ワイヤレスブリッジ

ユーザーマニュアル

法的情報

このドキュメントについて

- この文書には、製品の使用および管理に関する手順が記載されています。本文中に含まれる図、表、画像、およびその他の情報は、説明および参考目的のみを目的としています。
- 本ドキュメントに記載されている情報は、ファームウェアの更新またはその他の理由により、事前の通知なしに変更される場合があります。最新のバージョンは、Hikvisionのウェブサイト（**https://www.hikvision.com**）でご確認ください。別途合意がない限り、杭州 Hikvision デジタルテクノロジー株式会社またはその関連会社（以下「Hikvision」といいます）は、明示的または黙示的ないかなる保証もいたしません。
- 本ドキュメントは、製品をサポートする専門家の指導と支援を受けてご使用ください。

本製品について

この製品は、購入された国または地域でのみアフターサービスサポートを受けることができます。

知的財産権の承認商標の承認

- ヒクビジョンは、本文書に記載される製品に組み込まれた技術に関する著作権および/または特許権を保有しています。これには、第三者から取得したライセンスを含む場合があります。
- 本文書の一部（テキスト、画像、グラフィックなど）はすべてヒクビジョンに帰属します。本文書のいかなる部分も、書面による許可なしに、引用、複製、翻訳、または改変を行うことはできません。
- HIKVISIONおよびその他のヒクビジョンの商標およびロゴは、各管轄区域においてヒクビジョンの財産です。
- 本文書に記載されているその他の商標およびロゴは、それぞれの所有者の財産です。
- HDMIおよびHDMI High-Definition Multimedia Interface、ならびにHDMIロゴは、米国およびその他の国において、HDMI Licensing Administrator, Inc.の商標または登録商標です。

本文中に記載されたすべての商標およびロゴは、それぞれの所有者の財産です。

法的免責事項

- 適用される法律で許される最大限の範囲において、本文書および記載された製品（ハードウェア、ソフトウェア、ファームウェアを含む）は「現状有姿」かつ「一切の瑕疵およびエラーを含む」状態で提供されます。HIKVISIONOUR COMPANYは、明示的または黙示的ないかなる保証も提供しません。これには、商品性、満足のいく品質、または特定の目的への適合性を含むがこれらに限定されません。本製品の使用は、お客様の責任において行われます。いかなる場合においても、当社（HIKVISION）は、特別損害、間接損害、付随的損害、または派生的損害（事業利益の損失、事業の中断、データの損失を含むがこれらに限定されない）について、契約違反、不法行為（過失を含む）を理由とする場合であっても、一切の責任を負いません。

システム障害、または文書の損失を含む損害について、契約違反、不法行為（過失を含む）、製品責任、またはその他の理由によるものであっても、製品の使用に関連して生じた損害について、当社がそのような損害または損失の可能性について事前に通知を受けていた場合であっても、一切の責任を負いません。

- あなたは、インターネットの性質上、内在するセキュリティリスクが存在することを承認します。HIKVISION（当社）は、サイバー攻撃、ハッカー攻撃、ウイルス感染、またはその他のインターネットセキュリティリスクに起因する異常な動作、プライバシー漏洩、またはその他の損害について一切の責任を負いません。ただし、必要に応じて適切な技術サポートを提供いたします。
- お客様は、本製品を適用されるすべての法律に準拠して使用することに同意し、その使用が適用される法律に準拠していることを確保する責任はお客様にのみあります。特に、第三者の権利（ publicity rights、知的財産権、データ保護およびその他のプライバシー権を含むがこれらに限定されない）を侵害しない方法で本製品を使用する責任を負います。お客様は、大量破壊兵器の開発または製造、化学兵器または生物兵器の開発または製造、核爆発または安全でない核燃料サイクルに関連するいかなる活動、または人権侵害を支援する目的での使用を含みます。
- 本文書と適用される法律との間に矛盾が生じた場合、後者が優先されます。

©杭州HIKVISION JAPAN デジタルテクノロジー株式会社。著作権所有。

記号の規約

この文書で用いられる記号は、以下のとおり定義されます。

記号	説明
危険	危険な状況を示し、回避しない場合、死亡または重大なけがを引き起こす可能性があります。
注意	回避しない場合、機器の損傷、データ損失、性能の低下、または予期しない結果を引き起こす可能性がある危険な状況を示します。
注意	本文の重要な点を強調または補足するための追加情報を提供します。

目次

第1章 初回使用 **1**
1.1 アクティベーション 1
1.2 ログイン 3
1.3 デバイスペアリング 4
第2章 ウェブ設定 **5**
2.1 ネットワーク設定 6
2.1.1 WAN設定 6
2.1.2 LAN設定 7
2.1.3 データ転送設定 8
2.2 ワイヤレス設定 10
2.2.1 基本ワイヤレス設定 10
2.2.2 詳細なワイヤレス設定 13
2.2.3 管理者SSID 14
2.3 VLAN管理 15
2.4 PoE管理 16
2.5 端末セキュリティ 17
第3章 システムメンテナンス **19**
3.1 クラウドプラットフォームへのアクセス 19
3.2 システム診断 20
3.2.1 ログ管理 20
3.2.2 Pingツール 20
3.2.3 Ping 監視ツール 20
3.2.4 ワイヤレス帯域幅テスト 21
3.2.5 デバッグ情報の保存 21
3.3 システムセキュリティ 22
3.3.1 SSH 22
3.3.2 HTTP(S) 23

3.3.3 SADP 23
3.4 再起動と復元 24
3.5 デバイスのアップグレード 25
3.6 時間設定 25
3.7 インテリジェント電源管理 27
3.8 パスワードの変更 27
第4章 FAQ 2
4.1 デバイスがペアリングに失敗した理由は？ 28
4.2 デバイスが起動しない理由 28
4.3 信号強度が低すぎるのはなぜですか？ 28
4.4 信号品質が高いにもかかわらず、スループットが不十分な理由はなぜですか？ 29
4.5 無線接続率が相対的に低いのはなぜですか？ 29
4.6 PCがデバイスのIPアドレスにpingを送信した際に、パケット損失とタイム遅延が過剰に発生する理由は何か？ 29

第1章 初回使用時

1.1 アクティベーション

プライバシーとシステムデータのセキュリティを確保するため、初回使用時にパスワードの設定が必須です。パスワードを設定後、ウェブにログインしてさらに設定を行うことができます。

ワイヤレス接続でアクティベート

手順

1. パッケージに同梱のアクセサリーを使用して、ワイヤレスブリッジの電源を入れます。

   注意

   付属品はモデルによって異なります。クイックスタートガイドの「デバイス情報」をご確認ください。

2. ワイヤレスブリッジの背面にあるラベルを確認し、SNコードの最後の4桁（例：XXXX）を取得してください。

   SNコードの最後の4桁（例：XXXX）を確認してください。

3. スマートフォンまたはPCをワイヤレスブリッジのWi-Fiネットワークに接続してください。
   - **Wi-Fi 名称**: HIKVISION_XXXX
   - **パスワード**: 123456789abc

   注意

   管理用SSIDに接続しても、端末はインターネットにアクセスできません。

4. スマートフォンまたはPCのウェブブラウザを開き、**192.168.138.10** にアクセスしてください。
5. パスワードを設定し、確認してください。

   注意

   - デバイスのパスワードの強度は自動的にチェックされます。製品のセキュリティを強化するため、ご自身で選択したパスワード（大文字、小文字、数字、特殊文字の少なくとも3種類を含む8文字以上）に変更することを強くおすすめします。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをおすすめします。月次または週次でのパスワード変更は、製品の保護をさらに強化します。
   - すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストール担当者および/またはエンドユーザーの責任です。

6. **国/地域**を選択してください。
7. **「確認」**をクリックしてください。デバイスのアクティベーションが完了しました。

   注意

   ワイヤレス接続は一部のモデルでのみ利用可能です。アクティベーションに失敗した場合は、有線接続でデバイスをアクティベーションしてください。

有線接続でアクティベーション

手順

1. パッケージ内のアクセサリーを使用して、ワイヤレスブリッジの電源を入れます。

注意

付属品はモデルによって異なります。クイックスタートガイドの「デバイス情報」をご確認ください。

2. デバイスのLANポートを、PCのネットワークポートにイーサネットケーブルで接続してください。
3. PCのIPアドレスを、デバイスと同じネットワークセグメントに設定してください。
   a. PCの「**設定**」→「**→**」→「**ネットワークとインターネット**」→「**→**」→「**ネットワーク接続**」→「**→**」→「**Ethernet**」→「**→**」→「**一般**」→「**インターネットプロトコルバージョン4（TCP/IPv4）**」のプロパティを開きます。
   b. 「**次の IP アドレスを使用する**」にチェックを入れます。
   c. PCのIPアドレスを、デバイスと同じネットワークセグメントに設定します。

