

RG-HS2310-16GH2GT1XS

Web-GUI 操作マニュアル

著作権・商標権について

Copyright © 2023 Ruijie Networks

本文書に関する一切権利はRuijie Networksに保有します。営利目的で本文書のコンテンツを書面による事前许 可なく全体または部分的に、複製、抜粋、バックアップ、修正、転用、翻訳などの二次利用することはできま せん。

Ruíjie

以上は商標はRuijie Networksに保有します。

本文書に記載されているほかの商標または登録商標は各権利者に所属します。

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: <u>https://ruijie.co.jp</u>/_
- サポートサイト: <u>https://www.ruijie.co.jp/service</u>
- 故障・修理のお申し込み: <u>https://www.ruijie.co.jp/service/post-sales</u>
- サポートメールアドレス: <u>support_jp@ruijienetworks.com</u>

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。

はじぬ	かに		I
1 \	Web 管理システ	Д	1
1	.1 概要		1
1	.2 Web ログ-	イン	1
	1.2.1 機能の	D配置	1
1	.3 ネットワー	・ク管理システム	4
	1.3.1 クイッ	ックガイド	7
	1.3.2 よく傷	もいます	7
	1.3.2.1	ホームページ	8
	1.3.2.2	VLAN	8
	1.3.2.3	ポート	12
	1.3.2.4	再起動	15
	1.3.3 ネット	·ワーク	15
	1.3.3.1	MAC アドレス	15
	1.3.3.2	RLDP	19
	1.3.4 セキニ	1リティ	21
	1.3.4.1	ARP 攻擊防止	21
	1.3.4.2	ストームコントロール	23
	1.3.5 ハイス	スペック	25
	1.3.5.1	保護ポート	25
	1.3.5.2	ACL	26
	1.3.5.3	QoS	30
	1.3.6 シスラ	⁻ ム管理	34
	1.3.6.1	システム設定	34
	1.3.6.2	システムのアップグレード	38
	1.3.6.3	システムログ	38
	1.3.6.4	ネットワーク検出	40
	1.3.6.5	コマンドラインインターフェース	41

目次

1 Web 管理システム

1.1 概要

ユーザーは Google、Firfox 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。

ID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 1-1 ログインページ



WEB | ©2000-2023 Ruijie Networks Co., Ltd. | Official Website | Online Service | Service Mail

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
aummaumm	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 1-2 パスワードの変更

Modify password					
Username:	admin				
New Password:	Please enter a new password				
Confirm Password:	Please enter a new password				
	Modify				

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。

$\hat{\Box}$	Home	Home							
vorites	VLAN							007470	
Ø work		CPU: 2.4	40% Memory	7 : 26.4% 3	Current Tim Running Tir	e:1970-01-01 00:05:23 ne:0 d 00 h 05Min	Model:RG-HS2310-16GH Version:HS2310_RGOS 1 Device MAC:4826.0000.0	2GT1XS 11.4(1)B90 022	
D	Restart						Device SN:MACC942570	105	
curity		Port Ir	formation CRefres	1					
0 -00		Port	Input Rate 🍦	Output Rate 🏻 🌲	Status(Port real speed)	InOctets/OutOctets	UnderSize/OverSize	CRC/FCS Error	Collisio
		Ghn0/1	ОK	ОК	Not Connected	0/0	0/0	0/0	0
}} !om		Ghn0/2	OK	0K	Not Connected	0/0	0/0	0/0	0
lem		Ghn0/3	OK	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	ОK	ОK	Not Connected	0/0	0/0	0/0	0
		Ghn0/6	ОK	ОК	Not Connected	0/0	0/0	0/0	0
		Ghn0/7	ОK	0K	Not Connected	0/0	0/0	0/0	0
		Ghn0/8	ОK	ОК	Not Connected	0/0	0/0	0/0	0
		Ghn0/9	ок	ОK	Not Connected	0/0	0/0	0/0	0
		Ghn0/10	0.4K	5.9K	Connected(1000M)	91893/843078	0/0	0/0	0

図 1-3 ホームページ

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。
<u> </u>	選択したポートです。
517	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。
5-7	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。
	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
All Invert Deselect	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

Available 🚆 Unavailable 🚍 Sel	ected 17AG Port	Copper Fibber
17 18 19	2 4 6 8 10 12 14 16	

Note:Click and hold the left button as you drag the pointer across the section to select multiple ports. Ports 1-16 are G.hn ports.

● パネル操作

ポートをクリックまたはカーソルを移働してパネル上で復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

🚰 Available 🚆 Unavailable 🚆	Selected SI AG Port	Copper Fibber
	1 3 5 7 9 11 13 15 그그그그그그그그	
17 18 ¹⁹		

Note: Click and hold the left button as you drag the pointer across the section to select multiple ports. Ports 1-16 are G.hn ports.

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 1-4 クイックガイド

∃ Wizard		×
Mgmt Port:	vlan 1	
IP:	10.52.25.77	
Mask:	255.255.248.0	
Route :	10.52.24.1	
DNS:	172.30.44.20	
IPv6/Mask:		
IPV6 Route :		
Reset Time:	2023-9-19 09:20	
Time Zone:	UTC+8(CCT) *	
		Save Cancel

