RG-HS2310-16GH2GT1XS
Web-GUI 操作マニュアル

著作権・商標権について

利用条件・免責事項

ご購入の製品・サービス・機能などが契約書に基づいてご利用ください。

本文書の内容は製品のバージョンのアップデート等の事情による予告なく変更されることがありますので、最新の内容はRuijie Networksのホームページでご確認ください。

本文書は使用ガイドとして使われています。Ruijie Networksは内容の正確性に努めますが、内容の不正確や欠落等による損失及び損害はいかなる責任を負いかねますので、ご了承ください。

はじめに

弊社の製品をご利用いただき、ありがとうございます。このマニュアルは RGOS バージョン RGOS 11.4(1)B90 と一致します。

対象

このマニュアルは次の方々に適しています。

- インターネットエンジニア
- 技術普及者
- ウェブ管理者

技術サポート

- Ruijie Networks ホームページ: https://ruijie.co.jp/
- サポートサイト: https://www.ruijie.co.jp/service
- 故障・修理のお申し込み: https://www.ruijie.co.jp/service/post-sales
- サポートメールアドレス: support_jp@ruijienetworks.com

用語の説明

- G.hn

  Gigabit Home Networking と総称され、電源ケーブル、ツイストペアと同軸ケーブルをホームネットワークの有線伝送媒体として使用し、配置された各ケーブルを最大限に利用することで、ネットワークの高速伝送と信頼性の高い接続を実現することができます。

- DM

  Domain Master と総称され、ドメイン内のすべてのノード(アクセス、帯域予約、登録、その他のドメイン内の管理サービスなど)における操作を担当します。

- EP

  End Point と総称され、G.hn 内の DM 以外のノードを EP とします。

- GAM

  G.hn access multiplex と総称され、複数の DM を含むデバイスであり、複数の EP アクセスをサポートします。

記号の説明

本ガイドに使用される記号は次のように定義されます。

📖 豆知識を示しています。本マニュアルの補足説明です。ご使用に際し、より分かりやすくなります。
注意を払う必要がある情報を示します。

目次

1 Web 管理システム

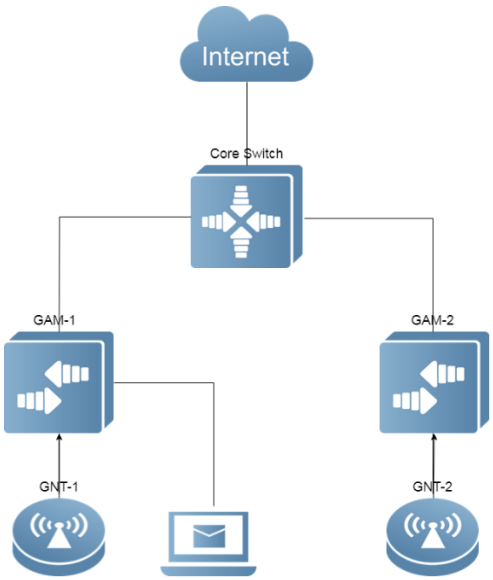
1.1 概要

ユーザーは Google、Firefox などのブラウザで GAM デバイスの Web システムにアクセスし、管理や構成を行います。

1.2 Web ログイン

図 1-1 に示すように、ユーザーは PC からブラウザで GAM にアクセスし、管理と構成を行うことが可能です。

図 1-1 基本トポロジ



1.2.1 機能の配置

環境要件の構成

管理者はクライアントの Web ブラウザから Web 管理システムにログインし、GAM を管理します。一般的にクライアントとは PC を指しますが、ノートパソコンやタブレットなどの他の端末を指すこともあります。

Google Chrome、Firefox などのブラウザをお勧めします。他のブラウザを使うと文字化けやフォーマットエラーなどの異常が発生することがあります。

解像度：解像度は 1024*768、1280*1024、1920*1080 に設定することをお勧めします。他の解像度を選択するとフォントの整列エラーや書式エラーなどの異常が発生することがあります。

GAM の要件

Web サービスをオンにする必要があります。デフォルトでオンになっており、自動的に HTTP から HTPPS にジャンプします。

デフォルトのユーザー名・パスワードは admin/admin で、初回ログイン後にパスワードのリセットが義務付けられています。パスワードは大小のアルファベット、数字、記号で構成されていなければなりません。

GAM のための管理 IP アドレスの設定が必要で、デフォルトは 192.168.1.200/24 です。

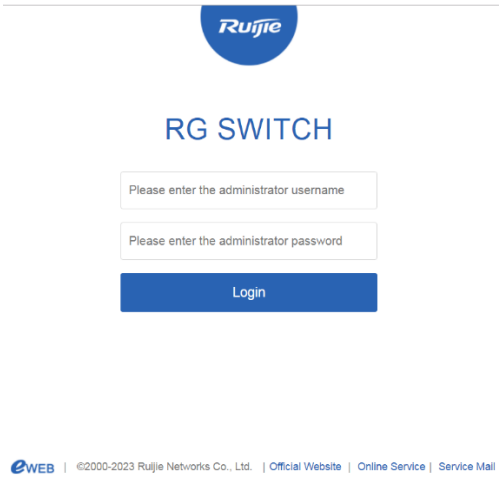
📖 コマンドラインインターフェース(CLI)上のスイッチの詳細な構成については、構成マニュアルをご参照ください。

📖 Web 構成と CLI 構成を同期させることができます。CLI 構成が完了した後に Write コマンドを実行することをお勧めします。Web ページを開いたら、Web と CLI の構成を同期させるようにそのページを更新してください。

ログイン

ブラウザのアドレスバーに http://x.x.x.x（管理 IP アドレス）を入力し、Enter キーを押すと、次の図のように、ログインページに進みます。

図 1-2 ログインページ



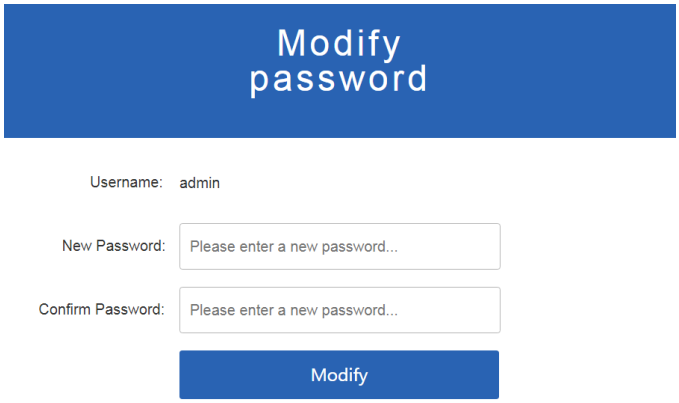
ユーザー名とパスワードを入力したら、「ログイン」をクリックします。下記の表はデフォルトのユーザー名とパスワードです。

デフォルトのユーザー名/パスワード	権限の説明
admin/admin	スーパーアドミニストレータで、あらゆる権限を持っています。

📖 コマンド「show running-config」を実行すると、デフォルトのユーザー名とパスワードは表示されません。

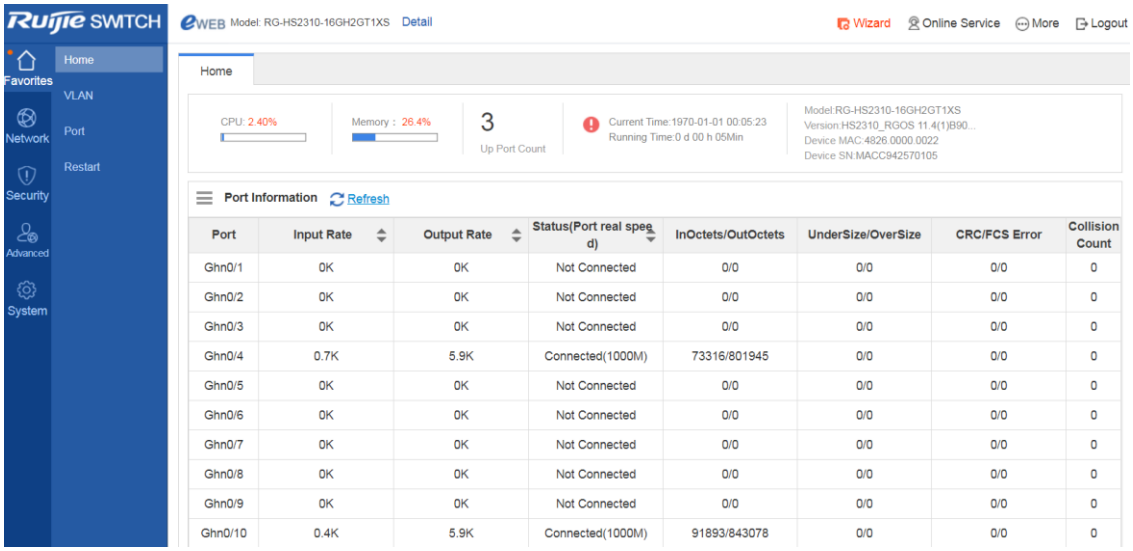
📖 デフォルトのユーザー名とパスワードでログインした後、パスワードを変更する必要があります。

図 1-3 パスワードの変更



認証を受けると、次の図のように Web 管理プラットフォームのホームページが表示されます。

図 1-4 ホームページ



📖 ページの詳細については、次のネットワーク管理システムを参照してください。

1.3 ネットワーク管理システム

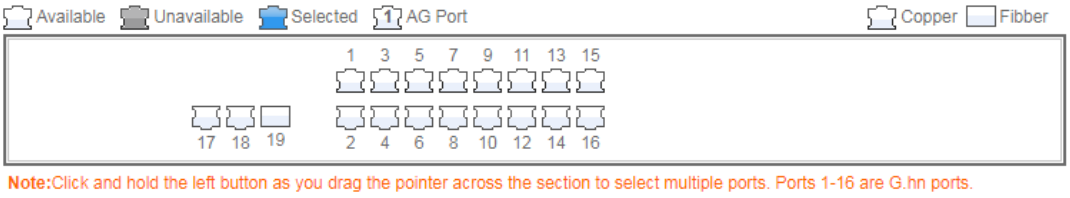
基本的な概念

GUI 上の各種のアイコンとボタン

アイコン/ボタン	説明
Edit	編集ボタンです。このアイコンをクリックすると、現在選択しているアイテムを編集することができます。
Delete	削除ボタンです。
ON	アイコンを有効/無効にします。
	オプションポートです。ポートをクリックまたは選択すると、ポートが選択されたポートになります。
	利用できないポートです。
	選択したポートです。
1	集約ポートです。ポート内の数字は集約ポート番号を表します。
	トランクポート(Trunk Port)です。このポートは「VLAN 管理/VLAN 設定」ページのパネルに表示されます。
Save	保存ボタンです。このボタンをクリックすると、入力した情報をコミットし保存します。
+	設定を追加します。
×	設定を削除します。
All Invert Deselect	パネルポートでのバッチ操作です。これらのアイコンはパネルの右下にあります。また、これらのアイコンは複数のポートを選択できるパネルでのみ利用可能です。
*	このマークがテキストボックスの後ろに表示されている場合は、そのテキストボックスに対応するアイテムを必須項目とします。

システム操作

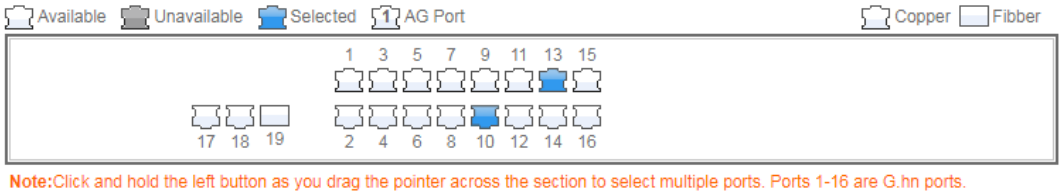
- デバイスパネル



- **パネル操作**

  ポートをクリックまたはカーソルを移動してパネル上で複数のポートを選択すると、利用可能なポートに変更することができます。選択されたポートに設定を追加します。例えば、ポート記述の追加、ポートミラーリングの構成、ポートレート制限の構成などです。選択されたポートは、ポートパネルの下の枠の中にスロットごとに配置されます。

- **選択されたポート**



メニュー

ページ左側のセカンダリーメニューの機能を説明すると次の表のようになります。

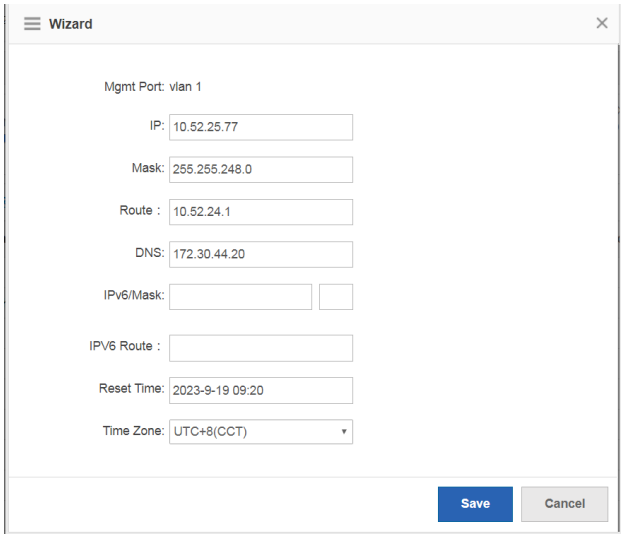
メニュー	説明文
ホームページ	ポート情報とデバイスの構成を表示するために利用されます。
VLAN	VLAN とトランクポートを設定します。
ポート	ポートの基本的な設定で、ポートの集約、ポートのミラーリング、ポートの制限速度などを配置します。
再起動	デバイスの再起動に使われます。
MAC アドレス	静的アドレスとフィルタリングアドレスを設定します。
RLDP	RLDP を構成します。
ARP 攻撃防止	ARP 詐欺防止設定、ARP チェック設定、DAI 設定と ARP テーブルエントリ設定を行うために使用されます。
ストームコントロール	ストームコントロールの実行に使用されます。
保護ポート	保護ポートを構成します。
ACL	ACL リスト、ACL 時間、ACL の適用を設定します。
QoS	ネットワークの性能及び信頼性を向上させるために、ネットワークリソースの割当て及び使用を保証するために使用されます。

システム設定	システム時間の設定、パスワードの変更、システムの再起動、工場出荷時の設定の復元、拡張機能の構成、SNMP と DNS の設定に使用されます。
システムアップグレード	ローカル・アップグレードとオンライン・アップグレードを行います。
システムログ	ログサーバーの設定やシステムログの閲覧に使います。
ネットワーク検出	ping、Traceroute、ケーブル検出、ワンクリックコレクションを設定します。
ネットワークコマンドラインインターフェース	CLI をシミュレートします。

