

H3C MSR

Open Multiservice Routerシリーズ

Comware 7 Web設定ガイド

Copyright(C)2023, New H3C Technologies Co.,Ltd. およびそのライセンサーAll rights reserved

本書のいかなる部分も、New H3C Technologies Co.,Ltd.の事前の書面による同意なしに、いかなる形式または手段によっても複製または送信することはできません。

商標

New H3C Technologies Co.,Ltd.の商標を除き、本書に記載されているすべての商標は、それぞれの所有者の所有物です。

お知らせ

本書に記載されている情報は、予告なしに変更されることがあります。本書の記述、情報、推奨事項を含むすべての内容は正確であると考えられますが、明示的または黙示的を問わず、いかなる種類の保証もなく提示されています。H3Cは、本書に含まれる技術的または編集上の誤りや脱落に対して責任を負いません。

はじめに

『Webコンフィギュレーションガイド』には、Webサーバーからデバイスをローカルに管理する方法の詳細が記載されています。

ここでは、マニュアルに関する次の内容について説明します。

- 対象読者
- 表記規則
- ドキュメントのフィードバック

対象読者

このマニュアルは、次の読者を対象としています。

- ネットワークプランナー。
- フィールドテクニカルサポートおよびサービスエンジニア。
- ネットワーク管理者。

表記規則

次の情報では、マニュアルで使用されている表記規則について説明します。

ここでは、マニュアルで使用されている表記法について説明します。

コマンドの表記法





規約	説明
太字	太字のテキストは、文字どおりに入力したコマンドとキーワードを示します。
イタリック体	斜体のテキストは、実際の値に置き換える引数を表します。
[]	角カッコは、オプションの構文選択(キーワードまたは引数)を囲みます。
{ x y ... }	中カッコは、必要な構文の選択肢を縦棒で区切って囲みます。この中から 1 つを選択します。
[x y ...]	角カッコは、オプションの構文選択のセットを縦棒で区切って囲みます。この中から 1 つまたは何も選択しません。
{ x y ... }*	アスタリスクの付いた中括弧は、必須構文の選択肢を縦棒で区切って囲みます。この中から少なくとも 1 つを選択します。
[x y ...]*	アスタリスクの付いた角括弧は、オプションの構文選択肢を縦棒で区切って囲みます。選択肢は 1 つ、複数、または何も選択しません。
&<1-n>	アンパサンド(&)記号の前の引数またはキーワードと引数の組み合わせは、1~n 回入力できます。
#	シャープ記号(#)で始まる行はコメントです。

GUIのルール













規約	説明
太字	ウィンドウ名、ボタン名、フィールド名およびメニューアイテムは太字で表示されます。たとえば、New User ウィンドウが開き、OK をクリックします。

規約	説明
>	マルチレベルメニューは、File > Create > Folder のように、山かっこで区切られています。

シンボル

規約	説明
 警告!	重要な情報を理解していない場合や、その情報に従っていない場合に、けがをするおそれがある場合に注意を促す警告。
 注意:	重要な情報が理解されていない場合、または情報が理解されていない場合に、データの損失、データの破損、またはハードウェアやソフトウェアの損傷につながる可能性がある場合に、注意を促す警告。
 重要:	重要な情報への注意を喚起するアラート。
注:	追加情報または補足情報を含むアラート。
 ヒント:	役立つ情報を提供するアラート。

ネットワークポロジアイコン

規約	説明
	ルーター、スイッチ、ファイアウォールなどの汎用ネットワーク装置を表します。
	ルーターまたはレイヤー3スイッチなどのルーティング対応装置を表します。
	レイヤー2スイッチやレイヤー3スイッチなどの汎用スイッチ、またはレイヤー2 および他のレイヤー2 機能をサポートするルーターを表します。
	アクセスコントローラー、Unified Wired-WLAN モジュール、または Unified Wired-WLAN スイッチ上のアクセスコントローラエンジンを表します。
	アクセスポイントを表します。
	ワイヤレスターミネータユニットを表します。
	ワイヤレスターミネータを表します。
	メッシュアクセスポイントを表します。
	全方向信号を表します。
	指向性信号を表します。
	ファイアウォール、UTM、マルチサービスセキュリティゲートウェイ、ロードバランシング装置などのセキュリティ製品を表します。
	ファイアウォール、ロードバランシング、NetStream、SSL VPN、IPS、または ACG モジュールなどのセキュリティモジュールを表します。

本書に記載されている例

このドキュメントの例では、ハードウェアモデル、設定、またはソフトウェアバージョンがデバイスと異なるデバイスを使用する場合があります。例に記載されているポート番号、サンプル出力、スクリーンショット、およびその他の情報が、デバイス上にあるものと異なるのは正常です。

ドキュメントに関するフィードバック

製品ドキュメントに関するご意見は、info@h3c.comまで電子メールでお寄せください。

ご意見をお寄せいただければ幸いです。

内容

製品	1
システム情報	2
システム情報の概要	2
システム情報を表示する	2
ウィザードを使用する	6
技術サポートを受ける	8
高速構成	9
高速設定の概要	9
WAN設定の構成	9
LAN設定の構成	13
ネットワーク	14
WAN設定	14
LANの設定	22
ポート管理	30
NAT設定	31
ネットワーク動作の管理	36
ユーザーグループ	36
時間範囲グループ	38
帯域幅管理	42
ネットワーク動作の管理	47
シングルチャデータベース	51
監査ログ	53
トラフィックランキング	54
ネットワークセキュリティ	56
ファイアウォール	56
攻撃防御	58
接続制限	62
MACアドレスモニター	65
ARP攻撃からの保護	67
認証管理	71
ポータル認証	71
PPPoEサーバー	76
ユーザー管理	78

仮想ネットワーク	81
IPsec VPN.....	81
L2TPサーバー	90
L2TPクライアント.....	96
EoGRE.....	101
応用設定	105
アプリケーションサービス.....	105
スタティックルーティング.....	108
ポリシーベースルーティング	110
SNMP.....	112
CWMP.....	115
システムツール	116
基本設定.....	116
診断.....	119
管理者アカウント管理	123
リモート管理.....	127
構成管理.....	132
ソフトウェアのアップグレード	134
ライセンス管理	138
再起動	141
システムログ	142
SmartMC.....	144
構成ウィザード	144
インテリジェントな管理	146
インテリジェントO&M.....	149
可視性	154

製品

H3C MSRオープンマルチサービスルーターシリーズには、次のものが含まれます。

- H3C MSR610ルーター
- H3C MSR 810ルーター
- H3C MSR 830ルーター
- H3C MSR 1000ルーター
- H3C MSR 2600ルーター
- H3C MSR 3600ルーター
- H3C MSR 5600ルーター

注:

製品モデルのシャーシビューと設置方法については、その製品モデルのインストレーションガイドまたはハードウェア情報と仕様を参照してください。

Webページは製品シリーズによって異なります。このドキュメントのWebページは、説明のみを目的としています。

このドキュメントの機能は、MSR810ルーターのリリース6728P26で設定および検証されています。

システム情報

システム情報の概要

システム情報を使用すると、デバイスの動作情報の取得、ウィザードを使用した基本設定の構成、および技術サポートの取得が可能になります。

システム情報を表示する CPU使用率とメモリ使用率

ネットワーク構成

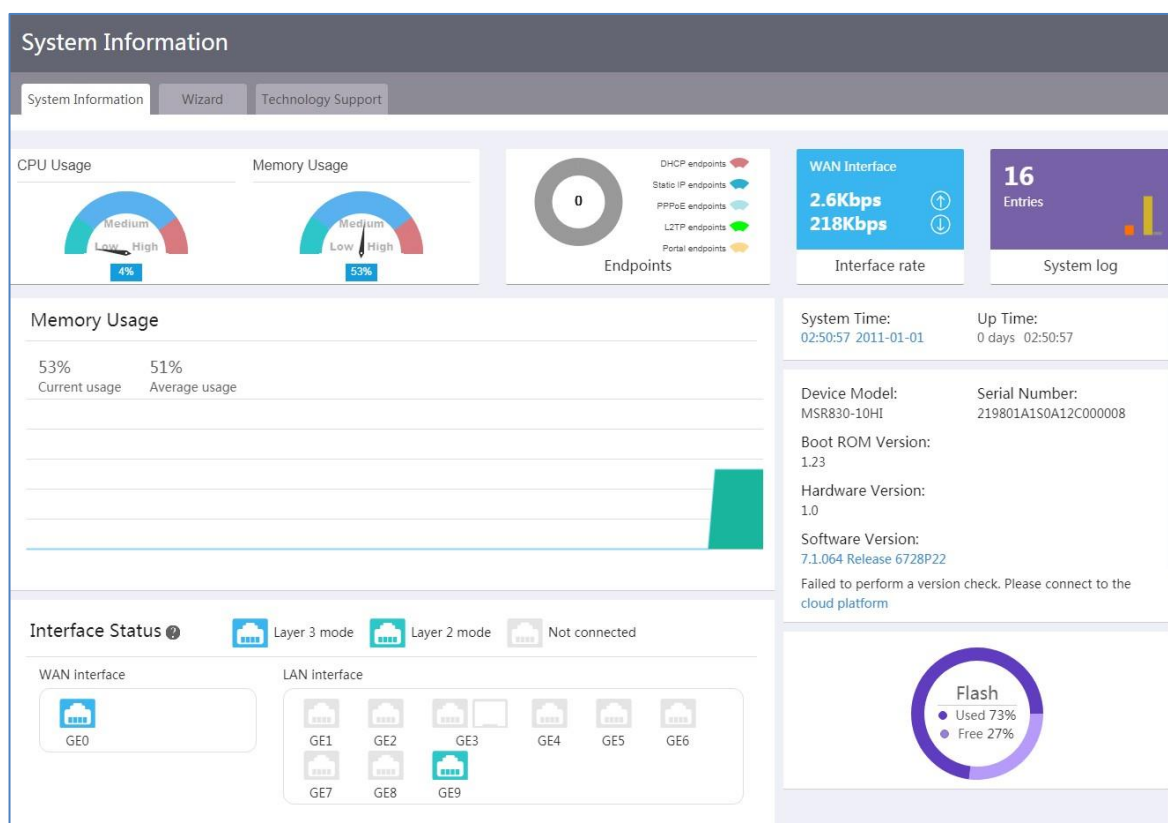
次のようなCPU使用率およびメモリ使用率に関する情報を表示するには、次の作業を実行します。

- 現在および平均のCPU使用率。
- 現在および平均のメモリ使用量。

手順

1. ナビゲーションペインで、**System Information**を選択します。
2. 現在および平均のCPU使用率、または現在および平均のメモリ使用率を表示するには、それぞれ**CPU Usage**領域または**Memory Usage**領域をクリックします。

図1 CPU使用率とメモリ使用率の表示



エンドポイント

ネットワーク構成

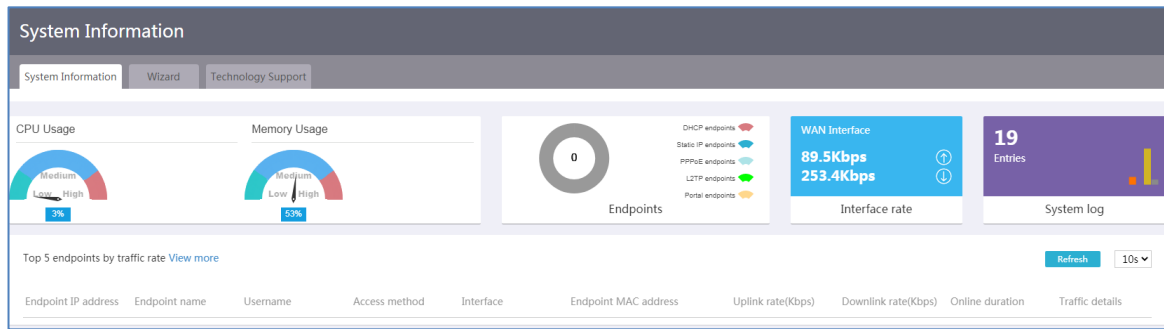
デバイスにアクセスするエンドポイントに関する次のような情報を表示するには、次の作業を実行します。

- トラフィックレート別の上位5つのエンドポイント。
- オンラインエンドポイントの数。
- エンドポイントIPアドレス、エンドポイント名、ユーザー名、アクセス方式、サーバー、およびエンドポイントMACアドレスを含むエンドポイントリスト。

手順

1. ナビゲーションペインで、**System Information**を選択します。
2. **Endpoints**領域をクリックします。トラフィックレート別の上位5つのエンドポイントをリアルタイムで表示できます。
3. ユーザートラフィックランキングを表示するには、**View more**をクリックします。

図2 トラフィックレートによる上位5つのエンドポイントの表示



モニターレート

ネットワーク構成

アップリンクトラフィック、アップリンクレート、ダウンリンクトラフィック、ダウンリンクレート、WANサーバーステータス、およびネットワークアクセスパラメータを含む、サーバーレート情報を表示するには、次の作業を実行します。また、サーバーの再接続、サーバーの切断、またはサーバー情報のリフレッシュもできます。

手順

1. ナビゲーションペインで、**System Information**を選択します。
2. **Interface rate**領域をクリックします。
3. サーバーに再接続するには、**reconnect**をクリックします。
4. サーバーを切断するには、**release**をクリックします。

システムログ

ネットワーク構成

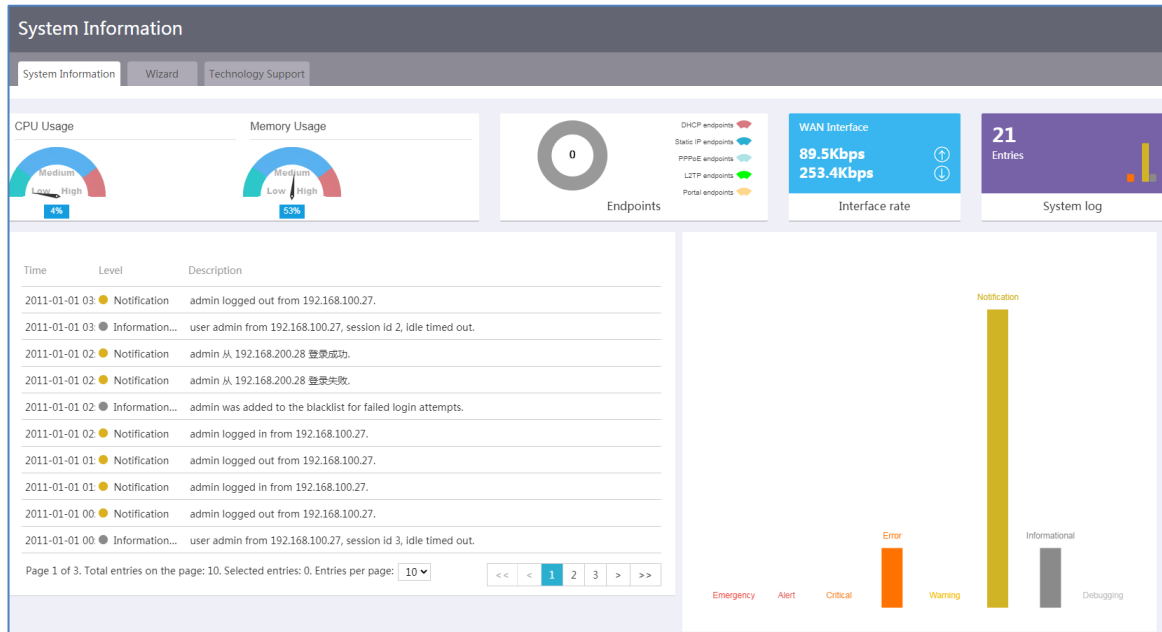
次のようなデバイスのシステムログ情報を表示するには、次の作業を実行します。

- デバイスのログ情報。
- 統計情報をログに記録します。

手順

1. ナビゲーションペインで、**System Information**を選択します。
2. **System log**領域をクリックします。

図3 システムログの表示



デバイス情報

ネットワーク構成

システム時間やデバイスモデルなどのデバイス情報を表示するには、次の作業を実行します。

手順

1. ナビゲーションペインで、**System Information**を選択します。
2. **System Time**領域には、デバイスのシステム時間と稼働時間が表示されます。**Device Model**領域には、デバイスモデル、シリアル番号、ブートRoMバージョン、ハードウェアバージョン、およびソフトウェアバージョンが表示されます。

モニターのステータス

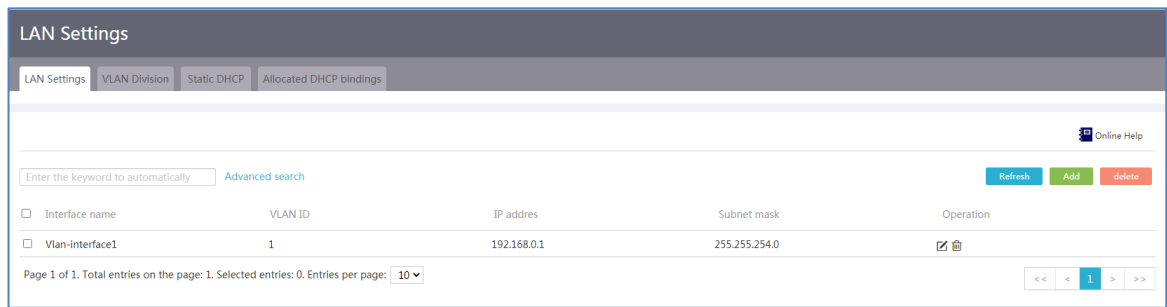
ネットワーク構成

WANサーバーステータスおよびLANサーバーステータスを表示するには、次の作業を実行します。

手順

1. ナビゲーションペインで、**System Information**を選択します。
2. WANサーバまたはLANサーバに関する情報を表示するには**Interface Status**領域で、WAN設定ページまたはLAN設定ページに移動します

図4 LAN Settingsページ



ストレージメディア

ネットワーク構成

ストレージメディアのストレージスペースの使用状況を表示するには、次の作業を実行します。

手順

1. ナビゲーションペインで、**System Information**を選択します。
2. ページの右下隅に、ストレージメディアのストレージスペース使用量が表示されます。

ウィザードを使用する

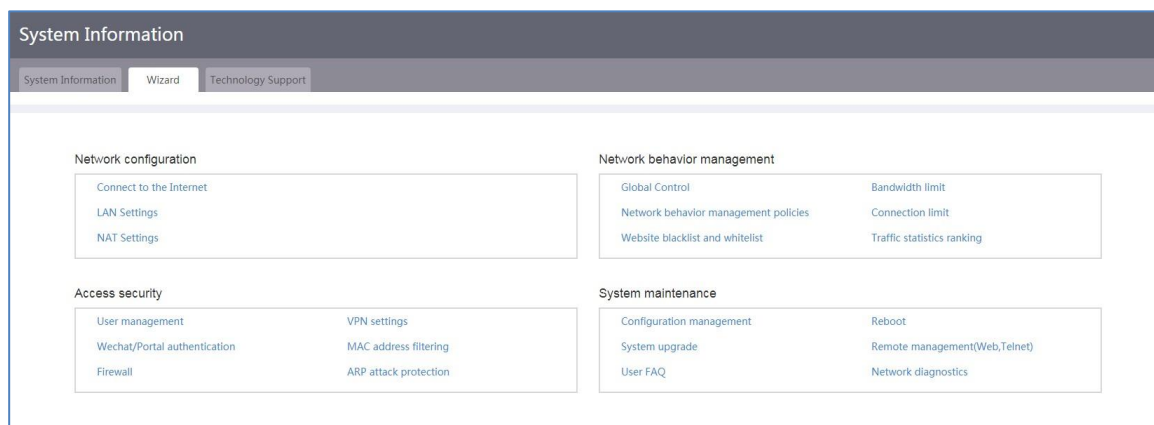
ウィザードからネットワーク設定をすばやく構成するには、次の手順に従います。

1. ナビゲーションペインで、**System Information**を選択します。
2. **Wizard**タブをクリックします。
3. リンクをクリックして、必要に応じて次の設定を構成します。
 - ネットワーク構成:
 - **Connect to the Internet: Connect to the Internet**リンクをクリックして、**WAN Settings**ページに移動します。
 - **LAN Settings: LAN Settings**リンクをクリックして、**LAN Settings**ページに移動します。
 - **NAT Settings: NAT Settings**リンクをクリックして、**NAT Settings**ページに移動します。
 - ネットワーク動作の管理:
 - **Global Control: Global Control**リンクをクリックして、**Network Behaviors > Global Control**ページに移動します。
 - **Bandwidth limit**リンクをクリックして、**Bandwidth Management > Bandwidth limits**ページに移動します。
 - **Network behavior management policies: Network behavior management policies**リンクをクリックして、**Network Behaviors > Network behavior management policy**ページに移動します。
 - **Connection limit: Connection limit**リンクをクリックして、**Connection Limits**に移動しま

す

- **Website blacklist and whitelist:** **Website blacklist and whitelist**リンクをクリックして、**Network Behaviors > Web blacklist and whitelist**ページに移動します。
- **Traffic statistics ranking:** **Traffic statistics ranking**リンクをクリックして、**Traffic Ranking > Global control**ページに移動します。
- **アクセスのセキュリティ:**
 - **User management:** **User management**リンクをクリックして、**User Management > User Settings**ページに移動します。
 - **VPN settings:** **VPN settings**リンクをクリックして、**IPsec VPN > IPsec policy**に移動します。
 - **Wechat/Portal authentication:** **Wechat/Portal authentication**リンクをクリックして、**Portal Authentication > Authentication Settings**ページに移動します。
 - **MAC address filtering:** **MAC address filtering**リンクをクリックして、**MAC Address Filter > MAC Filter Setting**ページに移動します。
 - **Firewall:** **Firewall**リンクをクリックして、**Firewall**ページに移動します。
 - **ARP attack protection:** **ARP attack protection**リンクをクリックすると、ダイナミックARPラーニング設定ページが表示されます。
- **システムメンテナンス:**
 - **Configuration management:** **Configuration management**リンクをクリックして**View Config**ページに移動します。
 - **Reboot:** **Reboot**リンクをクリックして、**Reboot now**ページに移動します。
 - **System upgrade:** **Upgrade**ページに移動するには、**System upgrade**リンクをクリックします。
 - **Remote management(Web,Telnet):** **Remote management(Web,Telnet)**リンクをクリックして、**Remote Login > Ping**ページに移動します。
 - **User FAQ:** **User FAQ**リンクをクリックして、**User FAQ**ページに移動します。
 - **Network diagnostics:** **Network diagnostics**リンクをクリックして、**Diagnostics > tracert**ページに移動します。

図5 ウィザードの使用

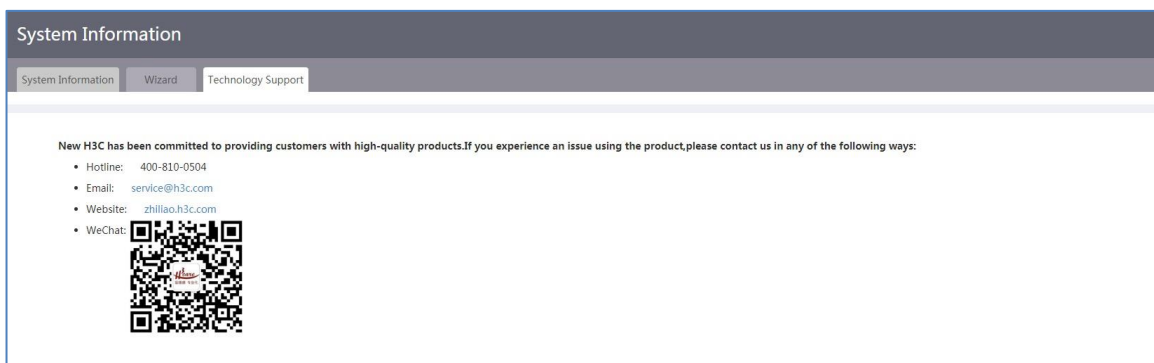


技術サポートを受ける

製品の使用中に問題が発生した場合は、図6に示すように、次のいずれかの方法で技術サポートを受けることができます。

- ホットライン: 400-810-0504。
- 電子メール: service@h3c.com
- ウェブサイト: zhiliao.h3c.com。
- WeChat公式アカウント。

図6 テクノロジーサポート



高速構成

高速設定の概要

高速設定により、基本的なWAN設定とLAN設定をすばやく完了できます。その後、LAN内のユーザーはWANにアクセスできます。

WAN設定の構成

ネットワーク構成

デバイスは、次のWANアクセスシナリオをサポートしています。

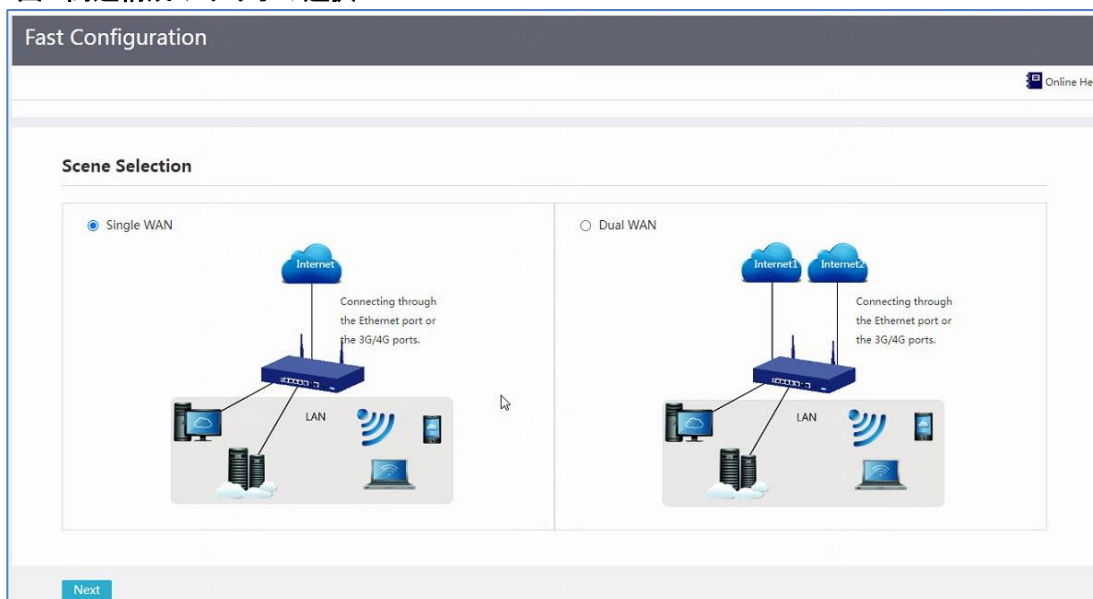
- **Single-WAN:** ユーザーが1つのオペレータネットワークだけをリリースする場合は、シングルWANシナリオを選択します。
- **Dual-WAN:** ユーザーが2つのオペレータネットワークをリリースする場合は、デュアルWANシナリオを選択します。構成手順は両方のシナリオで同じです。

デバイスは、物理サーバーまたはモバイル通信(3G/4G)モデムを介してWANに接続できます。

物理サーバーを介してWANに接続する

1. ナビゲーションペインで、**Fast Configuration**を選択します。
2. 必要に応じてシングルWANとデュアルWANのシナリオを選択し、WANアクセスパラメータを設定します。

図7 高速構成:シナリオの選択



3. **Line 1**または**Line 2**リストから、WANにアクセスするための物理サーバーWANxを選択します。

4. 必要に応じて、**Link mode**リストからリンクモードを選択します。
 - PPPoEリンクモードを選択する場合は、次の作業を実行します。
 - **Username**フィールドに、オペレータから提供されたPPPoEアクセスユーザー名を入力します。
 - **Password**フィールドに、オペレータから提供されたPPPoEアクセスパスワードを入力します。
 - DHCPリンクモードを選択すると、DHCPサーバーは、WANにアクセスするためのパブリックIPアドレスを自動的に割り当てます。
 - 固定IPリンクモードを選択する場合は、次の作業を実行します。
 - **IP address**フィールドに、WANにアクセスするための固定IPアドレスを入力します。
 - **IP mask**フィールドに、IPアドレスのマスクまたはマスク長を入力します
(例:255.255.255.0または24)。
 - **Gateway address**フィールドに、WANにアクセスするためのゲートウェイアドレスを入力します。
 - **DNS1**および**DNS2**フィールドに、WANにアクセスするためのDNSサーバーのIPアドレスを入力します。デバイスは、ドメイン名の変換にDNSサーバーDNS1を優先的に使用します。DNSサーバーDNS1がドメイン名の変換に失敗した場合、DNSサーバーDNS2が使用されます。
5. **NAT**フィールドで、**NAT**をイネーブルにするかどうかを選択します。
LAN内の複数のデバイスが1つのパブリックIPを共有する場合は、NATをイネーブルにします。
6. **Next**をクリックして、WANの設定を完了します。

図8 高速設定:単一WAN設定

The screenshot shows the 'Fast Configuration' interface for 'Single WAN config'. The fields are as follows:

- line1**: WAN0(GEO)
- Link mode**: PPPoE
- User name**: (1-80chars)
- Password**: (1-255chars)
- NAT**: Enabled

A tip on the right states: "Tips: By default, the load sharing mode is user-based average load sharing based on equal-cost routes. To modify and configure link load sharing, go to the Network > WAN Settings > Modify multi-WAN policy page."

Navigation buttons 'Previous' and 'Next' are located at the bottom.

図9 高速設定:デュアルWAN設定

Fast Configuration

Online Help

Dual WAN config

line1 *	WAN0(GE0)	line2 *	WAN1(GE1)
Link mode *	PPPoE	Link mode *	DHCP
User name	(1-80chars)	NAT	<input checked="" type="checkbox"/> Enabled
Password	(1-255chars)	<small>Tips: By default, the load sharing mode is user-based average load sharing based on equal-cost routes. To modify and configure link load sharing, go to the Network > WAN Settings > Modify multi-WAN policy page.</small>	
NAT	<input checked="" type="checkbox"/> Enabled		

Previous Next

モバイル通信(3G/4G)モデムを介してWAN1に接続する

1. ナビゲーションペインで、**Fast Configuration**を選択します。
2. 必要に応じてシングルWANとデュアルWANのシナリオを選択し、WANアクセスパラメータを設定します。
3. **Line 1**または**Line 2**リストから、モバイル通信モデムに対応する**Cellular interface**を選択します。
 - モバイル通信モデムがUSBモニターに挿入されている場合は、**USB SIM0(Cellular0/m)**モニターを選択します。
 - モバイル通信モデムがSICモジュールまたはデバイスに組み込まれたモデムである場合は、SIMカードが挿入されているモニター**SIMx(Cellularn/m)**を選択します。
4. **Operator**フィールドで、必要に応じて演算子を選択します。

オプションは、**CMCC**、**Unicom**、**Telecom**および**Custom**です。

- **CMCC**、**Unicom**、または**Telecom**を選択した場合は、次のタスクを実行します。
 - **Username**フィールドに、オペレータから提供されたユーザー名を入力します。
 - **Password**フィールドに、オペレータから提供されたパスワードを入力します。
 - **Auth method**フィールドで、ユーザー認証方式を選択します。

オプションには、**PAP or CHAP**、**PAP**および**CHAP**があります。**CHAP**は**PAP**よりもセキュアです。ネットワークがセキュアでない場合は、**CHAP**を選択します。デバイスおよびユーザーのエンドポイントが認証方式を自動的にネゴシエートするには、**PAP or CHAP**を選択します。認証方式を有効にするには、ユーザー名とパスワードを指定する必要があります。

- **Custom**を選択した場合は、次のタスクを実行します。
 - **APN**フィールドに、オペレータから提供されたAPNを入力します。
 - **Dialer number**フィールドに、オペレータから提供されたダイヤラ番号を入力します。

- **Username**フィールドに、オペレータから提供されたユーザー名を入力します。
- **Password**フィールドに、オペレータから提供されたパスワードを入力します。
- **Auth method**フィールドで、ユーザー認証方式を選択します。

オプションには、**PAP or CHAP**、**PAP**および**CHAP**があります。CHAPはPAPよりもセキュアです。ネットワークがセキュアでない場合は、CHAPを選択します。デバイスおよびユーザーのエンドポイントが認証方式を自動的にネゴシエートするには、**PAP or CHAP**を選択します。認証方式を有効にするには、ユーザー名とパスワードを指定する必要があります。

国外のオペレータまたはIoTオペレータのSIMカードを使用するには**Operator**リストから**Custom**を選択します。

5. **Network type**リストから、オペレータのネットワーク規格を選択します。
6. **NAT**フィールドで、NATをイネーブルにするかどうかを選択します。

LAN内の複数のデバイスが1つのパブリックIPを共有する場合は、NATをイネーブルにします。

7. **Next**をクリックして、WANの設定を完了します。

図10 高速設定:単一WAN設定

The screenshot shows the 'Fast Configuration' web interface. The main section is titled 'Single WAN config'. It contains the following fields and options:

- line1 ***: A dropdown menu showing 'USB SIM0(Cellular0/0)'.
- Operator ***: Radio buttons for 'CMCC' (selected), 'Unicom', 'Telecom', and 'Custom'.
- Username**: A text input field with '(1-32 chars)' next to it.
- Password**: A text input field with '(1-32chars)' next to it.
- Auth method**: A dropdown menu showing 'PAP Or CHAP'.
- Network type**: A dropdown menu.
- NAT**: A checkbox labeled 'Enabled' which is checked.

At the bottom of the form, there are two buttons: 'Previous' and 'Next'. A red tip message is visible on the right side of the form: 'Tips: By default, the load sharing mode is user-based average load sharing based on equal-cost routes. To modify and configure link load sharing, go to the Network > WAN Settings > Modify multi-WAN policy page.'

図11 高速設定:デュアルWAN設定

Fast Configuration

Online Help

Dual WAN config

line1 *

Operator * CMCC Unicom Telecom Custom

Link mode *

Link mode *

NAT Enabled

Username (1-32 chars)

Password (1-32chars)

Auth method

Network type

NAT Enabled

Tips: By default, the load sharing mode is user-based average load sharing based on equal-cost routes. To modify and configure link load sharing, go to the Network > WAN Settings > Modify multi-WAN policy page.

LAN設定の構成

WAN設定が完了すると、**LAN settings**ページが開きます。

1. **Local IP address**フィールドに、LAN内のデバイスで使用されるIPアドレスを入力します。
2. **IP mask**フィールドに、IPアドレスのマスクまたはマスク長を入力します。
(例:255.255.255.0または24)。
3. **DHCP server**フィールドで、必要に応じて**Enabled**を選択します。デバイスをDHCPサーバーとして機能させ、IPアドレスをLAN内のホストに割り当てるには、**Enabled**を選択します。
 - **Enabled**を選択した後、次のタスクを実行します。
 - **IP distribution range**フィールドに、割り当てるIPアドレスの開始IPアドレスと終了IPアドレスを入力します。
 - **Gateway address**フィールドに、デバイスがDHCPクライアントに割り当てるゲートウェイアドレスを入力します。
 - **DNS**フィールドに、デバイスがクライアントに割り当てるDNSサーバーのIPアドレスを入力します。
 - **Enabled**を選択しない場合、デバイスでDHCPは有効になりません。
4. **Next**をクリックして、LANの設定を完了します。

図12 高速設定:LANの設定

Fast Configuration

LAN config

Local IP address * 192.168.0.1

IP mask * 255.255.254.0 (Example:255.255.255.0)

DHCP server Enabled

IP distribution range 192.168.1.2 ~ 192.168.1.254

Gateway address 192.168.0.1

DNS 192.168.0.1

Previous Next

ネットワーク

WAN設定

WAN設定の概要

広域ネットワーク(WAN)は、地理的に広い範囲にわたって通信サービスを提供します。インターネットは巨大なWANネットワークです。

一般に、デバイスは、WANネットワークアクセス用に複数のWANサーバーを提供します。

シナリオの選択

このタスクについて

デバイスは、次のWANアクセスシナリオをサポートしています。

- **Single-WAN scenario:** ネットワークサービスが1つのインターネットサービスプロバイダーによってのみ提供される場合は、このシナリオを選択します。
- **Multi-WAN scenario:** ワークサービスが2つのインターネットサービスプロバイダーによって提供されている場合は、このシナリオを選択します。

どちらのシナリオでも、設定手順は同じです。

手順

1. ナビゲーションペインで、**Network > WAN Settings**を選択します。

デフォルトでは、**Scene**タブが表示されます。

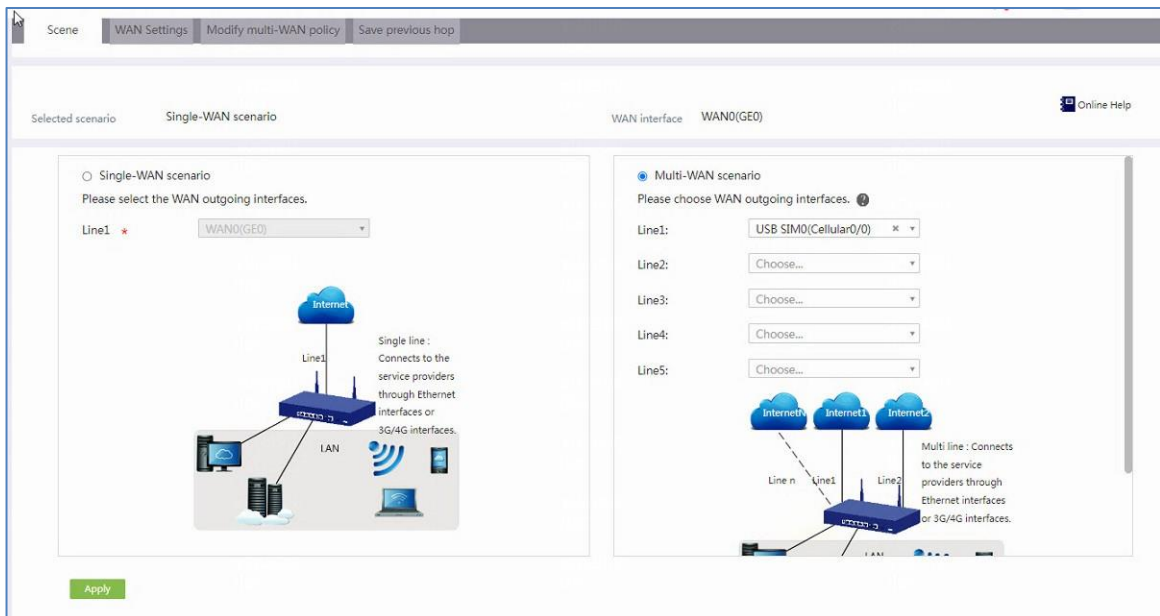
2. 必要に応じて、**Single-WAN scenario**または**Multi-WAN scenario**を選択します。
3. WANネットワークアクセス用に1つまたは複数のサーバーを選択します。これは、物理WANサーバーでも、モバイル通信モデム用のセルラーサーバーでもかまいません。

- 単一WANのシナリオでは、回線1のサーバーを選択します。
- マルチWANのシナリオでは、回線1、回線2、回線3、および回線4のサーバーを選択します。

モバイル通信モデムがUSBサーバーに挿入されている場合は、interface **USB SIM0(Cellular0/m)**を選択します。モバイル通信モデムがSICモジュールまたはデバイスに内蔵されているモデムの場合は、SIMカードが挿入されているサーバー**SIMx(Cellularn/m)**を選択します。

4. 適用をクリックします。

図13 シナリオの選択



WAN設定の構成

このタスクについて

物理サーバーまたはモバイル通信(3G/4G)モデムを使用して、WANネットワークにアクセスできます。

物理サーバーを介したWANネットワークへのアクセス

1. ナビゲーションペインで、**Network > WAN Settings**を選択します。
2. **WAN Settings**タブをクリックします。

図14 WANの設定

Line	Interface	Connection mode	IP address	MAC address	NAT	Operation
1	WAN0(GE0)	Fixed IP	192.168.200.14	1C-A8-34-C7-CF-34	Enable	<input checked="" type="checkbox"/>

3. 行の編集アイコンをクリックします。
4. 接続モードを選択します。オプションには、**PPPoE**、**DHCP**、および**Fixed IP**があります。
 - **PPPoE**を選択する場合は、次のパラメータを設定します。
 - **User ID**フィールドに、サービスプロバイダーから提供されたユーザー名を入力します。
 - **User password**フィールドに、サービスプロバイダーから提供されたパスワードを入力します。
 - **Online mode**で**Always online**を選択します。
 - **DHCP**を選択した場合、デバイスはWANアクセス用にDHCPサーバーからパブリックIPアドレスを取得します。
 - **Fixed IP**を選択した場合は、次のパラメータを設定します。
 - **IP address**フィールドに、固定IPアドレスを入力します。
 - **Subnet mask**フィールドに、サブネットマスクまたはサブネットマスクの長さ(たとえば、255.255.255.0または24)を入力します。
 - **Gateway**フィールドに、ゲートウェイのIPアドレスを入力します。
 - **DNS1**フィールドと**DNS2**フィールドに、プライマリDNSサーバーとセカンダリDNSサーバーのIPアドレスをそれぞれ入力します。プライマリDNSサーバーがドメイン名解決に失敗した場合、セカンダリDNSサーバーが使用されます。
5. **Using the interface to the default MAC(XX-XX-XX-XX-XX-XX)**または**Using the specified MAC for MAC**を選択します。

Using the specified MACを選択した場合は、MACアドレスを入力します。WANネットワークアクセス用にインターネットサービスプロバイダーによって割り当てられたIPアドレスを使用する場合は、スタティックMACアドレスを設定します。
6. NATを有効にするかどうかを選択します。

LANネットワーク上の複数のデバイスが同じパブリックIPアドレスを共有する場合は、この機能を有効にします。変換にアドレスプールを使用するには、**Use Address Pool for Translation**を選択し、アドレスプールを選択します。
7. **TCP MSS**フィールドに、**MSS**値を入力します。

8. **MTU**フィールドに、MTU値を入力します。
9. リンク検出を有効にするかどうかを選択します。

この機能は、指定されたIPアドレスへのリンクステータスを検出することで、リンクの可用性を向上させます。この機能をイネーブルにする場合は、次のパラメータを設定します。

- **Detection address**フィールドに、リンク検出用のIPアドレスを入力します。
 - **Detection interval**フィールドに、リンク検出間隔を入力します。
10. 適用をクリックします。

図15 WAN設定の変更

Modify WAN configuration

WAN interface: WAN0(GE0)

Connection mode: Fixed IP

IP address *: 192.168.200.14

Subnet mask *: 255.255.255.128

Gateway: 192.168.200.1

DNS1:

DNS2:

MAC: Using the interface to the default MAC(1C-AB-34-C7-CF-34)
 Using the specified MAC:

NAT function: Enable

Use Address Pool for Translation: Please Choose Address Pool

TCP MSS: 1280 (128-1610bytes)

MTU: 1500 (46-1650bytes)

Link detection: Disable

Detection address:

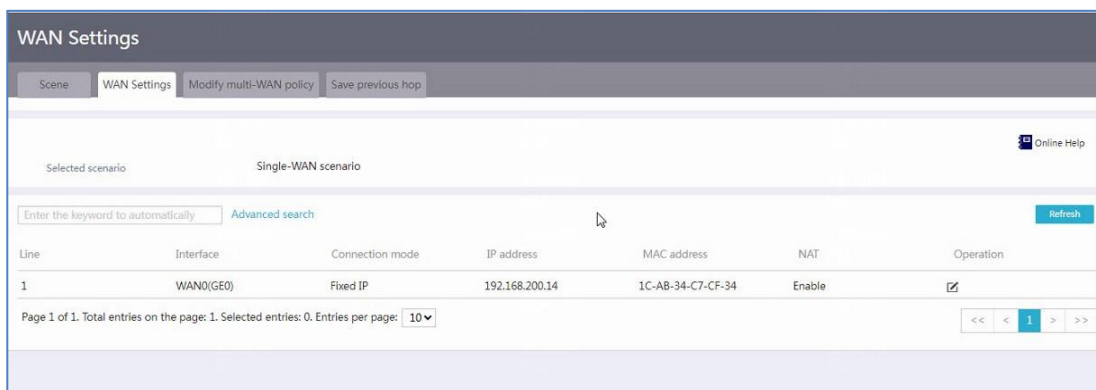
Detection interval: (1-10s)

Apply Cancel

モバイル通信(3G/4G)モデムを介したWANネットワークへのアクセス

1. ナビゲーションペインで、**Network > WAN Settings**を選択します。
2. **WAN Settings**タブをクリックします。

図16 WANの設定



3. 行の編集アイコンをクリックします。
 4. サービスプロバイダーを選択します。オプションには、**Mobile**、**Unicom**、**Telecom**および**Custom**があります。
 - **Mobile**、**Unicom**、および**Telecom**を選択した場合は、次のパラメータを設定します。
 - **Username**フィールドに、サービスプロバイダーから提供されたユーザー名を入力します。
 - **Password**フィールドに、サービスプロバイダーから提供されたパスワードを入力します。
 - **Auth method**フィールドで、ユーザー認証方式を選択します。

オプションには、**PAP or CHAP**、**PAP**および**CHAP**があります。CHAPはPAPよりもセキュアです。ネットワークがセキュアでない場合は、CHAPを選択します。デバイスおよびユーザーのエンドポイントが認証方式を自動的にネゴシエートするには、**PAP or CHAP**を選択します。認証方式を有効にするには、ユーザー名とパスワードを指定する必要があります。
 - **Custom**を選択した場合は、次のパラメータを設定します。
 - **APN**フィールドに、サービスプロバイダーが提供するAPNを入力します。
 - **Dialer number**フィールドに、サービスプロバイダーから提供されたダイヤルアップ文字列を入力します。
 - **Username**フィールドに、サービスプロバイダーから提供されたユーザー名を入力します。
 - **Password**フィールドに、サービスプロバイダーから提供されたパスワードを入力します。
 - **Auth method**フィールドで、ユーザー認証方式を選択します。

オプションには、**PAP or CHAP**、**PAP**および**CHAP**があります。CHAPはPAPよりもセキュアです。ネットワークがセキュアでない場合は、CHAPを選択します。デバイスおよびユーザーのエンドポイントが認証方式を自動的にネゴシエートするには、**PAP or CHAP**を選択します。認証方式を有効にするには、ユーザー名とパスワードを指定する必要があります。

海外のサービスプロバイダーのSIMカードまたはIoT SIMカードを使用する場合は、カスタムを選択します。
 5. **Mode**で、サービスプロバイダーのネットワークモードを選択します。
 6. NATを有効にするかどうかを選択します。
- LANネットワーク上の複数のデバイスが同じパブリックIPアドレスを共有する場合は、この機能を有

効にします。変換にアドレスプールを使用するには、**Use Address Pool for Translation**を選択し、アドレスプールを選択します。

7. リンク検出を有効にするかどうかを選択します。

この機能は、指定されたIPアドレスへのリンクステータスを検出することで、リンクの可用性を向上させます。この機能をイネーブルにする場合は、次のパラメータを設定します。

- **Detection address**フィールドに、リンク検出用のIPアドレスを入力します。
- **Detection interval**フィールドに、リンク検出間隔を入力します。

8. 暗証番号(PIN)は、SIMカードが他のユーザーによって使用されるのを防止します。PINコードを設定するには、**More Config**をクリックし、次のパラメータを設定します。

- PIN照合を有効にするかどうかを選択します。

この機能を有効にする場合は、PINコードを入力します。デバイスのセキュリティを強化するには、この機能を有効にすることをお勧めします。

- PINコードを変更するには、**Modify PIN**をクリックし、次のパラメータを構成します。
 - **Current PIN Code**フィールドに、古いPINコードを入力します。
 - **New PIN Code**フィールドに、新しいPINコードを入力します。
 - **Confirm New PIN Code**フィールドに、新しいPINコードをもう一度入力します。
 - 変更を送信するには、変更のコミットをクリックします。変更をキャンセルするには**Back**をクリックする。
- PINコードのロックを解除するには、**Unlock PIN**をクリックし、次のパラメータを構成します。
 - 「PINロック解除コード」フィールドに、PINロック解除コードを入力します。
 - **New PIN Code**フィールドに、新しいPINコードを入力します。
 - **Confirm New PIN Code**フィールドに、新しいPINコードをもう一度入力します。
 - PINコードのロックを解除するには、**Unlock**をクリックします。変更を取り消すには、**Back**をクリックします。
- モバイル通信モデムを再起動するには、**Reboot Modem**をクリックします。

9. **Save Config**をクリックします。

図17 WAN設定の変更

Modify WAN configuration

WAN interface: USB SIM0(Cellular0/0)

Service provide: Mobile Unicom Telecom Custom

Username: (1-32chars)

Password: (1-32chars)

Auth method:

Mode:

NAT function:

Use Address Pool for Translation

Link detection:

Detection address:

Detection interval: (1-10s)

More Config

Enable PIN Verification

PIN Code: (4-8 digits)

* Please ensure correct PIN code,for that consecutive PIN verification failures might lock a SIM/UIM card.

