

IPS-4220-16GT-240

IPS-4228-24GT-360

WEBブラウザマニュアル






序文

一般



本書では、RTLスイッチ(以下、本装置)のWebインターフェースの操作方法について説明します。Webブラウザでスイッチにアクセスし、スイッチを設定および管理できます。

安全上の注意

定義された意味を持つ次のカテゴリ化されたシグナルワードがマニュアルに表示されることがあります。

シグナルワード	意味
 DANGER	回避しなければ、死亡または重傷につながる潜在的な危険性が高いことを示します。
 WARNING	回避しなければ、軽度または中程度の傷害を招く恐れがある、中または低の潜在的な危険を示します。
 CAUTION	回避しなければ、所有物の損傷、データの損失、パフォーマンスの低下、または予期しない結果を招く恐れがある潜在的なリスクを示します。
 TIPS	問題の解決や時間の節約に役立つ方法を提供します。
 NOTE	テキストの強調と補足として追加情報を提供します。

アイコン

アイコン/パラメーター	説明
	項目を編集します。
 または Delete	項目を1つずつ、またはまとめて削除します。
<input type="checkbox"/> または <input checked="" type="checkbox"/>	項目を1つずつまたは一括で有効または無効にします。
更新または自動更新	コンテンツを更新または自動更新します。

改訂履歴

バージョン	改訂内容	リリースタイム
23.12.Y.01	最初のリリース	2023年12月


マニュアルについて

- マニュアルは参照用です。マニュアルと製品で違いがある場合があります。
- 取扱説明書に準拠していない方法で製品を動作させたために発生した損失については、当社は責任を負いません。
- すべての設計とソフトウェアは、予告なく変更されることがあります。製品のアップデートにより、実際の製品とマニュアルで表示が異なる場合があります。最新のプログラムと補足ドキュメントについては、カスタマーサービスにお問い合わせください。
- デバイスの使用中に問題が発生した場合は、弊社のWebサイトにアクセスし、カスタマーサービスに連絡してください。


重要な安全対策と警告

ここでは、機器の適切な取り扱い、危険の防止、物的損害の防止について説明します。ご使用前によくお読みになり、使用上の注意事項を守ってください。

輸送要件

 デバイスは、できるだけ湿度と温度の下で輸送してください。

ストレージ要件

 デバイスは、許可された湿度および温度の条件下で保管してください。

インストール要件

 **WARNING**

- アダプタの電源が入っている間は、電源アダプタをデバイスに接続しないでください。



- 日光の当たる場所や熱源の近くに置かないでください。
- 本装置を湿気、ほこり、およびすすからの発生する環境に置かないでください。
- 装置を通気の良い場所に置き、通気を妨げないようにします。
- メーカー提供のアダプターまたはキャビネット電源を使用してください。
- デバイスの損傷を防ぐため、デバイスを2種類以上の電源に接続しないでください。
- 装置は、2.5mm²の断面領域を持ち、接地抵抗が4オーム以下の銅線で接地しなければなりません。
- 電圧安定器および雷サージ保護器は、現場の実際の電源および周囲環境に応じてオプションです。
- 熱の拡散を確実にするため、デバイスと周囲の領域との間のギャップは、側面が10cm未満、デバイスの上部が10cm未満にならないようにしてください。
- デバイスを取り付ける際は、電源プラグとアプライアンスカブラに簡単に届いて電源が切れることを確認してください。

動作要件

 **WARNING**

- 専門的な指示なしに装置を分解しないでください。
- 電源の入出力の定格範囲内でご使用ください。
- ご使用前に、電源が正しいことを確認してください。
- アダプタの電源が入っているときは、デバイス側面の電源コードを抜かないでください。



- デバイスは、許可された湿度および温度の条件下で使用してください。
- 液体をデバイスに落としたりしないでください。
- 新聞、テーブルクロス、カーテンなどの物で装置の換気口をふさがないようにしてください。

メンテナンス要件

 **WARNING**

- メンテナンス前にデバイスの電源をオフにしてください。
- メンテナンス回路図の主要コンポーネントに警告サインで印を付けます。

目次

序文.....	I
重要な安全対策と警告.....	II
1 ログイン.....	1
1.1 スイッチの初期化.....	1
1.2 ログイン.....	1
2 クイック設定(Quick Config).....	3
2.1 一般情報の設定 (General).....	3
2.2 ポート情報 (Port Info).....	4
2.3 ONVIF.....	5
2.4 IPC&NVR.....	6
3 メンテナンス (Maintenance).....	6
3.1 システム時刻の設定 (System Time).....	6
3.2 法的情報の表示 (Legal Info).....	6
3.3 パスワードの変更 (Change Password).....	7
3.4 ファームウェアの設定 (Firmware Config).....	7
3.5 ファイル管理 (File Management).....	8
3.6 デバイス情報の表示 (Deveice Info).....	8
4 ネットワーク設定 (Network Settings).....	11
4.1ポートの設定 (Port).....	11
4.2VLANの設定 (VLAN).....	12
4.2.1 VLAN定義.....	12
4.2.2 VLAN機能.....	13
4.2.3 ポートベースVLAN.....	13
4.2.4 VLANの追加 (Add VLAN).....	13
4.2.5 ポートVLANの設定.....	14
4.3 VLANの設定 (VLAN Interface).....	15
4.4 IPとルーティングの設定 (Routing Setting).....	16
4.5 IGMPスヌーピングの設定 (IGMP Snooping).....	17
4.6 STPの設定 (STP).....	17
4.6.1 STP.....	18
4.6.2 ポートインスタンス (Port Instance).....	19
4.7 リンク・アグリゲーションの設定 (Link Aggregation).....	19
4.8 SNMPプロトコルの設定 (SNMP).....	20
4.8.1 SNMP V1およびV2の設定.....	21
4.8.2 SNMP V3の設定.....	22
4.9 MACテーブルの設定 (MAC Table).....	23
4.9.1 MACテーブルの追加.....	23
4.9.2 フィルタリングポートMAC (MAC Filtering).....	24

4.10 LLDPの設定 (LLDP)	24
5 PoE管理 (PoE Management)	25
5.1 PoE設定の構成 (PoE Setting)	25
5.2 永続的PoEの設定 (Long Distance PoE)	エラー! ブックマークが定義されていません。
5.3 長距離PoEの設定 (PoE Event Statistics)	26
5.5 グリーンPoEの設定 (Green PoE)	27
5.6 強制PoEの設定 (Force PoE)	27
5.7 PoEウォッチドッグの設定 (PoE Watchdog)	28
6 セキュリティ (Security)	28
6.1 HTTPSの設定 (HTTPS)	28
6.2 CA証明書の設定 (CA Certificate)	29
6.2.1 デバイス証明書のインストール (Device Certificate)	29
6.2.2 信頼できるCA証明書のインストール (Trusted CA Certificates)	30
6.3 攻撃防御の設定 (Attack Defense)	30
6.3.1 ファイアウォールの設定 (Firewall)	30
6.3.2 DoS対策攻撃の設定 (Anti-Dos Attack)	31
6.4 隔離ポートの設定 (Port Isolation)	32
7 制御ポリシー (Control Policy)	32
7.1 ポートプライオリティの設定 (Port Priority)	32
7.2 プライオリティマッピングテーブルの設定 (Priority Mapping Table)	33
7.3 キュースケジューリングの設定 (Queue Scheduling)	34
7.4 ポート速度制限の設定 (Port Speed Limit)	34
7.5 ストーム制御の設定 (Storm Control)	35
8 認証 (Authentication)	35
8.1 802.1xの設定 (802.1x)	35
8.2 RADIUSの設定 (RADIUS)	36

1 ログイン

1.1 スイッチの初期化

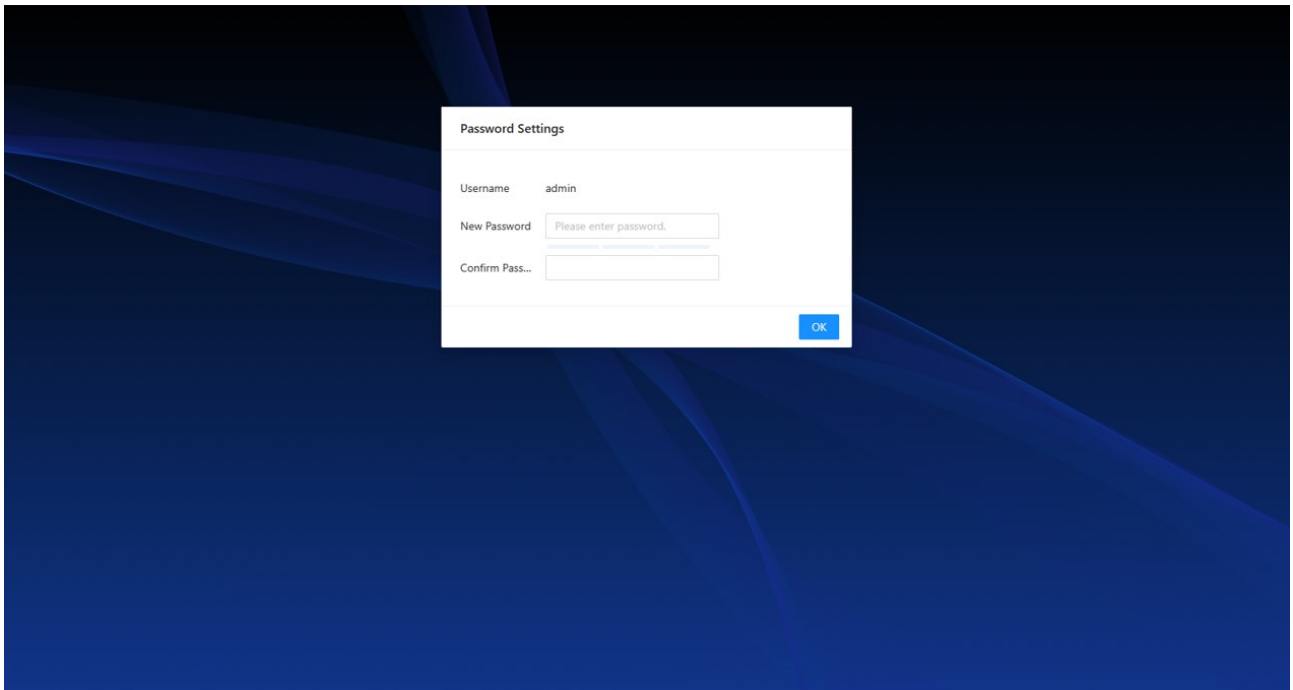
前提条件

ログインする前に、スイッチと設定デバイスが接続され、電源が入っていることを確認してください。

手順

ステップ1 IEブラウザを開き、WebブラウザのアドレスバーにスイッチのIPアドレス(デフォルトでは192.168.1.110)を入力し、Enterキーを押します。

