



# スマート管理スイッチ ウェブ

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

- このドキュメントには、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。本文中の図、表、画像を含むすべての情報は、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でないが、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

- 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。
- その他の商標およびロゴは、それぞれ該当する所有者の財産です。

### 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でないが、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基づくものであっても、本製品の使用に関連して生じた損害について、当社は一切の責任を負いません。

製品の使用に関連して、HIKVISIONがそのような損害または損失の可能性について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、あなたは、第三者の権利（パブリシティ権、知的財産権、データ保護権、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 デジタルテクノロジー株式会社。著作権所有。

## 序文

### 対象モデル

このマニュアルは、スマート管理スイッチに適用されます。

### デフォルト設定について

- デフォルトの管理者アカウント: **admin**
- スーパーIPアドレス: **10.180.190.200**



- デフォルトのユーザー名「**admin**」は、初回ログイン時に有効化する必要があります。
- スイッチのデフォルトIPアドレスは動的に割り当てられます。
- スーパーIPアドレスは変更できません。スイッチがPCに直接接続されている場合、スーパーIPアドレスを使用してスイッチにアクセスし、デバイス管理を行うことができます。

### 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
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 序論 .....	1
第2章 アクティベーションとログイン .....	2
第3章 デバイス情報 .....	5
3.1 デバイス概要 .....	5
3.2 ポートの状態 .....	9
3.3 ネットワーク状態 .....	10
第4章 デバイス設定 .....	13
4.1 ポート設定 .....	13
4.1.1 ポート属性の設定 .....	13
4.1.2 リンクアグリゲーションの設定 .....	14
4.1.3 ポートの隔離を設定する .....	15
4.1.4 ポートミラーリングの設定 .....	15
4.1.5 長距離モードの設定 .....	17
4.1.6 高優先度ポートの設定 .....	17
4.2 PoE設定 .....	18
4.3 VLAN設定 .....	19
4.3.1 VLAN の追加 .....	19
4.3.2 ポートのVLAN設定 .....	20
4.4 STP設定 .....	21
4.5 LLDP設定 .....	2
第5章 システム管理 .....	24
5.1 ネットワーク設定 .....	24
5.2 時刻同期 .....	27
5.3 システムメンテナンス .....	28
5.4 ログ管理 .....	30

## 第1章 概要

スマート管理スイッチは、ウェブ経由での管理をサポートし、アクティベーションとログイン、デバイス概要、ネットワーク設定、デバイス設定、システムメンテナンスなどの機能を提供します。



対応する機能はデバイスモデルによって異なります。本マニュアルに示されている図と実際のデバイスのインターフェースに相違がある場合、後者が優先されます。

---

## 第2章 アクティベーションとログイン

スイッチを初めて使用する場合は、アクティベーションを行い、パスワードを設定する必要があります。

### 開始前に

コンピュータとスイッチが同じネットワークセグメントに接続されていることを確認してください。

### 手順



注意

このマニュアル内のすべての図は、説明のための例示です。

---

1. ウェブブラウザのアドレスバーにスイッチのデフォルトのIPアドレスを入力し、**Enter**キーを押します。

図2-1 デバイスのアクティベーション



- スwitchのデフォルトのIPアドレスは、SADPツールを使用して取得できます。
- 以下のウェブブラウザの使用を推奨します：Microsoft Edge 89以降、Google Chrome 89以降、およびFirefox 78以降。

2. パスワードを設定し、パスワードを確認してください。



- パスワードは、8文字から16文字で構成され、以下のカテゴリから少なくとも2種類を含む必要があります：大文字、小文字、数字、および特殊文字。
- パスワードには、ユーザー名、'123'、または'admin'（大文字小文字を区別しない）、4つ以上の連続する増加または減少する数字（例：'1234'や'4321'）、または4つ以上の同一の文字（例：'1111'や'aaaa'）を含めることはできません。
- パスワードは一般的な危険なパスワードであってはなりません。

3. オプション：クラウド管理を確認してください。

Hik-Connect サービスが有効になっています。

4. OKをクリックします。

ネットワーク設定ページが表示されます。

5. オプション：ネットワーク設定を変更します。

1) システム管理→ネットワーク設定→ネットワーク設定 へ移動します。

The screenshot shows two sections of a web configuration page. The first section, 'Basic Configuration', includes a 'DHCP' toggle switch (currently off) and three input fields: '\* IPv4 Address' (10.184.), '\* IPv4 Subnet Mask' (255.255.), and '\* Default IPv4 Gateway' (10.184.). The second section, 'DNS Address Configuration', includes two input fields: '\* Preferred DNS Address' (8.8.) and '\* Alternate DNS Address' (8.8.). A red 'Save' button is located at the bottom of the form.

図2-2 ネットワークパラメーターの変更



- 2) IPv4アドレス、IPv4サブネットマスク、デフォルトのIPv4ゲートウェイ、優先DNSアドレス、および代替DNSアドレスを必要に応じて変更するか、**DHCP**を有効にしてIPアドレスの自動割り当てを有効にします。



ネットワーク設定を変更して、スイッチを適切に管理することをおすすめします。

- 3) 変更後、新しいIPアドレスでスイッチのウェブインターフェースに再ログインしてください。

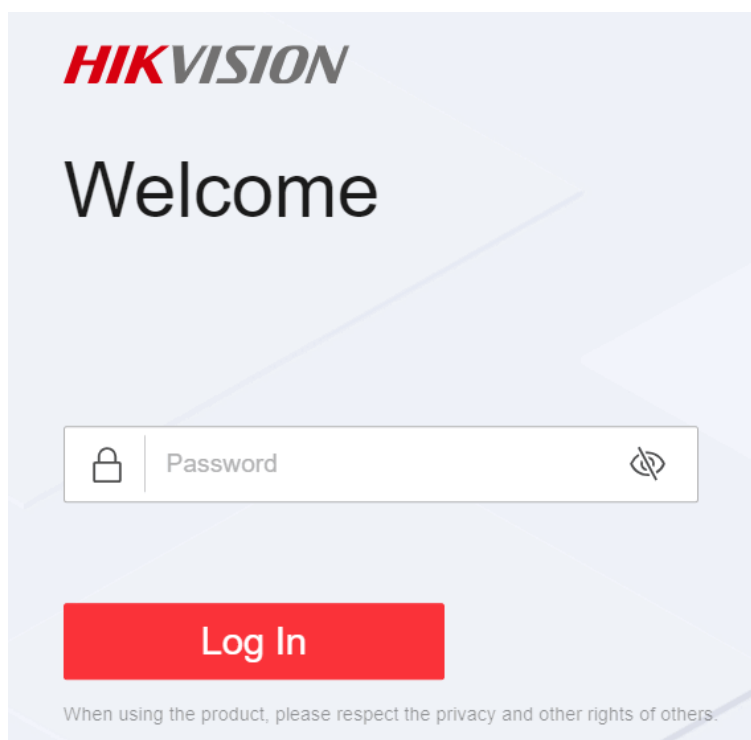


図2-3 ログイン

## 第3章 デバイス情報

スイッチのウェブにログインすると、デバイス概要情報、ポート状態情報、ネットワーク状態情報を含む、スイッチの詳細情報を取得できます。

### 3.1 デバイス概要

デバイス概要情報を表示または編集するには、**概要**ページに移動してください。


#### 基本デバイス情報

概要ページの右下隅で、スイッチのデバイスモデル、ソフトウェアバージョン、シリアル番号、IPアドレスおよびMACアドレス、CPU使用率、メモリ使用率を確認できます。