* After enabling PIN verification,please reboot modem.when the status prompts for "SIM/UIM Need PIN Verification" then enter the modem authentication pin and save the configuration.

* If unfortunately locked,please use the PUK code to unlock the card.

マルチWANポリシーの変更

制限事項およびガイドライン

このタスクは、マルチWANシナリオでのみサポートされます。

手順

1. ナビゲーションペインで、**Network > WAN Settings**を選択します。
2. **Modify Multi-WAN policy**タブをクリックします。
3. 次のように、マルチWANポリシーを変更します。
 - 複数のWANが同じサービスプロバイダーに属している場合は、**Average load sharing**またはベストプラクティスとしての**Bandwidth proportion load sharing**を選択します。
 - サービスプロバイダーがすべてのリンクに同じ帯域幅を提供する場合は、**Average load sharing**を選択します。

- リンク帯域幅が異なる場合は、**Bandwidth proportion load sharing**を選択します。
- 複数のWANが異なるサービスプロバイダーに属している場合は、ベストプラクティスとして **Service provider-based load sharing**または**Multilink advanced load sharing**を選択します。
 - 各サービスプロバイダーが同じリンク帯域幅を提供する場合は、**Service provider-based load sharing**を選択します。
 - リンク帯域幅が異なる場合は、**Multilink advanced load sharing**を選択します。
- ネットワークの安定性を確保するには、次のようにリンクをバックアップします。
 - **Main link (please select the WAN interface for the main link)** を選択し、回線を選択します。
 - **Backup link(please select the WAN interface for the backup link)**を選択し、回線を選択します。

メインリンクとバックアップリンクの行が異なることを確認します。

4. Applyをクリックします。

図18 マルチWANポリシーの変更

The screenshot shows the 'WAN Settings' configuration page. At the top, there are navigation tabs: 'Scene', 'WAN Settings', 'Modify multi-WAN policy', and 'Save previous hop'. The main content area is titled 'WAN Settings' and contains the following sections:

- When multiple WANs belong to the same service provider, select one of the following modes:**
 - Average load sharing ⓘ
 - Bandwidth proportion load sharing ⓘ
- When multiple WANs belong to different service providers, select one of the following modes:**
 - Service provider-based load sharing ⓘ
 - Multilink advanced load sharing ⓘ
- Link backup**
 - Main link (please select the WAN interface for the main link)

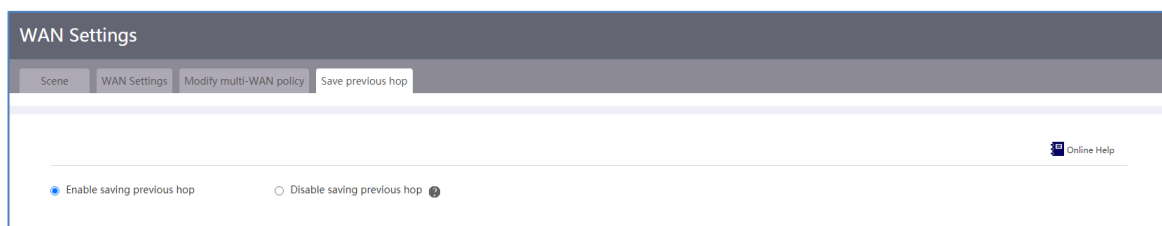
At the bottom left of the configuration area, there is a green 'Apply' button.

前のホップを保存

1. ナビゲーションペインで、ネットワーク **Network > WAN Settings** を選択します。
2. **Save previous hop** タブをクリックします。
3. 前のホップの保存を有効にするかどうかを選択します。

マルチWANのシナリオでは、この機能をイネーブルにして、LANネットワークを発信元または宛先とするパケットが同じWANサーバーを介して転送されるようにします。

図19 前のホップの保存



LANの設定

LAN設定の概要

内部ネットワークに接続するためのLANサーバーを設定し、DHCPをイネーブルにして、サーバーをVLANに割り当てるには、次の作業を実行します。

DHCPは、主にLAN内のホストにIPアドレスを割り当てるために使用されるLANプロトコルです。DHCPは、次の割り当てメカニズムをサポートしています。

- **Dynamic allocation:** この機能をサーバーに構成します。この機能は、IPアドレスをホストに動的に割り当てます。IPアドレスのリースが期限切れになった後、またはIPアドレスがホストによって明示的に拒否された後、IPアドレスは別のホストで使用できます。この割り当てメカニズムは、IPアドレスを一定期間ホストに割り当てる場合に適用されます。
- **Static allocation:** 静的IPアドレスはサーバーにバインドされず、ホストNICのMACアドレスにバインドされます。静的IPアドレスは永続的に使用できます。この割り当てのメカニズムは、IPアドレスをホストに永続的に割り当てる場合に適用されます。

LANサーバー設定を構成する

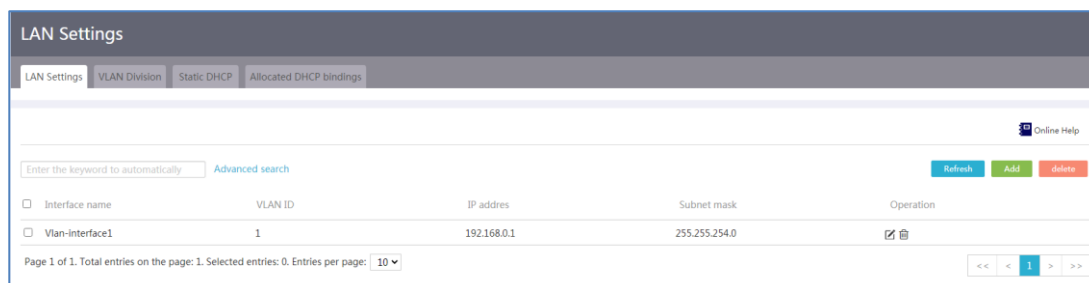
ネットワーク構成

内部ネットワークに接続するGEサーバーのIPアドレスを設定する場合、またはVLANとそのVLANサーバーを作成する場合は、次の作業を実行します。

手順

1. ナビゲーションペインで、**Network>LAN Settings**の順に選択します。
2. **LAN Settings**タブをクリックします。

図20 LANの設定



3. **Add**をクリックします。
4. **LAN interface type**フィールドで、サーバータイプを選択します。
 - VLANサーバーを選択した場合は、VLAN IDを入力して、VLANとそのVLANサーバーを作成します。
 - **GE interface**を選択する場合は、GEサーバーを選択します。
5. **Interface IP address**フィールドに、サーバーのIPアドレスを入力します。
6. **Subnet mask**フィールドに、IPアドレスのマスクまたはマスクの長さを入力します (例:255.255.255.0または24)。
7. **TCP MSS**フィールドで、サーバーのTCPパケットの最大セグメントサイズ(MSS)を設定します。
8. **MTU**フィールドに、サーバーのMTUを入力します。
9. 接続されているクライアント(コンピュータなど)にIPアドレスを動的に割り当てるデバイスの場合は、**Enable DHCP**を選択してデバイスのDHCPを有効にします。
10. **Apply**をクリックします。

図21 LANサーバーの追加

Add LAN

LAN interface type VLAN interface GE interface

Please choose GE interface * GE2

Interface IP address 192.168.1.1

Subnet mask 255.255.255.0

TCP MSS 1000 (128-1610bytes)

MTU 2000 (46-1650bytes)

Enable DHCP

Start address of pool 192.168.1.1

End address of pool 192.168.1.254

Forbidden address ? 192.168.1.1

Gateway address 192.168.1.1

DNS1 192.168.1.1

DNS2

Address lease

minute(range:1-11520,default:1440)

Apply Cancel

VLANの設定

ネットワーク構成

デバイス上のLANサーバーを指定されたVLANに割り当てて、同じVLAN内のホストが通信できるようにし、異なるVLAN内のホストが直接通信できないようにします。

制限事項およびガイドライン

詳細なポート設定ページでサーバーのPVIDとしてVLANを設定する場合は、VLANがすでに作成されていることを確認します。

注:

PVIDは、ポートのデフォルトVLANを識別します。ポートで受信されたタグなしパケットは、PVIDからのパケットと見なされます。

前提条件

デバイス上で各LANサーバーが属するVLANを計画し、LANサーバー設定ページで対応するVLANサーバーを作成します。

手順

1. ナビゲーションペインで、**Network > LAN Settings**の順に選択します。
2. **VLAN Division**タブをクリックします。

図22 VLANの分割

Port	PVID	Permitted VLANs	Operation
GE4	1		<input checked="" type="checkbox"/>
GE5	1		<input checked="" type="checkbox"/>
GE6	1		<input checked="" type="checkbox"/>
GE7	1		<input checked="" type="checkbox"/>
GE8	1		<input checked="" type="checkbox"/>
GE9	1		<input checked="" type="checkbox"/>

3. サーバーリストで、サーバーの**Edit**アイコンをクリックします。詳細なポート設定ページが開きます。
4. **PVID**フィールドに、サーバーのPVIDを入力します。
5. VLANにサーバーを割り当てたり、VLANからサーバーを削除したりするには、次の手順を実行します。
 - 使用可能なVLANリストでVLAN IDをクリックしてサーバーをVLANに割り当てるか、使用可能なVLANリストの上にある右矢印アイコンをクリックしてサーバーを使用可能なすべてのVLANに割り当てます。
 - VLANからサーバーを削除するには、許可VLANリストでVLAN IDをクリックします。選択したすべてのVLANからサーバーを削除するには、許可VLANリストの上にある左向き矢印アイコンをクリックします。
6. **Apply**をクリックします。

図23 ポート構成の詳細

Detailed port configuration

Port name * GE4

PVID * 1

Available VLANs

Permitted VLANs

→→ ←←

VLAN1

Apply Cancel

モニターでDHCPを有効にする

ネットワーク構成

デバイスが、モニターに接続されているクライアント(コンピュータなど)にIPアドレスを動的に割り当てるには、モニターでDHCPをイネーブルにします。

制限事項およびガイドライン

モニターで指定されたアドレスプールが、デバイスで指定されたWANサーバーのIPアドレス範囲と重複していないことを確認します。

手順

1. ナビゲーションペインで、**Network > LAN Settings**の順に選択します。
2. **LAN Settings**タブをクリックします。
3. サーバーの**Edit**アイコンをクリックします。
4. **Enable DHCP**オプションを選択します。
5. **Start address of pool**フィールドと**End address of pool**フィールドで、DHCPがクライアントに割

り当てることができるIPアドレスの範囲を指定します。

6. **Forbidden address**フィールドで、クライアントに割り当てることができないIPアドレスを指定します。
アドレス範囲内の一部のIPアドレス(ゲートウェイアドレスなど)をクライアントに割り当てることができない場合は、これらのアドレスを禁止アドレスとして指定します。
7. **Gateway address**、**DNS1**、および**DNS2**フィールドに、それぞれゲートウェイ、プライマリDNSサーバー、およびセカンダリDNSサーバーのIPアドレスを入力します。
8. **Address Lease**フィールドに、割り当てるIPアドレスのリース(分単位)を入力します。たとえば、IPアドレスのリースを5日間に指定するには、7200と入力します。
9. **Apply**をクリックします。

図24 LANサーバーの編集

The screenshot shows a 'Modify LAN' configuration window with the following fields and values:

VLAN ID *	1	(1-4094)
Interface IP address *	192.168.0.1	
Subnet mask *	255.255.254.0	
TCP MSS	1280	(128-1460bytes)
MTU	1500	(46-1500bytes)
<input checked="" type="checkbox"/> Enable DHCP		
Start address of pool	192.168.1.2	
End address of pool	192.168.1.254	
Forbidden address ?		
Gateway address	192.168.0.1	
DNS1	192.168.0.1	
DNS2		
Address lease	1440	minute(range:1-11520,default:1440)

Buttons: Apply (green), Cancel (red)

スタティックIP-MACバインディングを作成する

ネットワーク構成

一部のクライアントに固定IPアドレスを割り当てるには、クライアントのMACアドレスをIPアドレスにバインドするようにスタティックDHCPを設定します。

制限事項およびガイドライン

スタティッククライアントIPアドレスが、デバイスで指定されたWANサーバーIPアドレス範囲に含まれていないことを確認します。

前提条件

任意のサーバーでDHCPを有効にします。静的DHCPのみを使用してIPアドレスを割り当てるには、サーバーのDHCP設定も削除する必要があります。

手順

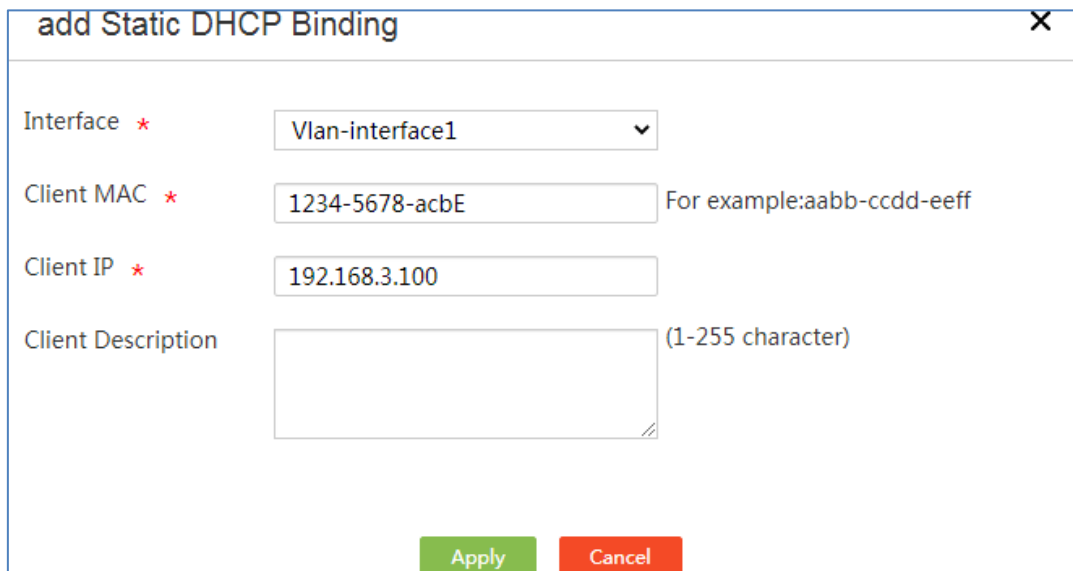
1. ナビゲーションペインで、**Network > LAN Settings**の順に選択します。
2. **Static DHCP**タブをクリックします。
3. **Add**をクリックします。
4. **Interface**リストから、DHCP対応のサーバーを選択します。
5. **Client MAC**フィールドに、クライアントのMACアドレスを入力します。

PCタイプのクライアントの場合は、MACアドレスのNIC情報を確認できます。

デバイスタイプクライアントの場合は、**display interface**コマンドを実行して、サーバーのMACアドレスを取得します。

6. **Client IP**フィールドに、デバイスに割り当てるIPアドレスを入力します。
7. **Apply**をクリックします。

図25 スタティックIP-MACバインディングの作成



複数のスタティックIP-MACバインディングを一括で作成する

制限事項およびガイドライン

スタティックIP-MACバインディングを一括して作成するには、クライアントMACアドレスとIPアドレス間のマッピングをインポートします。

手順

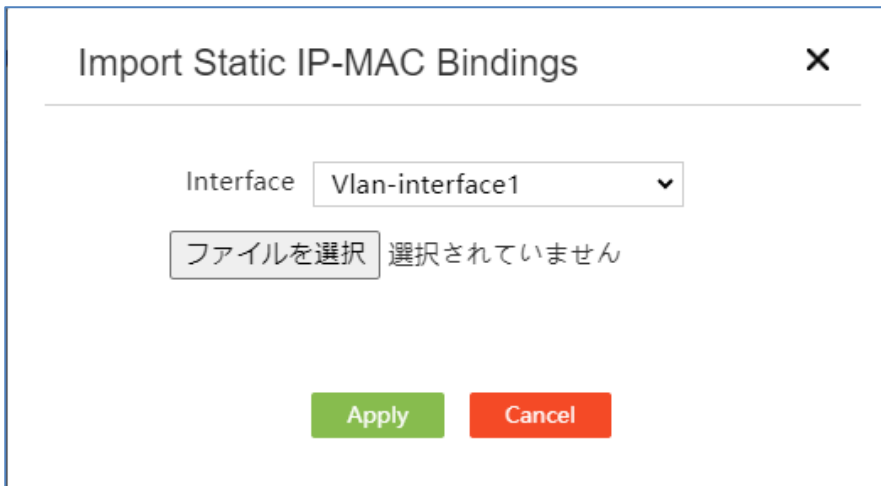
1. ナビゲーションペインで、**Network > LAN Settings**の順に選択します。
2. **Static DHCP**タブをクリックします。
3. **Import**をクリックします。
4. **Interface**リストから、DHCPサーバーとして動作するサーバーを選択します。
5. **Select File**をクリックし、スタティックIP-MACバインディングを保存するファイルを選択します。

注:

Excelを使用して、静的バインドテーブルを作成できます。このテーブルには、IP ADDRESS、MASK、MAC ADDRESSおよびDESCRIPTION(オプション)の各列が含まれます。必要に応じてこれらの列の内容を構成した後、テーブルをCSV形式で保存します。

6. **Apply**をクリックします。
7. DHCPクライアントに割り当てられたIPアドレスを表示するには、**Allocated DHCP bindings**タブをクリックします。

図26 スタティックIP-MACバインディングのインポート



割り当てられたDHCPバインディングを表示する

前提条件

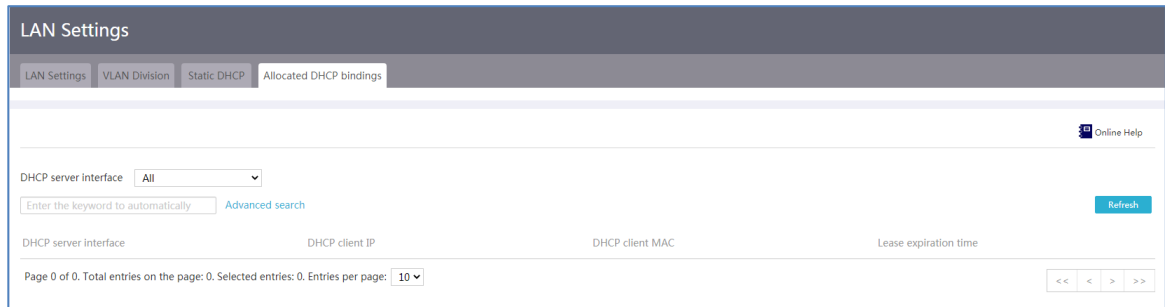
サーバーでスタティックまたはダイナミックDHCPを設定すると、DHCPクライアントに割り当てられたIPアドレスを表示できます。

手順

1. ナビゲーションペインで、**Network > LAN Settings**の順に選択します。
2. **Allocated DHCP bindings**タブをクリックします。
3. サーバーによって割り当てられたIPアドレスを表示するには、**DHCP server interface**リストから

DHCPサーバーがイネーブルになっているサーバーを選択します。

図27 割り当てられたDHCPバインディング



ポート管理

ポート管理の概要

ポート管理を使用すると、ポートタイプ、デュプレックスモード、速度、MACアドレスなどの各物理ポートに関する情報を表示したり、ポートの物理ステータスを変更したり、ポートのデュプレックスモードと速度を変更したりできます。

手順

1. ナビゲーションペインで、**Network > Port Management**を選択します。
2. **Physical Status**カラムのトグルボタンをクリックして、ポートをイネーブルまたはディセーブルにします。

図28 ポート管理

Physical Interface	Port Type	Duplex mode	Speed(Kbps)	MAC Address	Physical Status	option
GE0	Layer3	Full	1000000	1C-AB-34-C7-CF-34	Up	<input checked="" type="checkbox"/>
GE1	Layer2	Auto	1000000	1C-AB-34-C7-CF-35	Up	<input checked="" type="checkbox"/>
GE2	Layer2	Auto	1000000	1C-AB-34-C7-CF-36	Up	<input checked="" type="checkbox"/>
GE3	Layer2	Auto	1000000	1C-AB-34-C7-CF-37	Up	<input checked="" type="checkbox"/>
GE4	Layer2	Auto	1000000	1C-AB-34-C7-CF-38	Up	<input checked="" type="checkbox"/>
GE5	Layer2	Auto	1000000	1C-AB-34-C7-CF-38	Up	<input checked="" type="checkbox"/>
GE6	Layer2	Auto	1000000	1C-AB-34-C7-CF-38	Up	<input checked="" type="checkbox"/>
GE7	Layer2	Auto	1000000	1C-AB-34-C7-CF-38	Up	<input checked="" type="checkbox"/>
GE8	Layer2	Auto	1000000	1C-AB-34-C7-CF-38	Up	<input checked="" type="checkbox"/>
GE9	Layer2	Full	1000000	1C-AB-34-C7-CF-38	Up	<input checked="" type="checkbox"/>

3. ポートの**Edit**アイコンをクリックします。
4. **Fiber/Copper Mode**リストからポートモードを選択します。
5. **Speed**リストから速度オプションを選択します。
6. ポートのMACアドレスを表示します。
7. **Apply**をクリックします。

図29 ポートの編集

Modify port configuration

Port Name **Layer3 (GE3)**

Port Status **Up**

Fiber/Copper Mode

Port Duplex

Speed

MAC address
(HH-HH-HH-HH-HH-HH)

NAT設定

NATの概要

Network Address Translation(NAT)は、IPパケットヘッダー内のIPアドレスを別のIPアドレスに変換します。これにより、プライベートホストは外部ネットワークにアクセスでき、外部ホストはプライベートネットワークリソースにアクセスできます。

NATは、次のアドレス変換方式をサポートしています。

- **Port mapping:** 1つのパブリックIPアドレスと異なるポート番号を使用して、複数の内部サーバー(Webサーバー、メールサーバー、FTPサーバーなど)が外部ホストにサービスを提供できるようにします。この方法により、パブリックIPアドレスのリソースを節約できます。
- **One-to-one mapping:** プライベートアドレスとパブリックアドレス間の固定マッピングを作成します。固定ネットワークアクセス要件には、この方式を使用します。固定パブリックIPアドレスを使用して内部サーバーにアクセスする必要がある場合、この方式が推奨されます。

NATには、次の高度な機能があります。

- **NAT hairpin:** 内部ユーザーがNATアドレスを使用して内部サーバーにアクセスできるようにします。この機能は、パブリックIPアドレスを使用して外部ユーザーにサービスを提供する内部サーバー宛ての内部ユーザートラフィックをゲートウェイで制御する場合に適用されます。
- **NAT ALG:** 内部ネットワークと外部ネットワークの間にアプリケーション層サービス(FTPやDNSなど)が存在する場合は、このアプリケーション層プロトコルに対してNAT ALGをイネーブルにし

ます。これにより、アドレス変換後にこのプロトコルのデータ接続を正しく確立できます。

ポートマッピングの構成

1. ナビゲーションペインで、**Network > NAT Settings**を選択します。

2. **Port mapping**タブで、**Add**をクリックします。

3. **Interface**リストから、インターネットに接続するモニターを選択します。

4. **Protocol Type**に**TCP**、**UDP**、**TCP+UDP**、または**Custom**を選択します。

内部サーバーが使用するトランスポート層プロトコルを選択するか、Customを選択した後にトランスポート層プロトコルを表す番号を入力します。FTPサーバーはTCPを使用し、TFTPサーバーはUDPを使用します。

5. **Global IP address**に**Current IP address**または**Other IP addresses**を選択します。

6. **Global port number**リストから、**FTP**、**Telnet**、または**User-defined ports**を選択します。

内部サーバーによって提供されるサービスがFTPまたはTelnetでない場合は、サービスのポート番号を入力します。たとえば、HTTPサーバーの場合はポート80です。**Custom for Protocol Type**を選択した場合、このフィールドは設定できません。

7. **Local IP address**フィールドに、内部サーバーのプライベートIPアドレスを入力します。

8. **Local port number**フィールドに、内部サーバーのポート番号を入力します。**Protocol Type**に**Custom**を選択した場合、このフィールドは構成できません。

9. **Apply** をクリックします。

図30 NATポートマッピングの追加

The screenshot shows a dialog box titled "Add NAT Port Mapping". It contains the following fields and options:

- Interface ***: A dropdown menu with "WAN0(GE0)" selected.
- Protocol Type ***: Radio buttons for "TCP" (selected), "UDP", "TCP+UDP", and "Custom" (with a port range input field set to "(1-255)").
- Global IP address ***: Radio buttons for "Current IP address" (selected) and "Other IP addresses".
- Global port number * ?**: A dropdown menu with "FTP" selected.
- Local IP address ***: A text input field containing "192.168.1.10".
- Local port number * ?**: Two text input fields for "Start Port Number" and "End Port Number", both with "(1-65535)" as a hint.
- Description**: A text area with "(1-63 characters)" as a hint.

At the bottom of the dialog are two buttons: "Apply" (green) and "Cancel" (red).

1対1のマッピングの構成

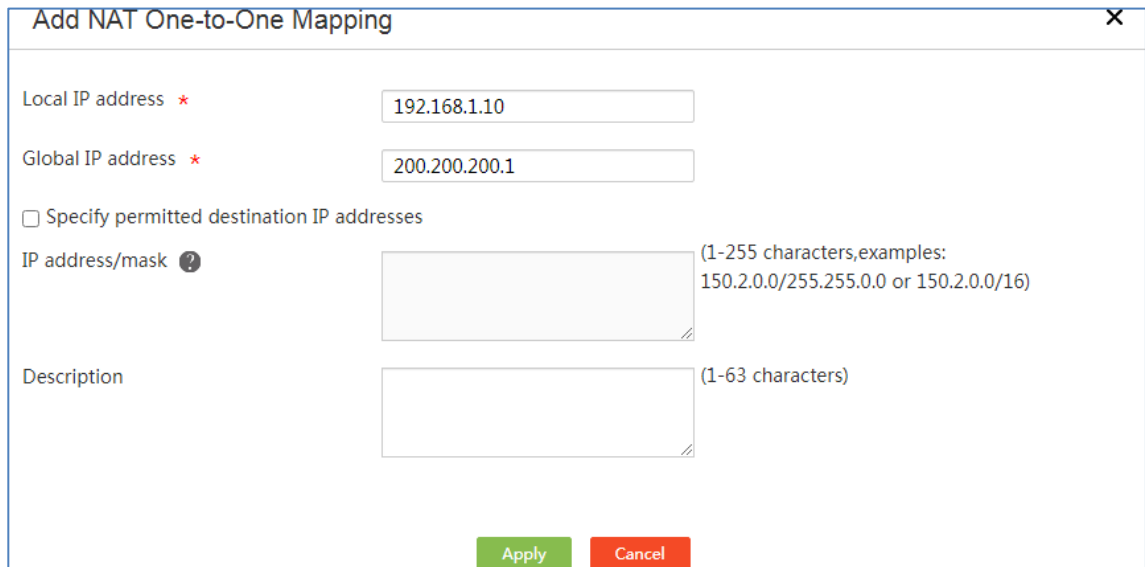
制限事項およびガイドライン

デバイスにパブリックIPアドレスが1つしかない場合は、1対1のマッピングを設定しないことを推奨します。

手順

1. ナビゲーションペインで、**Network > NAT Settings**を選択します。
2. **One-to-one mapping**タブをクリックします。
3. **Add**をクリックします。
4. **Local IP address**フィールドに、内部IPアドレスを入力します。
5. **Global IP address**フィールドに、外部IPアドレスを入力します。
6. 必要に応じて、**Specify allowed destination IP addresses**を選択します。
 - このオプションを選択する場合は、内部ユーザーがアクセスできる宛先IPアドレスを**IP address/mask**フィールドに入力します。アドレス変換は、指定された宛先アドレスを持つパケットに対して実行されます。
 - このオプションを選択しない場合、内部ネットワークから外部ネットワークに送信されるすべてのパケットに対してアドレス変換が実行されます。
7. **Apply**をクリックします。
8. **One-to-One mapping**タブで、**enable following OnetoOne mapping**を選択します。

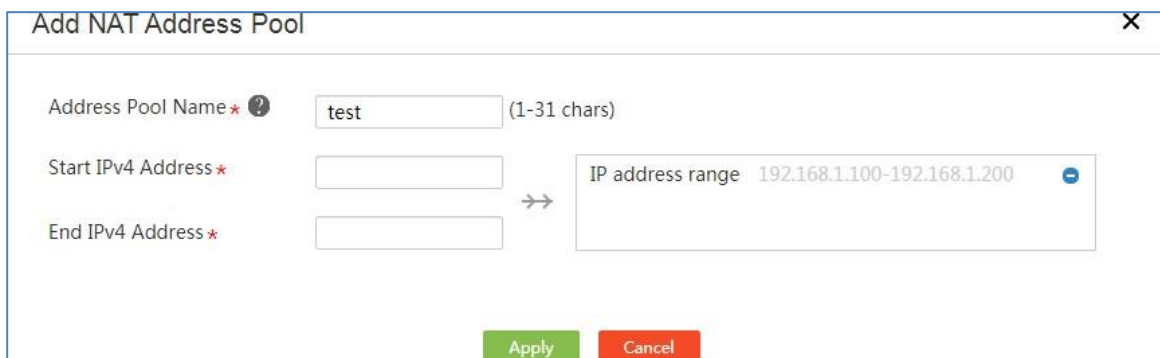
図31 NAT 1対1マッピングの追加



NATアドレスプールを設定する

1. ナビゲーションペインで、**Network > NAT Settings**を選択します。
2. **Address Pools**タブをクリックします。
3. **Add**をクリックします。
4. **Address Pool Name**フィールドに、アドレスプール名を入力します。
5. **Start IPv4 Address**フィールドに、開始IPv4アドレスを入力します。
6. **End IPv4 Address**フィールドに、終了IPv4アドレスを入力します。
7. アイコン \Rightarrow をクリックして、アドレスプール設定を送信します。
8. 複数のアドレス範囲を追加するには、手順5と手順6を繰り返します。
9. **Apply**をクリックします。

図32 NATアドレスプールの追加



NATヘアピンの設定

前提条件

NATヘアピンを設定する前に、ポートマッピングまたは1対1のマッピングを設定します。

手順

1. ナビゲーションペインで、**Network > NAT Settings**を選択します。
2. **Advanced Settings**タブをクリックします。
3. **NAT hairpin**領域で、**Open NAT hairpin function**を選択します。
4. **Apply**をクリックします。

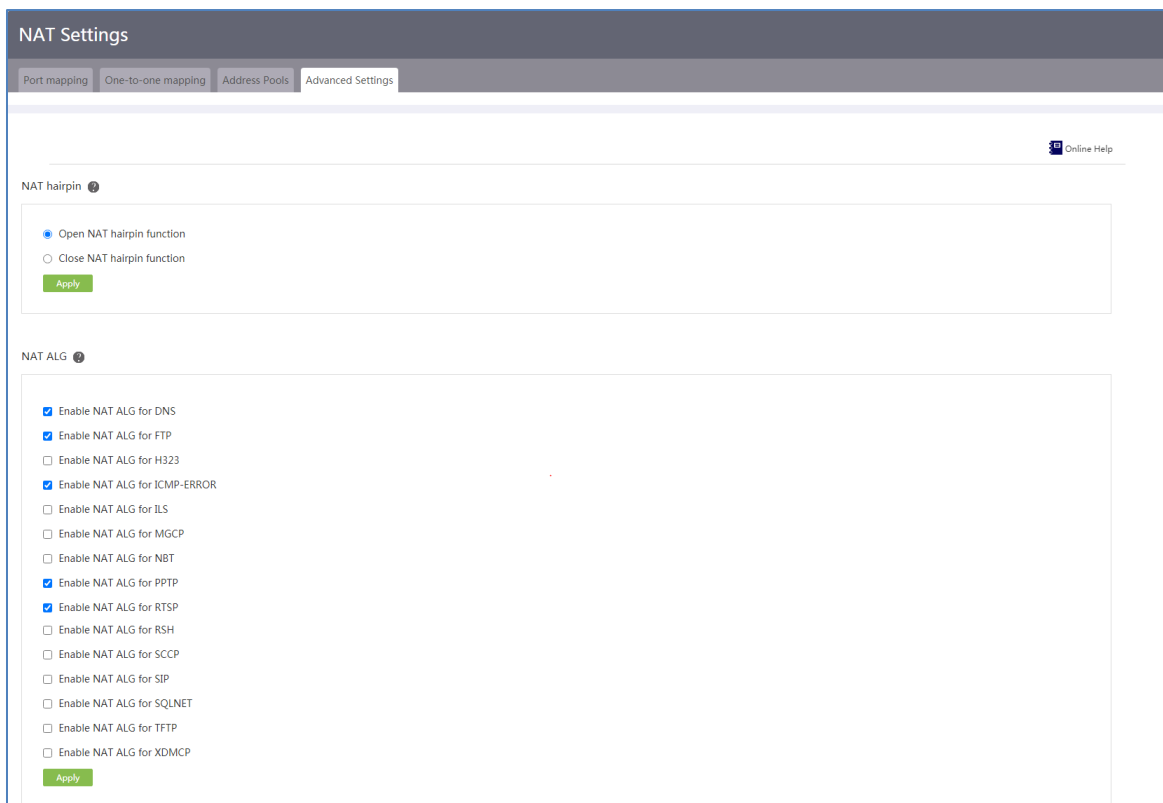
図33 詳細設定-NATヘアピン



NAT ALGの設定

1. ナビゲーションペインで、**Network > NAT Settings**を選択します。
2. **Advanced Settings**タブをクリックします。
3. プロトコルのNAT ALGをイネーブルにします。
4. **Apply**をクリックします。

図34 詳細設定-NAT ALG



ネットワーク動作の管理

ユーザーグループ

はじめに

ユーザーグループは、ホスト名またはIPアドレスのグループです。ユーザーグループには複数のメンバーを含めることができ、メンバーはホスト名、IPアドレスまたはIPアドレス範囲にすることができます。ユーザーグループを構成して、帯域幅管理などの一部のサービスのユーザーパケットを識別できます。

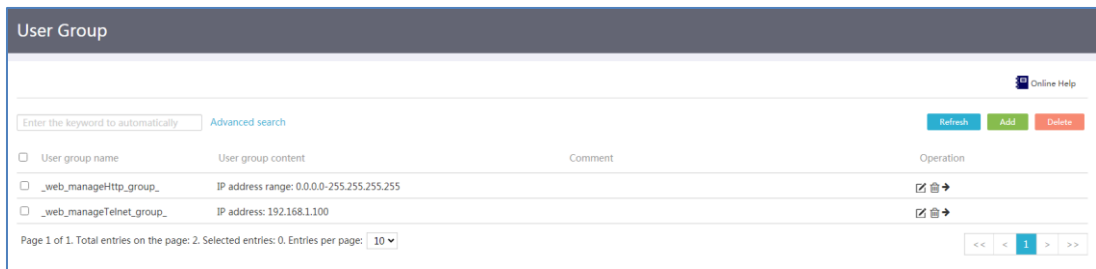
制限事項およびガイドライン

- IPアドレスメンバーに指定できるのはIPv4アドレスだけです。IPv6アドレスはサポートされていません。
- IPアドレス範囲の開始アドレスは、終了アドレスよりも小さくなければなりません。

手順

1. 左側のナビゲーションツリーから、**Network Behaviors > User Group**を選択します。

図35 ユーザーグループ



2. **Add**をクリックします。
3. **User group name**フィールドにユーザーグループ名を入力します。
4. **Comment**フィールドにユーザーグループの説明を入力します。
5. ユーザーグループのメンバーを設定します。
 - ユーザーグループに追加するホスト名を入力します。
 - ユーザーグループに追加するIPアドレスを入力します。
 - 開始アドレスと終了アドレスを入力して、ユーザーグループに追加するIPアドレス範囲を指定します。
 - IPアドレス範囲から除外するIPアドレスを指定します。
6. →→をクリックして、設定されたメンバーをコミットします。
7. 同じタイプの複数のメンバーを追加するには、手順5と6を繰り返します。
8. **Apply**をクリックします。

図36 ユーザーグループの追加

Add User Group

Online Help

User group name * ? test (1-63 chars)

Comment test (1-127 chars)

Host name ?

IP address

IP address range Start → End

Exclude IP address ?

