ワイヤレスルーター

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。
- この文書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、予告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使用してください。

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

- Hikvisionは、本文書に記載された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。
- 本文書の一切のコンテンツ（テキスト、画像、グラフィックなど）は、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。

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、本文書および本文書で説明される製品（ハードウェア、ソフトウェア、およびファームウェアを含む）は、「現状有姿」かつ「一切の欠陥およびエラーを含む」状態で提供されます。HIKVISION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、HIKVISIONは、特別損害、間接損害、付随的損害、または派生損害（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）、製品責任、またはその他の理由に基づくものであっても、一切の責任を負いません。システムの破損、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基づくものであっても、製品の使用に関連して生じた場合、HIKVISIONは一切の責任を負いません。これは、HIKVISION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も同様です。
- 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、HIKVISIONは異常な動作、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します。

- あなたは、この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、あなた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、あなたのみに帰属します。特に、あなたは、第三者の権利（publicity rights、知的財産権、データ保護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。

適用モデル

このマニュアルは無線ルーターに適用されます。

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
Note	本文の重要なポイントに関する追加情報を 強調 ま 補足 提供します。 た は
Caution	潜在的な危険な状況を指示し、回避されない場合、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ります。
Danger	高いリスクレベルの危険を示し、回避されない場合、死亡または重大なけがを引き起こします。

目次

第1章 初回使用

ルーター（以下、デバイスと呼びます）を初めて使用する前に、アクティベーションが必要です。アクティベーション後、ルーターはWeb経由で設定可能です。

1.1アクティベーション

デバイスはモバイルデバイスまたはPCから起動できます。起動前に、デバイスがネットワークと電源に接続されていることを確認してください。

Step 1スマートフォンまたはPCを無線ルーターに接続してください。

- ワイヤレスモード：デバイスのLANポートのいずれかを、PCのネットワークポートにイーサネットケーブルで直接接続してください。
- 有線モード：ルーターのラベルを確認し、Wi-Fi名（HIKVISION_XXXX）を取得し、スマートフォンまたはPCをWi-Fiに接続してください。

Step 2ブラウザのアドレスバーにIPアドレス（https://192.168.9.1）またはログインアドレス（https://hikrouter.net）を入力し、起動ページに移動してください。

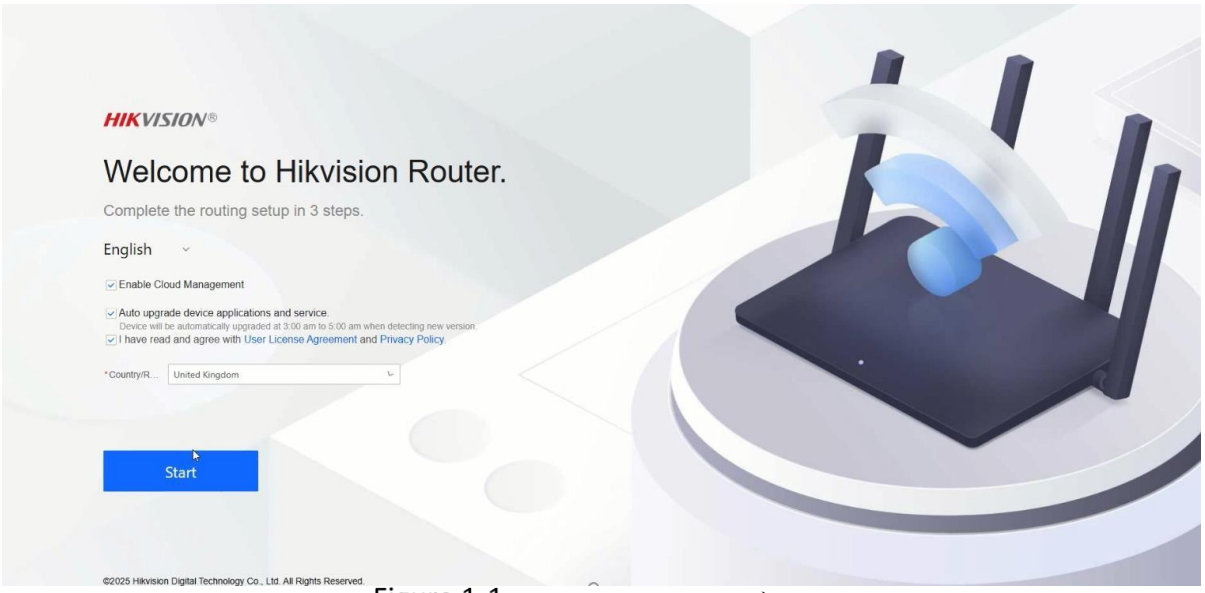

Figure 1-1アクティベーションページ

Step 3**国/地域**を選択し、**[開始]**をクリックします。

1.2セットアップウィザード

1.2.1 Create New Wi-Fi

Step 1**動作モード**を「**ルーターモード**」に選択します。

Figure 1-2操作モードを選択してください

Step 2システムは**インターネット接続モード**を自動的に検出します。または、手動で選択することもできます。

Figure 1-3インターネット接続モード

- **DHCP**: このモードを選択することをおすすめします。動的IPアドレスが自動的に割り当てられます。追加の設定は不要です。
- **PPPoE**: インターネットサービスプロバイダー（ISP）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、または古いルーターを新しいルーターに置き換える場合、このモードを選択できます。
- **静的IPアドレス**: ISPから静的IPアドレスとその他の情報が提供されていない限り、このモードを選択することはおすすめしません。

Step 3（オプション）古いルーターを新しいルーターに交換する：古いルーターがインターネットに正常に接続できる場合、新しいルーターと古いルーターを接続することで、PPPoEモードでデータを移行できます。

1) **PPPoE**モードを選択します。
2) **「自動取得」**をクリックします。

3) 新しいルーターと古いルーターを電源ケーブルに接続します。

4) 古いルーターのWANポートを、新しいルーターの任意のLANポートにイーサネットケーブルで接続します。

5) 「**取得**」をクリックして、古いルーターからブロードバンドアカウントとパスワードを取得します。

Step 4 （オプション）**VPNのクイック有効化**または**VLANの有効化**をサポートします。詳細情報は*4.3.8 VPN*および*4.3.9 VLANを参照してください*。

Note

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。

Step 5 「**次へ**」をクリックしてルート設定を構成します。

Figure 1-4Wi-Fi 設定

- **Wi-Fi 名称**: デフォルトでラベルに表示される名前です。編集が可能です。
- **Wi-Fi パスワード**: ルーターの Wi-Fi に接続する端末が入力するパスワードです。8 文字から 16 文字のカスタムパスワードがサポートされています。
- **管理者パスワード**: ルーターの設定を行うためのWeb管理ページにログインする際に入力するパスワードです。8～16文字のカスタムパスワードがサポートされています。
- **国/地域**: あなたの所在地を選択してください。

Step 6**次へ**をクリックしてください。ルーターはアクティベーション後、自動的に再起動します。

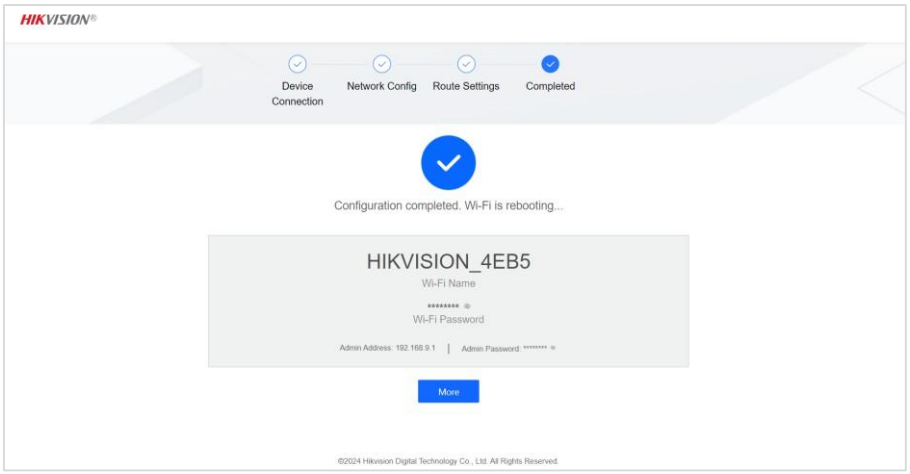

Figure 1-5図1-6 設定完了

Note

パスワードページを保存することをおすすめします。

1.2.2 Extend Wi-Fi Range

メッシュネットワークは、**サブルーターを**迅速にアクティベートし、**メインルーター**のWi-Fi範囲を拡張できます。

開始前に

- 両方のルーターがメッシュに対応しており、機能が有効になっていることを確認してください。
- デバイスがメッシュに対応していない場合、**ワイヤレスエクステンダーモード**でWi-Fiを拡張できます。**アクセスポイントモード**（***4.2.1 基本設定***を参照）。
- **メイン ルーターが**インターネットに正常に接続できることを確認してください。
- **サブルーターが**非アクティブ状態であることを確認してください（アクティブになっている場合は、WPSボタンを8秒間長押しして復元してください）。

手順

Step 1**サブルーターを**電源オンにし、**メインルーターの**近くに配置します**。サブルーターの**インジケーターが赤色で点灯しています。

Step 2**メイン**ルーターと**サブルーター**の両方のWPSボタンを1～3秒間押します。**サブルーターの**インジケーターが青色に点灯するまで待ちます。

Step 3**サブルーターの**電源を抜き、Wi-Fiのカバー範囲を拡大したい場所に設置します。

Step 4**サブルーターを**電源に再接続します。**サブルーターの**インジケーターが再び青色に点灯するまで待ちます。

Note

- メイン**ルーターとサブルーターの**Wi-Fi名前とパスワードは同じです。
- ステップ2が失敗した場合、**メインルーターの**LANポートと**サブルーターの**WANポートをイーサネットケーブルで接続し、**サブルーターの**インジケーターが青色に点灯するまで次の手順を繰り返してください。
- WPSボタンはモデルによって異なります。クイックスタートガイドをご参照ください。

1.3ログイン

デバイスがアクティベートされると、Wi-Fiパスワードが更新され、ログインするには再接続が必要です。Step 1アクティベート時に設定したWi-Fiパスワードを使用して、デバイスに再接続してください。

