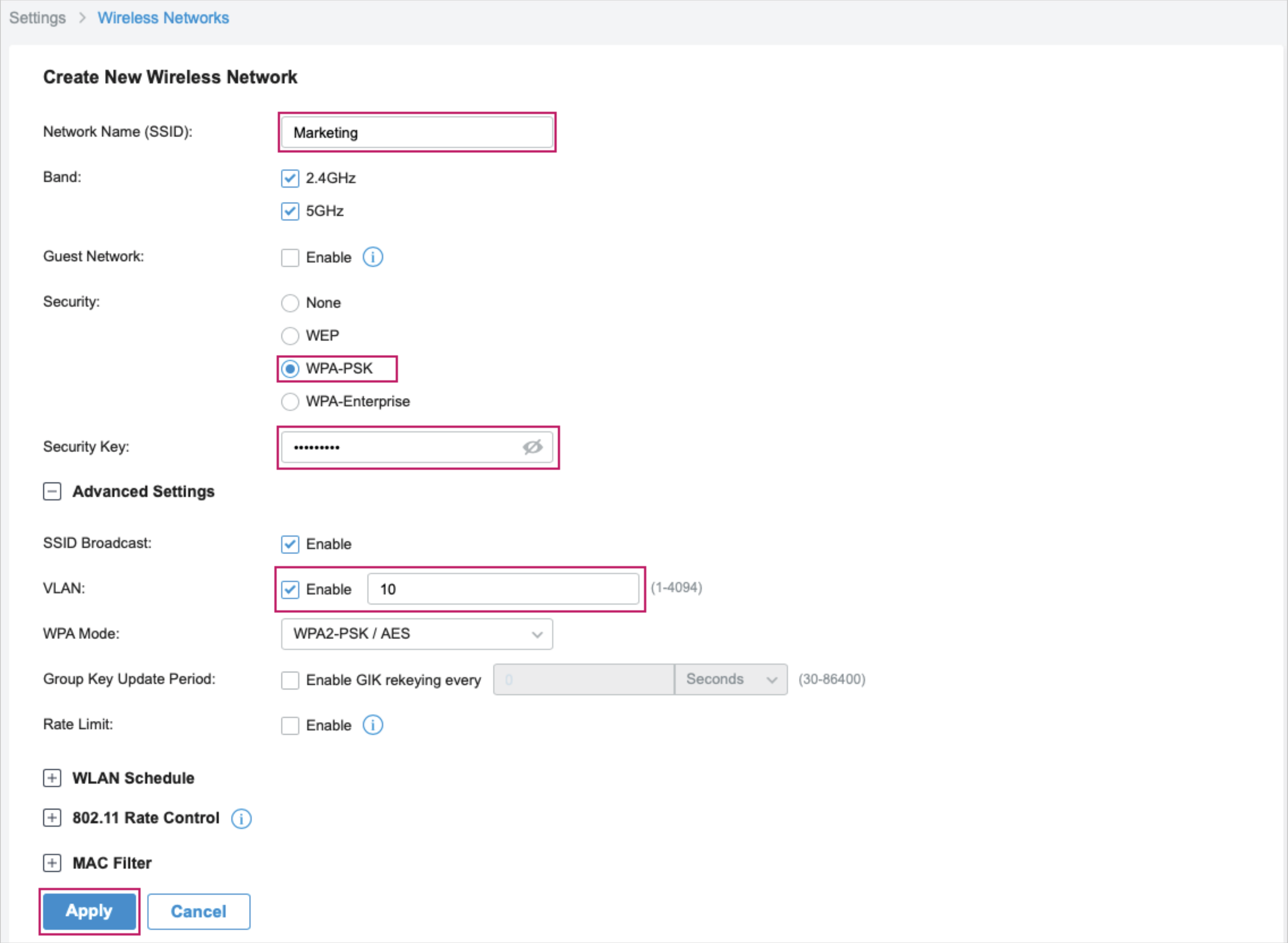
The wireless networks will take effect on all EAPs at the site.

Tip: For site Branch, only create a wireless network with the VLAN ID 20 for the R&D department.

a. Go to **Settings > Wireless Networks**.

b. Click + Create New Wireless Networks to create a wireless network for the Marketing department. Configure the network name as Marketing, the security mode as WPA-PSK, and configure a security key for the wireless network. In the **Advanced Settings** section, enable VLAN and configure the VLAN ID as 10.

Figure 2-5 Creating Wireless Network for Marketing Department



Settings > Wireless Networks

Create New Wireless Network

Network Name (SSID): Marketing

Band: ☑ 2.4GHz ☑ 5GHz

Guest Network: □ Enable

Security: ○ None ○ WEP ● WPA-PSK ○ WPA-Enterprise

Security Key: ••••••••••

⊟ **Advanced Settings**

SSID Broadcast: ☑ Enable

VLAN: ☑ Enable 10 (1-4094)

WPA Mode: WPA2-PSK / AES

Group Key Update Period: □ Enable GIK rekeying every 0 Seconds (30-86400)