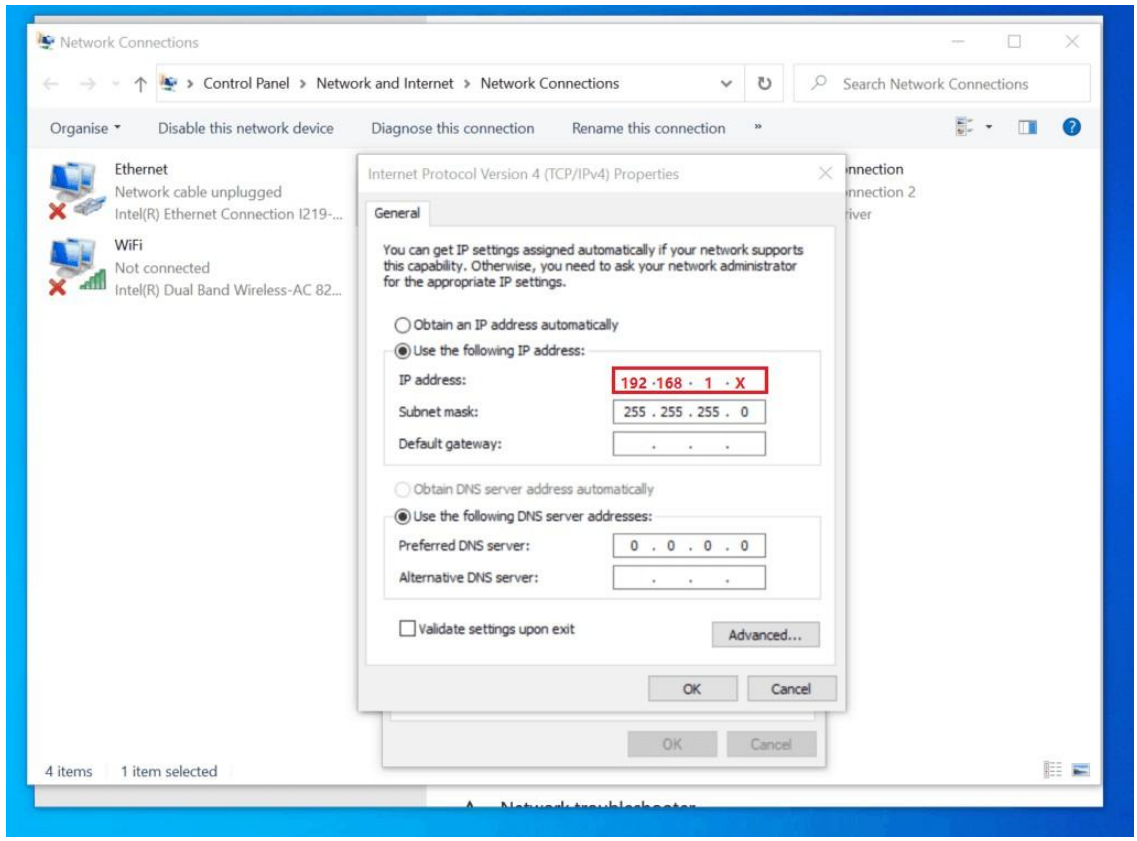

図1-1 PCのIPアドレスを設定する

4. ウェブブラウザを開き、アドレスバーにデバイスのIPアドレスを入力してアクセスしてください。
   - APのデフォルトIPアドレス: 192.168.1.35
   - CPEのデフォルトIPアドレス: 192.168.1.36
   - デフォルトのユーザー名: admin

注意

デバイスの背面のラベルを確認して、IPアドレスを確認してください。

5. パスワードを設定し、確認してください。

注意

- デバイスのパスワードの強度は自動的にチェックされます。製品のセキュリティを強化するため、ご自身で選択したパスワード（大文字、小文字、数字、特殊文字の少なくとも3種類を含む8文字以上）に変更することを強くおすすめします。また、特に高セキュリティシステムでは、パスワードを定期的に変更することをおすすめします。パスワードを毎月または毎週変更することで、製品の保護をさらに強化できます。
- すべてのパスワードおよびその他のセキュリティ設定の適切な設定は、インストール担当者および/またはエンドユーザーの責任です。

6. **国/地域**を選択してください。
7. **「確認」**をクリックしてください。デバイスのアクティベーションが完了しました。

デバイスにログインしてください

デバイスにログインして、デバイス情報を確認し、関連するパラメーターを設定してください。

手順

1. ウェブブラウザのアドレスバーにIPアドレスを入力し、Enterキーを押してください。
   - APのデフォルトIPアドレス: 192.168.1.35
   - CPEのデフォルトIPアドレス: 192.168.1.36
2. ユーザー名とパスワードを入力します。
   - デフォルトのユーザー名: admin
   - パスワードはアクティベーション時に設定したものです。
3. **ログイン**をクリックしてください。

1.2 ログイン

デバイスにログインして、デバイス情報を確認し、関連するパラメーターを設定します。

手順

1. ウェブブラウザのアドレスバーにIPアドレスを入力し、Enterキーを押します。
   - APのデフォルトIPアドレス: 192.168.1.35
   - CPEのデフォルトIPアドレス: 192.168.1.36
2. ユーザー名とパスワードを入力します。
   - デフォルトのユーザー名: admin
   - パスワードはアクティベーション時に設定したものです。
3. **ログイン**をクリックしてください。

1.3 デバイスペアリング

デバイスのペアリング

ペアで梱包されたデバイスは、アクティベーション後に自動的に互いにペアリングされます。

DIPスイッチ搭載デバイス

手順

1. デバイス上の**AP/CPE DIPスイッチ**を設定します。1つのデバイスを**AP**に、他のデバイスを**CPE**に設定してください。
2. デバイスの**SSID** DIPスイッチを設定します。グループ内のすべてのデバイスが同じSSIDに設定されていることを確認してください。

他のデバイス

ステップ

1. デバイスのウェブにログインしてください。
2. **ワイヤレス設定**に移動し、**→ 基本設定を選択します**。
3. 1つのデバイスを**AP**動作モードに設定し、他のデバイスを**CPE**動作モードに設定します。
4. すべてのデバイスの**PSKパスワードを**同じに設定します。

ペアリングに失敗しました

ペアリングに失敗した場合は、以下の項目を確認してください：

1. 2つのデバイスが宣言された距離内で向かい合って設置されているか確認してください。
2. デバイス上の**リセット**ボタンを4秒以上長押ししてデバイスを初期化してください。その後、デバイスを再起動してください。
3. ペアリングが失敗した場合は、技術サポート担当者までご連絡ください。

第2章 ウェブ設定

ウェブブラウザを通じて、ワイヤレスブリッジ（以下、デバイスと呼びます）のネットワーク設定、ワイヤレスネットワーク設定、システム管理など、各種設定を管理および構成できます。

注意
機能はデバイスモデルによって異なります。ここに示された画像は例示のためのものであり、実際のインターフェースが優先されます。

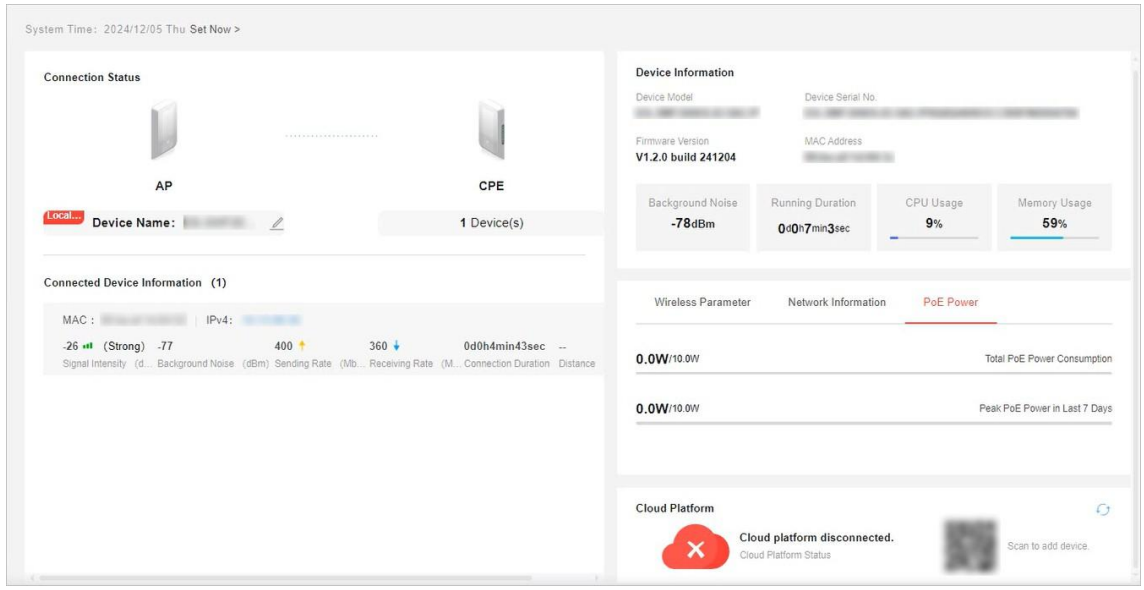

図2-1 概要 表2-1 概要 説明

情報と操作	説明
デバイス情報	デバイスの名前、モデル、シリアル番号、プログラムバージョン、MACアドレス、CPU使用率、メモリ使用率、動作時間、およびデバイスの背景ノイズ状態などを確認します。
接続状態	デバイスの接続状態を確認します。
接続されたデバイス情報	接続されたデバイス（例：ピアブリッジデバイス）のMAC/IPアドレス、信号強度、送信レート、受信レート、接続時間を確認します。
無線パラメーター	デバイスの動作シーン、SSID、無線モード、チャンネル、チャンネル幅、セキュリティモードを確認してください。LANパラメーターは設定可能です。詳細については***LAN設定***を参照してください。