Note

アクティベーション中にWi-Fi名が変更された場合は、再度Wi-Fiネットワークを選択してください。

Step 2アクティベーションページを再読み込みするか、アドレスバーに管理用IPアドレス（192.168.9.1）を入力し、ログインページに移動してください。

Step 3ルーターの管理者パスワードを入力し、**[ログイン]**をクリックしてください。

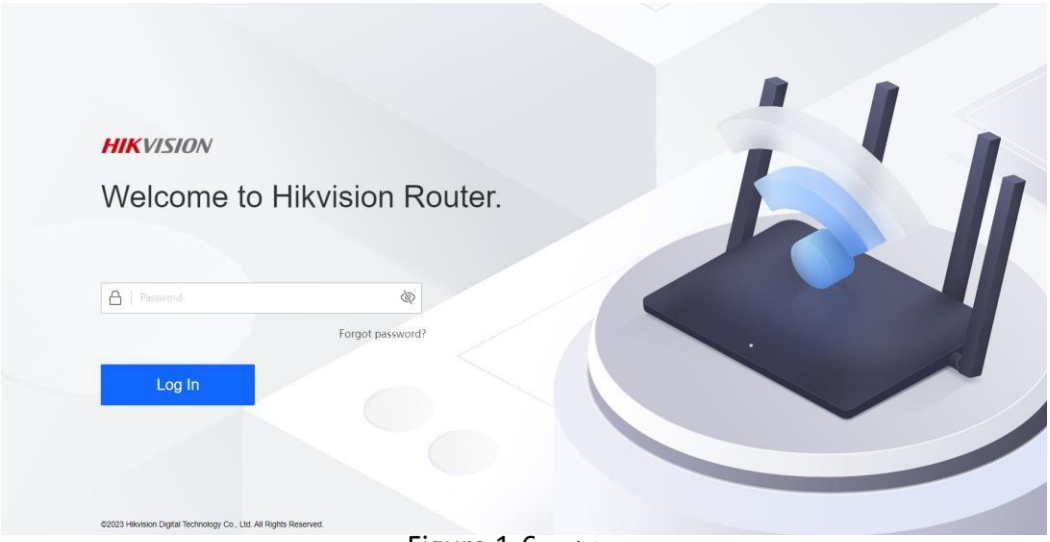

Figure 1-6ログイン

第2章 概要

デバイスにログイン後、概要ページに移動してネットワーク接続状態、端末の数、Wi-Fi 情報を確認できます。

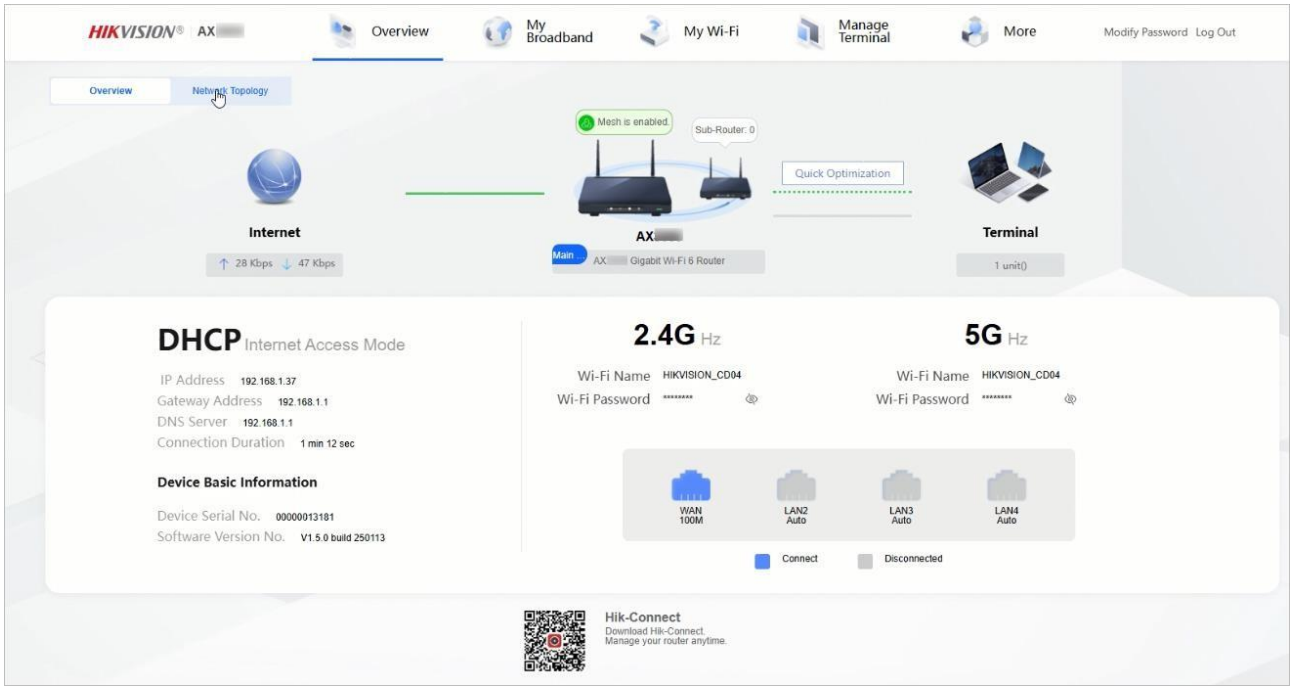

Figure 2-1 概要

2.1.2 Network Topology

ネットワークトポロジーをクリックして、ネットワーク情報を確認できます。

トポロジー内のルーターの名前変更、再起動、復元、管理を迅速に行えます。

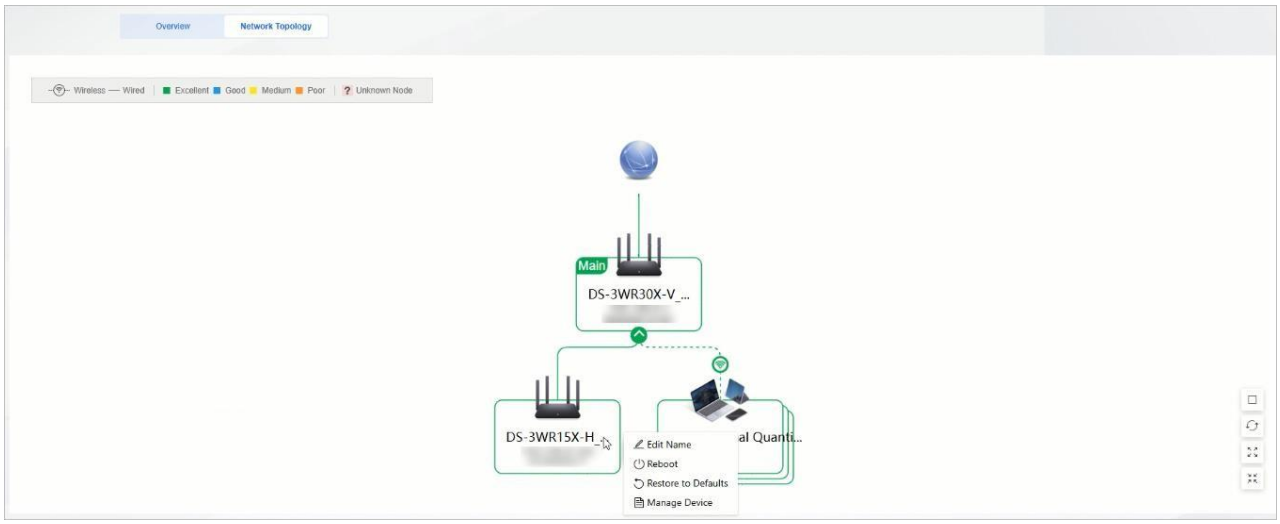

Figure 2-2ネットワークトポロジーを確認する

2.1.3 Quick Diagnosis

デバイスがネットワークに正常に接続されていない場合、**クイック診断**を使用して問題を診断できます。以下の診断結果に応じて適切な対応を実施してください。

- イーサネットケーブルが接続されていません：イーサネットケーブルがルーターのWANポートに接続されているかご確認ください。
- ネットワーク接続が切断されています：ブロードバンド設定が正しいか、アップリンクWi-Fiがネットワークに接続されているか、およびアップリンクルートブリッジがネットワークに接続されているかを確認してください。
- リレー失敗：リレーWi-Fiのパスワードを確認してください。
- ダイヤルアップ接続が切断されています：ルーターの物理的な接続が正常かどうかを確認してください。
- ユーザー名またはパスワードが正しくない: ブロードバンドの設定またはパスワードが正しいか確認してください。
- ダイヤルタイムアウト: ブロードバンドダイヤルアップサーバーが正常に動作しているか確認してください。
- IPアドレスの衝突：WANポートで取得したIPアドレスがLANポートと同じネットワークセグメントにあります。LAN設定でLANポートのIPアドレスを編集してください。

2.1.4 Quick Optimization

「詳細設定」→「→ Wi-Fi設定」→「→ クイック最適化」に移動してください。

システムは現在の作業チャネルの外部Wi-Fi干渉とリンク混雑を分析します。健康指数が100未満の場合、**クイック最適化**を通じて現在のネットワークを最適な状態に最適化できます。

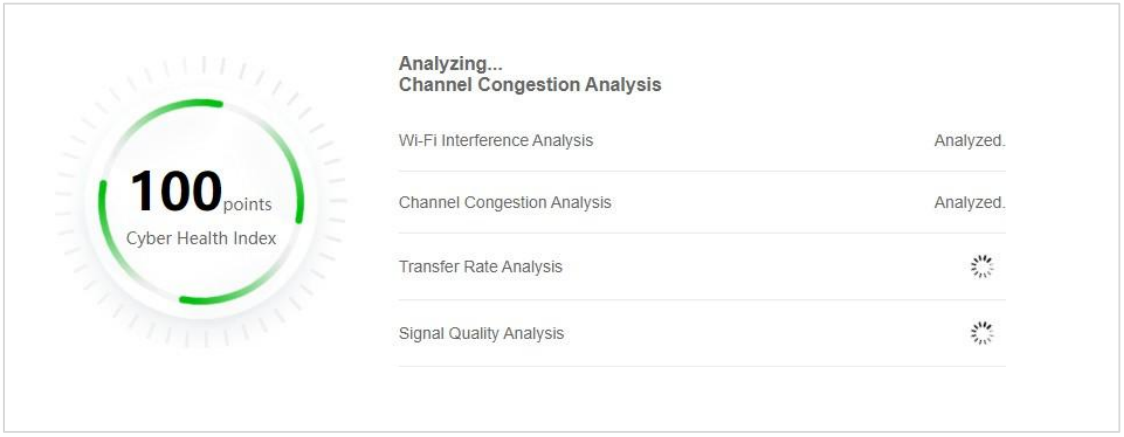

Figure 2-3クイック最適化

2.1.5 Check Port Status

概要ページの右側でポートの状態を確認してください。

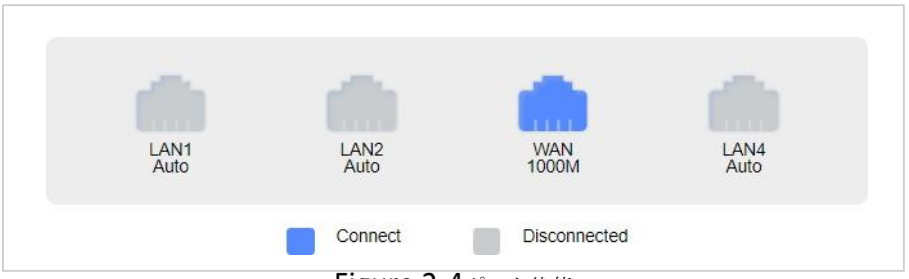

Figure 2-4ポート状態

2.1.6 Download Hik-Connect

インターフェースのボトルに表示されているQRコードをスキャンして、ルーターデバイスを管理するためのHik-Connectアプリケーションをダウンロードしてください。