Rate Limit: □ Enable

⊞ **WLAN Schedule**

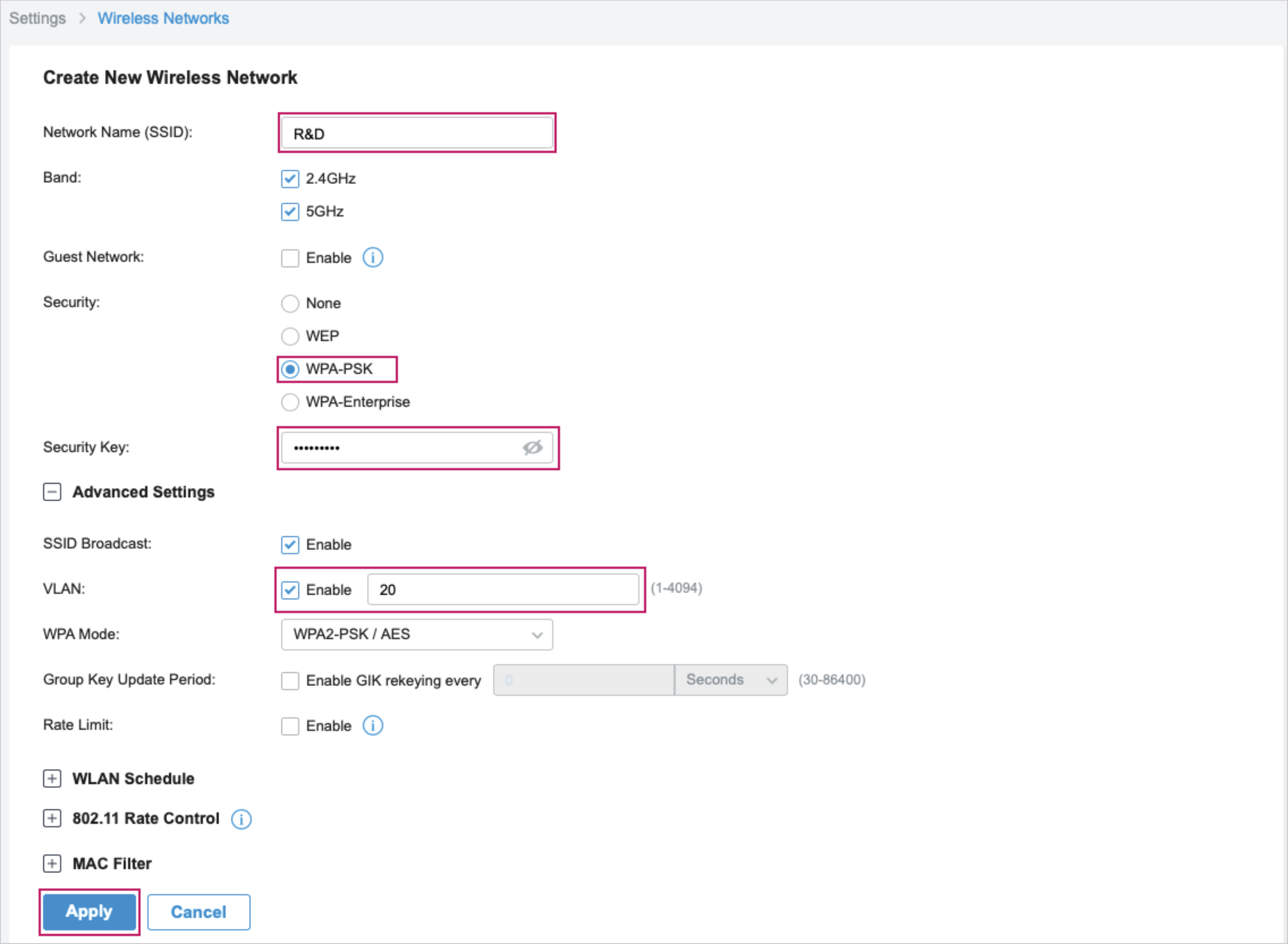
⊞ **802.11 Rate Control**

⊞ **MAC Filter**

Apply Cancel

c. Similarly, create a wireless network for the R&D department. Configure the network name as R&D and the VLAN ID as 20.

Figure 2-6 Creating Wireless Network for R&D Department



Settings > Wireless Networks

Create New Wireless Network

Network Name (SSID): R&D

Band: ☑ 2.4GHz ☑ 5GHz

Guest Network: □ Enable

Security: ○ None ○ WEP ● WPA-PSK ○ WPA-Enterprise

Security Key: •••••••••

Advanced Settings

SSID Broadcast: ☑ Enable

VLAN: ☑ Enable 20 (1-4094)

WPA Mode: WPA2-PSK / AES

Group Key Update Period: □ Enable GIK rekeying every 0 Seconds (30-86400)