Host name root

IP address 192.168.1.20

Apply Cancel

時間範囲グループ

はじめに

同じ機能(たとえば、帯域幅管理とネットワーク動作管理)を特定の期間だけ有効にする場合は、時間範囲グループを設定し、それを関連する機能に対して参照できます。

時間範囲グループには、複数の時間範囲を含めることができます。次のタイプの時間範囲を使用できません。

- **Periodic:** 毎週月曜日の8:00～12:00のように、特定の曜日に定期的に繰り返します。
- **Absolute:** 期間のみを表し、繰り返しません。たとえば、2015年1月1日の8:00から2015年1月3日の18:00までです。

時間範囲グループのアクティブ期間は、次のように計算されます。

- すべての定期ステートメントを結合します。
- すべてのabsoluteステートメントを結合します。
- 2つの文セットの共通部分を時間範囲グループのアクティブな期間とします。次の時間範囲を構成するとします。

- 定期的な時間範囲:月曜日から金曜日の08:30～12:00および13:30～18:00。
- 絶対時間範囲:2015年4月1日～2015年4月30日の10:00～12:00および14:00～16:00。

アクティブな期間は、2015年4月1日から2015年4月30日までの月曜日から金曜日の10:00～12:00お

よび14:00~16:00です。

制限事項およびガイドライン

- 最大1024の時間範囲を作成できます。各時間範囲には、最大32の周期時間範囲と12の絶対時間範囲が含まれます。
- CLIとWebモニターの両方から同じ時間範囲グループを設定することはできません。

1つのタイプの時間範囲のみを使用して時間範囲グループを設定する

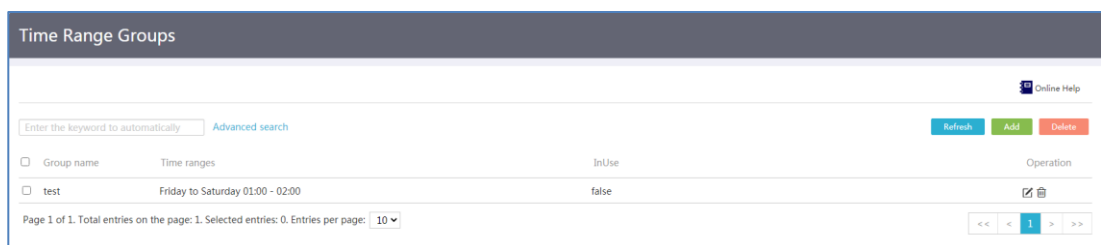
制限事項およびガイドライン

周期時間範囲または絶対時間範囲だけを含む時間範囲グループを設定するには、次の作業を実行します。

手順

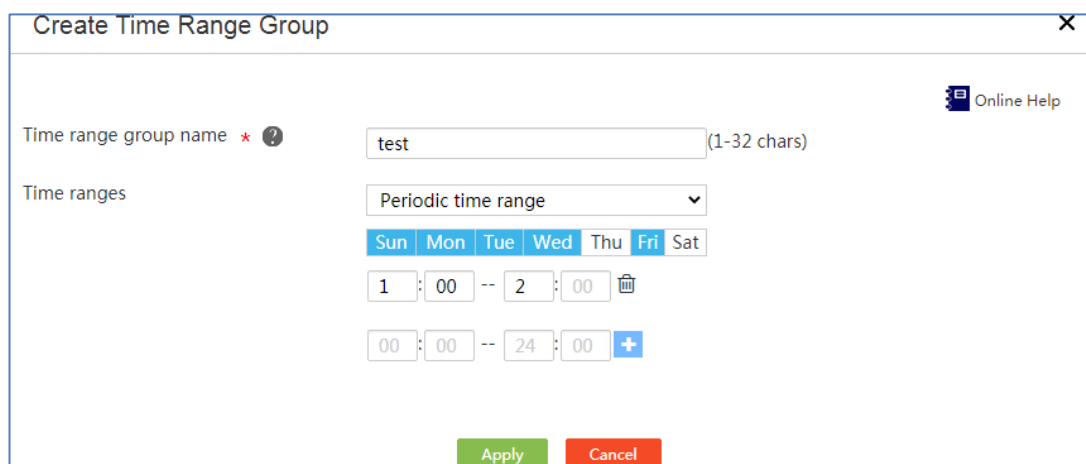
1. 左側のナビゲーションツリーから、**Network Behaviors > Time Range Group**を選択します。

図37 Time range group



2. **Add**をクリックします。
3. **Time range group name**フィールドに時間範囲グループ名を入力します。
4. **Time ranges**リストから、**Periodic time range**または**Absolute time range**を選択し、定期的な時間範囲または絶対時間範囲を設定します。
 - 定期的な時間範囲を設定するには、曜日を選択し、開始時刻と終了時刻を入力して、プラス記号をクリックします。
 - 絶対時間範囲を設定するには、開始日と終了日を選択し、開始時刻と終了時刻を入力して、プラス記号をクリックします。
5. **Apply**をクリックします。

図38 1つのタイプの時間範囲のみを使用した時間範囲グループの設定



定期的な時間範囲と絶対時間範囲の両方を含む時間範囲グループを設定する

制限事項およびガイドライン

定期的な時間範囲と絶対時間範囲の両方を含む時間範囲グループを設定するには、次の作業を実行します。

手順

1. 左側のナビゲーションツリーから、**Network Behaviors > Time Range Group**を選択します。
2. **Add**をクリックします。
3. **Time range group name**フィールドに時間範囲グループ名を入力します。
4. 時間範囲を設定します。
 - **Time ranges**リストから**Periodic time range**を選択します。曜日を選択し、開始時刻と終了時刻を入力して、プラス記号をクリックします。

図39 定期的な時間範囲の設定

Create Time Range Group

Time range group name * ? test (1-32 chars)

Time ranges

Periodic time range

Sun Mon Tue Wed Thu Fri Sat

1 : 00 -- 2 : 00

00 : 00 -- 24 : 00

Apply Cancel

- **Time range**リストから**Absolute time range**を選択します。開始日と終了日を選択し、開始時間と終了時間を入力して、プラス記号をクリックします。

図40 絶対時間範囲の設定

Create Time Range Group

Time range group name * ? test (1-32 chars)

Time ranges

Absolute time range

2022-11-07 -- 2022-11-07

1 : 00 -- 2 : 00

00 : 00 -- 24 : 00

Apply Cancel

5. **Apply**をクリックします。

時間範囲グループを編集する

制限事項およびガイドライン

周期時間範囲と絶対時間範囲の両方を含む時間範囲グループから、周期時間範囲または絶対時間範囲を削除するには、次の作業を実行します。

手順

1. 左側のナビゲーションツリーから、**Network Behaviors > Time Range Group**を選択します。
2. 時間範囲グループの**Operation**カラムで**Edit**をクリックします。
3. **Time ranges**リストから、**Periodic time range**または**Absolute time range**を選択します。

4. 各時間範囲の後に削除アイコンをクリックします。
5. **Apply**をクリックします。

図41 時間範囲グループの編集

帯域幅管理

はじめに

帯域幅管理では、トラフィックレートを制限し、ユーザーグループや時間範囲などの基準に基づいてトラフィックをきめ細かく制御できます。

遅延に影響されやすいインタラクティブトラフィックの場合は、グリーンチャネルをイネーブルにして帯域幅を保証できます。

帯域幅制限の設定

手順

1. ナビゲーションツリーから、**Network Behaviors > Bandwidth Management**を選択します。

図42 帯域幅の制限

User group	Time range	Interface	Upload(kbps)	Download(kbps)	Mode	Operation
<input type="checkbox"/>	_web_manageHttp_group_	any	100	200	Shared bandwidth	

2. **Bandwidth limits**タブで、**Add**をクリックします。**Add Bandwidth Policy**ページが開きます。
 - **Application Interface**リストからモニターを選択します。デバイスは、選択されたモニタ

一で帯域幅管理を実行します。

- **User range**エリアで、**Select existing groups**リストからユーザーグループを選択します。デバイスは、選択されたユーザーグループ内のユーザーに対して帯域幅管理を実行します。
- **Flow limitation**領域で、アップロード帯域幅とダウンロード帯域幅を設定し、帯域幅割り当て方式を選択します。アップロード帯域幅またはダウンロード帯域幅を指定しない場合、デバイスは使用されるアップロード帯域幅またはダウンロード帯域幅を制限しません。

帯域幅割り当て方式には、次のものがあります。

- **Sharing**: 指定した帯域幅がすべてのユーザーに均等に分配されます。
- **Monopoly**: 指定された帯域幅は、1人のユーザーによって排他的に使用されます。
- **Restricted period**領域で、時間範囲グループを選択します。

3. **Apply**をクリックします。

図43 帯域幅ポリシーの追加

Add Bandwidth Policy

Application Interface * ? WAN0(GE0) * ▾

User range *

Select existing groups ? _web_manageHttp_group_ ▾ New user group

Flow limitation *

Upload bandwidth 100 (8- 1000000kbps)

Download bandwidth 200 (8- 1000000kbps)

Traffic assignment ? Sharing Monopoly

Restricted period *

All time periods

Select existing time group ? ▾ New time group

Apply Cancel

グリーンチャネルを設定する

制限事項およびガイドライン

通常のトラフィックへの影響を回避するには、グリーンチャネルのレート値をあまり大きく設定しないでください。

手順

1. ナビゲーションツリーから、**Network Behaviors > Bandwidth Management**を選択します。
2. **Green channel**タブをクリックします。
3. **Enable the green channel**を選択します。
4. 遅延に影響されやすいインタラクティブトラフィック用に、アプリケーションのポート番号とポート番号を設定します。アプリケーションに一致するトラフィックだけがグリーンチャネルを介して送信されます。
 - a. **Define applications for the green channel**を選択し、**Add**をクリックします。
 - b. アプリケーション名、ポート番号、およびポート番号を設定します。
 - c. **Apply**をクリックします。
5. 定義されたすべてのアプリケーションに対して、次の制限パラメータを設定します。
 - トラフィックレートをすべてのWANモニターで同じ値に制限するには、**Bandwidth upper limit**

for the green channelを選択し、アップストリームまたはダウンストリームの最大トラフィックレートを設定します。

- トラフィックレートをWANモニターごとに異なる値に制限するには、**Bandwidth upper limit for the green channel**の選択を解除し、各WANモニターのアップストリームまたはダウンストリームの最大トラフィックレートを設定します。
- 最大パケット長を制限するには、**Match packets that are smaller than**を選択し、最大パケット長を設定します。最大パケット長を超えるパケットは、グリーンチャンネルでは送信されません。

6. Applyをクリックします。

図44 グリーンチャンネル

The screenshot shows the 'Bandwidth Management' configuration page. The 'Green channel' tab is selected. The 'Enable the green channel' checkbox is checked. The configuration includes fields for 'Upstream bandwidth of line 1' (set to 100 Mbps), 'Downstream bandwidth of line 1' (set to 300 Mbps), 'Upstream bandwidth of line 2' (set to 200 Mbps), and 'Downstream bandwidth of line 2' (set to 200 Mbps). There are also fields for 'Max guaranteed traffic rate for green channel' with sub-fields for 'Per-interface upstream traffic rate' and 'Per-interface downstream traffic rate'. The 'Match packets that are smaller than' checkbox is checked, with a 'Maximum length' field set to 1255535 Bytes. The 'Define applications for the green channel' checkbox is also checked. An 'Apply' button is visible at the bottom left. Below the main configuration area, there is a section for 'Define applications for the interface' with a search bar and a table with columns for 'No.', 'Application name', 'Application protocol', 'Port number', and 'Operation'. The table is currently empty.

帯域幅保証の設定

制限事項およびガイドライン

モニターの帯域幅保証ポリシーは、モニターの出力帯域幅が設定されている場合にだけ有効になります。

1つのモニターに設定できる帯域幅保証ポリシーは1つだけです。帯域幅保証ポリシーには複数の一致ルールを設定できます。一致ルールには複数の一致基準を設定できます。保証帯域幅は、一致するすべてのユーザーによって使用される帯域幅の合計です。

手順

1. ナビゲーションツリーから、**Network Behaviors > Bandwidth Management**を選択します。
2. **Bandwidth guarantee**タブをクリックします。
3. モニターの出力帯域幅を設定します。

- **Output bandwidth(Mbps)**フィールドに、サービスプロバイダーが提供する実際のリンク帯域幅を入力します。
- **Apply**をクリックします。

図45 帯域幅保証

The screenshot shows the 'Bandwidth Management' configuration page. The 'Bandwidth guarantee' tab is active. A table lists interfaces and their corresponding output bandwidths. The 'Apply' button is highlighted in green.

Interface	Output bandwidth (Mbps)
WAN0(GE0)	1-1000
USB1MU(Cellular/4G)	1-1000

4. モニターの帯域幅保証ポリシーを設定します。
 - **Add**をクリックします。**Create Bandwidth Guarantee Policy**ダイアログボックスが表示されます。
 - **Policy name**フィールドにポリシー名を入力します。
 - **Application interface**リストから、ポリシーを適用するモニターを選択します。

図46 帯域幅保証ポリシーの設定

The dialog box 'Create Bandwidth Guarantee Policy' is shown. The 'Policy name' field contains 'test' and the 'Application interface' dropdown is set to 'WAN0(GE0)'. An 'Add' button is visible. Below the form is a table with various configuration columns.

Queue ty...	Guarante...	Protocol	Proto...	Local subnet/mask	Local ... Peer subnet/mask	Peer ... Oper.
-------------	-------------	----------	----------	-------------------	----------------------------	----------------

- **Add**をクリックします。**Create Match Rule**ダイアログボックスが表示されます
- **Queue type**リストから、**EF**または**AF**を選択します。EFはAFよりも転送の優先順位が高くなります。
- **Guaranteed bandwidth**フィールドに、一致するすべてのユーザーが使用する合計帯域幅を入力します。
- **Match criteria configuration**領域で、プロトコル名を選択するかプロトコル番号を入力し、ローカルサブネット/マスクとローカルポート番号を設定し、ピアサブネット/マスクとピアポート番号を設定して、+アイコンをクリックします。
- **Apply**をクリックします。

5. **Create Bandwidth Guarantee Policy**ダイアログボックスで、**Apply**をクリックします。

図47 一致ルールの作成

Protocol	Protocol type	Local subnet/mask	Local port	Peer subnet/mask	Peer port
IP	0-255	192.168.1.0/24	0 - 65535	192.168.1.0/24	0 - 65535

ネットワーク動作の管理

はじめに

ネットワーク動作管理は、ユーザーがアクセスできるアプリケーションとWebサイトを制御し、ユーザーグループと時間範囲に基づいてネットワーク動作をきめ細かく制御します。

グローバルコントロールの設定

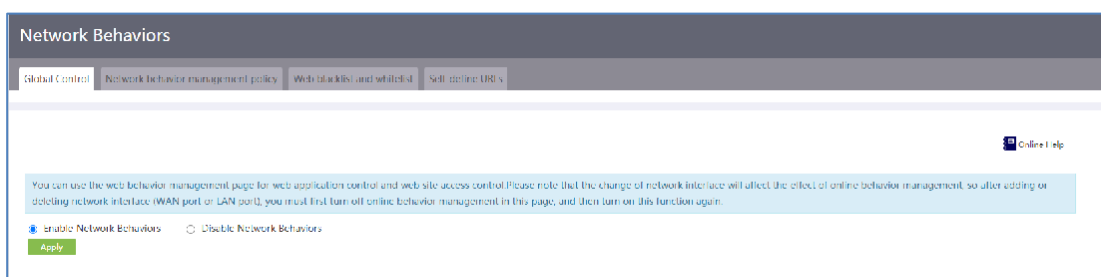
このタスクについて

ネットワーク動作管理ポリシーおよびURLモニタリングを有効にするには、次の作業を実行します。

手順

1. ナビゲーションツリーから、**Network Behaviors > Network Behaviors**を選択します。
2. **Global control**タブで、**Enable Network Behaviors**を選択します。
3. **Apply**をクリックします。

図48 グローバル制御



ネットワーク動作管理ポリシーを構成する

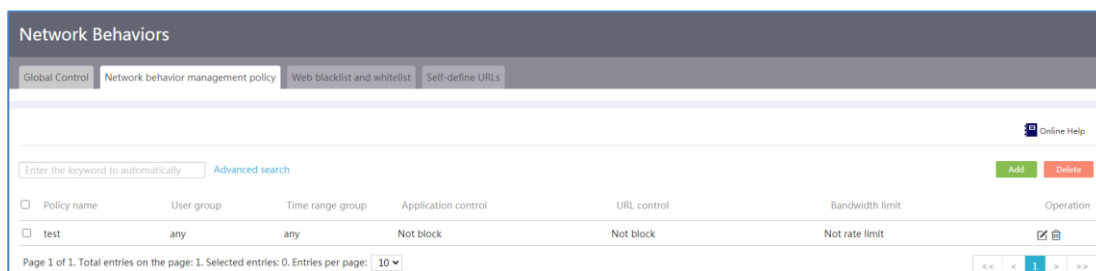
制限事項およびガイドライン

URLモニタリングはHTTPに基づいています。URLモニタリングを正しく機能させるには、HTTPをブロックしないでください。

手順

1. ナビゲーションツリーから、**Network Behaviors > Network Behaviors**を選択します。

図49 ネットワーク動作管理ポリシー



2. **Network behavior management policy**タブをクリックします。
3. **Add**をクリックし、次のパラメータを設定します。
 - **Policy name**フィールドにポリシー名を入力します。
 - **User range**領域で、ユーザーグループを選択します。
 - **Limit period**領域で、時間範囲グループを選択します。
 - **URL control**領域で、次の設定を行います。
 - **Select URL types**: 事前定義のURLタイプおよび自己定義のURLタイプを選択します。自己定義のURLの構成の詳細は、「自己定義のURLタイプの構成」を参照してください。
 - **Protocol**: プロトコルタイプ(HTTPまたはHTTPS)を選択します。デフォルトでは、HTTPSが選択されています。
 - **URL control action**: URL制御アクションを選択します。**Record**アクションを**Permit**アクションまたは**Deny**アクションとともに選択すると、許可または拒否動作に関する情報を記録できます。

- **Application control**領域で、**Select network applications**の右側にある**Details**アイコンをクリックしてアプリケーションを選択し、アプリケーションに対して次のいずれかのアクションを設定します。
 - **Block**: アプリケーションへのアクセスを拒否します。
 - **No blocking or rate limit**: レート制限なしでアプリケーションへのアクセスを許可します。
 - **Rate limit**: レート制限付きでアプリケーションへのアクセスを許可します。編集アイコンをクリックして、最大アップリンク帯域幅と最大ダウンリンク帯域幅を設定します。
- 4. **Apply**をクリックします。
- 5. **Global control**タブをクリックし、**Enable Network Behaviors**を選択して新しいポリシーを有効にします。

図50 ネットワーク動作管理ポリシーの設定

Webサイトのブラックリスト/ホワイトリストの設定

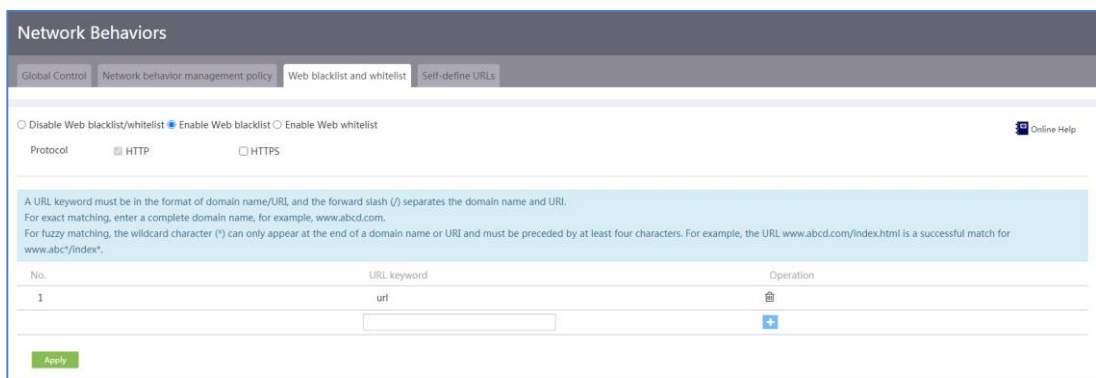
このタスクについて

特定のURLへのアクセスを許可またはブロックするには、次の作業を実行します。

手順

1. ナビゲーションツリーから、**Network Behaviors > Network Behaviors**を選択します。
2. **Web blacklist and whitelist**タブをクリックします。
3. **Enable Web blacklist**または**Enable Web whitelist**を選択します。
4. サポートするプロトコルタイプを選択します。オプションには、**HTTP**および**HTTPS**があります。デフォルトでは、**HTTP**が選択されています。
5. **URL keyword**フィールドにURLを入力し、**プラス記号**をクリックしてURLを追加します。
6. さらにURLを追加するには、手順4を繰り返します。
7. **Apply**をクリックして、**ブラックリスト**または**ホワイトリスト**の設定を完了します。

図51 Webサイトのブラックリスト/ホワイトリストの設定



自己定義URLタイプを設定する

このタスクについて

定義済みのURLタイプでは要件を満たせない場合に、このタスクを実行します。

制限事項およびガイドライン

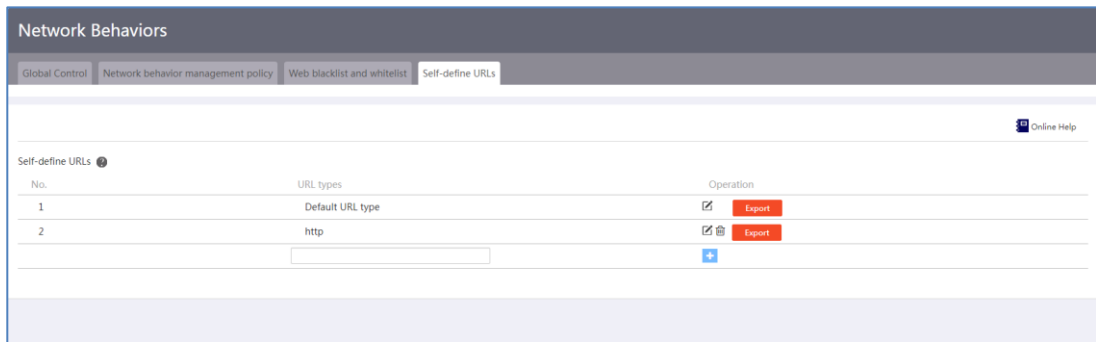
自己定義のURLをエクスポートできます。Internet Explorerブラウザを使用してURLをエクスポートするときにExcelの起動エラーが発生した場合は、IEの設定を次のように変更します。

1. IEツールバーで、**Tools**ボタンをクリックし、**Internet Options**を選択します。
2. **Security**タブをクリックし、**Custom level....**をクリックします。
3. **ActiveX controls and plug-ins**セクションで、**Initialize and script ActiveX controls not marked as safe for scripting**に対して**Enable**を選択します。

手順

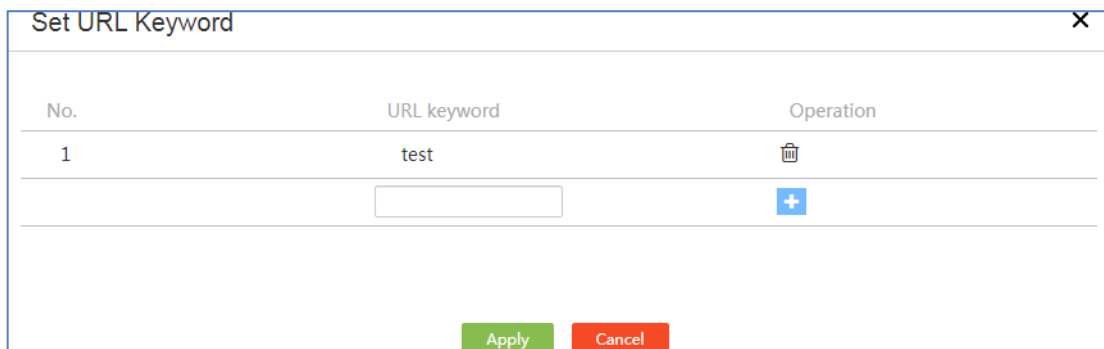
1. ナビゲーションツリーから、**Network Behaviors > Network Behaviors**を選択します。

図52 自己定義URL



2. **Self-define URLs**タブをクリックします。
3. URLタイプを入力し、プラス記号をクリックします。
4. URLをURLタイプに追加するには、編集アイコンをクリックします。
5. URLを入力し、プラス記号をクリックしてURLを追加します。
6. さらにURLを追加するには、手順5を繰り返します。
7. **Apply**をクリックします。

図53 URLキーワードの設定



シグニチャデータベース

シグニチャデータベースの概要

デバイスは、シグニチャを使用してアプリケーション層のトラフィックを識別します。デバイスは、アプリケーションシグニチャデータベースとURLシグニチャデータベースをサポートします。シグニチャデータベースを最新バージョンに更新できます。

デバイス上のシグニチャデータベースの更新には、次の方法を使用できます。

- シグニチャをインポートします。

最新のシグニチャファイルを手動でダウンロードし、そのファイルを使用してデバイス上のシグニ

チャデータベースを更新する必要があります。

- オンラインで更新します。

操作をトリガーした後、デバイスは自動的に最新のシグニチャファイルをダウンロードしてシグニチャデータベースを更新します。

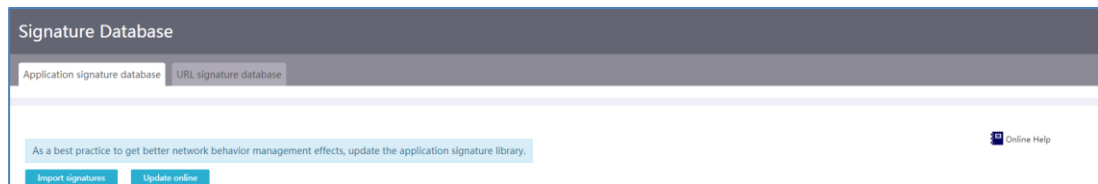
制限事項およびガイドライン

- シグニチャデータベースを更新する前に、ライセンスがインストールされ、有効であることを確認します。
- デバイスの空きメモリが通常の状態のしきい値を下回っている場合は、シグニチャデータベースの更新を実行しないでください。実行しないと、シグニチャデータベースの更新に失敗し、ネットワークの動作管理に影響を与えます。

シグニチャのインポート

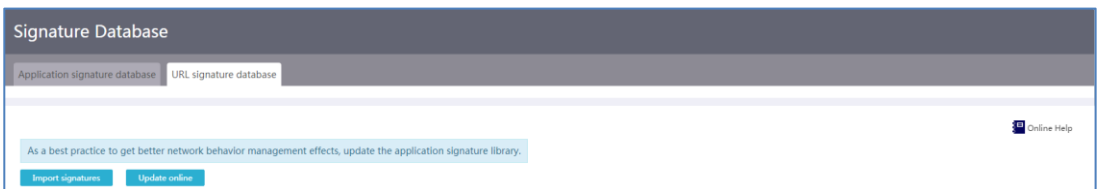
1. ナビゲーションペインで、**Network Behaviors > Signature Database**を選択します。

図54 アプリケーションシグニチャデータベース



2. **Application signature database**タブまたは**URL signature database**タブで、**Import signatures**をクリックします。
3. 開いたページで、シグニチャファイルを選択します。
4. **Apply**をクリックします。

図55 URLシグニチャデータベース



シグニチャデータベースをオンラインで更新する

制限事項およびガイドライン

オンラインシグニチャデータベースの更新を成功させるには、デバイスがDNSを介して公式Webサイト

のドメイン名をIPアドレスに解決できることを確認します。

手順

1. ナビゲーションペインで、**Network Behaviors > Signature Database**を選択します。
2. **Application signature database**タブまたは**URL signature database**タブで、**Update online**をクリックします。

監査ログ

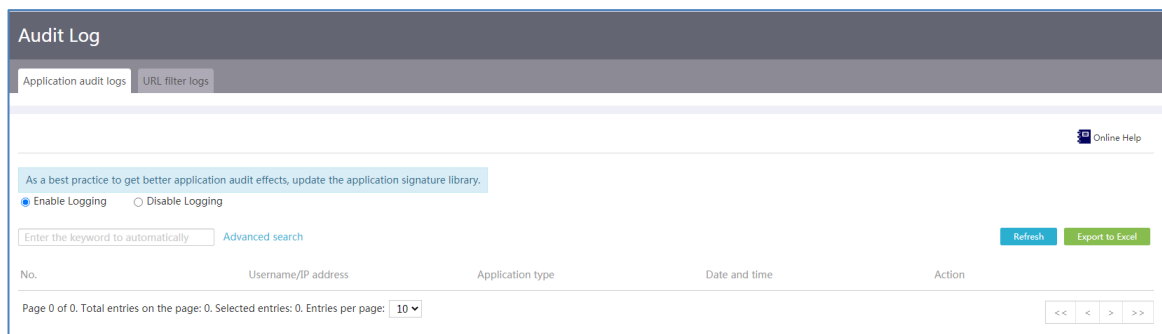
監査ログの概要

監査ログ機能を使用すると、アプリケーション制御およびURL制御機能に対して生成されたログを表示できます。ログは、ネットワーク動作の監査および分析の実行に役立ちます。

アプリケーション監査ログの構成

1. ナビゲーションペインで、**Network Behaviors > Audit Log**を選択します。
2. **Application audit logs**タブで、**Enable Logging**を選択します。
3. **Application audit logs**タブでは、アプリケーション監査ログを表示できます。ログをエクスポートするには、**Export to Excel**をクリックします。

図56 アプリケーション監査ログ



URLモニターログの設定

1. ナビゲーションペインで、**Network Behaviors > Audit Log**を選択します。
2. **Application audit logs**タブで、**Enable Logging**を選択します。
3. **URL Filter Logs**タブをクリックします。
4. **URL filter logs**タブでは、URLモニターログを表示できます。ログをエクスポートするには、**Export to Excel**をクリックします。

図57 URLモニターログ



トラフィックランキング

トラフィックランキングの概要

Global controlタブでは、ユーザートラフィックランキングおよびアプリケーショントラフィックランキングをイネーブルまたはディセーブルにできます。

- ユーザートラフィックランキングが有効になっている場合は、**User traffic ranking**でユーザートラフィックデータを表示できます。
見出しページを開きます。
- アプリケーショントラフィックのランキングがイネーブルになっている場合は**Application Traffic Ranking**タブでアプリケーショントラフィックデータを見ることができます。

グローバル制御の設定

制限事項およびガイドライン

- LANサーバーを追加したら、このページでこれらのサーバーのユーザートラフィックランキングをイネーブルにする必要があります。
- ポータル構成がサーバーに存在する場合、サーバーの名前は**Global control**タブに表示されません。サーバーからポータル構成を削除すると、サーバーは**Global control**タブに表示されます。

手順

1. ナビゲーションペインで、**Network Behaviors >Traffic Ranking**を選択します。
2. **Global control** タブで、アプリケーショントラフィックのランク付けを有効にするには、**Application traffic ranking**に続いて**On**を選択します。アプリケーショントラフィックのランク付けを無効にするには、**Application traffic ranking**に続いて**Off**を選択します。
3. サーバーリストで、サーバーの**On/Off**ボタンをクリックして、サーバーの静的IPおよびDHCPユーザートラフィックランキングを無効または有効にできます。または、複数のサーバーを選択し、右上隅の**Batch enable**をクリックして、これらのサーバーの静的IPおよびDHCPユーザートラフィック

クランキングを有効にできます。また、複数のサーバーを選択し、右上隅の**Batch disable**をクリックして、これらのサーバーの静的IPおよびDHCPユーザートラフィッククランキングを無効にできます。


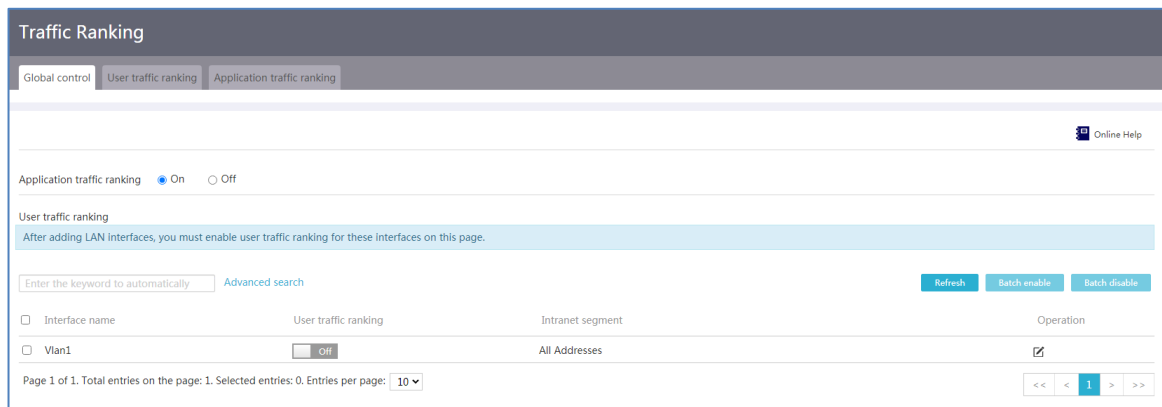
4. サーバーの**Operation**列で**Edit**アイコンをクリックします。**Add intranet segment**ページが開きます。システムは、イントラネットセグメント内のIPアドレスに対してのみトラフィック統計およびクランキングを実行します。デフォルトのイントラネットセグメントは、サーバーに直接接続されているネットワークセグメントです。ネットワーク接続を確認するには、イントラネットセグメントを正しく構成する必要があります。イントラネットセグメントが変更された場合は、速やかに編集します。
 - サーバー名には、編集中のサーバーの名前が表示されます。サーバー名は編集できません。
 - イントラネットセグメントに追加するIPアドレスを1つ設定します。
 - イントラネットセグメントに追加するIPアドレス範囲の開始IPアドレスと終了IPアドレスを設定します。
5. アイコン  をクリックして、イントラネットセグメントに設定を追加します。
6. **Apply**をクリックします。

図58 グローバル制御



ユーザートラフィッククランキングの設定

制限事項およびガイドライン

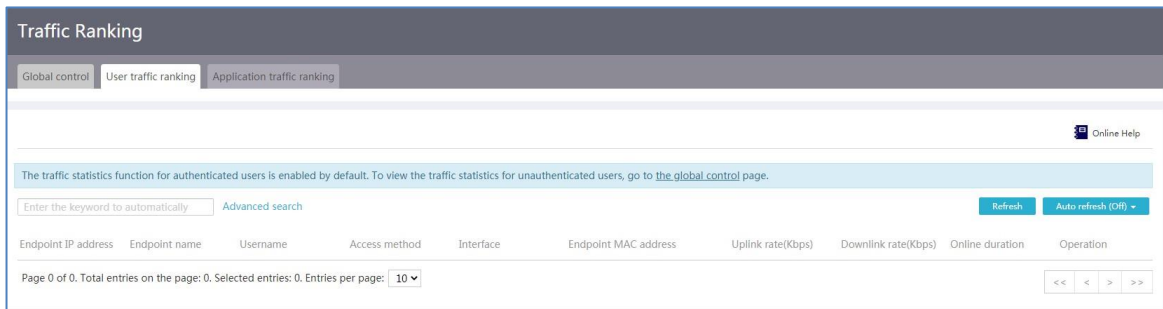
認証ユーザーのユーザートラフィッククランキング機能は常に使用可能であり、ユーザーの操作は必要ありません。非認証ユーザーのユーザートラフィッククランキング機能を表示するには、最初にグローバル制御ページで関連するサーバーのユーザートラフィッククランキング機能を使用可能にする必要があります。

手順

1. ナビゲーションペインで、**Network Behaviors > Traffic Ranking**を選択します。
2. **User traffic ranking**タブをクリックします。
3. サーバーの**Operation**カラムにある**Rate limit**アイコンをクリックします。

4. 開いたページで、アプリケーションサーバーを選択し、アップロード帯域幅とダウンロード帯域幅を設定します。
5. **Apply**をクリックして、エンドポイントレート制限の設定を完了します。
6. サーバーの**Operation**カラムにある**Details**アイコンをクリックして、ユーザートラフィックおよびその他の情報を表示する詳細ページに入ります。

図59 ユーザートラフィックランキング



アプリケーショントラフィックランキングの設定

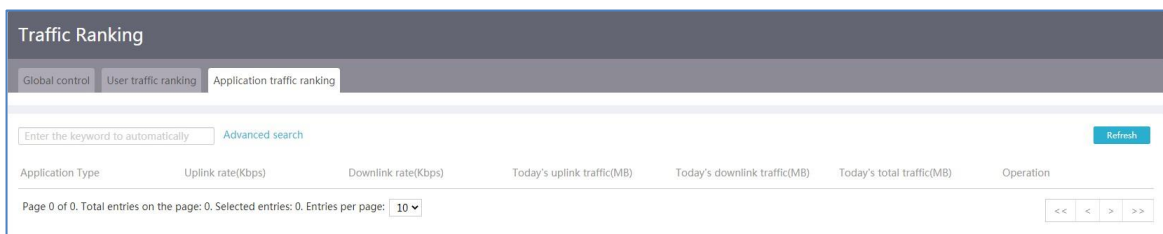
制限事項およびガイドライン

アプリケーショントラフィックランキングを設定するには、最初にグローバル制御ページでアプリケーショントラフィックランキングをイネーブルにする必要があります。

手順

1. ナビゲーションペインで、**Network Behaviors > Traffic Ranking**を選択します。
2. **Application traffic ranking**タブをクリックします。
3. アプリケーションの**Operation**列にある**Detail**アイコンをクリックして、アプリケーショントラフィックおよびその他の情報を示す詳細ページに入ります。

図60 アプリケーショントラフィックのランキング



ネットワークセキュリティ

ファイアウォール

ファイアウォール機能の概要

ファイアウォール機能は、セキュリティ規則に基づいてパケットを識別し、不正なパケットがネットワークに入るのを防ぐためのアクションを実行します。

制限事項およびガイドライン

セキュリティルールの優先度を慎重に指定します。セキュリティルールは優先度順に照合されます。一致するセキュリティルールが見つかったら、ファイアウォールはルールで指定されたアクションを実行します。

前提条件

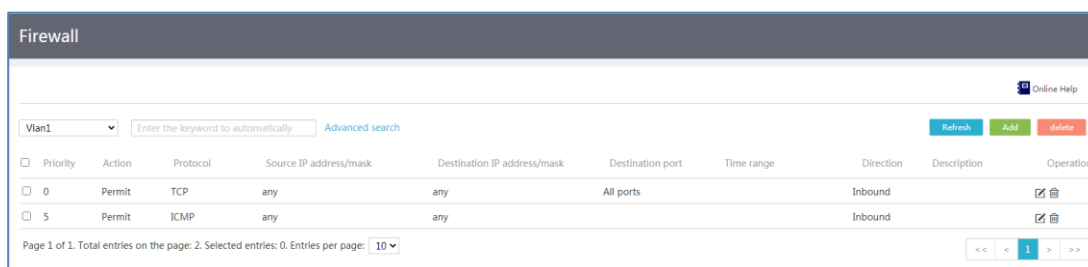
セキュリティ規則を設定する前に、次のタスクを完了します。

- WAN設定を構成します。
- セキュリティ規則に使用する時間範囲を設定します。

セキュリティの規則を追加する

1. ナビゲーションペインで、**Network Security > Firewall**を選択します。

図61 セキュリティルール



The screenshot shows the Firewall configuration interface. At the top, there is a dropdown menu for 'Vlan1' and a search bar. Below this is a table with columns: Priority, Action, Protocol, Source IP address/mask, Destination IP address/mask, Destination port, Time range, Direction, Description, and Operator. Two rules are listed: one with Priority 0, Action Permit, Protocol TCP, Source any, Destination any, and Destination port All ports; and another with Priority 5, Action Permit, Protocol ICMP, Source any, and Destination any. The table is on page 1 of 1, with 2 total entries and 0 selected entries.

Priority	Action	Protocol	Source IP address/mask	Destination IP address/mask	Destination port	Time range	Direction	Description	Operator
0	Permit	TCP	any	any	All ports		Inbound		<input type="checkbox"/> <input type="checkbox"/>
5	Permit	ICMP	any	any			Inbound		<input type="checkbox"/> <input type="checkbox"/>

2. **Add**をクリックします。
3. **Interface**フィールドで、セキュリティ規則を適用するサーバーを選択します。ファイアウォールは、この規則を使用して、サーバーに到着するパケットを照合します。
4. **Protocol**フィールドで、ターゲットパケットが使用するプロトコルを選択します。
 - トラnsポート層パケットを照合するには、**TCP**または**UDP**を選択します。
 - pingまたはtracertパケットを照合するには、**ICMP**を選択します。
 - すべてのプロトコルのパケットを照合するには、**All protocols**を選択します。
5. **Source IP address/mask**フィールドに、パケット送信者のIPアドレスとマスクを入力します。すべての送信者からのパケットを照合するには、**any**を入力します。

6. **Destination IP address/mask**フィールドに、目的の packets レシーバのIPアドレスとマスクを入力します。すべてのレシーバ宛ての packets を一致させるには、**any**を入力します。
7. **Destination port**フィールドに、ターゲット packets の宛先ポート番号を入力します。たとえば、HTTP packets の場合は80です。
8. **Time range**フィールドで、ルールを有効にする時間範囲を選択します。
9. **Action**フィールドで、ターゲット packets に対して実行するアクションを選択します。
10. **Priority**フィールドで、次のいずれかのタスクを実行します。
 - ルールに優先度を割り当てるには、**Auto**を選択します。ルール構成の順序に従って、ルールに優先度が割り当てられます。優先度の番号付けステップは5です。
 - 優先度の値を入力するには、**User-defined**を選択します。値が小さいほど優先度が高くなります。
11. **Description**フィールドに、規則の説明を入力します。
12. **Apply**をクリックします。

図62 セキュリティルールの追加

The screenshot shows the 'Add Firewall Rule' dialog box with the following configuration:

- Interface: Vlan1
- Protocol: TCP
- Source IP address/mask: 192.168.1.10/255.255.255.0
- Destination IP address/mask: 192.168.2.30/255.255.255.0
- Destination port: 30 (range: 0-65535)
- Time range: Choose...
- Action: Permit, Deny
- Priority: Auto, User-defined (range: 0-65534)
- Description: (1-127 chars)

Buttons: Apply, Cancel

攻撃防御

攻撃防御概要

DDoS攻撃はインターネット上で一般的であり、従来のDoS攻撃よりも大きな被害を引き起こす可能性が

あります。この機能により、次の種類の攻撃からデバイスとネットワークを保護できます。

- **Single-packet attacks:** 攻撃者は、不正な形式のパケットを使用してターゲットシステムを麻痺させます。たとえば、LAND攻撃では、ターゲットシステムのIPアドレスがTCPパケットの送信元IPアドレスと宛先IPアドレスの両方として使用されます。攻撃者は、これらのパケットを送信してターゲットシステムの接続リソースを枯渇させ、ターゲットシステムが通常のサービス処理できないようにします。
- **Abnormal flow attacks:** 異常なフロー攻撃には、次のタイプの攻撃が含まれます。
 - **Scanning attacks:** 攻撃者は、ターゲットネットワークに侵入する方法を見つけるために、ホストアドレスとポートをスキャンしてターゲットネットワークポロジをプローブし、ポートを開きます。
 - **Flood attacks:** 攻撃者は、ターゲットシステムに大量の偽造要求を送信します。システムは、これらの偽造要求に応答するのに忙しすぎて、正当なユーザーにサービスを提供できません。

デバイスは、次のDDoS攻撃の防止をサポートしています。

- **Single-packet attacks:** Fraggle攻撃、LAND攻撃、WinNuke攻撃、TCPフラグ攻撃、ICMP到達不能パケット攻撃、ICMPリダイレクトパケット攻撃、Smurf攻撃、IPソースルート攻撃、IPLレコードルート攻撃、および大規模ICMPパケット攻撃。
- **Abnormal flow attacks:** スキャン攻撃、SYNフラッド攻撃、UDPフラッド攻撃、およびICMPフラッド攻撃。

攻撃防御の設定

1. ナビゲーションペインで、**Network Security > Attack Defense**を選択します。
2. **Attack Defense**タブで、**Add**をクリックします。

図63 攻撃防御



3. 開いたページで、次のように攻撃防御を設定します。
 - **Interface**リストから、攻撃防御設定が適用されるサーバーを選択します。
 - 単一パケット攻撃に対する攻撃防御をイネーブルにします。

ベストプラクティスとして、すべてのタイプの単一パケット攻撃に対して攻撃防御をイネーブルにします。

- 異常なフロー攻撃に対する攻撃防御をイネーブルにします。

スキャン攻撃防御を有効にした後、パケットの送信元IPアドレスをブラックリストに追加することを選択できます。デバイスは、一致する送信元IPアドレスを持つパケットをドロップします。ブラックリストに追加されたIPアドレスを表示するには、**Blacklist Management**ページにアクセスします。

ベストプラクティスとして、ネットワークトラフィックタイプに基づいてフラッド攻撃防御をイネーブルにします。

4. **Apply**をクリックします。

図64 攻撃防御設定エントリーの追加

The screenshot shows a dialog box titled "Add Attack Defense Configuration". At the top right is a close button (X). Below the title bar, there is a field for "Interface" with a dropdown menu currently showing "WAN0(GE0)". The dialog is divided into two main sections: "Single-packet attack defense" and "Abnormal flow attack defense".