図3-1 基本デバイス情報の表示

### デバイス名

現在のデバイス名を確認できます。または、その横の「」をクリックして、**概要**ページでカスタマイズできます。

**DS-3E1106P-EI/M** 

図3-2 デバイス名の編集


### システム稼働時間

デバイスのシステム稼働時間は、概要ページの右上隅に表示されます。

System Uptime: 0 Week(s) 1 Day(s) 21 h 37 min 55 sec

図3-3 システム稼働時間の表示

### 追加されたVLAN

追加されたVLANの数をすばやく確認できます。または、をクリックしてVLAN管理ページに移動し、VLANの設定を行うことができます。

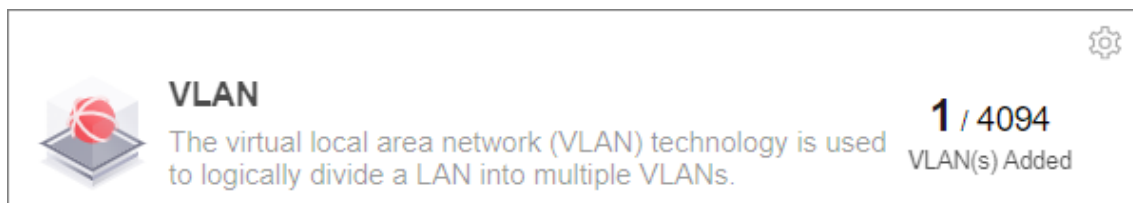


図3-4 追加されたVLANの数表示



デバイスが許可する最大VLAN数も確認できます。例えば、上記の図では4094です。デバイスが許可する最大VLAN数は、デバイスモデルによって異なります。

---

### クラウドプラットフォーム接続状態

クラウドプラットフォーム モジュールは、デバイスがHik-Connectに接続されているかどうかを表示します。

- クラウドプラットフォームが接続されている場合、QRコードをスキャンしてデバイスをHik-Partner Proアプリに追加し、リモート管理を行うことができます。

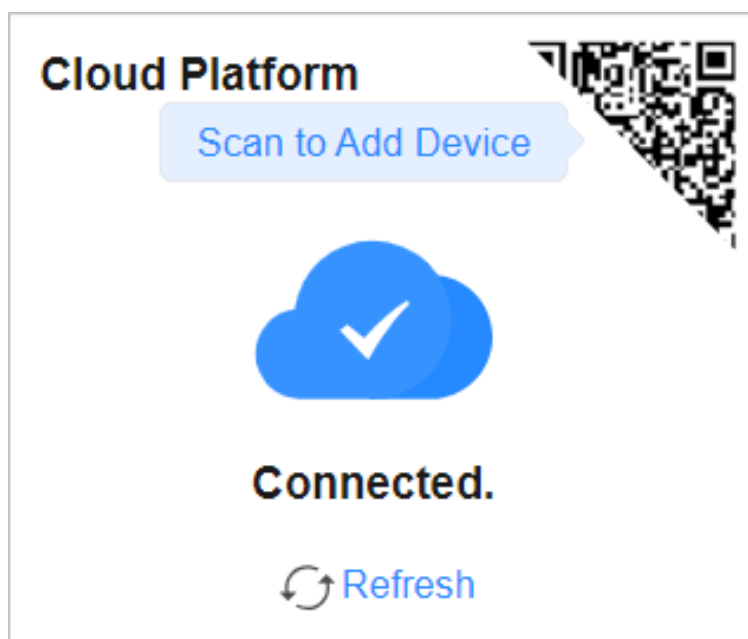


図3-5 クラウドプラットフォーム接続状態の表示（接続中）

- クラウドプラットフォームが接続されていない場合、[リフレッシュ]をクリックして再接続するか、[診断]をクリックして接続障害の原因を確認し、表示される指示に従ってクラウドプラットフォームの設定ページに移動して設定を行ってください。

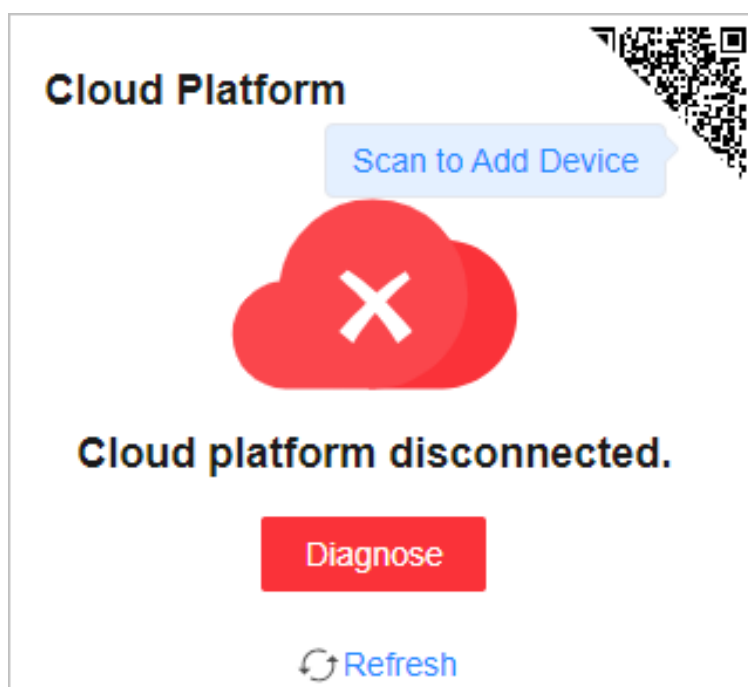


図3-6 クラウドプラットフォーム接続状態の表示（接続解除）

## 3.2 ポートの状態

**概要**ページでは、物理ポートの視覚的な表示を提供し、各ポートの接続状態または電源供給状態を表示します。これにより、ユーザーはスイッチポートの管理がより容易になります。

### ポートパネル

**ポートパネル** モジュールは、各ポートの接続状態と電源供給状態を表示します。マウスをポート上にホバーさせると、ポート名、接続状態、レート/デュプレックス、フロー制御状態、パケット受信/送信レートが表示されます。ポートが**PoE**ポートの場合、ポートの**PoE**電源を確認できます。

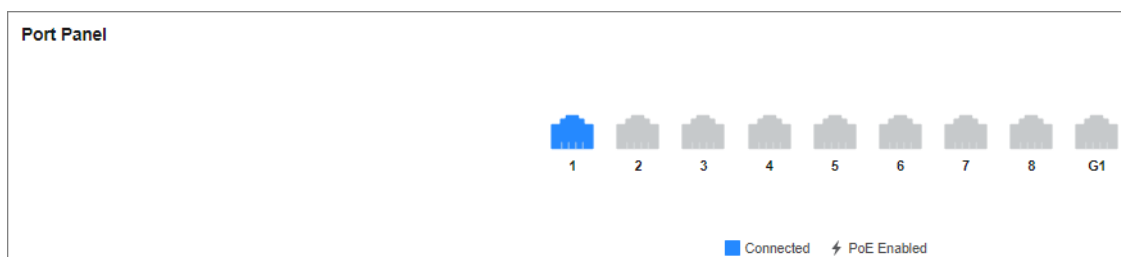


図3-7 ポートパネルの表示

### ポート詳細

**ポート詳細**モジュールでは、各ポートのステータスパラメーターが表示されます。各ポートのポートステータス、レート/デュプレックス、フロー制御を設定でき、各ポートのポート名、接続ステータス、実際のレート/デュプレックスを確認できます。

Port Details					
Port Name	Connection Status	Port Up	Actual Rate/Duplex	Configured Rate/Duplex	Flow Control
Eth1	Connected	<input checked="" type="checkbox"/>	100 Mbps/Full-Duplex	Auto/Auto	<input checked="" type="checkbox"/>
Eth2	Disconnected	<input checked="" type="checkbox"/>	--	Auto/Auto	<input checked="" type="checkbox"/>
Eth3	Disconnected	<input checked="" type="checkbox"/>	--	Auto/Auto	<input checked="" type="checkbox"/>
Eth4	Disconnected	<input checked="" type="checkbox"/>	--	Auto/Auto	<input checked="" type="checkbox"/>
Eth5	Disconnected	<input checked="" type="checkbox"/>	--	Auto/Auto	<input checked="" type="checkbox"/>
Eth6	Disconnected	<input checked="" type="checkbox"/>	--	Auto/Auto	<input checked="" type="checkbox"/>