情報と操作	説明
ネットワーク情報	デバイスのIPv4アドレス、サブネットマスク、ゲートウェイ、DNS、代替DNSを確認してください。
PoE 電源	過去7日間の総PoE電力消費量とピークPoE電力を確認してください。詳細については***PoE管理***を参照してください。
クラウドプラットフォーム	クラウドプラットフォームの接続状態を確認するか、QRコードをスキャンしてアプリにアドバイスを追加してください。詳細については、***VLAN管理***を参照してください。
クイック タイム設定	「今すぐ設定」をクリックしてシステム時間を設定します。詳細については*「タイム設定」*を参照してください。
クイックデバイス名変更	「 」をクリックしてデバイス名を変更します。または、**システム→ システム構成→ 基本情報** に移動します。
ユーザーマニュアルを確認してください	をクリックして、Web ユーザー マニュアルを確認します。
システムパスワードを変更する	をクリックしてシステムパスワードを変更します。詳細については「*パスワードの変更」*を参照してください。
ログアウト	をクリックしてログアウトします。

注意

このページの情報はモデルによって異なります。実際のインターフェースが優先されます。

2.1 ネットワーク設定

2.1.1 WAN 設定

ネットワーク設定に移動し、**→ WAN 設定を開き**、**ネットワーク接続**方法や **WAN IPv4** などの関連パラメーターを設定します。

注意

この機能はモデルによって異なります。また、一部のデバイスが**AP**サイトとして設定されている場合のみサポートされます。実際のインターフェースが優先されます

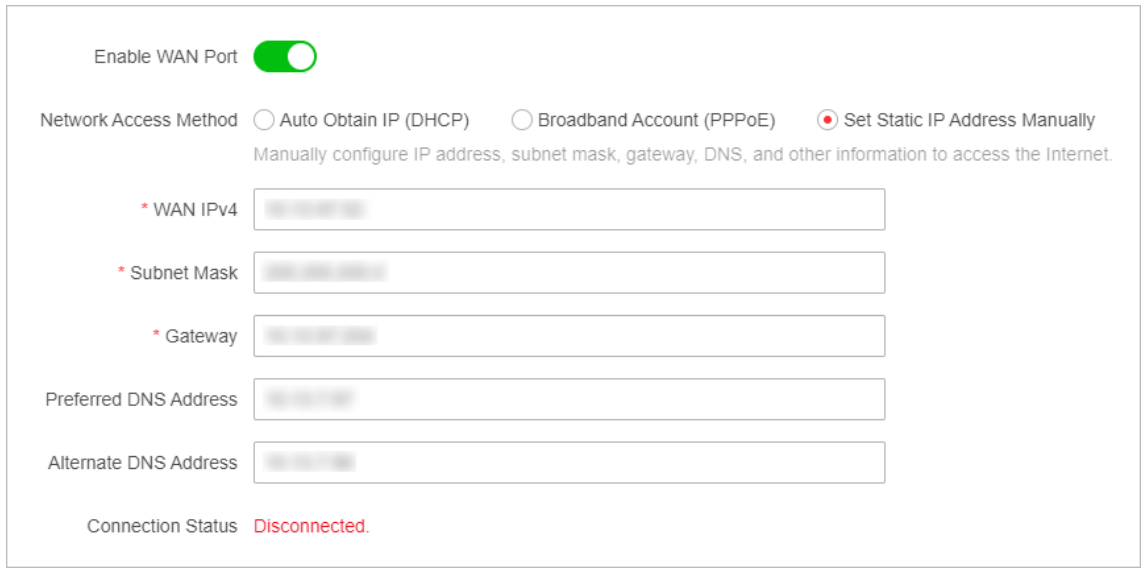

図2-2 WANポート設定表2-2 パラメータ

一説明

パラメーター	説明
DHCP	このモードを選択した場合、追加の設定は不要です。
PPPoE	ISP（インターネットサービスプロバイダー）からブロードバンドアカウントとパスワードが提供されている場合、このモードを選択してください。
静的IP	ISPからIPアドレスその他の関連情報が提供されている場合、このモードを選択してください。

2.1.2 LAN設定

ネットワーク設定に移動し、→ **LAN 設定**を選択して、詳細なネットワークパラメーターを設定します。
「**IPを自動取得**」を**有効**にすると、他のパラメーターは自動的に設定されます。

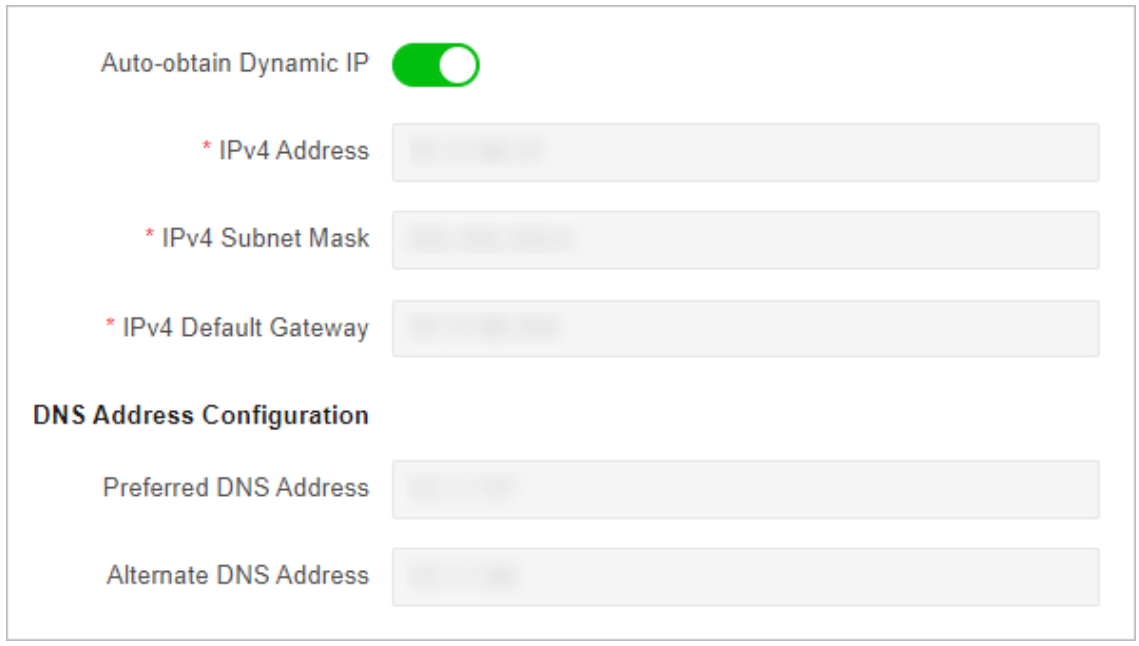

図2-3 LAN設定

注

- この機能はモデルによって異なります。WAN ポートを搭載したデバイスでは DHCP サーバーの設定が可能です。実際のインターフェースが優先されます。
- IPアドレスがリセットされると、ウェブページは新しく設定されたIPアドレスの新しいログイン画面にリダイレクトされます。
- IPアドレスの衝突を防止するため、デバイスIPアドレスを設定する際はSADPツールの使用を推奨します。

2.1.3 データ転送設定

複雑なLAN環境において、特定のマルチキャスト、ブロードキャスト、および未知のユニキャストパケットがデバイスに与える悪影響を軽減するため、必要に応じてパケットをフィルタリングできます。**ネットワーク設定→ データ転送設定**に移動し、デバイスのパケットフィルタリング機能を有効/無効に設定します。