ステップ2 パスワードを「New Password」「ConfirmPassword」欄に入力します。



ステップ3 OKをクリックします。

1.2 ログイン

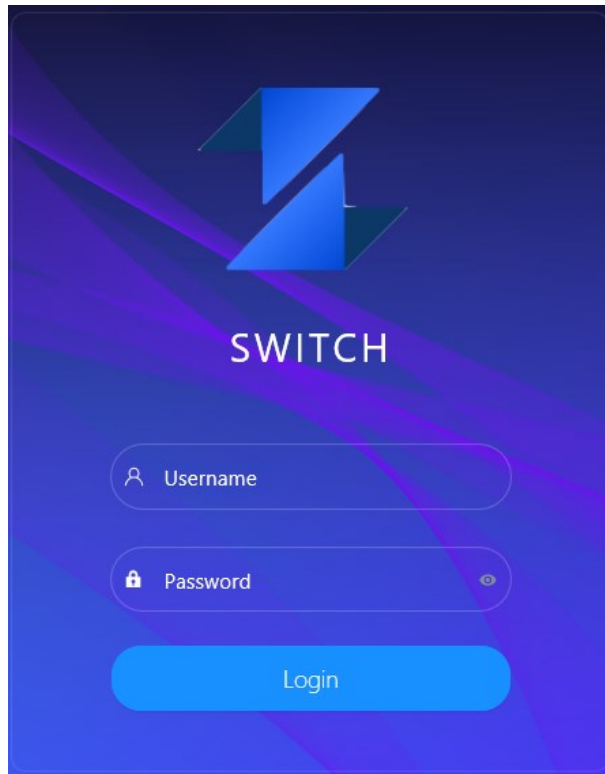
手順

ステップ1 WebブラウザのアドレスバーにスイッチのIPアドレス(デフォルトは192.168.1.110)を入力し、Enterキーを押します。

ステップ2 ユーザー名とパスワードを入力します。

ステップ3 ログインをクリックします。

図1-3ログイン



- 最初のログイン後にパスワードを変更します。パスワードは、8～32文字の非空白文字で構成し、大文字、小文字、数字、特殊文字(":",;, &を除きます)のうち少なくとも2種類の文字を含んでいる必要があります。
- パスワードの変更については、「4.3パスワードの変更」を参照してください。

図1-4ホームページ

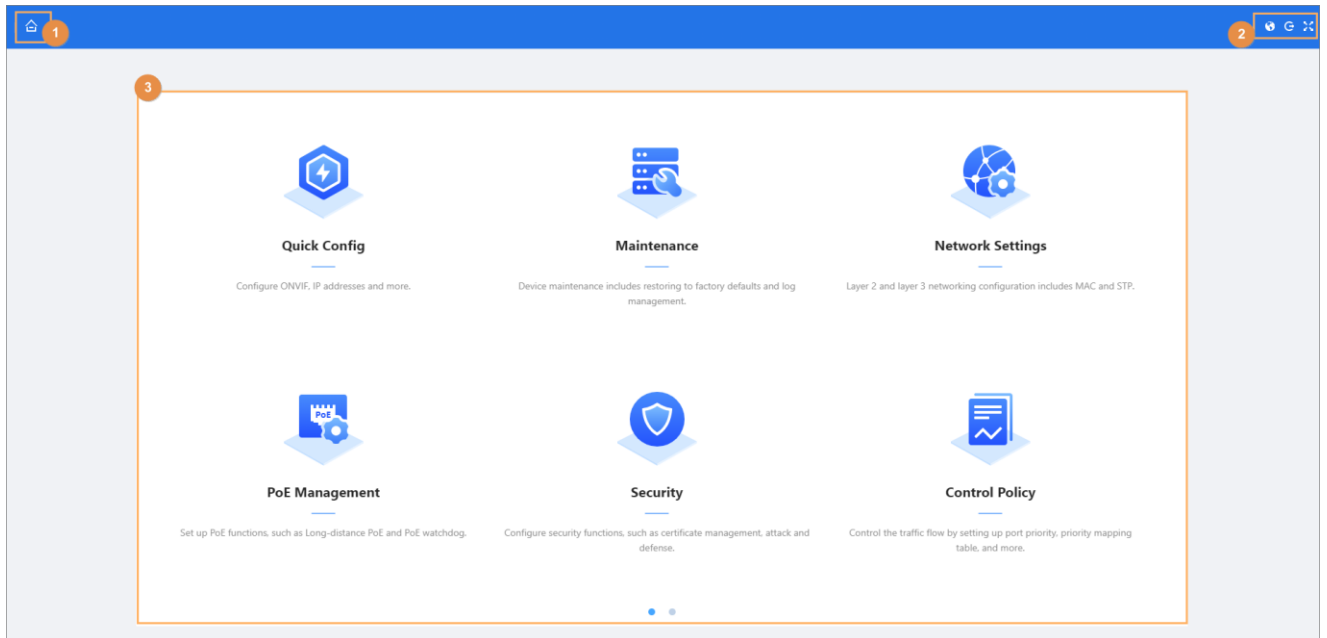






表1-1ホームページの説明

番号	名前	説明
1		ホームページに戻ります。
2		システム言語を切り替えます。複数の言語をサポート。
		ユーザーをログアウトしてから、ログインページに戻ります。

番号	名前	説明
		ホームページを全画面表示します。
	クイック設定	ONVIF、IPアドレスなどのクイック設定を行います。
	メンテナンス	工場出荷時のデフォルトへの復元やログ管理などのメンテナンス設定を行います。
	ネットワーク設定	MACおよびSTP設定を含むネットワーク設定を構成します。
	PoE管理	長距離PoEおよびPoEウォッチドッグを含むPoE設定を構成します。
	セキュリティ	証明書の管理、攻撃、防御などのセキュリティ設定を行います。
	制御ポリシー	ポートプライオリティ、プライオリティマッピングテーブルなどのトラフィックフロー設定を行います。
	認証	802.1xおよびRADIUSを含む認証管理を設定します。

2 クイック設定(Quick Config)

システム情報を表示し、ONVIF、IPアドレスなどのスイッチパラメータを設定できます。本書のページは参照専用であり、実際のページとは異なる場合があります。

2.1 一般情報の設定 (General)

名前、IPアドレス、サブネットマスク、デフォルトゲートウェイなどの一般情報を表示および設定できます。

手順

ステップ1 Quick Config>Generalを選択します。

ステップ2 スwitchの全般情報を表示および設定できます。

ステップ3 (DHCPにする場合は) をクリックして、DHCP機能を有効にします。


 この機能をお勧めします。DHCPを有効にすると、スイッチに接続されているルータまたはDHCPサーバが自動的にIPアドレスをスイッチに割り当てます。元のIPアドレスはWebページへのアクセスに失敗します。

図3-1一般情報

DHCP	<input type="checkbox"/>
Device Name	SWITCH
IP Address	192 . 168 . 1 . 110
Subnet Mask	255 . 255 . 255 . 0
Management ...	<input checked="" type="checkbox"/>
VLAN ID	1
<input type="button" value="OK"/> <input type="button" value="Refresh"/>	

表3-1 一般情報の説明

パラメーター	説明
DHCP	DHCPの有効化をサポートします。DHCPを有効にすると、新しいIPが自動的に取得され、割り当てられます。新しいIPが割り当てられる前に、デフォルトのIP192.168.1.110が採用されます。
デバイス名(DeviceName)	現在のデバイス名を表示します。名前の変更をサポートします。
IPアドレス(IPAddress)	現在のIPアドレスを表示します。手動設定をサポートします。
サブネットマスク(SubnetMask)	サブネットマスクの入力をサポートします。
管理対象VLAN(ManagementVLAN)	管理対象VLANを有効にすると、管理対象VLANからIP経由でのみWebページにアクセスできます。
VLAN ID	現在の管理対象VLAN IDを表示します。

2.2 ポート情報 (Port Info)

ポート、タイプ、リンクステータス、速度/二重化、VLAN、RX使用状況、TX使用状況、スイッチのメディアタイプなどの情報を表示できます。

手順

ステップ1 Quick Config>Port Infoを選択します。

ステップ2 スwitchのポート情報を表示します。

図3-2ポート情報

Port	Type	Link Status	Speed/Duplexing	VLAN	RX Usage	TX Usage	Media Type
1	Access	Down	Down	4094	0	0	Copper
2	Access	Down	Down	1	0	0	Copper
3	Access	UP	100M_Full	1	0	0	Copper
4	Access	Down	Down	1	0	0	Copper
5	Access	Down	Down	1	0	0	Fiber
6	Access	Down	Down	1	0	0	Fiber
7	Access	Down	Down	1	0	0	Fiber

表3-2ポート情報

パラメーター	説明
ポート(Port)	スイッチのすべてのポートを表示します。
説明(Description)	ポートの説明を設定します。大文字と小文字に関係なく、数字、文字、特殊文字()の入力をサポートします。16文字までの非空白文字を使用できます。デフォルトでは説明はありません。
型(Type)	Access、Hybrid、Trunkの3種類が含まれます。
リンクステータス(Link Status)	UpとDownの2つのステータスが含まれます。 ●Up:ポートが接続されます。 ●Down:ポートが接続されていないか、接続に失敗しています。
速度/二重化(Speed/Duplexing)	●オンライン:ポートレートとデュプレックスモードを表示します。 ●オフライン:下に表示します。
VLAN	VLANポート。 デフォルトのVLAN1。
RXの使用法(RX Usage)	受信時の使用状況を表示します。
送信時の使用状況(TX Usage)	送信時の使用状況を表示します。

パラメーター	説明
メディアタイプ (Media Type)	銅とファイバの2種類を含みます。 ●銅線:RJ-45ポート。 ●Fiber:ファイバーポート。

関連操作

- Refresh(更新)をクリックして、ポート情報を手動で更新します。
- 自動リフレッシュの横にある をクリックして、自動リフレッシュを有効にします。

2.3 ONVIF

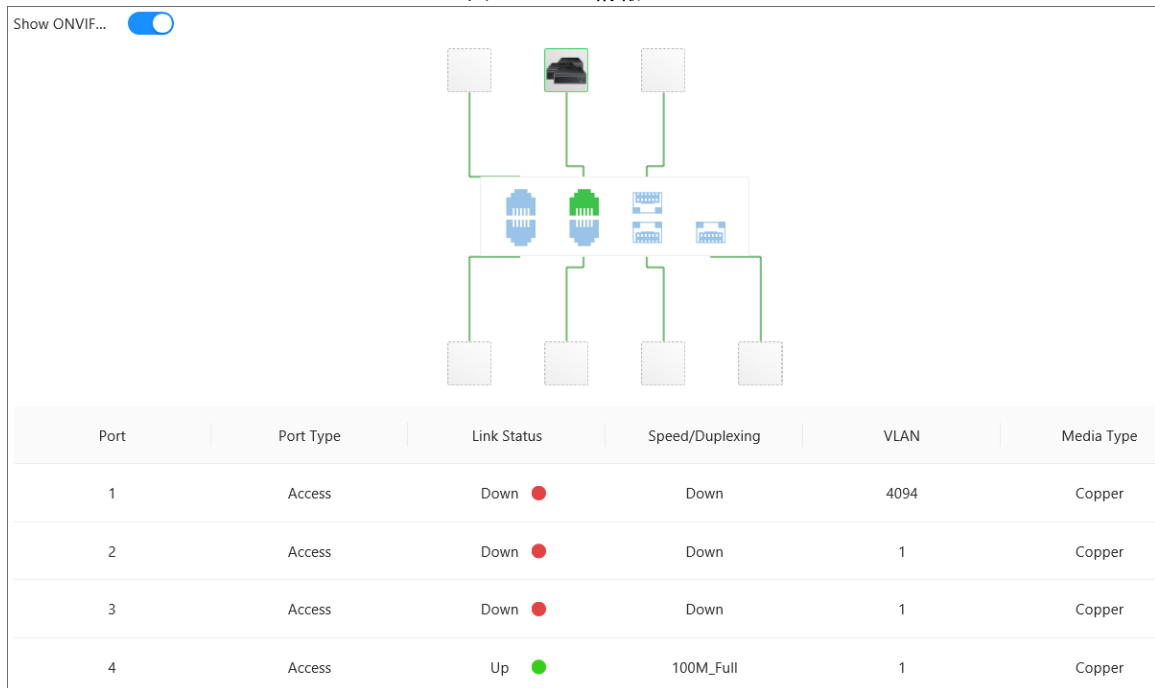
Quick Config>ONVIFを選択すると、デバイスのポート情報を表示できます。