図3-8 ポート詳細の表示

#### 接続状態

ポートの接続状態：**接続**中または**接続解除**。

#### ポートアップ

ポートを有効化（ポートアップ）または無効化（ポートダウン）します。デフォルトでは、ポートはアップ状態です。

#### 実際の速度/デュプレックス

ポートの実際の速度とデュプレックスモード。


#### 設定されたレート/デュプレックス

ポートの転送速度とデュプレックスモードを設定します。デフォルト値は「**Auto/Auto**」です。必要に応じて、転送速度とデュプレックスモードの異なる組み合わせを選択できます。

#### フロー制御

ポートのフロー制御を有効または無効にします。デフォルトでは、フロー制御は有効になっています。フロー制御を有効にすると、ネットワークへの大量のデータの影響を効果的に軽減し、ネットワークの安定性を維持できます。

#### PoE電源

スイッチの過去7日間の全体的なPoE電源とピークPoE電源を確認できます。モジュールの右上にある「」をクリックして、PoE管理ページに移動し、PoE機能の設定を行います。

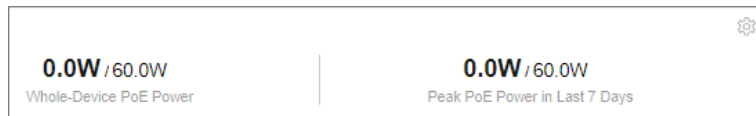


図3-9 PoE 電源の表示




#### 注意

PoE電源表示は、PoE対応のスイッチでのみ利用可能です。

## 3.3 ネットワーク状態

ネットワーク監視機能を使用すると、同一LAN内のネットワークデバイス情報、ポートが学習したMACアドレス、ポート統計情報、およびケーブル状態を確認できます。

#### ネットワークデバイスの検出

ネットワークデバイス検出は、スイッチと同じLAN内に存在する送信デバイスを自動的に検出し、これらのデバイスの情報を表示する機能です。ネットワーク監視に移動し、→ネットワークデバイス検出を選択すると、検出されたネットワークデバイスのIPアドレス、タイプ、モデル、シリアル番号を確認できます。デバイスを選択し、操作列のをクリックすると、デバイスのウェブ設定ページに移動できます。









IP Address	Device Type	Device Model	Serial Number	Operation
10.13. (Local)	Switch	DS-3E1308P-EI/M	AY	
10.13.	Switch	DS-3E1328P-EI/M	FC	
10.13.	Switch	DS-3E1528P-SI-24P-4F	FF	
10.13.	Switch		CR	
10.13.	Switch		FE	
10.13.	Switch		F	
10.13.	Switch	DS-3E1528P-S	AK	
10.13.	Switch		FE	

図3-10 ネットワークデバイスの検索

## ポートMACアドレスのクエリ

各ポートが学習したMACアドレスを照会できます。**ネットワーク監視** → **MACアドレス** を選択し、**ポート**のドロップダウンリストから対象のポートを選択し、**検索**をクリックします。ポートが学習したMACアドレスとMACアドレスのタイプが、下のリストに表示されます。

MAC Address	AA-BB-CC-DD-EE-FF	Port	All	Search	Reset
MAC Address	Type	Port			
e0 ca	Dynamic	Eth1			
1c 1b	Dynamic	Eth1			
04 03	Dynamic	Eth1			
1c 5e	Dynamic	Eth1			
98 f1	Dynamic	Eth1			
b8 3a	Dynamic	Eth1			

図3-11 ポートのMACアドレスの照会

## ポート統計情報の表示

デバイスポートの送信データに関する統計情報を監視および収集できます。**ネットワーク監視** → **ポート統計**に移動し、統計リストで各ポートの現在の接続状態と各ポートが送信したデータを表示できます。


Port Statistics							
							
Connected							
Statistics Data							
Clear All Refresh (30s) ▾							
Port Name	Sending Rate	Receiving Rate	Sent Packets	Received Packets	Inbound Error Packets	Peak Sending Rate	Peak Receiving Rate
Eth1	22.4Kbps	784.0Kbps	342,490	14,222,595	0	234.4Kbps	1.5Mbps
Eth2	--	--	--	--	--	--	--
Eth3	--	--	--	--	--	--	--
Eth4	--	--	--	--	--	--	--
Eth5	--	--	--	--	--	--	--
Eth6	--	--	--	--	--	--	--
Eth7	--	--	--	--	--	--	--
Eth8	--	--	--	--	--	--	--
Ge1	--	--	--	--	--	--	--

図3-12 ポート統計情報の表示

以下の操作も実行できます：

- ポート統計をクリアする: 「Clear All」をクリックすると、すべてのポート統計をクリアできます。
- ポート統計を手動で更新: 「Refresh」をクリックすると、ポート統計を手動で更新できます。
- ポート統計の自動更新: ポート統計の自動更新間隔を設定できます: 30秒または60秒。

## ケーブル状態の検出

**ケーブル検出**は、イーサネットポートのケーブルの状態を検出する機能です。例えば、ケーブルの受信側または送信側に短絡や断線があるかどうかを確認し、ある場合は故障したケーブルを特定します。**ネットワーク監視**の「**Cable Detection**」に移動し、左側のポートパネルで対象のポートを選択し、「Detect」をクリックして検出結果を表示します。



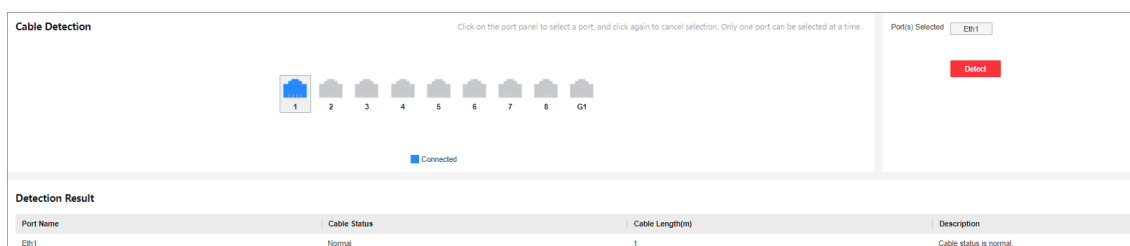


図3-13 ケーブル状態の検出

## ネットワークの診断

Pingは、ネットワーク接続の状態を診断し、ネットワーク障害を迅速に特定する機能です。

1. ネットワーク監視をクリックし、→ Ping を選択します。

\* IPv4 Address

10.13.

Ping

図3-14 Ping

2. IPv4アドレスフィールドにネットワークサーバーのアドレスを入力します。
3. 「Ping」をクリックします。



ネットワーク診断の結果は、Ping 結果領域に表示されます。

## 第4章 デバイス設定

### 4.1 ポート設定

#### 4.1.1 ポート属性の設定

基本属性はポートの動作状態に影響を与える可能性があります。必要に応じてパラメーターを設定してください。

手順

1. **L2 設定**に移動し、→ **ポート属性**を選択します。

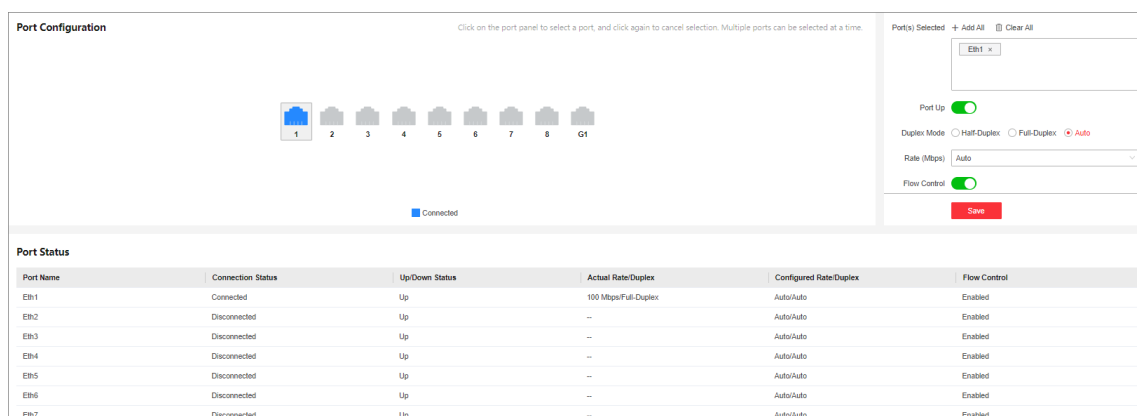


図4-1 ポート属性の設定

2. 対象のポートを選択し、パラメーターを設定します。

#### ポートのアップ

選択したポートを有効または無効にします。ポートが有効の場合、そのポートはアップ状態になります。ポートが無効の場合、そのポートはダウン状態になります。ダウン状態のポートではデータが送信されません。