注意

機能はモデルによって異なります。この機能は、一部のデバイスがAPサイトとして設定されている場合にのみサポートされます。実際のインターフェースが優先されます。

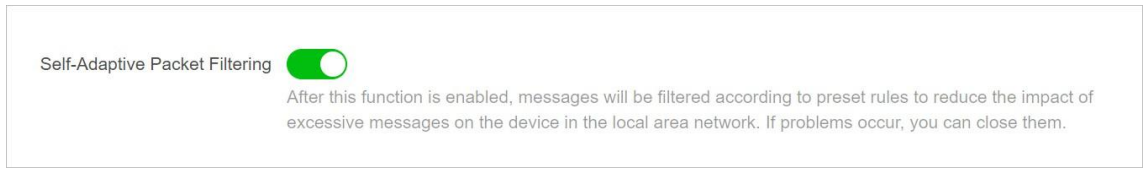

図2-4 自己適応パケットフィルタリングの有効化

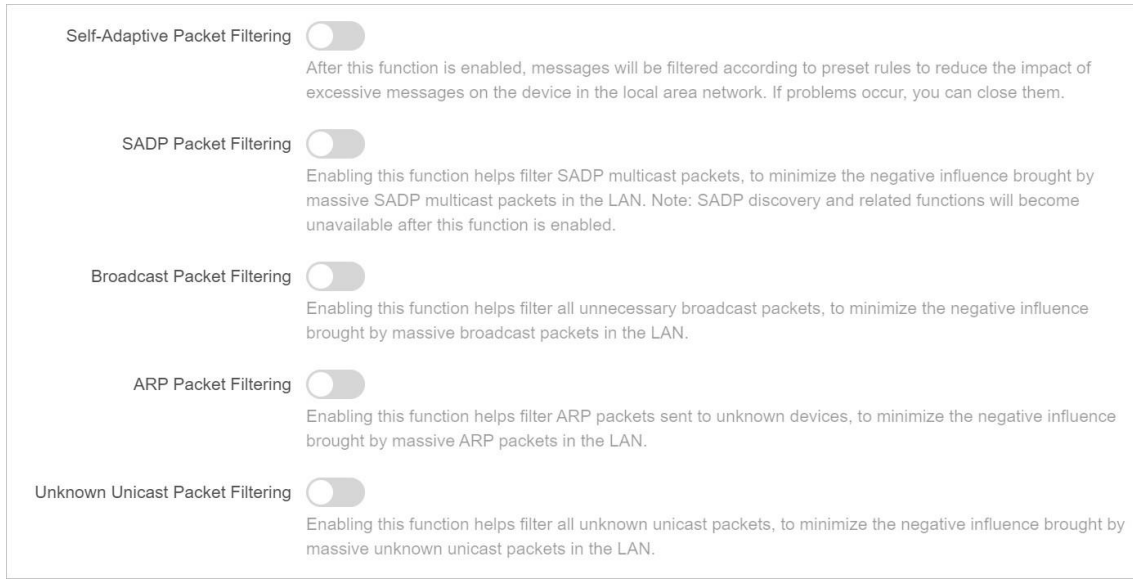

図2-5 自己適応型パケットフィルタリングの無効化表2-3 パラメ

ーター説明

パラメーター	説明
自己適応型パケットフィルタリング	デフォルトで有効です。現在のルールに従ってパケットをフィルタリングし、LAN内のデバイスへの過剰なメッセージの影響を軽減します。
SADP パケットフィルタリング	LAN内の大量のSADPマルチキャストパケットによる悪影響を最小限に抑えるため、SADPマルチキャストパケットをフィルタリングします。 **注意** この機能を有効にすると、SADPの検出および関連機能は利用できなくなります。
ブロードキャストパケットフィルタリング	LAN内で大量のブロードキャストパケットがもたらす悪影響を最小限に抑えるため、不要なブロードキャストパケットをすべてフィルタリングします。

パラメーター	説明
ARPパケットフィルタリング	未知のデバイス宛てに送信されるARPパケットをフィルタリングし、LAN内の大量のARPパケットによる悪影響を最小限に抑えます。
未知のユニキャストパケットのフィルタリング	LAN内で大量の未知のユニキャストパケットがもたらす悪影響を最小限に抑えるため、すべての未知のユニキャストパケットをフィルタリングします。

2.2 ワイヤレス設定

ワイヤレス設定をクリックして、ワイヤレスネットワークの基本設定と詳細設定を設定します。

2.2.1 基本ワイヤレス設定

ワイヤレス設定の「→ 基本設定」に移動し、ワイヤレスネットワークの基本パラメーターを設定します。

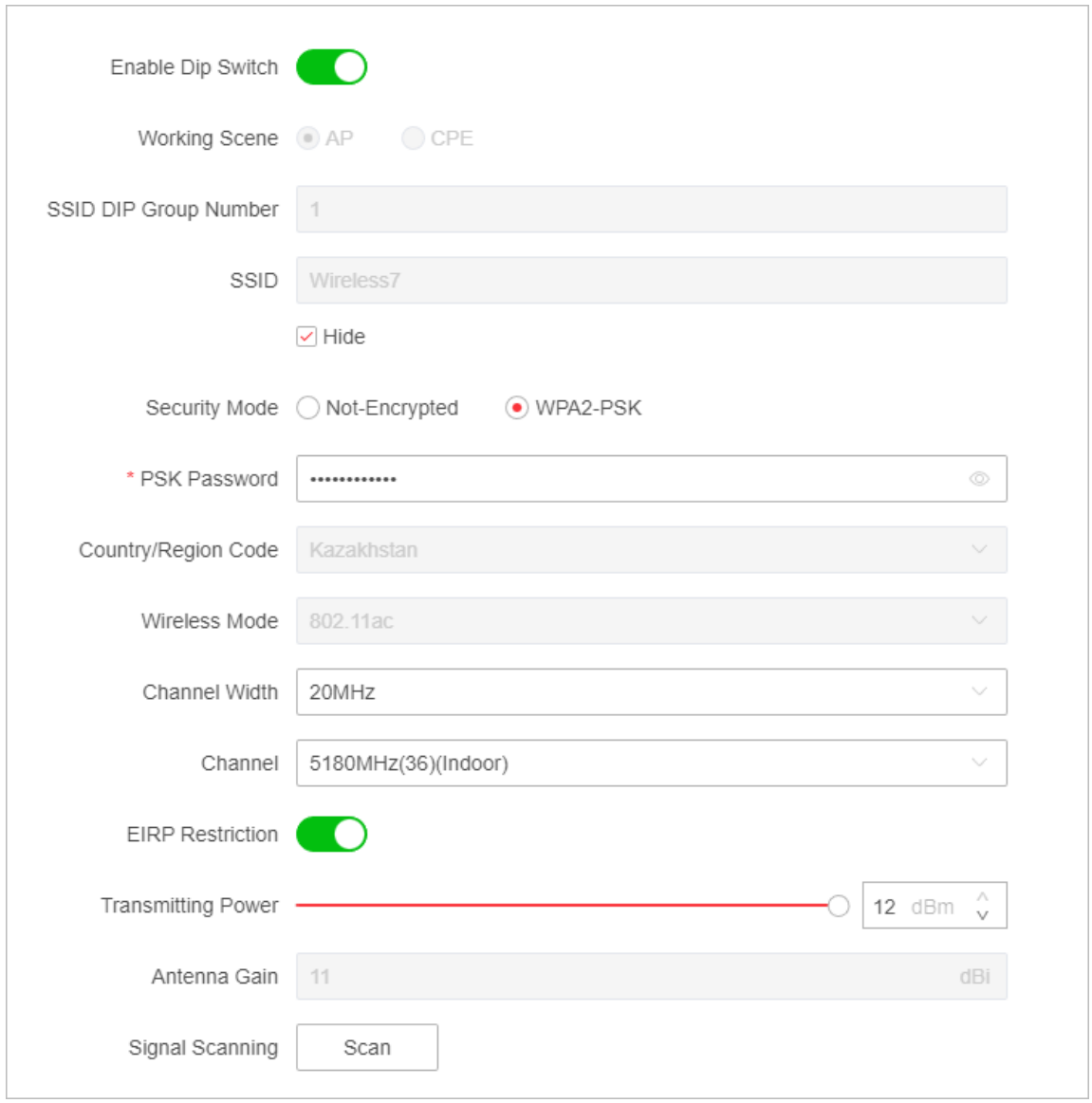

図2-6 無線ネットワークの基本設定

注

上記に示した図は、DIPスイッチ機能を備えたデバイスの例です。この機能のパラメーターはモデルによって異なります。実際のインターフェースが優先されます。

表2-4 パラメーター説明

パラメーター	説明
DIPスイッチの有効化	DIPスイッチを介してペアリングコードとシーン切り替え機能を有効/無効にします。この機能はデフォルトで有効になっています。

パラメーター	説明
	注意 • DIPグループ番号が不足している場合、この機能を無効化し、SSIDを適切に設定してください。 • DIPスイッチの有効/無効設定は、無線接続を切断します。操作にはご注意ください。 • このパラメーターは、DIPスイッチ機能を備えたデバイスでのみ利用可能です。
動作シーン	ウェブ経由で**作業シーン**を任意に設定できます。APを選択して作業シーンを設定します。 **APを動作シーン**として設定します。CPEを選択して**CPEを動作シーン**として設定します。
SSID DIPグループ番号	1から16まで。異なるグループ番号を示すために使用されます。この情報は、DIPスイッチが有効になっている場合のみ表示されます。 注意 このパラメーターは、DIPスイッチ機能を備えたデバイスでのみ利用可能です。
SSID	デフォルトでは、SSIDはダイヤルグループ番号によって決定され、CPEはSSIDに基づいてAPとペアリングします。 セキュリティのため、APのSSIDを非表示にすることをおすすめします。
セキュリティモード	• デフォルトでは**W**PA**2-PSK**が設定されており、暗号化方式はAESです。 • 「**暗号化なし**」を選択した場合、**PSK秘密鍵**を設定する必要はありません。
PSKパスワード	CPEとAPのペアリングパスワードです。**セキュリティモードがWPA2-PSK**に設定されている場合、**PSKパスワード**を設定する必要があります。
国/地域コード	デバイスを起動する際に設定します。選択後は変更できません。ただし、すべての設定をデフォルト設定に復元した場合を除きます。
ワイヤレスモード	設定できません。
チャネル幅	• APの場合：チャネル幅は選択可能です。具体的な値は国/地域コードによって異なります。 • CPEの場合：チャネル幅はAPに応じて自動的に変更されます。設定できません。
チャネル	• APの場合：デフォルトで「**自動**」が設定されています。ご希望の値を選択できます。 • CPEの場合：デフォルトで「**自動**」が設定されています。設定変更はできません。
EIRP制限	デバイスのEIRP（有効等方放射電力）を制限するために確認してください。
送信電力	無線のカバー範囲と最大達成可能な信号対雑音比に影響を与える重要な要因です。