1.3.1 クイックガイド

管理 IP とマスク(IPv6 オプション)、デフォルトゲートウェイ、DNS サーバーを設定し、「Save」をクリックします。「Configruation Succeeded」が表示されると、操作は成功します。

図 1-5 クイックガイド

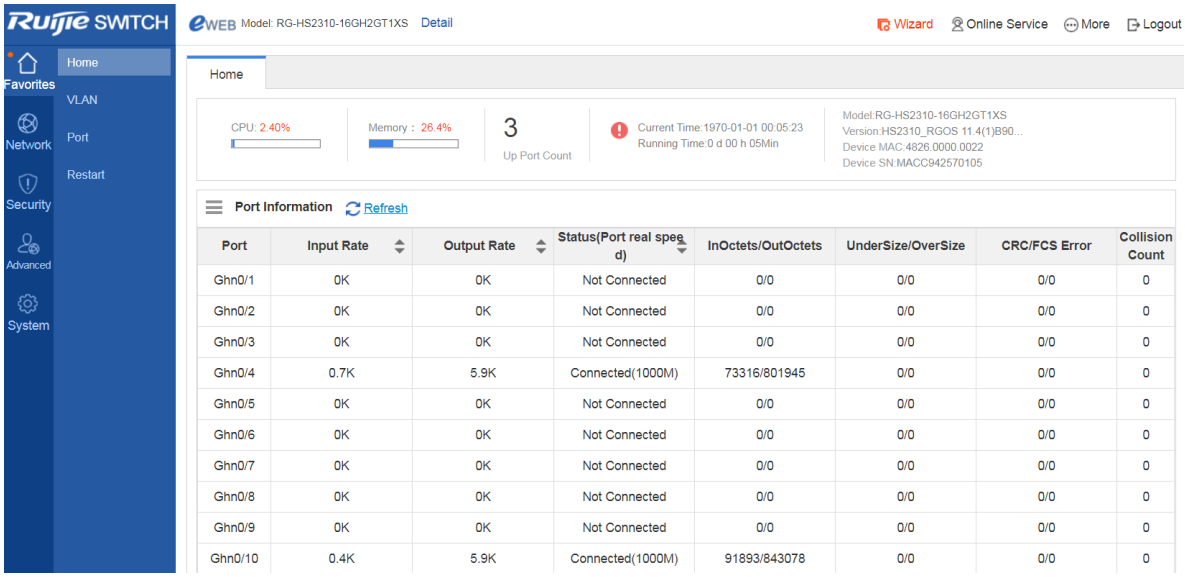


1.3.2 よく使います

「ホーム」、「VLAN」、「ポート」、「再起動」を含むセカンダリーメニューには、メインメニューの「よく使います」からアクセスできます。トップページにデバイスの配置、ポートの基本情報、ポートの統計情報を表示します。

次の図はホームページを示しています。

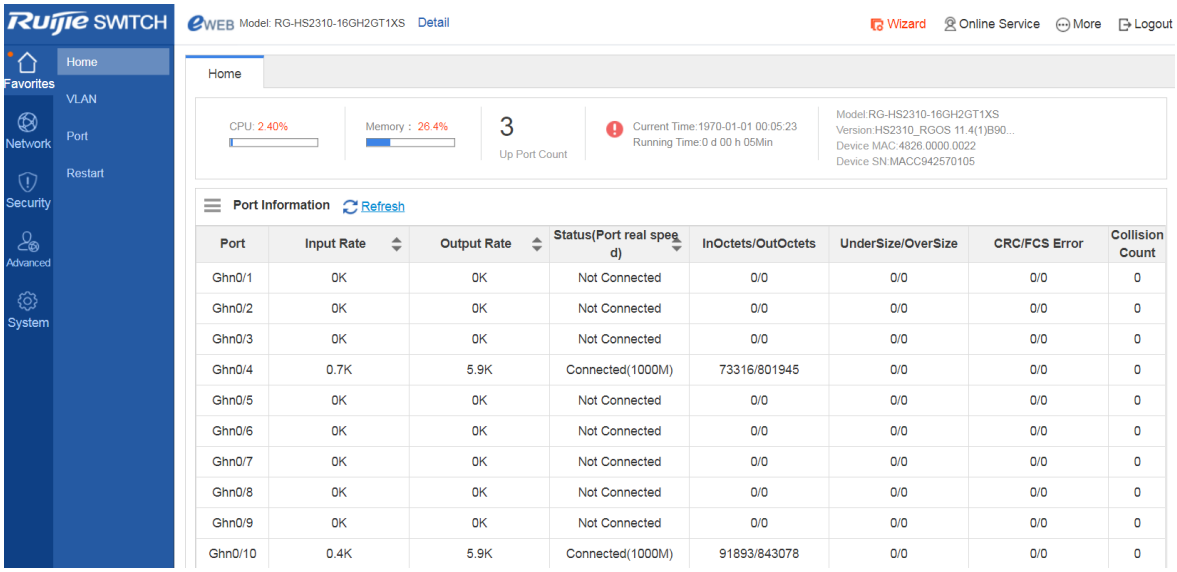
図 1-6 ホームページ



1.3.2.1 ホームページ

トップページには、デバイスの配置、ポートの基本情報、ポートの統計情報を表示します。

図 1-7 ホームページ



Port	Input Rate	Output Rate	Status(Port real speed)	InOctets/OutOctets	UnderSize/OverSize	CRC/FCS Error	Collision Count
Ghn0/1	0K	0K	Not Connected	0/0	0/0	0/0	0
Ghn0/2	0K	0K	Not Connected	0/0	0/0	0/0	0
Ghn0/3	0K	0K	Not Connected	0/0	0/0	0/0	0
Ghn0/4	0.7K	5.9K	Connected(1000M)	73316/801945	0/0	0/0	0
Ghn0/5	0K	0K	Not Connected	0/0	0/0	0/0	0
Ghn0/6	0K	0K	Not Connected	0/0	0/0	0/0	0
Ghn0/7	0K	0K	Not Connected	0/0	0/0	0/0	0
Ghn0/8	0K	0K	Not Connected	0/0	0/0	0/0	0
Ghn0/9	0K	0K	Not Connected	0/0	0/0	0/0	0
Ghn0/10	0.4K	5.9K	Connected(1000M)	91893/843078	0/0	0/0	0

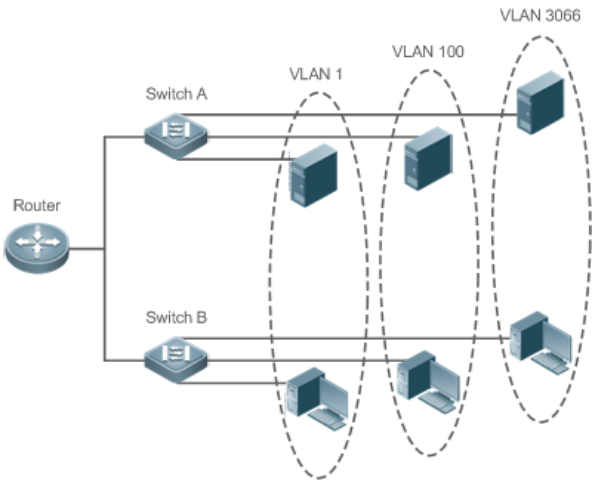
1.3.2.2 VLAN

VLAN（Virtual Local Area Network）は、物理的なネットワークをベースにした論理的なネットワークです。VLAN は OSI モデルのレイヤ 2 ネットワークに分類できます。

VLAN は通常の LAN と同じ特性を持ちますが、物理的な場所に制約があります。レイヤ 2 のユニキャスト、ブロードキャスト、マルチキャストフレームは VLAN 内で転送・伝送され、トラフィックを分離します。

ある 1 つのポートが VLAN のメンバーとして構成され、その後、そのポートに接続されたすべての端末がその VLAN の一部となることが可能です。ユーザーを追加、削除、修正する際にネットワークを物理的に変更する必要はありません。VLAN 間の通信は、次の図 1-8 のような 3 段階のデバイスによって行われます。

図 1-8 VLAN 通信図



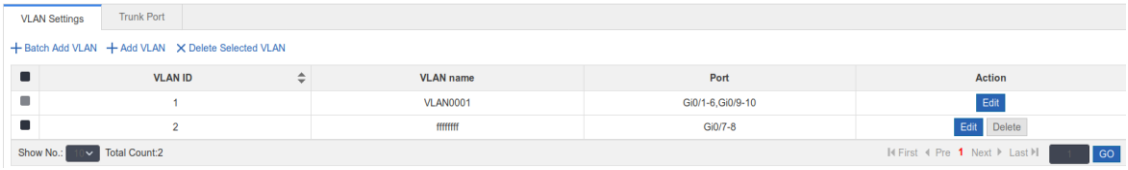
📖 対応する VLAN は IEEE802.1Q 規格に準拠します。最大 4094VLAN（VLAN ID 1-4094）をサポートしますが、VLAN 1 は削除できません。

Trunk ポートは、複数の VLAN に属するフレームを送受信するために、複数の VLAN に属することができます。

VLAN ページには、VLAN 設定とトランクポートという 2 つのタブがあります。

VLAN 設定

図 1-9 VLAN 設定



■ VLAN の追加

VLAN を追加するには、VLAN ID を入力し、必要に応じて別の情報を入力します。そして、「Save」をクリックすると、VLAN リストに新たに追加された VLAN が表示されます。

■ VLAN の編集

「Action」バーの「Edit」をクリックすると、対応する VLAN の情報がページに表示されます。メッセージを編集した後、「Save」をクリックすると新しい構成が表示されます。

■ VLAN の削除

(1) VLAN リストで複数の VLAN を選択し、「Delete Selected VLAN」をクリックすると、VLAN を一括削除することができます。

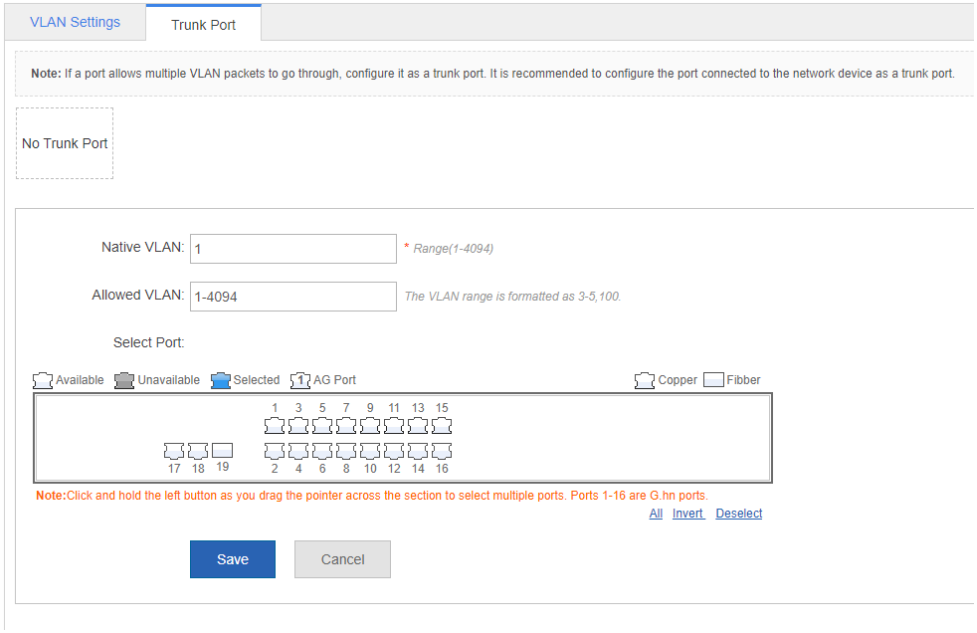
(2) 「Action」バーの「Delete」をクリックすると、「Are you sure you want to delete the VLAN?」というプロンプト情報が表示されます。操作を確認したら「Delete Succeeded.」が表示されます。VLAN1はデフォルト VLAN なので削除できません。

📖 VLAN 1 はデフォルト VLAN です。この VLAN は修正することができ、削除することはできません。VLAN 1 の IP アドレスを変更する前に、新しい IP アドレスが届くようにします。変更に成功すると、自動的にログインページに遷移し、ユーザーはログインし直さなければなりません。ログインページに遷移せず、「ページが見つかりません」とプロンプトが表示された場合、IP アドレスが届かない可能性があります。この場合、ネットワーク接続をチェックしてください。

トランクポート

次の図は「トランクポート」のページです。

図 1-10 トランクポート



■ トランクポートの追加

パネルポートを選択し、本体の VLAN と許可されている VLAN（例えば、3-5、8、10）を指定し、「Save」をクリックします。「Configuration Succeeded」が表示されたら、操作完了です。メッセージを表示します。このとき、新たに追加されたトランクポートがトランクポートリストに表示されます。

Allowed VLAN は Native VLAN を追加する必要があります。そうしないと、G.hn 通信に異常が生じます。

■ トランクポートの編集

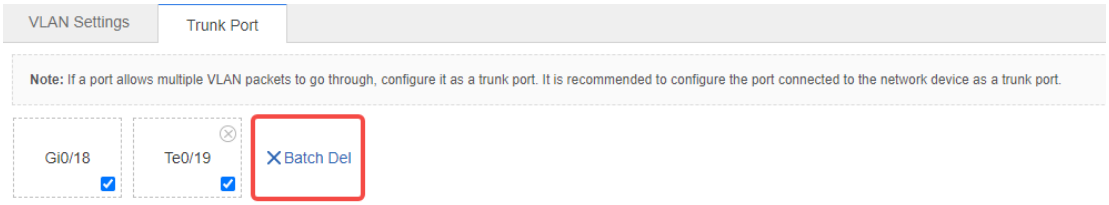
トランクポートのリストにあるトランク ポートをクリックすると、そのトランクポートの情報が表示されます。メッセージを編集したら、「Edit」をクリックします。「Configuration Succeeded」が表示されると、操作完了です。

■ トランクポートの削除

トランクポートのリスト内の特定のトランクポートにカーソルを移動したら、「削除」をクリックします。「Are you sure you want to delete the trunk port?」が表示したら、確認をクリックします。「削除に成功しました」が表示したら、操作完了です。

■ トランクポートの一括削除

削除するトランクポートを選択したら（トランクポートリストの中に）「一括削除」をクリックします。「Are you sure you want to delete the trunk port?」が表示されたら、確認をクリックします。「削除に成功しました」が表示されると、操作完了です。