第3章 端末管理

保護者は、ルーターのWi-Fiに接続された端末をリストに追加できます。これにより、家族メンバー（特に未成年者）が適切なオンライン習慣を身につけることができます。

3.1端末情報の確認

ホーム画面の**「端末」**をクリックして、オンライン、オフライン、無効化された端末を確認・管理できます。

Figure 3-1端末リスト

3.2インターネット接続を制限する

現在の端末のインターネットアクセスを制限するには、[⊖] をクリックします。

オプション: 端末のネットワーク接続制限を解除するには、**[オフライン & 禁止]** をチェックし、[OK] をクリックします。

⊖ をクリックします。

3.3ターミナルのネットワーク制限

クリックし 現在のターミナルの詳細を表示し、ターミナルの接続状態を設定します。

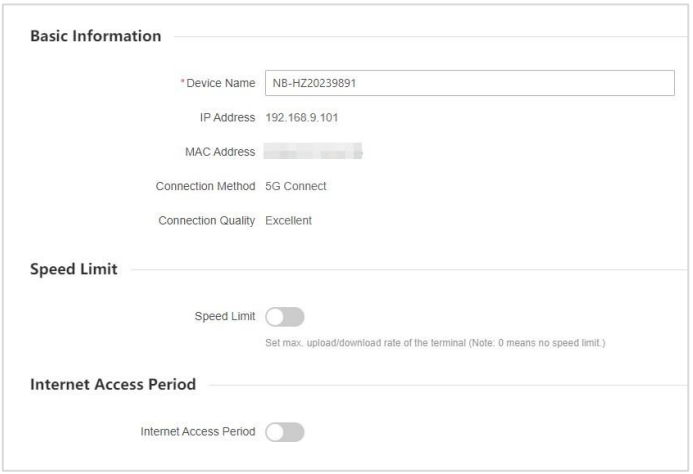

Figure 3-2端末の詳細

- **速度制限**：現在のターミナルのネットワーク速度を制限できます。

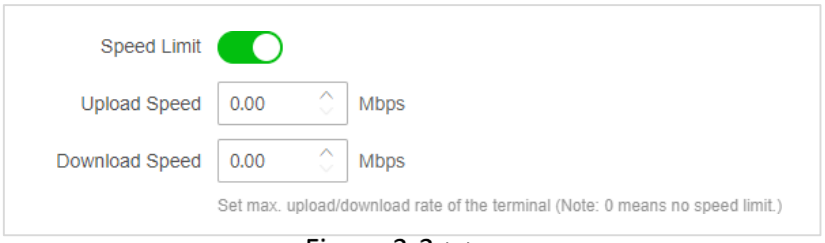

Figure 3-3速度制限

- **インターネット接続期間**: 現在の端末がネットワークに接続できる時間範囲です。設定された時間範囲外では、端末はWi-Fiに接続できますが、ネットワークには接続できません。最大3件まで設定可能です。

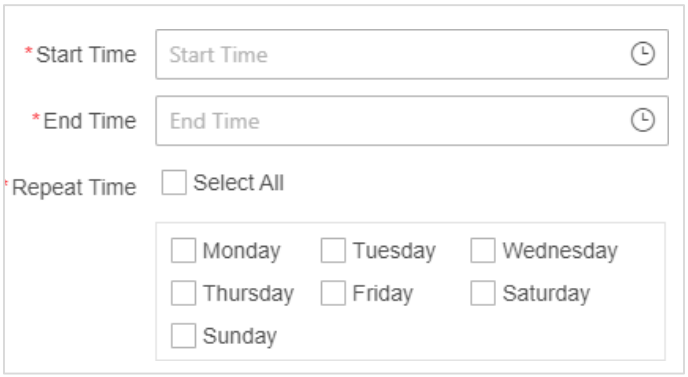

Figure 3-4インターネット接続期間を設定

- **URLフィルター**: 現在の端末からアクセスを禁止するドメイン名を設定します。最大16件まで設定可能です。

Figure 3-5URLを追加

第4章 インターネット設定

4.1Wi-Fi設定

Wi-Fiのパラメーターと機能（タイマー切り替え、クイック最適化、ゲストネットワークなど）を設定します。

4.1.1 Basic Settings

Step 1 **「マイWi-Fi」**をクリックします。

Step 2 Wi-Fiが有効になっていることを確認します。

Step 3 パラメーターを設定します。

Table 4-1基本パラメーター説明

パラメーター	**説明**
Wi-Fiを有効にする	Wi-Fi ネットワークを有効または無効にします。
デュアル周波数対応を有効にする	• 有効: 2.4 GHzまたは5 GHzのネットワークは、信号強度と距離に応じて自動的に推奨されます。 • 無効: 2.4 GHz と 5 GHz ネットワークは個別に設定可能です。
ネットワークを有効にする	**デュアル周波数（1つ）**が無効の場合、 2.4 GHzと5 GHzのネットワークを個別に有効にできます。
Wi-Fi 名	他の端末が検索するデバイスのWi-Fi名を設定します。
Wi-Fi 名を非表示にする	選択すると、このWi-Fiは端末から検索できなくなります。接続するにはWi-Fi名を手動で入力する必要があります。この機能はネットワークのセキュリティを強化します。
暗号化モード	**ハイブリッド ストロング**、**ハイブリッド**、**ストロング**、および **なし**（すべての接続を許可）に対応しています。 **Note** **ハイブリッドモード**を使用する際は、アクセスターミナルが対応していることを確認してください **Strongを使用している**ことを確認してください。接続問題が継続する場合、**ハイブリッド**または他の方法に切り替えてください。
Wi-Fi パスワード	8文字から63文字までが許可されています。数字、大文字、小文字、または特殊文字を含めることができます。
管理パスワードと同期	**Wi-Fiパスワードを管理者パスワード**に設定してください。

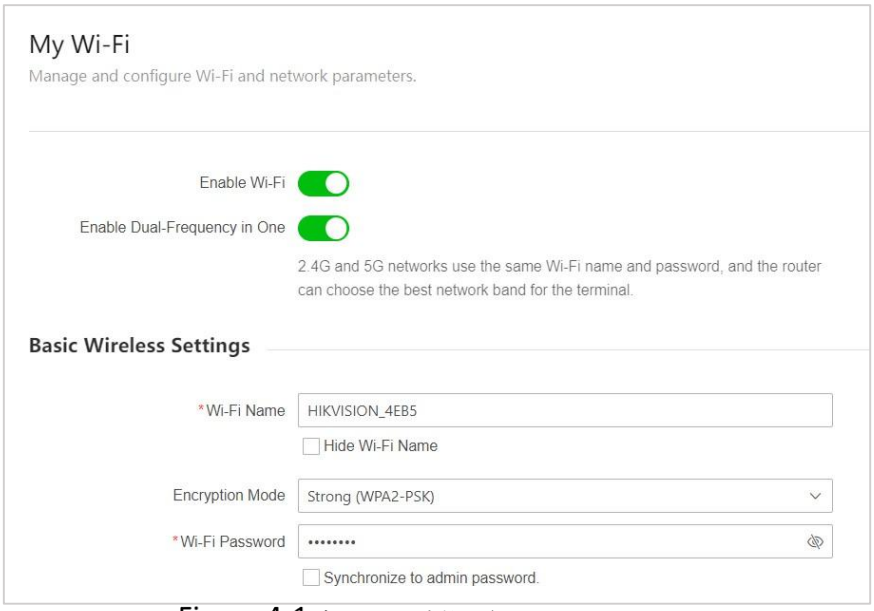

Figure 4-1デュアル周波数を有効にする

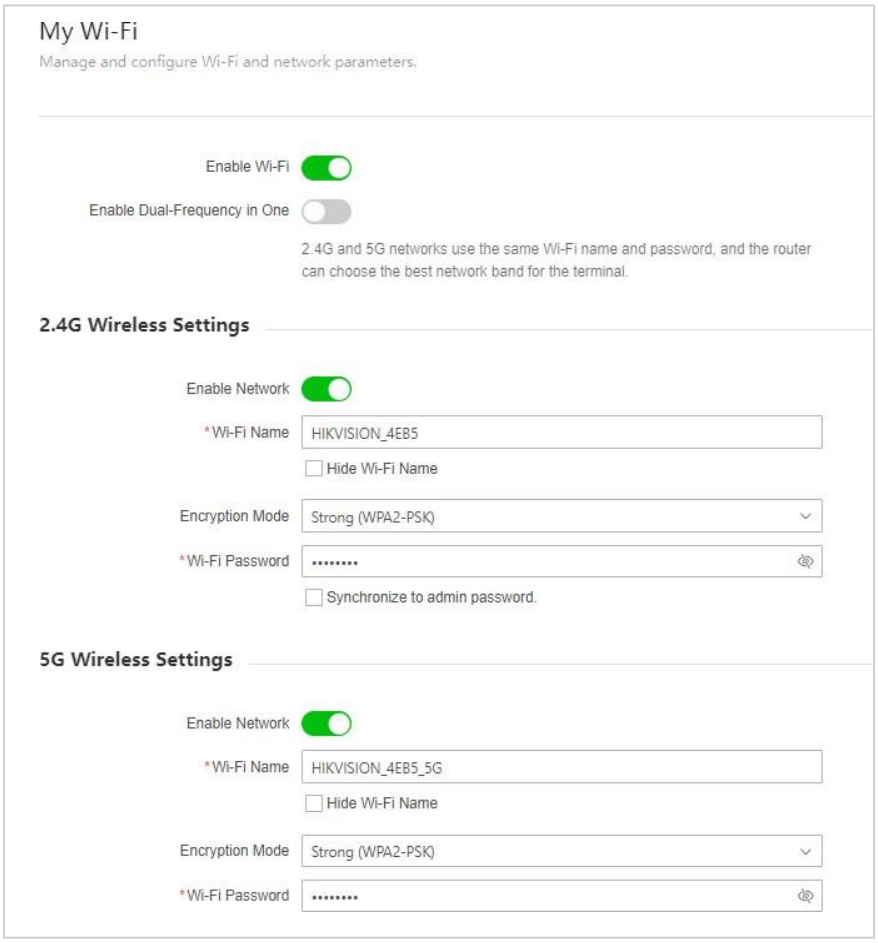

Figure 4-2デュアル周波数を1つに無効化

Step 4**保存**をクリック。

4.1.2 Advanced Settings

Step 1「**詳細**」→「→」→「**Wi-Fi設定**」→「→」→「**Advanced Wi-Fi Settings**」に移動します。

Note

機能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。

Step 2パラメーターを設定します。

Table 4-2詳細パラメーター説明

パラメーター		**説明**
2.4/5 G 無線設定	無線チャンネル	無線信号は、データ伝送の伝送媒体として使用されます。**自動**を選択した場合、ルーターは周囲の環境に応じて最適なチャンネルを選択します。
	無線モード	無線の動作モードを設定します。デフォルトの設定が推奨されます。
	チャネル幅	無線データ伝送に割り当てるチャネル幅を設定します。
無線詳細設定	TWT	**TWT**を有効にすると、デバイス間のリソーススケジューリングが自動的に最適化され、ランダムな競合を軽減し、デバイスのスリープ時間を延長し、電力消費を削減します。
	MU-MIMO	**MU-MIMO**を有効にすると、複数の端末と通信可能になり、オンライン体験を向上させます。
	OFDMA	**OFDMA**を有効にすると、マルチユーザー環境での伝送効率を向上させ、ネットワーク遅延を削減するために、マルチユーザー再利用チャネルリソースが利用されます。
Wi-Fi 信号強度		強化された無線信号は、広範囲や仕切り壁のカバーに適しています。

Step 3**保存**をクリックしてください。

4.1.3 Scheduled Wi-Fi On/Off

Wi-Fiを自動的に無効にする期間を設定します。Step 1 **[詳細]→ [Wi-Fi設定]→ [スケジュールされたWi-Fiのオン/オフ]**。

Step 2**「有効」**にチェック**を入れます。**

Step 3**開始**時間と**終了時間**を選択します。

Step 4**繰り返し時間**（月曜日から日曜日）を選択します。

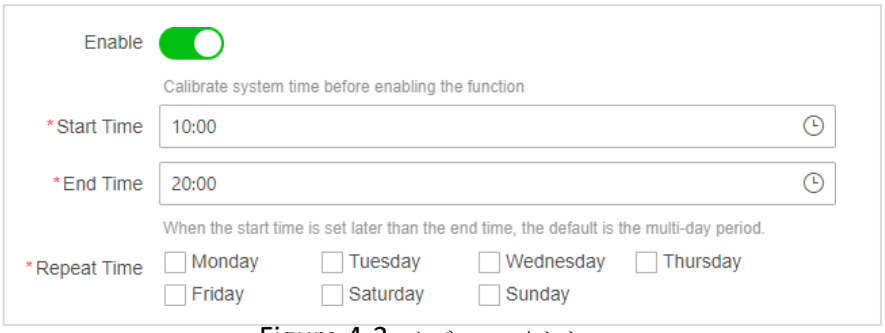

Figure 4-3スケジュールされたWi-Fi

Step 5**保存**をクリックします。

Note

この機能を有効にする前に、ルーターのシステム時間が正しいか確認してください。

4.1.4 Guest Network

ゲスト用のWi-Fiネットワークを設定し、ホストネットワークのデータと情報のセキュリティを保証し、ゲストのネットワーク要件を満たします。

Step 1**「詳細」→「→」→「Wi-Fi設定」→「→ ゲストネットワーク」**を選択します。「Step 2」の**「有効」にチェックを入れます。**

Step 3以下のパラメーターを設定します。

- **ゲストネットワーク名**：ホストネットワーク名と異なるWi-Fi名を設定します。
- **ゲストネットワークパスワード**：ゲストネットワークに接続するためのパスワードを設定します。
- 有効期間：無制限、4時間、8時間、または24時間から選択できます。
- **ゲスト共有ネットワークの速度**：お好みでカスタマイズ可能です。Step 4 **「保存」**をクリックします。