#### デュプレックスモード

ポートのデュプレックスモード。ポートの構成可能なデュプレックスモードには、**ハーフデュプレックス**、**フルデュプレックス**、および**オート**が含まれます。これらのモードは、デバイスモデルによって異なる場合があります。

#### レート (Mbps)

ポートのポートのデータ転送速度。ポートの構成可能なレートには、**10M**、**100M**、**1000M**、および**オート**が含まれます。これらの値はデバイスモデルによって異なる場合があります。

#### フロー制御

ポートのフロー制御を有効または無効にします。フロー制御を有効にすると、データ伝送時のデータ損失を防止できます。

3. **保存**をクリックします。

4. **オプション**：ポートステータス一覧でポートの属性を表示します。

## 4.1.2 リンクアグリゲーションの設定

リンクアグリゲーションは、複数の物理リンクを結合して論理的な高帯域幅のデータパスを作成し、より強固で高速なネットワーク接続を提供する技術です。

### 手順

1. **L2 設定**に移動→ **リンクアグリゲーション**。
2. **+Add** をクリックします。

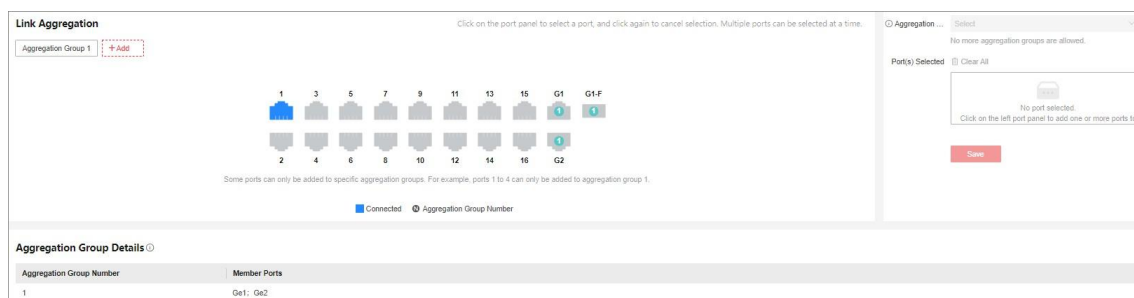


図4-2 リンクアグリゲーションの設定

3. 少なくとも2つのポートを選択します。



注

- 選択可能なポートのみをアグリゲーショングループに追加できます。
- 各リンクアグリゲーショングループには、2～4つのポートを指定できます。
- 一部のポートは、特定の集約グループにのみ追加可能です。実際の状況をご確認ください。
- 1つのアグリゲーショングループ内のポートのレート、デュプレックスモード、フロー制御、ロングレンジモード、およびVLAN設定は同じにする必要があります。

4. **アグリゲーショングループ番号**を設定します。



注意

許可されるアグリゲーショングループの数は異なります。

5. **保存**をクリックします。
6. **オプション: 集約グループを編集**します。
  - 1) 既存の集約グループ（例：「集約グループ1」）をクリックします。
  - 2) 左側のポートパネルでグループに追加したいポートを選択するか、右側のポートでグループから削除したいポートの選択を解除します。
  - 3) **編集**をクリックして変更を保存します。
7. **オプション: グループ化グループを削除**します。
  - 1) 既存の集約グループ（例：「Aggregation Group 1」）をクリックします。
  - 2) 右側の「**削除**」をクリックします。
8. **オプション**：下のリストで各アグリゲーショングループのメンバーポートを表示します。

### 4.1.3 ポート隔離を設定します。

ポート隔離は、複数のポートを隔離グループに追加し、同じ隔離グループ内のポート同士が通信できないようにする機能です。例えば、ポート隔離機能を使用することで、VLANを設定せずに、異なるポートに接続されたPC同士が通信できないようにすることができます。

#### 手順

1. セキュリティ→ポート隔離に移動します。

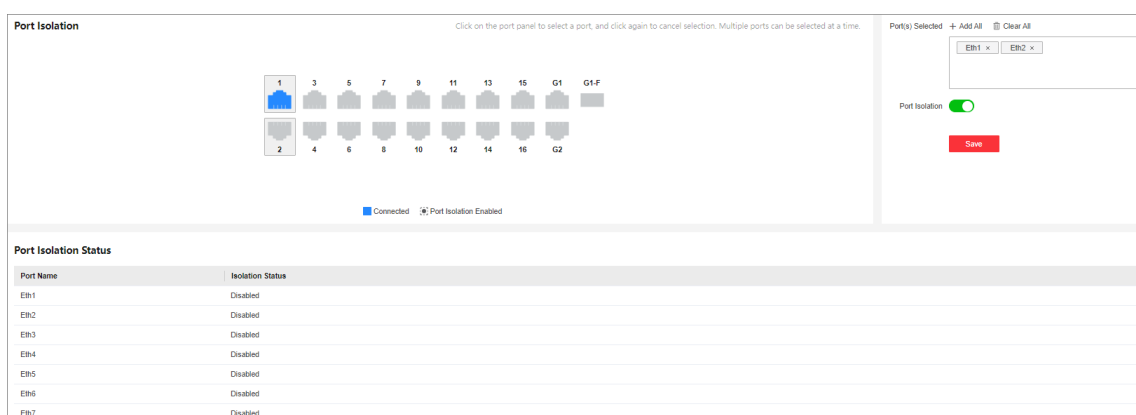


図4-3 ポート隔離の設定

2. ポートパネルで対象のポートを選択します。



また、クリックすることもできます。または、をクリックして、すべてのポートをまとめて選択または選択解除できます。

3. 必要に応じてポート隔離を有効または無効にします。
4. 保存をクリックしてください。
5. オプション: ポート隔離ステータス一覧で、各ポートのポート隔離ステータスを確認できます。

### 4.1.4 ポートミラーリングの設定

ポートミラーリングは、ネットワークスイッチの機能の一つで、管理者が1つのポート（ミラーポート）のトラフィックを監視し、そのデータを別のポート（ミラーリングポート）に複製して分析できるようにします。この複製はリアルタイムで行われ、管理者はミラーポートで移動するトラフィックの「ミラー」または正確な複製を確認できます。