をクリックするとONVIF表示機能が有効になります。有効にすると、ページにスイッチのすべてのポートと接続ステータスが表示されます。

- 緑色のポート:正常な接続を示します。
- 水色のポート:接続がないか、接続に失敗したことを示します。

 機種によって装備されるポートの数が異なります。次の図は参考用です。実際の製品を参照してください。


図3-3ONVIF情報



Port	Port Type	Link Status	Speed/Duplexing	VLAN	Media Type
1	Access	Down ●	Down	4094	Copper
2	Access	Down ●	Down	1	Copper
3	Access	Down ●	Down	1	Copper
4	Access	Up ●	100M_Full	1	Copper

表3-3ポートの説明

名前	説明
ポート(Port)	ポート番号を表示します。
ポートタイプ (Port Type)	Access、Hybrid、Trunkの3種類が含まれます。
リンクステータス (Link Status)	UpとDownの2つのステータスが含まれます。 ●Up:ポートが接続されます。 ●Down:ポートが接続されていないか、接続に失敗しています。
速度/二重化 (Speed/Duplexing)	●オンライン:ポートレートとデュプレックスモードを表示します。 ●オフライン:下に表示します。
VLAN	VLANポート。 デフォルトのVLAN1。

名前	説明
PoE	PoEの消費電力を表示します。  ●非PoEスイッチは、この機能をサポートしていません。 ●PoEポートの番号は、モデルによって装備されています。実際の製品を参照してください。
メディアタイプ (Media Type)	銅とファイバの2種類を含みます。 ●銅線:RJ-45ポート。 ●Fiber:ファイバーポート。

2.4 IPC&NVR

Quick Config>IPC&NVRを選択すると、スイッチに接続されているIPC、NVR、その他のデバイスの情報を表示できます。

3 メンテナンス (Maintenance)

3.1 システム時刻の設定 (System Time)

スイッチのシステム時刻を表示および設定できます。

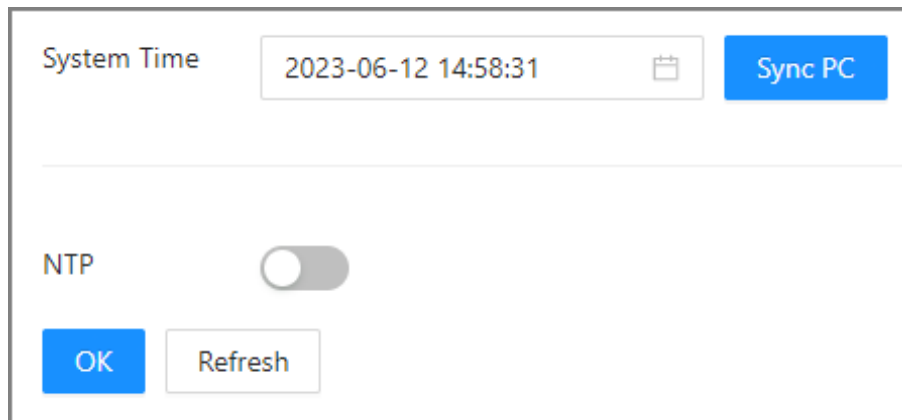
手順

ステップ1 Maintenance>System Timeを選択します。

ステップ2 システム時刻を設定します。3つの方法があります：

- システム時刻とタイムゾーンを手動で設定し、OKをクリックします。
- 「PCを同期」をクリックして、スイッチの時刻をコンピュータの時刻に同期させます。
- スイッチの時刻をサーバの時刻に同期する場合に をクリックします。

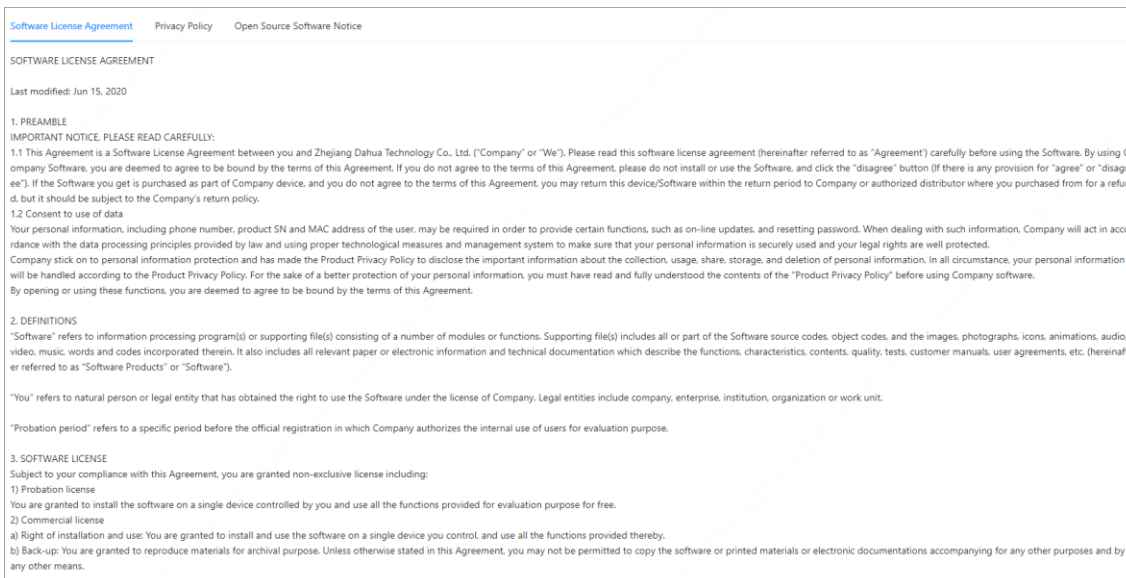
図4-1時間の構成



3.2 法的情報の表示 (Legal Info)

メンテナンス>法的情報を選択すると、オープンソースソフトウェア通知を表示できます。

図4-2法的情報



3.3 パスワードの変更 (Change Password)



- iLinksView機能を使用するには、iLinksViewプラットフォームとスイッチのユーザー名とパスワードが同じでなければなりません。
- ユーザー名はデフォルトでadminで、変更することはできません。

手順

- ステップ1** Maintenance>Change Passwordを選択します。
- ステップ2** 旧パスワード(Old Password)、新しいパスワード(New Password)および確認用パスワード(Confirm Password)を入力します。

パスワードは、8~32文字の非空白文字で構成し、大文字、小文字、数字、特殊文字("":&を除きます)のうち少なくとも2種類の文字を含んでいる必要があります。

- ステップ3** パスワード有効期限のリストでパスワードの有効期限を選択します。
パスワード有効期限は、無し、30日、60日、90日、および180日から選択できます。
- ステップ4** OKをクリックします。

3.4 ファームウェアの設定 (Firmware Config)

Maintenance>Firmware Configを選択すると、デバイスの復元、システムのアップデート、およびデバイスの再起動ができます。

工場出荷時のデフォルトに戻します(Restore Factory Default)

Restore Factory Defaultをクリックして、すべてのデバイスパラメータを工場出荷時のデフォルトに復元します。

VLAN1のIPアドレスを除くすべてのパラメータがデフォルト設定に復元されます。

ソフトウェアを更新します(Import Update File)

Browse(参照)をクリックしてアップデートファイルをインポートし、Update Now(今すぐアップデート)をクリックします。

ソフトウェアの更新には3分かかる場合があります。アップデート後、システムは自動的に再起動します。

デバイスの再起動(Device Restart)

今すぐ再起動(RestartNow)をクリックして、デバイスを再起動します。

図4-3ファームウェア構成

The screenshot shows a web interface for firmware configuration. At the top, there is a section for 'Restore Factory Default' with a 'Restore Now' button. Below this is a light blue box containing the text: 'Completely restore device parameters to factory default.' The next section displays 'System Version' with a blurred value and 'Security Baseline Version V2.2'. Below that is an 'Import Update File' section with a text input field, a 'Browse' button, and an 'Update Now' button. At the bottom, there is a 'Device Restart' section with a 'Restart Now' button.

3.5 ファイル管理 (File Management)

バックアップファイルとリストアファイルを設定できます。

バックアップ設定(Backup Config)


今後の参照用にログをバックアップすることをお勧めします。

Maintenance>File Management>Backup Configを選択し、Export Configuration Fileをクリックしてファイルをエクスポートします。

復元設定(Config Restore)

今後の参照用にログをバックアップすることをお勧めします。

Maintenance>File Management>Config Restoreを選択し、Browseをクリックしてファイルを選択し、Import Configuration Filesをクリックしてファイルをインポートします。

 インポートされた設定は、以前の設定を上書きします。

3.6 デバイス情報の表示 (Deveice Info)

Maintenance>Device Infoを選択すると、System、Software、Hardware、Timeの情報を表示できます。

図4-4デバイス情報

System	
Device Name	SWITCH
Device Model	4 Ports PoE Switch
IP Address	[Redacted]
Software	
Software Version	1.001.0000000.2.R
Compile Date	2022-03-31
Hardware	
MAC	[Redacted]
SN	000000000000000000
Time	
System Time	[Redacted]
Operation Time	18 Days 22 hr 13 min 53 sec

3.7 ログ情報の参照 (Log)

デバイス操作のログ情報を表示できます。

今後の参照のために、キーログをサーバに同期できるように、ログ機能を有効にすることをお勧めします。

手順

ステップ1 maintenance>Logを選択します。

ステップ2 Time(時間)とタイプ(Type)を設定し、検索(Serch)をクリックします。

ステップ3 ログ情報を表示できます。

ログタイプには、エラー、警告、メッセージがあります。

図4-5ログ情報

No.	Time	Type	User	IP Address	Description
1	2023-06-12 15:23:43	Warning	System		Interface 1/1, PoE DC Load Disconnect.
2	2023-06-12 15:23:35	Warning	System		Interface 1/1, PoE DC Load Disconnect.
3	2023-06-12 15:23:28	Warning	System		Interface 1/1, PoE DC Load Disconnect.
4	2023-06-12 15:23:21	Warning	System		Interface 1/1, PoE DC Load Disconnect.
5	2023-06-12 15:23:14	Warning	System		Interface 1/1, PoE DC Load Disconnect.