パラメーター	説明
アンテナ利得	ピーク放射方向における送信電力と等方性光源の放射方向における送信電力の比。
信号スキャン	**「スキャン」**をクリックし、周辺にある利用可能なチャンネルの信号強度を確認するために最適なチャンネルを選択します。

2.2.2 高度な無線設定

ワイヤレス設定に移動し、**→ を選択し、詳細設定を開きます。TDMA** と**インテリジェント周波数管理**を必要に応じて有効または無効に設定します。

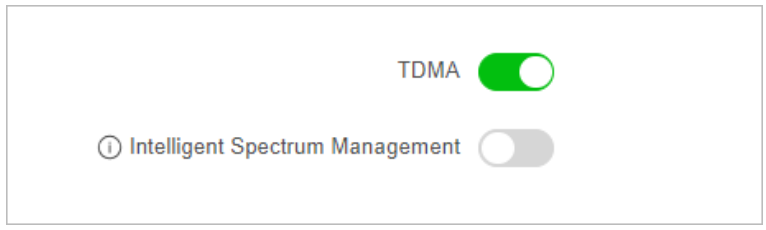

図2-7 詳細設定 表2-5 パラメーター説明

パラメーター	説明
TDMA	APが複数のデバイスに接続されている際に、作業環境の通過性能を向上させるためにTDMAを有効にします。 **注** この機能はモデルによって異なります。また、一部のデバイスがAPサイトとして設定されている場合のみサポートされます。実際のインターフェースが優先されます。
インテリジェント周波数管理	**インテリジェント周波数管理を**有効にすると、干渉が検出された際に安定した動画伝送を保証します。 **注意** • この機能は、**AP**を作業シーンとして設定した場合にのみ、一部のモデルで利用可能です。 • この機能を使用すると、作業チャンネルは、DFS（ダイナミック周波数選択）チャンネルと室内チャンネルを除くすべての選択肢の中から最適なチャンネルに自動的に切り替わります。

パラメーター	説明
	• この機能は国によって異なります。一部の国ではこの機能は利用できません。 • この機能を有効にしている場合、チャンネルとチャンネル幅を手動で設定できません。ローミングが必要な場合は、この機能を無効にすることをおすすめします。

2.2.3 管理用SSID

モバイル端末やPCからデバイスWi-Fiネットワークに接続し、AP/CPEデバイスの設定やメンテナンスなどの管理が可能です。

注意

- この機能は一部のモデルでのみ利用可能です。実際のインターフェースが優先されます。
- 管理用SSIDに接続しても、端末はインターネットにアクセスできません。
- 帯域幅が10 Mbpsの場合、管理用SSID機能は当該デバイスでのみサポートされます。

手順

1. **管理SSID**に移動します。
2. 管理用SSIDはデフォルトで有効になっています。PSKパスワードはデフォルトで***123456789abc***です。
3. **SSID**と**PSKパスワードを**カスタマイズします。セキュリティモードが「非暗号化」に設定されている場合、端末はパスワードなしでWi-Fiネットワークに接続できます。
4. 端末のブラウザから1***92.168.138.10にアクセス***し、ブリッジデバイスを管理します。

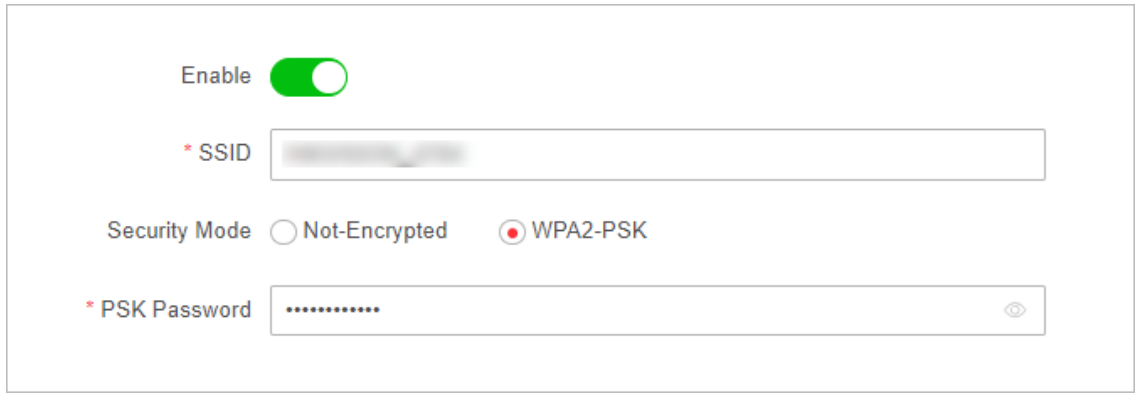

図2-8 セット管理SSID

2.3 VLAN管理

VLAN（Virtual Local Area Network）は、ローカルエリアネットワーク内のデバイスを物理的にではなく論理的に個々のネットワークセグメントに分割し、これによりローカルエリアネットワーク内のブロードキャストドメインの隔離を実現する技術です。

注
この機能は一部のモデルでのみ利用可能です。実際のインターフェースが優先されます。

手順

1. **VLAN管理**に移動します。
2. VLANを有効にします。
3. ポートのVLANを設定します。
   a. 設定するポートを選択します。
   b. VLAN タイプを選択します。
      - TRUNK ポート: すべての VLAN トラフィックを転送し、すべての VLAN を通過させるために使用されます。
      - ACCESS ポート: 指定された VLAN のパケットのみを送信します。
   c. PVIDを設定します。（範囲：1～4093）
4. **保存**をクリックします。
5. (オプション) 各ポートのVLAN情報を確認します。