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。

图 1-1	ホー	ムペー	・ジ
-------	----	-----	----

Rui	JIE SWITCH	WEB Mode	el: RG-HS2310-16GH2GT1XS	Detail			G Wizard 🙎	Online Service 💮 More	e ⊡ Logout
合	Home	Home							
Favorites	VLAN	CPU: 2	.40% Memory	: 26.4% 3	Current Tim	e:1970-01-01 00:05:23	Model:RG-HS2310-16GH	2GT1XS	
Network	Port			Up Port C	ount Running Tir	ne:0 d 00 h 05Min	Device MAC:4826.0000.0 Device SN:MACC942570	022	
() Security	Restart	Port	Information CRefresh						
		Port	Input Rate 🌲	Output Rate	Status(Port real spee d)	InOctets/OutOctets	UnderSize/OverSize	CRC/FCS Error	Collision Count
Auvanceu		Ghn0/1	ΟK	ОК	Not Connected	0/0	0/0	0/0	0
C)Evision		Ghn0/2	ОК	ОК	Not Connected	0/0	0/0	0/0	0
System		Ghn0/3	ОК	ОК	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	ОК	ОK	Not Connected	0/0	0/0	0/0	0
		Ghn0/6	ОК	ОK	Not Connected	0/0	0/0	0/0	0
		Ghn0/7	ОК	ОK	Not Connected	0/0	0/0	0/0	0
		Ghn0/8	ОК	ОK	Not Connected	0/0	0/0	0/0	0
		Ghn0/9	ОК	ОK	Not Connected	0/0	0/0	0/0	0
		Ghn0/10	0.4K	5.9K	Connected(1000M)	91893/843078	0/0	0/0	0

1.3.2.1 ホームページ

図 1-5 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。

Ruij	JIE SWITCH	WEB Mode	el: RG-HS2310-16GH2GT1XS	Detail			R Wizard 🙎	Online Service 💮 More	e 🕞 Logou
`	Home	Home							
Favorites	VLAN								
() Network		CPU: 2	.40% Memory	: 26.4% 3	Current Tim Running Tir	Model:RG-HS2310-16GH Version:HS2310_RGOS1 Device MAC:4826.0000.0			
Restart							Device SN:MACC942570	105	
Security		Port	Information CRefresh						
200 Actorphicad		Port	Input Rate 🏻 🌲	Output Rate	Status(Port real speed)	InOctets/OutOctets	UnderSize/OverSize	e CRC/FCS Error	Collision Count
Muvanceu		Ghn0/1	ОK	0K	Not Connected	0/0	0/0	0/0	0
ŝ		Ghn0/2	ОК	ОК	Not Connected	0/0	0/0	0/0	0
System		Ghn0/3	ОК	ОК	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	ОК	ОК	Not Connected	0/0	0/0	0/0	0
		Ghn0/6	ОК	ОК	Not Connected	0/0	0/0	0/0	0
		Ghn0/7	ОК	ОК	Not Connected	0/0	0/0	0/0	0
		Ghn0/8	ОК	ОК	Not Connected	0/0	0/0	0/0	0
		Ghn0/9	ОК	ОК	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 1-7 のような 3 段階のデバイスによって行われます。

図 1-6 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 1-7 VLAN 設定

VLAN Settings	ngs Trunk Port										
+ Batch Add VLAN + Add VLAN × Delete Selected VLAN											
	VLAN ID	\$	VLAN name	Port	Action						
	1		VLAN0001	Gi0/1-6,Gi0/9-10	Edit						
	2		rrrrrrr	Gi0/7-8	Edit Delete						
Show No.: 10×	Show No: V Total Count 2										

■ 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
 - 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 delet 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 1-9 トランクポート

VLAN Settings	Trunk Port		
Note: If a port allows	multiple VLAN packets to go thro	ough, configure it as a trunk port. It is	s recommended to configure the port connected to the network device as a trunk port.
No Trunk Port			
Native	VLAN: 1	* Range(1-4094)	
Allowed	VLAN: 1-4094	The VLAN range is	formatted as 3-5,100.
Selec	ct Port:		
Available 📃 U	Inavailable 📄 Selected 🛐 /	AG Port	Copper Fibber
		5 7 9 11 13 15 	
Note:Click and hold	the left button as you drag the po	pinter across the section to select mi	uttiple ports. Ports 1-16 are G.hn ports. <u>All Invert Deselect</u>
	Save	Cancel	

■ 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。

	VLAN Settings	Trunk Port								
	Note: If a port allows multiple VLAN packets to go through, configure it as a trunk port. It is recommended to configure the port connected to the network device as a trunk port.									
Ĩ										
	Te0/19 ×	Batch Del								
-										

■ 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。

VLAN Settings	Trunk Por	t	
Note: If a port allows	multiple VLAN p	ackets to go throug	ph, configure it as a trunk port. It is recommended to configure the port connected to the network device as a trunk port.
Gi0/18	⊗ Te0/19 ☑	× Batch Del	

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 1-10 ポート設定

July Control I	EMER MODEL HG-H52510-160H2011X5	Detail									C Wizard	2 Online Service	⊖ More	⊡ Log
Home	Port Settings Aggregate port	Port Mirroring	Rate Limiting											
VLAN	+ Batch Add + Add SVI													
Port	= 13 Port													
Restart	E Grant													
ity	Port	Stat	ıs	IP		N	lask		IPv6	Descriptio	n	Act	tion	
	VLAN 1 Up			10.52.25.7	7	255.2	55.248.0					Edit	Delete	
ed	VLAN 2 Up											Edit	Delete	
	Show No.: 10 Y Total Count:2										l∉First ∢ Pr	1 Next ⊁ Last	H 1	G
m	= L2 Port													
	Port	Status	Po	rt Type	Acce	is VLAN	Native \	/LAN	Permit VLAN	De	scription		Action	
	Ghn0/1	Up	A	CESS		1	1					E	fit Detail	
	Ghn0/2	Up	A	CESS		1	1					E	fit Detail	
	Ghn0/3	Up	A	CESS		1	1					E	fit Detail	
	Ghn0/4	Up	A	CESS		1	1					E	fit Detail	
	Ghn0/5	Up	A	CESS		1	1					E	fit Detail	
	Ghn0/6	Up	A	CESS		1	1					E	fit Detail	
	Ghn0/7	Up	A	CESS		1	1					E	fit Detail	
	Ghn0/8	Up	A	CESS		1	1					E	fit Detail	
	Ghn0/9	Up	A	CESS		1	1					E	fit Detail	
	Ghn0/10	Up	A	CESS		1	1					E	fit Detail	
	Show No.: 10 Total Count:19										I∢First ∢ Pre	2 Next I Last	H 1	GC
	Show No.: 10 V Total Count 19										Manar 4 199	a weat P Last		