Note

- **ゲストネットワークのパスワード**を設定しない場合、**ゲストネットワーク**はパスワードなしで利用可能です。
- 有効化する前に、ルーターが接続されていることを確認してください。接続されていない場合、機能は有効になりません。

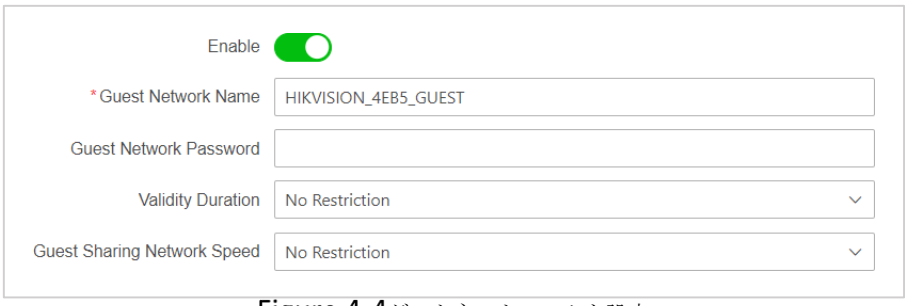

Figure 4-4ゲストネットワークを設定

4.2ブロードバンド設定

4.2.1 Basic Settings

「マイブロードバンド」にアクセスし、→ **の基本設定**でルーターの動作モードを設定します。

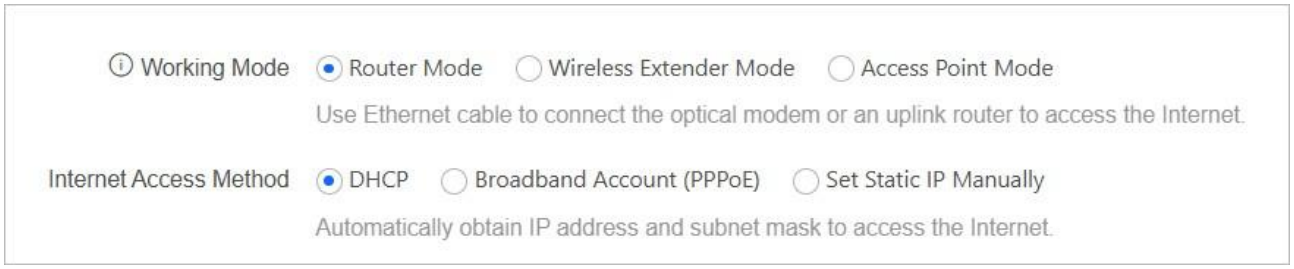

Figure 4-5 動作モード

ルーターモード

ルーターは新しいWi-Fiネットワークを作成するか、古いルーターを置き換えます。このモードでは、ルーターのWANポートはイーサネットケーブル経由でモデムまたはアップリンクルーターに接続できます。

Step 1「**My Broadband**」にアクセスし、→ **の基本設定**を開き、動作モードを「**ルーターモード**」に設定します。Step 2 **インターネット接続方法**を選択します。

Table 4-3インターネット接続方法の説明

方法	説明
DHCP	ルーターが自動的にIPアドレス、サブネットマスク、ゲートウェイ、DNSなどの情報を取得します。設定は不要です。 **Note** 静的DNSが有効になっている場合、優先DNS情報を入力する必要があります。デフォルトでは無効です。
ブロードバンドアカウント（PPPoE）	ブロードバンドアカウント（通信事業者、モバイル、ネットワーク接続）経由でダイヤルアップ接続してください。 **Note** • 古いルーターでネットワークに正常に接続できる場合、PPPoEモードでデータを移行できます。 古いルーターに接続することで、PPPoEモードでデータを移行できます。 • 静的DNSが有効になっている場合、優先DNS情報を入力する必要があります。デフォルトでは無効になっています。
静的IPを手動で設定	ISPからIPアドレスやその他の情報が提供されていない場合を除き、推奨されません。

Step 3**保存**をクリックします。

ワイヤレスエクステンダーモード

ルーターは、アップリンク ルーターに Wi-Fi 経由でワイヤレス接続され、アップリンク ルーターの Wi-Fi 範囲を拡張します。

Note

- アップリンクルーティング用にDHCPサーバーが有効になっていることを確認してください。
- ルーターのWANポートがイーサネットケーブルで他のデバイスに接続されていないことを確認してください。
- このモードでは、端末管理やLAN設定などの機能が非表示になります。Wi-Fiの設定はできません。

Step 1「**My Broadband**」にアクセスし、→ **の基本設定**に移動し、動作モードを「**Wireless Extender Mode**」に設定してください。

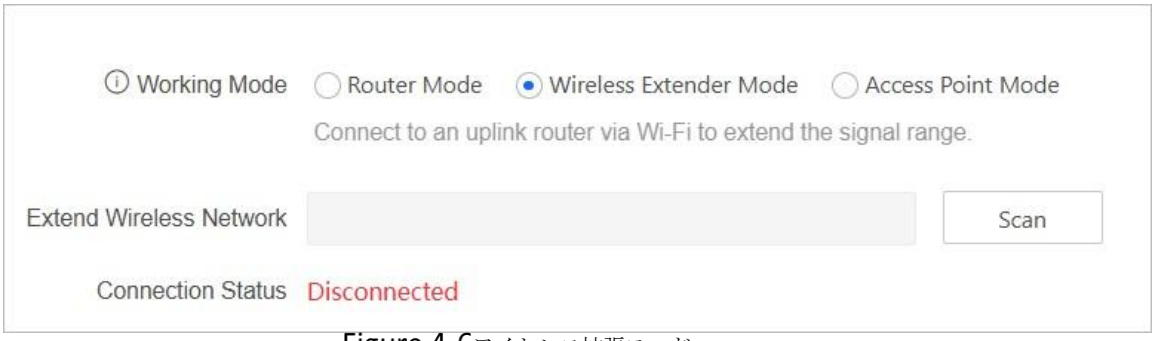

Figure 4-6ワイヤレス拡張モード

Step 2「スキャン」をクリックして、信号範囲を拡張するネットワークを選択し、Wi-Fiパスワードを入力してください。

Step 3 （ オプション） 「手動で追加」をクリックして、ネットワーク名とパスワードを入力し、信号範囲を拡張します。

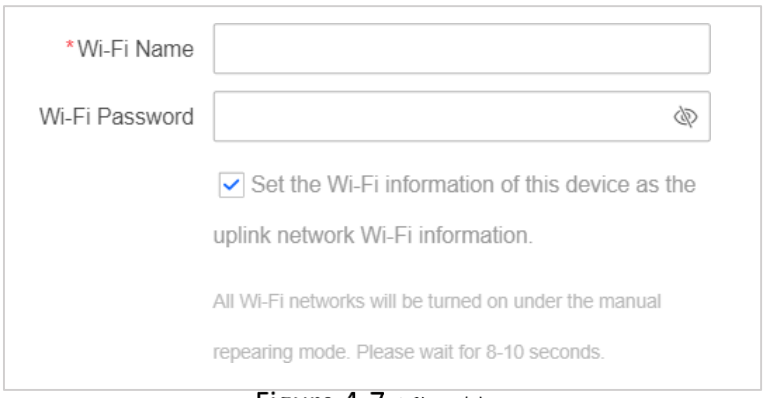

Figure 4-7手動で追加

Step 4「保存」をクリックします。Step 5「OK」をクリックします。 **アクセスポイントモード**

ユーザーは有線接続でアップリンク ルーターに接続し、ネットワーク インターフェースを拡張できます。ターミナル管理、LAN 設定などは非表示になります。

Note

- アップリンク ルーターのネットワーク モードが DHCP モードでないことを確認してください。
- ルーターをブリッジモードまたは汎用リレーモードに切り替えると、有効なビジターネットワークが無効になります。
- ブリッジモードからルートモードに切り替えた後、接続されたデバイスはルーターに再接続する必要があります。そうしないと、ネットワーク接続が切断される可能性があります。

Step 1「My Broadband」にアクセスし、→ **の基本設定**を開き、動作モードを「**ブリッジモード**」に設定します。Step 2 ルーターのWANポートとアップリンクルーターのLANポートを接続します。

Step 3「保存」をクリックします。

4.2.2 Advanced Settings

「**My Broadband**」にアクセスし、→ **の「詳細設定」**を選択します。デフォルト設定を維持することをおすすめします。

- データパッケージMTU：最大伝送単位（MTU）を設定します。PPPoEモードではデフォルト値は1480、DHCPおよび**手動で静的IPを設定**するモードでは1500です。
- MACアドレスのクローン作成: ブロードバンドの制限を解除し、ルーターがネットワークを共有できるようにします。デフォルトのMACアドレスを選択するか、管理用PCのMACアドレスをWANポートにクローン作成するか、またはMACアドレスを手動で設定できます。

Figure 4-8詳細設定

4.3ネットワーク設定

「→ ネットワーク設定」を選択して、ルーターのネットワークパラメーターを設定します。

4.3.1 LAN Settings

LANポートのIP設定は自動または手動を選択でき、どちらの場合もLAN-WAN衝突検出メカニズムが搭載されており、WANポートが取得したIPアドレスがLANポートのIPアドレスと同じネットワークセグメントにあるかどうかを検出します。通常は自動モードです。

「詳細設定」→「→ ネットワーク設定」→「→ LAN設定」に移動します。

- **自動**：衝突が検出されると、LAN ポートの IP アドレスが自動的に他のネットワーク セグメントに変更されます。
- **マニュアル**: 衝突が検出された後、LAN ポートの IP アドレスを手動で編集できます。

LANのIPアドレスを編集すると、ルーターに接続されているデバイスが再割り当てされます。

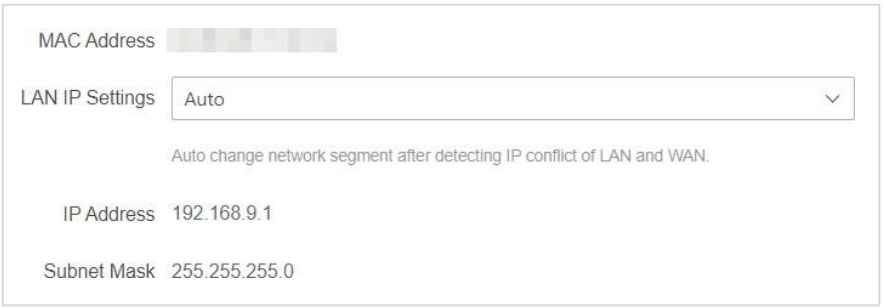

Figure 4-9LAN設定

4.3.2 DHCP Server Settings

DHCPサーバーは、必要に応じて有効または無効に設定できます。有効にすると、ルーターはLAN内のネットワークデバイスにIPアドレス、サブネットマスク、DNSなどのネットワークパラメーターを自動的に割り当てます。