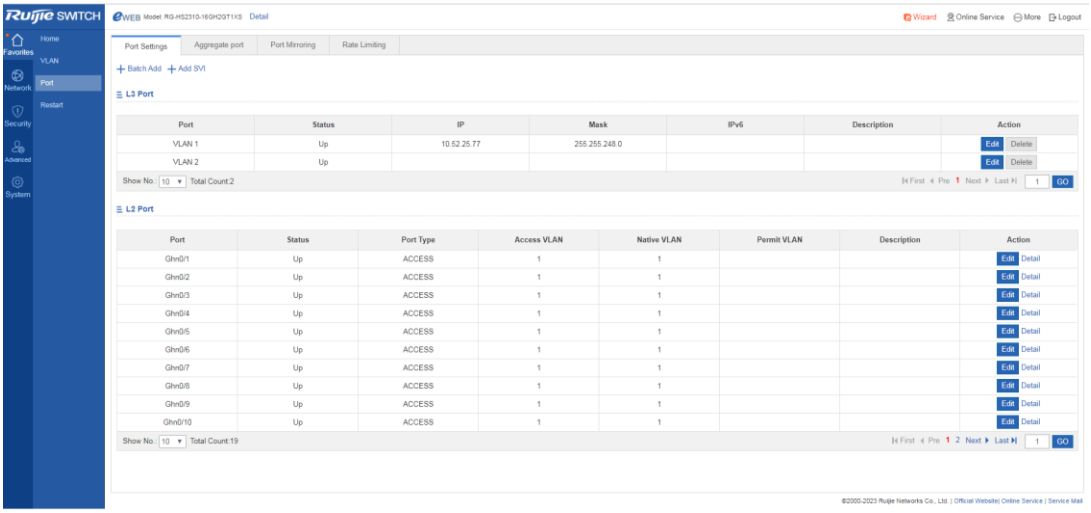


1.3.2.3 ポート

ポートは、ネットワークデバイスに接続するための物理的なインタフェイスです。

➘ ポート設定

図 1-11 ポート設定



■ ポートの追加

設定するポートを選択し、「ステータス」、「スピード」、「動作モード」を選択します。「Keep」は設定をそのまま残すことを意味します。バッチ設定は、「Save」を選択して 1 つまたは 2 つのアイテムをバッチ設定できます。

■ ポートの編集

「Action」バーの「Edit」をクリックすると、該当するポートの情報が表示されます。メッセージを編集したら、「Save」をクリックします。「Configuration Succeeded」が表示されると、操作完了です。

■ SVI ポートの追加

「Add SVI」をクリックして、VLAN ID、IP アドレスと、サブネットマスクを入力し、「Save」をクリックします。「Configuration Succeeded」が表示されると、操作完了です。

■ 詳細情報の表示

レイヤ 2 のポートリストの操作バーの詳細をクリックすると、ポートのステータス、速度設定、実際の速度、動作モード、実際の動作モード、メディアなどのポート情報を閲覧することができます。

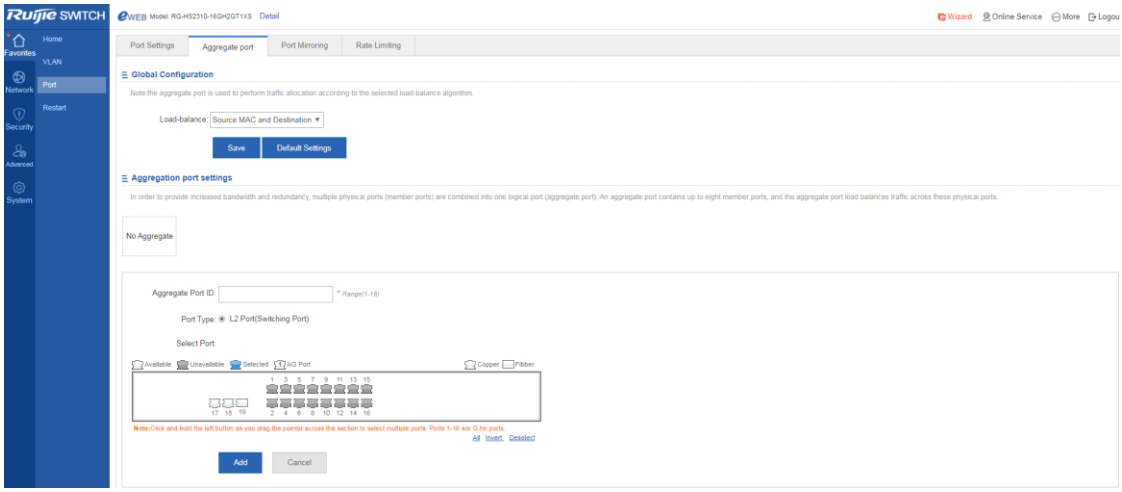
■ L3 ポートの削除

L3 ポートリストの「Action」バーで「Delete」をクリックし、確認画面で「OK」をクリックします。

➘ 集約ポート

次の図は、集約ポートのページです。

図 1-12 集約ポート



■ 集約ポートの追加

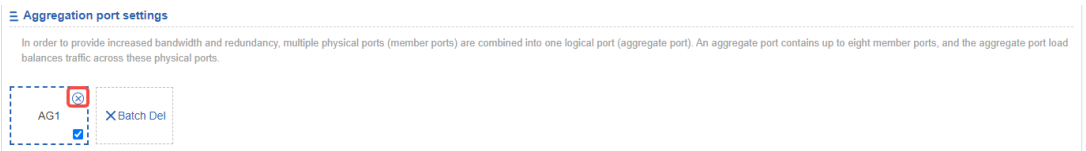
集約ポート ID を指定してメンバーシップポートを選択したら、「Add」をクリックします。「Configuration Succeeded」が表示されたら、操作完了です。パネルには新たに追加された集約ポートが表示されます。

■ 集約ポートの編集

パネルに表示されている集約ポートは利用できないポートです。それらを編集するには、集約ポートリストの中にある集約ポートをクリックします。その後、該当するメンバーシップポートが選択されたポートとなります。このポートをクリックすると、選択をキャンセルすることができます。その後、「Edit」をクリックして集約ポートを変更することができます。

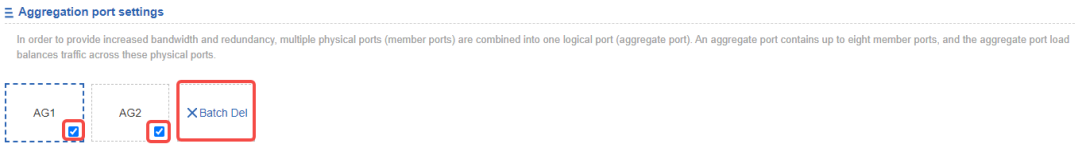
■ 集約ポートの削除

集約ポートリストの中にある集約ポートにカーソルを移動させ、「削除」をクリックすると、「Are you sure you want to delete the aggregate port?」が表示されます。操作確認後、集約ポートがパネル上の利用可能ポートになります。



■ 集約ポートの一括削除

集約ポートリストで削除する集約ポートを選択した後、「Batch Del」をクリックすると、「Are you sure you want to delete the aggregate port?」のプロンプトボックスが表示されます。メッセージが表示されます。操作確認後、これらの集約ポートはパネル上の利用可能ポートとなります。



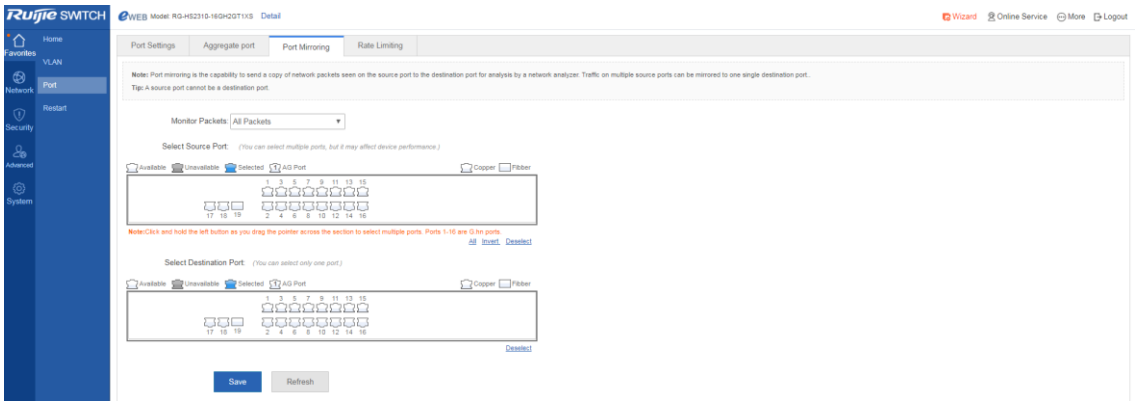
ARP チェック、ARP 詐欺防止、MAC VLAN 機能を可能にするポート及びポートミラーリング中の監視ポートは集約ポートに追加できません。それらはパネルに利用できないポートとして表示されます。カーソルが利用できないポートに移動すると、そのポートにある機能がオンになっていることを知らせるので、そのポートは利用できません。

G.hn ポートは集約ポートに対応していません。

ポートミラーリング

次の図はポートミラーリングページです。

図 1-13 ポートミラーリング



最初は、Web 上で 1 つのミラーポートしか設定できないため、ポートミラーリングページは編集状態です。ページには利用可能なパネルが 2 つあります。上部パネルから選択したポートがソースポートとなります(ミラーポート、複数のミラーポートが可能)。下部パネルは 1 つのポートのみを宛先ポート(ミラーポート)として選択できます。パネル上でポートを選択または変更した後、「Save」をクリックします。「Configuration Succeeded.」メッセージが表示されます。

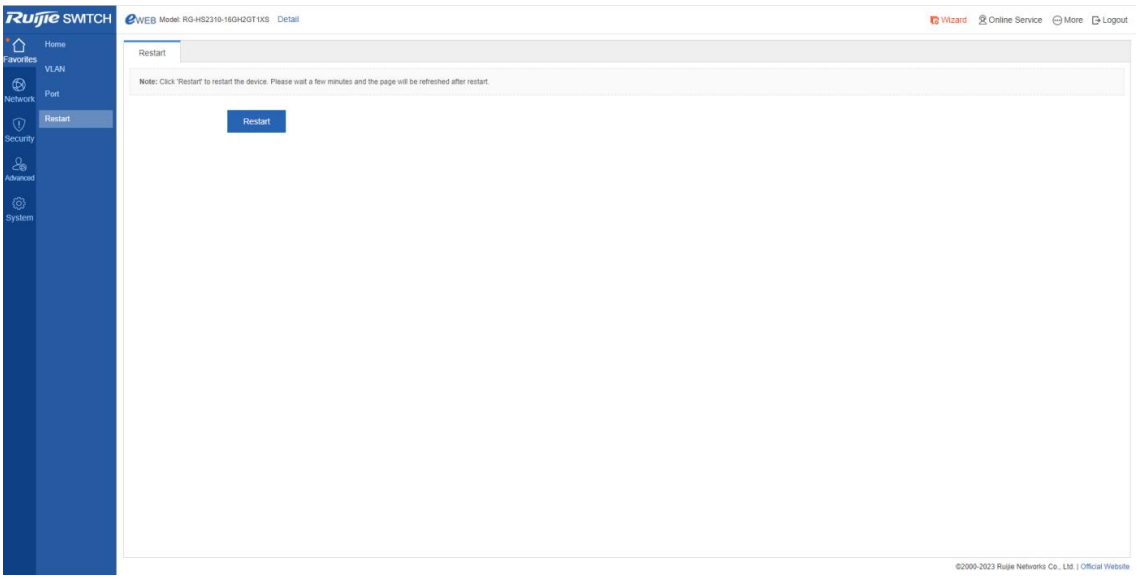
パネルには現在のポートミラーリングステータスが表示されており、編集状態になっています。変更後にポートを編集したくない場合は、「更新」をクリックして、現在のポートミラーリングステータスを表示することができます。

集約ポートのメンバーシップポートは宛先ポートまたはソース・ポートとして使用できません。1 つのポートを宛先ポートとソースポートの両方にすることはできません。G.hn ポートは宛先ポートとして使用できません。

1.3.2.4 再起動

次の図は再起動ページです。

図 1-14 再起動



「Restart」をクリックすると、「Are you sure you want to restart the device?」というメッセージが表示されます。操作確認後、デバイスが再起動します。再起動には数分かかります。デバイスの再起動後に自動的にページが更新されますので、お待ちください。

1.3.3 ネットワーク

「ネットワーク」メニューのセカンダリーメニューには MAC アドレスと RLDP があります。

1.3.3.1 MAC アドレス

コンピュータの媒体アクセスコントロールアドレス(MAC アドレス)は、ネットワークインターフェースに割り当てられた唯一の識別子であり、ネットワークセグメントデータリンク層の通信に使用されます。ethernet や wi-fi を含むほとんどの IEEE 802 ネットワーク技術は、MAC アドレスをネットワークアドレスとして使用します。論理的には、MAC アドレスは OSI 参照モデルのメディアアクセスコントロールプロトコルのサブレイヤに使用されます。

静的アドレスは、手動で構成された MAC アドレスです。静的アドレスの機能は動的アドレスと同じです。ただし、静的アドレスは手動で追加したり削除したりするだけで、静的アドレスの学習や解放はできません。静的アドレスは設定ファイルに保存されており、デバイスが再起動しても失われることはありません。

静的アドレスを手動で設定することによって、ネットワークデバイスの MAC アドレスとインタフェースを MAC アドレステーブルに結びつけることができます。

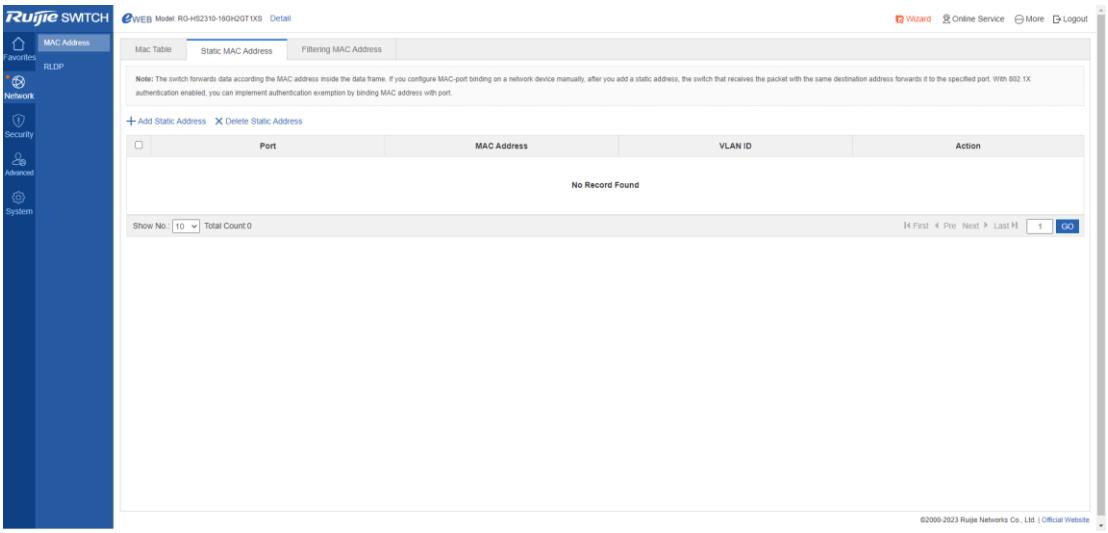
フィルタリングアドレスは手動で構成した MAC アドレスです。フィルタリングアドレスからのパケットが送られてくると、デバイスはそのまま廃棄します。フィルタリングアドレスの追加と削除は手動で行うことができますが、アドレスを劣化させることはできません。フィルタリングアドレスは設定ファイルに保存されており、デバイスが再起動しても失われることはありません。