#### 手順

1. l2 設定→ポートミラーリングに移動します。

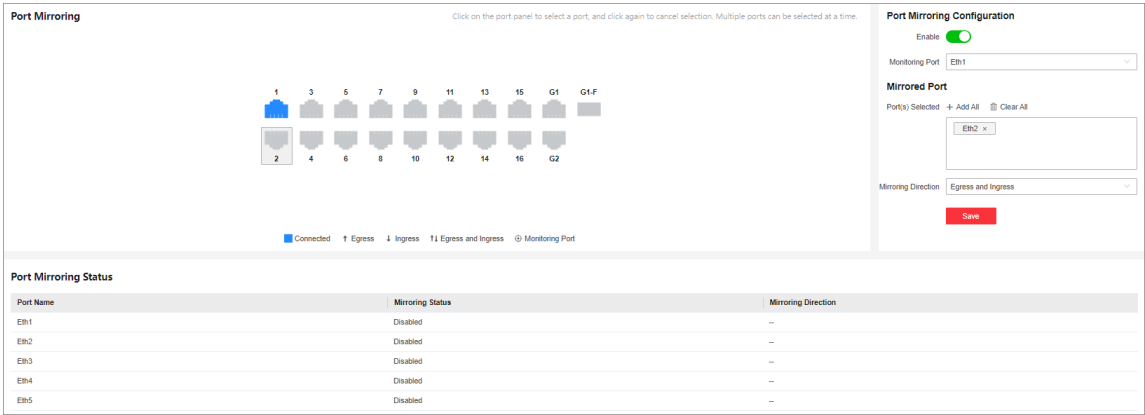


図4-4 ポートミラーリングの設定

2. ポートパネルでミラーリング対象のポートを選択し、必要なパラメーターを設定します。



クリックすることも **+ Add All** また **Clear All** 右側をクリックして、すべてのポートをまとめて選択または有効

選択したポートのポートミラーリングを有効または無効にします。

モニタリングポート

モニタリングポート（ミラーリングポート）として設定できるのは1つのポートのみです。

ミラーリング方向（入力）

ソースポートで受信したデータが監視対象となります。

送信

ソースポートから送信されるデータが監視対象となります。

エグレスとイングリッシュ

ソースポートから受信したデータとソースポートから送信されたデータの両方が監視対象となります。

3. 保存をクリックしてください。



最新の設定は以前の設定を上書きします。

4. オプション: ポートミラーリングステータス一覧で各ポートのミラーリング状態を確認できます。

### 4.1.5 長距離モードを設定

ポートに長距離モードを有効にすると、そのポートの伝送距離は10 Mbpsの速度で300メートルまで到達できます。

#### 手順

1. L2 設定→長距離モードへ移動します。

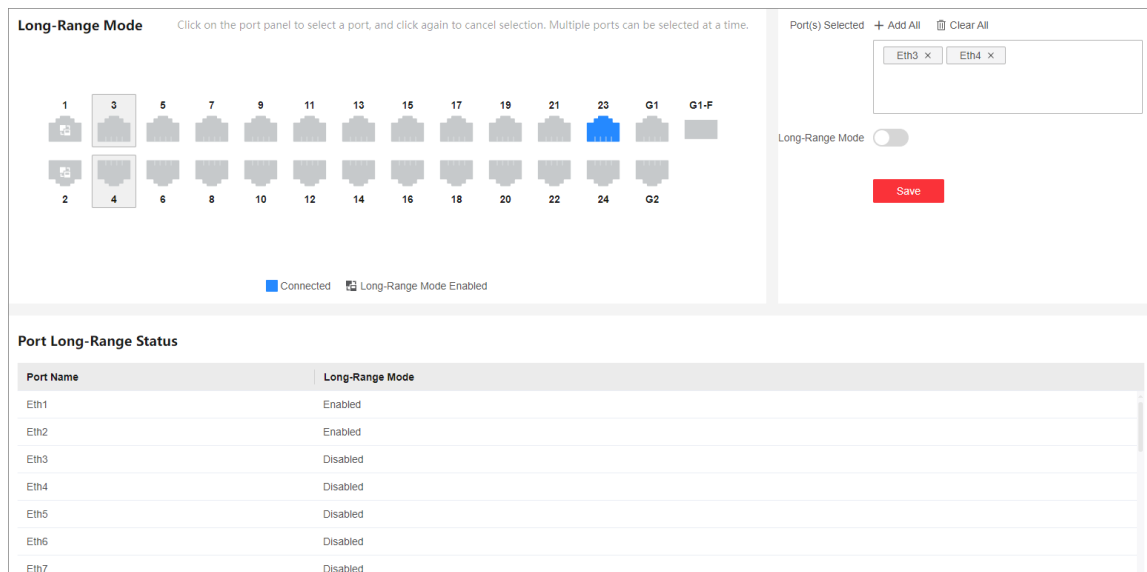


図4-5 長距離モードの設定

2. ポートパネルで希望のポートを選択します。



また、クリックすることもできます。または をクリックして、すべてのポートをまとめて選択または選択解除できます。

3. 必要に応じてロングレンジモードを有効または無効にします。
4. 保存をクリックしてください。
5. オプション: 各ポートのロングレンジ状態をポート ロングレンジ状態リストで確認できます。

### 4.1.6 高優先度ポートを設定します。

高優先度のポートは、デバイス前面パネルの赤い領域で識別されます。アップリンクの混雑が発生した場合、この領域内のポートのデータが優先的に送信されます。

#### 手順

1. サービス品質→高優先度へ移動します。



高優先度ポートの設定は、スイッチに高優先度ポートが搭載されている場合のみサポートされます。

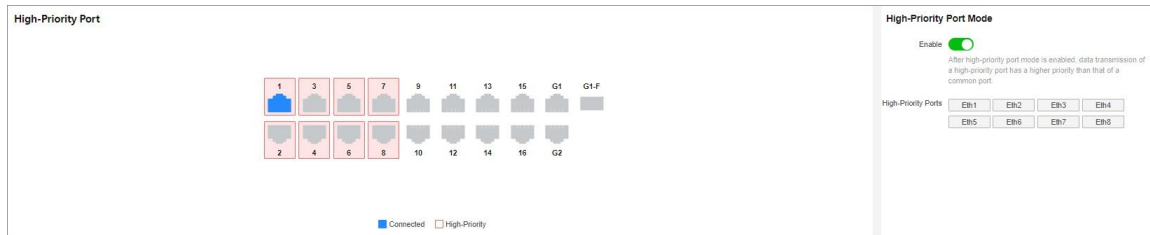


図4-6 高優先度ポートの設定

2. 高優先度ポートモードでは、**[有効]** をオンに切り替えて、高優先度ポートをバッチで有効にします。



高優先度ポートの数は、デバイスモデルによって異なります。実際の状況をご確認ください。

スイッチのすべての高優先度ポートは有効化されており、一般的なポートよりも高いデータ伝送優先度を持っています。

## 4.2 PoE設定

左側のナビゲーション パネルで「**PoE 管理**」をクリックします。

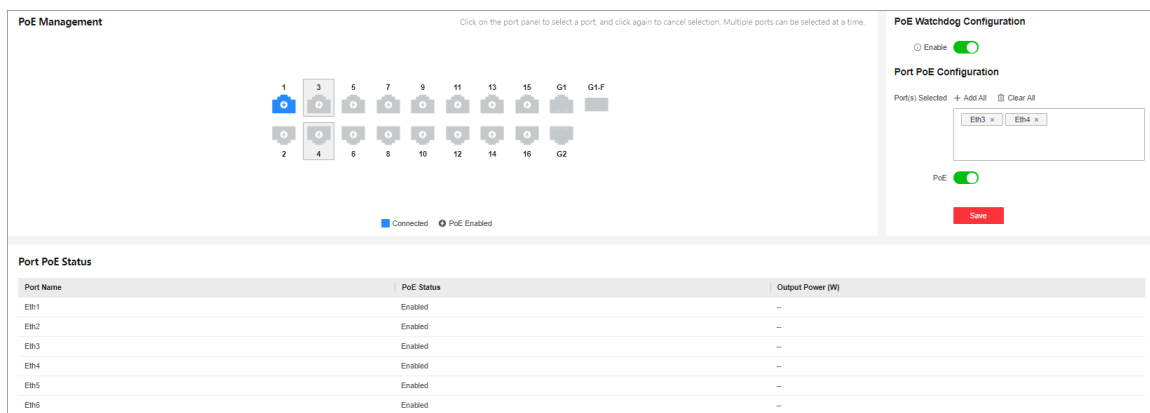


図4-7 PoEの設定

### PoE ウォッチドッグ

PoE ウォッチドッグを有効にすると、応答しない IP カメラを自動検出および再起動します。

### ポート PoE 設定

ポートパネルで希望のポートを選択し、**PoE**を有効にして、そのポートに接続された電源供給対象デバイスに電源を供給します。



クリックできま  ま  をクリックして、すべてのポートをまとめて

## PoE ステータス

ポートのPoEステータス一覧で、PoEポートのPoE有効状態と出力電力を表示します。

## 4.3 VLAN設定

仮想ローカルエリアネットワーク（**VLAN**）は、既存の物理ネットワークを複数の論理ネットワークに分割します。これにより、各**VLAN**は独自のブロードキャストドメインを作成します。スイッチに**VLAN**が設定されると、同じ**VLAN**内のユーザーは相互に通信でき、異なる**VLAN**内のユーザーは隔離されます。この **way**、異なるブロードキャストドメインが隔離され、ネットワークのセキュリティが強化されます。