■ 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。

义	1-11 集	約ポート				
Ruij	JIC SWITCH	CWEB MARE ROADSTO-HOROTOS Detail	🕞 Wizard	2 Online Service	⊖More [> Logou
Favorites	Home	Port Settings Aggregate port Port Mirroring Rate Limiting				
۲	VLAN	E Global Configuration				
Network	Restart	Note the aggregate port is used to perform traffic allocation according to the selected load-balance algorithm.				
U Security		Load-balance: Source MAC and Destination *				
2gg Advenced		Sare Default Settings				
0		E Aggregation port settings				
-,		No Aggregate				
		Aggregate Port ID * //respect-10				
		Select Port				
		Availability Concept If a Sort Concept If a Sort Image: Sort Sort Sort Sort Sort Sort Sort Sort				

■ 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。

Ξ Aggregation port settings
In order to provide increased bandwidth and redundancy, multiple physical ports (member ports) are combined into one logical port (aggregate port). An aggregate port contains up to eight member ports, and the aggregate port load balances traffic across these physical ports.
AG1 X Batch Del

■ 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。

⊒ Aggregation port settings
In order to provide increased bandwidth and redundancy, multiple physical ports (member ports) are combined into one logical port (aggregate port). An aggregate port contains up to eight member ports, and the aggregate port load balances traffic across these physical ports.
AG1 AG2 XBatch Def

▲ 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 1-12 ポートミラーリング

Ruij	IC SWITCH	WWEB MORE RG-H5216-MGH30TX/S Detail	C Wizard	오 Online Service	⊕ More []	Logout
Favorites	Home	Port Settings Aggregate port Port Mirroring Rate Limiting				
(Network	Port	Note: Plot minimity is the spatiality is send a source port is been on the source port to the destination port for analysis by a network analyzer. Traffic on multiple source ports can be minimed to one wrige destination port. Tips A source port sends to a destination port.				
() Security	Restart	Monitor Packets Al Packets +				
		Select Source Plot: (Viv can select multiple ports, but it may affect device performance.)				
System						
		Note:Clark and hold the left button as you drag the pointer across the section to select multiple ports. Firsts 1.16 are 0 An ports. All invest. Deselect				
		Select Destination Port: (You can select only one port)				
		Charaltable martine fabriced Carlos Port Corpor - Pitter				
		Danwinst				
		Save Refresh				

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、復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 1-13 再起動

Ruijie SWTCI	WEB Model: RG-H82310-160H2GT1X8 Detail	17 Wizard 2 Online Service ⊕ More 日 Logout
Home	Restart	
	Note: Click 'Restart to restart the device. Please wait a few minutes and the page will be refreshed after restart.	
Restart	Restart	
<ඊම Advanced		
©) System		

「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

Ruij	IE SWITCH	WEB Model: RG-H	S2310-16GH2GT1XS De	tail							C Wizard	Online Service	⊖ More	⊖ Logout
C Favorites	MAC Address	Mac Table	Static MAC Address	Filtering MAC Address										
Network	RLDP	Note: The switch fo authentication enable	rwards data according the h led, you can implement auth	AC address inside the data frame ventication exemption by binding N	. If you configure MAC-po MAC address with port.	rt binding on a network device	e manually, affer you add	a static address, the switcl	h that receives the packet with t	ne same destination addr	ress forwards it to t	he specified port. With i	102.1X	
() Security		+ Add Static Addre	ess 🗙 Delete Static Ad	tdress										
2a			Port			MAC Address			VLAN ID			Action		
Advanced							No Record Fou	ind						
		Show No.: 10 v	Total Count:0								H First ∢	Pre Next ▶ Last	1	GO

図 1-14 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。

⊟ Add Static Address			\times
MAC Address:			Î
VLAN ID:	*		
Select Port: *			
🚰 Available 💼 Unavailable	Selected AG Port	Copper Eibber	
17 II	1 3 5 7 9 11 13 15 <u>''''''''''''''''''''''''''''''''''''</u>		
C		Deselect	1
			•
		Save Cance	I

- 静的アドレスの削除
 - (1) 復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 staic 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 1-15 フィルタリングアドレスの設定

Ruij	IE SWITCH	WEB Model: RC	G-HS2310-16GH2GT1XS Deta						(G)	Mizard 🙎 Online Service 💮	More 🕞 Logout
Favorites	MAC Address	Mac Table	Static MAC Address	Filtering MAC Address	switch receives a packet with	h the source/destination MAC ad	dress which is configured as a filter ad	dress, it discards the packet. You	can prevent the ARP attack by cor	ifiguring a filter address the same as t	he MAC
Network ① Security		+ Add Filter Ad	packets.	55							
Advanced			M	AC Address		Nol	VLAN ID Record Found			Action	
(c) System		Show No.: 10	V Total Count 0						ł	(First ≮ Pre Next ⊁ LastM	1 60
										entre 1013 Duile Maharda Ca	

■ 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。

Mac Table	Static MAC Address	Filtering MAC Address				
Note: The switc configuring a filt	h forwards data according the MA er address the same as the MAC	C address inside the data frame. I address of ARP packets.	f a switch receives a packe	et with the source/destination MAC add	dress which is configure	id as a fitter address, it discards the packet. You can prevent the ARP attack by
+ Add Filter Ad	dress 🗙 Delete Filter Addr	ess	Add Filter Addres	\$\$	×	
Show No.: 10	MAC Add	ress	MAC Address:	•		Action
				Save	Cancel	

■ 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。

Note: The switch forwards data according the MAC address inside the data frame. If a switch receives a packet with the source/destination MAC address which is configured as a filter address, it discards the packet. You can prevent the ARP attack by configuring a filter address the same as the MAC address of ARP packets.						
+ Add Filter Address X Delete Filter Address						
	MAC Address	VLAN ID	Action			
4222.6522.8866 1 Edit Delete						
Show No. 10 V Total Count 1 I4 First 4 Pire 1 Next 1 Last 1 1 GO						