不正ユーザーをフィルタリングしたいデバイスの場合は、そのソース MAC アドレスをフィルタリングアドレスとして指定することができます。これにより、不正ユーザーはデバイスを介して外部と通信することができなくなります。

MAC アドレスページには、アドレステーブル、静的アドレス設定とフィルタリングアドレス設定の 2 つのタブがあります。

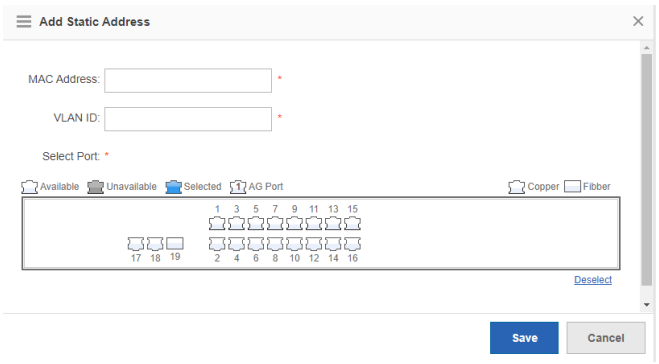
静的アドレスの設定

図 1-15 静的アドレスの設定



■ 静的アドレスの追加

静的アドレスを追加するには、MAC アドレス、VLAN ID を入力してポートを選択し、「Save」をクリックします。新たに追加された静的アドレスは、「Configuration Succeeded」情報の表示後にアドレスリストに表示されます。



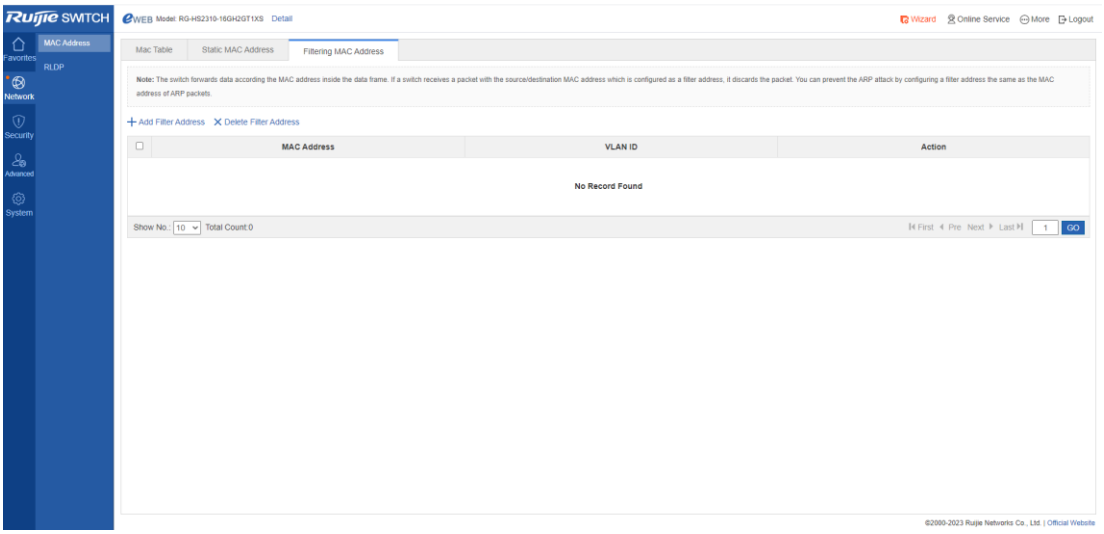
■ 静的アドレスの削除

(1) 複数の静的アドレスを選択することができます。「Delete Static Address」をクリックしてアドレスを一括削除することができます。

(2) 「Action」バーの「Delete」をクリックすると、「Are you sure you want to delete the static address?」が表示されます。操作確認後、「Delete Succeeded」（削除に成功しました）というメッセージが表示されます。

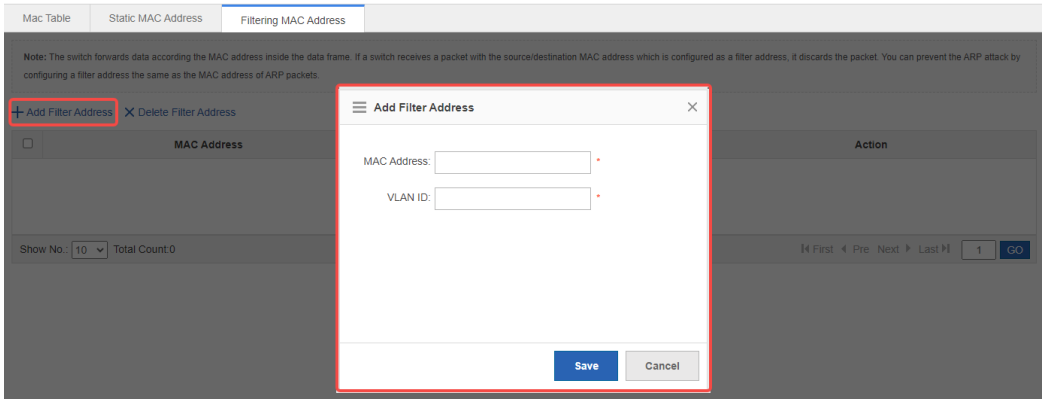
➘ フィルタリングアドレスの設定

図 1-16 フィルタリングアドレスの設定



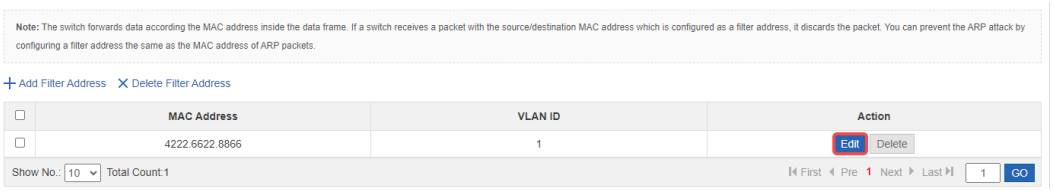
■ フィルタリングアドレスの追加

フィルタリングアドレスを追加するには、MAC アドレスと VLAN ID を入力して「Save」をクリックします。「Configuration Succeeded」のメッセージが表示された後、新たに追加されたフィルタリングアドレスがアドレスリストに表示されます。



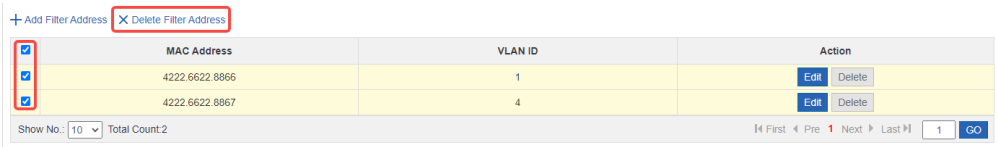
■ フィルタリングアドレスの編集

「Action」バーの「Edit」をクリックすると、対応するフィルタリングアドレスの情報が表示されます。メッセージを編集後、「Save」をクリックすると、「Configuration Succeeded」メッセージが表示されます。

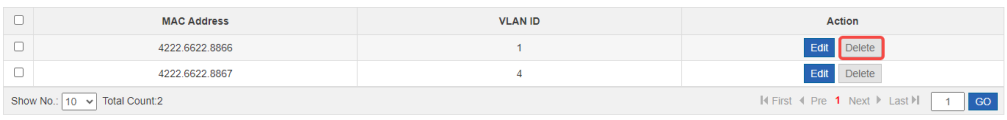


■ フィルタリングアドレスの削除

(1) フィルタリングアドレスを複数選択し、「フィルタリングアドレスを削除します」をクリックすると、アドレスを一括削除することができます。



(2) 「Action」バーの「Delete」をクリックすると、「Are you sure you want to delete the filter address?（フィルタリングアドレスを本当に削除しますか？）」のプロンプトが表示されます。操作確認後、「Delete succeeded（削除に成功しました）」メッセージが表示されます。



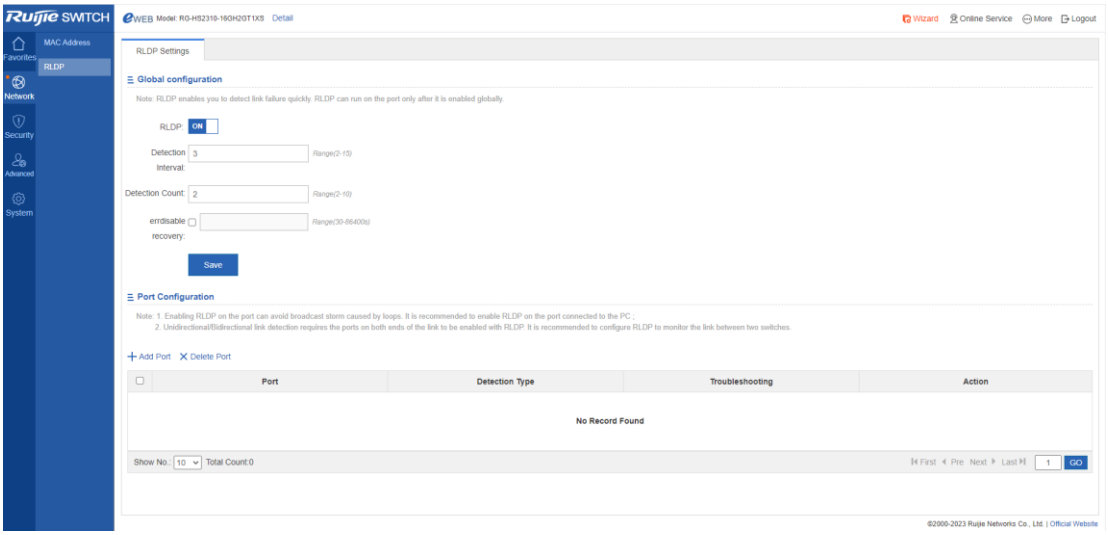
1.3.3.2 RLDP

高速リンク検出プロトコル（RLDP）は、イーサネットの一方向リンク障害、指向性転送障害及びダウンループ障害を迅速に検出します。障害が検出されると、障害処理構成に基づいて自動的に関連ポートを閉じるか、手動でポートを閉じるようにユーザーに通知し、誤ったトラフィック転送やイーサネットレイヤ 2 ループを回避します。

📖 G.hn ポートは RLDP 機能に対応しません。

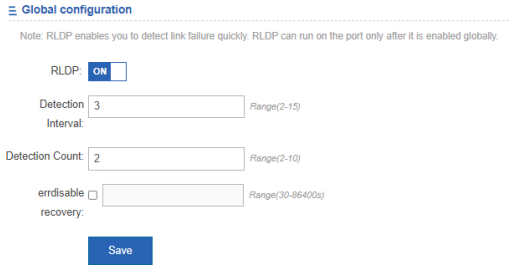
RLDP 設定

図 1-17 RLDP 設定



グローバル設定

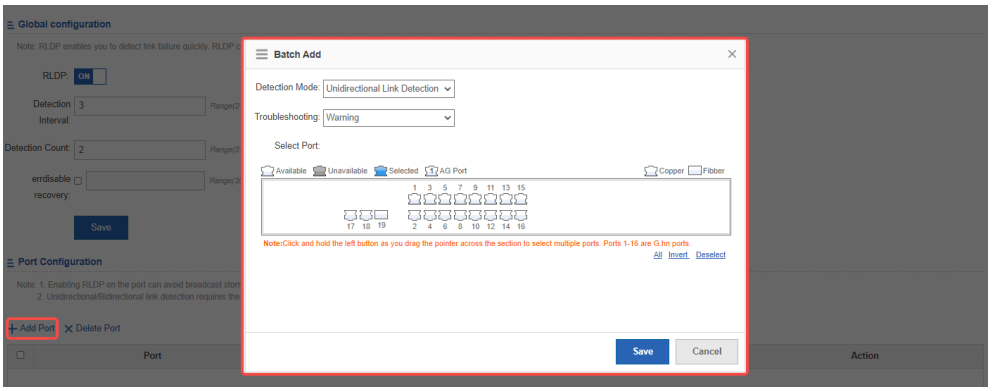
スイッチで RLDP を on / off にします。検出間隔とカウントを設定したら、「Save」をクリックします。このとき「Configuration Succeeded」メッセージが表示されます。



ポートの構成

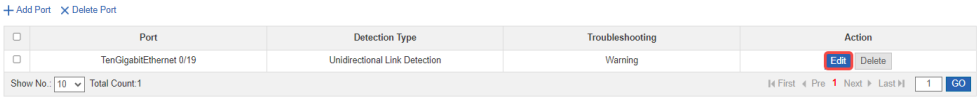
■ RLDP ポートの追加

検出モード、トラブルシューティングモードとポートを選択します。次に「Save」をクリックします。「Configuration Succeeded」メッセージが表示されると、新たに追加された RLDP ポートが RLDP ポートリストに表示されます。



■ RLDP ポートの編集

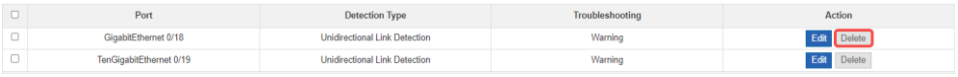
操作バーの編集をクリックすると、対応する RLDP ポートの情報が表示されます。メッセージを編集後、「Save」をクリックします。このとき「Configuration Succeeded」メッセージが表示されます。



■ RLDP ポートの削除

(1) RLDP ポートリストから複数の RLDP ポートを選択することができます。「Delete Port」（選択したポートを削除します）をクリックして、RLDP ポートを一括削除します。

(2) 「Action」バーの「Delete」をクリックすると、「Are you sure you want to delete the item?」が表示されます。操作確認後、「Delete Succeeded.」メッセージが表示されます。