Single-packet attack defense:

- Fraggle attack defense
- Land attack defense
- WinNuke attack defense
- TCP flag attack defense
- ICMP destination unreachable message attack defense
- ICMP redirect message attack defense
- Smurf attack defense
- Source routing option attack defense
- Record route option attack defense
- Large ICMP packet attack defense

Abnormal flow attack defense:

- Scanning attack defense
 - Source IP address join the Blacklist
- SYN flood attack defense
- UDP flood attack defense
- ICMP flood attack defense

At the bottom of the dialog, there are two buttons: "Apply" (green) and "Cancel" (red).

攻撃防御統計

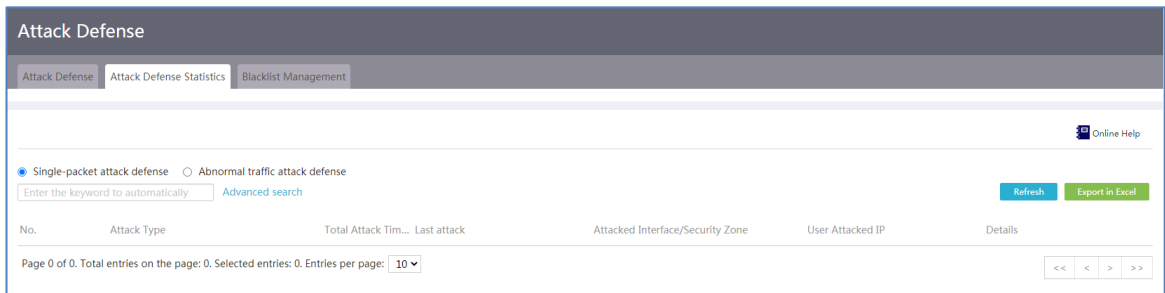
はじめに

この機能を使用して、攻撃タイプ、合計攻撃時間、最後の攻撃が発生した時間、攻撃されたサーバー/セキュリティゾーン、およびユーザーが攻撃したIPなど、デバイスに対するDDoS攻撃の詳細を表示します。

手順

1. ナビゲーションペインで、**Network Security > Attack Defense**を選択します。
2. **Attack Defense Statistics**タブをクリックします。
3. 単一パケット攻撃に関する統計情報を表示するには、**Single-packet attack defense**を選択します。
4. 異常なフロー攻撃に関する統計情報を表示するには、**Abnormal traffic attack defense**をクリックします。
5. 統計情報をエクスポートするには、**Export in Excel**をクリックします。

図65 攻撃防御統計



ブラックリスト管理

はじめに

スキャン攻撃防御を有効にした後、送信元IPアドレスをブラックリストに追加できます。デバイスは、一致する送信元IPアドレスを持つパケットをドロップします。

ブラックリストに追加されたIPアドレスを表示するには、**Blacklist Management**ページにナビゲートします。このページには、ブラックリストに追加されたIPアドレス、MACアドレス、タイプおよびアクションなど、ブラックリストに関する情報が記録されます。

手順

1. ナビゲーションペインで、**Network Security > Attack Defense**を選択します。
2. **Blacklist Management**タブをクリックします。
3. ブラックリストからIPアドレスを削除するには、IPアドレスの**Action**カラムにある削除アイコンをクリックします。

図66 ブラックリスト管理



接続制限

接続制限の概要

接続制限を使用してIPごとの接続を制限し、リソース割り当てと攻撃防止を向上させます。IPアドレスからのTCP接続またはUDP接続の数が接続制限を超えると、接続数が接続制限を下回るまで、そのIPアドレスからの接続は許可されません。

次の接続制限を設定できます。

- **Network connection limits:** IPアドレス範囲内の各IPアドレスからの接続数を制限します。この制限方法は、1つのIPアドレスからすべてのサーバーで受信される接続の合計数を制限するために使用されます。
- **VLAN-based network connection limits:** VLANサーバー上の各IPアドレスからの接続数を制限します。この制限方法は、1つのIPアドレスから1つのVLANサーバー上で受信される接続数を制限するために使用されます。

ネットワーク接続の制限を構成する

1. ナビゲーションペインで、**Network Security > Connection Limit**を選択します。
2. **Connection Limits**タブで、**Enable Network Connection Limit**を選択します。

図67 ネットワーク接続制限ルール



3. **Add**をクリックします。**Add Connection Limit Rule**ページが開きます。
4. **Start IP address**フィールドに開始IPアドレスを入力します。
5. **End IP address**フィールドに終了IPアドレスを入力します。
6. **Per-IP connection upper limit**フィールドに、各IPアドレスを送信元とするTCP接続とUDP接続の合計最大数を入力します。
送信元IPアドレスは同じでも、送信元ポート番号、宛先IPアドレス、宛先ポート番号、またはプロトコルタイプが異なる接続は、別の接続と見なされます。
7. IPアドレスごとにTCP接続を制限するには**Per-IP TCP connection upper limit**フィールドにTCP接続の最大数を入力します。
TCP接続の最大数は、TCP接続とUDP接続の合計最大数以下である必要があります。
8. IPアドレスごとにUDP接続を制限するには、**Per-IP UDP connection upper limit**フィールドにUDP接続の最大数を入力します。
UDP接続の最大数は、TCP接続とUDP接続の合計最大数以下である必要があります。
9. **Description**フィールドにルールの説明を入力します。
10. **Apply**をクリックします。

図68 ネットワーク接続制限ルールの追加/編集

VLANベースのネットワーク接続制限の設定

1. ナビゲーションペインで、**Network Security > Connection Limit**を選択します。
2. **VLAN-based Network Connection Limits**タブをクリックします。

図69 VLANベースのネットワーク接続の制限



3. **Add**をクリックします。**Add VLAN-based Connection Limits Rule**ページが開きます。
4. **VLAN Interface**リストからVLANサーバーを選択します。
5. **Enable Connection Limit**を選択します。
6. **IP Max Connection Limit**フィールドに、各IPアドレスを送信元とするTCPおよびUDP接続の最大合計数を入力します。

送信元IPアドレスは同じでも、送信元ポート番号、宛先IPアドレス、宛先ポート番号、またはプロトコルタイプが異なる接続は、別の接続と見なされます。

7. IPアドレスごとにTCP接続を制限するには**TCP Max Connection Limit**フィールドにTCP接続の最大数を入力します。

TCP接続の最大数は、TCP接続とUDP接続の合計最大数以下である必要があります。

8. IPアドレスごとにUDP接続を制限するには、**UDP Max Connection Limit**フィールドにUDP接続の最大数を入力します。

UDP接続の最大数は、TCP接続とUDP接続の合計最大数以下である必要があります。

9. **Description**フィールドにルールの説明を入力します。

10. **Apply**をクリックします。

図70 VLANベースのネットワーク接続制限ルールの追加

Add VLAN-based Connection Limits Rule ✕

VLAN Interface *

Enable Connection Limit

IP Max Connection Limit * (Range:2-10000,recommend 1000-2000)

TCP Max Connection Limit (Range:2-10000,recommend 1000-2000)

UDP Max Connection Limit (Range:2-10000,recommend 1000-2000)

Description ? (1-127 chars)

MACアドレスモニター

MACアドレスモニターの概要

特定のデバイスから送信されるパケットを許可または拒否する場合は、デバイスに接続するレイヤー3サーバーにMACアドレスモニターを設定できます。

MACアドレスモニターは、特定のMACアドレスを送信元とするパケットをモニタリングします。

- ホワイトリストがイネーブルの場合、デバイスは、ホワイトリストのMACアドレスから送信されたパケットだけを許可します。
- ブラックリストがイネーブルの場合、デバイスはブラックリストに記載されたMACアドレスから送信されたパケットだけをドロップします。

MACアドレスモニターを設定する

制限事項およびガイドライン

管理エンドポイントに接続するサーバーでホワイトリストMACアドレスモニターをイネーブルにする場合は、管理エンドポイントのMACアドレスがすでにホワイトリストに追加されていることを確認します。

手順

1. ナビゲーションペインで、**Network Security > MAC Address Filter**を選択します。
2. この機能をイネーブルにするサーバーのモニタリング方式として、**Whitelist**または**Blacklist**を選択し、**Enable**をクリックします。
3. **Apply**をクリックします。

図71 MACモニターの設定

MAC Address Filter

MAC Filter Setting | MAC Black and White List Management

Online Help

Please make sure that the MAC address of the management terminal is added to the white list.

Interface: Vlan1 | Filter Method: Please Select | Enable And Disable: Enable Disable

Page 1 of 1. Total entries on the page: 1. Selected entries: 0. Entries per page: 10

Apply

ホワイトリストまたはブラックリストのエントリーを追加する

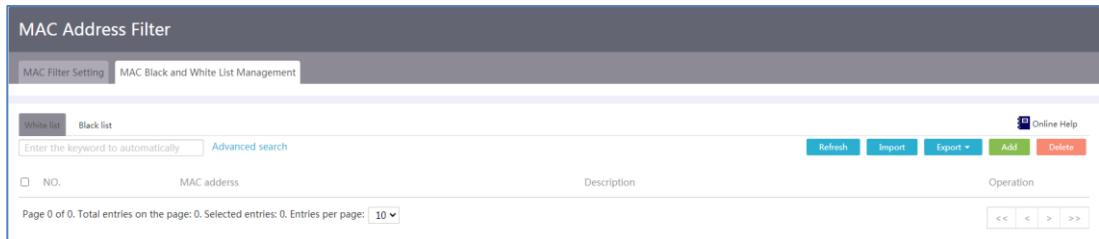
制限とガイドライン

MACアドレスホワイトリストとブラックリストの設定手順は類似しています。次の手順では、例としてMACアドレスホワイトリストの設定について説明します。

手順

1. ナビゲーションペインで、**Network Security > MAC Address Filter**を選択します。
2. **MAC Black and White List Management**タブをクリックします。
3. **White list**タブでは、MACアドレスをホワイトリストに追加できます。

図72 MACブラックリストおよびホワイトリスト



4. **Add**をクリックします。
5. 表示されたページで、ホワイトリストに追加するMACアドレスを入力します。
6. **Apply**をクリックします。

図73 ホワイトリストへのMACアドレスの追加

ホワイトリストまたはブラックリストのエントリーの一括追加

制限事項およびガイドライン

MACアドレスホワイトリストとブラックリストの設定手順は類似しています。次の手順では、例としてMACアドレスホワイトリストの設定について説明します。

手順

1. ナビゲーションペインで、**Network Security > MAC Address Filter**を選択します。
2. **MAC Black and White List Management**タブをクリックします。

3. **White list**タブでは、MACアドレスをホワイトリストに追加できます。
4. ホワイトリストの右上で、**Export > Export template**をクリックします。
5. ダウンロードしたテンプレートを開き、MACアドレスを追加して、ファイルを保存します。
6. ページで、**Import**をクリックします。
7. 開いたページで、**Choose File**をクリックし、前に編集したファイルを選択します。
8. **Apply**をクリックします。

ホワイトリストまたはブラックリストの編集

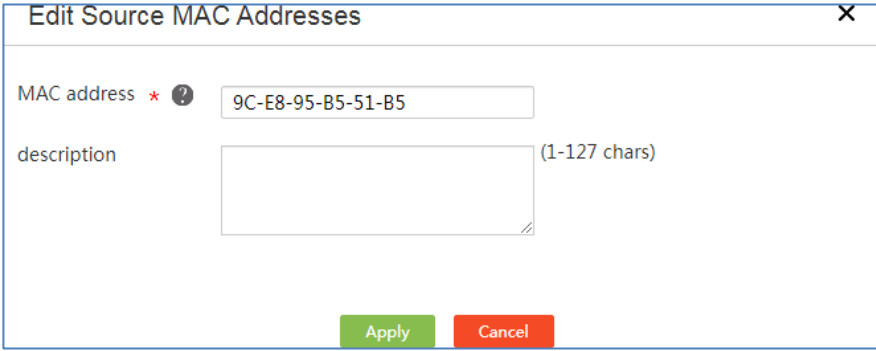
制限事項およびガイドライン

MACアドレスホワイトリストとブラックリストの設定手順は類似しています。次の手順では、例としてMACアドレスホワイトリストの設定について説明します。

手順

1. ナビゲーションペインで、**Network Security > MAC Address Filter**を選択します。
2. **MAC Black and White List Management**タブをクリックします。
3. **White list**タブでは、MACアドレスをホワイトリストに追加できます。
4. MACアドレスエントリーの**Edit**アイコンをクリックします。
5. 表示されたページで、新しいMACアドレスを指定し、**Apply**をクリックします。

図74 送信元MACアドレスの編集



The screenshot shows a dialog box titled "Edit Source MAC Addresses". It has a close button (X) in the top right corner. The dialog contains two input fields: "MAC address" with a red asterisk and a help icon, containing the value "9C-E8-95-B5-51-B5"; and "description" with a character count "(1-127 chars)". At the bottom, there are two buttons: "Apply" (green) and "Cancel" (red).

ARP攻撃からの保護

ARP攻撃からの保護の概要

ARPは本質的に脆弱です。攻撃者は、ARPの脆弱性を不正利用してネットワークデバイスを攻撃する可能性があります。デバイスは、LAN内のARP攻撃とウイルスを検出して防止するために、複数の

ARP攻撃保護機能を提供します。

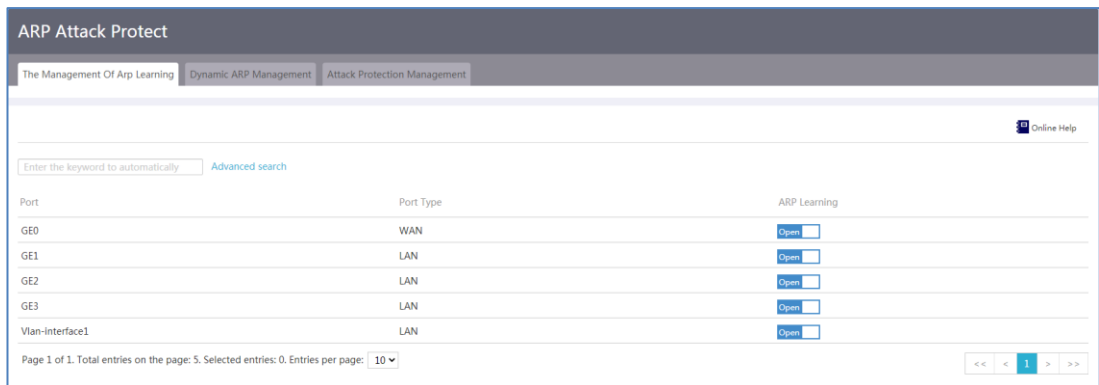
ARP攻撃からの保護には、次の機能があります。

- **Dynamic ARP learning:** モニター毎にダイナミックARPラーニングのイネーブル化ステータスを制御します。
ダイナミックARPラーニングがサーバーでディセーブルになっている場合、サーバーはダイナミックARPエントリーを学習できません。セキュリティを向上させるために、サーバーがすべての有効なホストのARPエントリーをすでに学習している場合は、ダイナミックARPラーニングをディセーブルにできます。
- **Dynamic ARP management:** ダイナミックARPエントリーマネジメント、ARPスキャン、および固定ARPが含まれます。
 - **Dynamic ARP entry management:** ダイナミックARPエントリーをリフレッシュ、追加、または削除できます。
 - **ARP scanning :**この機能は、LAN内の有効なホストのダイナミックARPエントリーを作成します。
 - **Fixed ARP :**この機能は、ダイナミックARPエントリーをスタティックARPエントリーに変換します。
ARPスキャンは通常、小規模で安定したネットワーク上で固定ARPとともに使用されます。デバイスが不正なARPエントリーを学習しないようにするには、ARPスキャンと固定ARPの両方が実行された後で、ダイナミックARP学習をディセーブルにします。
- **Attack protection management:** スタティックARPエントリーマネジメント、および外部ネットワークへのユーザーアクセスの制御が含まれます。
 - **Static ARP entry management:** スタティックARPエントリーのリフレッシュ、追加、削除、バッチインポート、またはバッチエクスポートを実行できます。
 - **Control of user access to the external network:** 不正な内部ユーザーによる外部ネットワークへの攻撃を防止するために、デバイスにスタティックARPエントリーがあるユーザーだけに外部ネットワークへのアクセスを許可するように選択できます。この設定を行う前に、まずARPスキャンと固定ARPを実行します。

ダイナミックARPラーニングの設定

1. ナビゲーションペインで、**Network Security > ARP Attack Protect**を選択します。
2. **Management Of Arp Learning**タブで、ダイナミックARPラーニングのイネーブルステータスを設定します。
 - ダイナミックARPラーニングをイネーブルにするには、**Open**をクリックします。
 - ダイナミックARPラーニングを無効にするには、**Close**をクリックします。

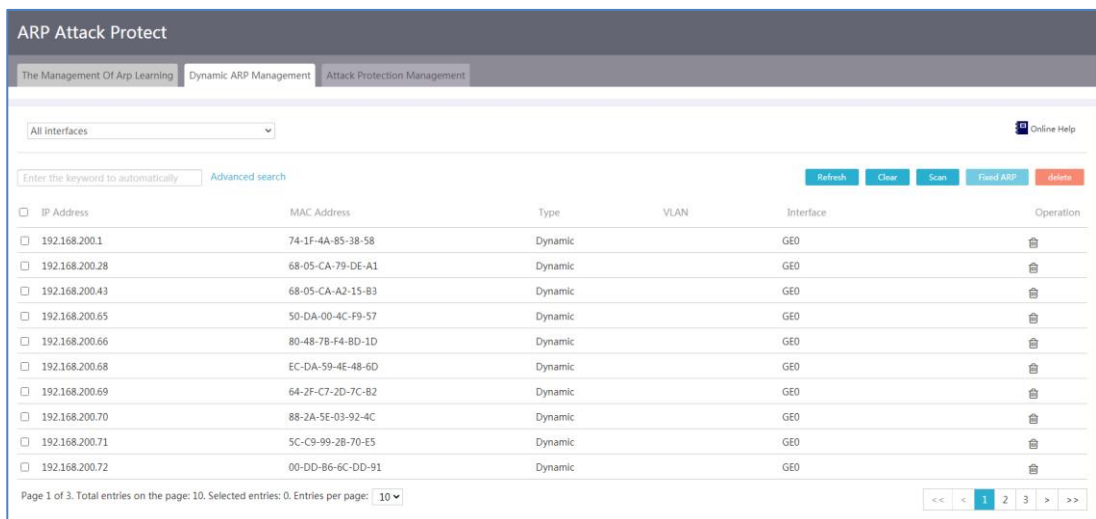
図75 ダイナミックARPラーニング



ダイナミックARP管理を設定する

1. ナビゲーションペインで、**Network Security > ARP Attack Protect**を選択します。
2. **Dynamic ARP Management**タブをクリックします。
3. 既存のダイナミックARエントリーに対して、次のいずれかのタスクを実行します。
 - 既存のARPエントリーを更新するには、**Refresh**をクリックします。
 - 既存のARPエントリーをすべて削除するには、**Clear**をクリックします。
 - 特定のダイナミックARPエントリーを削除するには、ダイナミックARPエントリーを選択し、**delete**をクリックして、**Yes**をクリックします。

図76 ダイナミックARP管理



4. ARPスキャンと固定ARPを実行します。
 - a. **Scan**をクリックします。
 - b. **Interface**リストからサーバーを選択します。

- c. 表示されたページの**Start Ipv4Address**フィールドと**End Ipv4Address**フィールドに、それぞれ開始IPv4アドレスと終了IPv4アドレスを入力します。IPアドレス範囲がサーバーと同じネットワークセグメント上にあることを確認します。
- d. **IP addresses already in existing ARP entries are also scanned**を選択します。
- e. ダイナミックARPエントリーをスタティックARPエントリーに変換するには、ダイナミックARPエントリーを選択し、**Fixed ARP**をクリックします。

図77 スキャン

攻撃防御管理の設定

制限事項およびガイドライン

デバイスへのログインに使用するホストのARPエントリーがスタティックARPエントリーであることを確認します。

前提条件

スタティックARPエントリーを一括して追加するには、スタティックARPエントリーをファイルに保存し、ローカルファイルからデバイスに一括インポートする必要があります。

スタティックARPエントリーを一括して正しくインポートするには、まず既存のスタティックARPエントリーをファイルにエクスポートします。このファイルはテンプレートファイルとして使用でき、必要に応じてスタティックARPエントリーを編集できます。

手順

1. ナビゲーションペインで、**Network Security > Attack Protect**を選択します。
2. **Attack Protection Management**タブをクリックします。
3. 外部ネットワークへのユーザーアクセスを制御します。
 - デバイスにスタティックARPエントリーがあるユーザーだけに外部ネットワークへのアクセスを許可するには、**Allow only users with static ARP entries to access the external**

networkを選択します。

- すべてのユーザーに外部ネットワークへのアクセスを許可するには、**Unlimited access**を選択します。
4. スタティックARPエントリーに対して、次のいずれかのタスクを実行します。
- スタティックARPエントリーを更新するには、**Refresh**をクリックします。
 - スタティックARPエントリーを一括してインポートするには、**Import**をクリックします。
 - スタティックARPエントリーをまとめてエクスポートするには、**Export**をクリックします。
 - スタティックARPエントリーを追加するには、**Add**をクリックします。表示されたページで、スタティックARPエントリーのIPアドレスとMACアドレスを入力します。
 - 特定のスタティックARPエントリーを削除するには、static ARP entriesを選択し、**Delete**をクリックして**Yes**をクリックします。

図78 攻撃防御管理

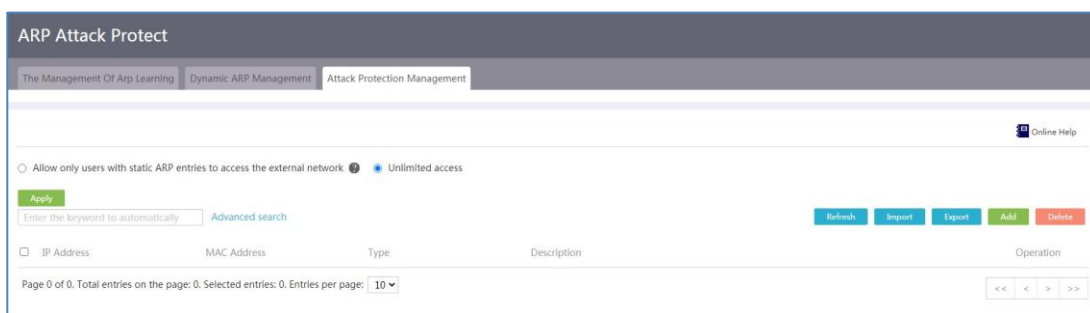


図79 ARPエントリーの追加

New ARP Entry

IP address * 192.168.1.100

MAC address * 9c-e8-95-b5-51-b5 (Format: HH-HH-HH-HH-HH-HH)

Description (case-sensitive, 1-255 chars)

Apply Cancel

認証管理

ポータル認証

ポータル認証の概要

ポータルは、ネットワークへのユーザーアクセスを制御するためにユーザーのIDを認証します。ユーザーは、ポータル認証を通過した後、ネットワークリソースにアクセスできます。デバイスは、次のタイプのポータル認証をサポートします。

- **Web page authentication:** ユーザーはWebブラウザを介してポータル認証を開始します。デバイスは、ユーザーが認証ページに入力したユーザー名とパスワードを使用してユーザーを認証します。
- **WeChat client recognition:** ユーザーは、ユーザーがフォローしているWeChat公式アカウントによって提供されるネットワーク接続リンクをクリックすることによって、ポータル認証を開始する。

どちらのポータル認証タイプでも、認証クライアントソフトウェアをインストールする必要はありません。

ポータル認証なしで特定のユーザーが指定されたネットワークリソースにアクセスできるようにするには、ポータルフリールールを構成できます。ポータルフリールールに一致する項目には、ユーザーのMACアドレス、IPアドレスまたはホスト名が含まれます。

Webページ認証用の認証ページを構成する

前提条件

ポータルユーザーに接続されているサーバーのIPアドレスを設定します。

バックグラウンドイメージとして使用するイメージを、デバイスへのログインに使用するクライアント上の **background-logon.jpg** という名前のローカルファイルとして、ポータル認証ページに保存します。イメージの解像度が1440x900で、サイズが255 Kであることを確認します。

手順

1. ナビゲーションペインで、**Authentication > Portal Authentication**を選択します。
2. **Web page authentication**を選択します。
3. **Enabling Web authentication service**を選択します。ポータル認証を構成するには、Web認証サービスを使用可能にする必要があります。
 - **Session timeout**フィールドにセッションタイムアウト時間を設定します。ユーザーのオンライン時間がこの値を超えると、デバイスはユーザーをログアウトします。
 - **Authentication service interface**リストから、ポータル認証を使用可能にするサーバーを選択します。選択したサーバーには、IPアドレスが構成されている必要があります。
 - **Language of Authentication**ページフィールドで言語を選択します。オプションには**English**または**Chinese**が含まれます。
この例では、**English**が使用されています。
4. パスワードの変更を許可するかどうかを決定します。ポータルユーザーがログインパスワードを変更できるようにするには、**Allow password change**オプションを選択します。
5. **Window title**フィールドにウィンドウタイトルを入力します。たとえば、**Welcome to Portal Authentication Page**などです。

6. **Window prompt information**フィールドに、ウィンドウプロンプト情報を入力します。次に例を示します。
xxx companyです。
7. **Import background images**フィールドの横にある**Choose File**をクリックし、認証ページでバックグラウンドイメージとして使用するイメージファイルを選択します。
8. **Submit**をクリックします。
9. **Preview**をクリックします。構成済の認証ページが表示されます。

図80 Webページ認証の設定

WeChatクライアント認識用の認証ページを設定する

前提条件

ポータルユーザーに接続されているサーバーのIPアドレスを設定します。

ポータル認証ページでバックグラウンドイメージとして使用するイメージを、デバイスへのログインに使用するクライアント上の**guanzhu.jpg**という名前のローカルファイルとして保存します。イメージの解像度が422×251で、サイズが47 Kであることを確認します。

手順

1. ナビゲーションペインで、**Authentication > Portal Authentication**を選択します。
2. **WeChat client recognition**を選択します。
3. **Enabling Web authentication service**を選択します。ポータル認証を構成するには、Web認証サービスを使用可能にする必要があります。
 - **Session timeout**フィールドにセッションタイムアウト時間を設定します。ユーザーのオンライ

ン時間がこの値を超えると、デバイスはユーザーをログアウトします。

- **Authentication service interface**リストから、ポータル認証を使用可能にするサーバーを選択します。選択したサーバーには、IPアドレスが構成されている必要があります。
4. **Window title**フィールドにウィンドウタイトルを入力します。たとえば、**Welcome to Portal Authentication Page**などです。
 5. **Window prompt information**フィールドに、ウィンドウプロンプト情報を入力します。次に例を示します。
xxx companyです。
 6. **Import background images**フィールドの横にある**Choose File**をクリックし、認証ページでバックグラウンドイメージとして使用するイメージファイルを選択します。
 7. **WeChat DNS**フィールドに、WeChat公式アカウントに設定されているデバイスのドメイン名を入力します。デバイスのドメイン名に使用できるのは、文字、数字、ハイフン(-)、アンダースコア(_)、およびドット(.)だけです。また、ドメイン名の先頭にドット(.)を使用することはできません。
 8. **Submit**をクリックします。
 9. **Preview**をクリックします。構成済みの認証ページが表示されます。

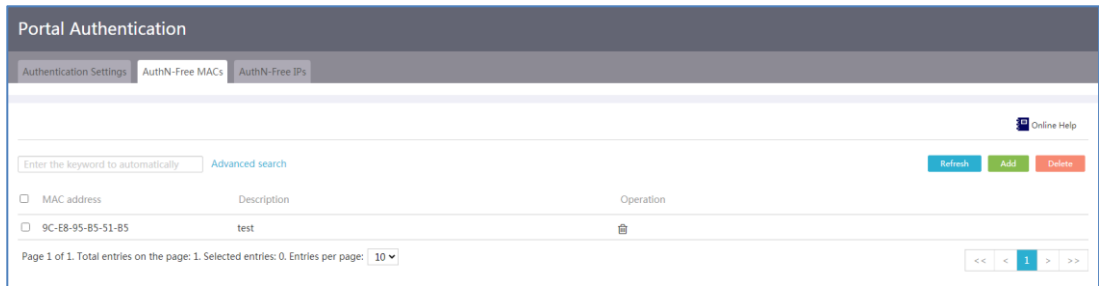
図81 WeChatクライアントの認識設定

The screenshot shows the 'Portal Authentication' configuration page. The 'Authentication Settings' tab is active. Under 'WeChat client recognition', the 'Enabling Web authentication service' checkbox is checked. The 'Session timeout' is set to 100 minutes. The 'Authentication service interface' is set to 'Vlan1'. The 'Window title' is 'test'. The 'Window prompt information' field is empty. The 'Import background images' section shows a 'Choose File' button and 'No file chosen'. The 'WeChat DNS' field is empty. At the bottom, there are 'Submit' and 'Preview' buttons.

認証不要MACアドレスを追加する

1. ナビゲーションペインで、**Authentication > Portal Authentication**を選択します。
2. **AuthN-Free MACs**タブをクリックします。

図82 認証不要MACアドレス設定ページ



3. **Add**をクリックします。
4. 表示されたページで、**MAC address**フィールドにMACアドレスを入力します。
5. **Description**フィールドに、認証不要MACアドレスの説明を入力します。
6. **Apply**をクリックします。

図83 認証不要MACアドレスの追加

MAC address * 9c-e8-95-b5-51-b5
(Format: HH-HH-HH-HH-HH-HH)

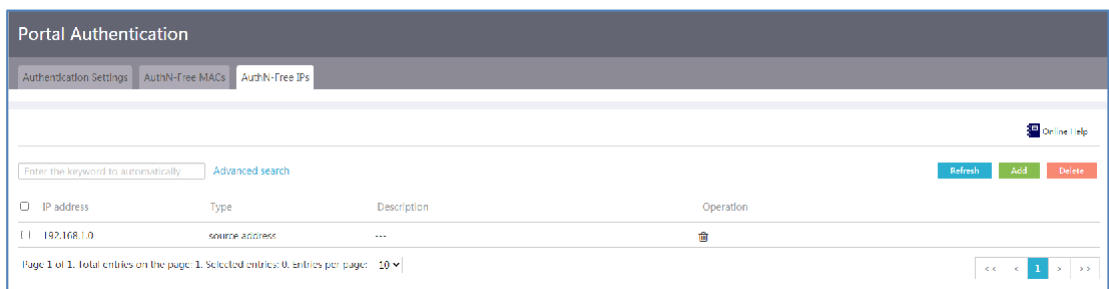
Description (1-255 chars)

Apply Cancel

認証不要IPアドレスまたはホスト名を追加する

1. ナビゲーションペインで、**Authentication > Portal Authentication**を選択します。
2. **AuthN-Free IPs**タブをクリックします。

図84 認証不要のIPアドレスまたはホスト名の設定ページ



3. **Add**をクリックします。

- 表示されたページで、**Address add mode**リストからアドレスタイプを選択します。サポートされるオプションには、**Source address**、**Destination address**および**Hostname**があります。
 - Source address**または**Destination address**を選択した場合は**IP Address**フィールドにIPアドレスとマスクを入力します。
 - Hostname**を選択した場合は、**Hostname**フィールドにホスト名を入力します。
- Description**フィールドに、認証不要IPアドレスまたはホスト名の説明を入力します。
- Apply**をクリックします。

図85 認証不要IPアドレスの追加

The screenshot shows a dialog box titled "Add no authentication address" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- Address add mode ***: A dropdown menu with "Source address" selected.
- IP Address: ***: Two input fields, the first containing "192.168.1.10" and the second containing "24".
- Description**: A text area with a "(1-255 character)" label to its right.
- At the bottom, there are two buttons: a green "Apply" button and a red "Cancel" button.

PPPoEサーバー

このタスクについて

IPアドレスを割り当て、ダイヤルアップユーザーの認証を実行できるPPPoEブロードバンドダイヤルアップサービスを提供するには、PPPoEサーバーを設定します。

制限事項およびガイドライン

この項の設定が完了すると、デバイスはPPPoEサーバーとして動作し、IPアドレスを割り当て、ダイヤルアップユーザーの認証を実行します。ダイヤルアップユーザーにインターネットアクセスサービスを提供するには、PPPoEサーバーの設定に加えて、WANの設定も行う必要があります。WANの設定を行うには、**Fast Configuration**ページまたは**Network > WAN Settings**ページにアクセスします。

手順

- ナビゲーションペインで、**Authentication > PPPoE Server**を選択します。

図86 PPPoEサーバー

PPPoE Server

Online Help

Enter the keyword to automatically Advanced search Refresh Add Delete

PPPoE Server	Interface	VT Interface Address/Mask	DNS1	DNS2	Operation
<input type="checkbox"/> Enabled	Vlan-interface1	192.168.1.20/255.255.255.0	192.168.1.20		

Page 1 of 1. Total entries on the page: 1. Selected entries: 0. Entries per page: 10

2. **Add**をクリックします。PPPoEサーバーを追加するためのページが開きます。
3. **Apply to**フィールドで、PPPoEダイヤルアップサービスの提供に使用するデバイスサーバーを選択します。
4. **VT interface address**フィールドに、VTサーバーのIPアドレスを入力して、PPPoEサーバーがIPアドレスを割り当てることができるようにします。
5. **Subnet Mask**フィールドに、VTサーバーIPアドレスのサブネットマスクを入力します。
6. **User address pool**フィールドに、PPPoEダイヤルアップユーザーに割り当てるIPアドレスを入力します。
7. **DNS1**フィールドに、PPPoEダイヤルアップユーザーのプライマリDNSサーバーのIPv4アドレスを入力します。
8. **DNS2**フィールドで、PPPoEダイヤルアップユーザーのセカンダリDNSサーバーのIPv4アドレスを指定します。
9. **Max. endpoints allowed on the server**フィールドに、インターネットアクセスのためのダイヤルアップを許可するユーザーの最大数を入力します。
10. **Apply**をクリックして、PPPoEサービスをイネーブルにします。

図87 PPPoEサーバーの追加

Add PPPoE Server

Apply to: Vlan-interface1

VT interface address *: 192.168.1.100

Subnet Mask *: 255.255.255.0

User address pool *: 192.168.1.101-192.168.1.200
This field can be a single address or an address range (for example, 192.168.1.100-192.168.1.200).

DNS1: 192.168.1.100

DNS2:

Max. endpoints allowed on the server: (1-65534,100 by default)

Note: Please add users of the PPP service type on the user management page.

Apply Cancel

ユーザー管理

このタスクについて

ユーザー管理を使用して、デバイスを介して外部ネットワークにアクセスするユーザーのユーザーカウントを管理します。ユーザーカウント情報には、ユーザー資格証明(ユーザー名とパスワード)およびネットワークサービス情報(使用可能なサービスと有効期間を含む)が含まれます。アイデンティティ認証(ポータル認証やPPPoE認証など)中に、デバイスはユーザーカウント情報を使用してユーザーを認証します。ユーザーカウント情報がユーザー管理モジュール内の情報と一致するユーザーのみが、アイデンティティ認証を通過して外部ネットワークにアクセスできます。

ユーザーカウントを追加する

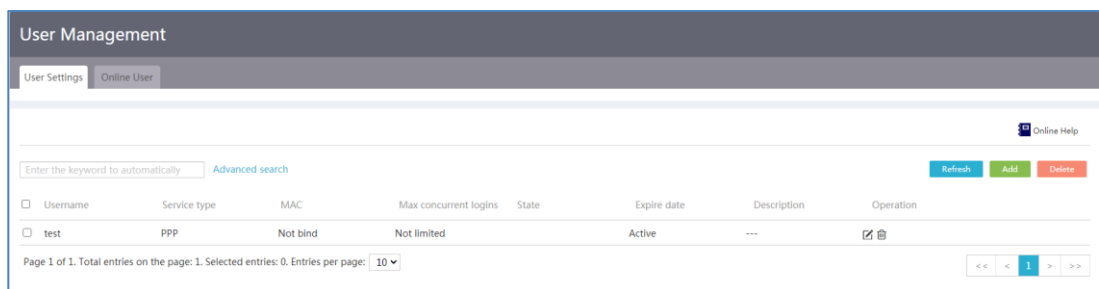
前提条件

ユーザーカウントとMACのバインドによってこのユーザーカウントを特定のホストにバインドするには、最初にホスト上のNICのMACアドレスを取得する必要があります。

手順

1. ナビゲーションペインで、**Authentication > User Management**を選択します。
2. **User Settings**タブで、**Add**をクリックします。

図88 ユーザー設定



3. 表示されたダイアログボックスで、**Username**フィールドにユーザー名を入力します。
4. **State**フィールドで、ユーザーカウントのステータスを設定します。
 - このアカウントを使用するユーザーがネットワークサービスを要求できるようにするには、**Active**を選択します。
 - ユーザーがこのアカウントを使用してネットワークサービスを要求できないようにするには、**Blocked**を選択します。このユーザーカウントを一時的に有効にしない場合は、このステータスを選択します。
5. **Password**フィールドに、パスワードを入力します。

パスワードを構成しない場合、システムはユーザーID認証にパスワードを必要としません。セキュ

リティを強化するためのベストプラクティスとして、ユーザーカウントのパスワードを構成します。

6. **Service type**フィールドで、ユーザーカウントのサービスを選択します。
7. **MAC**フィールドで、ユーザーカウントをMACアドレスにバインドするかどうかを選択します。

- ユーザーカウントをMACアドレスにバインドするには、**Bind**を選択し、xx-xx-xx-xx-xx-xxの形式でMACアドレスを入力します。

認証中、デバイスは指定されたMACアドレスを、このアカウントを使用するユーザーの実際のMACアドレスと照合します。2つのMACアドレスが一致しない場合、ユーザーは認証に失敗します。

- ユーザーカウントをMACアドレスにバインドしない場合は、**Not bind**を選択します。
ユーザーは、このユーザーカウントを使用して、任意のエンドポイントからこのデバイスを介して外部ネットワークにアクセスできます。

8. **Max concurrent logins**フィールドで、このアカウントを使用できる同時ユーザーの最大数を設定します。

制限を設定しない場合、デバイスは、このアカウントを使用する同時ユーザー数を制限しません。

9. **ExpireDate**フィールドで、ユーザーカウントの有効期間を設定します。
このユーザーカウントを使用するユーザーは、有効期間内にのみ認証を通過できます。

10. **Description**フィールドで、ユーザーカウントの説明を設定します。
ユーザーカウントを簡単に覚えて管理できるように、各ユーザーカウントの説明を設定します。

11. **Apply**をクリックします。

図89 ユーザーの追加

Add User

Username * (1-55 chars)

State Active Blocked

Password * (1-63 chars)

Service type * Portal PPP

MAC Not bind Bind

Max concurrent logins (1-1024)

ExpireDate Not set Set

Description (1-127 chars)

Apply Cancel

ユーザーアカウントを削除する

制限事項およびガイドライン

ユーザーアカウントを削除しても、このアカウントを使用するオンラインユーザーはログアウトされません。削除操作では、新しいユーザーがこのアカウントを使用してオンラインになることのみが禁止されます。

手順

1. ナビゲーションペインで、**Authentication > User Management**を選択します。
2. ユーザーアカウントの**Operation**列にある**Delete**アイコンをクリックします。
3. 表示されたダイアログボックスで、**Yes**をクリックします。

図90 ユーザーの削除

Confirm

Are you sure you want to delete the selected item(s)?