- 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。

+ Add Filt	Add Filter Address X Delete Filter Address							
	MAC Address	VLAN ID	Action					
	4222.6622.8866	1	Edit Delete					
	4222.6622.8867	4	Edit Delete					
Show No	Show No.: 10 V Total Count.2 M First 4 Pre 1 Next 1 Last M 1 600							

(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。

	MAC Address	VLAN ID	Action			
	4222.6622.8866	1	Edit Delete			
	4222.6622.8867	4	Edit Delete			
Show	Show No.: 10 v Total Count 2 III First 4 Pre 1 Next 1 Last 1 1 GO					

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 1-16 RLDP 設定

Ruíjie Switch	WEB Model: RG-HS2310-160H20T1XS Detail			🕞 Wizard	2 Online Service	⊡ More
Favorites PI DP	RLDP Settings					
·Ø	≡ Global configuration					
Network	Note: RLDP enables you to detect link failure quickly. RLDP can	run on the port only after it is enabled globally.				
() Security	RLDP: ON					
29 Advanced	Detection 3 Range(2-15 Interval:					
0	Detection Count: 2 Range(2-10					
System	errdisable Range(30-8 recovery:	5400n)				
	Save					
	Note: 1. Enabling RLDP on the port can avoid broadcast storm of 2. Unidirectional/Bidirectional link detection requires the po	aused by loops. It is recommended to enable RLDP on the port connected to the rts on both ends of the link to be enabled with RLDP. It is recommended to config	PC ; jure RLDP to monitor the link between two switches.			
	+ Add Port X Delete Port					
	Port	Detection Type	Troubleshooting		Action	
		No Record	Found			
	Show No.: 10 V Total Count:0			M First	€ Pre Next IF Last	H 1 GO
				#20	V5-2022 Duile Networks	Co. 141 LOBeini Webeite

ゾローバル設定

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。

⊒ Global confi	guration	
Note: RLDP ena	ables you to detect link failure quick	y. RLDP can run on the port only after it is enabled globally
RLDP:	ON	
Detection Interval:	3	Range(2-15)
Detection Count:	2	Range(2-10)
errdisable recovery:		Range(30-86400s)
	Save	

▶ 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。

Note: RLDP enables you to detect link failure quickly. RLDP c	Batch Add	×
RLDP: 00 Detection 3 Ranger2 Interval:	Detection Mode Underschool Link Detection V Troubleshooting Warning V	
Detection Count: 2 Program	Select Fort △ Available Selected ① Available Select Fort 1 3 5 7 8 11 13 15 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	er
Port Configuration Note: 1: Enabling RLDP on the port can avoid broadcast stor: 2: Underectional/Biddrectional link detection requires the Add Port X Delete Port	Al Intel Date	<u>ect</u>
Port	Save Cance	əl

■ 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。

+ A00								
	Port	Detection Type	Troubleshooting	Action				
0	TenGigabitEthernet 0/19	Unidirectional Link Detection	Warning	Edit Delete				
Shov	I∢ First ∢ Pre 1 Next ⊁ Last ⊁I 1 GO							

- RLDP ポートの削除
 - 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。

+ Add Po	+ Add Port X Delete Port								
	Port	Detection Type	Troubleshooting	Action					
•	GigabitEthernet 0/18	Unidirectional Link Detection	Warning	Edit Delete					
	TenGigabitEthernet 0/19	Unidirectional Link Detection	Warning	Edit Delete					
Show N	o.: 10 V Total Count:2	[« First ∢ Pre 1 Next ▶ Last ▶] 1 GO							

(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。

Port	Detection Type	Troubleshooting	Action
GigabitEthernet 0/18	Unidirectional Link Detection	Warning	Edit Delete
TenGigabitEthernet 0/19	Unidirectional Link Detection	Warning	Edit Delete

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 1-17 ARP エントリ

ARF	^o Entries					
🔡 Dyr	To Dynamic Binding>>Static Binding 🖁 Remove static Binding 📱 Manual Binding Search					
	IP	MAC	Туре	Action		
	192.168.1.200	00e0.4c00.2155	Local ARP Entry	Dynamic Binding>>Static Binding		
	192.168.21.1	0000.5e00.0115	Dynamic Binding	Dynamic Binding>>Static Binding		
	192.168.21.138	40b0.3438.536a	Dynamic Binding	Dynamic Binding>>Static Binding		
	192.168.21.229	00e0.4c00.2155	Local ARP Entry	Dynamic Binding>>Static Binding		
Show	Show No.: 10 ▼ Total Count: 4 If First 4 Pre 1 Next ▶ Last № 1 GO					

• 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。

ARP Entries						
På Dynamic Binding>>Static Binding 😵 Remove static Binding 🔹 Manual Binding Search						
	IP	MAC	Туре	Action		
	10.52.24.1	ecb9.70b7.00ee	Dynamic Binding	Dynamic Binding>>Static Binding		
	10.52.24.35	0023.24e3.f94b	Dynamic Binding	Dynamic Binding>>Static Binding		
	10.52.25.61	00d0.f822.3377	Dynamic Binding	Dynamic Binding>>Static Binding		
	10.52.25.65	300d.9e3e.ae48	Dynamic Binding	Dynamic Binding>>Static Binding		
	10.52.25.76	00e0.4c00.215f	Local ARP Entry	Dynamic Binding>>Static Binding		

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。

IP	MAC	Туре	Action
10.52.24.1	ecb9.70b7.00ee	Dynamic Binding	Dynamic Binding>>Static Binding
10.52.24.35	0023.24e3.f94b	Dynamic Binding	Dynamic Binding>>Static Binding
10.52.25.61	00d0.f822.3377	Dynamic Binding	Dynamic Binding>>Static Binding

● 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 Bingding(静的バインディングを削除 します)」をクリックします。

ARF	ARP Entries							
Rà Dynamic Binding>>Static Binding 🐕 Remove static Binding 💲 Manual Binding Static and Binding Static Binding Static Binding Remove static Binding Remov								
	IP	MAC	Туре	Action				
	10.52.30.150	c85b.76a4.4dad	Static Binding	Remove static Binding				
	10.52.24.1	ecb9.70b7.00ee	Static Binding	Remove static Binding				