### 4.3.1 VLANを追加

#### 手順

1. 左のナビゲーションパネルで「**VLAN 管理**」をクリックします。
2. グローバル**VLAN**設定で「**編集**」をクリックします。
3. 「**追加**」をクリックします。

	VLAN ID
<input type="checkbox"/>	1

図4-8 VLANの追加

4. 追加モードを選択します。
  - **単一**: 一度に1つの**VLAN**のみを追加します。
  - **バッチ**: 複数の**VLAN**をバッチ単位で追加します。



バッチで追加できる**VLAN**の最大数は、デバイスモデルによって異なります。実際の状況をご確認ください。

5. **VLAN ID**を設定します。
  - **単一**: **VLAN ID**を入力します。
  - **バッチ**: 開始**VLAN ID**と終了**VLAN ID**を入力します。





- VLAN IDは、デバイスで許可されている最大VLAN数以内の整数でなければなりません。例えば、最大VLAN数が4094の場合、VLAN IDは1から4094までの整数でなければなりません。
- 終了VLAN IDは開始VLAN IDよりも大きい必要があります。
- バッチで追加するVLANの数は、バッチで追加可能な最大VLAN数を超えてはなりません。例えば、バッチで追加可能な最大VLAN数が128の場合、開始VLAN IDを1に設定した場合、終了IDは128を超えてはなりません。

6. 保存をクリックします。

7. オプション：削除したいVLANを選択し、削除をクリックして1つまたは複数のVLANを削除します。



デフォルトのVLAN 1は削除できません。

## 4.3.2 ポート VLAN を設定

手順

1. ポートパネルで対象のポートを選択します。



- 右側の「+ Add All」または「Clear All」をクリックすると、すべてのポートをまとめて選択または選択解除できます。
- アグリゲーショングループ内のポートではVLAN設定は許可されていません。

2. ポートのVLANタイプを設定します。

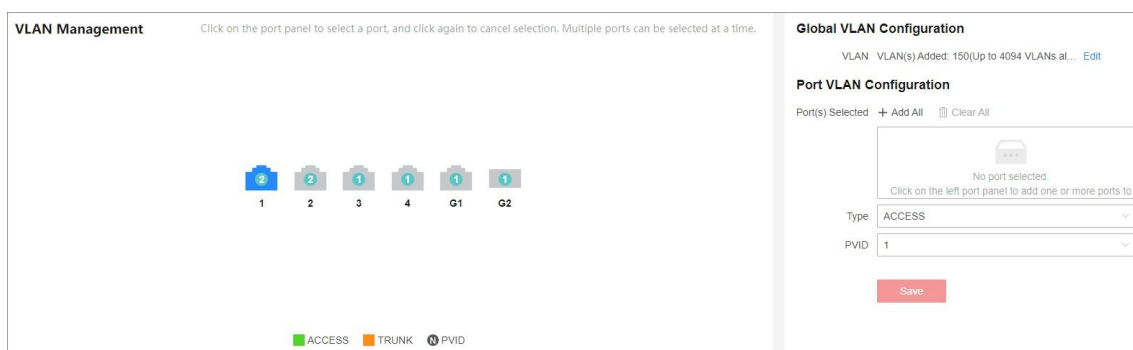


図4-9 ポートVLANの設定

- **ACCESS:** ACCESSポートは、インターフェースに1つのVLANのみを設定でき、通常はデフォルトのVLAN (VLAN 1) のトラフィックのみを転送できます。タイプをACCESSに選択し、PVIDを設定します。
- **TRUNK:** TRUNKポートには、インターフェースに2つ以上のVLANを設定でき、複数のVLANのトラフィックを同時に転送できます。タイプをTRUNKに選択し、PVIDを設定し、アクセス可能なVLANを入力します。

3. 保存をクリックします。

4. オプション: ポート VLAN 詳細リストで各ポートの VLAN 設定情報を表示します。

Port VLAN Details			
Port Name	Type	PVID	Accessible VLANs
Eth1	ACCESS	1	1
Eth2	ACCESS	1	1
Eth3	ACCESS	2	2
Eth4	ACCESS	2	2
Eth5	ACCESS	1	1
Eth6	ACCESS	1	1

図4-10 ポートVLAN詳細

## 4.4 STP 設定

スパニングツリープロトコル（STP）は、ネットワークトポロジにおけるパス冗長性を提供し、ループを防止するレイヤー2のリンク管理プロトコルです。STPはスパニングツリーアルゴリズムを使用して、スパニングツリーのルートとなるスイッチを1つ選択し、デバイス間でブリッジプロトコルデータユニット（BPDU）パケットを送信することでネットワークトポロジを決定し、安定したネットワークの構築を支援します。

### 手順

1. L2設定に移動し、→ STP を選択します。

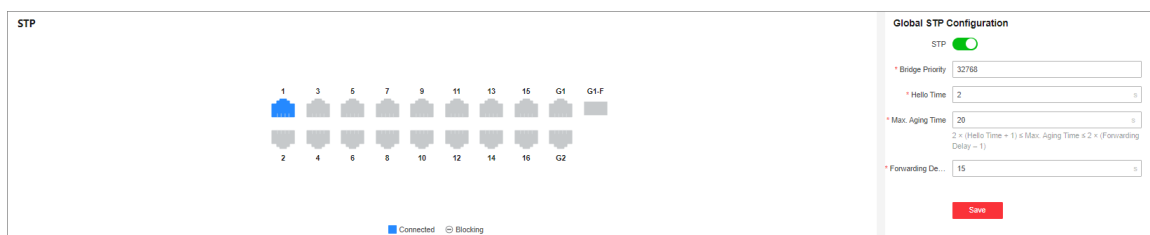



図4-11 STPの設定

2. グローバルSTP設定で、STPを有効にします。

3. 必要に応じてSTPパラメーターを設定します。

表4-1 STP パラメーター

パラメーター	説明
ブリッジ優先度	<ul style="list-style-type: none"> <li>値の範囲は0から61440で、4096ずつ増加します。デフォルト値は32768です。有効な値は0、4096、8192、12288、16384、...です。 61440.</li> <li>値が小さいほど、スイッチのブリッジ優先度が上昇します。ブリッジ優先度が高いスイッチは、ルートブリッジになる可能性が高くなります。</li> </ul>
Hello Time	ポート上で送信される各BPDUの間隔で、ポートのリンク状態を診断するために使用されます。値の範囲は1秒から10秒で、デフォルト値は2秒です。
最大エイジング時間	<p>STP有効ポートが構成BPDU情報を保存する最大時間間隔です。値の範囲は6秒から40秒です。デフォルト値は20秒です。</p> <p> 注</p> <p>最大エイジング時間は、以下の条件を満たす必要があります：<math>2 \times (\text{Hello Time} + 1) \leq \text{Max. Aging Time} \leq 2 \times (\text{Forwarding Delay} - 1)</math></p>
転送遅延	トポロジが変更された際に、リスニングと学習状態に費やされる時間間隔です。値の範囲は4秒から30秒です。デフォルト値は15秒です。

4. 保存をクリックします。

5. オプション：ポートの状態またはSTPの状態をクリックして、各ポートのSTP状態またはグローバルSTP設定を確認できます。



- ポート状態情報には、ポート名、パスコスト、ポート役割、およびポート状態が含まれます。
- STP ステータス情報には、ブリッジ ID、ルートブリッジ ID、およびルートブリッジの Hello 時間、最大エイジング時間、転送遅延が含まれます。

## 4.5 LLDP 設定

リンク層発見プロトコル（LLDP）は、デバイスが直接接続されたピア/ネイバーにデバイス情報を広告するレイヤー2のネイバー発見プロトコルです。LLDPを有効にすると、ネットワークデバイスはLLDPデータユニット（LLDPDU）を送信し、他のデバイスに自身の状態を通知できます。LLDPはネットワークトポロジーの描画を支援し、ネットワーク内の不正な構成を検出します。