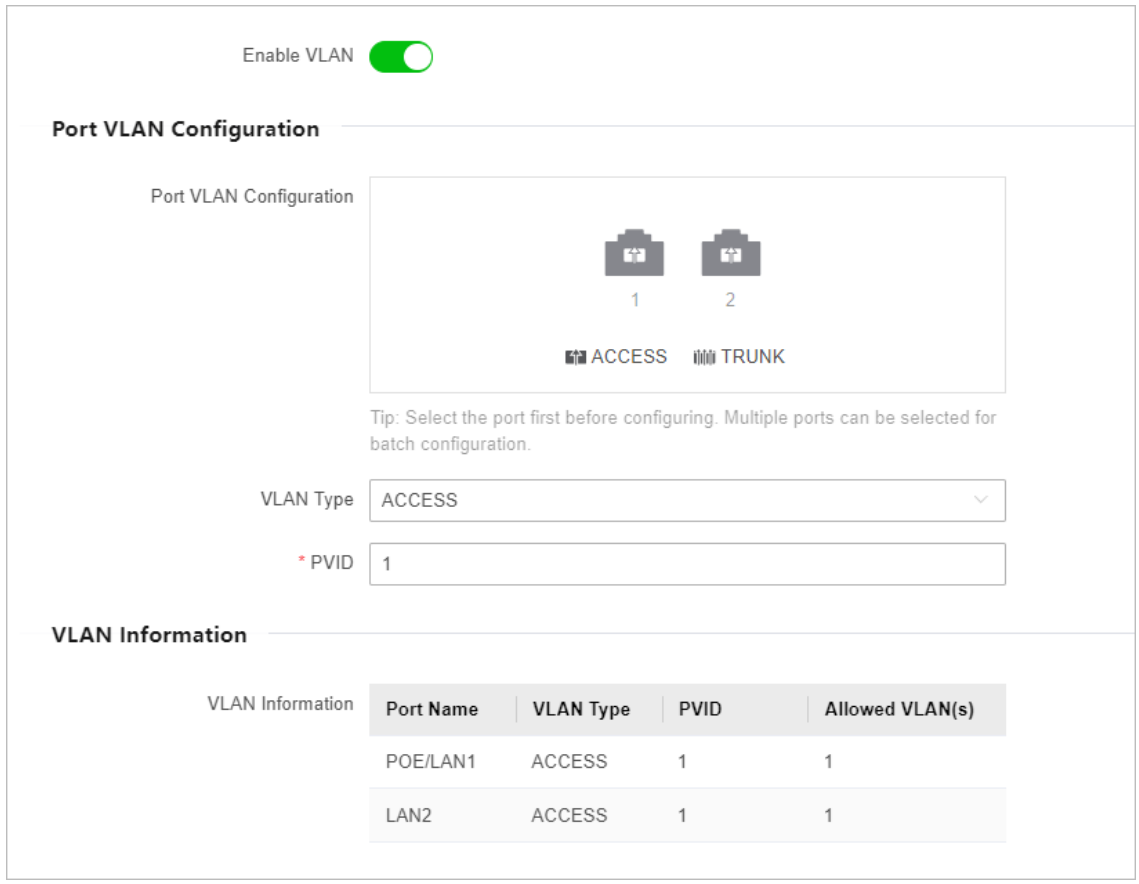

図2-9 VLAN管理

2.4 PoE 管理

PoE管理をクリックして、PoEポートを必要に応じて管理します。

注

この機能は一部のモデルでのみ利用可能です。実際のインターフェースが優先されます。

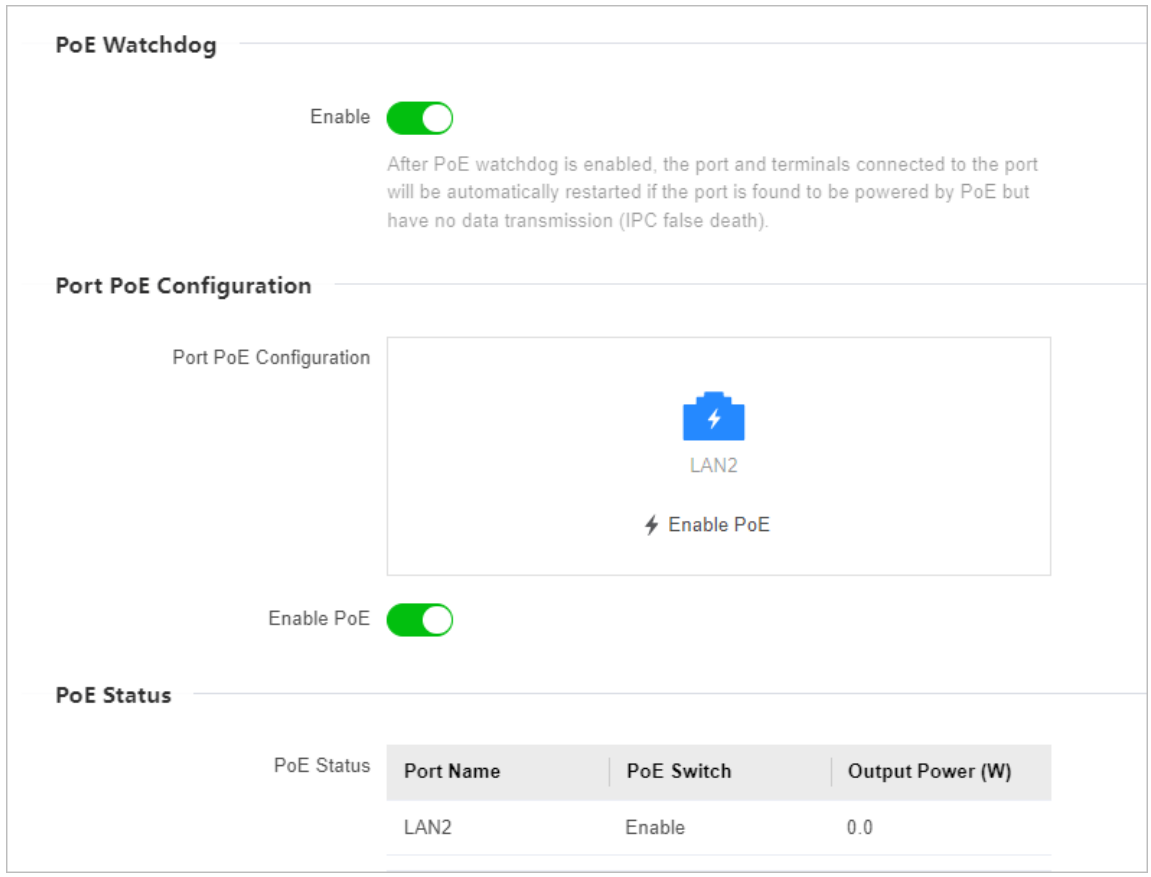

図2-10 PoE管理

PoE ウォッチドッグ

PoE ウォッチドッグを有効にすると、PoE ポートに接続されたデバイスの接続状態を自動的に検出します。特定のポートの IPC で通信障害が発生した場合、PoE は自動的に検出・再起動し、デバイスの正常な動作を保証します。

PoE ステータス制御

PoE を配布する必要があるポートのアイコンを選択し、そのポートの PoE 機能を**有効**または**無効**にするためにクリックし、設定を保存するために **OK** をクリックします。

2.5 ターミナルセキュリティ

ターミナルセキュリティに移動し、適切なモードを選択します。

デバイスはターミナルのブランドを識別し、セキュリティポリシーを一致させてターミナルの分類管理を実現します。

注意

この機能は一部のモデルでのみ利用可能です。実際のインターフェースが優先されます。

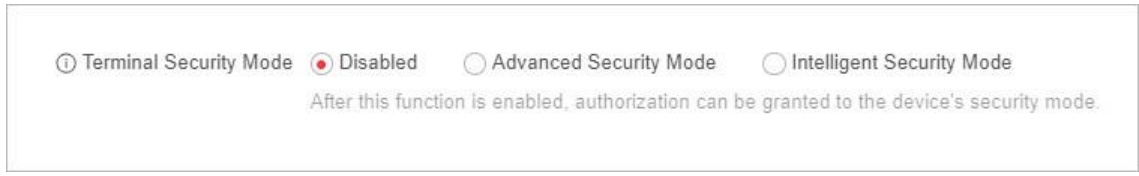

図2-11 ターミナルセキュリティ

- **高度なセキュリティモード**: この無線ブリッジ経由でアクセスされた端末の情報を端末認証リストに表示し、ユーザーは手動でそれらの端末を構成できます（未認証の端末はネットワークにアクセスできません）。
- **インテリジェントセキュリティモード**: 端末認証リストには、このネットワークブリッジ下のアクセス端末情報が表示されます。端末デバイスは、無線ブリッジ自体のインテリジェントセキュリティポリシーに基づいてバインディングされます。

注

ウェブ上で高度なセキュリティモードを有効にした後、他のクライアント（例：HPPアプリ）での設定変更はサポートされません。

第3章 システムメンテナンス

コンセプトの短い説明を入力してください（任意）。これがコンセプト
の開始点です。

3.1 クラウドプラットフォームへのアクセス

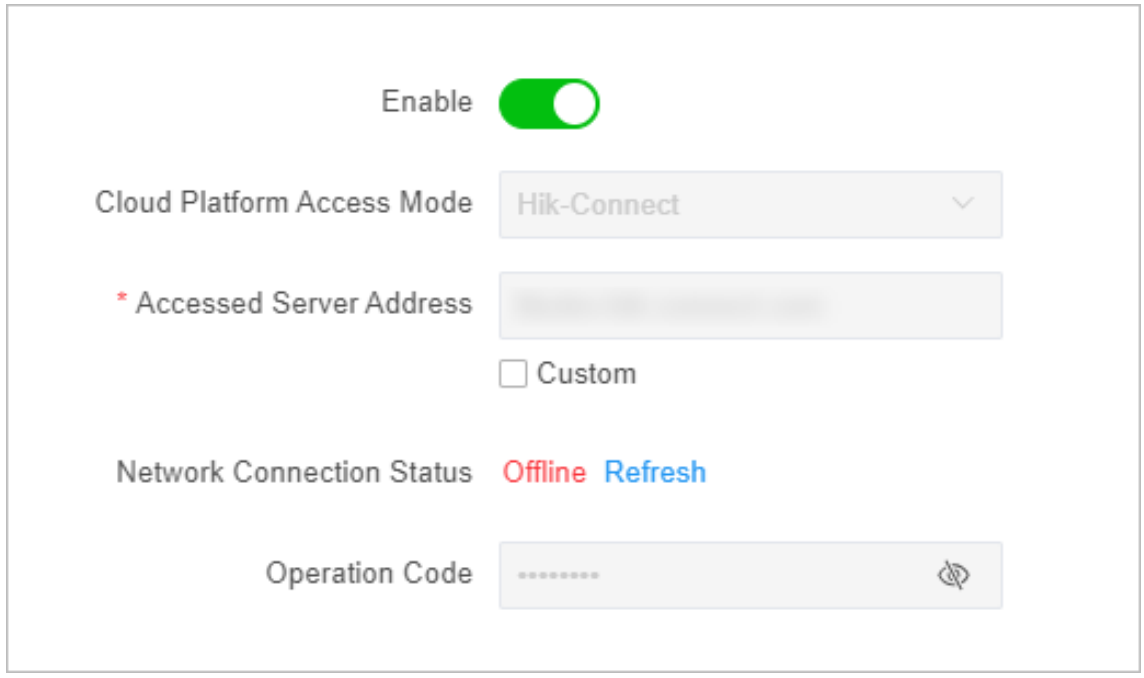

図3-1 クラウドプラットフォームの設定表3-1 パラ

メーター説明

パラメーター	説明
有効	有効化後、デバイスはHIK-Connectプラットフォームに接続されます。デバイスがパブリックネットワークに接続されていることを確認してください。
クラウドプラットフォームアクセスモード	HIK-Connectのみがサポートされています。
アクセスするサーバーアドレス	HIK-Connectプラットフォームのサーバーアドレス（ドメイン名）。ユーザーはサーバーへのアクセス用にアドレスをカスタマイズすることもできます。

パラメーター	説明
ネットワーク接続状態	HIK-Connectプラットフォームに接続されているデバイスの状態。
操作コード	HPPアプリ経由でデバイスを追加する際、ユーザーのデバイスの所有権を確認するために使用されます。