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

IP	MAC	Туре	Action
10.52.30.150	c85b.76a4.4dad	Static Binding	Remove static Binding
10.52.24.1	ecb9.70b7.00ee	Static Binding	Remove static Binding

- 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。

ARP	ARP Entries						
1월 Dyr	På Dynamic Binding>Static Binding 🕏 Remove static Binding 🖥 Manual Binding 🕼 Search						
	IP	MAC	Туре	Action			
	10.52.30.150	c85b.76a4.4dad	Static Binding	Remove static Binding			

(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。

Manual binding ARP		×
IP:	*	
MAC:	*	
ок	Cancel	

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。

Storm Co	Storm Control						
+ Add Port X Delete Selected Port							
	Port	Broadcast	Multicast	Unicast	Action		
	Ghn0/1	÷	-	-	Edit Delete		
	Ghn0/2	÷	-	-	Edit Delete		
	Ghn0/3	÷	÷	-	Edit Delete		
	Ghn0/4	÷	÷	-	Edit Delete		
	Ghn0/5	÷	÷	-	Edit Delete		
•	Ghn0/6	· ·	· ·		Edit Delete		
	Ghn0/7		-	-	Edit Delete		
	Ghn0/8				Edit Delete		
	Ghn0/9				Edit Delete		
	Ghn0/10		-	-	Edit Delete		
Show No.	.: 10 V Total Count:19			14 First			

図 1-18 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。

🕜 Available 💼 Unavailable 💼	Selected 11AG Port	Copper Elibber
222		
17 18 15	2 4 6 8 10 12 14 16	
Note:Click and hold the left button a	s you drag the pointer across the section to select multiple port	s. Ports 1-16 are G.hn ports. All Invert Deselect
Туре: 🖲 В	indwidth Usage 🔿 Packets 🔿 Kilobits	
Benaderat		
Broaucasi.	1	
Multicast:	96	
	%	
Unicast:		
Unicast:		

- 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。

Storm Con	Storm Control						
+ Add Port X Delete Selected Port							
	Port	Broadcast	Multicast	Unicast	Action		
	Ghn0/1	1%	1%	1%	Edit Delete		

(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。

Edit Port - Ghn0/1		×
Туре:	Bandwidth Usage Packets	⊖ Kilobits
Broadcast:	1	%
Multicast:	1	%
Unicast:	1	%
	Save	e Cancel

■ 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。

Stor	m Control						
+ Add	+ Add Port × Delete Selected Port						
	Port	Broadcast	Multicast	Unicast	Action		
	Ghn0/1	1%	1%	1%	Edit Delete		
	Ghn0/2	-	-	-	Edit Delete		

「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。

Storm Control											
+ Add	+ Add Port X Delete Selected Port										
	Port	Broadcast	Multicast	Unicast	Action						
	Ghn0/1	1%	1%	1%	Edit Delete						
	Ghn0/2		-	-	Edit Delete						

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 1-19 ポート保護設定

Ruij	JIE SWITCH	WEB Model: RG-H52310-160H20T1XS Detail
	Port Protect	Port Protect
Favorites		
(S) Network		Note: Protect ports can not communicate with each other. The selected ports on the panel are the protected ports Please click 'Display Protected Port' to refresh the panel.
\bigcirc		Select Port:
Security		Capacitados 💼 Unavailados 👚 Selected 🔐 AG Port
• 2 Advanced		1357911315 202022222222 2221 2222
کی) System		17 18 19 2 4 6 8 10 12 14 16 Note:Click and hold the left button as you drag the pointer across the section to select multiple ports. Ports 1-16 are G. In ports. All Innet: Deselect
		Save Display Protected Port

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 1-20 アクセスコントロールリスト

ACL List	ACL List ACL Time ACL Application								
ACL List:	ACL List Add ACL Delete ACL + Add Access Rule X Delete Selected Access Rule								
NO.	Source IP/Wildcard	Source Port	Access Control	Protocol	Destination IP/Wildcard	Destination port	Time Period	Status	Action
	No Record Found								
Show No.: 1	w No.: 10 v Total Count 0 [4 First 4 Pre Next > Last)] 1 GO								

■ 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。

\equiv Add ACL					×				
Α	ACL Type: Standar Control)	d ACL (Source-addre:	ss-based Control) 🔿 E	Extended ACL (Flow-ba	ised				
	ACL List. A Both Chinese and English are supported. If you want configure a number, please make sure that it is in the range of 1-99 or 1300-1999.								
				OK Cancel					
ACL List	ACL Time	ACL Application							
ACL List: 2	∽ Add	ACL Delete ACL	+ Add Access Rule	X Delete Selected A	Access Rule				
□ <mark>\</mark> 2	dcard	Source Port	Access Control	Protocol	Destination IP/Wildc ard	Destination port	Time Period	Status	Action

■ 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。

ACL List	ACL Time	ACL Application							
ACL List: 2	~	Add ACL Delete ACL	+ Add Access Rule	X Delete Selected A	Access Rule				
□ N ²	1_ildo	ard Source Port	Access Control	Protocol	Destination IP/Wildc ard	Destination port	Time Period	Status	Action

■ 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。

	×
ACL Type: Standard ACL (Source-address-based Control)	
ACL List: 2	
Access Rule Settings	
Access Control: Permit Deny Time Period Period Time manager	
Any IP: (For all IP)	
Single IP V IP:	
OK Canor	el

■ 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。

ACI	. List	ACL Time A	CL Application							
ACL L	ist: 2	✓ Add Ad	CL Delete ACL	+ Add Access Rule	X Delete Selected Access Rule					
	NO.	Source IP/Wildcard	Source Port	Access Control	Protocol	Destination IP/Wildc ard	Destination port	Time Period	Status	Action
	1	10.52.32.21/0.0.0.0		Permit				All Time	Effective	Edit Move
Sho	Show No.: 10 v Total Count 1 I First 4 Pre 1 Next 1 GO									