### 手順

1. L2設定に移動→ LLDP。

2. LLDPを有効または無効にします。

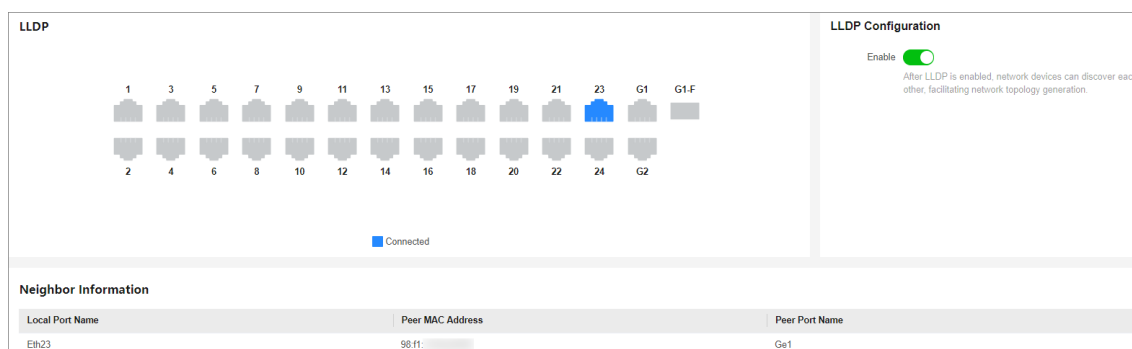


図4-12 LLDPの設定




注  
LLDPを有効にすると、ネットワークデバイスが相互に検出できるようになり、ネットワークトポロジーの描画が容易になります。

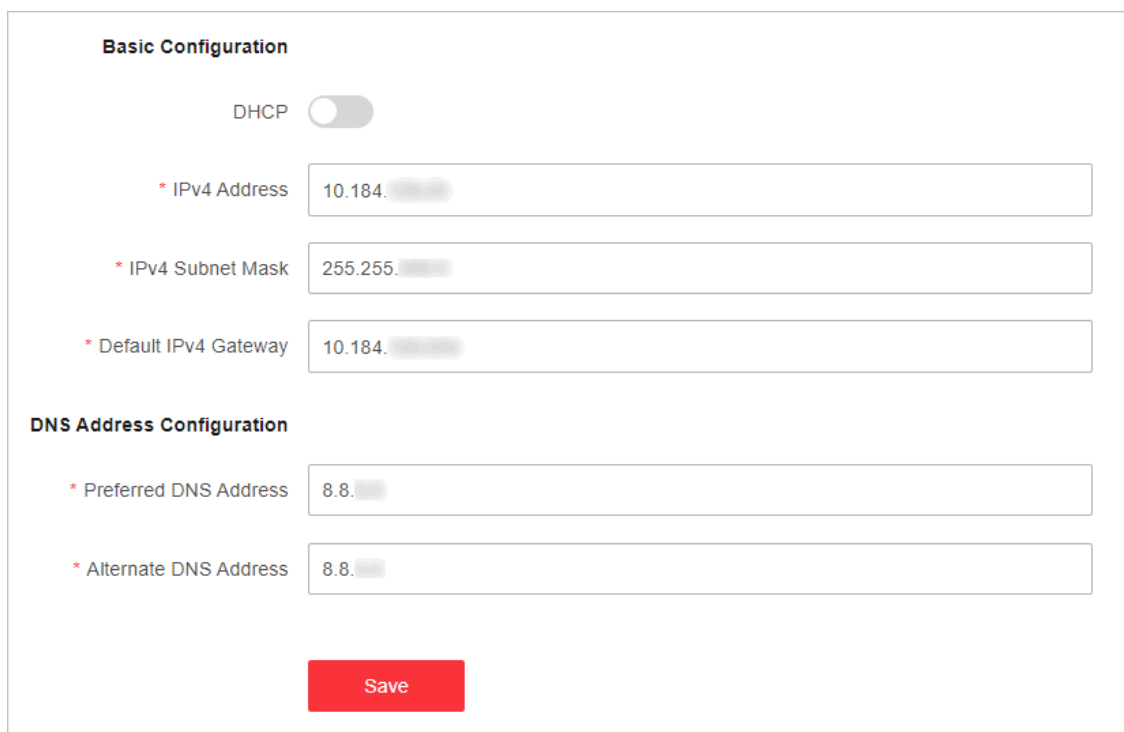
3. オプション: ピアデバイスのローカルポート、MACアドレス、およびピアポートを「Neighbor Information」リストで確認できます。

## 第5章 システム管理

### 5.1 ネットワーク設定

ホーム画面で「」をクリックしてHik-Connectの接続状態を確認するか、システム管理の「→ネットワーク設定」に移動して、ネットワーク設定、クラウドプラットフォーム設定、およびSADP設定を行うことができます。

#### ネットワーク設定



**Basic Configuration**

DHCP ☐

\* IPv4 Address 10.184.

\* IPv4 Subnet Mask 255.255.

\* Default IPv4 Gateway 10.184.

**DNS Address Configuration**

\* Preferred DNS Address 8.8.

\* Alternate DNS Address 8.8.

Save

図5-1 ネットワーク設定

必要に応じてIPv4アドレス、IPv4サブネットマスク、デフォルトのIPv4ゲートウェイ、優先DNSアドレス、代替DNSアドレスを設定するか、**DHCP**を有効にしてIPアドレスの自動割り当てを有効にします。

#### クラウドプラットフォーム設定

Hik-Partner Proにデバイスを追加した際にデバイスがオフライン表示される場合は、DNSサーバーアドレスを変更し、Hik-Connectパラメーターを設定する必要があります。

システム管理→ネットワーク設定→クラウドプラットフォーム設定に移動し、Hik-Connectが有効になっていることを確認してください。操作コードを確認することもでき、Hik-Partner Proアプリでデバイスをクラウドアカウントに紐付けることができます。

Enable ☒

\* Server Address  ☐ Customize

Network Connection Status ✓ Online [Refresh](#)

\* Operation Code

**Save**

**Account Binding Settings**

Account Status ✓ Cloud account bound.

If required, unbind the cloud account on Hik-Partner Pro app.

Account Binding Settings

**Binding via QR Code**

Scan the device QR code via Hik-Partner Pro app to bind your cloud account.

Device QR Code

[Click to View](#)

図5-2 クラウドプラットフォームの設定



Hik-Connect サービスへの再接続には数分かかる場合があります。

## SADP 設定

① SADP Server ☒

① SADP Agent ☐

**Save**

図5-3 SADPの設定

必要に応じて、**SADP サーバー**または**SADP エージェント**を有効にします。



- SADP サーバーを有効にすると、SADP 対応デバイスを検索し、デバイスの情報が表示されます。
- SADPエージェントが有効化されると、ネットワークポロジの描画のために、LANに対して定期的に（1分ごとに）クエリ要求が送信されます。

## リモート管理

システム管理に移動し、→ネットワーク構成→リモート管理を選択し、HTTPまたはHTTPS経由でリモートデバイスの管理を行います。

The screenshot shows a web interface for configuring remote management. It is divided into three main sections: HTTP, HTTPS, and SSH. In the HTTP section, there is a field for 'Port Number' with the value 80. The HTTPS section contains a toggle switch for 'HTTPS' which is currently turned on (green), a 'Port Number' field with the value 443, and a toggle switch for 'Redirect HTTP to HTTPS' which is turned off (grey). The SSH section has a toggle switch for 'SSH' which is turned off (grey). At the bottom of the form is a red button labeled 'Save'.