注意

最初の設定では、操作コードは空に設定されます。クラウドプラットフォームへのアクセスが有効化され、設定が保存されると、デバイスの操作コードが自動的に取得されます。

3.2 システム診断

3.2.1 ログ管理

必要なログをローカルストレージにエクスポートします。

手順

1. 診断→ **ログ管理**に移動します。
2. **エクスポート**をクリックしてログファイルを保存します。

3.2.2 Ping ツール

Ping ツールを使用すると、ネットワークの状態情報を取得でき、技術サポートに役立ちます。

手順

1. **診断**に移動し、→ **ネットワークツール**→ **Ping ツールを選択します**。
2. IPアドレスを入力してください。
3. 「**診断を開始**」をクリックしてください。診断結果が表示されます。

3.2.3 Ping ウォッチドッグ

特定のIPアドレスにPingを送信し、パケット損失を確認することで、技術サポート担当者はデバイスの動作状態を調査できます。デバイスが異常状態の場合、技術サポート担当者はデバイスを再起動する可能性があります。

手順

1. **診断**に移動→ **ネットワーク**ツール→ **Ping Watchdog**。
2. **Ping Watchdog を**有効にします。
3. 関連情報を入力します。

- **間隔**: Ping パケットの間隔。
- **開始遅延**: デバイスが異常状態にある場合の再起動までの遅延時間。
- **連続失敗回数**: パケット損失時間の制限値です。パケット損失時間がこの制限値に達すると、デバイスは異常と判定されます。

4. **保存**をクリックします。

3.2.4 無線帯域幅テスト

技術者は、無線帯域幅テストにより無線ネットワークがスムーズかどうかを確認できます。

注 機能は一部のモデルでのみ利用可能です。実際のインターフェースが優先されます。

手順

1. 診断→ **ネットワークツール**→ **ワイヤレス帯域幅テスト**に移動します。
2. **テスト**をクリックして結果を取得します（ソースIP、ターゲットIP、平均帯域幅、最小帯域幅を含む）。

3.2.5 デバッグ情報を保存

異なる印刷レベルのデバッグ情報をフラッシュに保存し、保存された情報はデバイスが電源を切断され再起動された後も復元可能のため、技術サポート担当者が原因の調査や後のメンテナンスを容易に行うことができます。

手順

1. **システム**→ **システムメンテナンス**→ **デバイスデバッグ**に移動します。

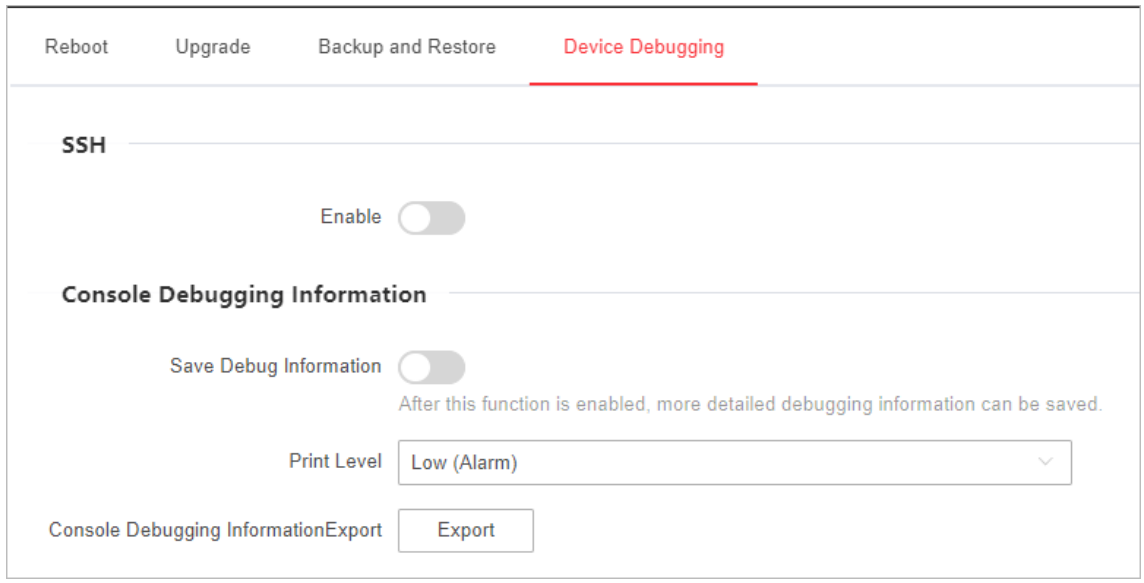

図3-2 デバイスデバッグ

2. 印刷レベルを選択します。レベルが高いほど、保存される情報が詳細になります。
3. **デバッグ情報を保存する機能を**有効にします。7日後に、この機能は自動的に無効になります。
4. **保存**をクリックします。
5. (オプション) デバッグ情報ファイルをエクスポートします。

3.3 システムセキュリティ

3.3.1 SSH

SSHプロトコルは、リモート管理による情報漏洩を防止します。SSHサービスが有効になっている場合、デバイスをリモートで管理できます。SSHサービスはデフォルトで無効になっています。

ネットワークセキュリティを強化するため、SSHサービスを無効にすることをおすすめします。この設定は、機器のデバッグを行う専門技術者専用です。

手順

1. **システム→ システムメンテナンス→ デバイスデバッグ** へ移動します。
2. **SSHを**有効にします。

注意

SSHクライアントのユーザー名は**rootです**。パスワードはウェブログイン時のパスワードと同じです。

3.3.2 HTTP(S)

HTTPプロトコル（Hypertext Transfer Protocol）は、TCPプロトコルを基盤とするアプリケーション層のトランスポートプロトコルです。一方、HTTPSプロトコル（Secure Hypertext Transfer Protocol）は、SSL+HTTPプロトコルを基盤として構築されたネットワークプロトコルで、暗号化通信と身分認証を行うことができます。

注 ポート情報は一部のモデルでのみ利用可能です。実際のインターフェースが優先されます。

手順

1. システム→ セキュリティ管理→ **HTTP(S)** へ移動します。
2. HTTPS サービスを有効にします。
3. HTTPSまたはHTTP接続用のサーバーポート番号を入力します。

図3-3 HTTP(S) サービス

注

- HTTPS サービスは、有効化されている場合、デフォルトでポート 443 で利用可能です。
- HTTPサービスはデフォルトでポート80で利用可能です。
- HTTPS サービスのサーバーポート番号は、443 または 2000 から 65535 までの任意の番号に設定できます。

3.3.3 SADP

SADP サービスが有効になっている場合、ソフトウェアを通じてデバイスのアクティベーション、パスワードの変更、IP アドレスの修正を行うことができます。SADP サービスはデフォルトで有効になっています。

手順

1. **システム→ セキュリティ管理→ SADP** へ移動します。
2. **SADPを**有効にします。

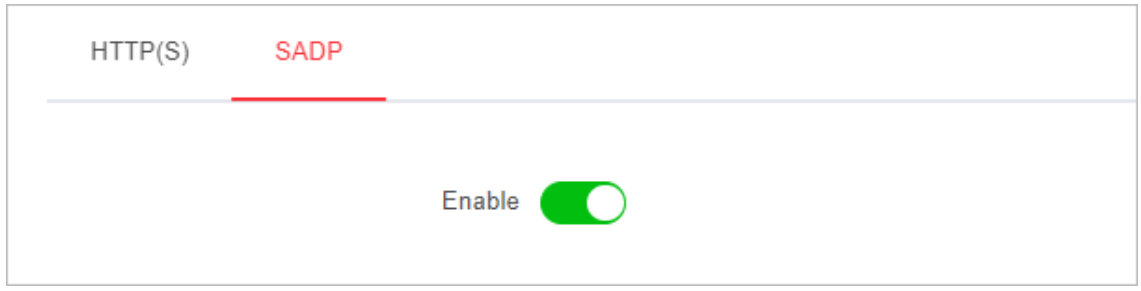

図3-4 SADP サービス

注

SADP サービスが無効になっている場合、一部の機能が利用できなくなる可能性があります。このサービスを有効にすることをおすすめします。

3.4 再起動と復元

ウェブページ経由でデバイスをリモートで再起動または復元できます。

デバイスの再起動

手順

1. **システム→ システムメンテナンス→ リブート** を選択します。
2. 「**再起動**」をクリックします。

バックアップと復元

システム→ システムメンテナンス→ バックアップと復元を選択し、バックアップまたはデフォルト設定の復元を行います。

- **バックアップ**：[エクスポート] をクリックし、デバイス パラメーター ファイルのパスワードを設定します。
- **デバイスパラメーターのインポート**：クリックし、以前にエクスポートしたデバイスパラメーターファイルを選択します。
- **簡易復元**：ネットワーク設定とユーザー設定を除く、すべてのパラメーターをデフォルト設定に復元します。設定を除く。
- **すべて復元**：すべてのパラメーターをデフォルト設定に復元します。

注意

- すべてのパラメーターを復元すると、すべての設定が消去されます。操作にはご注意ください。
- 復元前にすべての設定ファイルをエクスポートすることをおすすめします。
- デバイス パラメーター ファイルのインポートにはパスワードが必要です。デバイス パラメーター ファイルがインポートされると、デバイスは自動的に再起動します。