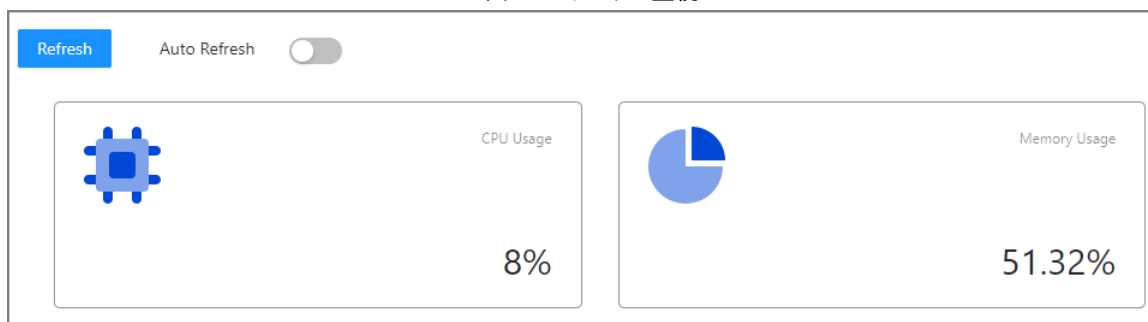
表4-1パラメータの説明

パラメーター	説明
バックアップ(Backup)	タップして検索したログをバックアップします。
ログバックアップを暗号化 (Encrypt Log Backup)	チェックボックスをクリックして、バックアップログを暗号化します。

3.8 ステータス監視 (Status Management)

Maintenance>Status Monitoringを選択すると、CPU使用量とメモリ使用量を表示できます。

図4-6ステータス監視



3.9 診断の表示 (Diagnosis)

手順

ステップ1 Maintenance>Diagnosisを選択します。

ステップ2 「送信先IP(DestinationIP)」を入力し、「パケットサイズ(Packet Size)」と「Ping回数(Ping Times)」を選択します。

ステップ3 Diagnoseをクリックします。

図4-7診断

The screenshot shows a form for configuring a diagnosis. It contains three input fields: 'Destination IP' (an empty text box), 'Packet Size' (a dropdown menu currently set to '64'), and 'Ping Times' (a text box set to '1' with '(1-10000)' to its right). At the bottom left of the form is a blue 'Diagnose' button.

3.10 ミラーリングの設定 (Mirror)

ミラーリングは、指定された送信元で送受信されたトラフィックまたはその両方を、分析のために宛先ポートにコピーします。指定されたソースはミラーソースと呼ばれ、宛先ポートはオブザベーションポートと呼ばれ、コピーされたトラフィックはミラートラフィックと呼ばれます。ミラーリングは、スイッチの監視ポートを介してトラフィックのコピーを監視デバイスに送信し、サービス分析を行います。

手順

ステップ1 Maintenance>Mirrorを選択します。

ステップ2 追加をクリックします。

ステップ3 Add Mirroring Groupページで、Mirroring Group No.、Mirroring Destination Portを選択し、実際の状況に応じてTX Only、RX Only、Bothから選択します。

ステップ4 OKをクリックします。

図4-8ミラーリンググループの追加

表4-2ソースポート(Source Port)の説明

名前	説明
送信のみ(TX)	トラフィックの送信のみをサポートします。
受信のみ(RX)	受信トラフィックのみサポートします。
両方(Both)	送信と受信の両方をサポートします。

関連操作

- クリックすると、ミラーリンググループの情報を編集できます。✎
- ミラーリンググループを削除するには、✖をクリックまたは削除します。

4 ネットワーク設定 (Network Settings)

4.1ポートの設定 (Port)

速度/二重化、フロー制御、およびその他のパラメータを含むポートパラメータを設定できます。ポートパラメータは、ポートの作業モードに直接影響します。実用的な要件に従って構成を行います。



Webページはデバイスによって異なる場合があります。実際のページを参照してください。

手順



- ステップ1 NetworkSettings>Portを選択します。
- ステップ2 パラメータを表示および設定できます。

図5-1ポート設定

Port	Description	Type	Link Stat...	Speed/D...	Speed/Duplexing	Flow Co...	RX Usage	TX Usage	Details
1	<input type="text"/>	Ethernet...	Down	Down	Auto <input type="button" value="v"/>	<input type="checkbox"/>	0	0	℄
2	<input type="text"/>	Ethernet...	Down	Down	Auto <input type="button" value="v"/>	<input type="checkbox"/>	0	0	℄
3	<input type="text"/>	Ethernet...	Down	Down	Auto <input type="button" value="v"/>	<input type="checkbox"/>	0	0	℄
4	<input type="text"/>	Ethernet...	UP	100M Full	Auto <input type="button" value="v"/>	<input type="checkbox"/>	0	0	℄
5	<input type="text"/>	Optical...	Down	Down	Auto <input type="button" value="v"/>	<input type="checkbox"/>	0	0	℄
6	<input type="text"/>	Optical...	Down	Down	Auto <input type="button" value="v"/>	<input type="checkbox"/>	0	0	℄
7	<input type="text"/>	Optical...	Down	Down	Auto <input type="button" value="v"/>	<input type="checkbox"/>	0	0	℄

OK Refresh

表5-1ポートパラメータ

パラメーター	説明
ポート(Port)	スイッチのすべてのポートを表示します。
説明(Description)	<p>ポートの説明を入力します。</p> <p> 説明は16文字を超えることはできません。数字、文字、および次の特殊文字のみが使用可能です。_。最初の文字は文字でなければならず、最後の文字は特殊文字であってはなりません。</p>
メディアタイプ (Media Type)	<p>2種類のメディアタイプを表示します。銅線とファイバーの2種類があります。</p> <ul style="list-style-type: none"> ● 銅線:イーサネットポート。 ● Fiber:光ポート。
リンクステータス (Link Status)	<p>UpとDownの2つのステータスが含まれます。</p> <ul style="list-style-type: none"> ● Up:ポートが接続されます。 ● Down:ポートが接続されていないか、接続に失敗しています。
速度/二重化状態 (Speed/Duplexing Status)	<ul style="list-style-type: none"> ● オンライン:ポートレートとデュプレックスモードを表示します。 ● オフライン:下に表示します。
速度/二重化 (Speed/Duplexing)	<p>速度とデュプレックスモードをDown、Auto、10M Half、10M Full、100M Half、100M Full、および1000M Fullから設定します。</p> <p> 速度/二重化は、コンボポートではAutoに設定されています。</p>
フロー制御 (Flow Control)	<p>クリックして機能を有効または無効にします。 <input type="checkbox"/></p>
RXの使用法 (RX Usage)	受信時の使用状況を表示します。
送信時の使用状況 (TX Usage)	送信時の使用状況を表示します。
詳細(Details)	<ul style="list-style-type: none"> ● 各ポートの合計RXと合計TXを表示します。各ポートの詳細情報を更新またはクリアできます。 ● エラーバイト数を表示します。

ステップ3 OKをクリックします。

4.2 VLANの設定 (VLAN)

4.2.1 VLAN定義

論理的には、1つのLAN(ローカルエリアネットワーク)を多くのサブセットに分割できます。各サブセットには、独自のブロードキャスト領域(仮想LAN(VLAN))があります。VLANは、物理的ではなく論理的にLANから分割され、VLAN内の分離されたブロードキャスト領域を実現します。

4.2.2 VLAN機能

- ネットワークのパフォーマンスを向上させます。ブロードキャストパケットはVLAN内にあり、ネットワークブロードキャストストームを効果的に制御し、ネットワーク帯域幅を削減し、ネットワーク処理能力を強化することができます。
- ネットワークセキュリティを強化します。異なるVLANのスイッチは相互にアクセスできず、異なるVLANのホストは相互に通信できません。彼らはメッセージを転送するためにルータか3層スイッチを必要とします。
- ネットワーク管理を簡素化します。同じバーチャル・ワーキング・グループのホストは、1つの物理的なエリアに限定されません。これにより、ネットワーク管理が簡素化され、異なるエリアのユーザのためのワーキング・グループの確立が容易になります。


4.2.3 ポートベースVLAN

ポートタイプには、アクセス、トランク、ハイブリッドがあります。

- アクセス:ポートは1つのVLANに属し、コンピュータポートへの接続に使用されます。
- Trunk:ポートは複数のVLANを通過させ、複数のVLANのメッセージを送受信し、スイッチ間の接続に使用されます。
- ハイブリッド:ポートは複数のVLANを通過させ、複数のVLANのメッセージを送受信し、スイッチ間の接続に使用され、コンピュータを接続します。

4.2.4 VLANの追加 (Add VLAN)

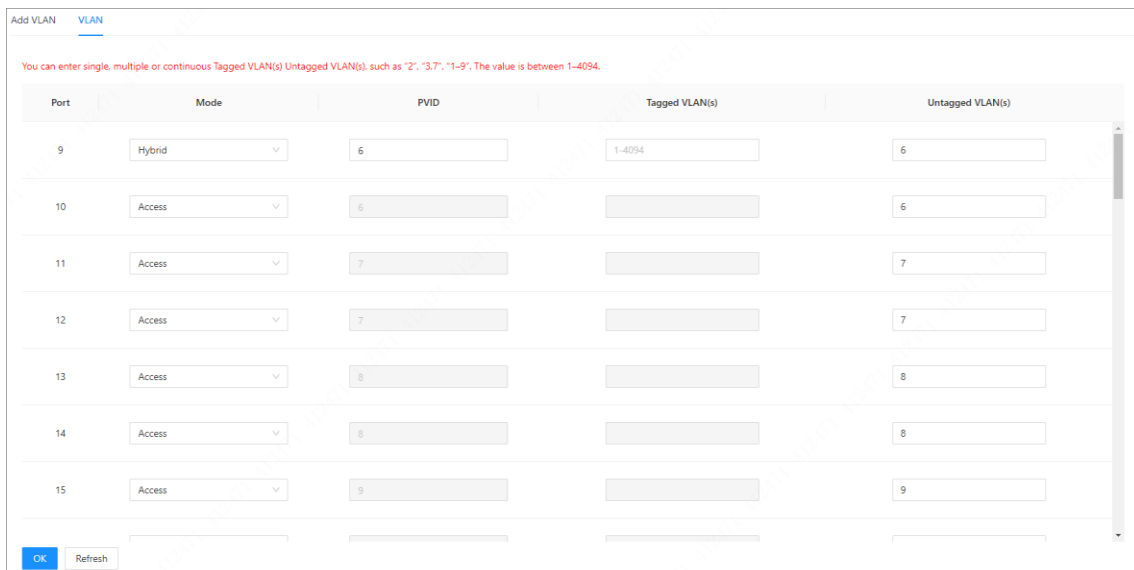
ポートをVLANに追加できます。VLANは、デフォルトではVLAN1です。

 隔離ポートとVLANを同時に有効にすることはできません。いずれかが有効になると、もう一方も自動的に無効になります。注意してください。

手順

ステップ1 NetworkSetting>VLANを選択します。

図5-3VLAN設定



Port	Mode	PVID	Tagged VLAN(s)	Untagged VLAN(s)
9	Hybrid	6	1-4094	6
10	Access	6		6
11	Access	7		7
12	Access	7		7
13	Access	8		8
14	Access	8		8
15	Access	9		9

ステップ2 Add VLAN(VLANの追加)ページで、Add(追加)をクリックし、VLAN IDと説明を入力します。

図5-4VLANの追加

ステップ3 OKをクリックします。

VLAN1は削除できません。

関連操作

- クリックしてVLANを編集します。
- クリックしてVLANを削除します。

4.2.5 ポートVLANの設定

ポートVLANパラメータを設定できます。

図5-5VLANの設定

表5-2ポートVLAN設定パラメータ

パラメーター	説明
ポート(Port)	スイッチのすべてのポートを表示します。

パラメーター	説明
モード(Mode)	アクセス、ハイブリッド、トランクの3つのモードがあります。 <ul style="list-style-type: none"> ●アクセス:1つのVLANに属します。コンピュータポートの接続に一般的に使用されます。 ●Trunk:複数のVLANの通過を許可します。複数のVLANパケットを送受信します。通常、スイッチ間の接続に使用します。 ●ハイブリッド:複数のVLANの通過を許可します。複数のVLANパケットを送受信します。スイッチ間、またはスイッチとコンピュータ間の接続に使用されます。
タグ付きVLAN (Tagged VLAN)	パケット送信時にタグ付けを許可するポートのVLAN IDを設定します。
タグ無VLAN (Untagged VLAN)	パケット送信時にタグなしを許可するポートのVLAN IDを設定します。