■ 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。

ACL List ACL Time ACL Application										
ACL I	ist: 2	✓ Add Ad	CL Delete ACL	+ Add Access Rule	X Delete Selected A	Access Rule				
	NO.	Source IP/Wildcard	Source Port	Access Control	Protocol	Destination IP/Wildc ard	Destination port	Time Period	Status	Action
	1	10.52.32.21/0.0.0.0		Permit				All Time	Effective	Edit Move
	2	10.52.32.20/0.0.0.0		Permit				All Time	Effective	Edit Move
Sho	Show No.: 10 ▼ Total Count2 II First 4 Pre 1 Next ▶ Last № 1 GO									

■ 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。

ACL L	ist: 2	► Add A	CL Delete ACL	+ Add Access Rule	× Delete Selected	I Access Rule				
0	NO.	Source IP/Wildcard	Source Port	Access Control	Protocol	Destination IP/Wildc ard	Destination port	Time Period	Status	Action
	1	10.52.32.21/0.0.0.0		Permit				All Time	Effective	Edit Move
	2	10.52.32.20/0.0.0.0		Permit				All Time	Effective	Edit Move
Show	v No.: [10 👻 Total Count:2		≡ Sele	ct Rule		×		€ Pre 1 Next 🕨 La	st≯I GO
l				Swap selec (Note: The ru	cted rule 1 with rule le's priority is in descen	2 Sing order from top to bottom)	Моче			

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 1-8 ACL 時間

ACL List	ACL Time	ACL Application							
Note: The A	CL active time must be	periodic.							
+ Add Time Object X Delete Selected Time Object									
	Ti	me Object	Day	Time Period	Action				
No Record Found									
Show No.:	10 🔻 Total Count	t.0			I∢ First ∢ Pre Next ▶ Last ▶ 1 GO				

■ 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。

Add Time Object		×
Object Name:	•	
Time Period	Please select V Start time C End time X +Add	
	Save Canc	el

■ 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。

≡ Edit Time Period			×
Object Name:	1 *		
Time Period	Monday V 0:00	~ 0:05	× +Add
		Sa	ve Cancel

■ 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。

+ Ade	Time Object X Delete Selected Time Object				
	Time Object	Day	Time Period	Action	
	1	Monday	0:00-0:05	Edit Delete	
Show	Show No.: 10 v Total Count:1 I v Total Count:1 I GO				

▲ ACL の適用

ACL 適用申請ページは次の図に示します。

図 1-22 ACL の適用

ACL List	ACL Time ACL Application					
+ Add Port X	Delete Port					
	ACL	Port	Direction	Action		
No Record Found						
Show No.: 10	▼ Total Count:0			I∢ First ∢ Pre Next ▶ Last ▶ 1 GO		

■ 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。

⊟ Add Port	>
ACL LIST 1	
Direction: Input	
Select Port:	
🖸 Available 💼 Unavailable 💼 Selected 🛱 AG Port	ibber
1 3 5 7 9 11 13 15 <u> <u> <u> </u> <u> </u></u></u>	
Note:Click and hold the left button as you drag the pointer across the section to select multiple ports. Ports 1-16 are G.hn ports. All Invent. Des	select
Save	Cancel

■ 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。

+ Add Po	ort 🗙 Delete Port			
	ACL	Port	Direction	Action
	1	Ghn0/1	in	Edit Delete
Show No	0.: 10 V Total Count:1			l∉ First ∢ Pre 1 Next ▶ Last № 1 GO

■ 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。

ACL List	ACL Time ACL Application			
+ Add Port	× Delete Port			
	ACL	Port	Direction	Action
	1	Ghn0/1	in	Edit Delete
	2	Ghn0/7	in	Edit Delete
Show No.: 1	10 V Total Count:2		1	First 4 Pre 1 Next ▶ Last ▶ 1 GO

「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。

+ Add	+ Add Port X Delete Port					
	ACL	Port	Direction	Action		
	1	Ghn0/1	in	Edit Delete		
	2	Ghn0/7	in	Edit Delete		
Shov	v No.: 10 V Total Count:2			I4 First 4 Pre 1 Next ▶ Last ▶ 1 GO		

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 1-23 クラス設定

Class Settings	Policy Settings Flow Settings						
Note: Classification is	Note: Classification is used to identify and mark certain data flows that match the ACL rule.						
+ Add Class X De	+ Add Class X Delete Selected Class						
	Class Name	ACL	Action				
No Record Found							
Show No.: 10	V Total Count.0		I∉ First ∉ Pre Next ▶ Last ▶ 1 GO				

■ 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。

⊟ Add Class		×
Class Name:		* (1-31) Bytes
ACL List: 1		 [ACL List]
	Save	Cancel

■ 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。

Class Settings	Iss Settings Policy Settings Flow Settings					
Note: Classification	Note: Classification is used to identify and mark certain data flows that match the ACL rule.					
+ Add Class 🗙 🛛	Delete Selected Class					
	Class Name ACL Action					
	1		1	Edit Delete		
	3		1	Edit Delete		
Show No.: 10 -	Total Count:2			li First ∢ Pre 1 Next ▶ Last ▶ 1 GO		
	Class N	ame	ACL	Action		
0	1		1	Edit Delete		
	3		1	Edit Delete		
Show No.: 10 🗸	Total Count:2			I First		

■ 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。

Note: Classification is used to identify and mark certain data flows that match the ACL rule.					
+ Add Class ×	Delete Selected Class				
	Class Name	Edit Class	×	Action	
	1			Edit Delete	
	3	Class Name: 1	* (1-31) Bytes	Edit Delete	
Show No.: 10	V Total Count:2	ACL List: 1	Y [ACL List]	I∢ First ∢ Pre 1 Next ▶ Last ▶ 1 GO	
			Save Cancel		