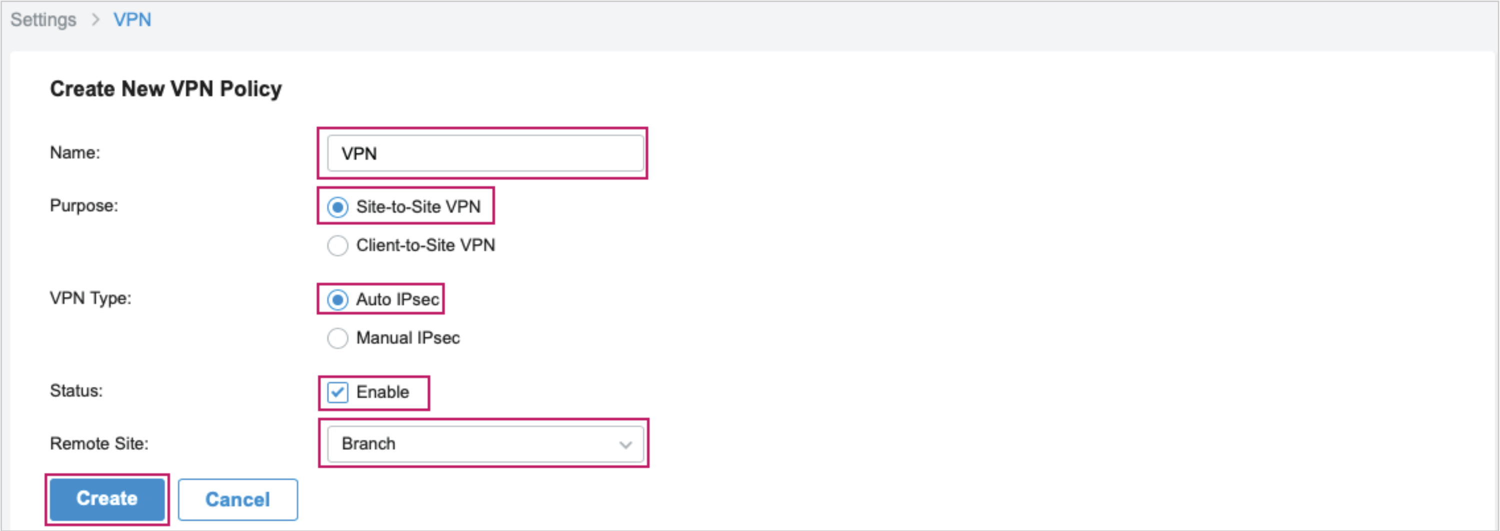
Rate Limit: □ Enable

6) Build a VPN tunnel for the two sites.

a. Go to **Settings > VPN** and click

b. Configure the purpose as Site-to-Site VPN, the VPN type as Auto IPsec, the status as Enable, and specify the remote site as Branch. Then click Create. A VPN tunnel will be automatically set up between the current site (Headquarter) and the specified remote site (Branch).

Figure 2-7 Creating VPN Policy



Settings > VPN

Create New VPN Policy

Name: VPN

Purpose: ● Site-to-Site VPN ○ Client-to-Site VPN

VPN Type: ● Auto IPsec ○ Manual IPsec

Status: ☑ Enable

Remote Site: Branch

Till now, you have finished the configurations. All devices will automatically obtain the configuration files from Omada Cloud and build up an Omada network.

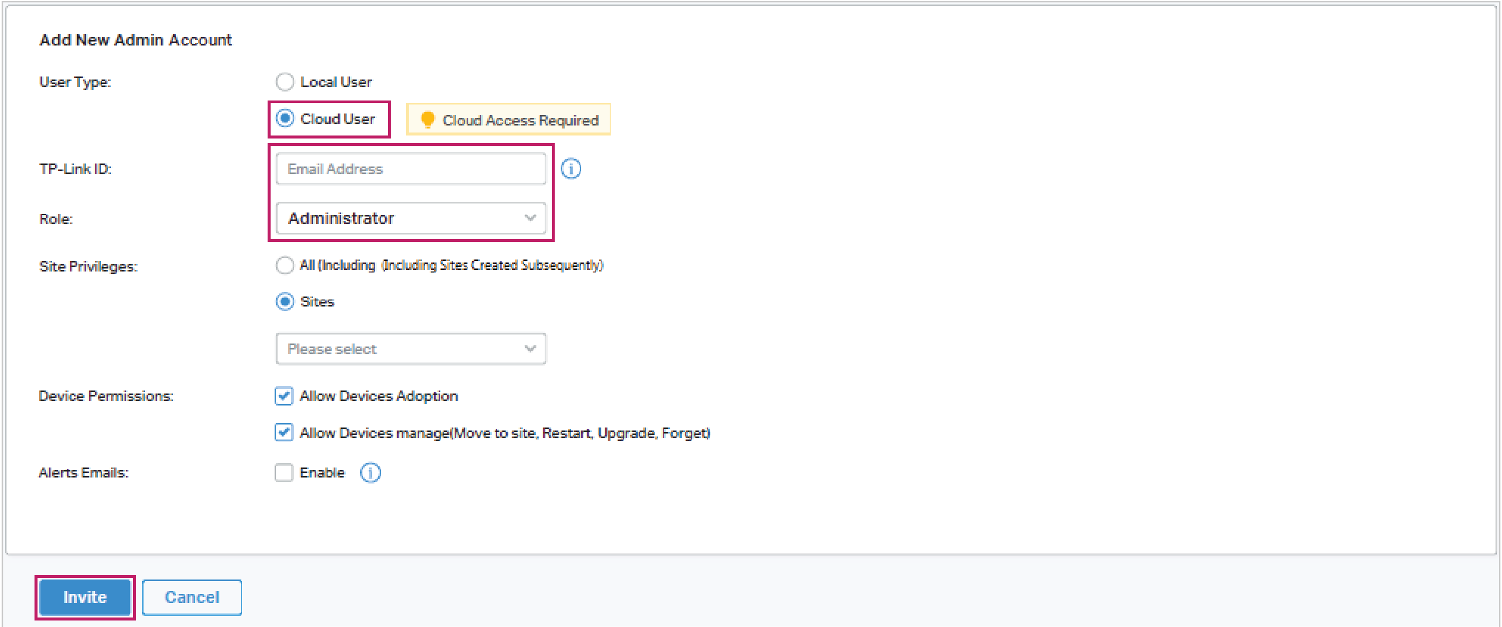
2.4 Authorizing the Customer to Manage the Network

To allow the customer to monitor and manage the network, follow the steps below to create an Admin account. Then provide the Admin account and the IP address of the cloud-based controller to the customer.

1) Click 👤 in the sidebar to go to the **Admins** page.

2) Click + Add New Admin Account to create an account.