「詳細」→「→」→「ネットワーク設定」→「→」→「DHCPサーバー設定」に移動します。

Table 4-4パラメーター説明

パラメーター	**説明**
アドレスプール開始/終了IPアドレス	DHCP サーバーが自動的に割り当てる IP アドレスの開始/終了アドレスです。 **Note** DHCPアドレスプール内のIPアドレスは、LANポートのIPアドレスと同じネットワークセグメントに属する必要があります。
アドレスリース期間	IPアドレスの自動割り当ての有効期間です。この期間が経過すると、デバイスは再度IPアドレスを取得する必要があります。
ゲートウェイ	ルーターのLANポートのIPアドレスは編集できません。
優先/代替DNSサーバー	ドメイン名をサーバーアドレスに解決するサーバー。

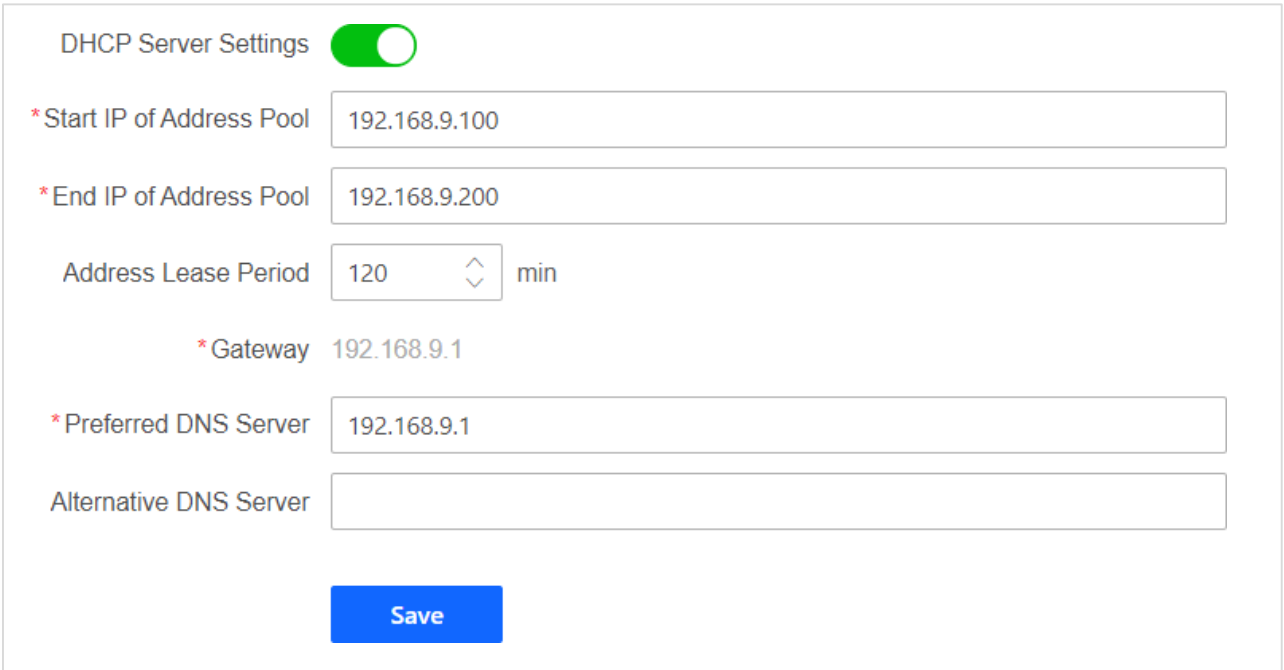

Figure 4-10DHCPサーバー

4.3.3 DHCP Client List

「詳細」→「→」→「ネットワーク設定」→「→」→「DHCPクライアント一覧」に移動します。DHCPサーバー経由でIPアドレスを取得する端末のリストを確認します。

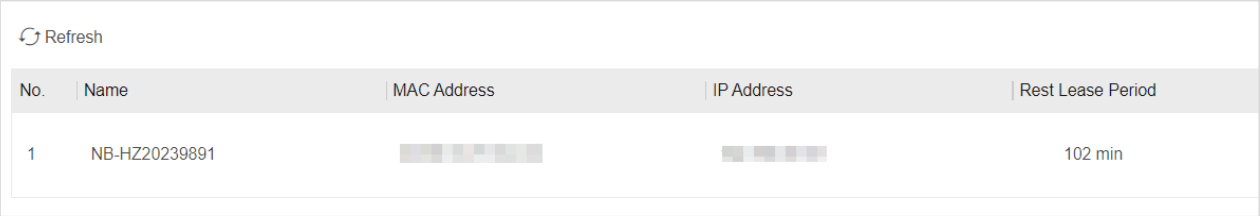

Figure 4-11DHCPクライアント一覧

4.3.4 Bind IP and MAC

IPアドレスを端末のMACアドレスにバインドし、端末デバイスに固定IPアドレスを割り当てます。これにより、ユーザーの有効なIPアドレスが不正に使用されたり悪用されたりするのを防ぎ、ARP攻撃からも保護されます。

「詳細」→「→」→「ネットワーク設定」→「→」→「IPとMACをバインド」を選択します。

- 「 」 をクリックして、バインドされた端末を編集します。

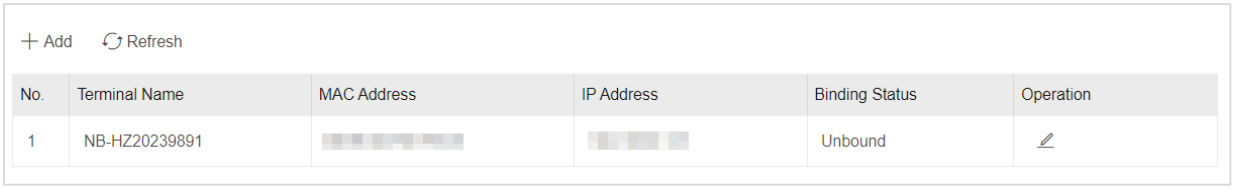

Figure 4-12端末バインディング一覧

- Add をクリックして新しい端末をバインドします。

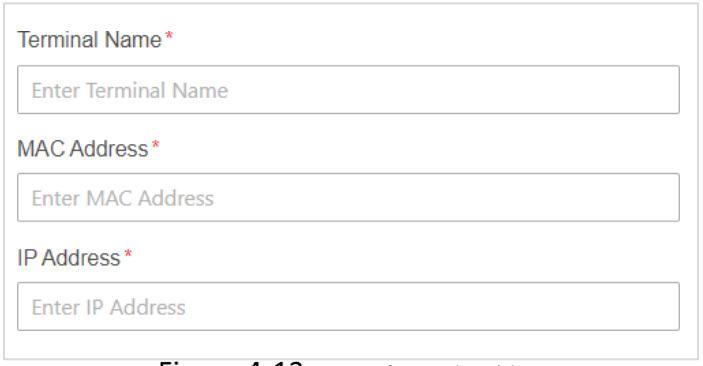

Figure 4-13バインディングの追加

4.3.5 IPv6

「詳細」→「→」→「ネットワーク設定」→「→」→「IPv6」を選択します。WAN接続モードとLANアドレス配布モードを設定できます。

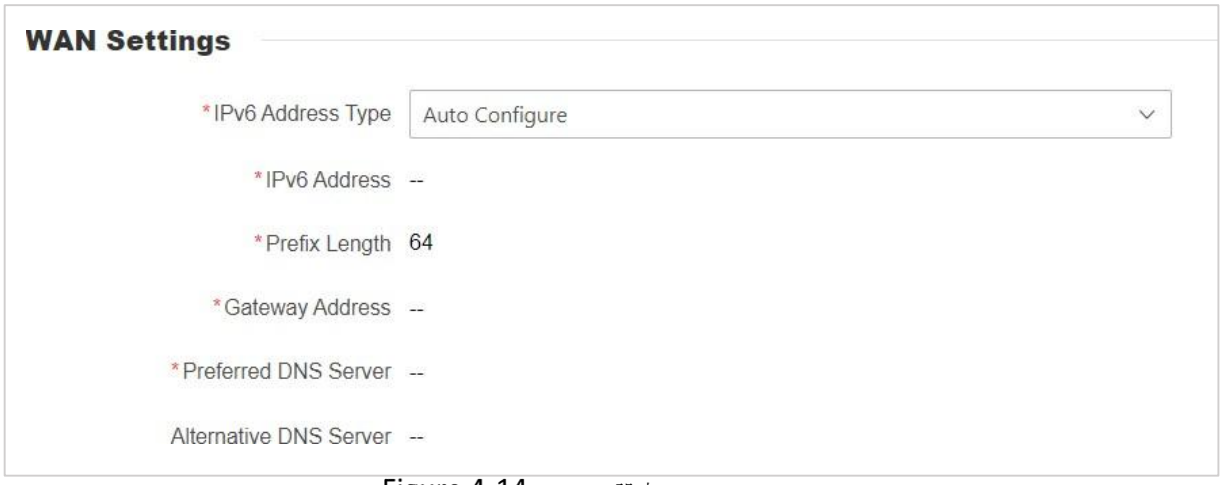

Figure 4-14IPv6-WAN設定

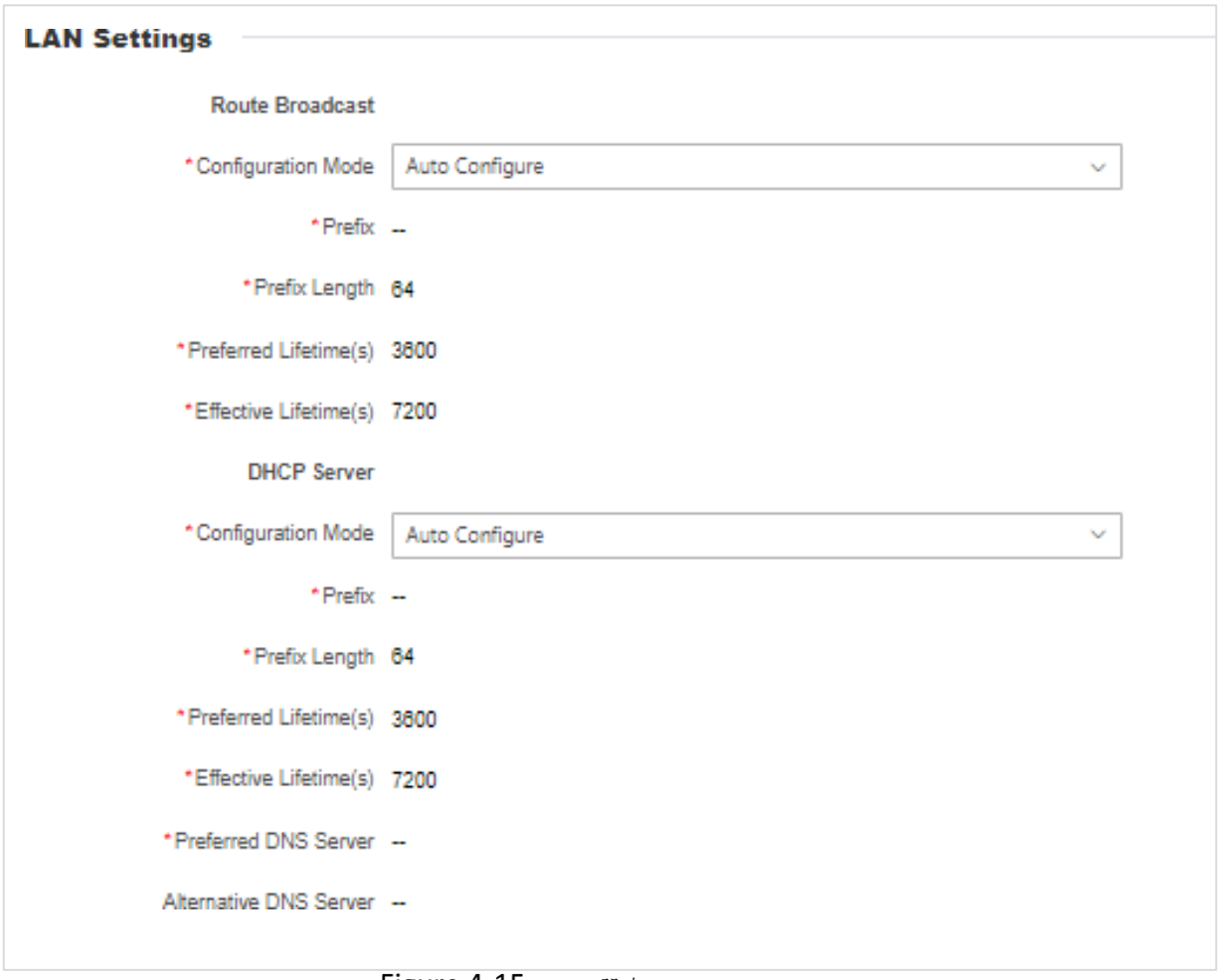

Figure 4-15IPv6-LAN設定

4.3.6 DDNS

DDNSは、ドメイン名とIPアドレスの対応関係を動的に更新する機能を備えたDNS（ドメインネームシステム）の拡張版です。これにより、ユーザーは固定されたドメイン名を通じて動的に変更されるパブリックIPアドレスにアクセスできます。