表5-3フレーム処理の比較

ポートタイプ	Untaggedフレーム処理	タグ付きフレーム処理	フレーム送信
アクセス (Access)	タグなしフレームを受信し、デフォルトVLAN IDのタグをフレームに追加します。	<ul style="list-style-type: none"> ●フレームのVLAN IDがデフォルトのVLAN IDと一致する場合、タグ付きフレームを受け入れます。 ●フレームのVLAN IDがデフォルトVLAN IDと異なる場合、タグ付きフレームを破棄します。 	PVIDタグが削除された後、フレームが送信されます。
トランク (Trunk)	<ul style="list-style-type: none"> ●デフォルトVLAN IDのタグをタグなしフレームに追加し、インターフェイスがデフォルトVLAN IDを許可する場合はフレームを受け入れます。 ●デフォルトVLAN IDのタグをUntaggedフレームに追加し、インターフェイスがデフォルトVLAN IDを拒否した場合はフレームを廃棄します。 	<ul style="list-style-type: none"> ●フレームで伝送されるVLAN IDがインターフェイスで許可されている場合、タグ付きフレームを受け入れます。 ●フレームで伝送されているVLAN IDがインターフェイスによって拒否された場合、タグ付きフレームを破棄します。 	<ul style="list-style-type: none"> ●フレームのVLAN IDがデフォルトのVLAN IDと一致し、VLAN IDがインターフェイスによって許可されている場合、デバイスはタグを削除してフレームを送信します。 ●フレームのVLAN IDがデフォルトのVLAN IDと異なりますが、VLAN IDがまだインターフェイスによって許可されている場合、デバイスはフレームを直接送信します。
ハイブリッド (Hybrid) ^ド			フレームのVLAN IDがインターフェイスによって許可されている場合、フレームは送信されず、タグ付きフレームを送信するかどうかを設定します。

4.3 VLANの設定 (VLAN Interface)

VLANインターフェイスは、異なるネットワークセグメント間の異なるVLANにあるホスト間のレイヤ3通信を実装するために最も一般的に使用されるレイヤ3論理インターフェイスです。

各VLANIFインターフェイスはVLANに対応します。VLANインターフェイスにIPアドレスが設定されると、VLANインターフェイスはそのVLAN内のユーザホストのゲートウェイとなり、レイヤ3のネットワークセグメント間でパケットを転送します。

手順

ステップ1 NetworkSetting>VLANInterfaceを選択します。

ステップ2 Add(追加)をクリックし、VLAN番号を入力し、Mode as Dynamic(ダイナミック)でポートのDHCPを有効にします。



DHCPを無効にすると、IPアドレスとマスク長を入力する必要があります。

図5-6VLANIFの追加

関連操作

- VLANを削除する:VLANを選択し、削除またはを クリックします。
- Refresh the parameter:Refreshをクリックして、VLANパラメータを更新します。

4.4 IPとルーティングの設定 (Routing Setting)

スイッチのIP設定とルーティング設定を紹介します。

手順

- ステップ1 NetworkSetting>RoutingSettingを選択します。
ステップ2 ルーティング設定タブで追加をクリックし、パラメータを設定します。

図5-7ルーティング設定

表5-4ルーティングパラメータの説明

パラメーター	説明
ネットワーク(Network)	IPパケットを識別する宛先アドレスまたは宛先ネットワークを入力します。
マスク長(Mask Length)	宛先アドレスを持つ宛先スイッチまたはルータを識別するセグメントを設定します。
ネクストホップ(Next Hop)	ルータのネクストホップアドレスを設定します。

関連操作

- ルーティングを削除する:VLANとルーティングを選択し、Delete(削除)またはを クリックします。

- Refresh the parameter: Refreshをクリックして、ルーティングのパラメータを更新します。

4.5 IGMPスヌーピングの設定 (IGMP Snooping)

IGMPスヌーピング(Internet Group Management Protocol Snooping)は、マルチキャストを管理および制御するために、レイヤ2のデバイスで実行されるマルチキャスト制約メカニズムです。受信したIGMPパケットを解析することにより、IGMP Snoopingを実行するレイヤ2の装置は、ポートとMACマルチキャストアドレス間のマッピングを作成し、マッピングに従ってマルチキャストデータを転送します。


手順

ステップ1 NetworkSetting>IGMPsnoopingを選択します。

ステップ2 IGMP Snoopingの横にあるを クリックして機能を有効にします。

ステップ3 「IGMP Leave Group Messages Drop Unknown Multicast Messages」の横の をクリックして、機能を有効にします。

- 機能を有効にする: 機能を有効にすると、スイッチは登録されていないグループメッセージを受信した場合、メッセージを残します。帯域幅が節約され、転送レートが増加します。
- 機能を無効にする: グループメッセージが登録されていない場合、メッセージはVLANにブロードキャストされます。帯域幅が占有され、転送レートが低下します。

 IGMP Leave Group Messages Drop Unknown Multicast Messagesを有効にすることをお勧めします。有効にしないと、マルチキャストが失敗する可能性があります。

ステップ4 Add(追加)をクリックし、パラメータを設定します。

図5-10 IGMPパラメータ



表5-7パラメータの説明

パラメーター	説明
VLAN	VLANの番号。
クエリア(Querier)	クリックして機能を有効にします。 <input type="checkbox"/>
アドレス検索(Search Address)	スイッチのIPアドレスを入力し、スイッチをクエリアとして設定します。

ステップ5 OKをクリックします。

4.6 STPの設定 (STP)

スパニングツリープロトコル(STP)は、LANのループフリーの論理トポロジを構築します。これは、任意の2つのネットワークデバイス間の冗長リンクをブロックし、ループを排除するために、それらの間に単一のアクティブリンクを残します。

STP、RSTP、およびMSTPは、次の機能を提供します:

- STP: データリンク層の管理プロトコルは、レイヤ2ネットワーク上のループを検出して防止するために使用されます。ただし、ネットワークトポロジはゆっくりと収束します。
- RSTP: STPの拡張により、ネットワークトポロジコンバージェンスが迅速に実現されます。ただし、RSTPとSTPの両方に、同じLAN上のすべてのVLANが同じスパニングツリーを共有するという欠陥があります。

- MSTP:VLAN IDがスパニングツリーインスタンスに関連付けられる仮想VLANマッピングテーブル。これだけでなく、MSTPはスイッチングネットワークを複数のリージョンに分割し、それぞれが相互に独立した複数のスパニングツリーインスタンスを持ちます。STPやRSTPとは異なり、MSTPはデータ転送用に複数の冗長パスを提供します。さらに、VLAN間のロードバランシングを実装します。

4.6.1 STP

 スパニングツリーが有効な場合、iLinkViewは使用できません。

手順

- ステップ1 NetworkSetting>STPを選択します。
- ステップ2 STPの横の をクリックして、STP機能を有効にします。
- ステップ3 WorkingMode(作業モード)を選択します。
- ステップ4 Advanced(詳細設定)をクリックしてから、詳細パラメータを設定します。

図5-11STPの設定

STP Port Instance

STP

Working Mode RSTP

▼ Advanced

Input Rules Max Aging Time ≥ (Hello Timer + 1) × 2
Max Aging Time ≤ (Forwarding Delay Time - 1) × 2

Hello Timer 2 s(1~10)

Max. Aging Time 20 s(6~40)

Forwarding Delay Time 15 s(4~30)

Bridge Priority 0 (0-61440)

OK Refresh

表5-8詳細パラメータの説明

パラメーター	説明
STP	基本的なスパニングツリープロトコル。
RSTP	STPの強化により、迅速なネットワークポロジコンバージェンスが可能になりました。
ハロータイマー (Hello Timer)	BPDUを送信するルートブリッジの周期。時間の範囲は1秒から10秒です。
最大エージングタイム (Max.Aging Time)	現在のBPDUのエージングタイム。時間の範囲は6秒から40秒です。
フォワードディレイタイム (Forwarding Delay Time)	トポロジ変更を設定した後、ブリッジはスヌーピングとスタディステートの時間を維持します。時間の範囲は4秒から30秒です。

パラメーター	説明
ブリッジプライオリティ(Bridge Priority)	値の範囲は0~61440です。

4.6.2 ポートインスタンス (Port Instance)

手順

ステップ1 NetworkSetting>STP>PortInstanceを選択します。

ステップ2 各ポートの優先度とルートパスコストを入力します。



- Priorityの値は0~240の範囲で、16の整数倍である必要があります。
- Priorityの値はデフォルトで128です。

図5-12ポートインスタンス

Port	Role	Status	Priority	Root Path Cost	Designated Bridge ID	Designated Port ID
1	Disabled Port	Discard	128	0	0000-000000000000	0
2	Disabled Port	Discard	128	0	0000-000000000000	0
3	Disabled Port	Discard	128	0	0000-000000000000	0
4	Disabled Port	Discard	128	0	0000-000000000000	0
5	Disabled Port	Discard	128	0	0000-000000000000	0
6	Disabled Port	Discard	128	0	0000-000000000000	0
7	Disabled Port	Discard	128	0	0000-000000000000	0

OK Refresh

表5-9ポートインスタンスのパラメータの説明

パラメーター	説明
役割(Role)	基本的なSTP。
ステータス(Status)	STPの強化により、迅速なネットワークポロジコンバージェンスが可能になりました。
優先順位(Priority)	ポートのプライオリティ。
ルートパス・コスト(Root Path Cost)	ポートのルートパスコスト。
指定ブリッジID(Designated Bridge ID)	ポートの指定ブリッジID。
指定ポートID(Designated Port ID)	ポートの指定ポートID。

4.7 リンク・アグリゲーションの設定 (Link Aggregation)

リンクアグリゲーションは、スイッチの複数の物理ポートを論理ポートに形成することです。同じグループ内の複数のリンクは、帯域幅が大きい論理リンクと見なすことができます。

集約により、同じグループ内のポートは通信フローを共有し、帯域幅を大きくすることができます。また、同じグループ内のポートを相互に動的にバックアップして、リンクの信頼性を高めることができます。



- リンク・アグリゲーションは、STPモード、IGMPスヌーピングおよび802.1xモードと相互に排他的です。STPモードが有効な場合、リンク・アグリゲーションは設定できません。リンク・アグリゲーションを設定する前にSTPモードを無効にする必要があります。
- リンクアグリゲーションに使用するポートには、コンフィグレーション機能と拡張機能を実装しないでください。
- リンクアグリゲーションは、スタティックアグリゲーションとLACPIに分割できます。一般的に、スイッチリンクアグリゲーションを持つピアデバイスは、スイッチとネットワークアダプタです。
- 1つの集約グループに設定できるのは、同じ速度、デュプレックス、ロングディスタンス、およびVLAN設定のポートのみです。

手順

- ステップ1** NetworkSetting>LinkAggregationを選択します。
- ステップ2** Add(追加)をクリックします。
- ステップ3** AggregationGroupNo.(集計グループNo.)を選択します。
- ステップ4** AggregationGroupMode(集約グループモード)を選択し、「OK」をクリックします。