図5-4 リモートでのデバイス管理

- HTTP: ポート番号を設定し、保存をクリックします。



HTTP ポート番号は 2000 から 65535 の整数、またはデフォルトの 80 です。

- HTTPS: 必要なパラメーターを設定し、[保存]をクリックします。

### HTTPS

HTTPS を有効または無効にします。

### ポート番号

HTTPSが有効になっている場合、HTTPSのポート番号を設定します。



HTTPS ポート番号は、2000 から 65535 の整数、またはデフォルトの 443 です。

### HTTPをHTTPSにリダイレクト

HTTPをHTTPSにリダイレクトする機能を有効または無効にします。



HTTP を HTTPS にリダイレクトが有効の場合、ポート 80 経由でアクセスされたトラフィックは自動的にポート 443 にリダイレクトされます。

- SSH: SSHは技術サポートによる障害調査に使用され、ユーザーには利用できません。

## 5.2 タイムシンクロナイズ

### 手順

1. システム管理に移動し、→タイム設定 を選択します。
2. タイムゾーンを設定します。
3. 時間同期モードを設定します。
  - 手動: 日付と時間を手動で設定するか、コンピュータの時刻と同期するを選択してシステムの日付と時刻を同期します。

図5-5 手動で時間を設定する

- NTP サーバーを使用：自動的な時間同期のため、NTP サーバーのアドレス、ポート番号、および時間同期間隔を入力します。

図5-6 NTPサーバーを使用した時間設定

- Hik-Connect サーバーを使用：Hik-Connect サーバーを使用して自動的な時間校正と同期を行います。パラメーターの設定は不要です。



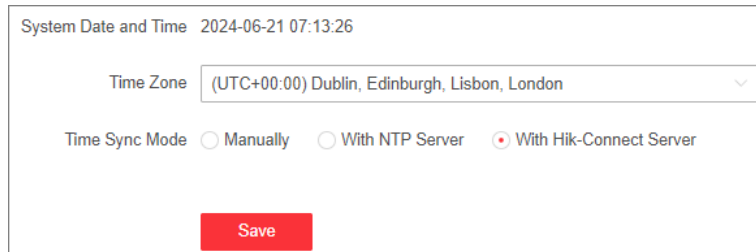


図5-7 Hik-Connect サーバーとの時間設定

4. 保存をクリックします。

## 5.3 システムメンテナンス

システム管理に移動します→システムメンテナンスで、デバイスの再起動、アップグレード、バックアップ、またはリセットを行います。

### デバイスの再起動

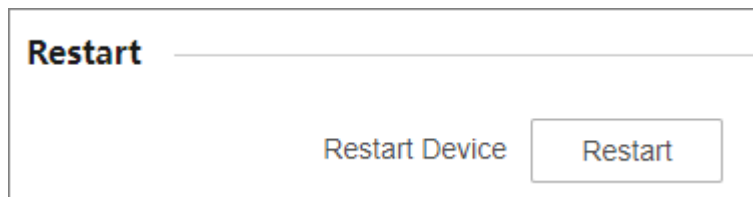


図5-8 再起動

再起動画面で、リモートでスイッチを再起動するには「再起動」をクリックします。




デバイスが再起動されると、自動的にログイン画面が表示されます。

### デバイスのアップグレード

アップグレードファイルをアップロードしてスイッチをアップグレードします。



図5-9 アップグレード

1. アップグレード画面で、[  ] をクリックしてアップグレードパッチファイルを選択します。
2. 「アップグレード」をクリックします。



- アップグレードに失敗した場合、またはデバイスが正常に動作しない場合は、当社の技術サポートエンジニアまでご連絡ください。
- アップグレードが完了すると、デバイスは自動的に再起動し、ログイン画面が表示されます。

### デバイスのバックアップ

設定ファイルをローカルにバックアップするためにエクスポートしてください。

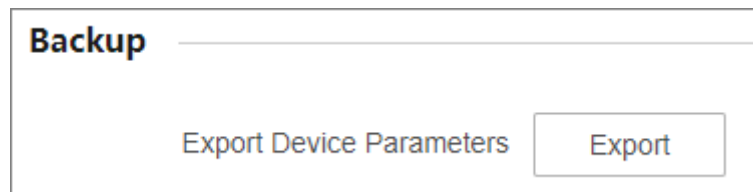


図5-10 バックアップ

1. バックアップ画面で「エクスポート」をクリックし、デバイスパラメーターを含む設定ファイルをエクスポートします。
2. ファイルの暗号化用にパスワードを設定し、パスワードを確認してください。



パスワードは、デバイスパラメーターのインポート時に必要になりますので、必ず覚えておいてください。

3. **OK**をクリックしてください。

### デバイスをリセット

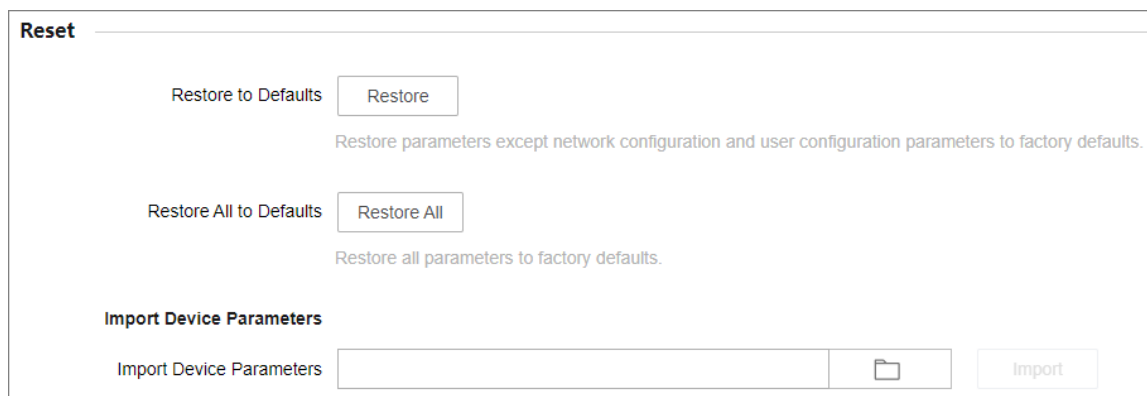


図5-11 リセット

- **デフォルトに戻す: [復元]** をクリックすると、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が工場出荷時のデフォルト設定に戻ります。
- **すべてをデフォルトに戻す: [すべてを復元]** をクリックすると、すべてのパラメーターが工場出荷時のデフォルト設定に戻ります。



注意

- 工場出荷時設定に復元すると、デバイスのパラメーターは復元できません。
- デバイスは工場出荷時設定に復元された後、自動的に再起動します。
- デバイスパラメーターのインポート:** **インポート** をクリックしてデバイスパラメーターを含む設定ファイルを選択し、**[インポート]** をクリックします。ファイルの復号化パスワードを入力し、**[OK]** をクリックして設定ファイルをインポートし、デバイスの設定を迅速に完了します。



注意

設定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、ログイン画面が表示されます。

## 5.4 ログ管理

システム操作ログを検索し、バックアップのためにエクスポートできます。

手順

1. システム管理→システムメンテナンス→ログ管理 へ移動します。

Major Type		Subtype		Date and Time			Search	Export
All		All		2000-01-01 00:00:00 - 2024-06-21 23:59:59				
No.	Operation Time	Major Type	Subtype	Remote Operator	Remote Host IP Address	Description		
01	2024-06-21 16:53:55	Operation	Remote User Login	admin	10.184.	(HTTP)		
02	2024-06-21 15:21:47	Operation	Remote User Login	admin	10.184.	(HTTP)		
03	2024-06-21 14:52:21	Operation	Remote User Login	admin	10.13.	(HTTP)		
04	2024-06-21 14:51:20	Operation	Remote User Login	admin	10.9.	(HTTP)		
05	2024-06-21 14:45:58	Operation	Remote User Login	admin	10.9.	(HTTP)		
06	2024-06-21 14:45:08	Operation	Remote User Login	admin	10.9.	(HTTP)		
07	2024-06-21 14:42:22	Operation	Remote User Login	admin	10.9.	(HTTP)		
08	2024-06-21 06:36:52	Operation	Remote User Login	admin	10.13.	(HTTP)		
09	2024-06-21 06:36:24	Event	Port Link Up	None	None	(Eth2)		
10	2024-06-21 06:36:19	Event	Port Link Down	None	None	(Eth1)		

図5-12 ログの管理

2. 検索条件を設定します（主要タイプ、サブタイプ、日付と時間を含む）。
3. 検索をクリックします。



注

検索結果は最大1024件まで表示できます。検索結果が多すぎる場合は、検索範囲を絞り込んでください。

4. オプション：すべての検索結果をエクスポートするには、**エクスポート** をクリックします。



注

ログはTXTファイルとしてエクスポートできます。ログのエクスポートが正常に完了すると、確認メッセージが表示されます。