▶ ポリシー設定

次の図は QoS ポリシーの設定ページです。

図 1-24 ポリシーの設定

Class Settings	Class Settings Policy Settings Flow Settings							
Note: The policy is	used to constrain the bandwidth that the	classified data flow consumes.						
Policy List:	Policy List: Add Policy Delete Policy + Add Policy Rule X Delete Selected Rule							
	Class Name	Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action			
No Record Found								
Show No.: 10	Show No.: 10 ~ Total Count 0 II First 4 Pre Next 1 Last 1 1 GO							

■ 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。

Add Policy	>	<
Policy Name:	* (1-31) Bytes	6
	Save Cancel	

■ 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。

Class Settings	Policy Settings	Flow Settings			
Note: The policy is use	d to constrain the bandwidth	hat the classified data flow consumes.			
Policy List: 1	Add Policy	Delete Policy + Add Polic	cy Rule X Delete Selected Rule		
	Class Name	Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action
			No Record Found		

■ 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。

⊟ Add Policy Rule	×
Policy Name: 1	* (1-31) Bytes
Bandwidth:	* (16-10000000) KBps
Burst Traffic:	* (1-8192)KByles
Limit Violation Disposal: Drop O DSCP Priority: 	* (0-63)
Class List: 1	~
	Save Cancel

■ 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。

Clas	s Settings Policy Settings	Flow Settings			
Note	: The policy is used to constrain the bandwidth	that the classified data flow consumes.			
Policy	List: 1 Y Add Policy	Delete Policy + Add Policy Rule	X Delete Selected Rule		
	Class Name	Bandwidth (KBps)	Burst Traffic (KBytes)	Bandwidth Violation Disposal	Action
	1	20	56	Drop	Edit Delete
Shov	v No.: 10 V Total Count:1			I€ First €	Pre 1 Next 🕨 Last 🕅 1 GO

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 1-25 フローポリシー設定

Class Settings	Policy Settings	Flow Settings				
Note: The policy is us	ed to constrain input and o	output flows (Input and out)	put flows of one port must be in the same trust mode	e but they can be configured with different policies)		
+ Add Port X Dele	ete Selected Port					
	Port		Direction	Policy Name	Trust Mode	Action
				No Record Found		
Show No.: 10	 Total Count:0 					I4 First 4 Pre Next ▶ Last № 1 GO

■ 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。

∃ Add Port	×
Rate-limiting Direction: Input v	
Trust Mode: Untrusted	
Policy List: 1	
Select Port:	
🖓 Available 💼 Unavailable 💼 Selected 🛱 AG Port	
1 3 5 7 9 11 13 15 <u> </u>	
Note:Click and hold the left button as you drag the pointer across the section to select multiple ports. Ports 1-16 are G in ports. All Inset. Deselect	
Save Cano	el:

■ 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。

Clas	s Settings	Policy Settings	Flow Settings					
Note	Note: The policy is used to constrain input and output flows (Input and output flows of one port must be in the same trust mode but they can be configured with different policies)							
+ Add	I Port 🗙 De	lete Selected Port						
		Port		Direction	Policy Name	Trust Mode	Action	
	C Gh0/1 Input 1 Untrusted Delete							
Show	→ Total Count 1 I GO							

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 1-26 システム時間

Ruț	JIE SWITCH	WEB Model: RG-H	HS2310-16GH2GT1X	5 Detail			
	Settings	System Time	Password	Reset	Web Access Control	SNMP	
-	Upgrade						
(Ø) Network	System Logging	Currer	nt Time: 1970-1-	1-10:06:32			
	Detection	Rese	et Time: 2023-9-27	16:47			
Security	Web Cli	Time	e Zone: UTC+8(C	CT)	*		
2 Advanced		Time Synchron	ization: 📄 Automa	tically synchro	nize with an Internet time se	rver(Please se	t <u>DNS Server</u> first, otherwise the system time will not be synchronized.)
් (ිූි System			Save				

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。

凶 パスワード

次の図は「パスワード」ページです。

図 1-27 パスワード

Rui	JIE SWITCH	WEB Model: RG-H	IS2310-16GH2GT1X	s Detail			
C Favorites	Settings	System Time	Password	Reset	Web Access Control	SNMP	
Ø	Upgrade	⊒ Web Managen	nent Password				
Network	System Logging	Use	rname: admin				
(!) Security	Detection	Old Pa	ssword		*		
, La	WED CII	New Pas	sword.		*		
Advanced		Confirm Day	www.ord:				
් (ි) System		Coniim Pas	sword.		^		
Cycloni			Save				

■ 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	-28 リセ	ット					
Ruj	JIE SWITCH	WEB Model: RG-	HS2310-16GH2GT1X	(S Detail			
Favorites	Settings	System Time	Password	Reset	Web Access Control	SNMP	
Ø	Upgrade System Logging	⊟ Restore Factore	ory Settings				
Network	Detection	Note: After the d	evice is reset to the	factory default se	ettings, all configurations will be	e removed. Plea	se Export Current Configuration before resetting the device.
Security	Web Cli	Restore Fa	ctory Settings				
2 Advanced		Display Current	Configuration				
୍ଦି System							
oyacın							
		≘ Import/Expor	t Configuration				
		Note: Please dor	n't close or update th	ne page during in	nport, or import will fail. If you v	vant to apply the	new configuration, please restart the device on this page, or the configuration will not take effect.
		File	e Name:		File Imp	ort Export	Current Configuration

■ 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 1-29 Web 管理

Ru	JIE SWITCH	WEB Model: RG-H	S2310-16GH2GT1XS	B Detail			
Eavorites	Settings	System Time	Password	Reset	Web Access Control	SNMP	
R avonics	Upgrade	= Basic Informat	ion				
Network	System Logging						
	Detection	Web Acces	s Port: 443	* (Range:4	43,1025-65535)		
Security	Web Cli	Login Tir	meout: 10 min		v		
2® Advanced		Device Lo	cation:	_			
• {्रे System			Save				