集約グループモードには、Static(スタティック)、LACPActive(LACPアクティブ)、およびLACPPassive(LACPパッシブ)が含まれます。

- Static:Staticはマニュアルモードとも呼ばれます。Eth-Trunkインターフェイスは手動で作成する必要があり、メンバーインターフェイスは手動で追加する必要があります。LACPプロトコルは無効です。
- LACP active:Eth-Trunkインターフェイスを手動で作成し、メンバーインターフェイスを手動で追加する必要があります。スタティックと比較して、インターフェイスの選択はLACPプロトコルによって設定されます。このモードでは、インターフェイスがアクティブネゴシエーション状態になります。このモードでは、インターフェイスはLACPDUを送信することによって、他のインターフェイスとのネゴシエーションを開始します。
- LACP passive:Eth-Trunkインターフェイスが作成され、LACPプロトコルによってメンバーインターフェイスが追加されます。このモードでは、インターフェイスはパッシブネゴシエーション状態になります。このモードでは、インターフェイスは受信したLACPDUに応答しますが、LACPDUネゴシエーションを開始しません。

ステップ5 追加するポートを選択し、OKをクリックします。



- リンクアグリゲーションは、Aggregation Group ModeがLACPに設定されている場合にのみ設定できます。
- 値の範囲は1～65535です。

図5-13リンクアグリゲーション

Aggregation Group No.	Aggregation Group Mode	Port ID	Operation
2	Static	1,2,3,4,5,6,7,8	✎ ✖

4.8 SNMPプロトコルの設定 (SNMP)

SNMP(Simple Network Management Protocol)は、インターネットにおけるネットワーク管理の標準プロトコルであり、管理対象デバイスへのアクセスと管理に広く適用されています。SNMPには次の機能があります:

- ネットワークデバイスのインテリジェントな管理をサポートします。ネットワーク管理者は、SNMPをベースとしたネットワーク管理プラットフォームを利用することで、ネットワーク機器の稼働状況やパラメータを問い合わせ、パラメータの設定、エラーの発見、故障診断の実施、容量の計画、レポートの作成を行うことができます。
- SNMPは、さまざまな物理機能のデバイスを管理することをサポートします。SNMPは最も基本的な関数ライブラリのみを提供します。さまざまなメーカーのデバイスを管理するために、管理タスクと物理機能、および管理対象デバイスのネットワークテクノロジーを独立したものにします。

SNMPネットワークには、NMSとエージェントの2つの要素があります。

- NMS(Network Management System)は、SNMPネットワークのマネージャであり、ネットワーク管理者がネットワーク管理作業のほとんどを完了するのに役立つ、フレンドリーなヒューマンマシンインタフェースを提供します。

●エージェントはSNMPネットワークで管理された役割であり、NMSから要求パケットを受信して処理します。ポートのステータスが変化した場合など、緊急時には、エージェントはNMSに積極的にアラームパケットを送信できます。

4.8.1 SNMP V1およびV2の設定

SNMPは、TCP/IPネットワークで広く使用されている標準のネットワーク管理プロトコルです。ネットワーク管理システムで使用して、ネットワークに接続されているデバイスの例外を監視できます。

SNMPにはSNMPv1、SNMPv2c、SNMPv3の3つのバージョンがあります。

●SNMPv1:SNMPv1は、コンピュータネットワークを監視および管理する方法を提供するSNMPの初期バージョンです。コミュニティ名に基づいて認証を提供し、セキュリティレベルが低く、いくつかのエラーコードのみを返すことができます。

●SNMPv2c:SNMPv1と比較して、SNMPv2cには標準エラーコード、データ型、およびGet BulkやInformなどの操作が拡張されています。

●SNMPv3:SNMPv2cのセキュリティがまだ低下していることを確認するために、IETFはUSM(User Security Module)認証と暗号化を提供するSNMPv3と、データベースのアクセス制御モデル(VACM)をリリースしました。SNMPv3は、これまでで最も安全なバージョンです。

手順

ステップ1 NetworkSetting>SNMPを選択します。

ステップ2 SNMPバージョンを選択します。

●V1を選択すると、スイッチはSNMP V1の情報のみを処理できます。

●V2を選択すると、スイッチはSNMP V2の情報のみを処理できます。



サーバがスイッチにアクセスする必要がある場合、セキュリティ検証を完了するために、対応するユーザ名、パスワード、および認証タイプを設定する必要があります。また、V1およびV2バージョンは使用できません。

ステップ3 Read Community、Write Community、Trap Address、Trap Portなどのパラメータを設定します。

ステップ4 OKをクリックします。

図5-14SNMP

表5-10SNMPパラメータの説明(1)

パラメーター	説明
読み取りコミュニティ (Read Community)	ネットワーク管理者にアクセスするためのコミュニティ名。許可が読み取られます。デフォルトのセットアップはpublicです。

パラメーター	説明
書き込みコミュニティ (Write Community)	ネットワーク管理者にアクセスするためのコミュニティ名。許可はwriteです。デフォルトのセットアップはprivateです。
トラップアドレス (Trap Address)	サーバのIPアドレスを指定します。
トラップポート(Trap Port)	トラップ送信先ポートを設定します。
keep-aliveパケット送信	チェックボックスをクリックすると、この機能が有効になります。

4.8.2 SNMP V3の設定

手順

ステップ1 NetworkSetting>SNMPを選択します。

ステップ2 V3を選択します。

ステップ3 パラメータを設定します。

図5-15SNMP V3

V1
 V2
 V3 (Recommended)

Read Community

Write Community

Trap Address

Trap Port

Send Keep-alive Packet

Read-Only Username

Authentication Type MD5 SHA

Authentication Password

Encryption Type CBC-DES CFB-AES

Encryption Password

Read/Write Username

Authentication Type MD5 SHA

Authentication Password

Encryption Type CBC-DES CFB-AES

Encryption Password

表5-11SNMPパラメータの説明(2)

パラメーター	説明
読み取りコミュニティ (Read Community)	これらのパラメータの説明については、「SNMPパラメータの説明(1)」を参照してください。
書き込みコミュニティ (Write Community)	
トラップアドレス (Trap Address)	
トラップポート(Trap Port)	
keep-aliveパケット送信	
読み取り専用ユーザー名 (Read-Only Username)	読み取り専用ユーザー名を設定します。これはV3専用です。
認証タイプ(Authentication Type)	セキュリティレベルがAuthentication no encryptionまたはAuthentication and encryptionの場合に認証モードを設定します。認証モードにはMD5とSHAが含まれます。
認証パスワード(Authentication Password)	認証パスワードを設定します。
暗号化タイプ(Encryption Type)	認証モードがAuthentication and encryptionの場合に暗号化モードを設定します。
暗号化パスワード (EncryptionPassword)	認証モードがAuthentication and encryptionの場合の暗号化パスワードを設定します。
読み取り/書き込みユーザー名 (Read/Write Username)	読み出し/書き込みユーザを設定します。

ステップ4 OKをクリックします。

4.9 MACテーブルの設定 (MAC Table)

MAC(Media Access Control)テーブルは、MACアドレスとポートの関係、およびポートが属するVLANを含む情報を記録します。デバイスは、パケットを転送するときに、パケットの宛先MACアドレスをMACアドレステーブルで照会します。パケットの宛先MACアドレスがMACアドレステーブルに含まれている場合、パケットはテーブル内のポートを介して直接転送されます。また、パケットの宛先MACアドレスがMACアドレステーブルに含まれていない場合、デバイスはブロードキャストを採用して、VLAN内の受信ポートを除くすべてのポートにパケットを転送します。

4.9.1 MACテーブルの追加

特定のVLAN上のポートにMACアドレスをバインドできます。

手順

ステップ1 NetworkSetting>MACTableを選択します。

ステップ2 MACTableタブで、Add(追加)をクリックします。

ステップ3 MACアドレス、VLAN、ポートを設定します。たとえば、MACアドレス00:00:00:00:01をVLAN2のポート3にバインドします。

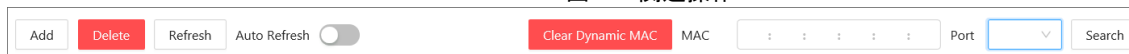
ステップ4 OKをクリックします。

図5-16MACテーブルの追加

The image shows a dialog box for adding a MAC entry. It has a title bar with a close button (X). The form contains three rows: 'MAC' with a text input field containing colons, 'VLAN' with a text input field, and 'Port' with a dropdown menu. At the bottom right, there are two buttons: 'Cancel' and 'OK'.

関連操作

図5-17関連操作




- 静的MACアドレスの削除:MACを選択し、Delete(削除)をクリックします。
- MACアドレスリストを更新する:Refresh(更新)またはAutoRefresh(自動更新)を有効にします。
- 動的MACアドレスのクリア:ClearDynamicMAC(動的MACのクリア)をクリックします。
- MACアドレスとポートを検索する:右上隅にMACアドレスまたはポート番号を入力し、Search(検索)をクリックします。

4.9.2 フィルタリングポートMAC (MAC Filtering)

ポートMACフィルタリングを有効にした後、次の2つのMACデバイスはポートと通信できません。

- MAC allowlistのデバイス。
- ダイナミックMACデバイスから変更されるスタティックMACデバイス。

 ポートMACフィルタリングを有効にした後、ポートは管理アドレスまたはログインにアクセスできません。

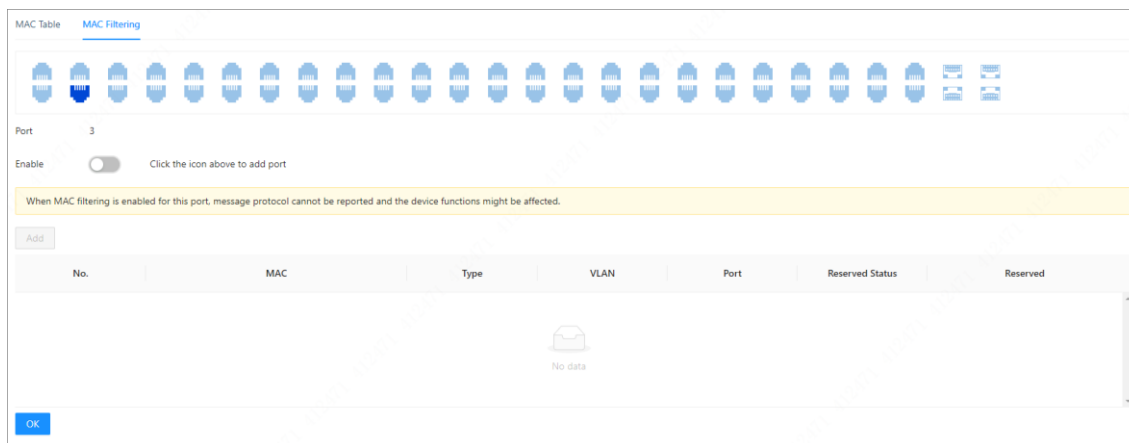
手順

- ステップ1 NetworkSetting>MACTableを選択します。
- ステップ2 MAC Filteringタブでポートを選択し、 をクリックしてフィルタリング機能を有効にします。
- ステップ3 ポートのMACフィルタリングを設定します。

- 動的から静的に変更します。
 - 1.1つのレコードを選択し、予約の横にある を選択します。
 - 2.OKをクリックします。タイプが動的から静的に変わります。スタティックMACデバイスは、ポートと正常に通信できます。

- MAC allowlistを作成します。
 - 1.Add(追加)をクリックします。
 - 2.MACアドレスとVLANを設定します。
 - 3.OKをクリックします。

図5-18MACフィルタリング



4.10 LLDPの設定 (LLDP)

LLDP(Link Layer Discovery Protocol)は、標準のリンク層検出方法です。主な機能、管理アドレス、デバイス番号、ポート番号をTLV(Type Length Value)として形成し、LLDPDU(Link Layer Discovery Protocol Data Unit)にカプセル化し、ネイバーに解放できます。ネイバーは、受信した情報を標準MIB(Management Information Base)の形式で保持し、ネットワーク管理者がリンクの通信状態を問い合わせる判断できるようにします。