「詳細」→「→」→「ネットワーク設定」→「→」→「DDNS」へ移動してください。

サーバーパートナーはORAYのみ対応しています。ユーザー名とパスワードを設定してください。

Figure 4-16 DDNSを設定

4.3.7 UPnP

UPNP（UniversalPlugandPlay、汎用プラグアンドプレイ）を有効にすると、内部ネットワークのホストはUPNPプロトコルを通じてルーターにポートを自動的にマッピングするよう要求できます。UPNPプロトコルをサポートするP2Pソフトウェアを使用する場合、ダウンロード速度を向上させて
ネットワークの安定性が向上します。

「詳細」→「→」→「ネットワーク設定」→「→」→「UPnP」を選択してください。

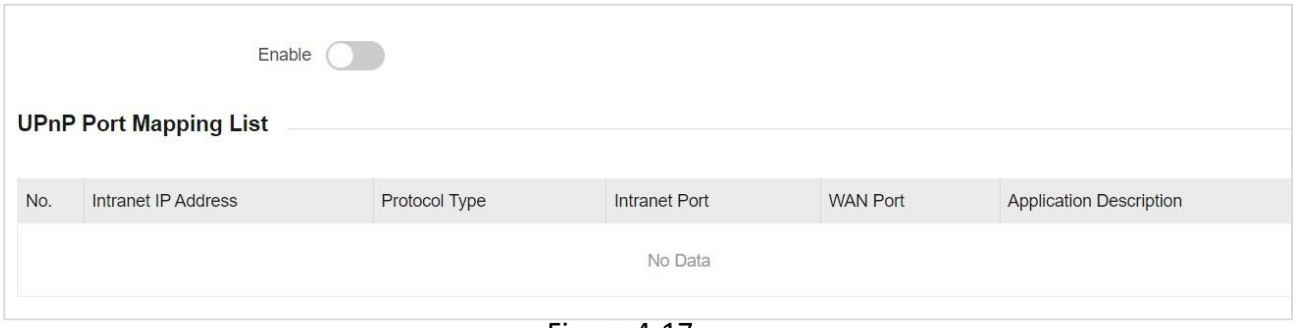

Figure 4-17UPnP

4.3.8 VPN

VPNサーバーに接続すると、インターネット経由でVPNサーバーの内部ネットワークリソースに簡単かつ安全にアクセスできます。

Step 1 **「設定」→「→」→「ネットワーク設定」→「→ VPN」**を選択します。

Step 2 **「追加」**をクリックし、必要な情報を入力してVPNを追加します。

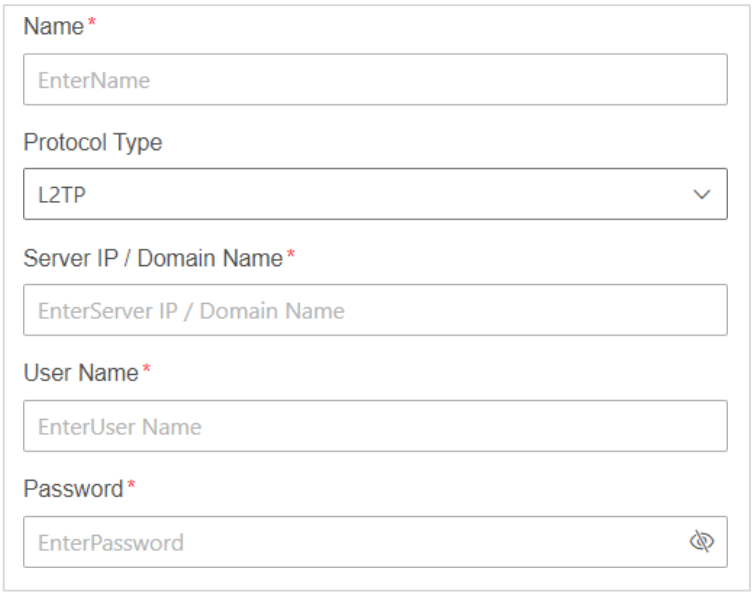

Figure 4-18VPNを追加

Note

プロトコルタイプとしてL2TPまたはPPTPを選択できます。

Step 3 **「保存」**をクリックします。

Step 4(オプション) **インテリジェント VPN による転送は**、選択したサーバーまたはデバイスのデータ転送を VPN チャネルに切り替えます。

- **サーバーアドレスによる転送**：ルーターは、指定されたサービスアドレスを宛先アドレスとして、VPNリンク経由でデータを送信します。
- **デバイスによるシャント**: ルーターは、指定されたMACアドレスを持つデバイスまたは選択されたオンラインデバイスからデータをVPNリンク経由で送信します。

Note

- 名前は1～128バイトまで指定可能です。
- 同時に少なくとも8つのルールをサポートします。
- フロー規則は独立して有効になります。

4.3.9 VLAN

ISPが提供するアップリンクネットワーク環境では、アドレス割り当て時に固定のVLANが設定されます。そのため、ルーターはWAN側で対応するVLANをサポートする必要があります。同時に、LAN側ではビジネス用にIPアドレスを取得するため、対応するVLAN IDを指定する必要があります。

Note

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。Step 1 **「詳細」**に移動し、**→ネットワーク設定→ VLAN** を選択します。

Step 2VLANを有効にします。

Step 3**ISP プロファイルを選択します。**ISP として「MANUAL」を選択しない限り、**インターネット VLAN ID は**デフォルトで設定されます。

Step 4(オプション) ISPとして「MANUAL」を選択した場合、**インターネットサービスインターフェース、IPTVサービスインターフェース、**および**VoIPサービスインターフェースを**個別に設定し、それぞれのVLAN IDを設定する必要があります。

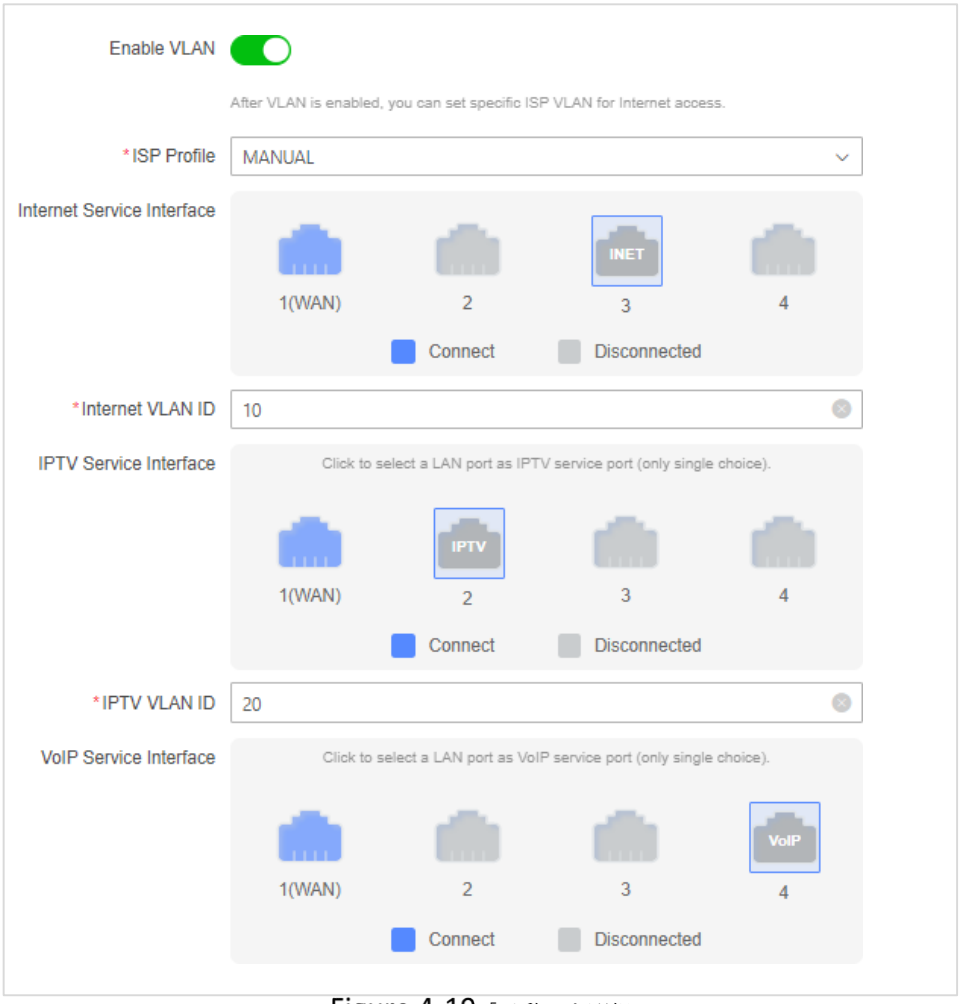

Figure 4-19「手動」を選択

Step 5**保存**をクリックします。

Note

- VLANを有効にすると、WANポートはデフォルトでネットワークポート1に固定されます。イーサネットケーブルをポート1に再接続してください。
- MANUAL パラメーターを設定する際、LAN ポートは1つのサービス種類のみに設定可能です。
- VLAN IDは5～4094の範囲内で設定する必要があります。

4.3.10 Mesh

メッシュネットワークは、新しいルーターをアクティブ化しペアリングすることで、既存のルーターのWi-Fi範囲を拡張するのに役立ちます。

「More」→「→」→「Network Settings」→「→」→「Mesh」を選択し、この機能を有効にします。

操作手順の詳細は、ページ内の「**クイック ネットワーク ガイド**」または「***1.2.2 Wi-Fi 範囲の拡張***」を参照してください。

4.3.11 Auto Select WAN Port

ルーターの4つのネットワークポートは、デフォルトでWANまたはLANに自動適応します。

「詳細」→「→」→「ネットワーク設定」→「→」→「Auto Select WAN Port」を選択し、この機能を無効にすると、WANポートはネットワークポート1に固定されます。