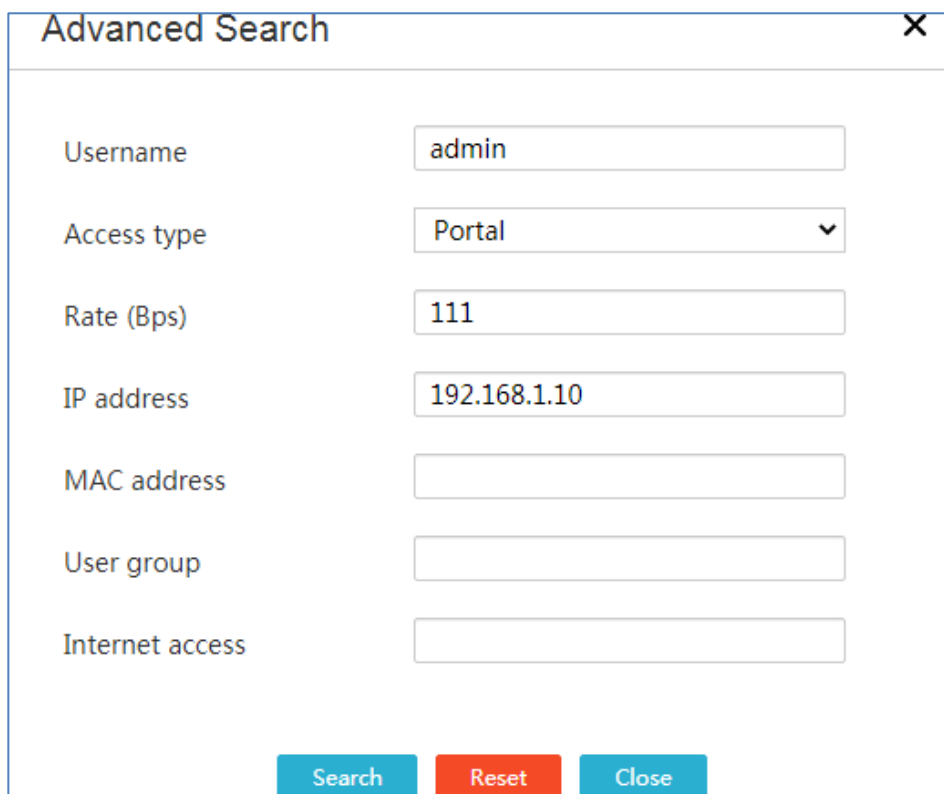
Yes No

オンラインユーザーの表示

手順

1. ナビゲーションペインで、**Authentication > User Management**を選択します。
2. **Online User**タブでは、オンラインユーザーを表示できます。
3. **Advanced search**をクリックします。表示されたダイアログボックスで、モニター条件を構成し**Search**をクリックします。

図91 高度な検索



Field	Value
Username	admin
Access type	Portal
Rate (Bps)	111
IP address	192.168.1.10
MAC address	
User group	
Internet access	

仮想ネットワーク

IPsec VPN

IPsec VPNの概要

IPsec VPNは、IPsecテクノロジーを使用して確立された仮想プライベートネットワークです。IPsecは、2つのエンドポイント間に確立されたセキュアチャネルでデータを送信します。このようなセキュアチャネルは、通常、IPsecトンネルと呼ばれます。

IPsecは、次のプロトコルとアルゴリズムを備えたセキュリティフレームワークです。

- 認証ヘッダー(AH)。
- Encapsulating Security Payload(ESP)。
- Internet Key Exchange(IKE)。

- 認証と暗号化のアルゴリズム。

AHおよびESPは、セキュリティサービスを提供するセキュリティプロトコルです。IKEは自動キー交換を実行します。

デバイスは、次のネットワークモードをサポートします。

- **Center-branch mode:** 企業の各ブランチゲートウェイは、エンタープライズセンターのゲートウェイへのIPsecトンネルを確立します。ブランチは、IPsecを介してエンタープライズセンターと安全に通信できます。
- **Branch-branch mode:** ブランチゲートウェイは、企業の別のブランチゲートウェイへのIPsecトンネルを確立します。ブランチ間のデータ通信は、IPsecによって保護されます。

デバイスをブランチノードとして設定する

このタスクについて

センター/ブランチネットワークでは、ブランチノードはセンターノードとIPsecトンネルを確立する必要があります。

ブランチ間ネットワークでは、ブランチノードは別のブランチノードとIPsecトンネルを確立する必要があります。

基本的なIPsec設定を構成する

1. ナビゲーションペインで、**Virtual Network > IPsec VPN**を選択します。
2. **IPsec policy**タブをクリックします。

図92 IPsecポリシー設定ページ

Name	Network mode	Interface	Local address	Peer address	Operation
a2233	Branch gateway	WAN0(GE0)	192.168.200.14	3.3.3.254	

3. **Add**をクリックします。
4. **Name**フィールドにIPsecポリシー名を入力します。
5. **Interface**フィールドから、IPsecポリシーを適用するサーバーを選択します。選択したサーバーがピアに到達できることを確認します。
6. **Branch gateway**モードを選択します。

7. **Peer gateway address**フィールドに、IPsecトンネルのリモートIPアドレスを入力します。
IPアドレスは、多くの場合、本社ゲートウェイまたは支店ゲートウェイのWANサーバードレスです。
8. デフォルトで唯一の認証方式である事前共有キーを使用します。
9. **Preshared key**フィールドに、ピアで使用される事前共有キーを入力します。事前共有キーは事前にネゴシエートされ、アドバタイズされます。
10. **IPsec protected flows**領域で、次の設定を行います。
 - a. **Protocol**リストから、IPsecトンネルで保護するプロトコルを選択します。
 - b. **Local subnet/mask**フィールドに、ローカル保護IPアドレス/マスクを入力します。
 - c. **Local port**フィールドにローカル保護ポートを入力します。
このフィールドは、保護プロトコルがTCPまたはUDPの場合にだけ設定できます。
デバイスは、送信元の保護ポートおよびIPアドレスから送信されたパケットに対してIPsecカプセル化を実行します。
 - d. **Peer subnet/mask**フィールドに、ピアで保護されたIPアドレス/マスクを入力します。
 - e. **Peer port**フィールドに、ピア保護ポートを入力します。
このフィールドは、保護プロトコルがTCPまたはUDPの場合にだけ設定できます。
デバイスは、宛先の保護ポートおよびIPアドレスから受信したIPsecパケットだけをカプセル化解除します。
 - f. **Add**アイコンをクリックします。
 - g. 前の手順を繰り返して、IPsecで保護されたフローエントリをさらに追加します。

図93 IPsecポリシーの追加

Add IPsec Policy

Add IPsec Policy

Name * a2233 (1-33 chars)

Interface * WAN0(GE0)

Network mode Branch gateway Headquarters gateway

Peer gateway address * 3.3.3.254 (Example: 1.1.1.1)

Authentication method Preshared key

Preshared key * (1-128 chars)

Protected data flows *

ID	Protocol	Local subnet/mask	Local port	Peer subnet/mask	Peer port
1	IP	3.3.3.0/255.255.255.0		3.3.3.0/255.255.255.0	

[Show advanced settings...](#)

Apply Cancel

IKE設定の構成

デフォルトのIKE設定を変更するには、次の作業を実行します。

1. **Add IPsec Policy**ページの**Show advanced settings**リンクをクリックします。
2. IKE settingsタブで、ネゴシエーションモードを選択します。オプションには**Main mode**と**Aggressive mode**があります。

アグレッシブモードはメインモードより高速ですが、アイデンティティ情報の保護は提供されません。メインモードはアイデンティティ情報の保護を提供しますが、低速です。要件に応じて適切なネゴシエーションモードを選択します。

デバイスのパブリックIPアドレスが動的に割り当てられる場合は、アグレッシブモードを選択することをお勧めします。

3. IDタイプを選択し、IKE認証の**Local ID**フィールドにローカルIDを入力します。IDタイプには、IPアドレス、FQDN、および**User-FQDN**があります。

IDタイプとローカルIDが、ピアのリモートID設定と同じであることを確認します。IKEネゴシエーションモードがメインモードの場合は、**IP address**を選択する必要があります。

4. IDタイプを選択し、IKE認証の**Remote ID**フィールドにリモートIDを入力します。IDタイプには、**IP address**、**FQDN**、および**User-FQDN**があります。

IDタイプとリモートIDが、ピアのローカルID設定と同じであることを確認します。

5. DPDをイネーブルにするかどうかを選択します。DPDはデッドピアを検出し、デバイスはデッドピアで確立されたIPsecトンネルを削除します。

ベストプラクティスとして、デバイスでDPDをイネーブルにして、IPsecトンネルの可用性の問題を迅速に検出します。

6. 推奨されたアルゴリズムの組み合わせを使用する場合は**Recommended**を選択し、IKEネゴシエーションプロセスの暗号化、認証、およびPFSアルゴリズムの組み合わせをカスタマイズする場合は**Customize**を選択します。

IPsecトンネルの2つのピアに、同じ暗号化、認証、およびPFSアルゴリズムが設定されていることを確認します。

7. **SA lifetime**フィールドにIKE SAライフタイムを入力します。ライフタイムが期限切れになると、IKEパラメータが再ネゴシエーションされます。

図94 IKEの詳細設定の構成

The screenshot shows the 'IKE settings' configuration page. It features three tabs: 'Advanced settings', 'IKE settings', and 'IPsec settings'. The 'IKE settings' tab is selected. The configuration includes the following fields and options:

- Negotiation mode:** A dropdown menu set to 'Main mode'.
- Local ID:** A dropdown menu set to 'IP address' and a text input field containing '2.2.2.2'. An example '(Example: 1.1.1.1)' is shown to the right.
- Remote ID:** A dropdown menu set to 'IP address' and a text input field containing '1.1.1.1'. An example '(Example: 1.1.1.1)' is shown to the right.
- DPD:** Radio buttons for 'Enable' (selected) and 'Disable'.
- Algorithm suite:** A dropdown menu set to 'Recommended'. A list of options is visible below: 'DES- SHA1- GROUP1 (Factory default)' and 'AES128- SHA1- GROUP2 (Windows7 default)'.
- SA lifetime:** A text input field containing '86400' and a label 'seconds (60-604800. Default: 86400.)'.

A blue button labeled 'Back to basic settings' is located at the bottom left of the configuration area.

IPsecの詳細設定を構成する

デフォルトの高度なIPsec設定を変更するには、次の作業を実行します。

1. 基本的なIPsec設定を構成し、**Show advanced settings**リンクをクリックします。
2. 表示されたページで、**IPsec settings**タブをクリックします。
3. 推奨されるセキュリティプロトコル、暗号化アルゴリズム、および認証アルゴリズムを使用する場合は**Recommended**を選択し、セキュリティプロトコル、認証アルゴリズム、暗号化アルゴリズム、カプセル化モード、およびPFSアルゴリズムをカスタマイズする場合は**Customize**を選択します。

ローカルIPsec保護ネットワークセグメントとピア保護ネットワークセグメントの両方がプライベートネットワークに属している場合は、トンネルカプセル化モードを選択することをお勧めします。

IPsecトンネルの2つのピアに、同じセキュリティプロトコル、認証アルゴリズム、暗号化アルゴリズム、カプセル化モード、およびPFSアルゴリズムが設定されていることを確認します。

4. **Time-based SA lifetime**フィールドに、IPsec再ネゴシエーションをトリガーする間隔を入力します。間隔が終了すると、IPsecパラメータが再ネゴシエーションされます。

5. **Traffic-based SA lifetime**フィールドでIPsec再ネゴシエーションをトリガーするトラフィックの量を入力します。トラフィックが設定されたトラフィック制限を超えると、IPsecパラメータが再ネゴシエーションされます。
6. **Trigger mode**フィールドで、IPsec SAネゴシエーションの**Trigger mode**を選択します。**Flow trigger**と**Long connection trigger**次のオプションがあります。
 - **Flow trigger**: 送信されるトラフィックがIPsec保護要件を満たしている場合に、IPsec SAネゴシエーションをトリガーします。
 - **Long connection trigger**: 必要なIPsec設定が完了したときに、IPsec SAネゴシエーションをトリガーします。
7. **Back to basic settings**をクリックして、**Add IPsec Policy**ページに戻ります。
8. **Apply**をクリックします。

図95 IPsecの詳細設定

デバイスをセンターノードとして設定する

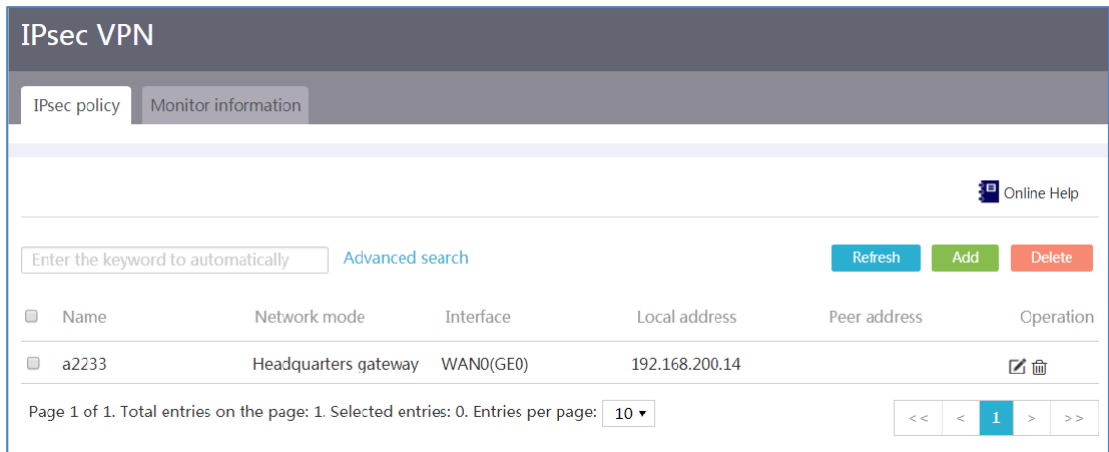
このタスクについて

センターブランチネットワークでは、センターノードはブランチノードとIPsecトンネルを確立する必要があります。

基本的なIPsec設定を構成する

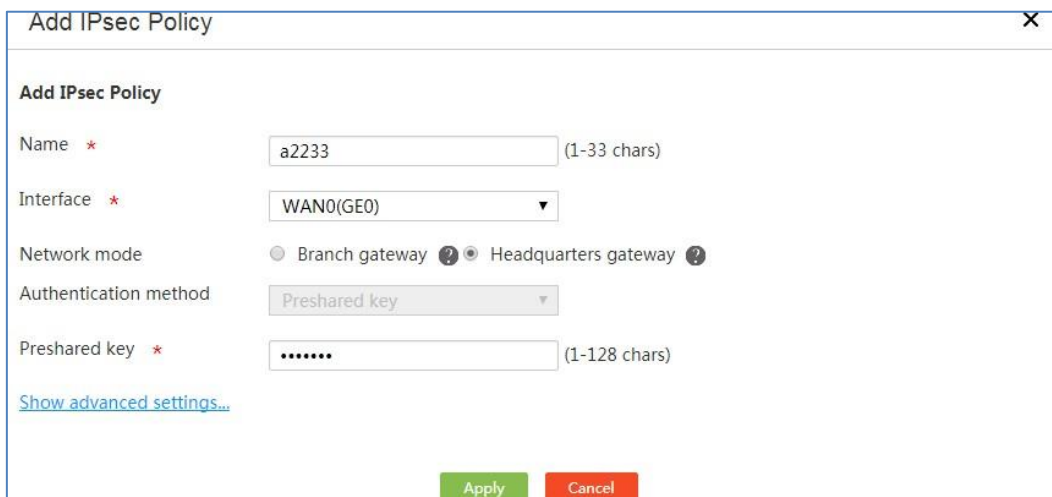
1. ナビゲーションペインで、**Virtual Network > IPsec VPN**を選択します。
2. **IPsec policy**タブをクリックします。

図96 IPsecポリシー設定ページ



3. **Add**をクリックします。
4. **Name**フィールドにIPsecポリシー名を入力します。
5. **Interface**フィールドで、IPsecポリシーを適用するサーバーを選択します。選択したサーバーがブランチに到達できることを確認します。
6. **Headquarters**ゲートウェイモードを選択します。
7. **Preshared key**認証方式を使用します。
デバイスは、事前共有キー認証方式だけをサポートします。
8. **Preshared key**フィールドに、ピアで使用される事前共有キーを入力します。事前共有キーは事前にネゴシエートされ、アドバタイズされます。

図97 IPsecポリシーの追加



IKE設定の構成

デフォルトのIKE設定を変更するには、次の作業を実行します。

1. **Add IPsec Policy**ページの**Show advanced settings**リンクをクリックします。

2. IKE settingsタブで、ネゴシエーションモードを選択します。オプションには、**Main mode**と**Aggressive mode**があります。

アグレッシブモードはメインモードより高速ですが、アイデンティティ情報の保護は提供されません。メインモードはアイデンティティ情報の保護を提供しますが、低速です。要件に応じて適切なネゴシエーションモードを選択します。

デバイスのパブリックIPアドレスが動的に割り当てられる場合は、アグレッシブモードを選択することをお勧めします。

3. IDタイプを選択し、IKE認証の**Local ID**フィールドにローカルIDを入力します。IDタイプには、**IP address**、**FQDN**、および**User-FQDN**があります。

IDタイプおよびローカルIDが、ブランチで設定されているリモートIDタイプおよびリモートIDと同じであることを確認します。

IKEネゴシエーションモードがメインモードの場合は、**IP address**を選択する必要があります。

4. DPDをイネーブルにするかどうかを選択します。DPDはデッドピアを検出し、デバイスはデッドピアのあるIPsecトンネルを削除します。

ベストプラクティスとして、デバイスのDPDをイネーブルにして、IPsecトンネルの可用性を時間内に取得します。

5. 推奨されたアルゴリズムの組み合わせを使用する場合は**Recommended**を選択し、IKEネゴシエーションプロセスの暗号化、認証、およびPFSアルゴリズムの組み合わせをカスタマイズする場合は**Customize**を選択します。

IPsecトンネルの2つのピアに、同じ暗号化、認証、およびPFSアルゴリズムが設定されていることを確認します。

6. **SA lifetime**フィールドにIKE SAライフタイムを入力します。ライフタイムが期限切れになると、IKEパラメータが再ネゴシエーションされます。

図98 IKEの詳細設定の構成

Advanced settings	IKE settings	IPsec settings
Negotiation mode	Main mode ▼	
Local ID	IP address ▼	2.2.2.2 (Example: 1.1.1.1)
DPD	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Algorithm suite	Recommended ▼ DES- SHA1- GROUP1 (Factory default) AES128- SHA1- GROUP2 (Windows7 default)	
SA lifetime	86400	seconds (60-604800. Default: 86400.)
Back to basic settings		

IPsecの詳細設定を構成する

デフォルトの高度なIPsec設定を変更するには、次の作業を実行します。

1. 基本的なIPsec設定を構成し、**Show advanced settings**リンクをクリックします。
2. 表示されたページで、IPsec settingsタブをクリックします。
3. 推奨されるセキュリティプロトコル、暗号化アルゴリズム、および認証アルゴリズムを使用する場合は**Recommended**を選択し、セキュリティプロトコル、認証アルゴリズム、暗号化アルゴリズム、カプセル化モード、およびPFSアルゴリズムをカスタマイズする場合は**Customize**を選択します。
ローカルIPsec保護ネットワークセグメントとピア保護ネットワークセグメントの両方がプライベートネットワークに属している場合は、トンネルカプセル化モードを選択することをお勧めします。
IPsecトンネルの2つのピアに、同じセキュリティプロトコル、認証アルゴリズム、暗号化アルゴリズム、カプセル化モード、およびPFSアルゴリズムが設定されていることを確認します。
4. **Time-based SA lifetime**フィールドに、IPsec再ネゴシエーションをトリガーする間隔を入力します。間隔が終了すると、IPsecパラメータが再ネゴシエーションされます。
5. **Traffic-based SA lifetime**でIPsec再ネゴシエーションをトリガーするトラフィックの量を入力します。トラフィックが設定されたトラフィック制限を超えると、IPsecパラメータが再ネゴシエーションされます。
6. **Back to basic settings**をクリックして、**Add IPsec Policy**ページに戻ります。
7. **Apply**をクリックします。

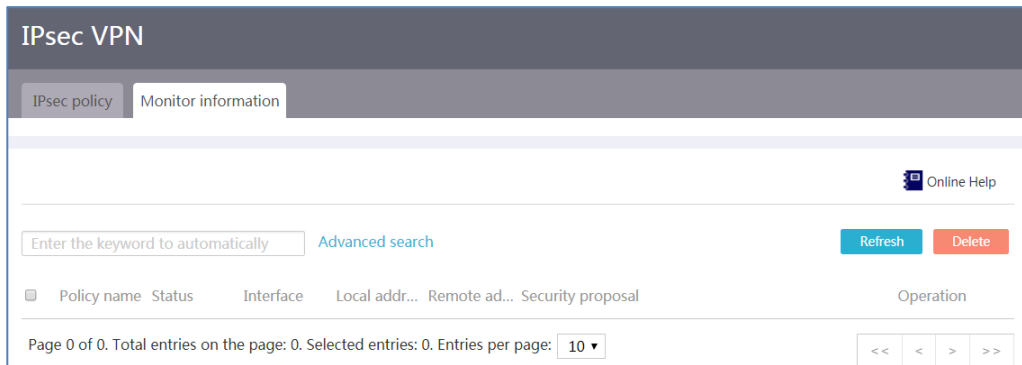
図99 IPsecの詳細設定の構成

Advanced settings	IKE settings	IPsec settings
Algorithm combination	Recommended ▼ ESP-SHA1-3DES(Recommend) ESP-SHA1-AES128 (Windows7 default) ESP-SHA1-AES256(Recommend)	
Encapsulation mode *	<input type="radio"/> Transport <input checked="" type="radio"/> Tunnel	
PFS	▼	
Time-based SA lifetime	3600	seconds (180-604800. Default: 3600)
Traffic-based SA lifetime	1843200	Kilobytes (2560-4294967295. Default: 1843200)
Back to basic settings		

モニター情報

1. ナビゲーションペインで、**Virtual Network > IPsec VPN**を選択します。
2. **Monitor information**タブをクリックします。

図100 モニター情報



L2TPサーバー

L2TPサーバーの概要

基本的なL2TPサーバーパラメータを設定し、L2TPをイネーブルにするには、次の作業を実行します。

企業のリモートユーザー(支社や出張者など)が企業の内部ネットワーク内のリソースにアクセスするための、安全でコスト効率に優れたソリューションを提供するには、L2TPサーバーを構成します。

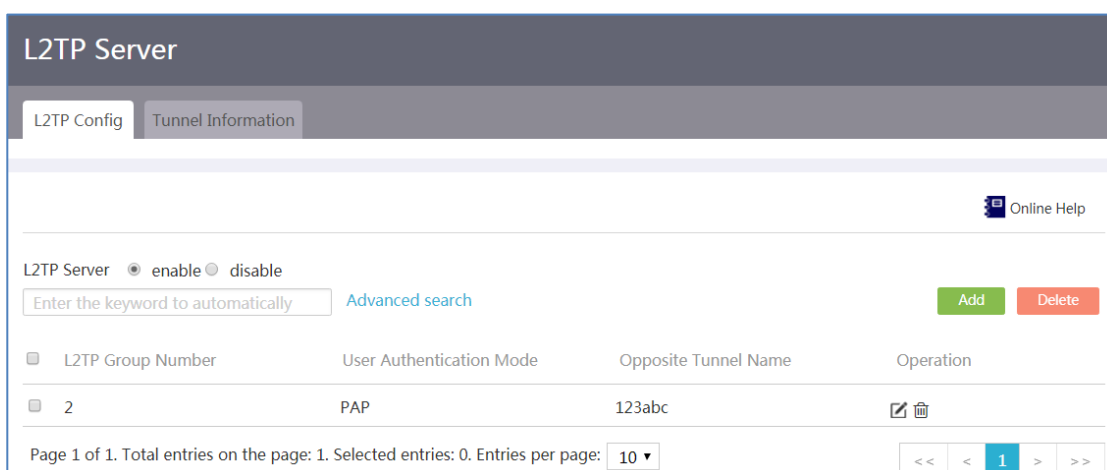
L2TPサーバーは、PPPおよびL2TPプロトコルパケットを処理できるデバイスです。通常、L2TPサーバーは企業の内部ネットワークの境界に配置されます。

L2TPサーバーを構成する

手順

1. ナビゲーションペインで、**Virtual Network > L2TP Server**を選択します。
2. **L2TP Config**タブをクリックします。
3. **L2TP Server**フィールドで**enable**を選択します。

図101 L2TPサーバー構成



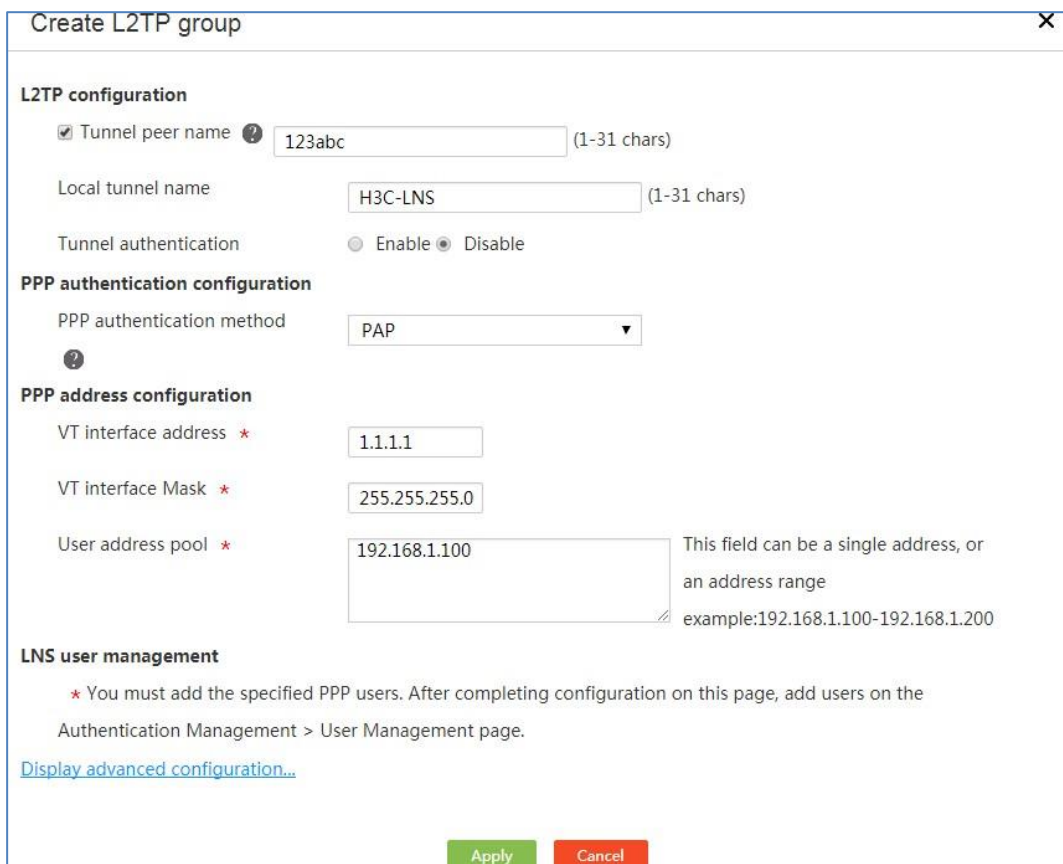
4. **Add**をクリックします。
5. **L2TP configuration**領域で、次のようにL2TPトンネルパラメータを設定します。
 - 必要に応じて、**Tunnel peer name**オプションを選択します。このオプションを選択する場合は、L2TPクライアントのトンネル名を入力します。
 - **Local tunnel name**フィールドに、L2TPサーバーのトンネル名を入力します。
 - **Tunnel authentication**パラメータで、必要に応じて**Enable**または**Disable**を選択します。
 - **Enable**を選択した場合は、**Tunnel password**フィールドにトンネルパスワードを入力します。トンネル認証機能により、セキュリティが強化されます。この機能を使用するには、L2TPサーバーとL2TPクライアントの両方でトンネル認証を有効にし、両方のパスワードが同じであることを確認する必要があります。
 - **Disable**を選択すると、L2TPサーバーとL2TPクライアントの間にトンネルを確立するための認証は実行されません。
6. **PPP authentication method**リストから、必要に応じて**None**、**PAP**、または**CHAP**を選択します。
 - **None**を選択すると、ユーザーに対して認証が実行されません。この認証方法はセキュリティが最も低いため、注意して使用してください。
 - **PAP**を選択すると、ユーザーに対して双方向ハンドシェイク認証が実行されます。この認証方式のセキュリティは中程度です。
 - **CHAP**を選択すると、ユーザーに対して3ウェイハンドシェイク認証が実行されます。この認証方式は最高のセキュリティを備えています。
7. **PPP address configuration**領域で、PPPアドレスパラメータを設定します。
 - **VT interface address**フィールドに、VTサーバーのIPアドレスを入力して、L2TPサーバーがL2TPクライアントまたはユーザーにIPアドレスを割り当てることができるようにします。
 - **VT interface Mask**フィールドに、VTサーバーのIPアドレスのサブネットマスクを入力します。
 - **User address pool**フィールドに、L2TPクライアントまたはユーザーに割り当てるIPアドレ

スを入力します。

8. **LNS user management**領域で、プロンプトに従ってPPPユーザーを追加します。
9. **Display advanced configuration**をクリックして、詳細設定領域を表示します。
10. **Advanced configuration**領域で、次のように詳細パラメータを設定します。
 - **Hello interval**フィールドに、Hello間隔を入力します。
 - **AVP hidden**フィールドで、必要に応じて**Enable**または**Disable**を選択します。
 - **Enable**を選択すると、隠しモードでAVPデータ(トンネルネゴシエーションパラメータ、セッションネゴシエーションパラメータ、およびユーザー認証情報を含む)を転送するためにトンネルパスワードが使用されます。この機能により、データ伝送のセキュリティが強化されます。
 - **Disable**を選択すると、AVPデータは非表示モードで転送されません。
 - **Flow control**フィールドで、必要に応じて**Enable**または**Disable**を選択します。
 - **Enable**を選択すると、L2TPデータパケットの送受信時に、パケットに含まれるシーケンス番号を使用して、パケットが失われたかどうかを識別され、パケットの順序が変更されます。この機能により、L2TPデータパケット転送の正確性と信頼性が向上します。この機能を有効にするには、L2TPサーバーとL2TPクライアントのいずれかでフロー制御を有効にします。
 - **Disable**を選択すると、パケットは検出されず、順序も変更されません。
 - **Mandatory CHAP authentication**フィールドで、必要に応じて**Enable**または**Disable**を選択します。
 - **Enable**を選択すると、L2TPクライアントがユーザーを認証した後、L2TPサーバーはCHAPを使用してユーザーの認証を再度実行します。この機能により、セキュリティが強化されます。必須のCHAP認証を有効にするには、PPP認証方法がCHAPIに設定されていることを確認します。
 - **Disable**を選択すると、L2TPサーバーはユーザーに対して必須のCHAP認証を実行しません。2番目のCHAP認証をサポートしていないユーザーに対しては、この機能を無効にすることをお勧めします。
 - **Mandatory LCP renegotiation**フィールドで、必要に応じて**Enable**または**Disable**を選択します。
 - **Enable**を選択すると、L2TPクライアントがユーザーを認証した後、L2TPサーバーはLCP再ネゴシエーションを使用して、ユーザーに対して再度LCPネゴシエーションと認証を実行します。この機能により、セキュリティが強化されます。必須のLCP再ネゴシエーションと必須のCHAP認証の両方を有効にすると、必須のLCP再ネゴシエーションのみが有効になります。
 - **Disable**を選択すると、L2TPサーバーはユーザーに対して必須のLCP再ネゴシエーションを実行しません。LCPネゴシエーションをサポートしていないユーザーに対しては、この機能を無効にすることをお勧めします。

11. **Apply**をクリックします。

図102 L2TPグループの作成



Create L2TP group

L2TP configuration

Tunnel peer name ? 123abc (1-31 chars)

Local tunnel name H3C-LNS (1-31 chars)

Tunnel authentication Enable Disable

PPP authentication configuration

PPP authentication method PAP

PPP address configuration

VT interface address * 1.1.1.1

VT interface Mask * 255.255.255.0

User address pool * 192.168.1.100 This field can be a single address, or an address range example:192.168.1.100-192.168.1.200

LNS user management

* You must add the specified PPP users. After completing configuration on this page, add users on the Authentication Management > User Management page.

[Display advanced configuration...](#)

Apply Cancel

L2TPグループを編集する

手順

1. ナビゲーションペインで、**Virtual Network > L2TP Server**を選択します。
2. **L2TP Config**タブをクリックします。
3. L2TPグループの**Edit**をクリックします。
4. 必要に応じてパラメータを編集し、**Apply**をクリックします。

図103 L2TPグループの編集

Modify L2TP group

L2TP configuration

Tunnel peer name ? 123abc (1-31 chars)

Local tunnel name H3C-LNS (1-31 chars)

Tunnel authentication Enable Disable

PPP authentication configuration

PPP authentication method PAP

PPP address configuration

VT interface address * 1.1.1.1

VT interface Mask * 255.255.255.0

User address pool * 192.168.1.100 This field can be a single address, or an address range example:192.168.1.100-192.168.1.200

LNS user management

* You must add the specified PPP users. After completing configuration on this page, add users on the Authentication Management > User Management page.

[Display advanced configuration...](#)

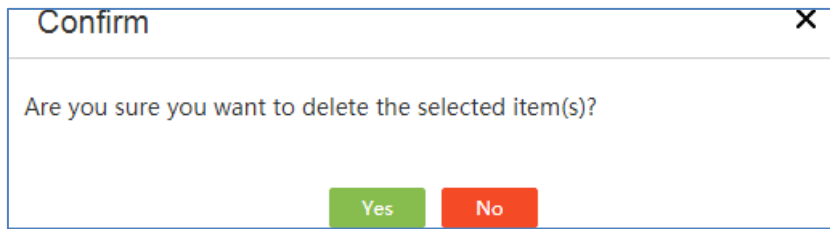
Apply Cancel

L2TPグループの削除

手順

1. ナビゲーションペインで、**Virtual Network > L2TP Server**を選択します。
2. **L2TP Config**タブをクリックします。
3. 次のいずれかのタスクを実行します。
 - L2TPグループの**Delete**をクリックします。
 - 複数のL2TPグループを選択し、**Delete**をクリックします。
4. **Yes**をクリックします。

図104 削除の確認

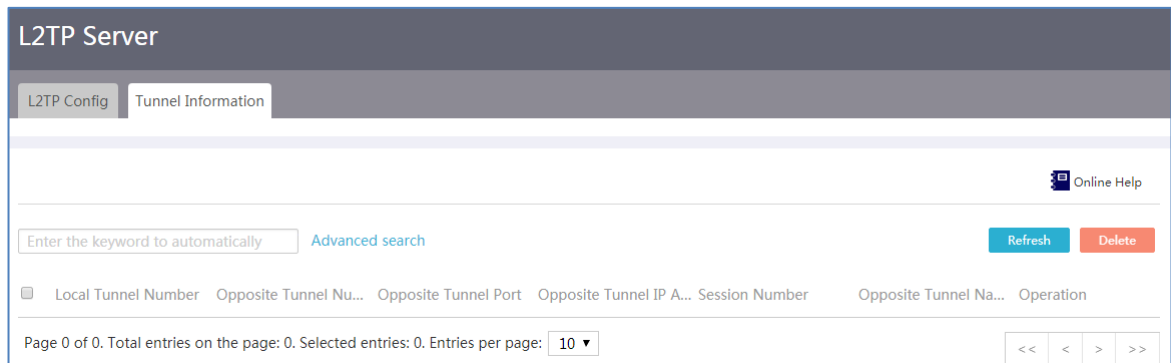


L2TPトンネルの表示

手順

1. ナビゲーションペインで、**Virtual Network > L2TP Server**を選択します。
2. **Tunnel Information**タブをクリックします。

図105 L2TPトンネル

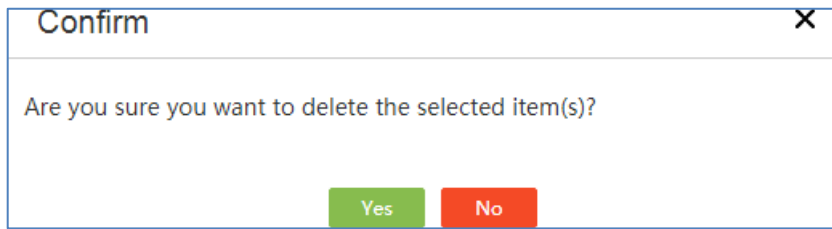


L2TPトンネルの削除

手順

1. ナビゲーションペインで、**Virtual Network > L2TP Server**を選択します。
2. **Tunnel Information**タブをクリックします。
3. 次のいずれかのタスクを実行します。
 - L2TPトンネルの**Delete**をクリックします。
 - 複数のL2TPトンネルを選択し、**Delete**をクリックします。
4. **Yes**をクリックします。

図106 削除の確認



L2TPクライアント

L2TPクライアントの概要

基本的なL2TPクライアントパラメータを設定し、L2TPをイネーブルにするには、次の作業を実行します。

企業の支店が企業の内部ネットワーク内のリソースにアクセスするための安全でコスト効率に優れたソリューションを提供するには、L2TPサーバーを構成します。

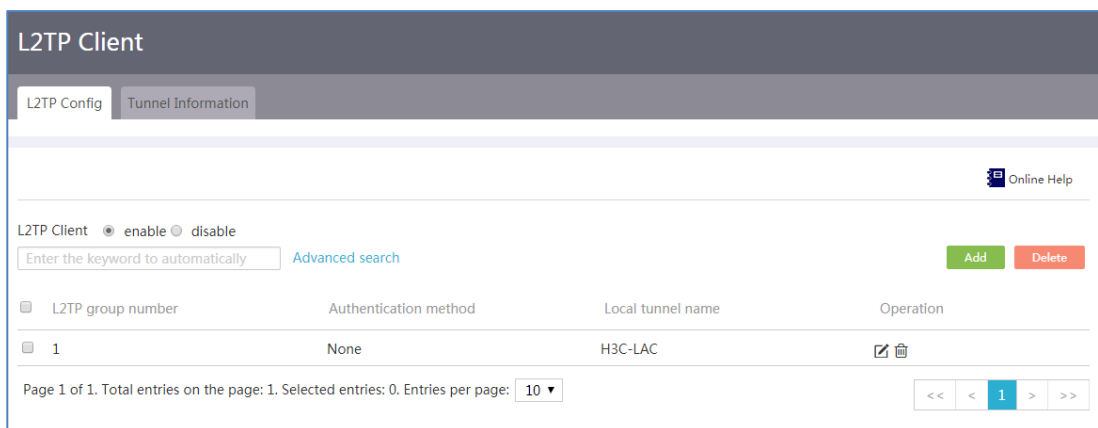
L2TPクライアントは、PPPおよびL2TPプロトコルパケットを処理できるデバイスです。通常、L2TPクライアントは企業の支店の出口に配置されます。

L2TPクライアントを設定する

手順

1. ナビゲーションペインで、**Virtual Network > L2TP Client**を選択します。
2. **L2TP Config**タブをクリックします。
3. L2TPを有効にするには、**L2TP Client**フィールドで**enable**を選択します。

図107 L2TPクライアント構成



4. **Add**をクリックします。
5. **L2TP configuration**領域で、次のようにL2TPトンネルパラメータを設定します。

- **Local tunnel name**フィールドに、L2TPクライアントのトンネル名を入力します。
 - **Address assignment method**フィールドで、必要に応じてStaticまたはDynamicを選択します。
 - **Static**を選択した場合は、**Static IP address**フィールドで仮想PPPモニターのIPアドレスを手動で設定する必要があります。
 - **Dynamic**を選択した場合、LNSは仮想PPPモニターにIPアドレスを動的に割り当てます。
 - **Tunnel authentication**パラメータで、必要に応じて**Enable**または**Disable**を選択します。
 - **Enable**を選択した場合は、**Tunnel password**フィールドに認証パスワードを入力します。トンネル認証機能により、セキュリティが強化されます。この機能を使用するには、L2TPサーバーとL2TPクライアントの両方でトンネル認証を有効にし、両方のパスワードが同じであることを確認する必要があります。
 - **Disable**を選択すると、L2TPサーバーとL2TPクライアントの間にトンネルを確立するための認証は実行されません。
6. **PPP authentication method**リストから、必要に応じて**None**、**PAP**、または**CHAP**を選択します。
- **None**を選択すると、ユーザーに対して認証が実行されません。この認証方法はセキュリティが最も低いため、注意して使用してください。
 - **PAP**を選択すると、ユーザーに対して双方向ハンドシェイク認証が実行されます。この認証方式のセキュリティは中程度です。
 - **CHAP**を選択すると、ユーザーに対して3ウェイハンドシェイク認証が実行されます。この認証方式は最高のセキュリティを備えています。
7. **L2TP server configuration**領域の**L2TP server address**フィールドに、L2TPサーバーのIPアドレスを入力します。
8. **Advanced configuration**領域で、次のように詳細パラメータを設定します。
- **Hello interval**フィールドに、**Hello**間隔を入力します。
 - AVP hiddenフィールドで、必要に応じて**Enable**または**Disable**を選択します。
 - **Enable**を選択すると、トンネル認証パスワードを使用して、AVPデータ(トンネルネゴシエーションパラメータ、セッションネゴシエーションパラメータ、およびユーザー認証情報を含む)が非表示モードで転送されます。この機能により、データ伝送のセキュリティが強化されます。
 - **Disable**を選択すると、AVPデータは非表示モードで転送されません。
 - **Flow control**フィールドで、必要に応じて**Enable**または**Disable**を選択します。
 - **Enable**を選択すると、L2TPデータパケットの送受信時に、パケットに含まれるシーケンス番号を使用して、パケットが失われたかどうかを識別され、パケットの順序が変更されません。この機能により、L2TPデータパケット転送の正確性と信頼性が向上します。この機能を有効にするには、L2TPサーバーとL2TPクライアントのいずれかでフロー制御を有効にします。
 - **Disable**を選択すると、パケットは検出されず、順序も変更されません。

9. **Apply**をクリックします。

図108 L2TPグループの作成

Create L2TP group

L2TP configuration

Local tunnel name (1-31 chars)

Address assignment method Static Dynamic

Static IP address

Tunnel authentication Enable Disable

PPP authentication configuration

PPP authentication method

L2TP server configuration

L2TP server address * (Comma-separated list of 1 to 5 IP addresses or host names)

Advanced configuration

Hello interval seconds (60 to 1000, and 60 by default)

AVP hidden Enable Disable

Flow Control Enable Disable

L2TPグループを編集する

手順

1. ナビゲーションペインで、**Virtual Network > L2TP Client**を選択します。
2. **L2TP Config**タブをクリックします。
3. L2TPグループの**Edit**をクリックします。
4. 必要に応じてパラメータを編集し、**Apply**をクリックします。

図109 L2TPグループの編集

Modify L2TP group

L2TP configuration

Local tunnel name: H3C-LAC (1-31 chars)

Address assignment method: Static Dynamic

Static IP address: 0.0.0.0

Tunnel authentication: Enable Disable

PPP authentication configuration

PPP authentication method: None

L2TP server configuration

L2TP server address *: 3.3.3.3 (Comma-separated list of 1 to 5 IP addresses or host names)

Advanced configuration

Hello interval: 60 seconds (60 to 1000, and 60 by default)

AVP hidden: Enable Disable

Flow Control: Enable Disable

Apply Cancel

L2TPグループの削除

手順

1. ナビゲーションペインで、**Virtual Network > L2TP Client**を選択します。
2. **L2TP Config**タブをクリックします。
3. 次のいずれかのタスクを実行します。
 - L2TPグループの**Delete**をクリックします。
 - 複数のL2TPグループを選択し、**Delete**をクリックします。
4. **Yes**をクリックします。

図110 削除の確認

Confirm

Are you sure you want to delete the selected item(s)?