手順

- ステップ1 ネットワーク設定>LLDPを選択します。
- ステップ2 LLDPリモートデバイスタブで、LLDPリモートデバイスの情報を表示します。

図5-19LLDPリモートデバイス

Local Port	Port ID	Port Description	System Name	System Capacity	Address Management
GigabitEthernet1/0/48	eth-0-36	eth-0-36	qwert	Bridge(+), Router(+)	

5 PoE管理 (PoE Management)

PoEとは、デバイスがネットワークケーブルを使用して、イーサネットの電気ポートを介してPD(Powered Device)にリモート電源を外部接続することを意味します。PoE機能により、集中電源と便利なバックアップが可能です。ネットワーク端末には外部電源は必要ありませんが、ネットワークケーブルは1本です。IEEE802.3af、IEEE802.3およびIEEE802.3bt標準に準拠し、デバイスはグローバルに統一された電源ポートを使用します。IP電話、ワイヤレスAP(アクセスポイント)、携帯充電器、クレジットカード機、ネットワークカメラ、データ収集に使用できます。

- 非PoEスイッチは、この機能をサポートしていません。
- PoEスイッチの一部のモデルのみがIEEE802.3at規格に準拠しています。シングルBTポートは最大90Wをサポートします。実際の製品を参照してください。

5.1 PoE設定の構成 (PoE Setting)

PoE Management>PoE Settingsを選択すると、電源設定、電源ステータス、ポートステータス、および制御を設定できます。


手順

- ステップ1** PowerSetting(電源設定)では、4つのポートの合計電力を表示し、予約電力とアラート電力を設定できます。
- ステップ2** Power Status(電源状態)では、消費電力、残り電力、および予約電力を表示できます。
- ステップ3** Port Status and Control(ポートステータスと制御)で、PoE Management(PoE管理)の下のリストから選択して、対応するポートのPoEを有効または無効にします。
- ステップ4** OKをクリックします。

図6-1PoE設定


Port	Level	Consumed Power	PoE Management
1	-	0	Enable
2	-	0	Enable
3	-	0	Enable
4	-	0	Enable

表6-1PoEパラメータの説明

パラメーター		説明
電源設定 (Power Setting)	総電力(Total Power)	PoE電力の合計が表示されます。
	予約電源(Reserved Power)	予約PoE電力を設定します。
	アラート電源(Alert Power)	アラートPoE電力を設定します。
電源状態 (Power Status)	消費電力(Consumed Power)	すべてのポートが消費している現在のPoE電力を表示します。
	残りの電力(Remaining Power)	現在の残りPoE電力を表示します。
	予約電源(Reserved Power)	使用不可能なPoE電源。予約電力=総電力-過負荷電力。
ポートのステータスと制御	レベル(Level)	端末機器の電源レベルを表示します。電源レベルは0~8の範囲で、Hi-PoE電源の標準レベルは5+と表示されます。
	消費電力(Consumed Power)	対応するシングルポートで消費されている現在のPoE電力を表示します。
	PoE管理(PoE Management)	有効、無効から選択します。 ●Disable(無効)を選択すると、システムはPDに電源を供給したり、PDのために電力を予約したりしません。 ●「Enable」を選択すると、PoEポートはPoE電力過負荷になりません。そうでない場合、PoEポートのPoEを有効にすることはできません。  ●デフォルトでは、PoEはPoEポートで無効になっています。 ●PSE電力過負荷:すべてのポートの電力消費量の合計がPSEの最大電力を超えると、システムはPSEが過負荷と見なします。

5.2 長距離PoEの設定 (PoE Long Statistics)

長距離PoEを有効にすると、最大伝送距離は100mから250mに変化し、伝送速度は100Mbpsから10Mbpsに減少します。

 拡張モードでは、PoEポートの伝送距離は最大250mですが、伝送速度は10Mbpsに低下します。実際の伝送距離は、接続する機器の消費電力やケーブルの種類、状態により変化することがあります。

手順

- ステップ1 PoE Management>Long Distance PoEを選択します。
- ステップ2 対応するポートを クリックして、長距離PoEを有効にします。
- ステップ3 OKをクリックします。

図6-2長距離PoE

After long distance PoE is enabled, the maximum transmission distance will be increased from 100 meters to 250 meters, but the transmission speed will be reduced from 100 Mbps to 10 Mbps.

Port	<input type="checkbox"/> Long Distance PoE
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>
9	<input type="checkbox"/>
10	<input type="checkbox"/>
11	<input type="checkbox"/>

OK Refresh

5.3 PoEイベント統計の表示(PoE Event Statistics)

PoEイベント統計を表示するには、PoEマネジメント>PoEイベント統計を選択します。

表6-2PoEイベント統計情報の説明

パラメーター	説明
オーバーロード(Overload)	電力電流が現在のしきい値を超えると、シングルポートが起動します。
短絡(Short Circuited)	電源チップがポートに電力を送ると、ショート状態になります。
DC切断(DC Disconnection)	シングルポートパワーオフ。
起動時の短絡(Short Circuit During Startup)	電源チップが電力を送出する際に、電力が短絡しています。
過熱保護(Overheat Protection)	電源チップの温度がしきい値を超えると、シングルポートが起動します。

5.4 グリーンPoEの設定 (Green PoE)

Green PoEは、既存の機器との完全な互換性を保持しながら、消費電力を削減できます。

手順

- ステップ1 PoE Management>Green PoEを選択します。
- ステップ2 PoE On TimeとPoE Off Timeを設定します。
- ステップ3 ポートを選択し、 をクリックして緑色のPoEを有効にします。
- ステップ4 OKをクリックします。

図6-3緑色のPoE

PoE On Time	Sun	00:00:00
PoE Off Time	Sun	23:59:59
Port	Green PoE	
1	<input type="checkbox"/>	
2	<input type="checkbox"/>	
3	<input type="checkbox"/>	
4	<input type="checkbox"/>	
<input type="button" value="OK"/>		

5.5 強制PoEの設定 (Force PoE)

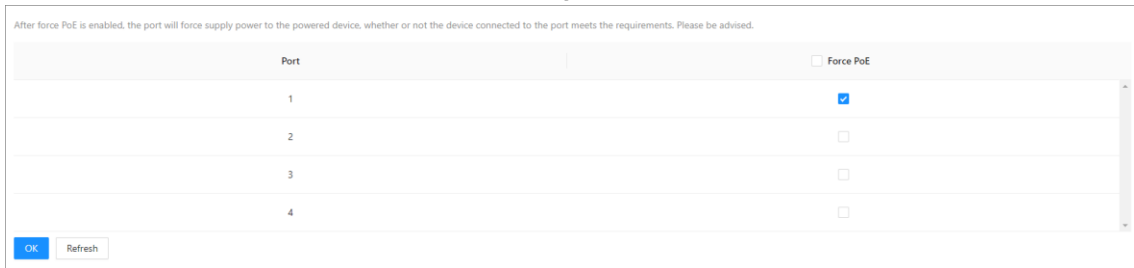


PoEを強制的に有効にすると、ポートに接続されているデバイスが要件を満たしているかどうかにかかわらず、ポートは強制的に電源を供給します。注意してください。

手順

- ステップ1 PoE Management>Force PoEを選択します。
- ステップ2 対応するポート をクリックして、PoEを強制有効にします。
- ステップ3 OKをクリックします。

図6-4強制PoE



5.6 PoEウォッチドッグの設定 (PoE Watchdog)

PoEウォッチドッグを有効にすると、PDを監視してオンライン状態を維持し、60秒ごとにPDデバイスのステータスを確認できます。データ送信がない場合、PoEポートは自動的に電源がオフになり、再起動します。

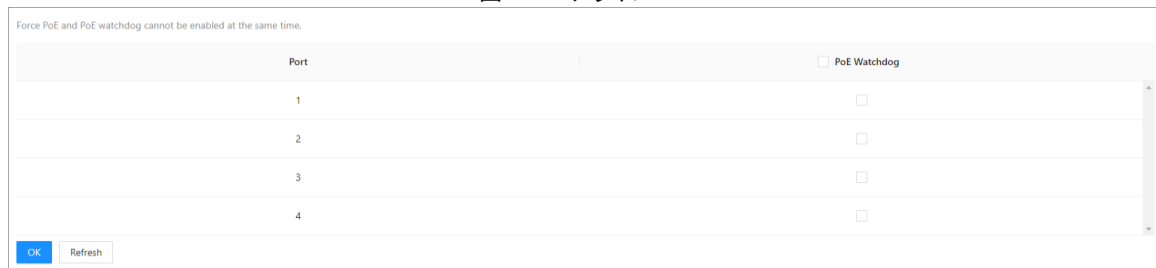


PoEとPoEウォッチドッグを同時に有効にすることはできません。

手順

- ステップ1 PoE Management>PoE watchdogを選択します。
- ステップ2 対応するポートを をクリックしてPoEウォッチドッグを有効にします。
- ステップ3 OKをクリックします。

図6-5PDアライブ



6 セキュリティ (Security)

6.1 HTTPSの設定 (HTTPS)

HTTPS(Hyper Text Transfer Protocol over Secure Socket Layer)は、Transport Layer Security(TLS)に基づくサービスエントリです。HTTPSはWebサービス、ONVIFアクセスサービス、RTSPアクセスサービスを提供します。

手順

- ステップ1 Security>HTTPSを選択します。
- ステップ2 HTTPSタブで、 をクリックしてHTTPSを有効にします。
- ステップ3 (オプション)必要に応じて をクリックしてTLS1.1を有効にし、OKをクリックします。



デフォルトでは、WebページはTLS1.2のみをサポートします。TLS1.1を使用する必要がある場合は、WebページでTLS1.1を有効にする必要があります。TLS1.1はセキュリティ上のリスクがあることをお勧めします。予期しないリスクを避けるために、TLS1.1を無効にすることをお勧めします。

- ステップ4 デバイス証明書を選択します。
- ステップ6 OKをクリックします。

図7-2HTTPSの設定

Enable

HTTPS is a service entry based on Transport Layer Security (TLS). HTTPS provides web service and ONVIF access service.

Compatible with TLSv1.1 and earlier versions

There might be security risks if TLS of earlier versions are enabled. Please select carefully.

Select a device certificate Certificate Management

No.	Custom Name	Certificate Number	Validity Period	User	Issued by	Used by
<input checked="" type="radio"/> 1		66346231633236643...	2049-12-19 09:01:15	192.168.1.110	General Device TS CA	HTTPS

OK Refresh Download Root Certificate

6.2 CA証明書の設定 (CA Certificate)

6.2.1 デバイス証明書のインストール (Device Certificate)

デバイス証明書は、デバイスの正当なステータスの証明です。例えば、ブラウザがHTTPS経由でデバイスを訪問している場合、デバイス証明書を検証する必要があります。

手順

- ステップ1 security>CACertificate>DeviceCertificateを選択します。
- ステップ2 DeviceCertificate (デバイス証明書) タブで、Install Device Certificate (デバイス証明書のインストール) をクリックします。
- ステップ3 必要に応じてインストールモードを選択します。

図7-3インストールモードの選択

Step 1: Select installation mode. ✕

Create Certificate

Fill in certificate information, and the device will create and issue the certificate.

Apply for CA Certificate and Import (Recommended)

After you fill in certificate information, the device will generate a certificate request file. Please submit the file to a CA institute to apply for a signature and certificate, and then import them into the device.