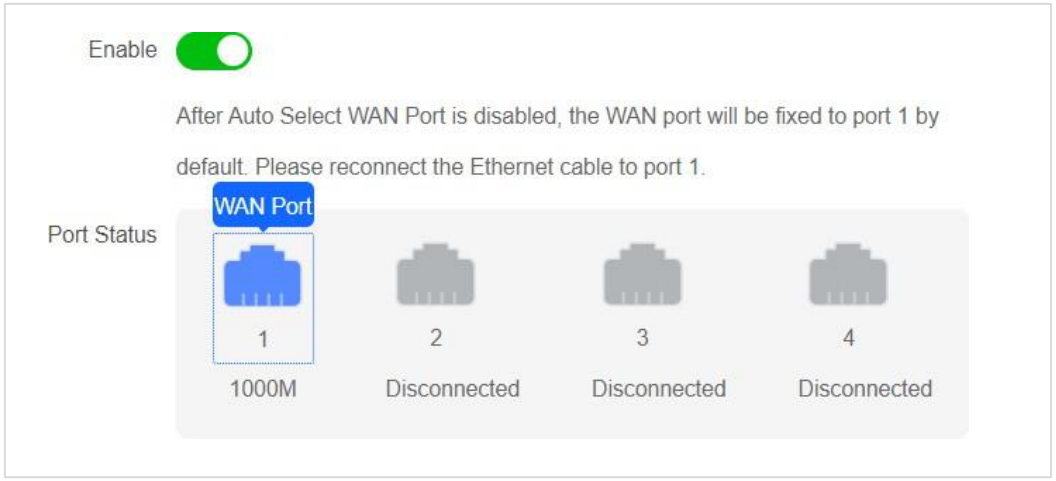

Figure 4-20WANポートの自動選択

Note

この機能を無効にした場合は、イーサネットケーブルをポート1に再接続してください。

4.3.12 TR-069

CPE WAN管理プロトコル（TR-069）は、自動設定サーバー（ACS）が顧客拠点設備

(CPE) を構成、接続、診断し、ルーターの遠隔管理を実現します。

「詳細設定」に移動し、→**ネットワーク設定**→**TR-069** を有効にします。

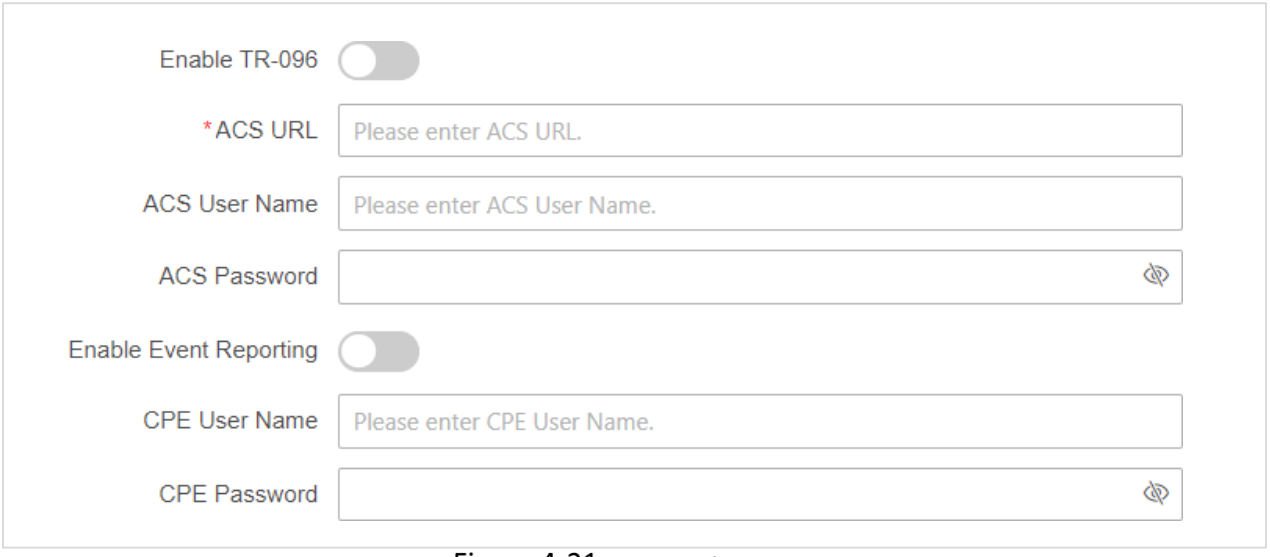

Figure 4-21TR069 を設定

- **TR-096 を有効にする**: TR-069 を有効/無効にします。TR-096 が有効の場合、ルーターは ACS にセッション設定要求を送信します。TR-069 はデフォルトで無効です。
- **ACS URL**: ACS サーバーの IP アドレスまたはドメイン名が必要です。文字数範囲は 1～255 文字です。
- **ACS ユーザー名**: ルーターからセッション設定要求を受信した後に ACS によって認証されるユーザー名 です。文字数範囲は 1～256 文字です。
- **ACS パスワード**: ACS によって認証されるパスワードです。文字数範囲は 1～64 文字です。
- **イベント報告を有効にする**: 有効にすると、ルーターは設定された間隔時間でACSにイベントを報告します。
- イベント**報告間隔**: イベント報告の間隔時間です。値の範囲は5～3600秒です。
- **CPEユーザー名**: ACSから接続要求を受信した後にCPEによって認証されるユーザー名。ユーザー名はACSで指定されています。文字数範囲は1～256文字です。
- **CPE パスワード**: ACS から接続要求を受信した後に CPE によって認証されるパスワードです。このパスワードは ACS で指定されています。文字数は 1～64 文字です。

第5章 ルーター管理

5.1デバイス情報

「詳細」をクリックし、→ **の基本情報**を選択して、基本デバイス情報とネットワーク情報を表示します。

基本情報: デバイスモデル、シリアル番号、システムバージョンを確認し、デバイス名をカスタマイズできます。

Figure 5-1基本情報

ネットワーク情報: デバイスのネットワークIPアドレス、サブネットマスク、ゲートウェイ、およびDNSサーバー情報を確認します。

5.2システム設定

「詳細」をクリックし、→ **システム設定**を選択して、時刻同期、インジケーターなどの設定を行います。

5.2.1 System Time

時刻同期

デバイスのシステム時間をネットワーク時間と同期し、システム時間の正確性を確保します。デフォルト設定は一般ユーザー向けです。

- **PCの時刻同期**: ネットワーク接続がない場合に使用可能です。

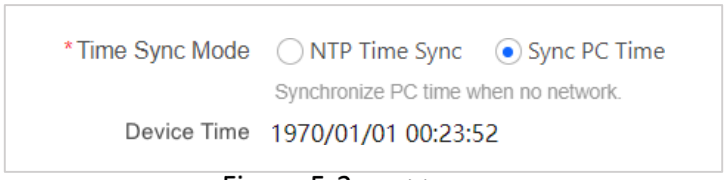

Figure 5-2PCの時刻を同期

- **NTP 時刻同期**：ネットワークと自動的に時刻を同期します。

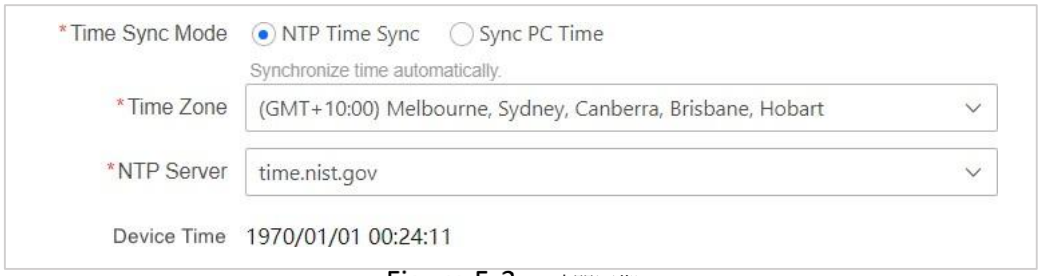

Figure 5-3NTP時間同期

夏時間

夏時間（DST）の開始時間と終了時間の設定をサポートします。有効化後、システム時間がDSTの開始時間に達すると、1時間遡って調整されます。システム時間がDSTの終了時間に達すると、1時間進めて調整されます。

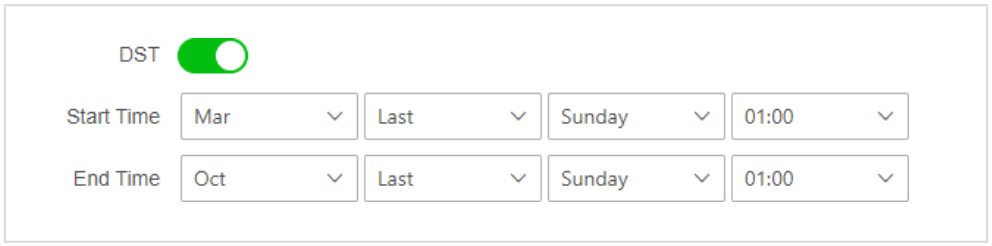

Figure 5-4 DST

5.2.2 Cloud Management

クラウドベースのネットワーク管理に対応しています。

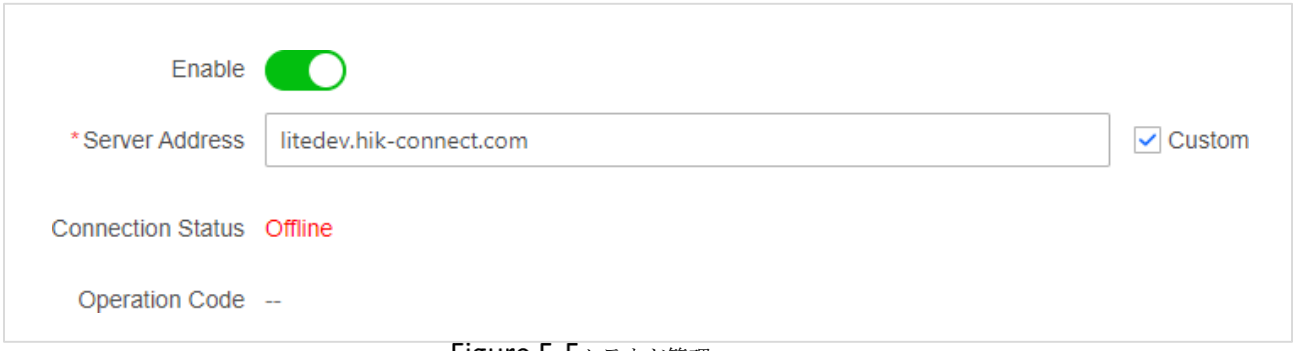

Figure 5-5クラウド管理

5.2.3 Indicator

Webページスイッチ経由でデバイスインジケーターの有効/無効を切り替えることができます。

5.3セキュリティ設定

「→ セキュリティ設定」を選択し、ルーターのセキュリティを設定します。

5.3.1 Firewall

ファイアウォールは、インターネットと家庭内LANの間の安全なバリアです。ファイアウォールを有効にすると、デバイスはインターネットからLANに流入するデータをフィルタリングし、外部ネットワークからのネットワーク攻撃を防止します。これにより、内部ネットワークのユーザーとデータのセキュリティが保護されます。常に有効にしておくことをおすすめします。

5.3.2 DMZ

ローカルエリアネットワーク（LAN）のホストをDMZホストとして設定すると、外部ネットワークからそのホストにアクセスできます。例えば、ウェブサーバーやFTPサーバーをDMZホストとして設定すると、インターネット経由でDMZホストにアクセスできます。DMZを有効化する際に、DMZホストのIPアドレスを入力してください。

Figure 5-6DMZを設定する

Note

ポートマッピングは、指定されたポートのみをマッピングするために使用されます。DMZはすべてのポートをマッピングし、ホストをゲートウェイに直接公開します。ポートマッピングよりも簡単ですが、セキュリティは低くなります。