3.5 デバイスのアップグレード

利用可能なアップグレードには最新のファームウェアを使用し、ウェブページ経由でリモートでデバイスをアップグレードしてください。

開始前に

リモートアクセスに使用するPCのローカルディレクトリにアップグレードパッケージをコピーしてください。

手順

1. **システム→ システムメンテナンス→ アップグレード**。
2. クリックしてローカルディレクトリに移動し、希望のアップグレードパッケージを選択してください。
3. **アップグレード**をクリックします。

注意

- アップグレード後、デバイスは自動的に再起動します。再度ログインする必要があります。
- アップグレードに失敗し、デバイスが正常に動作しない場合は、サプライヤーに連絡して復旧してください。

3.6 時間設定

手動での時間同期とNTP時間同期の両方がサポートされています。

手動設定

手順

1. **システム→ システム構成→ 時間構成**。
2. **タイムゾーン**を選択してください。

   注意

   国/地域コードを設定した後、タイムゾーンは自動的に選択されます。必要に応じて、希望のタイムゾーンを選択することもできます。

3. **時間同期方法**として「**手動時間同期**」を選択してください。
4. 希望の時刻を設定するか、または「**コンピュータの時刻と同期**」に**チェック**を入れます。

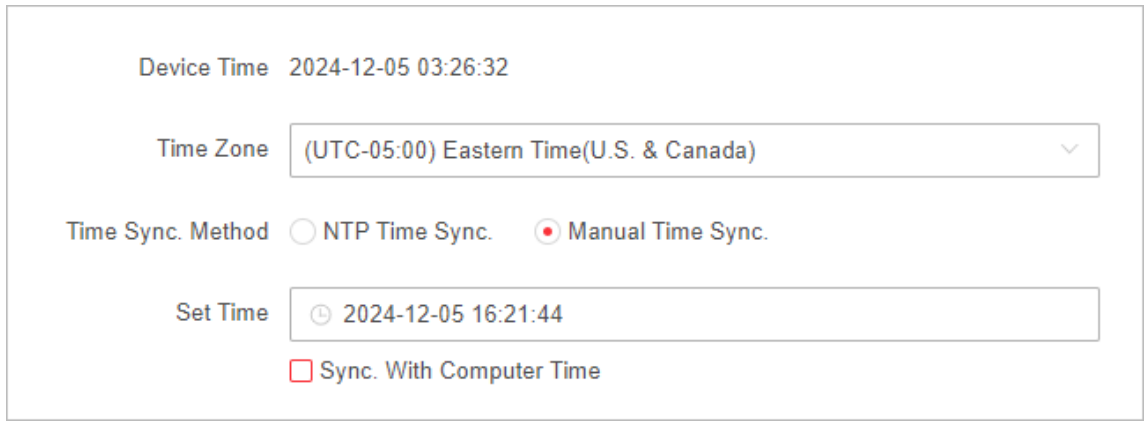

図3-5 手動設定

5. 「**保存**」をクリックします。

NTP設定

NTP 時刻同期は、特定の NTP サーバーの時刻と同期させるために使用されます。

手順

1. **システム→ システム構成→ 時間構成** へ移動します。
2. **タイムゾーン**を選択してください。

注意

国/地域コードを設定した後、タイムゾーンは自動的に選択されます。必要に応じて、希望のタイムゾーンを選択することもできます。

3. **タイム同期方法**として「**NTP タイム同期**」を選択してください。

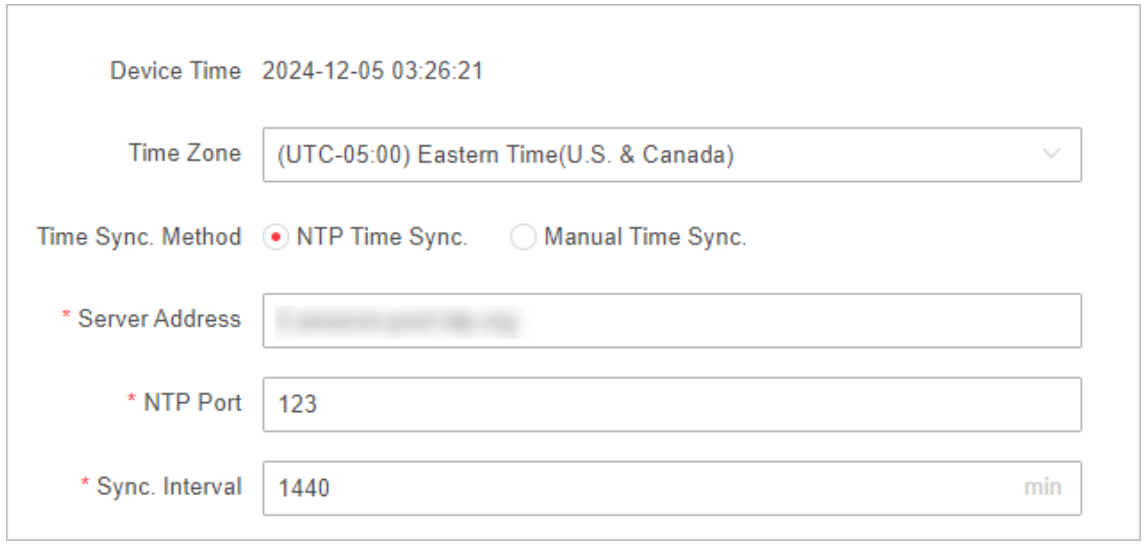

図3-6 NTP設定

4. NTP サーバー情報を入力してください。

- サーバーアドレス：NTP サーバーの IP アドレス。
- NTP ポート：NTP サーバーの監視ポート。デフォルト値：123。値の範囲：1 から 65535
- 同期間隔: デバイスがNTPサーバーと同期する頻度。値の範囲: 1分から10080分。

3.7 インテリジェント電源管理

インテリジェント電源管理機能が有効になっている場合、デバイスは解決不能なデバイス障害が発生した場合に自動的に電源をオフにします。

システム管理に移動し、→**デバイスメンテナンス**→**インテリジェント電源管理**を必要に応じて**有効にします**。

注 機能は一部のモデルでのみ利用可能です。実際のインターフェースが優先されます。

3.8 パスワードを変更

データセキュリティのため、パスワードを定期的に変更することを強くおすすめします。

手順

1. 画面の右上隅をクリックしてください。
2. 元のパスワード、新しいパスワードを入力し、確認します。
3. 「**保存**」をクリックします。ウェブページがログイン画面にリダイレクトされます。

第4章 FAQ

4.1 デバイスペアリングが失敗した理由は？

原因

デバイスのペアリング状態は、距離、方向、SSID名、およびPSKパスワードに依存します。

解決方法

以下の手順で確認してください：

1. 距離と方向を確認：APとCPEが互いに直接向かい合っていることを確認し、その間の距離が制限内にあることを確認してください。
2. SSID名とPSKパスワードを確認してください：SSID名とPSKパスワードが正しいことを確認してください。

4.2 デバイスが起動しない理由

原因

1. 無線ブリッジとPoEモジュールを接続するネットワークケーブルの長さが60mを超えています。
2. ネットワークケーブルがカテゴリー5eの規格を満たしていません。
3. ネットワークケーブルのジャックがしっかり接続されていないか、接続順序が間違っています。

解決方法

1. 60m未満のネットワークケーブルを使用してください。
2. カテゴリー5e以上の規格のネットワークケーブルを使用してください。
3. 登録ジャックを再接続してください。

4.3 信号強度が低すぎるのはなぜですか？

原因

1. CPEとAPの間に大きな障害物があります。
2. CPEがAPと直接向かい合っていない。

解決方法

1. 障害物を除去するか、迂回してください。
2. CPEとAPの角度を調整してください。

4.4 信号品質が高いにもかかわらずスループットが不十分な理由は？

原因

1. 過剰な干渉またはマルチパス干渉。
2. 有線デバイスの故障。

解決

1. 干渉を除去するか、デバイスの周波数を変更してください。

注意

周波数変更の方法:ワイヤレスブリッジのAPを再起動し、利用可能な信号チャンネルの自動検索を有効にします。

2. ネットワークケーブルを変更するか、別のPCを使用してください。

4.5 無線接続速度が比較的低いのはなぜですか？

原因

無線システムは最大通信速度で接続し、実際の通信速度は距離と環境によって異なります。

解決策

以下の手順で確認し、最高の接続速度を確保してください：

1. デバイスの位置: デバイスの位置と方向を調整してください。
2. 無線チャンネルまたは周波数: 干渉を軽減するため、別の信号チャンネルまたは周波数に変更してください。
3. 無線干渉: 干渉を引き起こすデバイスを調整、シールド、または無効化してください。

4.6 PCがデバイスのIPアドレスにpingを送信した際に、過剰なパケット損失とタイムラグが発生する理由はなぜですか？

原因

1. ネットワークケーブルのジャックがしっかり接続されていません。
2. 複数のデバイスのIPアドレスが衝突しています。

解決方法

同じスイッチに接続されているAPに対してポート隔離を実施してください。

1. 登録されたジャックを再接続してください。
2. 異なるデバイスのIPアドレスを変更してください。

See Far, Go Further