Figure 2-8 Creating Admin Account for the Customer



Add New Admin Account

User Type: ○ Local User

● Cloud User Cloud Access Required

TP-Link ID: Email Address

Role: Administrator

Site Privileges: ○ All (Including (Including Sites Created Subsequently)

● Sites

Please select

Device Permissions: ☑ Allow Devices Adoption

☑ Allow Devices manage(Move to site, Restart, Upgrade, Forget)

Alerts Emails: □ Enable

a. Select the user type as Cloud User and enter the customer’s email address. The controller will send an invitation email to the email address. If the email address is already registered with a TP-Link ID, it will become a valid cloud user account after accepting the invitation. If not, it will be invited for registration, and automatically becomes a valid cloud user account after finishing the registration.

b. Configure the role as Administrator and assign site privileges for the account. If the cloud-based controller is used only by the customer, select **All (Including Sites Created Subsequently)**; if it is shared by other customers, select **Sites** and assign only sites Headquarter and Branch to the account.

c. Specify the device permissions and click **Invite**.

The customer will be able to access the controller’s management page after accepting the invitation. Omada SDN Controller provides an easy-to-use dashboard, allowing the customer to easily monitor real-time network status, check the network usage and traffic distribution, or even track the key data of customers for better business results.

In addition, the controller supports muti-account login. The customer can create other Admin accounts with different roles (Administrator or Viewer) according to actual needs.

3 Configuring Advanced Features

Omada SDN network provides rich features to ensure high performance and excellent user experience. This chapter lists the most common used features. Tune the network with the features according to your customer's actual needs.

3.1 Optimizing Bandwidth Usage with Bandwidth Control

What is Bandwidth Control?

Bandwidth Control allows you to distribute the network bandwidth based on users, networks or IP groups. By configuring bandwidth control rules, you can restrict how much of the bandwidth a user or users in specific networks or IP groups can use.

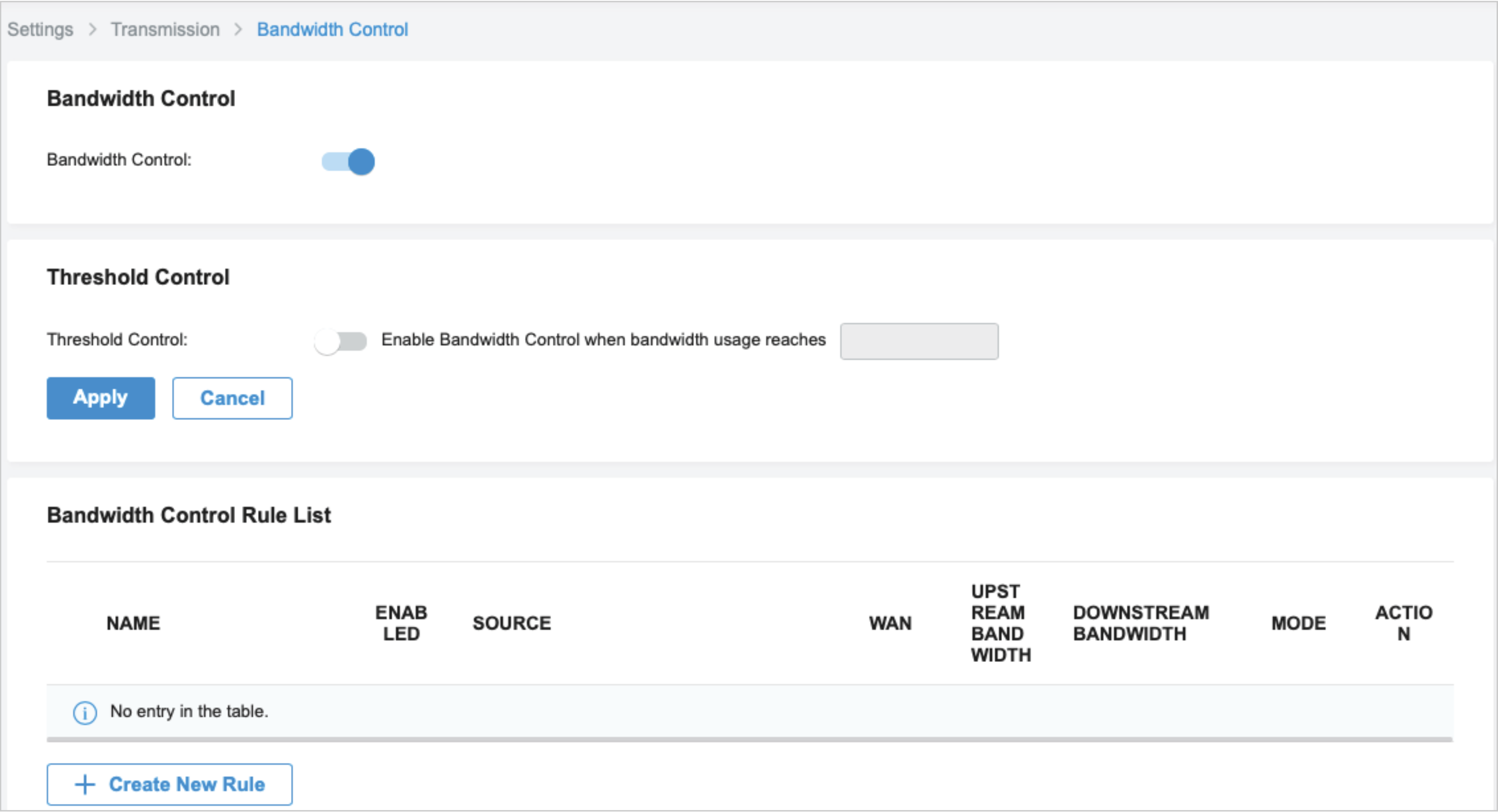
Bandwidth Control is important to avoid network traffic "bottlenecks". Normally the bandwidth from the ISP is shared by all terminals under the gateway. When any of the terminals use high-bandwidth applications like torrent programs, the others may experience a slowdown of normal network activities like transferring files between computers or just browsing the web.