1.3.4 セキュリティ

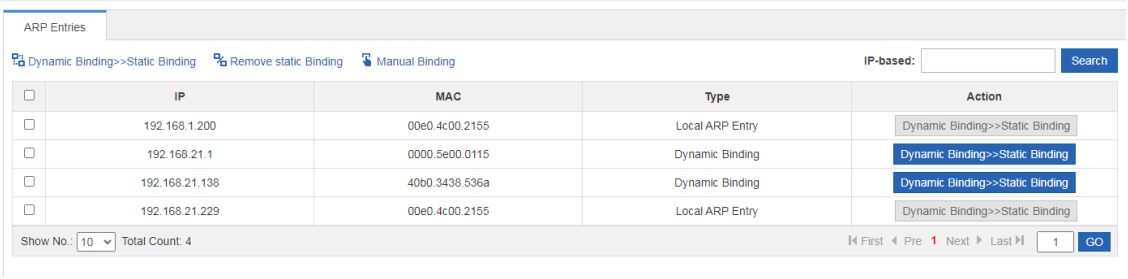
セキュリティメニューのセカンダリーメニューには、ARP 攻撃防止とストームコントロールが含まれています。

1.3.4.1 ARP 攻撃防止

ARP エントリを閲覧し、静的アドレスをバインディングできます。

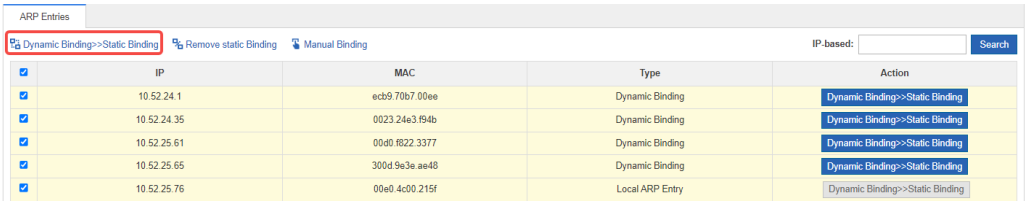
➘ **ARP エントリ**

図 1-18 ARP エントリ

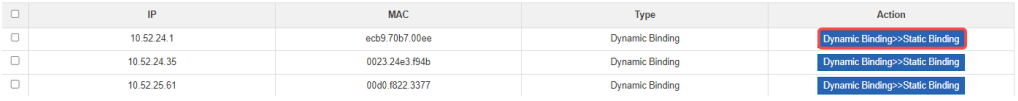


- 動的バインディング >> 静的バインディング

複数のエントリを選択し、リストの上部にある「Dynamic Binding>>Static Binding（動的バインディング>>静的バインディング）」をクリックします。

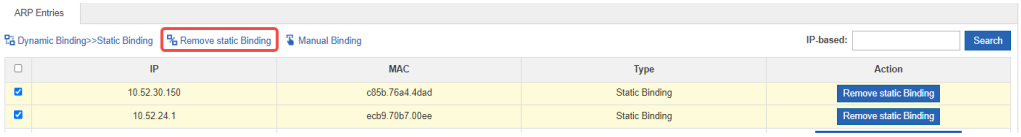


操作バーの動的バインディング>>静的バインディングをクリックします。

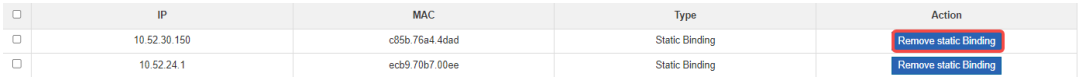


- 静的バインディングの削除

  複数のエントリを選択し、リストの上部にある「Remove Static Binding（静的バインディングを削除します）」をクリックします。

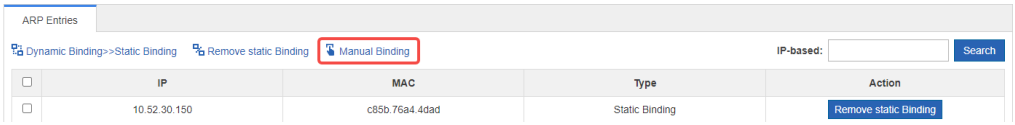


  操作バーの「Remove Static Binding（静的バインディングを削除します）」をクリックします。

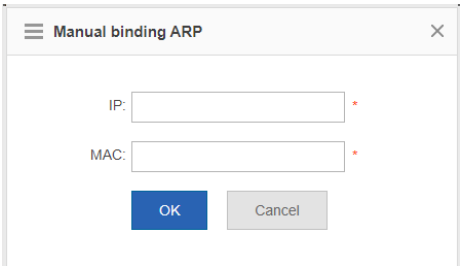


- 手動でのバインディング

  (1) リストの上部にある「Manual Binding (手動バインディング)」をクリックします。



  (2) IP と MAC アドレスを入力して、「OK」をクリックします。このエントリはリストに表示されます。



1.3.4.2 ストームコントロール

ローカルエリアネットワーク(LAN)にブロードキャストデータストリーム、マルチキャストデータストリーム、未知のユニキャストデータストリームがありすぎると、ネットワークスピードが遅くなり、パケット伝送のタイムアウトの確率が高くなります。これをローカルエリアネットワークストームと呼びます。トポロジプロトコルが実行された場合、またはネットワーク構成が正しくない場合、ストームが発生する可能性があります。

ストームコントロールは、ブロードキャストデータストリーム、マルチキャストデータストリーム、または未知のユニキャストデータストリームを制限するために使用することができます。デバイスポートによって受信したデータストリームレートが、構成された帯域幅しきい値、1 秒当たりのパケットしきい値、または 1 秒当たりのキロビットしきい値の範囲内である場合、データフローは許容されます。レートがしきい値を超える場合、レートがしきい値以内に落ちるまで、余分なデータストリームは廃棄されます。こうすることで、フローディングデータがローカルネットワークに入ってストームになることを防ぐことができます。

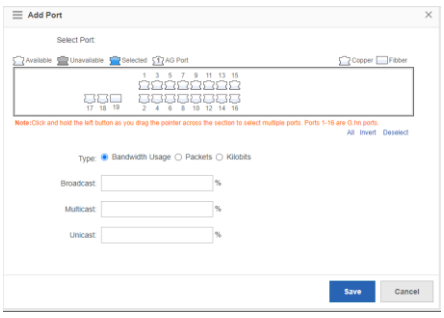
次の図はストームコントロール設定ページです。

図 1-19 ストームコントロール設定

■ ストームコントロールポートの追加

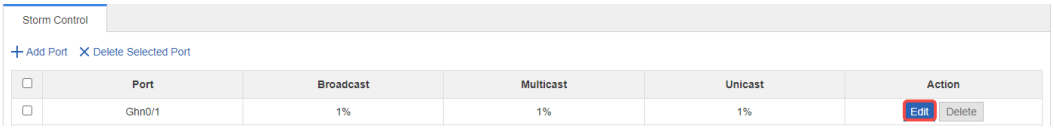
(1) ストームコントロールポートを追加するには、少なくともブロードキャスト、ユニキャスト、またはマルチキャストを設定する必要があります。

(2) 「Save」をクリックします。「Configuration Succeeded.（設定に成功しました）」メッセージが表示されると、新たに追加されたストームコントロールポートがストームコントロールリストに表示されます。

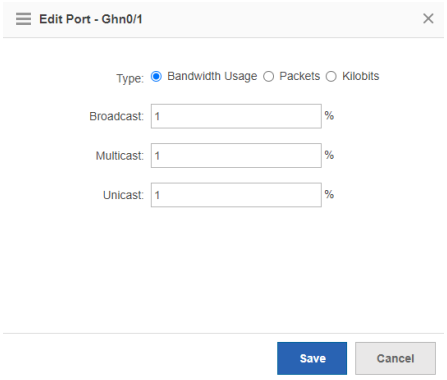


■ ストームコントロールポートの編集

(1) 「Action」バーの「Edit」をクリックすると、対応するストームコントロールポートの情報が表示されます。

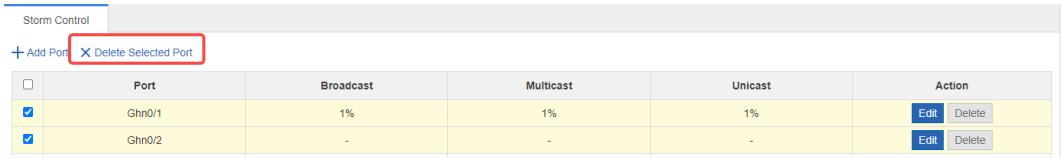


(2) メッセージを編集後、「Save」をクリックします。「Configuration Succeeded.（設定に成功しました）」メッセージが表示されると、操作完了です。

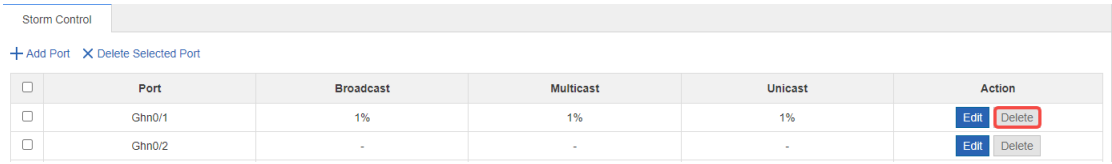


■ ストームコントロールポートの削除

ストームコントロールポートリストから複数のポートを選択することができます。「Delete Selected Port（選択したポートを削除します）」をクリックすると、ポートを一括削除することができます。



「Action」バーの「Delete」をクリックすると、「Are you sure you want to delete the port?（本当にポートを削除しますか？）」が表示されます。操作確認後、「Delete Succeeded.（削除に成功しました）」メッセージが表示されます。



1.3.5 ハイスペック

1.3.5.1 保護ポート

アプリケーション環境に応じて、特定のポート間の通信を禁止する場合があります。それは保護されたポートを構成することによって実現できます。保護されたポート間は互いに通信できないが、非保護ポートと通信することができます。

保護されたポートは 2 つのモードで動作します。

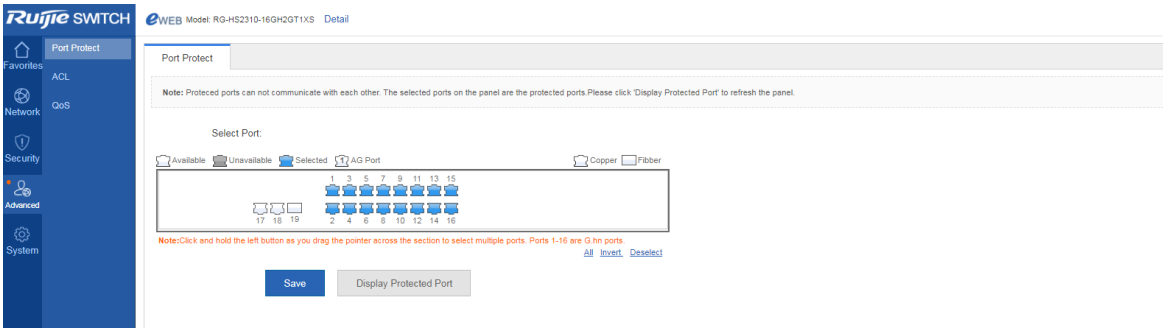
モード 1：保護ポート間のレイヤ 2 通信は隔離されているが、レイヤ 3 ルーティングで通信することができます。

モード 2：保護ポート間のレイヤ 2 とレイヤ 3 の通信はすべて隔離されます。保護されたポートが上記の両方のモードを同時にサポートする場合、最初のモードがデフォルトで使用されます。

集約ポートを保護ポートとして構成すると、その下にあるすべてのメンバーシップポートが保護ポートとして構成されます。G.hn ポートはデフォルトでポート保護がオンになっているので、オフにしないことをお勧めします。

次の図はポート保護設定ページです。

図 1-20 ポート保護設定



ポートを保護ポートに設定するには、パネル上でポートを選択して「Save」をクリックします。

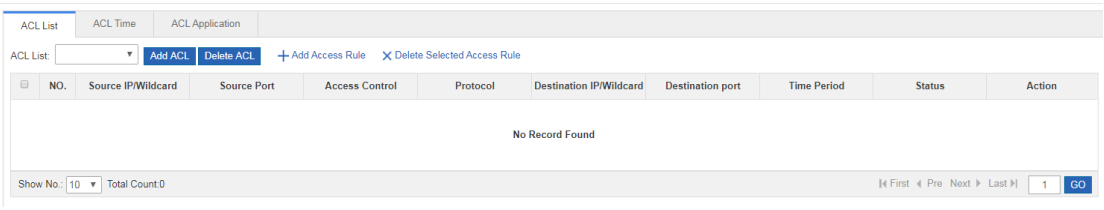
1.3.5.2 ACL

アクセスコントロールリスト(ACL)は、アクセスリストまたはファイアウォールとも呼ばれ、ACL ルールによってネットワークインターフェースに到着したパケットを転送するか破棄するかを判定します。時間ベースのアクセスコントロールリストは、時間帯に応じてネットワークリソースへのアクセスを制限したり許可したりすることができます。

➘ アクセスコントロールリスト

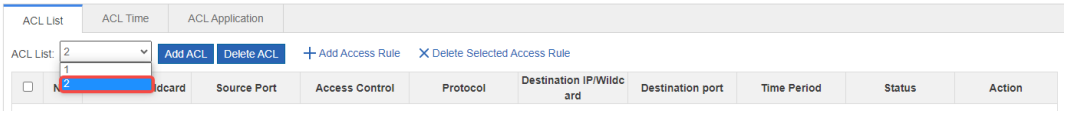
次の図は ACL リストページです。

図 1-21 アクセスコントロールリスト



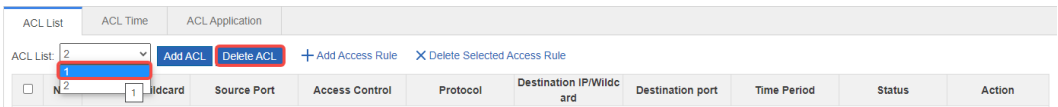
■ ACL の追加

「Add ACL」をクリックし、ポップアップページで設定を行います(ACL リストは必須項目)。次に、「OK」をクリックします。「Add Succeeded (追加に成功しました)」なら、追加が成功したことを示すプロンプト情報が表示され、ACL List のドロップダウンリストに新たに追加された ACL が表示されます。