Install Existing Certificate

If you already have a certificate and private key file, please import the certificate and private key file in this way.

- ステップ4 証明書情報を入力し、証明書の作成とインストール、作成とダウンロード、インポートとインストールをクリックします。
- ステップ5 (オプション)編集モードに入るをクリックしてカスタム名を編集し、設定の保存をクリックします。

図7-4証明書の編集

No.	Custom Name	Certificate Num...	Validity Period	User	Issued by	Used by	Certificate Status	Download	Delete
1		323032313131...	2029-12-24 08:...	192.168.1.110	TS	HTTPS	Normal	📄	🗑️

関連操作

- 証明書をダウンロードする: 📄 をクリックします。
- 証明書を削除する: 🗑️ をクリックします。

6.2.2 信頼できるCA証明書のインストール (Trusted CA Certificates)

信頼できるCA証明書は、ホストの合法的なステータスを検証するために使用されます。たとえば、802.1x認証用にスイッチCA証明書をインストールする必要があります。

📖 下位CA証明書のインストールのみをサポートします。

手順

ステップ1 security>CACertificatesを選択します。

ステップ2 Trusted CA Certificates(信頼済みCA証明書)タブで、Install Trusted Certificate(信頼済み証明書のインストール)をクリックします。

ステップ3 Browse(参照)をクリックし、OKをクリックします。

図7-5信頼済み証明書のインストール

ステップ4 (オプション)編集モードに入るをクリックしてカスタム名を編集し、設定の保存をクリックします。

図7-6証明書の編集

No.	Custom Name	Certificate N...	Validity Period	User	Issued by	Used by	Certificate St...	Download	Delete
1		6364336236...	2030-10-17...	TS	TS		Expired	📄	🗑️

関連操作

- 証明書をダウンロードする: 📄 をクリックします。
- 証明書を削除する: 🗑️ をクリックします。

6.3 攻撃防御の設定 (Attack Defense)

6.3.1 ファイアウォールの設定 (Firewall)

手順

ステップ1 security>AttackDefenseを選択します。

ステップ2 Firewall(ファイアウォール)タブで、All(すべて)を選択します。

すべての送信元ホストIP/MACがすべてのデバイスポートにアクセスできます。

Allowlist(許可リスト)をクリックし、IP/MACが次のリストにある送信元ホストのみがデバイスの対応するポートにアクセスできます。Add(追加)をクリックして、allowlistにホストを追加します。

図7-7allowlistに追加

Blocklist(ブロックリスト)を選択すると、リストされているIPアドレス/MACの対応する送信元ホストが、ネットワーク接続によってデバイスの対応するポートにアクセスできなくなります。追加をクリックして、ホストをブロックリストに追加します。

図7-8ブロックリストに追加

表7-1ファイアウォール

パラメーター	説明
すべて(All)	すべての送信元ホストIP/MACは、すべてのデバイスポートへのアクセスを許可されます。
許可リスト(Allowlist)	IP/MACが以下のリストにある送信元ホストのみが、デバイスの対応するポートにアクセスできます。
ブロックリスト(Blocklist)	リストされている対応するIPアドレス/MACの送信元ホストは、デバイスの対応するポートにアクセスできません。

ステップ3 OKをクリックします。

6.3.2 DoS攻撃対策の設定 (Anti-Dos Attack)

手順

ステップ1 security>AttackDefenseを選択します。

ステップ2 Anti-DoS Attack(DoS攻撃対策)タブで  をクリックし、必要に応じて異なる防御機能を有効にします。

ステップ3 保存をクリックします。

図7-9アンチDoS攻撃

Firewall Anti-DoS Attack

SYN Flood Attack Defense

An attacker might send out repeated SYN messages to the device, leaving many half-open TCP connections on the device, which will make the device crash. When hit by an SYN flood attack, the device will defend itself by discarding the first message.

ICMP Flood Attack Defense

An attacker might send out an abnormally large number of ICMP packets to the device, which will use up all computing resources and thus make the device crash. When hit by an ICMP flood attack, the device will defend itself by using the ICMP message filtering tactic.

Save Refresh

6.4 隔離ポートの設定 (Port Isolation)

隔離ポートとは、メッセージ間のレイヤ2の隔離を実現することです。隔離グループのポート間でレイヤ2データを隔離するには、隔離グループにポートを追加するだけで済みます。隔離ポート機能は、より安全で柔軟なネットワーキングソリューションをユーザーに提供します。

手順

- ステップ1 security>PortIsolationを選択します。
- ステップ2 Add(追加)をクリックします。
- ステップ3 IsolatedGroupNo.(分離グループ番号)とIsolated Member(分離メンバー)を選択し、OKをクリックします。

関連操作

図7-10隔離グループの追加

Add Isolated Group X

Isolated Group No. 1

Isolated Member

Cancel OK

- 分離グループの編集:クリック
- 隔離グループのクリア:クリック

7 制御ポリシー (Control Policy)

7.1 ポートプライオリティの設定 (Port Priority)

デフォルトでは、音声VLANの802.1pプライオリティとDSCPプライオリティは、それぞれ6と46です。さまざまな音声サービスのプライオリティを計画するために、802.1pプライオリティとDSCPプライオリティを動的に設定できます。

●802.1pプライオリティは、各802.1Q VLANフレームの3ビットPRIフィールドの値によって示されます。このフィールドは、スイッチングデバイスが輻輳したときのデータパケットの送信優先順位を決定します。

●DSCP値は、IPv4パケットヘッダーのType of Service(ToS)フィールドの6ビットによって示されます。DSCPは、DiffServのシグナ

リングとして、IPネットワーク上のQoS保証に使用されます。ネットワークゲートウェイ上のトラフィックコントローラは、6ビットによって伝送される情報に基づいてアクションを実行します。

手順

ステップ1 ControlPolicy>PortPriorityを選択します。

ステップ2 優先順位と信頼モードから選択します。

 信頼モードには、802.1P、DSCP、およびDSCP&802.1Pの4種類のUntrustが含まれます。

ステップ3 OKをクリックします。

図8-1ポートプライオリティの設定

Port	Priority	Trust Mode
1	0	Untrust
2	0	Untrust
3	0	Untrust
4	0	Untrust
5	0	Untrust
6	0	Untrust
7	0	Untrust

OK Refresh


7.2 プライオリティマッピングテーブルの設定 (Priority Mapping Table)

手順

ステップ1 ControlPolicy >PriorityMappingTableを選択します。

ステップ2 DSCP>localPriorityまたは「802.1p」>「ローカル優先度」の順に選択します。

ステップ3 出力値を選択します。

 入力値と出力値はモードによって異なります。

ステップ4 OKをクリックします。

図8-2優先度マッピング

Input Value	Output Value
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	1

OK Refresh

7.3 キュースケジューリングの設定 (Queue Scheduling)


●PQ:プライオリティキューイング。PQは、パケットを優先度の高い順にスケジュールします。優先度の低いキュー内のパケットは、優先度の高いキュー内のすべてのパケットがスケジュールされた後でのみスケジュールできます。

●WRR:Weighted Round Robin.WRRスケジューリングでは、デバイスはキューの重みに基づいてポーリング方式でパケットをキューにスケジューリングします。1ラウンドのスケジューリングの後、すべてのキューの重みは1減少します。重みが0に減ったキューはスケジュールできません。

手順












ステップ1 ControlPolicy >QueueSchedulingを選択します。

ステップ2 キューアルゴリズムから選択します。

 WRRモードでは、優先キューの重み比率はQueo:Queo1:Queue2:Queue3=1:2:4:8です。

ステップ3 OKをクリックします。

図8-3キューのスケジューリング

Interface	Queue Algorithm	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Operation
		Weight	Weight	Weight	Weight	Weight	Weight	Weight	Weight	
1	SP									
2	SP									
3	SP									
4	SP									
5	SP									
6	SP									
7	SP									
8	SP									
9	SP									
10	SP									
11	SP									

Total 52 records < 1 2 3 > Go to Page

7.4 ポート速度制限の設定 (Port Speed Limit)

手順

ステップ1 ControlPolicy >PortSpeedLimitを選択します。

ステップ2 追加をクリックします。

図8-4ポート速度制限の追加

Add Port Speed Limit

* Interface

* Direction

* CIR kbps Range: 64 - 200000

Cancel OK

ステップ3 Interface、Direction、CIRを入力します。



- Directionの値には、InとOutがあります。
- CIRの入力ルール:16~1000000の範囲。16の整数倍である必要があります。

ステップ4 OKをクリックします。

7.5 ストーム制御の設定 (Storm Control)

ネットワーク上のブロードキャストフレームは連続的に転送され、これは適切な通信に影響を与え、ネットワーク性能を大きく低下させる。ストーム制御は、ポートのブロードキャストフローを制限し、フローが指定されたしきい値を超えるとブロードキャストフレームを破棄できます。これにより、ブロードキャストストームのリスクを低減し、ネットワークの適切な動作を保証できます。

手順

ステップ1 ControlPolicy >StormControlを選択します。

ステップ2 追加をクリックします。

図8-5ストーム制御の追加

ステップ3 ポート、タイプ、速度を入力します。

ステップ4 OKをクリックします。

8 認証 (Authentication)

8.1 802.1xの設定 (802.1x)

802.1Xは、組織がユーザのIDを認証し、ネットワークへのアクセスを許可するときに、ネットワークアクセス用のポートを開くネットワーク認証プロトコルです。

手順

ステップ1 有効の横にある をクリックして、NAS(ネットワーク接続ストレージ)を有効にします。

ステップ2 ポートステータスから選択します。



ステータスには、Auto、Force unAuthorized、Force Authorizedがあります。

図9-1802.1xの設定

表9-1802.1xの説明

パラメーター	説明
自動(auto)	ポートは、認証結果に従ってステータスを自動的に設定します。
強制的に未認可 (Force unAuthorized)	<ul style="list-style-type: none"> ● ポートは常に無許可ステータスになり、ユーザーは認証を許可されません。 ● デバイスは、このポートを介してアクセスするユーザに認証サービスを提供しません。
強制認証(Force Authorized)	ポートは常に許可ステータスであり、ユーザは認証なしでネットワークリソースにアクセスできます。

ステップ3 OKをクリックします。

8.2 RADIUSの設定 (RADIUS)

RADIUS(Remote Authentication Dial-In User Service)は、AAA(Authentication,Authorization and Accounting)を実現するための一般的なプロトコルです。RADIUSは分散・C/S構築の情報対話プロトコルです。不正な訪問からネットワークを保護できます。これは、リモートアクセスを許可しますが、より高いセキュリティを要求するネットワークで使用されます。RADIUSパケットフォーマットとメッセージ送信メカニズムを定義します。これは、RADIUSパケットをカプセル化するために、トランスポート層プロトコルとしてUDPを使用することを規定します。

当初、RADIUSはダイヤルアップユーザーのみのAAAプロトコルです。ユーザアクセスの開発により、RADIUSはイーサネットアクセスやADSLアクセスを含む様々なアクセスに適応します。認証と認可を通じてサーバにアクセスし、アカウントングを通じてネットワークソースの使用状況を記録します。

手順

ステップ1 Authentication >RADIUSを選択します。

ステップ2 Add(追加)をクリックします。

ステップ3 IPアドレス、ポート、キーを設定します。

ステップ4 OKをクリックします。

図9-2RADIUS

図9-3RADIUSの追加

* IP Address Invalid entry. Please enter again.

* Port (0~65535)

Secret Key

Cancel OK