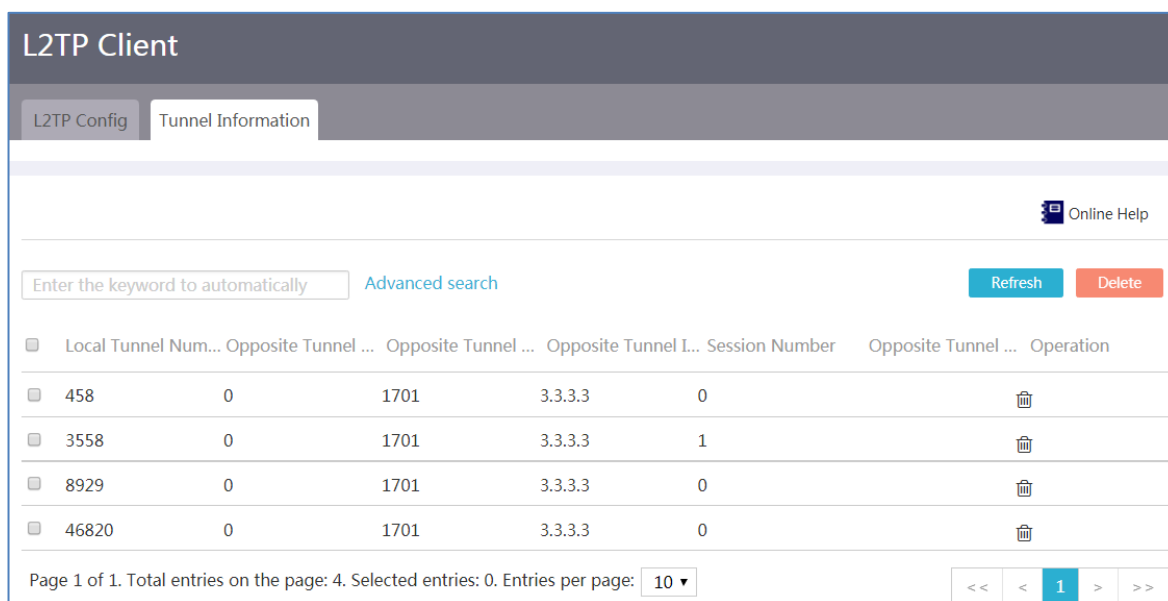
Yes No

L2TPトンネルの表示

手順

1. ナビゲーションペインで、**Virtual Network > L2TP Client**を選択します。
2. **Tunnel Information**タブをクリックします。

図111 L2TPトンネル



The screenshot shows the 'L2TP Client' interface with the 'Tunnel Information' tab selected. It features a search bar, 'Refresh' and 'Delete' buttons, and a table of tunnel entries. The table has columns for Local Tunnel Number, Opposite Tunnel Number, Opposite Tunnel IP, Opposite Tunnel ID, Session Number, and Operation. There are four entries in the table, each with a delete icon.

Local Tunnel Num...	Opposite Tunnel ...	Opposite Tunnel ...	Opposite Tunnel I...	Session Number	Opposite Tunnel ...	Operation
458	0	1701	3.3.3.3	0		
3558	0	1701	3.3.3.3	1		
8929	0	1701	3.3.3.3	0		
46820	0	1701	3.3.3.3	0		

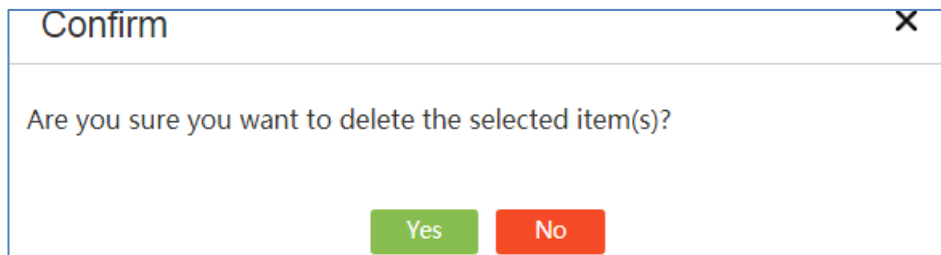
Page 1 of 1. Total entries on the page: 4. Selected entries: 0. Entries per page: 10

L2TPトンネルの削除

手順

1. ナビゲーションペインで、**Virtual Network > L2TP Client**を選択します。
2. **Tunnel Information**タブをクリックします。
3. 次のいずれかのタスクを実行します。
 - L2TPトンネルの**Delete**をクリックします。
 - 複数のL2TPトンネルを選択し、**Delete**をクリックします。
4. **Yes**をクリックします。

図112 削除の確認



EoGRE

EoGREの概要

Ethernet over GRE(EoGRE)は、イーサネットプロトコルをIPネットワーク上の仮想ポイントツーポイントトンネルにカプセル化できるトンネリングプロトコルです。イーサネットフレームは、一方のトンネルエンドでカプセル化され、もう一方のトンネルエンドでカプセル化が解除されます。

EoGREは、EoGREトンネルモードおよびEoGRE-in-UDPトンネルモードをサポートします。レイヤー2イーサネットパケットがNATトラバーサルを使用してレイヤー3ネットワークを介して転送される場合に限り、トンネルモードをEoGRE-in-UDPに設定します。NATデバイスが存在しない場合は、トンネルモードをEoGREに設定します。

EoGREトンネルを設定する

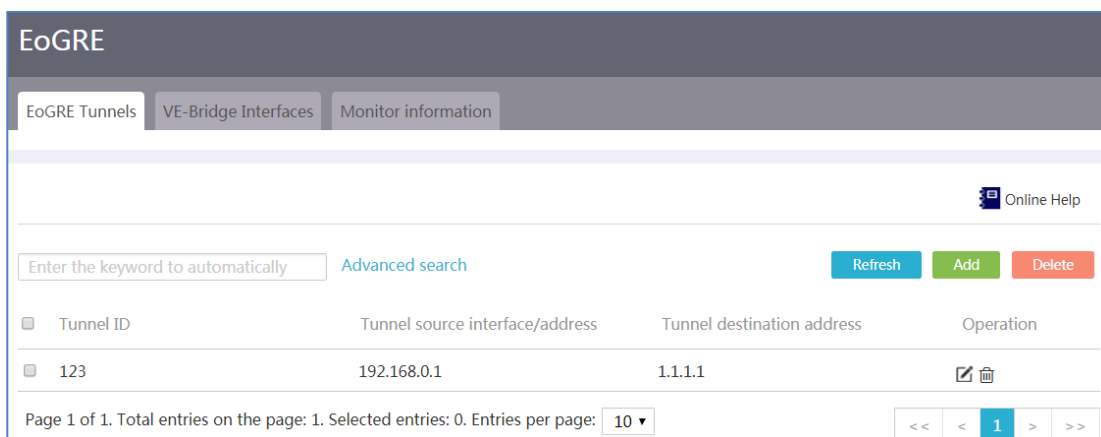
制限事項およびガイドライン

EoGREトンネルの作成時にトンネルモードを指定します。トンネルの作成後にトンネルモードを変更することはできません。

手順

1. ナビゲーションペインで、**Virtual Network > EoGRE**を選択します。
2. **EoGRE Tunnels**タブをクリックします。

図113 EoGREトンネル



3. **Add**をクリックします。
4. EoGREトンネルパラメータを設定します。
 - **Tunnel ID**フィールドに、トンネルIDを入力します。
 - **Tunnel source**フィールドで、トンネル送信元モニターを選択するか、トンネル送信元アドレスを設定します。
5. **Tunnel destination address**フィールドで、トンネルの宛先IPアドレスを設定します。
6. **Show advanced settings**をクリックして、トンネルモードを設定します。
 - トンネルモードをEoGRE-in-UDPに設定するには、**UDP encapsulation**オプションを選択します。デフォルトのUDPポート番号を使用することも、別のUDPポート番号を指定することもできます。
 - トンネルモードをEoGREに設定するには、**UDP encapsulation**オプションをクリアします。
7. **Apply**をクリックします。

図114 EoGREトンネルの追加

The screenshot shows the 'Add EoGRE Tunnel' dialog box. It has a title bar with 'Add EoGRE Tunnel' and a close button (X). The dialog contains three main fields: 'Tunnel ID' with a red asterisk, a text input field containing '123', and a range '(1-1024)'; 'Tunnel source' with a red asterisk, a radio button for 'Source interface' (selected), a dropdown menu showing 'WAN0(GE0)', a radio button for 'Source address', and a text input field containing '192.168.0.1'; and 'Tunnel destination address' with a red asterisk and a text input field containing '1.1.1.1'. Below these fields is a blue button labeled 'Show advanced settings'. At the bottom of the dialog are two buttons: 'Apply' (green) and 'Cancel' (red).

VE-Bridgeモニターを設定する

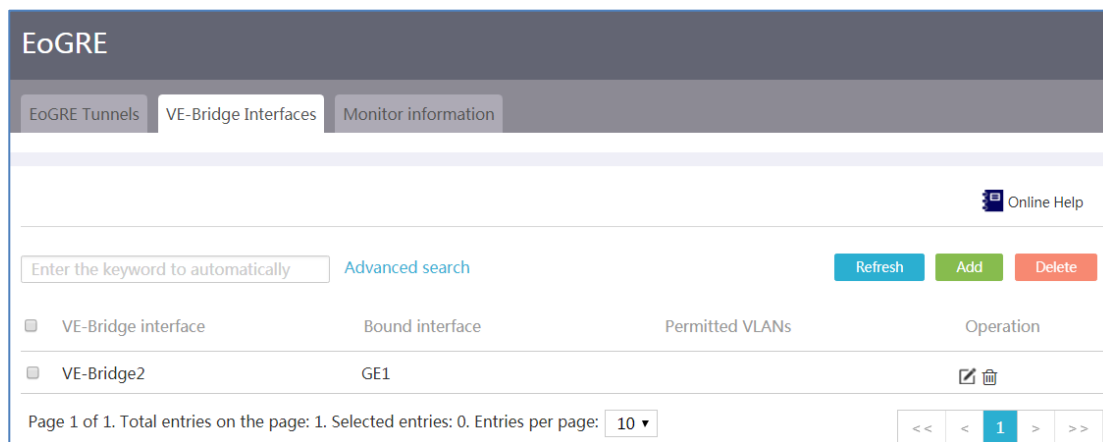
制限事項およびガイドライン

- トンネルモニターまたはGEモニターが1つのVE-Bridgeモニターにバインドされている場合、そのトンネルモニターまたはGEモニターを別のVE-Bridgeモニターにバインドできます。ただし、元のバインドは最初のVE-Bridgeモニターから自動的に削除されます。
- VE-BridgeモニターにバインドされたGEモニターは、レイヤー2転送だけを実行できます。他のサービスの設定は、GEモニターでは有効になりません。

手順

- ナビゲーションペインで、**Virtual Network > EoGRE**を選択します。
- VE-Bridge Interfaces**タブをクリックします。

図115 VE-Bridgeモニター



- Add**をクリックします。
- Interface number**フィールドに、VE-Bridgeモニターの番号を入力します。
- Default VLAN**フィールドで、VE-BridgeモニターのPVIDを設定します。
- Link type**フィールドで、リンクの種類を選択します。
 - デフォルトVLANからのトラフィックだけがモニターを通過できるようにするには、**Access**を選択します。
 - 複数のVLANからのトラフィックがモニターを通過できるようにするには、**Trunk**を選択し、許可されたVLANのIDを指定します。
- Bound interface**フィールドで、レイヤー2転送用にモニターをVE-Bridgeモニターにバインドします。
 - トンネルモニターをVE-Bridgeモニターにバインドするには、**Tunnel interface**オプションを選択し、EoGREトンネルモニターを選択します。または、**No bound interface**を選択して、トンネルモニターをVE-Bridgeモニターにバインドしないようにすることもできます。
 - レイヤー3モニターをVE-Bridgeモニターにバインドするには、**GE interface**オプションを選択し、レイヤー3モニターを選択します。または、**No bound interface**を選択して、レイヤー3

モニターをVE-Bridgeモニターにバインドしないようにすることもできます。

8. **Apply**をクリックします。

図116 VE-Bridgeモニターの追加

Add VE-Bridge Interface

Interface number * 2 (1-1023)

Default VLAN 1

Link type * Access

Permitted VLANs ? All VLANs

Bound interface * Tunnel interface Tunnel123 GE interface GE1

Apply Cancel

モニター情報を表示する

1. ナビゲーションペインで、**Virtual Network > EoGRE**を選択します。
2. **Monitor information**タブをクリックします。
3. EoGREトンネルID、ステータス、送信元モニターまたはアドレス、および宛先アドレス情報を表示します。

トンネルがアップ状態の場合は、パケットを正しく転送できます。トンネルがダウン状態の場合は、パケットを転送できません。

図117 EoGREトンネルモニター情報

EoGRE

EoGRE Tunnels VE-Bridge Interfaces Monitor information

Online Help

Enter the keyword to automatically Advanced search Refresh

Tunnel ID	Tunnel status	Tunnel source interface/address	Tunnel destination address
123	UP	192.168.0.1	1.1.1.1

Page 1 of 1. Total entries on the page: 1. Selected entries: 0. Entries per page: 10

応用設定

アプリケーションサービス

アプリケーションサービスの概要

アプリケーションサービスを使用すると、ドメインネームシステム (DNS) を構成できます。DNS は、TCP/IP アプリケーションでドメイン名を IP アドレスに変換するために使用される分散データベースです。ドメイン名から IP アドレスへのマッピングは、DNS エントリーと呼ばれます。DNS は静的または動的に設定できます。

静的DNS

静的DNS (SDNS) を使用すると、ドメイン名と IP アドレスの間のマッピングを手動で作成できます。ドメイン名を使用してサービス (Web、メール、FTP サービスなど) にアクセスする場合、システムはドメイン名にマッピングされた IP アドレスを DNS キャッシュで検索します。

ダイナミックDNS

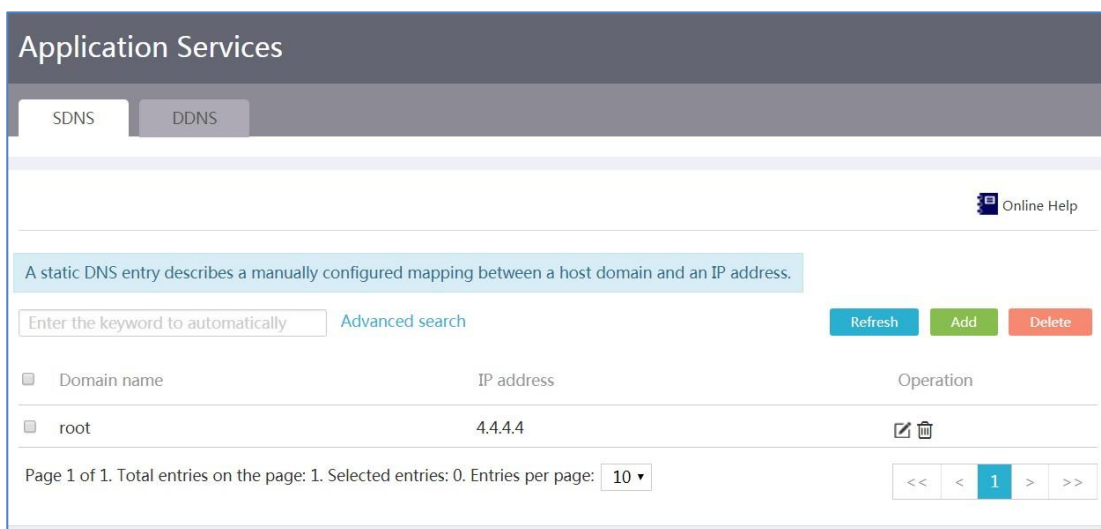
Dynamic DNS (DDNS) は、DNS サーバーのドメイン名と IP アドレス間のマッピングを動的に更新できません。

ダイヤルアップアクセスのシナリオなど、一部のシナリオでは、WAN モニターを使用して Web、メール、または FTP サービスが提供され、モニターの IP アドレスが変更されます。ユーザーが固定ドメイン名を使用してサービスにアクセスできるようにするには、WAN モニターで DDNS を設定します。WAN モニターの IP アドレスが変更されると、デバイスは自動的にパケットを DDNS サーバーに送信して、ドメイン名と IP アドレスのマッピングを更新します。

静的DNSの構成

1. ナビゲーションペインで、**Advanced Settings > Application Services** を選択します。
2. **SDNS** タブで、**Add** をクリックします。**New SDNS Entry** ページが開きます。

図118 SDNS



3. **Domain name**フィールドに、ネットワークデバイスのドメイン名を入力します。
4. **IP address**フィールドに、ネットワークデバイスのIPアドレスを入力します。
5. **適用**をクリックします。

図119 SDNSエントリーの追加

ダイナミックDNSの設定

制限事項およびガイドライン

デバイスがDDNSサーバーからドメイン名を申請するときに、WANモニターがパブリックIPアドレスを使用していることを確認します。

前提条件

DDNSを設定する前に、DDNSサービスプロバイダー(PeanutHullなど)のWebサイトにアクセスし、アカウントを登録します。

手順

1. ナビゲーションペインで、**Advanced Settings > Application Services**を選択します。
2. **DDNS**タブをクリックします。

図120 DDNS

Application Services

SDNS DDNS

Online Help

Enter the keyword to automatically [Advanced search](#) Refresh Add Delete

<input type="checkbox"/>	WAN interface	Domain name	Service provider	Server address	Update interval	Username	Status	Opera
<input type="checkbox"/>	WAN0(GE0)	www.3322.org	members.3322.org		0d1h0m		Disconnected	

Page 1 of 1. Total entries on the page: 1. Selected entries: 0. Entries per page: 10 ▾ << < 1 > >>

3. **Add**をクリックします。**New DDNS Policy**ページが開きます。
4. 開いたページで、WANモニターの一覧から、Web、メール、またはFTPサービスを提供する**WAN interface**リストを選択します。
5. **Domain name**フィールドに、デバイスのドメイン名を入力します。
6. 次のDDNSサーバーパラメータを設定します。
 - **Service provider**リストからサービスプロバイダー(PeanutHullなど)を選択します。
 - **Server address**フィールドに、DDNSサーバードレスを入力します。サーバードレスがデフォルト設定と異なる場合は、**Modify server address**を選択してIPアドレスを変更します。
 - デバイスがDDNSアップデート要求を送信する間隔を設定します。間隔を0に設定すると、WANモニタードレスが変更された場合、またはWANモニターがダウン状態からアップ状態になった場合に限り、デバイスはアップデート要求を送信します。
7. **Username**フィールドと**Password**フィールドに、DDNSサーバーに登録されているユーザー名とパスワードをそれぞれ入力します。
8. **Apply**をクリックします。

図121 DDNSポリシーの追加

New DDNS Policy

WAN interface * Choose...

Domain name (1-253 chars)

Server Settings

Service provider * www.3322.org

Server address * members.3322.org (1-64 chars)

Modify server address

Update interval

0 days(0-365)

1 hours(0-23)

0 minutes(0-59)

Account Settings

Username admin1 (1-32 chars)

Password

Apply Cancel

スタティックルーティング

はじめに

静的ルートは手動で構成されます。ネットワークのトポロジーが単純で安定している場合は、ネットワークが正しく動作するように静的ルートを構成するだけで済みます。たとえば、正しい通信のために、ネットワーク出力モニターとゲートウェイIPアドレスに基づいて静的ルートを構成できます。

同じ宛先に到達するために複数のスタティックルートが使用可能な場合は、スタティックルートに異なるプリファレンス値を割り当てることができます。スタティックルートのプリファレンス値が低いほど、ルートのプライオリティは高くなります。

制限事項およびガイドライン

スタティックルートのネクストホップに関連付けられたモニターが無効になった場合、スタティックルートはローカルデバイスから削除されません。この問題を解決するには、ネットワーク環境を確認し、スタティックルート設定を編集する必要があります。

手順

1. ナビゲーションペインで、**Advanced Settings > Static Routing**を選択します。

図122 スタティックルートリスト

Destination	Mask Length	Preference	Next Hop	Interface	Description	Operation
0.0.0.0	0	60	192.168.200.1	GEO		

2. **Add**をクリックします。
3. **Destination IP address**フィールドに、スタティックルートの宛先ネットワークIPアドレスを入力します。
4. **Mask length**フィールドに、宛先ネットワークのマスク長を入力します。
5. Next hopフィールドで、出力モニターを選択し、スタティックルートのネクストホップIPアドレスを入力します。
 - 出力モニターを選択します。サポートされるモニタータイプには、WAN、セルラー、およびVLANモニターが含まれます。
 - ネクストホップIPアドレスを入力します。
6. **Preference**フィールドに、スタティックルートのプリファレンスを入力します。
7. **Description**フィールドに、スタティックルートの説明を入力します。
8. **Apply**をクリックします。

図123 IPv4スタティックルートの追加

New IPv4 Static Route

Destination IP address * 192.168.3.100

Mask length * 24 (0-32)

Next hop ? * Output interface
GE0

Next hop IP address

Preference ? 60 (1-255)

Description (1-60 chars)

Apply Cancel

ポリシーベースルーティング

はじめに

Policy-Based Routing(PBR)を使用すると、一連のパケット一致基準とアクションを含むポリシーを設定することで、パケットの特性に基づいてパケットを柔軟に転送できます。たとえば、PBRポリシーを設定して、指定した送信元または宛先IPアドレスを持つパケットを、指定したネクストホップに転送したり、指定したモニターから転送したりできます。

手順

1. ナビゲーションペインで、**Advanced Settings > PBR**を選択します。
2. PBRポリシーを適用するモニターを選択します。

図124 PBRポリシーリスト

3. **Add**をクリックします。
4. **Match rule**領域で、必要に応じて一致基準を設定します。
 - **Protocol type**フィールドで**Protocol type**を選択します。
 - **Protocol number**を選択した場合は、プロトコル番号を入力する必要があります。たとえば、80(HTTPの場合)です。
 - **TCP**または**UDP**を選択した場合は、照合するパケットの送信元ポート番号と宛先ポート番号を入力する必要があります。
 - **Source address range**フィールドおよび**Destination address range**フィールドに、送信元および宛先のIPアドレス範囲を入力します。アドレス範囲を指定するには、1.1.1.1-1.1.1.2のように、開始IPアドレスと終了IPアドレスをハイフン(-)で区切ります。1つのIPアドレスのみを指定するには、1.1.1.1-1.1.1.1のように、そのIPアドレスを開始IPアドレスと終了IPアドレスの両方として入力します。
 - **Source Port**および**Destination Port**フィールドに、ソースポートおよび宛先ポートを入力します。**Source Port**および**Destination Port**フィールドは、プロトコルタイプがTCPまたはUDPの場合にのみ必要です。
 - **Valid period**セクションで、PBRポリシーが有効になる期間を指定します。1日全体を指定するには、期間を00:00-23:59に設定します。
5. **Output interface or Next hop**フィールドで、一致するパケットの出力モニターまたはネクストホップを設定します。
6. 管理を容易にするために、**Description**フィールドにPBRポリシーの説明を入力します。
7. **Apply**をクリックします。

図125 PBRポリシー設定の構成

Match rule

Protocol type * TCP (0-255)

Source address range * 192.168.1.100-192.168.1.200

Destination address range * 192.168.1.200-192.168.1.249

Source port * 90 (1 to 65535. You can enter a single port number or a port number range, for example, 3000-4000.)

Destination port * 8080 (1 to 65535. You can enter a single port number or a port number range, for example, 3000-4000.)

Valid period * 00 : 00 - 24 : 00 Sun Mon Tue Wed Thu Fri Sat

Output interface WAN0(GE0) Next hop ?

Description (Optional. Value range: 1 to 15 chars.)

Apply Cancel

SNMP

SNMPの概要

Simple Network Management Protocol(SNMP)を使用すると、MIBブラウザなどの Network Management System(NMS)を使用して、デバイスにアクセスし、管理できます。SNMPが設定されている場合、重要なイベント(モニターのアップまたはダウン、高いCPU使用率、メモリ不足など)が発生すると、デバイスは自動的にトラップまたはインフォームをNMSに送信します。

デバイスは、SNMPv1、SNMPv2c、およびSNMPv3をサポートします。SNMPv3は、SNMPv1およびSNMPv2cよりも優れたセキュリティを提供します。

- SNMPv1およびSNMPv2cは、認証にパスワードを使用します。
- SNMPv3は認証にユーザー名を使用するため、認証キーとプライバシーキーを設定して通信のセキュリティを確保する必要があります。
 - ユーザー名と認証キーは、無効なNMSがデバイスにアクセスするのを防ぐために、NMSの認証に使用されます。
 - プライバシーキーは、NMSとデバイス間で送信されるメッセージを暗号化して、メッセージが盗聴されないようにするために使用されます。

前提条件

使用するSNMPバージョンを決定します。NMSとデバイスは、同じSNMPバージョンを使用する必要があります。

SNMPv1またはSNMPv2cの設定

制限事項およびガイドライン

NMSとデバイスでは、同じSNMPパスワードを使用する必要があります。SNMPパスワードには、読み取り専用パスワードと読み取り/書き込みパスワードがあります。少なくとも1つを設定する必要があります。

- デバイスからパラメータ値を取得するには、読み取り専用パスワードだけを設定します。
- デバイスのパラメータ値を取得して設定するには、読み取りパスワードと書き込みパスワードを設定します。

手順

1. ナビゲーションペインで、**Advanced Settings > SNMP**を選択します。
2. SNMPをイネーブルにします。
3. **SNMPv1 and SNMPv2c**のバージョンを選択します。
4. SNMPパスワードを指定します。
5. **Trust Host IPv4 Address**フィールドにNMSのIPアドレスを入力します。

指定したNMSのみがデバイスを管理できます。このパラメータを構成しない場合、正しいSNMPパスワードを使用するすべてのNMSがデバイスを管理できます。

6. **Trap Target Host IPv4 Address/Domain**フィールドに、通知を受信するホストのIPアドレスまたはドメイン名を入力します。
7. **Contact Information**フィールドに、デバイス管理者の連絡先情報を入力します。
8. **Device Location**フィールドに、デバイスの物理的な場所を入力します。
9. **Apply**をクリックします。

図126 SNMPv1およびSNMPv2cの設定

SNMP

Online Help

SNMP Enable Disable

SNMP Version SNMPv1 and SNMPv2c SNMPv3

SNMP Password * Read-only password

admin (1-32 chars)

Read-write password

admin123 (1-32 chars)

Trust Host IPv4 Address 1.1.1.1

Trap Target Host IPv4 Address/Domain 2.2.2.2 (1-253 chars)

Contact Information New H3C Technologies Co., Ltd. (1-255 chars)

Device Location Hangzhou, China (1-255 chars)

*Provide a read-only password, a read-write password, or both. To configure both passwords, make sure they are not the same.

Apply

SNMPv3の設定

制限事項およびガイドライン

NMSとデバイスは、同じユーザー名、認証キー、およびプライバシーキーを使用する必要があります。

手順

1. ナビゲーションペインで、**Advanced Settings > SNMP**を選択します。
2. SNMPをイネーブルにします。
3. **SNMPv3**バージョンを選択します。
4. usernameを指定します。
5. authentication keyを指定します。
6. privacy keyを指定します。
7. **Trust Host IPv4 Address**フィールドにNMSのIPアドレスを入力します。

指定されたNMSだけがデバイスを管理できます。このパラメータを設定しない場合、正しいSNMPユーザー名、認証キー、およびプライバシーキーを使用するすべてのNMSがデバイスを管理できません。

8. **Trap Target Host IPv4 Address/Domain**フィールドに、通知を受信するホストのIPアドレスまたはドメイン名を入力します。
9. **Contact Information**フィールドに、デバイス管理者の連絡先情報を入力します。
10. **Device Location**フィールドに、デバイスの物理的な場所を入力します。

11. **Apply**をクリックします。

図127 SNMPv3の設定

SNMP

Online Help

SNMP Enable Disable

SNMP Version SNMPv1 and SNMPv2c SNMPv3

Username * (1-32 chars)

Authentication Key * (1-64 chars)

Privacy Key * (1-64 chars)

Trust Host IPv4 Address

Trap Target Host IPv4 Address/Domain (1-253 chars)

Contact Information (1-255 chars)

Device Location (1-255 chars)

Apply

CWMP

CWMPの概要

CPE WAN Management Protocol(CWMP)ネットワークでは、Auto-Configuration Server(ACS)からCPE(Customer Premises Equipment)を一括してリモートで均一に管理できます。これにより、CPE管理の問題が解決され、メンテナンスコストが節約されます。

前提条件

ACS機能をサポートするサーバーを準備し、事前にACSサーバーの設定を行います。

手順

1. ナビゲーションペインで、**Advanced Settings > CWMP**を選択します。
2. CWMPをイネーブルにします。
3. **ACS**領域で、ACSのURLアドレス、ユーザー名、およびパスワードを入力します。

CPEによって開始されたACSへの接続要求には、ACSユーザー名とパスワードが含まれていません。ACSは、要求内のACSユーザー名とパスワードが、ACSサーバーに対してローカルに設定されたものと同じである場合に限り、要求を受け入れます。

4. **CPE**領域で、次のタスクを実行します。

- a. CPEユーザー名とパスワードを指定します。

CPEでの悪意のある制御を回避するために、ACSはCPEのユーザー名とパスワードを含む管理命令を送信します。ACSがCPEを制御できるのは

手順のユーザー名とパスワードは、CPEに対してローカルに設定されたものと同じです。

- b. 必要に応じて、定期的なインフォームを有効または無効にします。この機能を有効にする場合は、インフォームパケットの送信間隔を設定します。

CPEは、CPEとACSのユーザー名とパスワードをそれぞれ含むインフォームパケットを送信することによって、ACSへの接続要求を開始します。

デバイスを特定の間隔で自動的にACSに接続させるには、定期的な通知機能をイネーブルにする必要があります。

- c. ACSに接続するCPE上のモニターを指定します。

5. **Certain**をクリックします。

図128 CWMPの設定

CWMP

Online Help

CWMP Enable Disable

ACS URL * (8-255 chars)

Username (1-255 chars)

Password (1-255 chars)

CPE Username (1-255 chars)

Password (1-255 chars)

Periodic Inform Enable Disable

CPE connection interface

Apply

システムツール

基本設定

基本設定の概要

デバイス情報とシステム時刻を設定するには、次の作業を実行します。

デバイス情報には、デバイス名、デバイスの場所、および連絡先情報が含まれます。デバイス名は編集可能ですが、デバイスの場所と連絡先情報は編集できません。

システム時刻には、日付、時刻、およびタイムゾーンが含まれます。正しいシステム時刻は、ネットワーク管理と通信に不可欠です。ネットワーク上でデバイスを実行する前に、システム時刻を正しく設定してください。

デバイスは、次のいずれかの方法を使用してシステム時刻を取得できます。

- システム時刻を手動で設定します。

このデバイスは、ローカルに設定されたシステム時間を使用し、次に、内蔵の水晶発振器によっ

て生成されたクロック信号を使用してシステム時間を維持する。

デバイスが再起動すると、システム時刻は工場出荷時のデフォルトに戻ります。

- NTPサーバーと日時を自動的に同期させます。

デバイスは、NTPサーバーから取得した時刻を現在のシステム時刻として使用し、定期的にNTPサーバーと時刻を同期します。デバイスが再起動しても、デバイスはNTPサーバーとシステム時刻を迅速に再同期します。ネットワーク上にNTPサーバーがある場合は、この方法をお勧めします。

タイムソースからの時間を使用して計算されるシステム時間は、より正確です。

注:

Webモニターにアクセスするには、次のいずれかのブラウザを使用することをお勧めします。

- Internet Explorer 10以降。
 - Chrome 57以降。
 - Firefox 35以降。
-

基本的なデバイス情報の設定

1. ナビゲーションペインで、**System Tool > Basic Settings**を選択します。
2. **Device information**タブで、デバイス名を入力します。
3. **Apply**をクリックします。

図129 デバイス情報

The screenshot shows the 'Basic Settings' web interface. At the top, there is a navigation bar with 'Basic Settings' and a button labeled '按 F11 即可退出全屏模式'. Below the navigation bar, there are two tabs: 'Device information' (selected) and 'Date/Time'. In the top right corner, there is an 'Online Help' link. The main content area contains three form fields: 'Device name' with the value 'H3C' and a '(1-64 chars)' label; 'Device location' with the value 'Hangzhou, China'; and 'Contact information' with the value 'New H3C Technologies Co., Ltd.'. At the bottom left, there is a green 'Apply' button.

システム時刻を手動で設定する

制限事項およびガイドライン

デバイスをリブートすると、工場出荷時のシステム時刻設定が復元されます。

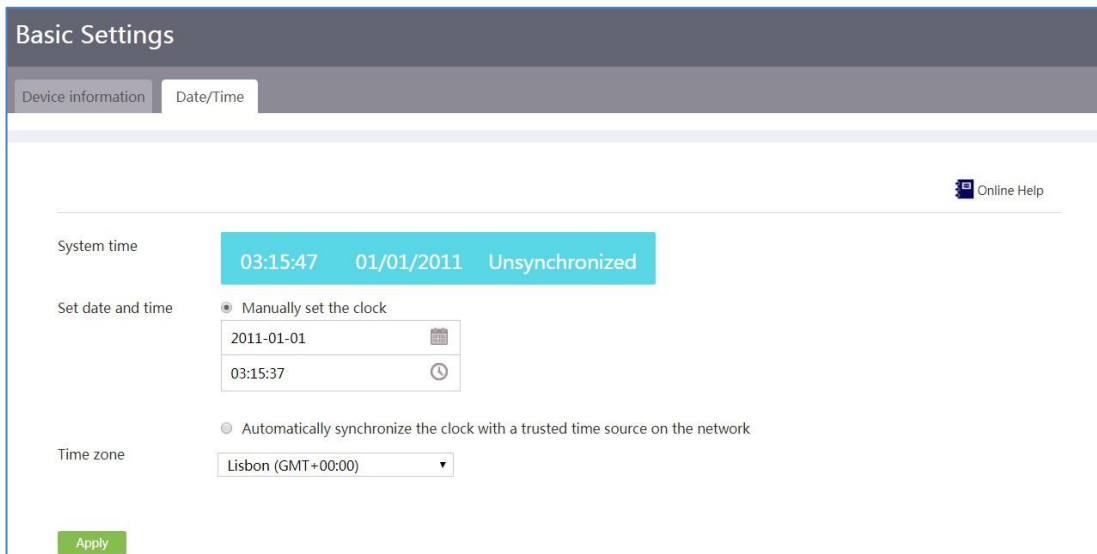
前提条件

デバイスが存在する場所のタイムゾーンを識別します。

手順

1. ナビゲーションペインで、**System Tool > Basic Settings**を選択します。
2. **Date/Time**タブをクリックします。
3. **Manually set the clock**を選択します。
4. システム時刻を、デバイスが設置されている地域の現在時刻に設定します。
 - a. 日付を選択します。
 - b. 時間を選択します。Webモニターで使用可能な分と秒の値は、3の倍数(00、03、06、09、..、57)です。上下の矢印を使用して値を微調整できます。たとえば、分の値を20に設定するには、最初に18を選択し、次に上矢印を2回クリックして20を取得します。
5. デバイスが存在する場所のタイムゾーンを選択します。
6. **Apply**をクリックします。

図130 システム時刻の手動設定



UTC時刻を自動的に同期させる

制限事項およびガイドライン

デバイスがNTPサーバーと同じタイムゾーンを使用していることを確認します。

前提条件

デバイスが存在する場所のタイムゾーンを識別します。

手順

1. ナビゲーションペインで、**System Tool > Basic Settings**を選択します。
2. **Date/Time**タブをクリックします。
3. **Automatically synchronize the clock with a trusted time source on the network**を選択します。
4. **Default NTP Server List**をクリックして、デフォルトのNTPサーバーを指定します。
5. IPアドレスまたはホスト名を入力して、NTPサーバーを指定します。
6. タイムゾーンを選択します。
7. **Apply**をクリックします。

図131 UTC時刻の自動同期

Basic Settings

Device information | Date/Time

Online Help

System time: 03:16:16 01/01/2011 Unsynchronized

Set date and time:

- Manually set the clock
- Automatically synchronize the clock with a trusted time source on the network

No.	NTP Server	Operation
	1 - 253 chars.	+

Default NTP Server List

Time zone: Lisbon (GMT+00:00)

Apply

注:

- デバイスにデフォルトのNTPサーバーが設定されているかどうかは、デバイスのモデルによって異なります。
- デフォルトのNTPサーバーを使用するか、必要に応じてNTPサーバーを指定できます。デバイスは、最高の時刻精度を提供する使用可能なNTPサーバーからUTC時刻を自動的に取得します。使用可能なNTPサーバーがない場合、デバイスは内部クロック信号を使用します。NTPサーバーの復旧後、デバイスは再びNTPサーバーと時刻を同期します。

診断

診断の概要

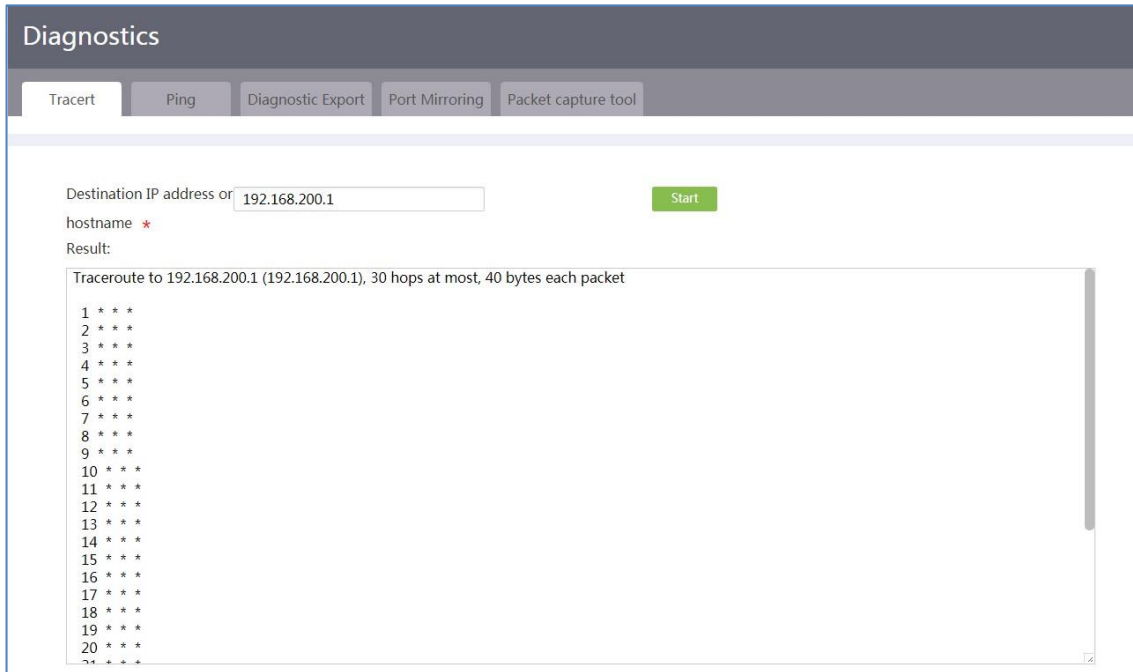
この機能を使用して、ネットワーク障害を診断します。診断を使用すると、次のタスクを実行できます。

- **tracert:** パケットがデバイスから宛先ホストまで通過するパスを追跡します。
- **ping:** 別のデバイスまたはホストの到達可能性をテストします。
- **Diagnostic export:** システムの診断とトラブルシューティングのために、フィーチャモジュールの動作情報を収集します。デバイスは、収集した情報を圧縮ファイルに自動的に保存し、そのファイルをWebログイン端末に保存します。
- **Port mirroring:** ポートミラーリングは、監視対象ポートを通過するパケットを自動的に監視ポートにコピーし、各ポートの伝送情報をリアルタイムで提供します。ネットワーク管理者は、この情報を使用して、トラフィック監視、パフォーマンス分析、および障害診断を実行できます。
- **Packet capture tool:** ネットワークデータパケットをキャプチャして、ネットワーク障害をより効果的に分析します。このツールは、バックエンドで実行するためにtcpdumpを使用し、キャプチャされたパケットをWebログイン端末上のflash--packetCapture.pcapという名前のファイルに自動的に保存します。

tracertの構成

1. ナビゲーションペインで、**System Tool > Diagnostics**を選択します。
2. **Tracert**タブをクリックします。
3. 宛先IPアドレスまたはホスト名を入力します。
4. **Start**をクリックします。
5. **Result**領域で、tracertの結果を表示します。

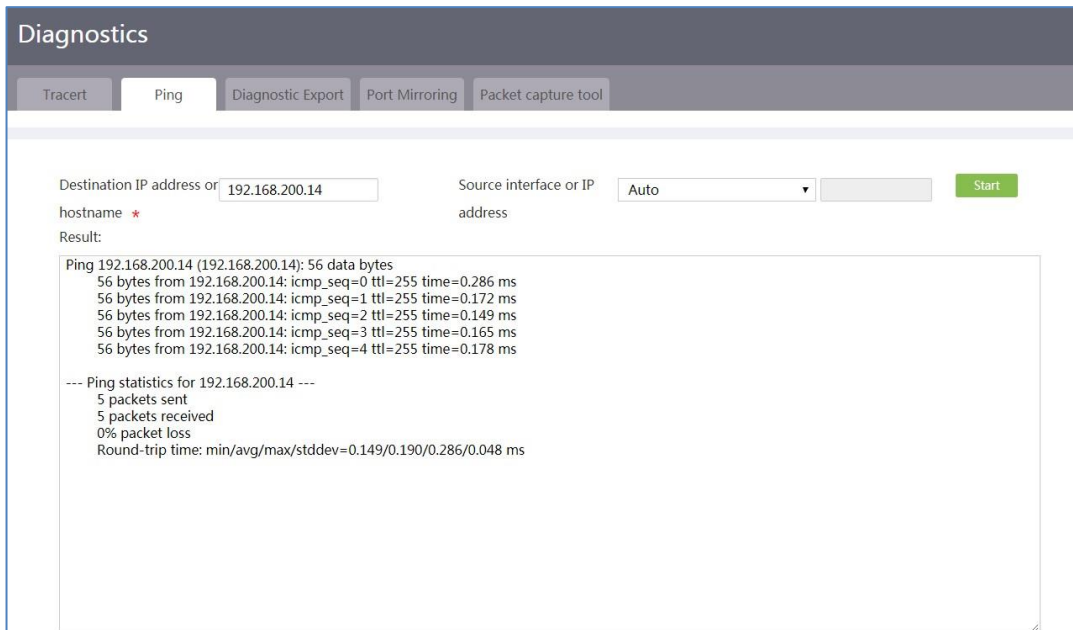
図132 tracertの構成



pingの設定

1. ナビゲーションペインで、**System Tool > Diagnostics**を選択します。
2. **Ping**タブをクリックします。
3. 宛先IPアドレスまたはホスト名を入力します。
4. pingパケットの送信元モニターまたは送信元IPアドレスを設定します。
5. **Start**をクリックします。
6. **Result**領域で、pingの結果を表示します。

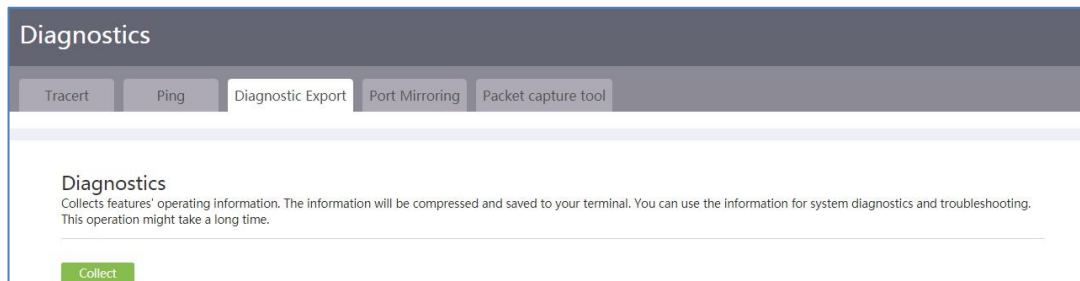
図133 pingの設定



診断情報の収集

1. ナビゲーションペインで、**System Tool > Diagnostics**を選択します。
2. **Diagnostic Export**タブをクリックします。
3. **Collect**をクリックします。

図134 診断情報の収集



ポートミラーリングの構成

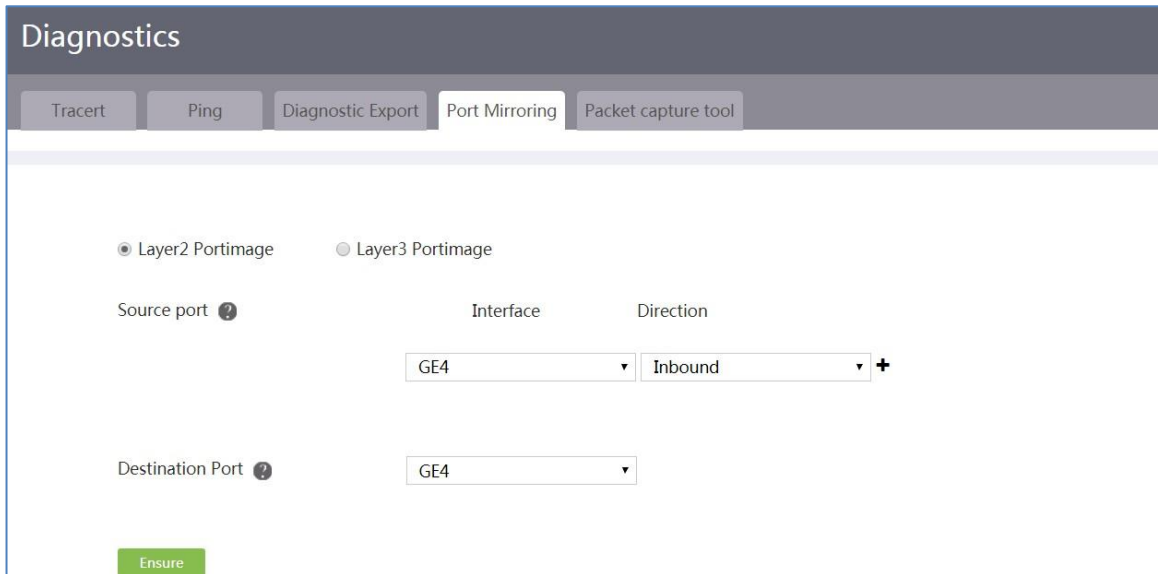
1. ナビゲーションペインで、**System Tool > Diagnostics**を選択します。
2. **Port Mirroring**タブをクリックします。
3. レイヤー2モニターまたはレイヤー3モニターのポートミラーリングを設定する場合に選択します。
4. 送信元ポートを設定します。
ソースポートを選択します。次に、ソースポートの方向を選択します。次のオプションを使用できます。
 - **Inbound**: 送信元ポートで受信されたパケットだけをミラーリングします。
 - **Outbound**: 送信元ポートから送信されたパケットだけをミラーリングします。

- **Both:** 送信元ポートで受信されたパケットと送信元ポートから送信されたパケットの両方をミラーリングします。

送信元ポートをさらに追加するには、+アイコンをクリックします。

5. 宛先ポートを選択します。
6. **Ensure**をクリックします。

図135 ポートミラーリングの構成



パケットキャプチャツールを設定する

制限事項およびガイドライン

この機能を使用する前に、ストレージメディアにパケットキャプチャファイルを保存するための十分な領域があることを確認してください。ストレージ領域が不足している場合、パケットキャプチャタスクは完了する前に停止します。

手順

1. ナビゲーションペインで、**System Tool > Diagnostics**を選択します。
2. **Packet capture tool**タブをクリックします。
3. パケットをキャプチャするモニターを選択します。ルーター上の任意のWANモニターを選択できます。
4. キャプチャするパケットのサイズをバイト単位で設定します。capture lengthパラメータは、デバイスがパケットからキャプチャできる最大長を表します。パケットの長さが指定された長さより長い場合、デバイスはそのパケットから指定された長さのコンテンツのみをキャプチャします。
キャプチャ長を長くすると、パケット処理時間が長くなり、tcpdumpがキャッシュできるパケットの数が少なくなります。その結果、パケットが失われる可能性があります。必要なパケットをキャプチャできることを前提として、キャプチャ長を短く指定します。
5. 必要に応じて、パケットをキャプチャするためのプロトコルタイプを指定します。allを選択すると、モニター上のすべてのパケットがキャプチャされます。
6. キャプチャされたパケットを保存するファイルの最大サイズをMB単位で設定します。
7. パケットキャプチャ期間を秒単位で設定します。
8. 送信元ホストパラメータによってキャプチャされるパケットをモニターします。次のオプションを使用

きます。

- **Any:** すべての送信元ホストのパケットをキャプチャします。
 - **Filter by IP address:** 特定のIPアドレスを持つホストから送信されたパケットをキャプチャします。
 - **Filter by MAC address:** 特定のMACアドレスを持つホストから送信されたパケットをキャプチャします。
9. 宛先ホストパラメータによって取得されるパケットをモニターします。次のオプションを使用できます。
- **Any:** すべての宛先ホストのパケットをキャプチャします。
 - **Filter by IP address:** 特定のIPアドレスを持つホストが受信したパケットをキャプチャします。
 - **Filter by MAC address:** 特定のMACアドレスを持つホストが受信したパケットをキャプチャします。
10. **Start**をクリックします。

現在のページには、パケットキャプチャプロセスと現在キャプチャされているパケット数が表示されます。**Cancel**をクリックすると、パケットキャプチャを終了し、キャプチャファイル**flash -- packetCapture.pcap**をエクスポートできます。

図136 パケットキャプチャツールの設定

The screenshot shows the 'Packet capture tool' configuration page under the 'Diagnostics' menu. The page has tabs for 'Tracert', 'Ping', 'Diagnostic Export', 'Port Mirroring', and 'Packet capture tool'. The main content area contains the following settings:

- Interface: **GE0** (dropdown menu)
- Bytes to capture: **1518** (input field, range 64-8000Bytes)
- Protocol: **ALL** (dropdown menu)
- Maximum packet file size: **5** (input field, range 1-10MB)
- Duration: **20** (input field, range 1-30s)
- Capture filter: Source host: **Any** (dropdown menu), Destination host: **Any** (dropdown menu)
- A green **Start** button is located at the bottom center.