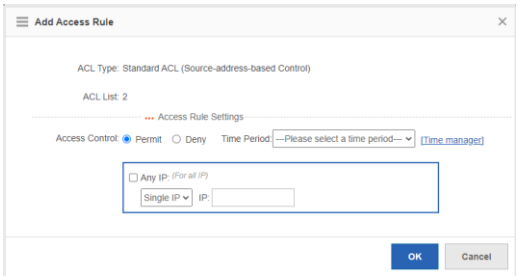
■ ACL の削除

「ACL List」で削除する ACL を選択し、「Delete ACL（ACL を削除します）」をクリックします。



■ アクセスルールの追加

ACL ルールを追加するには、アクセスコントロールのタイプ、プロトコル、有効期間、IP アドレスを選択し、「Save」をクリックします。追加に成功すると、ACL ルールリストに新たに追加された ACL ルールが表示されます。

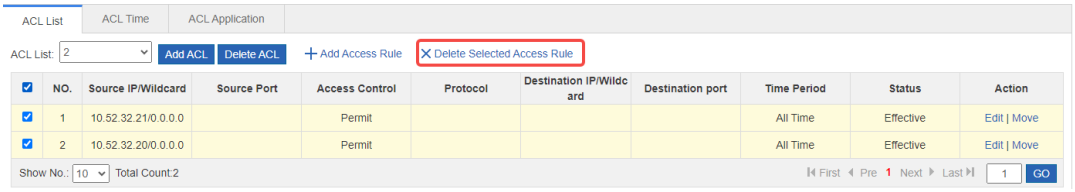


■ アクセスルールの編集

「Action」バーの「Edit」をクリックすると、対応する ACL ルールの情報が表示されます。メッセージを編集後、「Save」をクリックします。

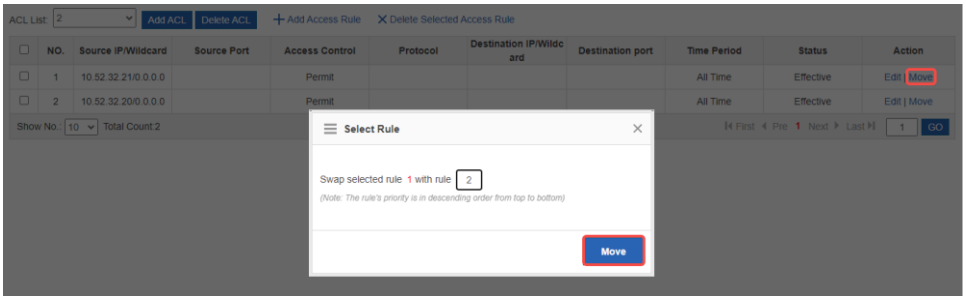
■ アクセスルールの削除

ACL ルールリストから複数のアクセスルールを選択できます。「Delete Selected Access Rule（選択したアクセスルールを削除します）」をクリックすると、アクセスルールを一括削除することができます。



■ アクセスルールの移動

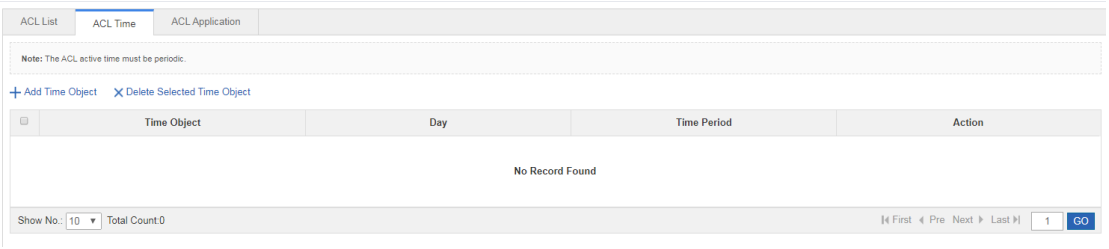
移動する ACL 番号を入力して、「Move」をクリックします。



アクセスコントロール時間

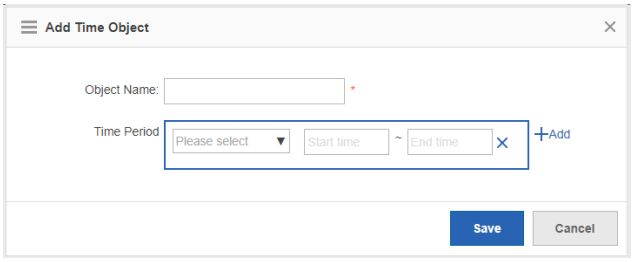
次の図は「ACL 時間」ページです。

図 1-22 ACL 時間



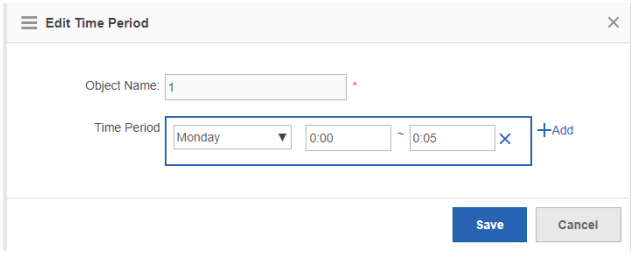
■ ACL 時間の追加

ACL 時間を追加するには、時間オブジェクト、日付と期間を設定する必要があります。次に、「Save」をクリックします。保存に成功すると、新たに追加された ACL 時間が ACL 時間リストに表示されます。



■ ACL 時間の編集

「Action」バーの「Edit」をクリックすると、対応する ACL 時間の情報が表示されます。メッセージを編集後、「Save」をクリックします。



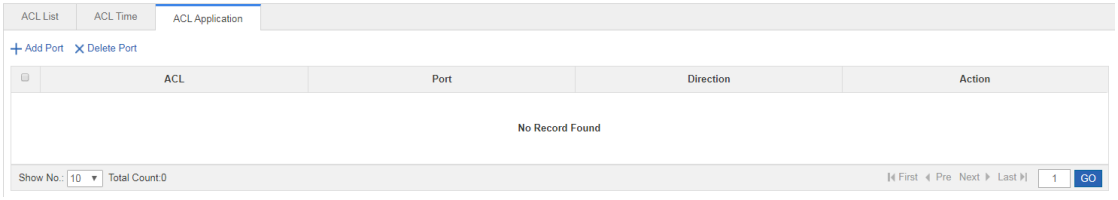
■ ACL 時間の削除

ACL 時間リストから複数の時間オブジェクトを選択できます。「Delete Selected Time Object（選択した時間オブジェクトを削除します)」をクリックすると、時間オブジェクトを一括削除することができます。

ACL の適用

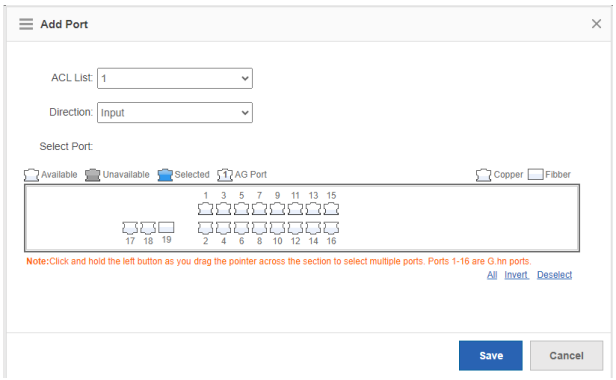
ACL 適用申請ページは次の図に示します。

図 1-23 ACL の適用



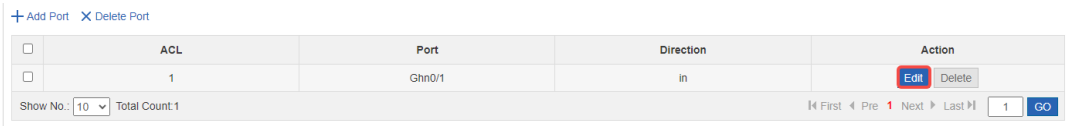
■ ACL 適用の追加

ACL 適用を追加するには、ACL 適用時間、フィルタ方向、ポートを設定する必要があります。次に、「**Save**」をクリックすると、ACL 適用リストに新たに追加された ACL 適用が表示されます。



■ ACL 適用の編集

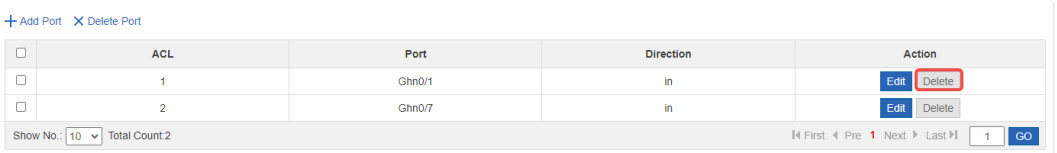
「Action」バーの「Edit」をクリックすると、対応する ACL 適用情報が表示されます。メッセージを編集後、保存をクリックすると、「Configuration Succeeded (設定に成功しました)」が表示されます。



■ ACL 適用の削除

ACL 適用リストから複数のポートを選択できます。「Delete Port (ポートを削除します)」をクリックしたら、ポート上の ACL 適用を一括削除することができます。

「Action」バーの「Delete」をクリックすると、「Are you sure you want delete the item? (本当にこの ACL 適用を削除しますか？)」のプロンプトボックスが表示され、操作確認後、削除に成功します。



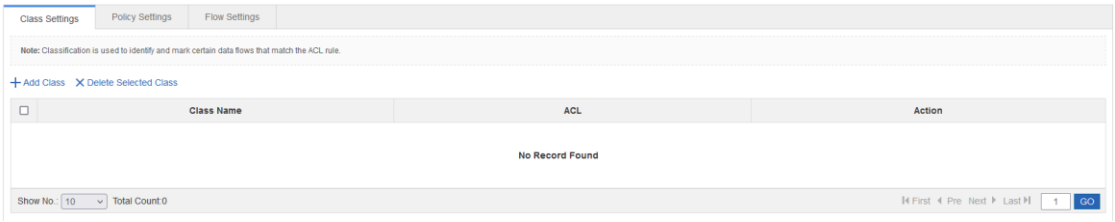
1.3.5.3 QoS

QoS（Quality of Service、サービス品質）とは、あるネットワークがさまざまな基盤技術を利用して、指定されたネットワーク通信によりよいサービスを提供できる能力のことです。QoS を配置したネットワーク環境は、ネットワーク性能の予測可能性を高め、ネットワークの帯域幅を効率的に割り振ることができ、ネットワーク資源をより合理的に利用することができます。

➘ クラス設定

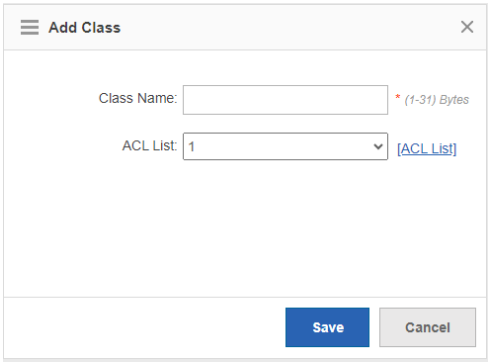
次の図は QoS クラス設定ページです。

図 1-24 クラス設定



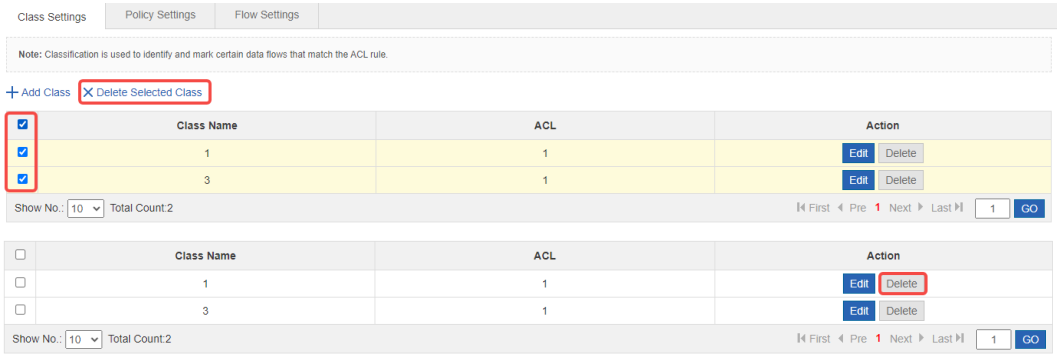
■ クラスの追加

「Add Class」をクリックすると、ポップアップページでクラス名及び関連する ACL List の設定が表示されます。次に、「Save」をクリックします。「Add Succeeded」ことを示すプロンプト情報が表示されたら、追加に成功しました。



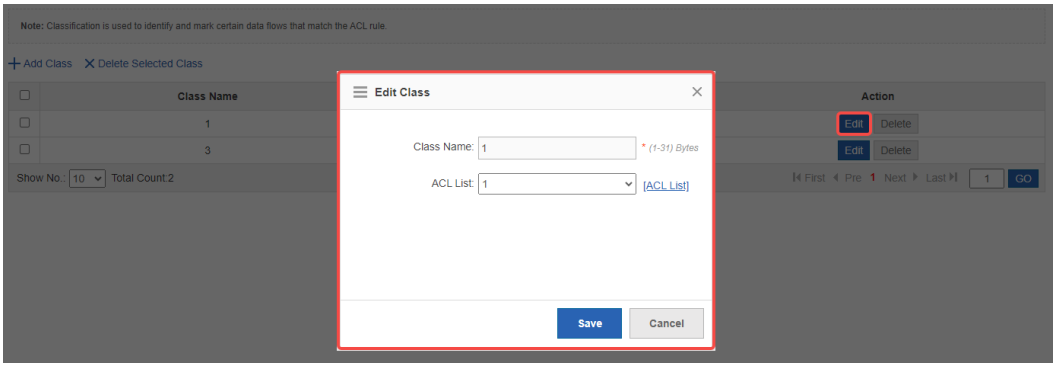
■ クラスの削除

「Delete Selected Class」をクリックして、削除するクラスを選択します。クラスリストでは、対応するクラスの後にある「Delete」をクリックして、対応するクラスを削除することもできます。



■ クラスの編集

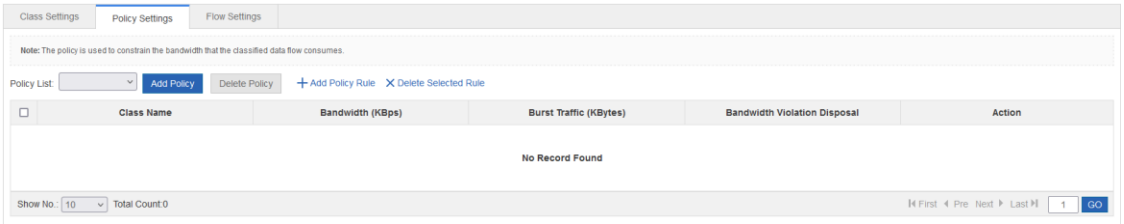
クラスリストの「Edit」をクリックすると、対応するクラスの情報が表示されます。メッセージを編集したら、「Save」をクリックします。