With Bandwidth Control, you can minimize the impact caused by the network congestion. By setting limits for each user, network or IP group, the network bandwidth can be reasonably distributed and utilized.

How to Configure it?

Go to **Settings > Transmission > Bandwidth Control** to load the following page.

Figure 3-1 Configuring Bandwidth Control



Bandwidth Control

Bandwidth Control: ●

Threshold Control

Threshold Control: ○ Enable Bandwidth Control when bandwidth usage reaches

Bandwidth Control Rule List

NAME	ENABLED	SOURCE	WAN	UPSTREAM BANDWIDTH	DOWNSTREAM BANDWIDTH	MODE	ACTION

No entry in the table.

To configure Bandwidth Control, follow the steps below:

1) Enable Bandwidth Control. It is enabled by default.

2) Enable Threshold Control and configure the threshold. Bandwidth Control takes effect only when the total bandwidth usage reaches the threshold.

3) Click + Create New Rule to create bandwidth control rules.

3.2 Blocking Unauthorized Users with 802.1X Authentication

What is 802.1X Authentication?

802.1X provides port-based authentication service to restrict unauthorized clients from accessing to the network through publicly accessible switch ports. An 802.1X-enabled port allows only authentication messages and forbids normal traffic until the client passes the authentication.

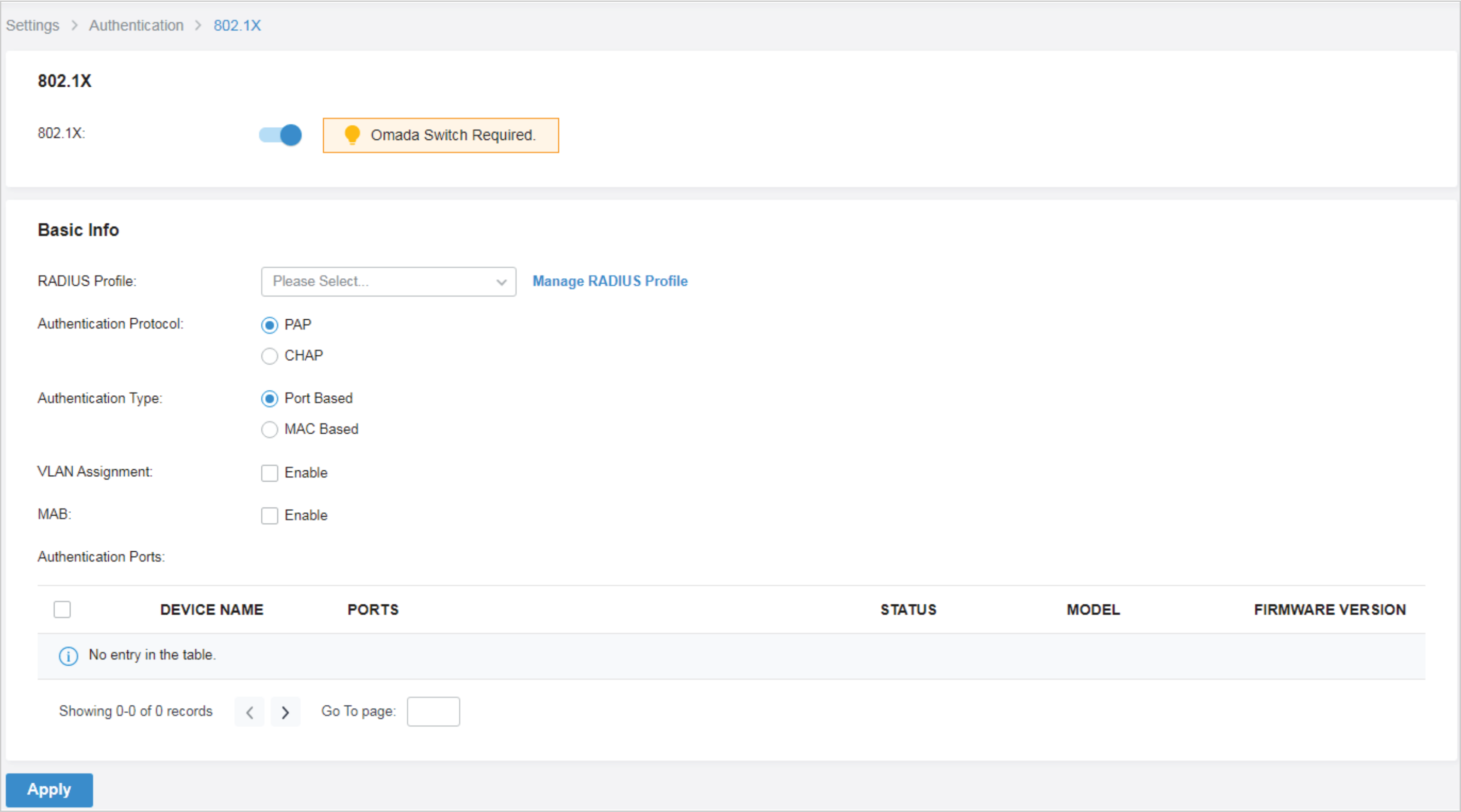
The switch also provides two features that are based on 802.1X authentication:

- VLAN Assignment: dynamically assigns the authenticated ports to VLANs. The username-to-VLAN mappings must already be stored in the RADIUS server database.
- MAB (MAC Authentication Bypass): allows clients to be authenticated without any client software installed. MAB is useful for authenticating devices without 802.1X capability like IP phones.