5.3.3 Port Mapping

LANホストの特定のポートをWAN IPアドレスとポートにマッピングし、パブリックネットワークから容易にアクセスできるようにします。

マッピングポートを追加するには、IPアドレス、IPポート、および外部ポートの情報が必要です。

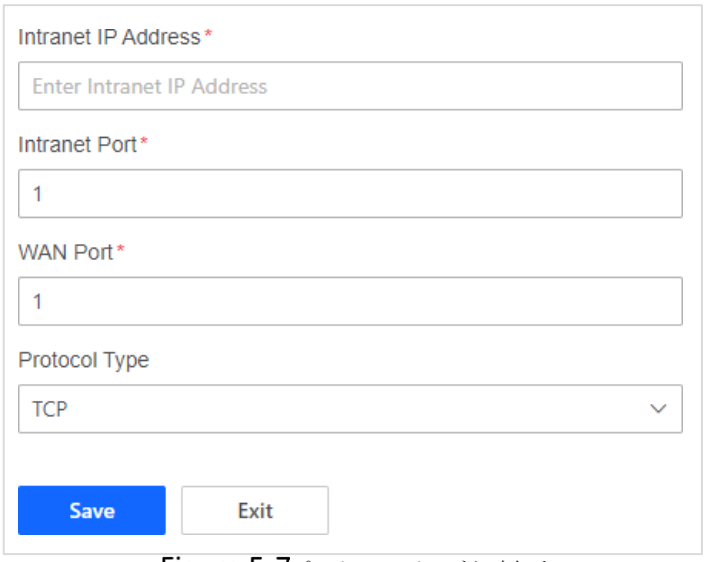

Figure 5-7ポートマッピングを追加する

5.3.4 Remote Web

リモートWeb機能が有効化されると、ルーターのWANポートIPをHTTPSプロトコル経由で入力することで、デバイスを管理できます。有効化後は、
ハッカーによる攻撃を受けるリスクがあり、長期的な有効化は推奨されません。

Caution

リモートウェブを有効化すると、ルーターが攻撃を受けるリスクがあります。リモートウェブを適時無効化してください。

5.3.5 WPS

ルーターのWPSキーを使用すると、パスワードなしで端末デバイスをルーターのネットワークに接続したり、ルーターをアップリンクデバイスにパスワードなしで接続したりできます。

Note

- 接続されたデバイスまたはアップリンク ルーターが WPS をサポートしていることを確認してください。
- ルートが有効になっていることを確認してください。

Step 1端末をルーターから1メートル以内に配置してください。Step 2 WLANを有効にし、ネットワークをタップして接続してください。

Step 3ルーターのフレームにあるWPSボタンを1～3秒間長押しします。ルーターのインジケーターが青色に点滅し、ペアリング中であることを示します。

Note

5秒以上長押しすると、WPSモードが有効な他のルーターとのセキュアなリレーが実現します。

5.4システムメンテナンス

「→ システムメンテナンス」を選択し、デバイスのアップグレード、バックアップ、工場出荷時設定への復元、ログ記録などを行います。

5.4.1 Software Upgrade

「→」を選択し、システムメンテナンスから「→」を選択し、ソフトウ

ェアアップグレードを選択します。 **の自動アップグレード**

この機能はデフォルトで有効になっています。**自動アップグレード**が有効になっている場合、毎日午前2時から5時30分の間に、WANポートのトラフィックが一定の閾値未満で新しいバージョンが

検出されると、デバイスは自動的に新しいバージョンにアップグレードされます。

手動アップグレード

オンラインアップグレードとローカルアップグレードがサポートされています。

- **オンラインアップグレード**：新しいバージョンがオンラインで検出された後、**[更新を確認]**をクリックします。
- **ローカルアップグレード**: ローカルアップグレードパッケージファイルをインポートし、**[アップグレード]** をクリックします。

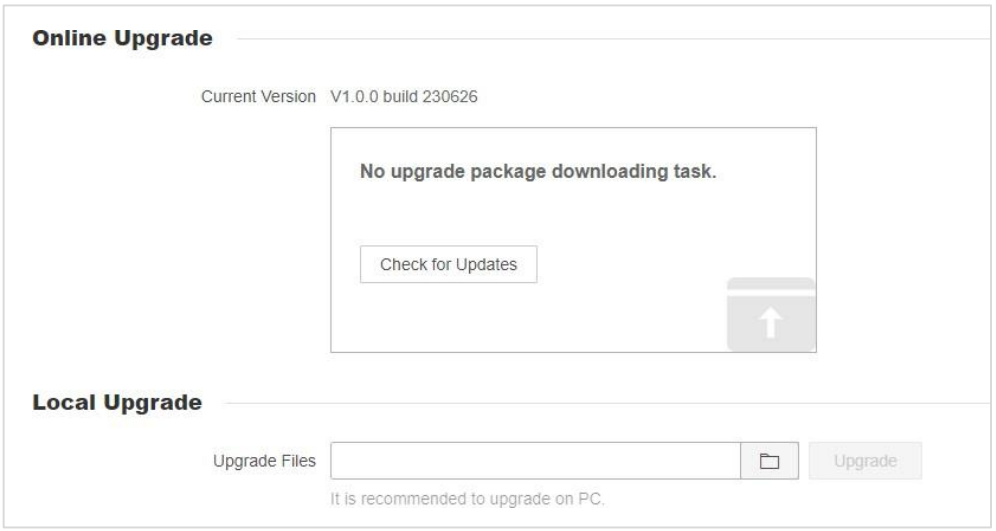

Figure 5-8手動アップグレード

Caution

アップグレード中はデバイスを電源オフにしないでください。

5.4.2 Reboot Device

「詳細」を選択し、**→、システムメンテナンス、→、デバイスを再起動**

を選択します。 手動再起動

「再起動」をクリックしてデバイスを手動で再起動します。

スケジュールされた再起動

デフォルトでは無効になっています。**スケジュールされた再起動**を有効にすると、WAN ポートのトラフィックが一定の閾値未満の場合、毎日午前3時から5時の間にデバイスが自動的に再起動します。デバイス再起動中は、すべての接続が切断されます。

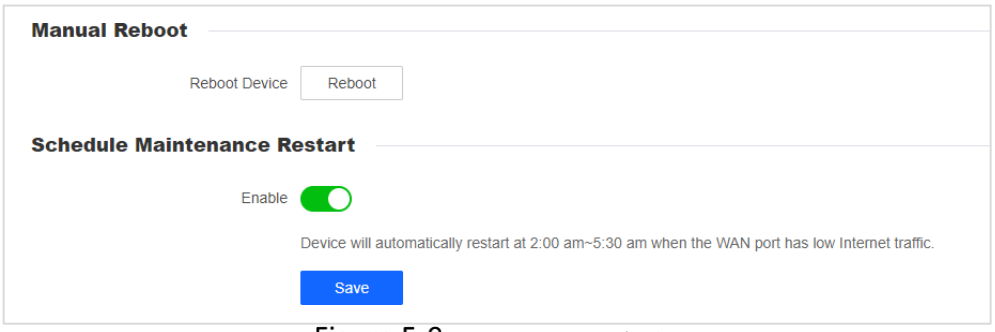

Figure 5-9タイマーによる再起動

5.4.3 Backup and Restore

→「詳細設定」を選択し、システムメンテナンスの「」を選択し、「→」を選択します。

- **バックアップ**:「**エクスポート**」をクリックして、ルーターの設定ファイルをローカルにエクスポートします。
- **復元**: 保存した設定ファイルをデバイスにインポートし、以前の設定を復元します。
- **デフォルトに復元**: デバイスのすべての設定を工場出荷時状態に復元します。

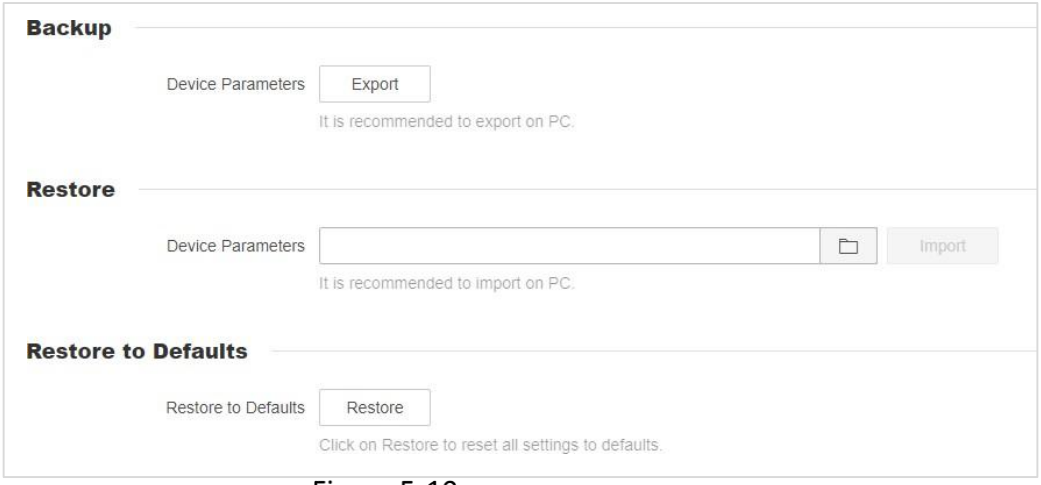

Figure 5-10バックアップと復元

Note

以前の設定を復元しても、デバイスの管理IPアドレスとパスワードは復元されません。

5.4.4 Log Management

→「**詳細**」を選択し、**システムメンテナンスの「→ ログ**」を選択してログを管理します。

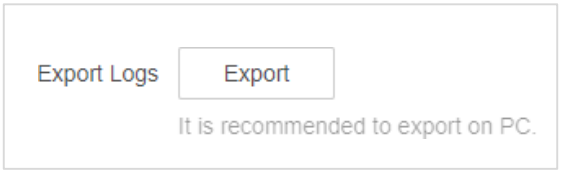

Figure 5-11ログ管理

「**エクスポート**」をクリックして、デバイスのログ情報をローカルコンピュータにエクスポートします。

Note

エクスポートされたログファイルは、メンテナンス担当者だけが閲覧および使用可能です。

5.4.5 Diagnosis

→「**More**」を選択し、**システムメンテナンスの「→」**を選択し、「**Diagnose**」をクリックしてルーターのネットワーク接続状態を確認します。接続状態を確認し、結果をクラウドサーバーにアップロードするかどうかを選択してください。

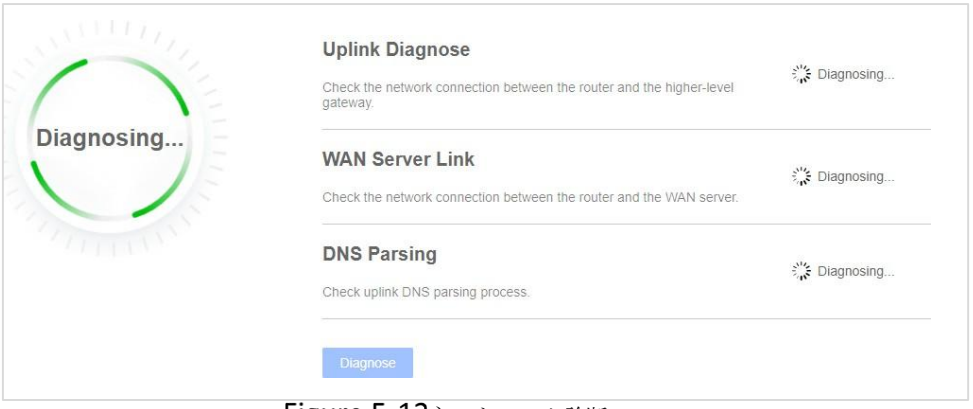

Figure 5-12ネットワーク診断

5.5パスワード管理

Table 5-1パスワード管理

操作	説明
Wi-Fi パスワードの確認	オーバービューページで「 」 をクリックします。
Wi-Fi パスワードを変更する	「**マイ Wi-Fi**」に移動し、**→ の基本ワイヤレス設定を開きます**。
管理者パスワードを変更	ページの右上にある「**パスワードを変更**」をクリックします。
管理者パスワードを忘れた場合	リセットボタンを8秒間押した後、ルーターを再起動して新しい管理者パスワードを設定してください。

遠くを見据え、さらに先へ