管理者アカウント管理

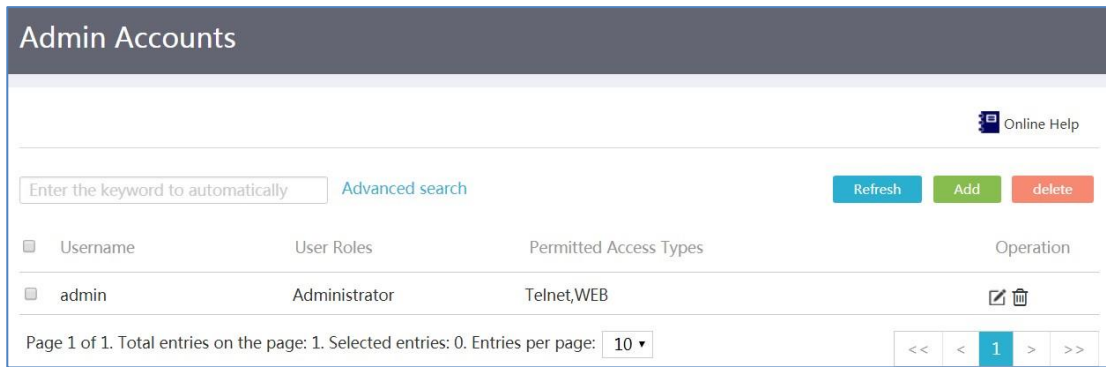
adminアカウント管理について

このページを使用して、ユーザーがデバイスへのログインに使用する管理者アカウントを管理および保守します。管理者アカウントを追加、編集または削除できます。

adminアカウントを追加する

1. ナビゲーションペインで、**System Tool > admin Accounts**を選択します。

図137 管理アカウント



2. **Add**をクリックします。
3. 表示されたダイアログボックスで、ユーザー名フィールドにアカウント名を入力します。
4. **Password**フィールドにパスワードを入力し、**Confirm password**フィールドで確認します。
パスワードを設定しない場合、ユーザーがこのアカウントを使用してデバイスにログインするときに、システムはパスワードを要求しません。セキュリティを向上させるには、adminアカウントのパスワードを設定します。
5. **User roles**フィールドで、ユーザーロールを選択します。
 - この管理者アカウントに最高の管理特権を割り当てるには、**Administrator**を選択します。
 - この管理者アカウントに表示権限のみを割り当てるには、**Operator**を選択します。
6. **Permitted access types**フィールドで、access servicesを選択します。
 - コンソールサービスをこの管理者アカウントに割り当てるには、**Console**を選択します。
コンソールサービスを使用すると、ユーザーはコンソールポート経由でデバイスにログインできます。
 - Telnetサービスをこの管理者アカウントに割り当てるには、**Telnet**を選択します。
Telnetサービスを使用すると、デバイスがTelnetサーバーとして動作している場合、ユーザーはTelnetクライアントからデバイスにTelnet接続できます。
 - FTPサービスをこの管理者アカウントに割り当てるには、**FTP**を選択します。
FTPサービスを使用すると、デバイスがFTPサーバーとして動作している場合、ユーザーはFTPクライアントからデバイス上のファイルシステムリソースにアクセスできます。
 - Webサービスをこの管理者アカウントに割り当てるには、**WEB**を選択します。Webサービスを使用すると、ユーザーはWeb経由でデバイスにログインできます。
 - SSHサービスをこの管理者アカウントに割り当てるには、**SSH**を選択します。
SSHサービスを使用すると、デバイスがSSHサーバーとして動作する場合、ユーザーはSSHクライアントからデバイスにログインできます。SSHログインは、Telnetログインよりも安全です。
7. **Max concurrent online users**フィールドで、この管理者アカウントを使用できる同時ユーザーの最大数を設定します。
制限を設定しない場合、デバイスはこの管理者アカウントを使用する同時ユーザーの数を制限しません。
この設定では、このadminアカウントを使用してFTP経由でデバイスにログインする同時ユーザー数は制限されません。
8. **FTP working directory**フィールドに、作業ディレクトリを入力します。管理アカウントにFTPサービスが割り当てられている場合は、このパラメータを構成する必要があります。

有効な作業ディレクトリを入力するためのベストプラクティスとして、最初に既存のファイルパスを表示する**System Tool > Upgrade > File Management**ページにアクセスします。

9. **Apply**をクリックします。

図138 adminアカウントの追加

New Administrator

Username * test (1-55 chars)

Password ? (1-63 chars)

Confirm password (1-63 chars)

User roles Administrator x ▾
Administrator 🗑

Permitted access types Console Telnet FTP WEB SSH

Max concurrent online users 3 (1-1024)

FTP working directory (1-255 chars)

Apply Cancel

adminアカウントの編集

1. ナビゲーションペインで、**System Tool > Admin Accounts**を選択します。
2. **admin**アカウントの**Operation**カラムにある**Edit**アイコンをクリックします。
3. 表示されたダイアログボックスで、**Change password**フィールドに新しいパスワードを入力し、**Confirm password**フィールドで確認します。
adminアカウントのパスワードを変更した後、このadminアカウントを使用するユーザーは、次回のログイン時にパスワードを再度変更する必要があります。
4. **User roles**リストで、新しいロールを選択します。
 - この管理者アカウントに最高の管理特権を割り当てるには、**Administrator**を選択します。
 - この管理者アカウントに表示権限のみを割り当てるには、**Operator**を選択します。
5. **Permitted access types**フィールドで、**new access services**を選択します。
 - コンソールサービスをこの管理者アカウントに割り当てるには、**Console**を選択します。
コンソールサービスを使用すると、ユーザーはコンソールポート経由でデバイスにログインできます。
 - Telnetサービスをこの管理者アカウントに割り当てるには、**Telnet**を選択します。
Telnetサービスを使用すると、デバイスがTelnetサーバーとして動作している場合、ユーザーはTelnetクライアントからデバイスにTelnet接続できます。
 - FTPサービスをこの管理者アカウントに割り当てるには、**FTP**を選択します。
FTPサービスを使用すると、デバイスがFTPサーバーとして動作している場合、ユーザーは

FTPクライアントからデバイス上のファイルシステムリソースにアクセスできます。

- Webサービスをこの管理者アカウントに割り当てるには、**WEB**を選択します。Webサービスを使用すると、ユーザーはWeb経由でデバイスにログインできます。
- SSHサービスをこの管理者アカウントに割り当てるには、**SSH**を選択します。
SSHサービスを使用すると、デバイスがSSHサーバーとして動作する場合、ユーザーはSSHクライアントからデバイスにログインできます。SSHログインは、Telnetログインよりも安全です。

6. **Max concurrent online users**フィールドで、新しい値を設定して、この管理者アカウントを使用できる同時ユーザーの最大数を変更します。

制限を設定しない場合、デバイスはこの管理者アカウントを使用する同時ユーザーの数を制限しません。

この設定では、このadminアカウントを使用してFTP経由でデバイスにログインする同時ユーザー数は制限されません。

7. **FTP working directory**フィールドに、新しい作業ディレクトリを入力します。管理アカウントにFTPサービスが割り当てられている場合は、このパラメータを構成する必要があります。

有効な作業ディレクトリを入力するためのベストプラクティスとして、最初に既存のファイルパスを表示するため **System Tool > Upgrade > File Management** ページにアクセスします。

8. **Apply**をクリックします。

図139 adminアカウントの編集

The screenshot shows a dialog box titled "Edit Administrator". It contains the following fields and controls:

- Username ***: Input field containing "admin" (1-55 chars).
- Change password ?**: Input field with masked characters (1-63 chars).
- Confirm password**: Input field with masked characters.
- User roles**: Dropdown menu showing "Administrator" with a delete icon.
- Permitted access types**: Checkboxes for Console, Telnet (checked), FTP, WEB, and SSH.
- Max concurrent online users**: Input field (1-1024).
- FTP working directory**: Input field containing "flash:" (1-255 chars).
- Buttons**: "Apply" (green) and "Cancel" (red) buttons at the bottom.

管理者アカウントを削除する

1. ナビゲーションペインで、**System Tool > Admin Accounts**を選択します。
2. adminアカウントの**Operation**カラムにある**Delete**アイコンをクリックします。
3. 表示されたダイアログボックスで、**Yes**をクリックします。

リモート管理

リモート管理の概要

リモート管理を使用して、ネットワーク接続検出またはデバイスのリモートログインおよび管理のパラメータを設定します。

リモート管理を使用すると、次のタスクを実行できます。

- **Permit ping on interfaces:** モニターがpingパケットを送信できるようにするには、次の作業を実行します。pingは、ネットワーク接続を検出し、ネットワークの実行ステータスを取得するためのユーティリティです。
- **Permit Telnet login on interfaces:** ログインの許可ユーザーが特定のモニターを介してデバイスにTelnet接続できるようにするには、次の作業を実行します。Telnetはリモートログインプロトコルです。ユーザーはPCからデバイスにTelnet接続して、デバイスをリモート管理できます。
- **Permit SSH login:** デバイスアクセスを保護するには、この作業を実行してSecure Shell(SSH)サービスをイネーブルにします。SSHはネットワークセキュリティプロトコルです。暗号化と認証を使用して、SSHはセキュアなリモートアクセスとセキュアでないネットワーク上でのファイル転送を実装できます。SSHサーバーとして動作するデバイスは、次のSSHサービスをサポートします。
 - **Stelnet:** Secure Telnet(Stelnet)の実装はTelnetの実装と同じですが、Stelnetの方がより安全です。
 - **SFTP:** Secure FTP(SFTP)は、SSH接続を使用してセキュアなファイル転送を提供します。デバイスでは、セキュアなファイル管理および転送のために、リモートユーザーがデバイスにログインできます。
 - **SCP:** Secure Copy(SCP)は、ファイルを安全にコピーする方法を提供します。
- **Permit HTTP/HTTPS login on interfaces:** ユーザーがHTTPまたはHTTPSを使用して特定のモニター経由でデバイスにログインできるようにするには、このタスクを実行します。Webログインでは、HTTPまたはHTTPSを使用できます。HTTPSログインは、HTTPログインよりも安全です。ユーザーは、HTTPまたはHTTPSを使用してPCからデバイスのWebモニターにログインし、デバイスの設定と管理をリモートで行うことができます。
- **Use the cloud service:** このタスクを実行して、インターネット経由でH3Cクラウドサーバーとのリモート管理トンネルを確立します。ネットワーク管理者は、クラウドサーバーを介してデバイスをリモートで管理および保守できます。

モニター上でpingを許可する

1. ナビゲーションペインで、**System Tool > Remote Login**を選択します。
2. **Ping**タブで、モニターの**Permit ping**を選択して、モニターがpingパケットを送信できるようにします。
3. **Apply**をクリックします。

図140 pingサービスの設定

The screenshot shows the 'Remote Login' configuration page with the 'Ping' tab selected. The page has a navigation bar with tabs for 'Ping', 'Telnet', 'SSH', 'HTTP/HTTPS', and 'Cloud Service'. An 'Online Help' icon is in the top right. The main content area contains a table with two columns: 'Inter face' and 'Ping'. The first row is for 'GE0' with a checked 'Permit ping' checkbox. The second row is for 'Vlan-interface1' with a checked 'Permit ping' checkbox. A green 'Apply' button is at the bottom left.

Inter face	Ping
GE0	<input checked="" type="checkbox"/> Permit ping
Vlan-interface1	<input checked="" type="checkbox"/> Permit ping

Telnetログインの設定

1. ナビゲーションペインで、**System Tool > Remote Login**を選択します。
2. **Telnet**タブをクリックします。
3. **Telnet service**の横にあるボタンをクリックして、Telnetサービスを有効にします。Telnetサービスが**ON**状態の場合、サービスは有効になります。
4. **IPv4 Listening Port**フィールドまたは**IPv6 Listening Port**フィールドに、Telnetサービスのポート番号を入力します。

ネットワーク要件に応じて、IPv4リスニングポート番号またはIPv6リスニングポート番号を入力します。

- ユーザーがIPv4ネットワーク内のデバイスにTelnet接続する場合、ユーザーが使用するポート番号は、**IPv4 Listening Port**フィールドで指定したポート番号と同じである必要があります。
- ユーザーがIPv6ネットワーク内のデバイスにTelnet接続する場合、ユーザーが使用するポート番号は、**IPv6 Listening Port**フィールドで指定したポート番号と同じである必要があります。

5. **Apply**をクリックします。

図141 Telnetサービスの設定

The screenshot shows the 'Remote Login' configuration page with the 'Telnet' tab selected. The 'Telnet service' is turned on. Below it are two input fields for 'IPv4 Listening Port' and 'IPv6 Listening Port', both set to '23'. Below these is an 'Administrator IP Address List' section with an 'Edit' button. The 'IP Address' field contains '192.168.1.100'. There are also empty fields for 'IP Address Range' and 'Exclude IP Address'.

6. **Administrator IP Address List**の右側にある**Edit**をクリックします。
7. 表示されたページで、リモートログイン用のモニターのIPv4アドレスを1つ以上指定します。
 - 個々の管理者IPアドレスを追加するには、**IP address**フィールドにIPアドレスを入力します。


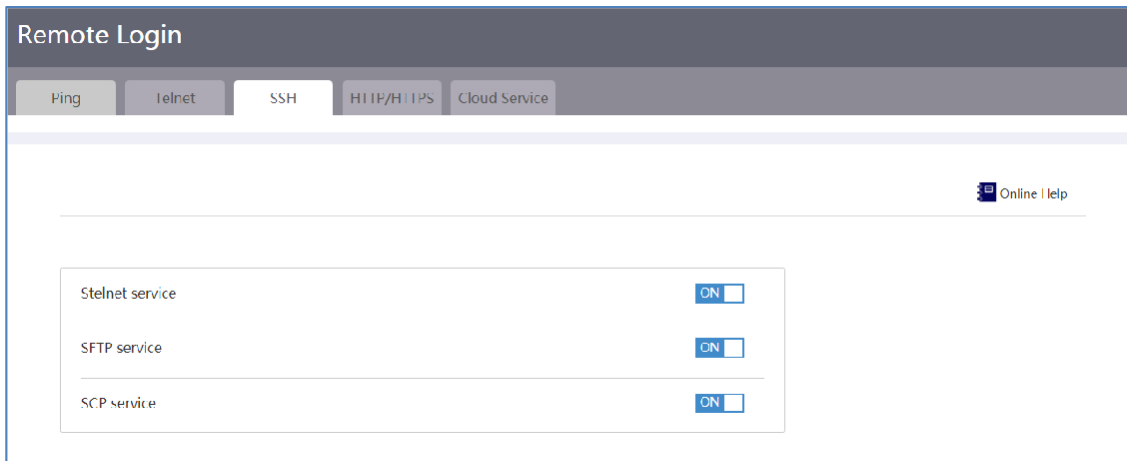
- 管理者IPアドレスの範囲を追加するには、IP address rangeフィールドに**IP address range**を指定します。
開始アドレスは終了アドレスよりも小さくする必要があります。個別に指定されたIPアドレスは、指定されたIPアドレスの範囲外であってもかまいません。
 - IPアドレス範囲からIPアドレスを除外するには、除外するIPアドレスを**Exclude IP address**フィールドに入力します。
除外されたIPアドレスは、指定されたIPアドレス範囲内である必要があります。除外されたIPアドレスは、Telnetを介してデバイスにアクセスできません。
8. アイコン  をクリックして、指定したIPアドレス、アドレス範囲、または除外されたIPアドレスを、右側の管理者IPアドレスリストに追加します。
 9. 手順7～8を繰り返して、管理者IPアドレスをさらに追加します。
 10. **Apply**をクリックします。

図142 管理者IPアドレスの設定

SSHログインの設定

1. ナビゲーションペインで、**System Tool > Remote Login**を選択します。
2. **SSH**タブをクリックします。
3. ネットワーク要件に応じて、1つまたは複数のSSHサービスを有効にします。
 - Stelnetサービスを有効にするには、**Stelnet service**フィールドの横にあるボタンをクリックして、サービスの状態を**ON**に設定します。
 - SFTPサービスをイネーブルにするには、**SFTP service**フィールドの横にあるボタンをクリックして、サービスの状態を**ON**に設定します。
 - SCPサービスをイネーブルにするには、**SCP service**フィールドの横にあるボタンをクリックして、サービス状態を**ON**に設定します。

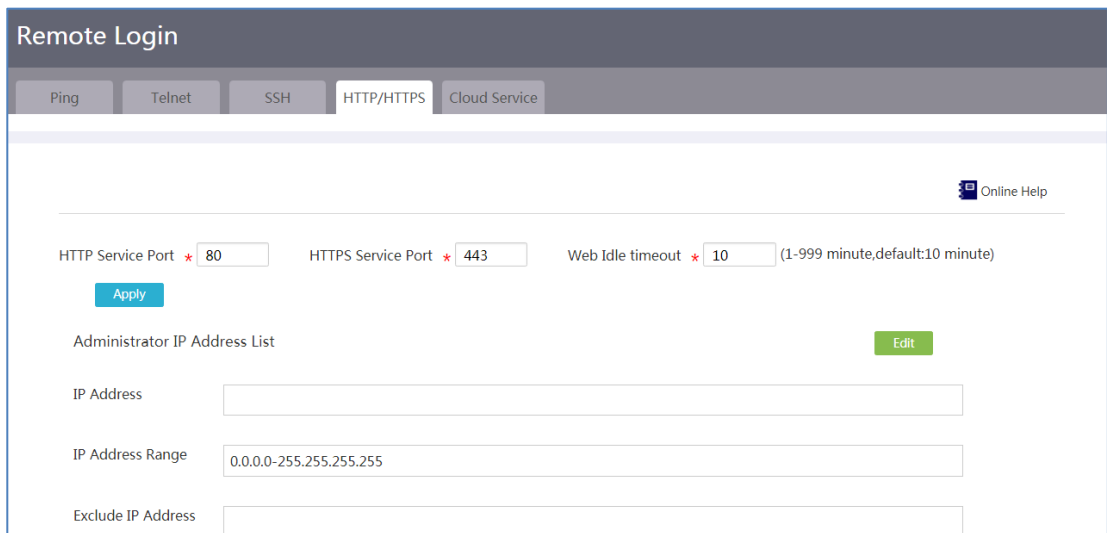
図143 SSHサービスの設定



HTTPログインとHTTPSログインの設定

1. ナビゲーションペインで、**System Tool > Remote Login**を選択します。
2. **HTTP/HTTPS**タブをクリックします。
3. **HTTP Service Port**フィールドで、HTTPログインのポート番号を入力します。HTTPログインには、10000より大きいポート番号を使用することをお勧めします。
4. **HTTPS Service Port**フィールドに、HTTPSログイン用のポート番号を入力します。HTTPSログインには、10000より大きいポート番号を使用することをお勧めします。
5. **Web Idle timeout**フィールドにタイムアウト時間を入力します。
6. **Apply**をクリックします。

図144 HTTP/HTTPSサービスの設定



7. **Administrator IP Address List**の右側にある**Edit**をクリックします。
8. 開いたページで、管理者IPアドレスを追加します。
 - 個々の管理者IPアドレスを追加するには、**IP address**フィールドにIPアドレスを入力します。
 - 管理者IPアドレスの範囲を追加するには、**IP address range**フィールドにIPアドレスの範囲を指定します。

開始アドレスは終了アドレスよりも小さくする必要があります。個別に指定されたIPアドレスは、指定されたIPアドレスの範囲外であってもかまいません。

デフォルトでは、デバイスはIPアドレス範囲1.1.1.1-255.255.255.255からのWebアクセスを許可します。必要に応じてアドレス範囲を編集できます。IPアドレスの変更後も、管理者がWebページにアクセスできることを確認してください。

ベストプラクティスとして、管理者IPアドレスリストを設定して、ユーザークライアントに接続するVLANモニターが存在するネットワークセグメントを含めます。

- IPアドレス範囲からIPアドレスを除外するには、除外するIPアドレスを**Exclude IP address**フィールドに入力します。

除外されたIPアドレスは、指定されたIPアドレス範囲内である必要があります。デバイスは、除外されたIPアドレスからのWebアクセスを許可しません。


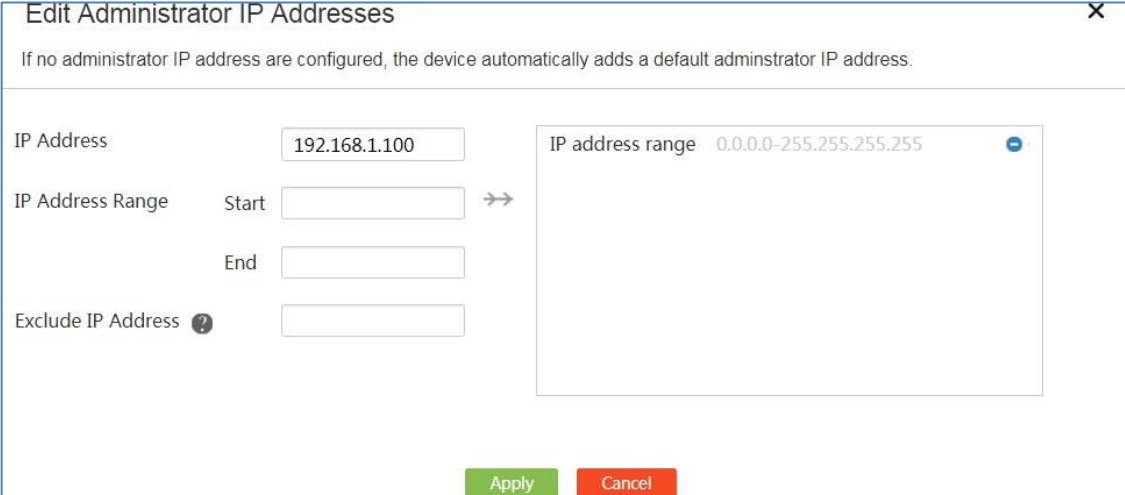
9. アイコン  をクリックして、指定したIPアドレス、アドレス範囲、または除外されたIPアドレスを、右側の管理者IPアドレスリストに追加します。
10. 手順8～9を繰り返して、管理者IPアドレスをさらに追加します。
11. **Apply**をクリックします。

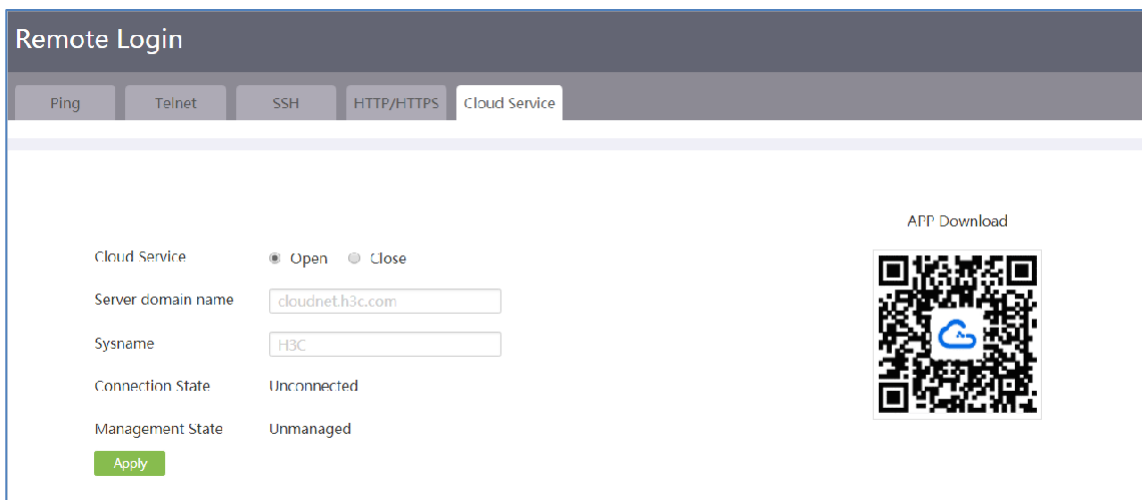
図145 管理者IPアドレスの設定



クラウドサービスを構成する

1. ナビゲーションペインで、**System Tool > Remote Login**を選択します。
2. **Cloud Service**タブをクリックします。
3. **Cloud Service**フィールドから**Open**を選択して、クラウドサービスを有効にします。
4. **Server domain name**フィールドに、クラウドサーバーのドメイン名を入力します。
5. **Sysname**フィールドに、デバイスのシステム名を入力します。
6. **Apply**をクリックします。
7. ページ上のQRコードを携帯で読み取り、Cloudnetアプリをダウンロードしてインストールします。次に、携帯でアプリを開き、クラウドサーバーにログインして、デバイスのリモート管理とメンテナンスを行います。

図146クラウドサービスの設定



構成管理

構成管理の概要

構成管理を使用して、デバイス上の構成ファイルを管理します。構成管理を使用すると、次のタスクを実行できます。

- **View the running configuration:** デバイスの実行コンフィギュレーションを表示します。たとえば、ソフトウェアのバージョンとモニターのIPアドレスを指定するには、ナビゲーションペインから **System Tool > Config Management** を選択し、**View Config** タブをクリックします。
- **Restore the factory defaults:** このタスクは、設定を工場出荷時のデフォルトに復元します。デバイスにスタートアップコンフィギュレーションファイルがない場合、またはスタートアップコンフィギュレーションファイルが壊れている場合は、次のスタートアップ時にデバイスを起動できるように、このタスクを実行します。
- **Save the running configuration:** このタスクでは、実行コンフィギュレーションをメインの next-startup コンフィギュレーションファイル (プライマリ next-startup コンフィギュレーションファイル) に保存します。次の手順を実行します。
タスクは、1つまたは複数の設定タスクを完了した後に実行します。これにより、作成した新しい設定がデバイスのリブート後も維持されます。
- **Restore the configuration from a backup file:** このタスクは、実行コンフィギュレーションをバックアップファイルからのコンフィギュレーションに置き換えます。実行コンフィギュレーションに誤った設定または望ましくない設定が含まれている場合に、このタスクを実行します。
- **Export the running configuration:** このタスクでは、実行コンフィギュレーションをコンフィギュレーションファイルにエクスポートします。将来使用するために実行コンフィギュレーションをバックアップするには、このタスクを実行します。

工場出荷時のデフォルト設定に戻します。

1. ナビゲーションペインで、**System Tool > Config Management** を選択します。
2. **Restore Config** タブをクリックします。
3. **Reset** をクリックします。

図147 工場出荷時のデフォルト設定の復元



4. 表示されたダイアログボックスで、**Yes**をクリックして工場出荷時のデフォルト設定を復元し、システムを強制的にリポートすることを確認します。
その後、デバイスは自動的にリポートし、工場出荷時のデフォルト設定に戻ります。

実行コンフィギュレーションを保存します。

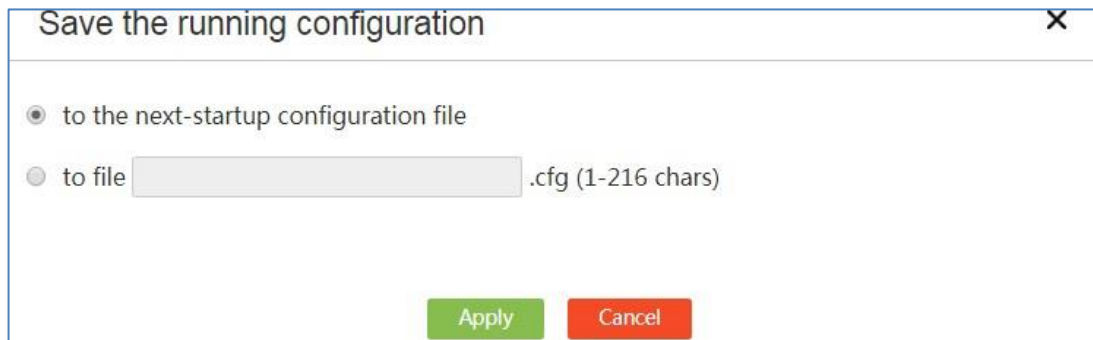
1. ナビゲーションペインで、**System Tool > Config Management**を選択します。
2. **Save Config**タブをクリックします。
3. **Save Running Configuration**をクリックします。

図148 Save Configページ



4. 開いたページで、次のいずれかの方法を使用して、メインのnext-startupコンフィギュレーションファイルに実行コンフィギュレーションを保存します。
 - **to the next-startup configuration file:** このオプションを選択すると、ファイルを選択できなくなります。実行コンフィギュレーションは、ストレージメディアのルートディレクトリにあるファイルに直接保存され、このファイルがメインのnext-startupコンフィギュレーションファイルとして指定されます。
 - **to file:** このオプションを選択すると、実行コンフィギュレーションを保存するファイルを選択し、そのファイルをメインのnext-startupコンフィギュレーションファイルとして指定できます。

図149 実行コンフィギュレーションの保存

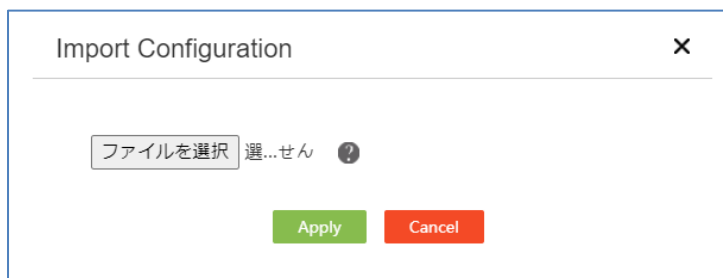


5. **Apply**をクリックします。

バックアップファイルから構成を復元する

1. ナビゲーションペインで、**System Tool > Config Management**を選択します。
2. **Save Config**タブをクリックします。
3. **Import Configuration**をクリックします。
4. 開いたページで、**Choose File**をクリックしてバックアップコンフィギュレーションファイルを選択します。

図150 バックアップファイルの選択



5. **Apply**をクリックします。
6. デバイスをリブートします。

実行コンフィギュレーションのエクスポート

1. ナビゲーションペインで、**System Tool > Config Management**を選択します。
2. **Save Config**タブをクリックします。
3. 実行コンフィギュレーションをローカルPCにエクスポートするには、**Export Running Configuration**をクリックします。

ソフトウェアのアップグレード

はじめに

ソフトウェアアップグレードを使用して、デバイスソフトウェアをアップグレードし、デバイス上のファイルを管理します。デバイスソフトウェアをアップグレードすることで、新機能を追加したり、バグを修正したりできま

す。

次の方法を使用して、デバイスソフトウェアをアップグレードできます。

- **Manual upgrade:** デバイスにアップロードされたローカルIPEファイルを使用して、デバイスソフトウェアをアップグレードします。
- **Auto upgrade:** クラウドプラットフォームから最新のソフトウェアイメージファイルをダウンロードして、デバイスソフトウェアをアップグレードします。

ファイル管理では、次の操作をサポートしています。

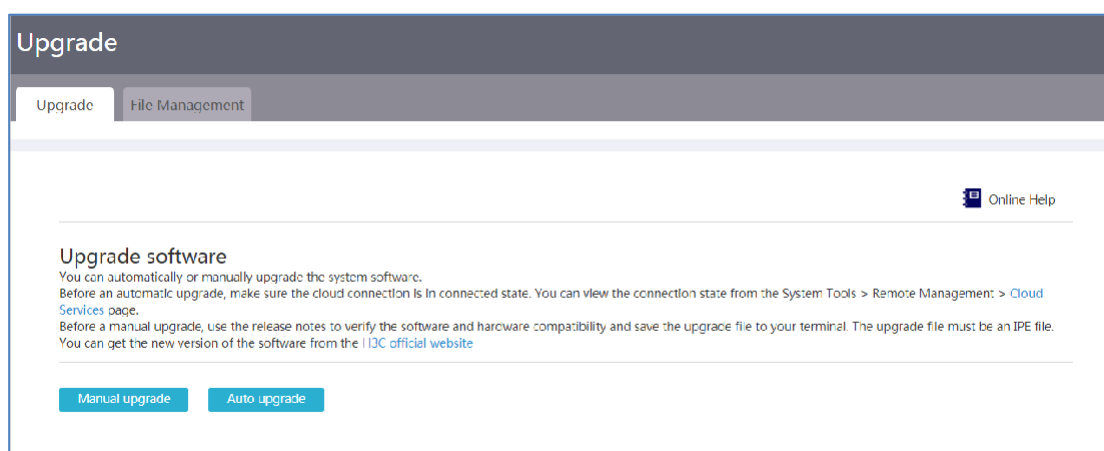
- **Upload:** デバイスにファイルをアップロードします。たとえば、.ipeファイルをデバイスにアップロードしてから、そのファイルを使用してデバイス上のソフトウェアをアップグレードできます。
- **Delete:** 重要でないファイルをデバイスから削除して、ファイルによって使用されているストレージ領域を解放します。
- **Download:** データのバックアップまたは分析のために、デバイスからPCにファイルをダウンロードします。

デバイスソフトウェアのアップグレード

デバイスソフトウェアを手動でアップグレードする

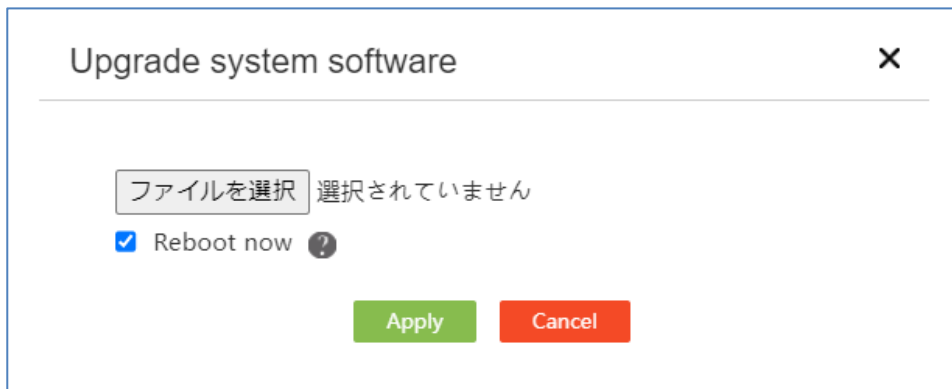
1. ナビゲーションツリーから、**System Tool > Upgrade**を選択します。
2. **Upgrade**タブで、**Manual upgrade**をクリックします。

図151 アップグレード



3. **Select File**をクリックし、目的のIPEファイルを選択します。
4. デバイスに新しいソフトウェアをすぐにロードするには、**Reboot Now**を選択します。
5. **OK**をクリックします。

図152 システムソフトウェアの手動アップグレード



デバイスソフトウェアを自動的にアップグレードする

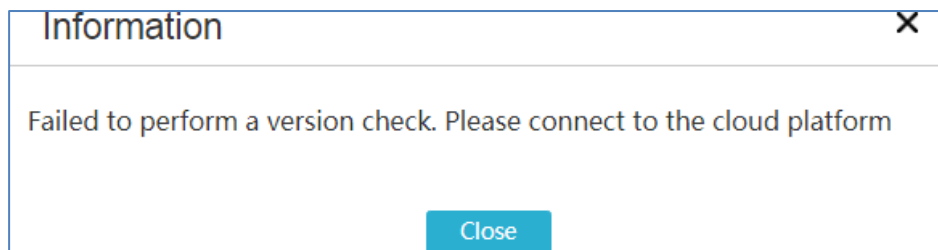
- 制限事項およびガイドライン

自動アップグレードの前に、クラウド接続が接続状態であることを確認します。接続状態は、**System Tool > Remote Management > Cloud Services**ページで確認できます。

- 手順

1. ナビゲーションツリーから、**System Tool > Upgrade**を選択します。
2. **Upgrade**タブで、**Auto upgrade**をクリックして、自動アップグレード用の最新のソフトウェアバージョンをクラウドプラットフォームからダウンロードします。