How to Configure it?

Go to **Settings > Authentication > 802.1X** to load the following page.

Figure 3-2 Configuring 802.1X Authentication



Settings > Authentication > 802.1X

802.1X

802.1X: ● Omada Switch Required.

Basic Info

RADIUS Profile: Please Select... Manage RADIUS Profile

Authentication Protocol: ● PAP ○ CHAP

Authentication Type: ● Port Based ○ MAC Based

VLAN Assignment: □ Enable

MAB: □ Enable

Authentication Ports:

□	DEVICE NAME	PORTS	STATUS	MODEL	FIRMWARE VERSION
ⓘ No entry in the table.					

Showing 0-0 of 0 records < > Go To page:

Apply

To configure 802.1X authentication, follow the steps below:

1) Enable 802.1X.

2) Select the RADIUS profile you have created and configure other parameters. The RADIUS profile includes the information of the RADIUS server which acts as the authentication server during 802.1X authentication.

3) Select the ports on which 802.1X Authentication will take effect.

3.3 Providing Temporary Access for Visitors with Portal Authentication

What is Portal Authentication?

Portal authentication provides authentication service to the clients that only need temporary access to the network, such as visitors in an office or customers in a restaurant. To access the network, these clients need to enter the authentication login page and use the correct login information to pass the authentication. You can advertise your business by customizing the authentication login page.

To allow unauthenticated clients to access the specific network resources, you can configure Pre-Authentication policies.

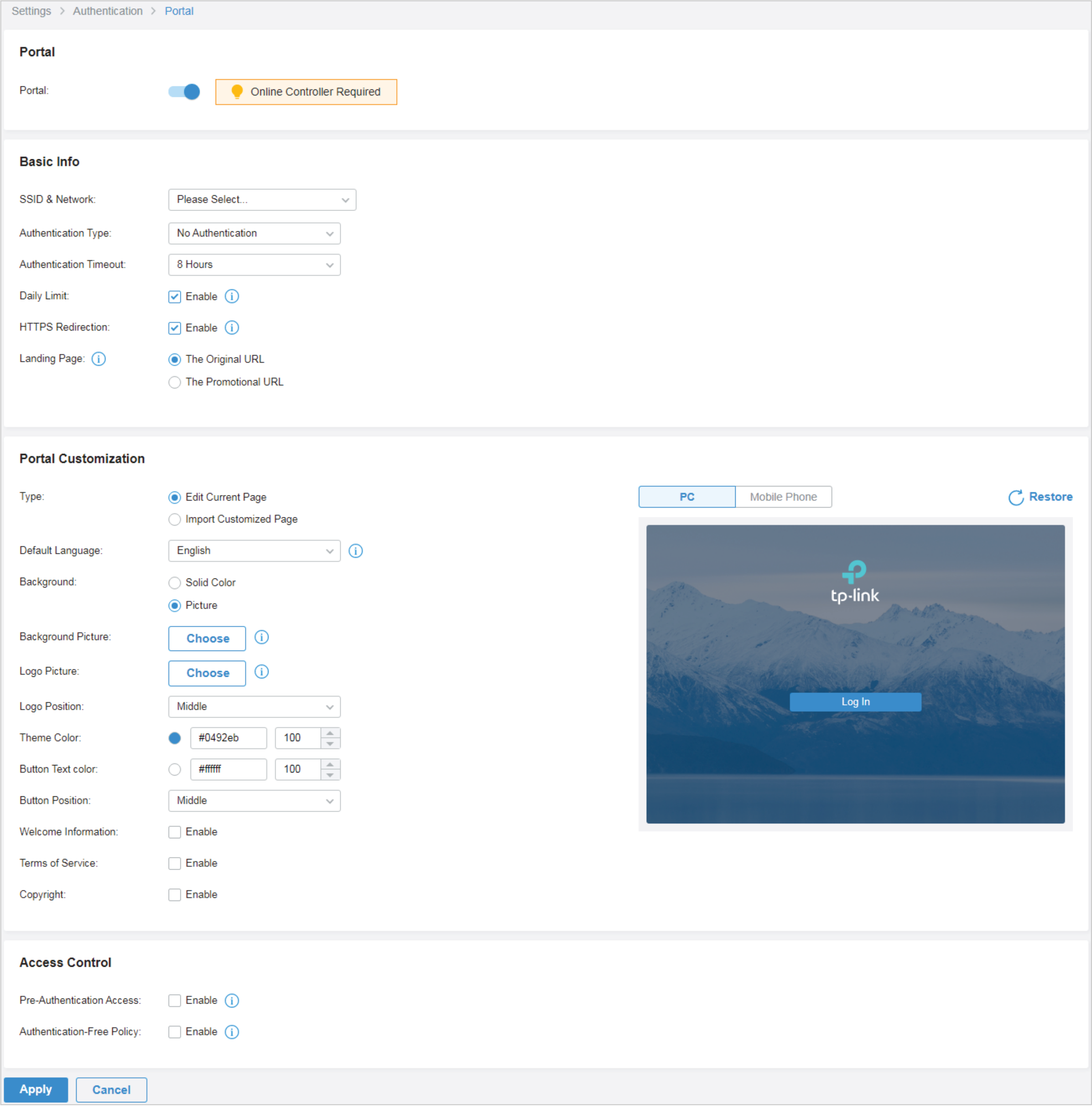
To allow the specific clients like the employees to access the network without authentication, you can configure Authentication-Free policies.