➘ ポリシー設定

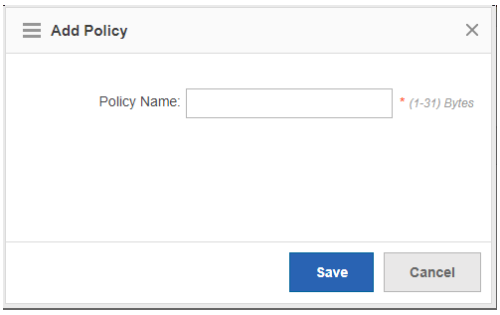
次の図は QoS ポリシーの設定ページです。

図 1-25 ポリシーの設定



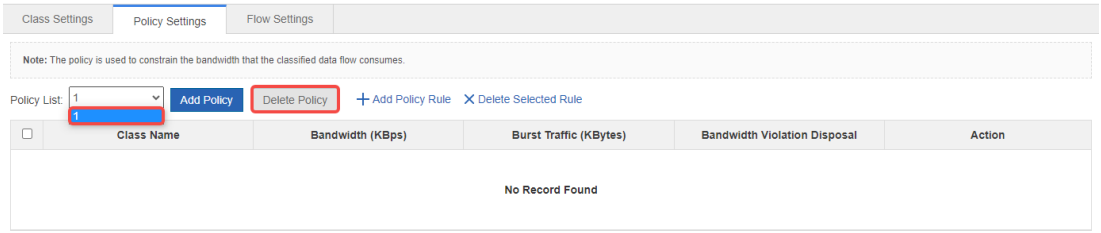
■ ポリシーの追加

「Add Policy」をクリックしてポップアップページでポリシーの名前を設定します。次に、「Save」をクリックします。「Add Succeeded」ことを示すプロンプト情報が表示されたら、追加に成功しました。



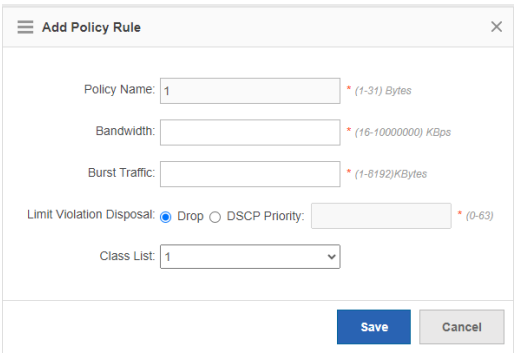
■ ポリシーの削除

「Delete Policy」をクリックすると、対応するポリシーを削除できます。



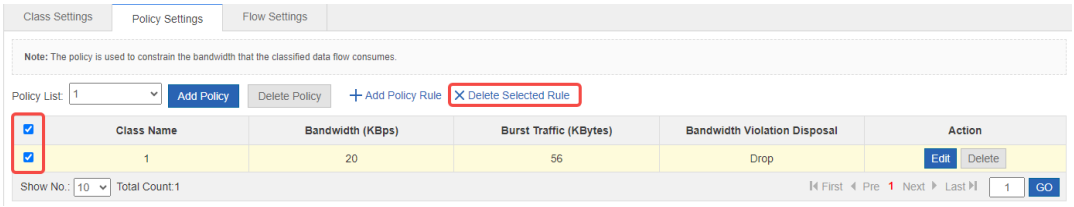
■ ポリシールールの追加

「Add Policy Rule」をクリックすると、ポリシーにルールを追加できます。ポリシー名、帯域幅、バーストトラフィック制限、オーバーラン動作、ポリシーに対応するクラスを設定できます。次に、「Save」をクリックします。



■ ポリシールールの削除

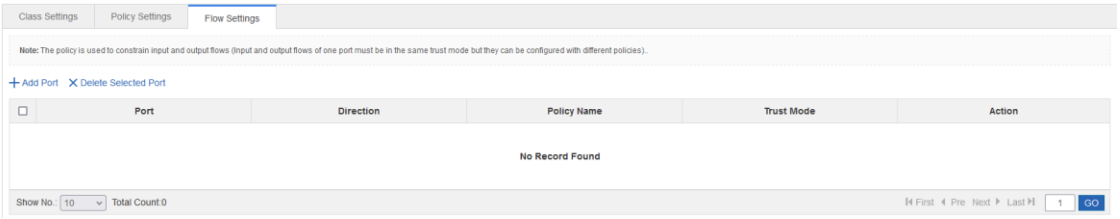
削除するルールを選択して、「Delete Selected Rule」をクリックすると、削除すべきポリシールールを削除することができます。



フローポリシー設定

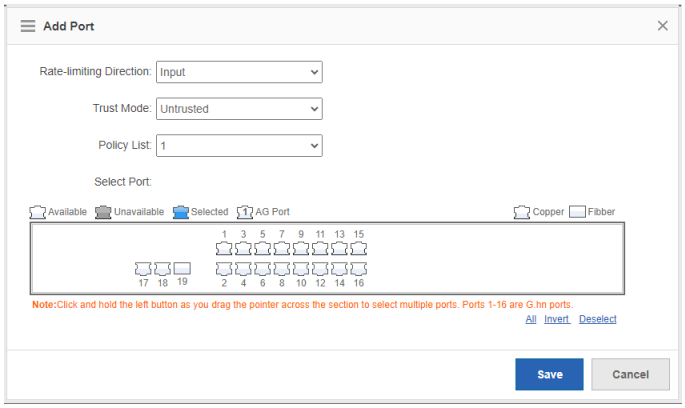
次の図は QoS フローポリシー設定ページです。

図 1-26 フローポリシー設定



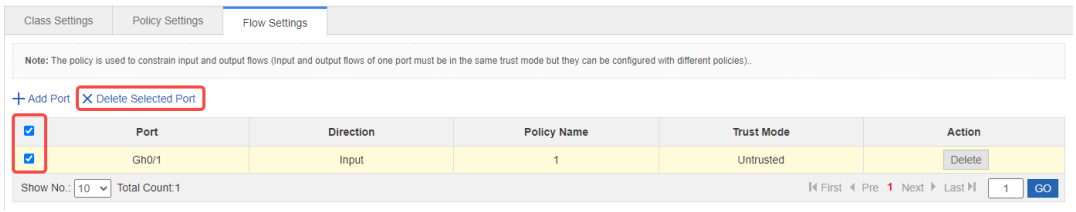
■ ポートの追加

「Add Port」をクリックすると、ポリシーをポートに適用できます。ポリシー適用のポート、ポリシー名、ポート信頼モード、速度制限方向を設定できます。次に、「Save」をクリックします。



■ ポートの削除

ポートリストの中の対応するポートを選択して、「Delete Selected Port」をクリックすると、対応するポリシー適用ポートを削除できます。



1.3.6 システム管理

システム管理ページでは、システム設定、システムのアップグレード、構成管理、管理者権限の構成を行うことができます。

1.3.6.1 システム設定

システム設定ページには、システム時間、パスワード、リセット、Web アクセス制御、SNMP の 5 つのタブがあります。

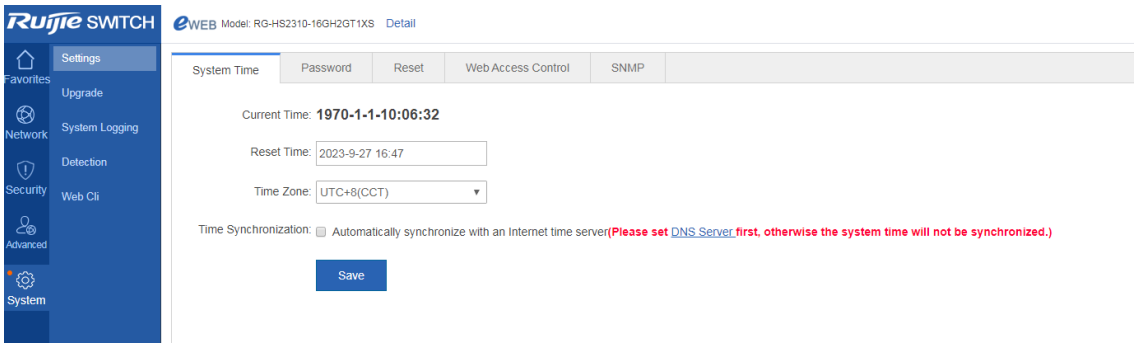
➘ **システム時間**

ネットワークデバイスのシステムクロックは、デバイス上で発生したイベントの時刻を記録します。例えば、システムログに表示されている時刻は、システムクロックから取得したものです。時間は*年-月-日、時間：分：秒、曜日*の形式で記録します。

初めてネットワークデバイスをご利用の場合は、システムクロックを現在の日時に手動設定します。

次の図は「システム時間」ページです。

図 1-27 システム時間



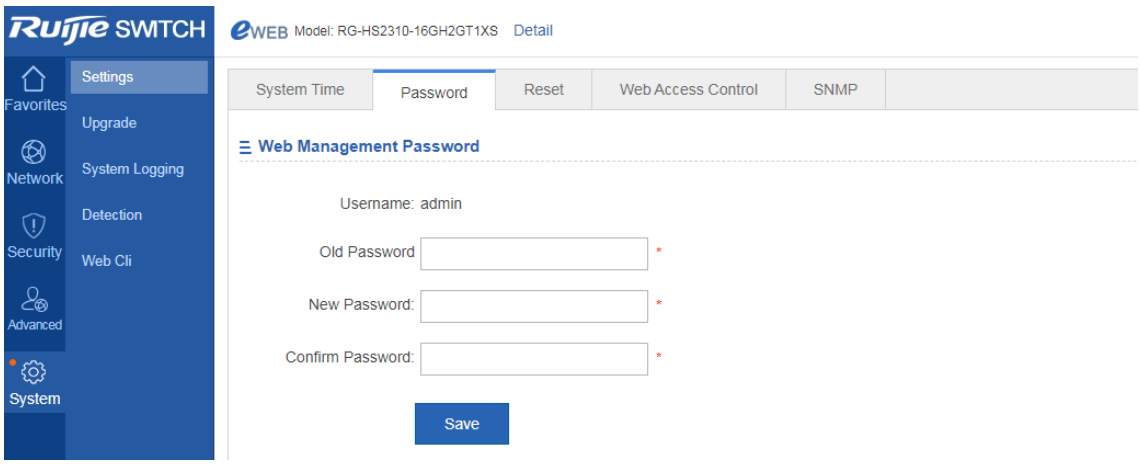
ページには現在のシステム時刻を表示します。現在のシステム時間は手動で設定できます。または、時間を設定するためにインターネットのタイムサーバーと自動的に同期することもできます。次に、「Save」をクリックします。「Save Succeeded」メッセージが表示されます。

📖 管理 IP アドレスが変わった場合、新しい IP アドレスが届くようにしなければなりません。そうでないと、Web 管理システムにログインできません。

パスワード

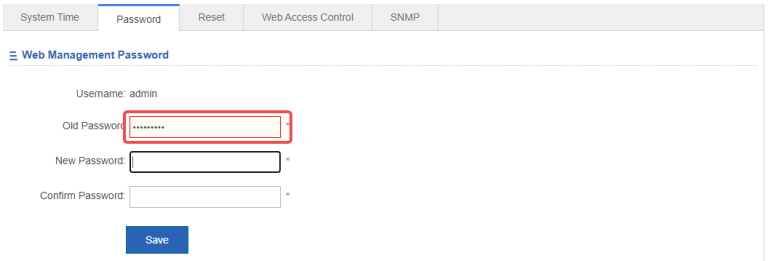
次の図は「パスワード」ページです。

図 1-28 パスワード



■ Web 管理用パスワード

Web ユーザーのパスワードを変更するには、古いパスワードを入力し、新しいパスワードを 2 回入力する必要があります。古いパスワードを誤って入力した場合、「古いパスワードは正しくありません」というメッセージが赤色で表示されます。その場合は、正しい古いパスワードを入力して「Save」をクリックします。