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 1-30 簡単なネットワーク管理プロトコル

RUÏ	JIE SWITCH	WEB Model: RG-HS	32310-16GH2GT1X8	B Detail			
Eavorites	Settings	System Time	Password	Reset	Web Access Control	SNMP	
ravonies Ra	Upgrade	Note: Either SNMPv	2 or SNMPv3 is sup	ported			
Network	System Logging						
1	Detection	SNMP Ve	ersion: v2 vv	/3			
G	Web Cli	Device Loo	ation:				
∠ි⊚ Advanced		SNMP Comm	nunity:		*		
• (3)		Trap Comm	nunity:		The Trap Community	must be the same a	as the SNMP Community.
System		Trap Recipient Ad	dress:		* You can configure up	o to 9 Trap recipient	ts. Please use ',' or press the Enter key to separate addresses.
					17		
			Save				

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。

义.	1-31 アッ	· プグレードローカル
Ruț	JIE SWITCH	WEB Model: RG-HS2310-16GH2GT1XS Detail QWizard
$\hat{\Box}$	Settings	Upgrade Local
R	Upgrade	Note: Piesse download the corresponding software version from the official website, and then upgrade the device with the following tops.
Network	System Logging	Tips: 1. Make sure that the software version (main program or Web package) matches the device model 2. The page may have no response during upgrade. Please do not power off or restart the device until an upgrade succeeded message is displayed.
1		File Name Eta Liverada Chaval
Security		THE Upged United
Advanced		
ै(्) System		

「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 1-32 ログサーバ設定

Ruíjie SWITCH		WEB Model: RG-HS2310-16GH2GT1XS Detail						
C Favorites	Settings	Log Server Settings Display System Log						
Ø	Upgrade	Note: Logging is rated on 8 different levels: 0-Emergency, 1-Alert, 2-Critical, 3-Error, 4-Warning, 5-Notification, 6-Informational, 7-Debugging. The smaller the number, the higher the level.						
Network	System Logging	Server Logging: ON						
U. Security	Web Cli	Server IP:						
2 Advanced		Logging Level: Informational(6) •						
් (ිූි System		Save						

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 1-33 システムログの表示

Ruj	JE SWITCH	WEB Model: RG-H\$2310-18GH2GT1XS Detail							
C Favorites	Settings	Log Server Settings Display System Log							
R	Upgrade								
Network	System Logging	System Log (Snow the last 200 logs) Update Log							
	Detection	Syslog logging: enabled							
Security	Web Cli	Console logging: level debugging, 29 messages logged							
0_		Monitor logging: level debugging, O messages logged							
 ∠® Advanced 		Buffer logging: level debugging, 29 messages logged							
		Standard format:false							
ŝ		Timestamp debug messages: datetime							
System		Timestamp log messages: datetime							
		Sequence-mumber log messages: disable							
		Symme log messages: disable							
		Count log messages: disable							
		Trap logging: level informational, 29 message lines logged, 0 fail							
		Log Buffer (Total 131072 Bytes): have written 2636,							
		*Jan 1 09:05:20: %SYS-5-COMFIG_I: Configured from console by console							
		*Jan 1 08:54:31: %DHCP_CLIENT-6-ADDRESS_ASSIGN: Interface VLAN 1 assigned DHCP address 10.52.25.77, mask 255.255.248.0.							
		*Jan 1 08:54:26: %SYS-5-CONFIG_I: Configured from console by console							
		*Jan 1 08:20:47: %SYSLOG-6-DEBUG_FRINT: The debug print time 20 minutes has expired!							
		*Jan 1 08:03:02: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ghn 0/5, changed state to up.							
		*Jan 1 08:03:02: %LINK-3-UFDOWN: Interface Ghm 0/5, changed state to up.							
		*Jan 1 08:03:02: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ghn 0/2, changed state to up.							
		*Jan 1 08:03:02: %LINK-3-UFDOWN: Interface Ghm 0/2, changed state to up.							

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。

Y 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 1-34 Ping

Ping Trace	rt Cable Detection	on Collection
Destination IP or Do	main	•
na	ame:	
Timeout Period (1-	10): 2	
Repetition Count (1-	100): 5	
	Detect	

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。

🗵 1-35 Tracert

Ruíjie switch		WEB Model: RG-HS2310-16GH2GT1XS Detail	🕞 Wizard	Online Service	- More	☐ Logout
C	Settings	Ping Tracert Collection				
ravonies	Upgrade					
Ø Network	System Logging	Destination IP or Domain* name:				
(\mathbf{I})	Detection	Timeout Period (1-10) : 2				
Security	Web Cli					
2 Advanced		Detect				
^ৰ (্ৰ্ট) System						

▶ 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 1-36 ワンクリックコレクション

Ruíjie SMTCH		WEB Model: RG-HS2310-16GH2GT1XS Detail						
Eavorites	Settings	Ping	Tracert	Collection				
6	Upgrade	Note: O	ne-Click Collection	is used to collect fault information for travblachontion				
® Network	System Logging	Note: 0						
(!)	Detection			One-Click Collection				
Security	Web Cli							
2 Advanced								
• 💮 System								

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 1-37 ネットワークコマンドラインインターフェース

Ruj	JIE SWITCH	WEB Model: R	3-H623I0-86H2GT1XS Detail	C Wizard	Online Service	⊖ More	🕞 Logk		
$\hat{\Box}$	Settings	Web Cli	Web Cli						
Favorites	Upgrade								
(D) Network	System Logging	Console Output:	Console Output:						
~	Detection	led"blink	Ding for searching a device						
Security	Web Cli	acu-upgrade	Ncu upgrade						
0		akdir	Nake directories						
2 ©S Atlancet		nore	Display contents of a file						
		no	Negate a command or set its defaults				- 10		
* @>		ping	Send ocho mossages						
System		pvd	Fint has of current working directory						
		reload	Keload device						
		rename	Nove or remake files						
		renew	Renew						
		rldp	Ridp exec operation				*		
		rndir	Remove a directory				11		
		Command Input:	Stitz-signal Sterd Clear Screen Sterd Clear Screen C						