Portal authentication takes effect on SSIDs and LAN networks. EAPs authenticate wireless clients which connect to the SSID with Portal configured, and the gateway authenticates wired clients which connect to the network with Portal configured. To make Portal authentication available for wired and wireless clients, ensure that both the gateway and EAPs are connected and working properly.

How to Configure it?

Go to **Settings > Authentication > Portal** to load the following page.

Figure 3-3 Configuring Portal Authenticaiton



Settings > Authentication > Portal

Portal

Portal: ● Online Controller Required

Basic Info

SSID & Network: Please Select...

Authentication Type: No Authentication

Authentication Timeout: 8 Hours

Daily Limit: ☑ Enable

HTTPS Redirection: ☑ Enable

Landing Page: ● The Original URL ○ The Promotional URL

Portal Customization

Type: ● Edit Current Page ○ Import Customized Page

Default Language: English

Background: ○ Solid Color ● Picture

Background Picture: Choose

Logo Picture: Choose

Logo Position: Middle

Theme Color: ● #0492eb 100

Button Text color: ○ #ffffff 100

Button Position: Middle

Welcome Information: □ Enable

Terms of Service: □ Enable

Copyright: □ Enable

Access Control

Pre-Authentication Access: □ Enable

Authentication-Free Policy: □ Enable

Apply Cancel

To configure Portal authentication, follow the steps below:

1) Enable Portal.

2) Select the SSIDs and LAN networks for the portal to take effect on and configure other basic parameters.

3) Customize the Portal page including the background picture, logo picture and so on.

4) Configure access control rules including Pre-Authentication Access and Authentication-Free Policy if needed.

3.4 Building a Seamless Wi-Fi with Mesh and Fast Roaming

What are Mesh and Fast Roaming?

In a traditional home network, one access point (AP) connects to the internet and broadcasts Wi-Fi signals, which usually cannot cover every corner of the site. Sometimes you may use several APs to extend the Wi-Fi coverage. However, each AP forms a separated network with different Wi-Fi settings. When roaming from one AP to another, your internet experience will suffer from long loading times and lag. How to keep a constant internet connection? You have two choices: building a mesh network or enabling Fast Roaming.

- Mesh

In a mesh Wi-Fi network, multiple APs link together to form a single, unified network that shares the same Wi-Fi settings. These settings include network name, password, access control settings, and more. This unified Wi-Fi system provides your site with Wi-Fi coverage. To build the unified Wi-Fi system, all EAPs should support Omada Mesh.

- Fast Roaming

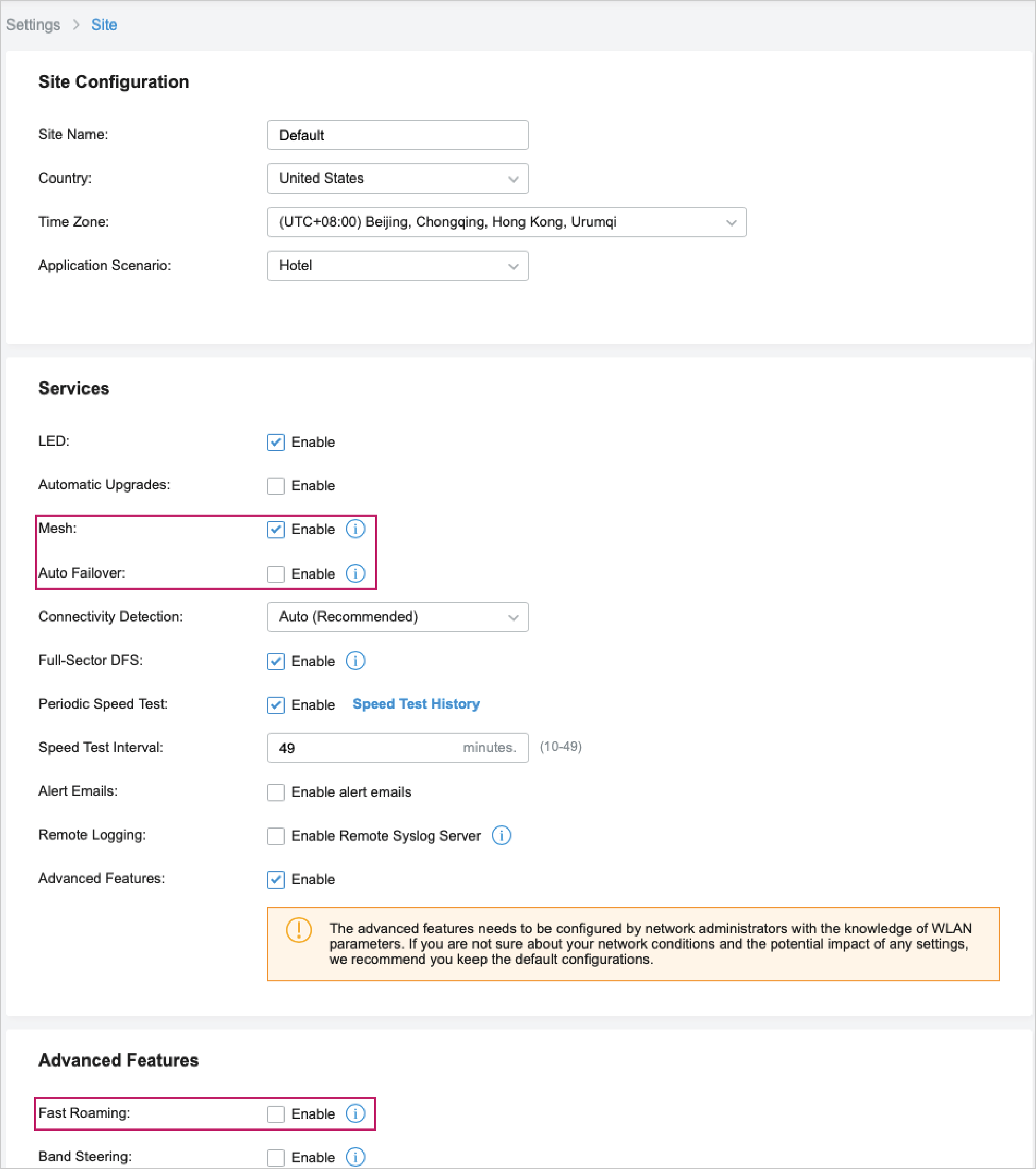
Fast Roaming improve the roaming experience by shortening the time it takes a wireless client to move from one AP to another. From the user’s perspective, the signal interruption when using a phone, tablet, or laptop will be unnoticeable because Fast Roaming makes the transition so quick.