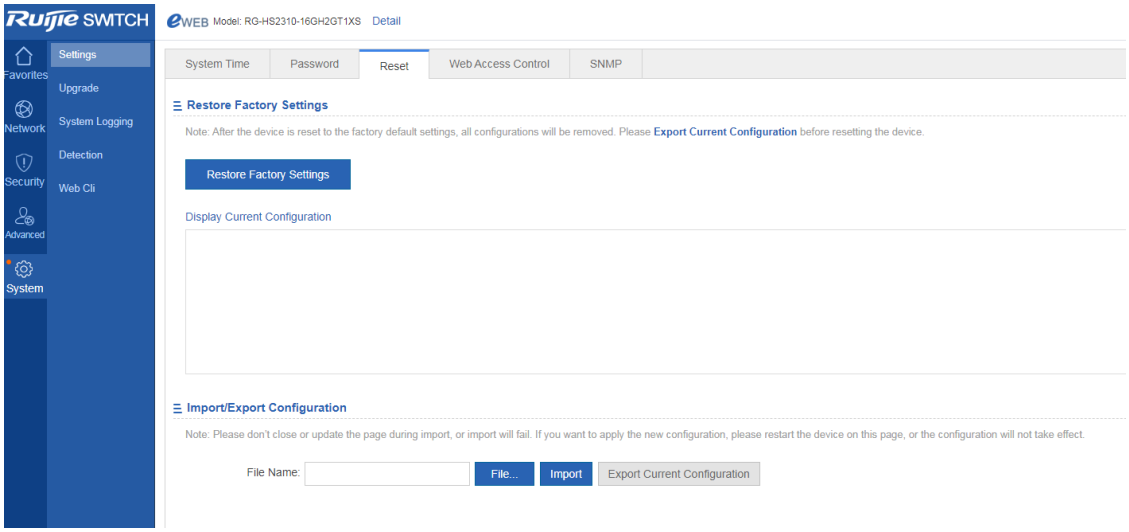


📖 Web 管理用パスワードを変更すると、デフォルト有効化パスワードも変更されます。

出荷時設定の復元

次の図はリセットページです。

図 1-29 リセット



■ インポート/エクスポート構成

構成をインポートしてデバイス構成を変更したり、デバイスを再起動して新しい構成をインストールしたり、現在の構成をバックアップとしてエクスポートすることができます。

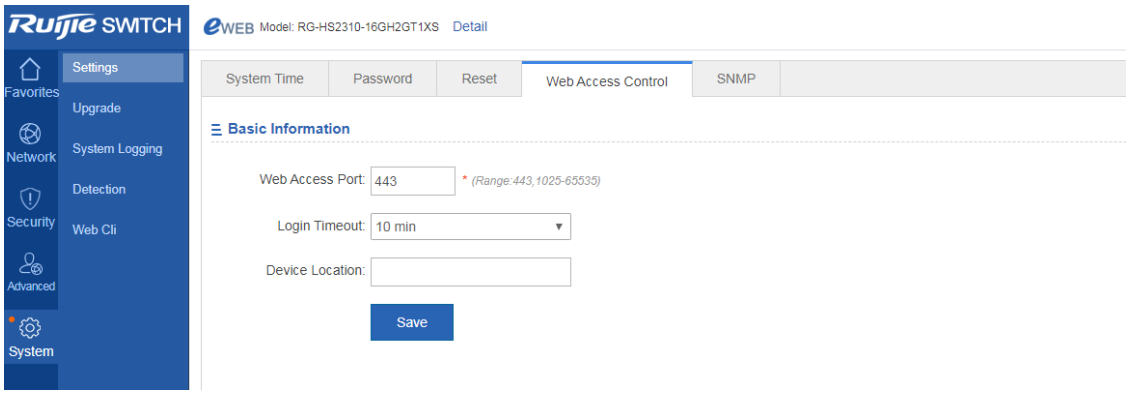
■ 出荷時設定の復元

「Restore Factory Settings」をクリックすると、現在の構成を工場出荷時の設定に戻すことができます。

ウェブアクセスコントロール

次の図は Web アクセスコントロールページです。

図 1-30 Web 管理



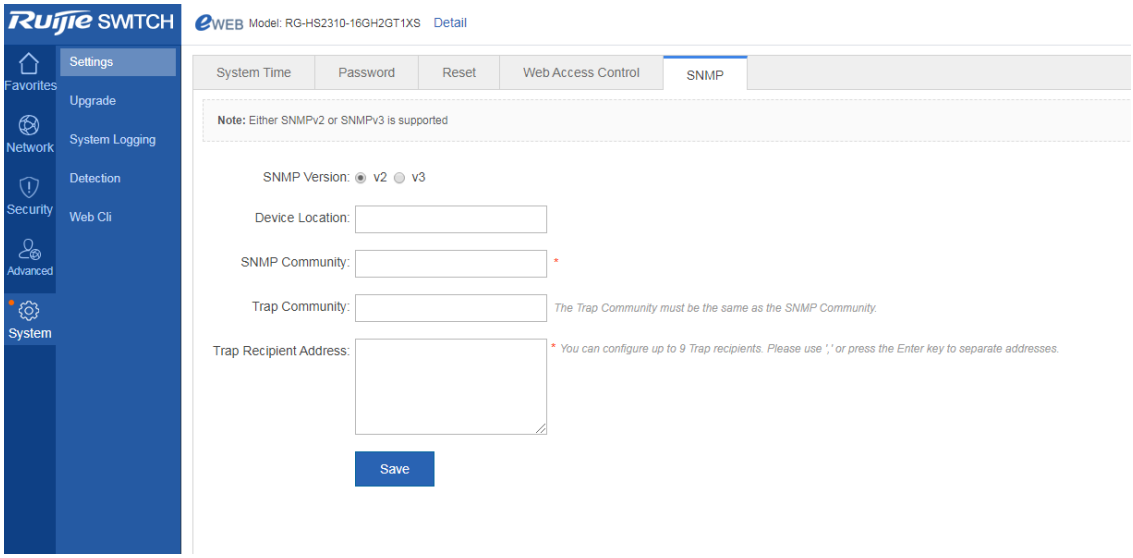
Web アクセスポート(必須)を指定し、必要に応じてログインタイムとデバイスの場所を指定して、「Save」をクリックします。

シンプルネットワーク管理プロトコル

シンプルネットワーク管理プロトコル(SNMP)は、これまでのネットワーク管理における支配的なプロトコルであり、ネットワーク管理のニーズに対応するために容易に実現できる基本的なネットワーク管理ツールとして設計されています。非常に分かりやすいので簡単なネットワーク管理プロトコルと名付けられました。これが広く受け入れられている重要な理由の 1 つは、ネットワーク管理のための主要なインターネット基準に加えて、それが比較的簡単であることです。SNMP には、SNMPv1、SNMPv2、SNMPv3 といったバージョンがあります。

次の図は SNMP ページです。

図 1-31 簡単なネットワーク管理プロトコル

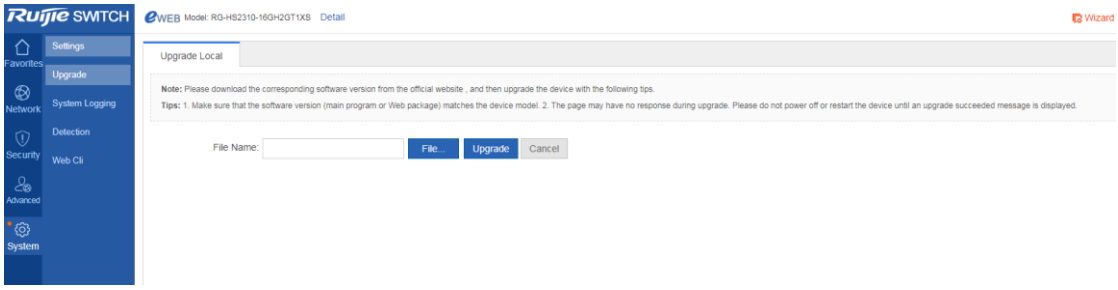


このページでは、SNMP バージョン、デバイス位置、SNMP パスワード、Trap コミュニティが必須です。その他のパラメータはオプションです。設定が完了したら、「Save」をクリックしま。

1.3.6.2 システムのアップグレード

次の図はアップグレードローカルページです。

図 1-32 アップグレードローカル



「File…」をクリックします。ローカルに保存されている bin ファイルを選択し、「Upgrade」をクリックしてアップグレードローカルを開始します。

1.3.6.3 システムログ

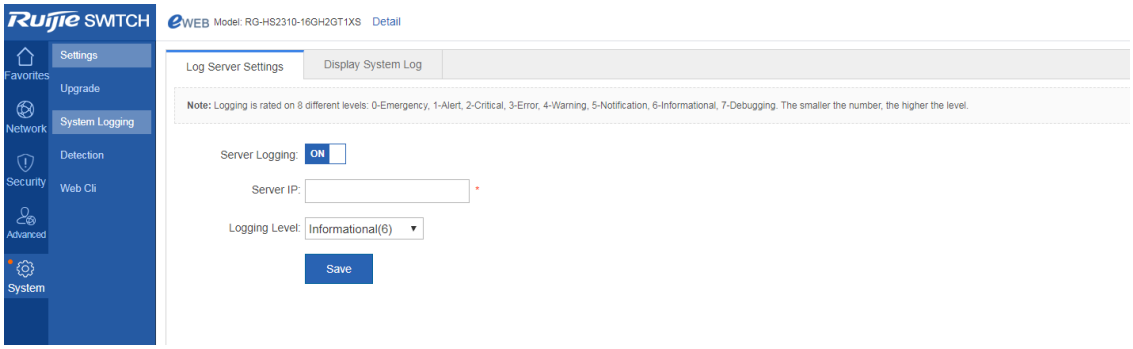
状態変化(リンクのオンとオフなど)や異常イベントはいつでも起こり得ます。Ruijie 製品は syslog メカニズムを提供しています。状態変化やイベント発生時に一定書式のメッセージ(ログパケット)を自働的に生成します。これらのメッセージは、コンソールや監視端末などの関連ウィンドウに表示され、メモリバッファやログファイルなどの媒体に記録され、または、ネットワーク上のログサーバに送信して、管理者がログパケットに基づいてネットワーク性能を分析し障害を識別することができるようにさせます。ログメールはタイムスタンプや番号を付けたり、深刻度別に分類したりできるので、管理者が簡単に読み込み、管理できます。

システムログページには、「ログサーバ設定」と「システムログの表示」の 2 つのタブがあります。

➘ ログサーバ設定

次の図はログサーバ設定ページです。

図 1-33 ログサーバ設定

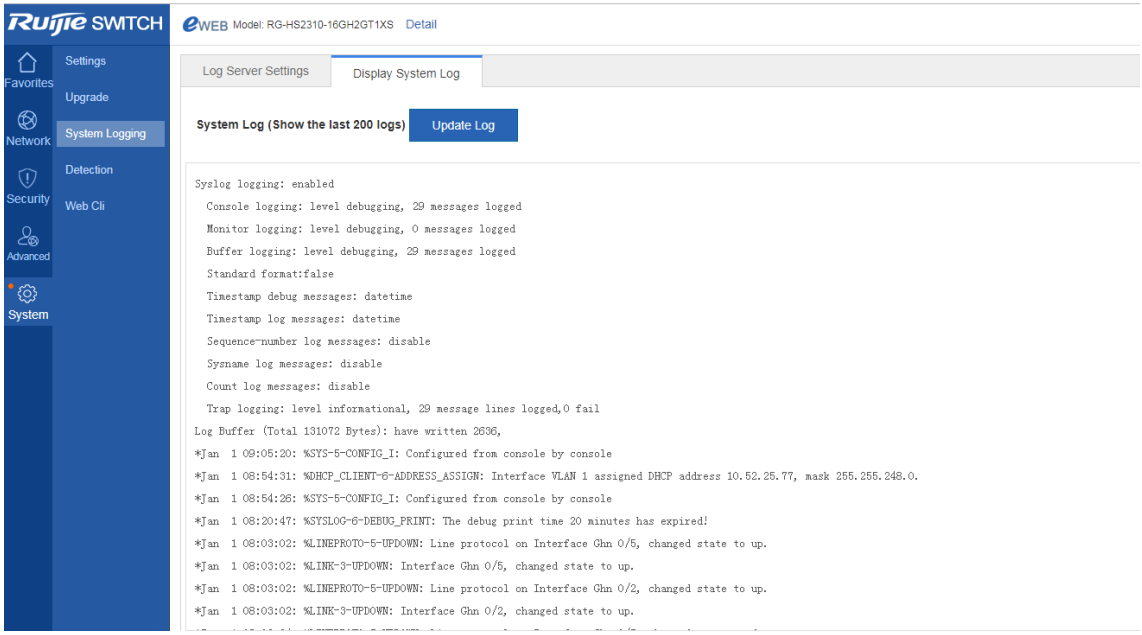


サーバーの IP アドレスやログレベルなど各種パラメータを設定します。構成が完了すると、デバイスは SYSLOG ログを該当するサーバーに送信します。

システムログの表示

次の図は「システムログの表示」ページです。

図 1-34 システムログの表示



テキストボックスに現在のログ情報が表示されます。「Update Log」をクリックすると、ログ情報が更新されます。

1.3.6.4 ネットワーク検出

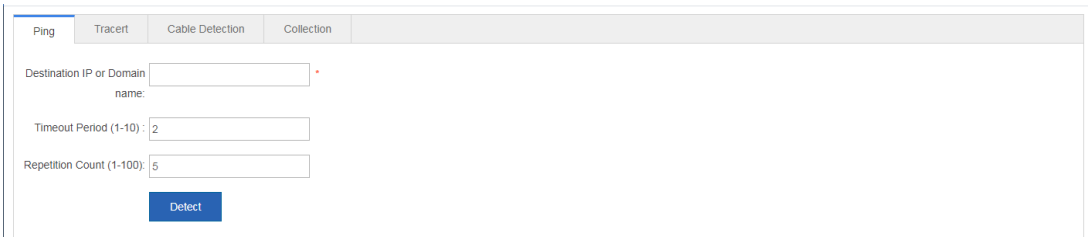
ネットワーク接続検出ページは、Ping、Tracert、Collection の 3 つのページに分かれています。

Ping

Ping ツールは、ICMP Echo Reply メッセージを要求するために、Internet control message protocol (ICMP) 要求メッセージをターゲットホストに送ります。これによって、Ping ツールは 2 つのネットワークデバイス間の遅延と接続性を決定します。

Ping ページは次の図のようになります。

図 1-35 Ping

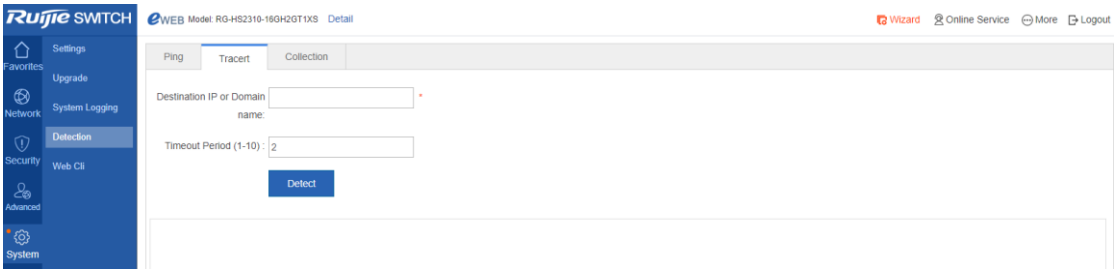


宛先の IP アドレスを入力し、「Detect」をクリックします。次に、検出結果がテキストボックスに表示されます。

Tracert

Tracert ツールは、ICMP Echo Reply メッセージを要求するための Internet Control Message Protocol (ICMP)要求メッセージをターゲットホストに送信します。これによって、tracert ツールは 2 つのネットワークデバイス間のすべての次のホップを決定します。

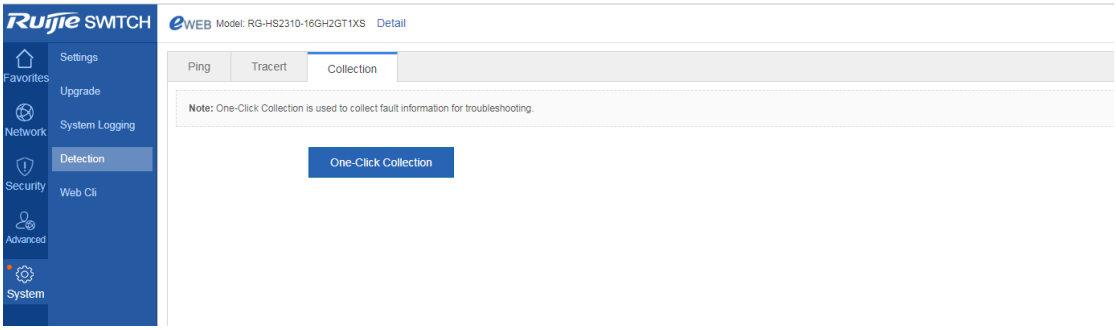
図 1-36 Tracert



➘ ワンクリック収集

「One-Click Collection」をクリックして、トラブルシューティングのためにトラブル情報を収集します。

図 1-37 ワンクリック収集



1.3.6.5 コマンドラインインターフェース

このページは CLI をシミュレートし、CLI コマンドを入力し、Enter を押すか「Send」をクリックします。Tab キーと「?」と組み合わせて使用することもできます。

図 1-38 ネットワークコマンドラインインターフェース