How to make roaming faster? IEEE provides three solutions: IEEE 802.11k, 802.11v and 802.11r. TP-Link combines the advantages of 802.11k and 802.11v to develop its Fast Roam technology. To enjoy fast roaming, clients need to support IEEE 802.11k/v.

How to Configure Them?

Go to **Settings > Site** to load the following page.

Figure 3-4 Enabling Mesh and Fast Roaming



Settings > Site

Site Configuration

Site Name:	Default
Country:	United States
Time Zone:	(UTC+08:00) Beijing, Chongqing, Hong Kong, Urumqi
Application Scenario:	Hotel

Services

LED:	☑ Enable
Automatic Upgrades:	□ Enable
Mesh:	☑ Enable
Auto Failover:	□ Enable
Connectivity Detection:	Auto (Recommended)
Full-Sector DFS:	☑ Enable
Periodic Speed Test:	☑ Enable Speed Test History
Speed Test Interval:	49 minutes. (10-49)
Alert Emails:	□ Enable alert emails
Remote Logging:	□ Enable Remote Syslog Server
Advanced Features:	☑ Enable

The advanced features needs to be configured by network administrators with the knowledge of WLAN parameters. If you are not sure about your network conditions and the potential impact of any settings, we recommend you keep the default configurations.

Advanced Features

Fast Roaming:	□ Enable
Band Steering:	□ Enable

- To build a mesh network, enable Mesh in the **Services** section. All EAPs that support Mesh at the site will automatically build a mesh network. Additionally, to ensure the stability of the mesh network, enable Auto Failover. When a link in the mesh network fails, the controller will automatically establish another link to ensure all EAPs are still in the mesh network.
- To experience fast roaming, enable Fast Roaming in the **Advanced Features** section. 802.1k/v clients can seamlessly roam among the EAPs.

3.5 Controlling Access Rights with ACL

What is ACL (Access Control List)?

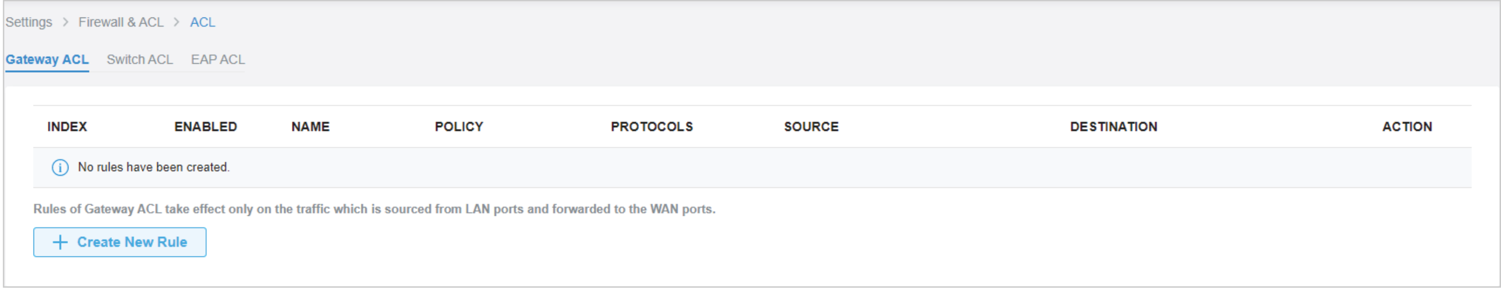
ACL (Access Control List) allows a network administrator to create rules to restrict access to network resources. ACL rules filter traffic based on specified criteria such as source IP addresses, destination IP addresses, and port numbers, and determine whether to forward the matched packets. These rules can be applied to specific clients or groups whose traffic passes through the gateway, switches and EAPs.

The system filters traffic against the rules in the list sequentially. The first match determines whether the packet is accepted or dropped, and other rules are not checked after the first match. Therefore, the order of the rules is critical. By default, the rules are prioritized by their created time. The rule created earlier is checked for a match with higher priority. To reorder the rules, select a rule and drag it to a new position. If no rules match, the device forwards the packet because of an implicit Permit All clause.

How to Configure it?

Go to **Settings > Firewall & ACL > ACL** to load the following page. Three types of ACL are supported: Gateway ACL, Switch ACL, and EAP ACL.

Figure 3-5 Configuring ACL



INDEX	ENABLED	NAME	POLICY	PROTOCOLS	SOURCE	DESTINATION	ACTION
ⓘ No rules have been created.							

Rules of Gateway ACL take effect only on the traffic which is sourced from LAN ports and forwarded to the WAN ports.

1) Click the tab to choose your desired type.
2) Create an ACL with the desired type and configure packet-filtering criteria for the rule.