図153 システムソフトウェアの自動アップグレード

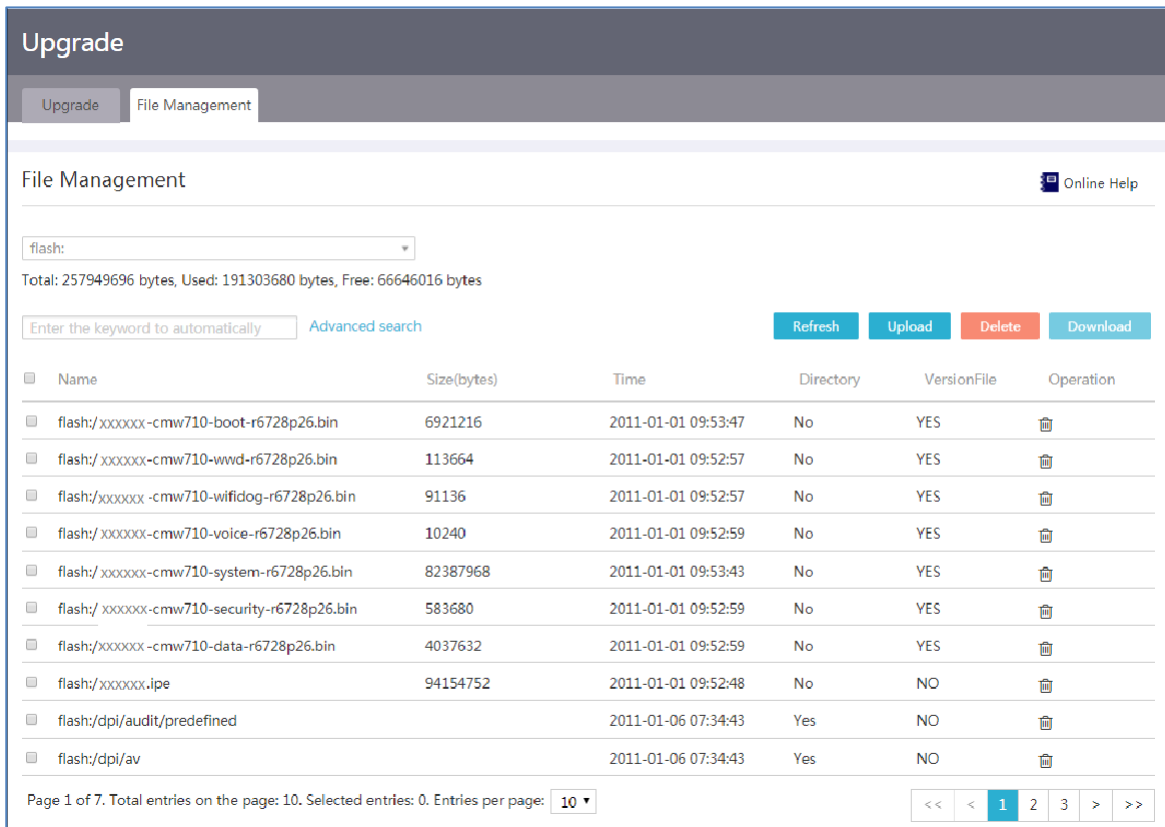


ファイルの管理

ファイルをアップロードする

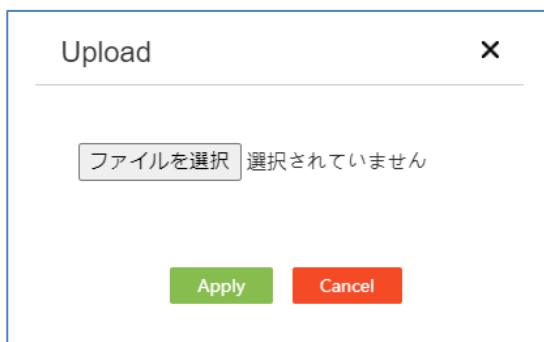
1. ナビゲーションツリーから、**System Tool > Upgrade**を選択します。
2. **File Management**タブをクリックします。

図154 ファイル管理



3. Uploadをクリックします。
4. Select File,をクリックし、アップロードするファイルを選択します。
5. Applyをクリックします。

図155 ファイルのアップロード



ファイルを削除する

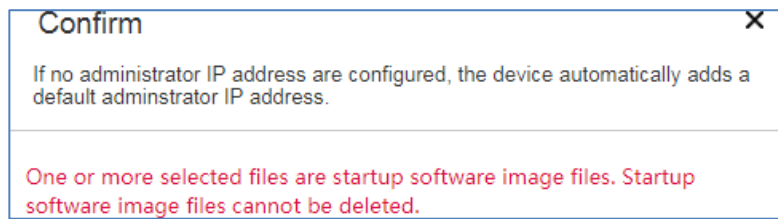
制限事項およびガイドライン

デバイスで使用されているイメージファイルは削除しないでください。ファイルを削除すると、デバイスが正常に動作しなくなります。

手順

1. ナビゲーションツリーから、**System Tool > Upgrade**を選択します。
2. **File System**タブをクリックします。
3. 削除するファイル(複数可)を選択します。
4. **Delete**をクリックします。

図156 ファイルの削除



ファイルのダウンロード

1. ナビゲーションツリーから、**System Tool > Upgrade**を選択します。
2. File Systemタブをクリックします。
3. ダウンロードするファイル(複数可)を選択します。
4. **Download**をクリックし、ダウンロード先のパスを選択します。

ライセンス管理

ライセンス管理について

デバイスでライセンスベースの機能を使用するには、ライセンスキーを購入し、それを使用してアクティベーションファイルを要求し、アクティベーションファイルをデバイスにインストールする必要があります。ライセンスが必要な機能を表示するには、**Licenses and features**タブをクリックします。

注:

アクティベーションファイルは、デバイスのWebモニターではライセンスファイルとも呼ばれます。

ライセンス管理の制限事項とガイドライン

デバイスでライセンスを管理している間は、他のユーザーがライセンス管理タスクを実行していないことを確認してください。

ライセンスが必要な機能を表示する

1. ナビゲーションペインで、**System Tool > License Management**を選択します。
2. **Licenses and features**タブをクリックします。
3. ライセンスベースの機能、ライセンスステータス、およびライセンスタイプを表示します。
 - **Feature name:** 使用する前にライセンスが必要な機能を表示します。
 - **Licensed or Not:** 機能のライセンス状態を表示します。
 - **N:** ライセンスされていません。
 - **Y:** ライセンス済み。
 - **Status:** ライセンスの種類を表示します。
 - **Formal:** 購入したライセンス。この状態は、有効な正式ライセンスがインストールされていることを示します。
 - **Trial:** 試用ライセンス。この状態は、有効な試技ライセンスがインストールされていることを示します。

示します。

- **Pre-licensed:** プレインストールされたライセンス。この状態は、有効なプレインストールされたライセンスがインストールされていることを示します。

機能にライセンスが適用されていない場合、このフィールドにはハイフン(-)が表示されます。機能を使用するには、有効なライセンスをインストールする必要があります。

図157 ライセンスと機能

The screenshot shows the 'License Management' interface with the 'Licenses and features' tab selected. It displays a table with the following data:

Feature name	Licensed or Not	Status
ACG	N	-
APMGR	Y	Trial
IPS	N	-
SSLVPN	N	-
UFLT	N	-
WEB-CACHE	N	-
pkg_data	N	-
pkg_security	N	-
pkg_voice	N	-

Page 1 of 1. Total entries on the page: 9. Selected entries: 0. Entries per page: 10

ライセンスストレージを圧縮する

このタスクについて

ライセンスストレージを圧縮して、期限切れのライセンス情報を削除します。この操作により、新しいライセンスをインストールするための十分なストレージ領域が確保されます。

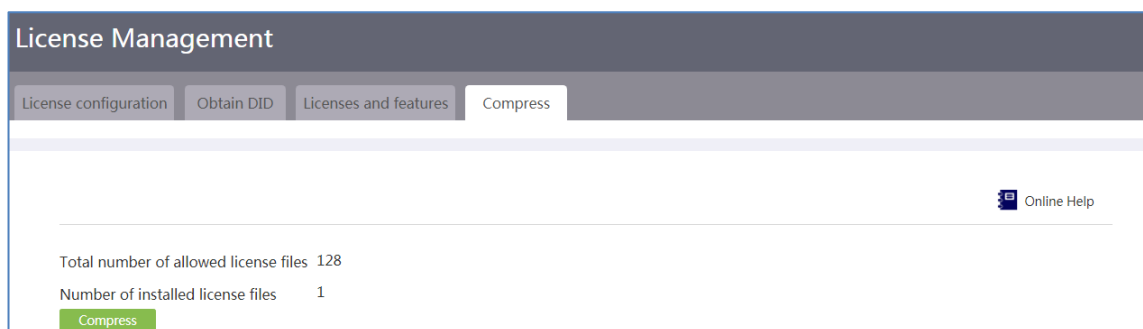
制限事項およびガイドライン

有効期限が切れたライセンスがデバイスに存在する場合、圧縮操作によってDIDが変更されます。圧縮を実行する前に、古いDIDに登録されているすべてのライセンスがインストールされていることを確認してください。圧縮後は、このようなライセンスをインストールできなくなります。

手順

1. ナビゲーションペインで、**System Tool > License Management**を選択します。
2. **Compress**タブをクリックします。
3. 許可されているアクティベーションファイルの残りの数が、インストールされるアクティベーションファイルの数よりも少ない場合は、開いたページで**Compress**をクリックできます。
許可されたアクティベーションファイルの残りの数=許可されたアクティベーションファイルの合計数-インストールされたアクティベーションファイルの数
4. **Apply** をクリックします。

図158 ライセンスストレージの圧縮



アクティベーションファイルを要求する

制限事項およびガイドライン

誤って失われたり削除されたりしないように、アクティベーションファイルを適切に保存してバックアップします。ライセンスの失敗を避けるために、アクティベーションファイルの名前や内容を変更しないでください。

H3Cライセンス管理プラットフォームに正しい情報を入力してもアクティベーションファイルを取得できない場合は、H3Cサポートに連絡してください。

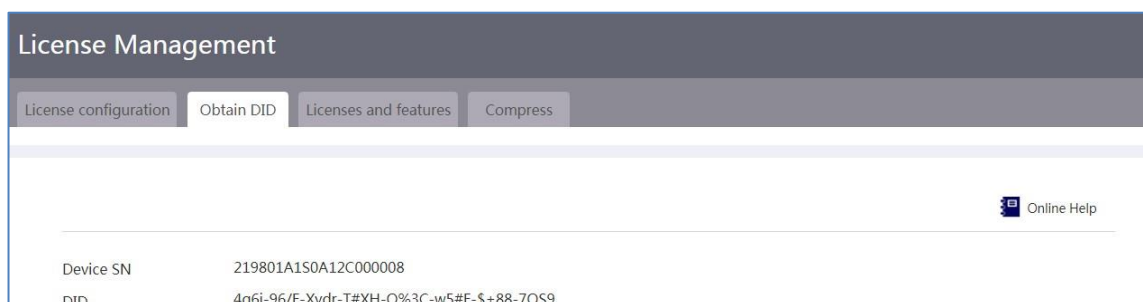
前提条件

ソフトウェアライセンス証明書を購入して、ライセンスキーを取得します。

手順

1. ナビゲーションペインで、**System Tool > License Management**を選択します。
2. **Obtain DID**タブをクリックします。
3. デバイスのSNとDIDを取得します。
4. H3C License Management Platformにログインします。
<https://new-licensing.h3c.com/website/anonymous/navIndex/en-US/activate/input-license>を使用して、アクティベーションファイルを取得します。アクティベーションファイルの要求の詳細については、『h3c Switches and Routers Licensing Guide』を参照してください。

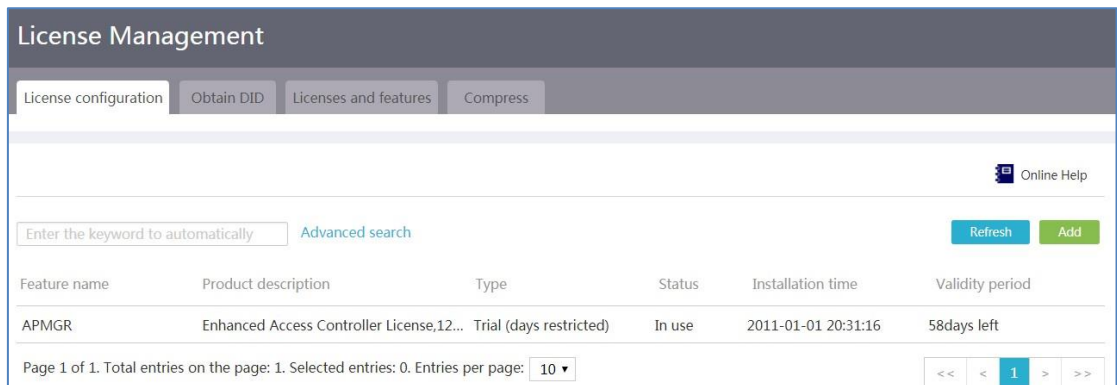
図159 DIDの取得



ライセンスをインストールする

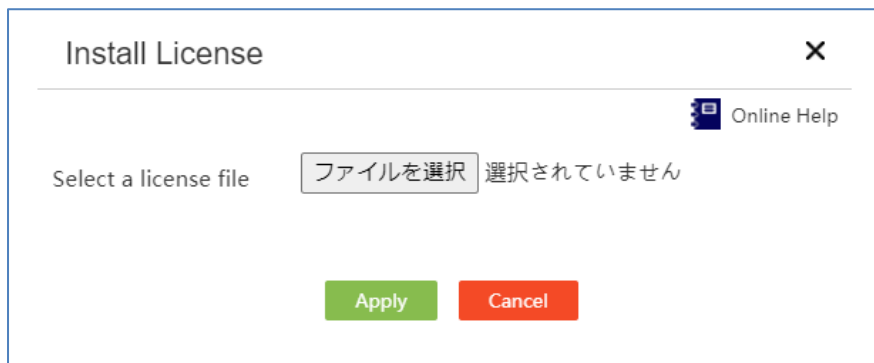
1. ナビゲーションペインで、**System Tool > License Management**を選択します。
2. **License configuration**タブで、**Add**をクリックします。

図160ライセンス設定



3. 表示されたダイアログボックスで、アクティベーションファイルを選択し、**Apply**をクリックします。

図161 ライセンスのインストール



再起動

リブートの概要

デバイスをただちに、またはスケジュールした時刻にリポートするには、次のタスクを実行します。

今すぐ再起動

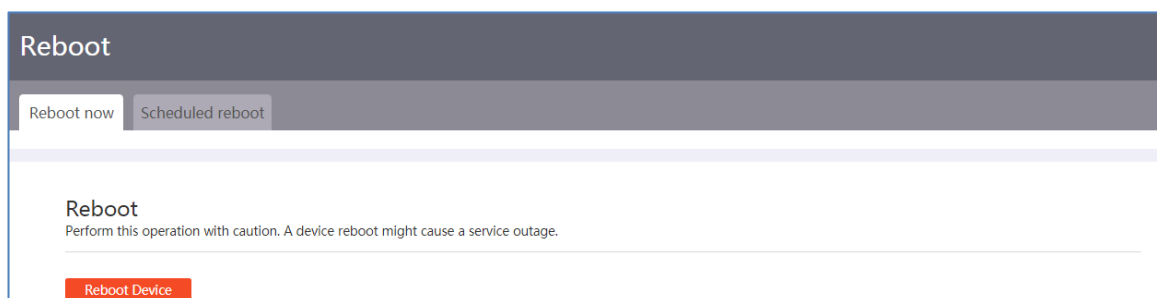
制限事項およびガイドライン

デバイスを再起動すると、サービスが中断されます。この操作は注意して実行してください。

手順

1. ナビゲーションペインで、**System Tool > Reboot**を選択します。
2. **Reboot now**タブで、**Reboot Device**をクリックします。
3. 表示されたダイアログボックスで、次のいずれかのオプションを選択します。
 - **Save running configuration before the reboot**
 - **Force reboot the device immediately without performing any software check**
4. **Apply**をクリックします。

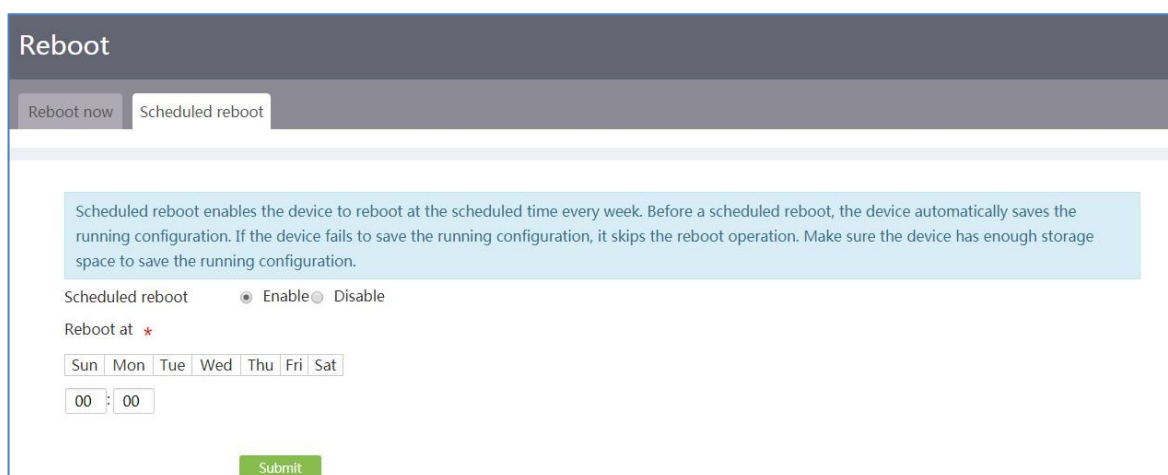
図162 デバイスの再起動



スケジュールされた再起動

1. ナビゲーションペインで、**System Tool > Reboot**を選択します。
2. **Scheduled reboot**タブをクリックします。
3. **Scheduled reboot**フィールドで、**Enable**を選択します。
4. **Reboot at**フィールドで、毎週のデバイスの再起動時間を指定します。
5. **Submit**をクリックします。デバイスはスケジュールされた時刻に再起動します。

図163 リブートのスケジューリング



システムログ

システムログの概要

動作中、デバイスはシステムログを生成し、管理者が設定した設定、デバイスの状態の変更、およびデバイス上の重要なイベントを記録します。システムログに基づいて、デバイスのパフォーマンスを監視し、ネットワークの問題をトラブルシューティングできます。

システムログをログサーバーに送信して一元管理することも、Webページでログエントリを直接表示することもできます。

ログは、表1に示すように、重要度の高い順に0～7の8つの重要度レベルに分類されます。

表1 ログレベル

重要度の値	レベル	説明
0	緊急	システムは使用できません。たとえば、システム認証の期限が切れています。
1	警告	モニター上のトラフィックが上限を超えた場合など、すぐに対処する必要があります。
2	クリティカル	クリティカルな状態。たとえば、デバイスの温度が上限を超えている、電源モジュールが故障している、ファントレイが故障しているなどです。
3	エラー	エラー状態。たとえば、リンクの状態が変化した場合など。
4	警告	警告状態。たとえば、モニターが切断されたり、メモリリソースが使い果たされたりします。
5	お知らせ	正常であるが重大な状態。たとえば、端末がデバイスにログインしたり、デバイスがリポートしたりします。
6	情報	情報メッセージ。たとえば、コマンドやping操作が実行されます。
7	デバッグ中	デバッグメッセージ。

システムログをログサーバーに送信する


前提条件

デバイスとログサーバーが相互に到達できることを確認します。

手順

1. ナビゲーションペインで、**System Tool > System Log**を選択します。
2. **System Log**タブで、**System Log**を選択し、ログサーバーのIPアドレスまたはホスト名を入力します。
3. **Apply**をクリックします。

図164 システムログのログサーバーへの送信



The screenshot shows a web interface for 'System Log'. At the top, there is a dark header with the text 'System Log'. Below the header, there is a form with a checkbox labeled 'Send to a log server' which is checked. To the right of the checkbox is a red asterisk. Next to the checkbox is a text input field containing '127.0.0.1'. To the right of the input field is the text '(IP address or host name)'. In the top right corner of the form area, there is a small icon and the text 'Online Help'. At the bottom left of the form area, there is a green button labeled 'Apply'.

Webページでシステムログを表示する

1. ナビゲーションペインで、**System Tool > System Log**を選択します。
2. **System Log**タブでは、ログエントリーが時間、レベルおよび説明情報とともにリストされます。検索条件を指定すると、特定のログエントリーを表示できます。
3. **Export**をクリックして、ログインしたPCにログエントリーをエクスポートします。

図165 システムログの表示

The screenshot shows the 'System Log' interface. At the top, there is a search bar with the text 'Enter the keyword to automatically' and a button for 'Advanced search'. Below this is a table of log entries. The table has three columns: 'Time', 'Level', and 'Description'. The entries are as follows:

Time	Level	Description
2011-01-01 03:29:	Notification	-EventIndex=2-CommandSource=snmp-ConfigSource=startup-ConfigDestination=running; Configuration changed.
2011-01-01 03:23:	Informational	User (admin, 192.168.200.28, session ID) performed an edit-config operation: message ID=, operation result=Failed, XPat...
2011-01-01 03:22:	Notification	admin logged out from 192.168.100.27.
2011-01-01 03:22:	Informational	user admin from 192.168.100.27, session id 2, idle timed out.
2011-01-01 03:19:	Notification	-EventIndex=1-CommandSource=snmp-ConfigSource=startup-ConfigDestination=running; Configuration changed.
2011-01-01 03:15:	Notification	admin logged in from 192.168.100.27.
2011-01-01 03:02:	Notification	admin logged in from 192.168.100.27.
2011-01-01 03:00:	Notification	admin logged out from 192.168.100.27.
2011-01-01 03:00:	Informational	user admin from 192.168.100.27, session id 2, idle timed out.
2011-01-01 02:53:	Notification	admin 从 192.168.200.28 登录成功.

At the bottom of the log view, there is a pagination control showing 'Page 1 of 3. Total entries on the page: 10. Selected entries: 0. Entries per page: 10' and navigation buttons for '<<', '<', '1', '2', '3', '>', and '>>'.

SmartMC

構成ウィザード

SmartMCの紹介

Smart Management Center(SmartMC)は、ネットワークエッジに分散したネットワークデバイスを一元的に管理および維持します。SmartMCネットワークでは、1つのデバイスがコマンダーとして機能し、メンバーとして機能する残りのデバイスを管理します。

このページでは、デバイスロールをコマンダーに設定できます。コマンダーを指定した後、**Intelligent Management**、**Intelligent O&M**および**Visibility**の各ページにアクセスし、これらのページに用意されている機能を使用してメンバーを一様に管理できます。コマンダーを設定すると、**Configure Wizard**ページにアクセスできなくなります。

メンバーは、SmartMCネットワークに自動的に参加できます。メンバーを手動で追加するには、**Visibility > Topology**ページにアクセスし、**Add**をクリックします。メンバーデバイスの場合、**Configuration Wizard**ページ、**Intelligent Management > Roles**ページ、および**Intelligent Management > Disable SmartMC**ページにアクセスできます。デバイスロールをメンバーからコマンダーに切り替えるには、**Configuration Wizard**ページまたは**Intelligent Management > Roles**ページにアクセスします。

制限事項およびガイドライン

SmartMCのネットワークにはコマンダーが1人しかいません。

メンバーがSmartMCネットワークに自動的に参加するには、最初にコマンダーを設定してから、何も設定せずにメンバーを開始する必要があります。

手順

1. ナビゲーションペインで、**Configuration Wizard**を選択します。

2. **Management IP address**タブをクリックします。
3. **Configure management IP address**領域で、デバイスVLANモニター1のIPアドレスを入力します。

VLANモニター1のIPアドレスを適用すると、SmartMCネットワークがVLAN 1に作成されます。VLANモニター1のIPアドレスが設定されている場合は、そのアドレスを管理IPアドレスとして直接使用できます。

4. **Mask length**領域で、管理IPアドレスのマスク長を指定します。

図166 管理IPアドレスの設定

The screenshot shows the 'Configuration Wizard' interface for 'Management IP address'. The 'Configure management IP address' field is set to '172.16.10.1' and the 'Mask length' field is set to '23'. A 'Next' button is located at the bottom left of the form area.

5. **Next**をクリックします。
Outgoing interfaceタブが表示されます。

デバイスとVLAN 1(SmartMCネットワークが存在する場所)が同じネットワークセグメントにない場合、デバイスを使用してメンバーのWebモニターに直接アクセスすることはできません。この問題に対処するには、デバイスに接続するコマンダーモニターを発信モニターとして設定し、**Visibility > Typology**ページにアクセスして、トポロジーマップでメンバーを選択し、そのメンバーの**Log in to Web Interface**をクリックします。

6. **Outgoing interface**領域で、デバイスに接続するモニターを発信モニターとして指定します。

図167 発信モニターの設定

The screenshot shows the 'Configuration Wizard' interface for 'Outgoing interface'. The 'Outgoing interface' dropdown menu is set to 'GigabitEthernet0/0'. 'Previous' and 'Next' buttons are located at the bottom of the form area.

7. **Next**をクリックします。

Management userページが表示されます。

管理ユーザーはコマンドのローカルユーザーです。指定されたユーザーが存在しない場合、システムはユーザーをローカルユーザーとして作成します。

8. Username領域に、ローカルユーザー名を入力します。
9. Password領域に、ローカルユーザーログインのパスワードを入力します。

図168 管理ユーザーの構成

The screenshot shows the 'Management user' step of the Configuration Wizard. The interface includes a sidebar with the H3C logo and 'Configuration Wizard' text. The main content area has a progress bar with four steps: 'Management IP address', 'Outgoing interface', 'Management user', and 'Commit'. The 'Management user' step is active. Below the progress bar, there are two input fields: 'Username' with a character count of '(1-55 :chars)' and 'Password' with a character count of '(1-63 :chars)'. At the bottom, there are 'Previous' and 'Next' buttons.

10. Nextをクリックします。
Commitページが表示されます。
11. 設定が正しいことを確認し、Certainをクリックします。

図169 設定の完了

The screenshot shows the 'Commit' step of the Configuration Wizard. The progress bar now highlights the 'Commit' step. The main content area displays a summary of the configuration: 'Management IP address : 172.16.10.1', 'Mask length : 23', 'Outgoing interface : GigabitEthernet0/0', and 'Username :'. At the bottom, there are 'Previous' and 'Certain' buttons.

インテリジェントな管理

デバイスの役割の設定

デバイスロール設定の概要

デバイスロールをコマンダーまたはメンバーに切り替えるには、次の作業を実行します。

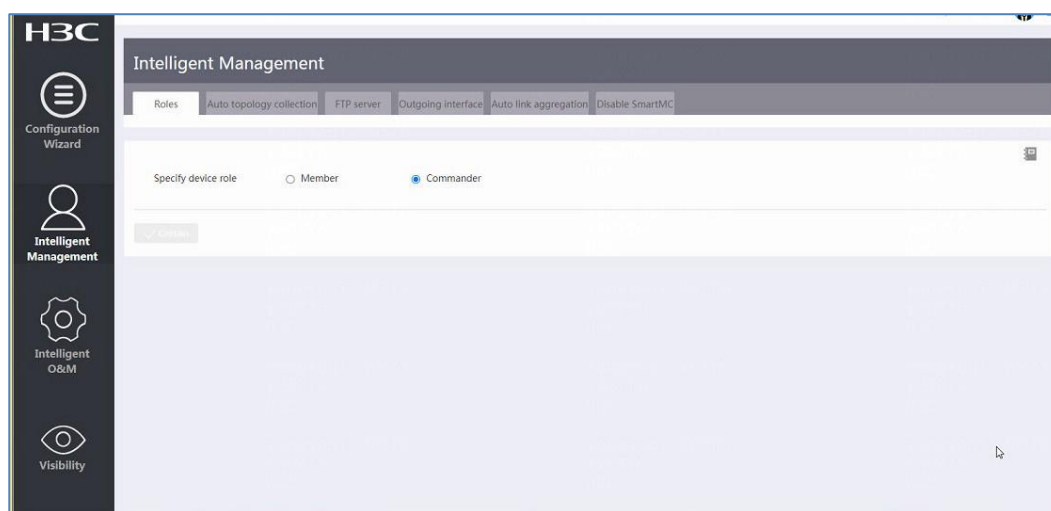
制限事項およびガイドライン

デバイスの誤ったコンフィギュレーションファイルをダウンロードしないようにするには、デバイスロールをコマンダーからメンバーに切り替えた後で、元のコマンダーのバックアップコンフィギュレーションファイルをFTPサーバーから削除します。

手順

1. ナビゲーションペインで、**Intelligent Management**を選択します。
2. **Roles**タブをクリックします。
3. **Specify device role**領域で、**Commander**または**Member**を選択します。
4. **Certain**をクリックします。

図170 デバイスの役割の指定



発信モニターの設定

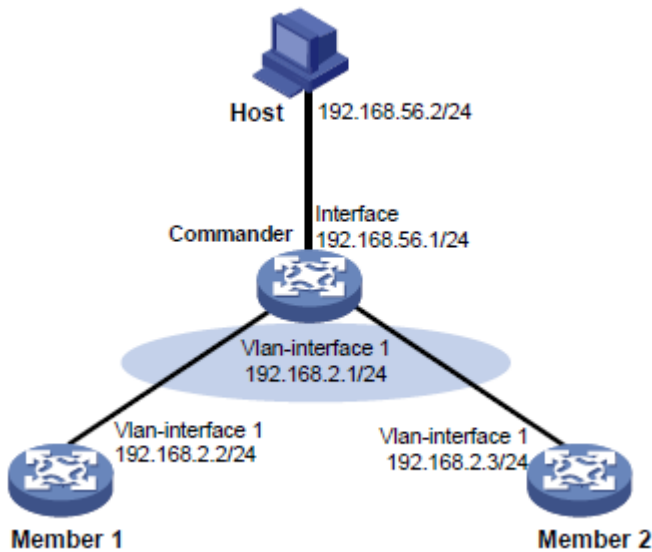
発信モニター設定の概要

発信モニターは、コマンダー上のレイヤー3イーサネットモニターです。デバイスがメンバーのWebモニターに直接アクセスするために使用されます。

図171に示すように、ホストはモニターを介してコマンダーに接続し、ネットワークセグメントは192.168.56.0/24です。SmartMCネットワークは、ネットワークセグメント192.168.2.0/24に存在するVLAN 1にあります。この場合、ホストはコマンダーのWebモニターにアクセスできますが、メンバーのWebモニターにはアクセスできません。

この問題に対処するには、SmartMCネットワークの発信モニターとしてモニターを設定します。設定後、メンバーのWebモニターにアクセスするには、コマンダーのモニターにアクセスし、**Visibility > Typology**を選択し、タイプマップでメンバーを選択して、**Log in to Web interface**をクリックします。この場合、コマンダーはメンバードレスをOutgoing_IP_address:Port_number形式の新しいアドレスにミラーリングし、新しいアドレスを使用してメンバーのWebモニターにアクセスできます。

図171 ネットワークダイアグラム



制限事項およびガイドライン

SmartMCネットワークはVLAN 1に存在し、SmartMCネットワークの発信モニターとしてVLAN-interface 1を設定できません。

手順



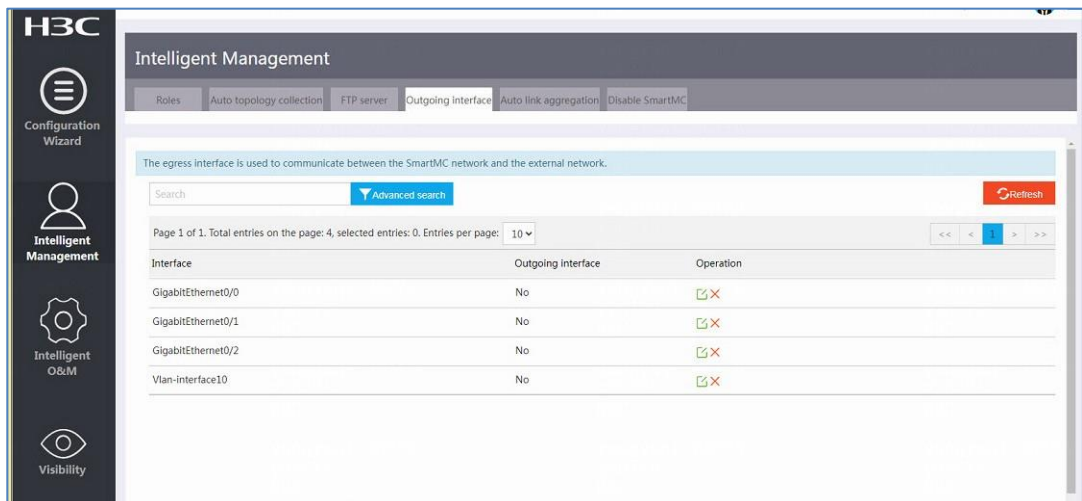
1. ナビゲーションペインで、**Intelligent Management**を選択します。
2. **Outgoing interface**タブをクリックします。
3. モニターを発信モニターとして設定するには、リストからモニターの**Operation**カラムにあるアイコンをクリックします。
4. モニターを削除するには、リストからモニターの**Operation**カラムにあるアイコンをクリックします。

図172 発信モニターの設定



インテリジェントO&M

デバイスのアップグレード

デバイスアップグレードの概要

コマンダーからスタートアップソフトウェアとメンバーのコンフィギュレーションファイルをアップグレードするには、次の作業を実行します。

メンバーがFTPサーバーからアップグレードファイルをダウンロードしているときに、ダウンロードをキャンセルするには、**Cancel Downloading**をクリックします。


アップグレードの進行中にアップグレードを取り消すには、**Cancel Upgrade**をクリックします。

制限事項およびガイドライン

アップグレードの前に、FTPサーバーが設定されていることを確認します。**Intelligent Management > FTP server**ページにアクセスして、設定を構成できます。

アップグレードの前に、アップグレードファイルがFTPサーバーに保存されていることを確認します。アップグレード中、メンバーはFTPサーバーからファイルを自動的にダウンロードします。

アップグレードファイルを設定する

1. ナビゲーションペインで、**Intelligent O&M**を選択します。
2. **Upgrade device**タブをクリックします。
3. アップグレードファイルを設定するには、リストからデバイスの**Operation**カラムにあるアイコン  をクリックします。
4. 表示されたページで、アップグレードファイルの種類を指定します。
 - IPEファイルを選択した場合は、IPEファイル名を入力します。
 - BINファイルを選択した場合は、ブートパッケージ名とシステムパッケージ名を入力します。
 - 設定ファイルを選択した場合は、設定ファイル名を入力します。
5. アップグレードするすべてのデバイスのアップグレードファイルを設定するには、前の手順を繰り返します。

デバイスのアップグレード

1. ナビゲーションペインで、**Intelligent O&M**を選択します。
2. **Upgrade device**タブをクリックします。
3. リストからアップグレードするデバイスを選択します。
4. **Upgrade**をクリックします。
5. 表示されたページで、アップグレードするオブジェクトとアップグレード時間を指定します。
 - アップグレードの遅延を選択する場合は、遅延時間を指定します。
 - スケジュールされた時刻にアップグレードを開始することを選択した場合は、アップグレード時刻を指定します。
6. **Certain**をクリックします。

アップグレードのキャンセル

1. ナビゲーションペインで、**Intelligent O&M**を選択します。
2. **Upgrade device**タブをクリックします。
3. アップグレードをキャンセルするデバイスを選択します。

4. **Cancel upgrade**をクリックします。

VLANをワンステップで導入

ワンステップでのVLAN導入の概要

次の基準を満たすメンバー上のすべてのポートを指定したVLANに割り当てるには、次の作業を実行します。

- ポートは他のメンバーまたはコマンダーに接続されていません。
- ポートはアクセスポートです。

制限事項およびガイドライン

- オフラインメンバーに接続されているアクセスポートは、指定されたVLANに割り当てることができません。
- 1つ以上のアクセスポートをVLANに割り当てることができない場合、メンバーのVLAN作成は失敗します。VLANの作成に失敗した場合、アクセスポートのVLANメンバーシップは、VLANが作成される前の状態に復元されます。
- メンバーのVLANの作成に失敗しても、他のメンバーのVLAN作成には影響しません。

手順

1. ナビゲーションペインで、**Intelligent O&M**を選択します。
2. **Deploy VLAN in one step**タブをクリックします。
3. **Please select operation object**エリアで、**Members**または**SmartMCグループ**を選択します。
4. 展開するメンバーまたはSmartMCグループをリストから選択し、**Deploy VLAN in one step**をクリックします。
5. 開いたページで、VLAN IDを入力します。
6. **Certain**をクリックします。
7. 設定結果を表示するには、**View deployment result**をクリックします。

インテリジェントなポート識別

インテリジェントポートIDの概要

この機能により、コマンダーは、指定されたバッチファイル内の設定を管理し、APまたはIP Phoneがネットワークにアクセスするポートに展開できます。

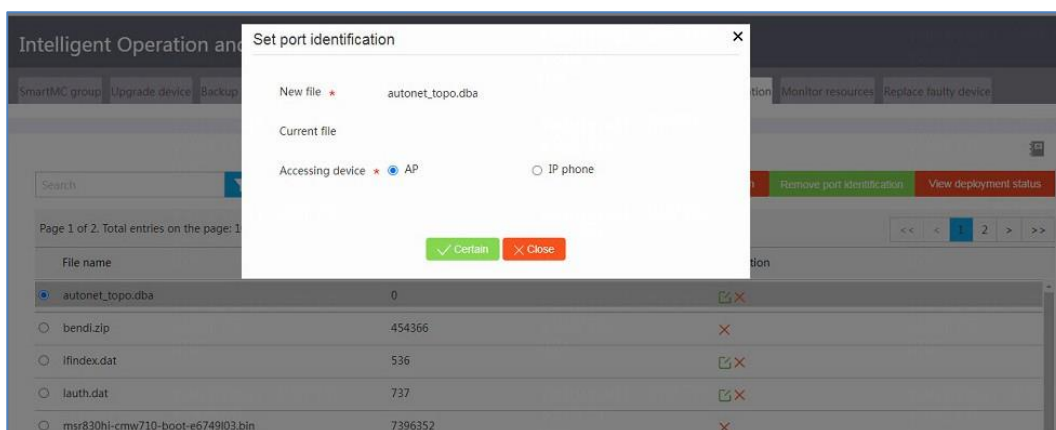
制限事項およびガイドライン

- 設定エラーを回避するには、バッチファイル内のすべてのコマンドがモニタービューで実行できることを確認します。
- バッチファイルには、最大8190文字を含めることができます。
- バッチファイルを指定するときは、ファイル名が正しいことを確認してください。これは、ファイル名が正しいかどうかをシステムが検証しないためです。バッチファイルを指定した後は、ファイルを削除したり、ファイルの名前を変更しないでください。
- 設定の展開前に、システムはポート設定をデフォルト設定に復元します。
- APまたはIP Phoneがポートから切断されても、ポートの設定は変更されません。

ポートIDの設定

1. ナビゲーションペインで、**Intelligent O&M**を選択します。
2. **Intelligent port identification**タブをクリックします。
3. **Create**をクリックし、ポートのバッチ構成ファイルを作成します。作成後、ファイルリストが自動的にリフレッシュされます。バッチファイルがすでに存在する場合は、次の手順に直接進みます。
4. リストからバッチファイルを選択します。
5. **Set port identification**をクリックします。
6. **Accessing device**エリアで、**AP**または**IP phone**を選択します。
7. **Certain**をクリックします。

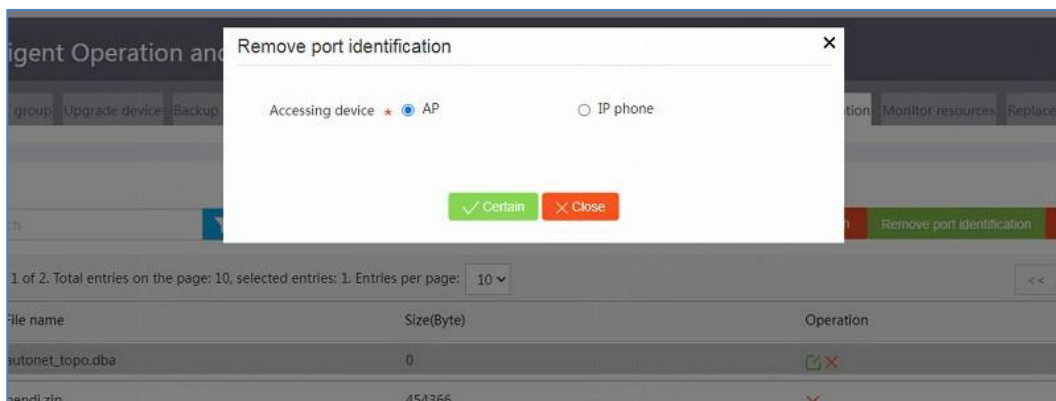
図173 ポートIDの設定



ポートIDの削除

1. ナビゲーションペインで、**Intelligent O&M**を選択します。
2. **Intelligent port identification**タブをクリックします。
3. **Remove port identification**をクリックします。
4. 表示されたページの**Accessing device**領域で、**AP**または**IP phone**を選択します。
5. **Certain**をクリックします。

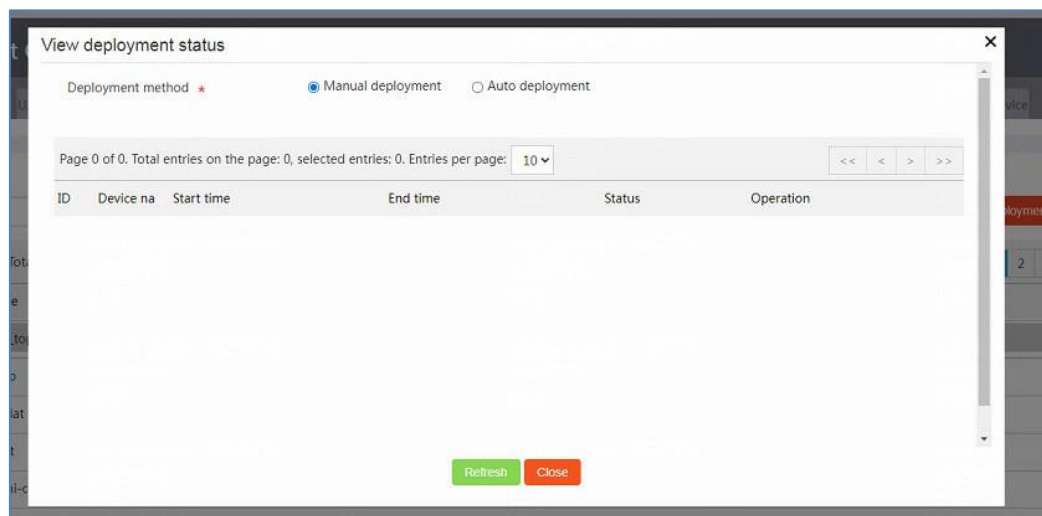
図174 ポートIDの削除



展開ステータスの表示

1. ナビゲーションペインで、**Intelligent O&M**を選択します。
2. **Intelligent port identification**タブをクリックします。
3. **View deployment status**をクリックします。
4. 開いたページの**Deployment method**領域で、**Manual deployment**または**Auto deployment**を選択します。
5. **Auto deployment**を選択した場合は、**Accessing device**で**AP**または**IP phone**を選択します。

図175 ポート設定状態の表示



障害のあるデバイスを交換する

障害のあるデバイスの交換の概要

自動交換または手動交換を使用して、障害のあるメンバーを交換できます。

- 手動交換を実行するには、新しいメンバーと障害のあるメンバーのデバイスタイプが同じである必要があります。
- 自動置換を実行するには、次の要件を満たす必要があります。
 - デバイスタイプは、新しいメンバーと障害のあるメンバーで同じです。
 - LLDP情報は、新しいメンバーと障害のあるメンバーで同じです。
 - 新しいメンバーに対して取得されたLLDP情報は、1時間以内に3回連続して同じです。

コマンダーは、障害のあるメンバーの構成ファイルをFTPサーバーからダウンロードするように新しいメンバーに指示します。構成ファイルをダウンロードした後、新しいメンバーは構成ファイルを実行して置換を完了します。

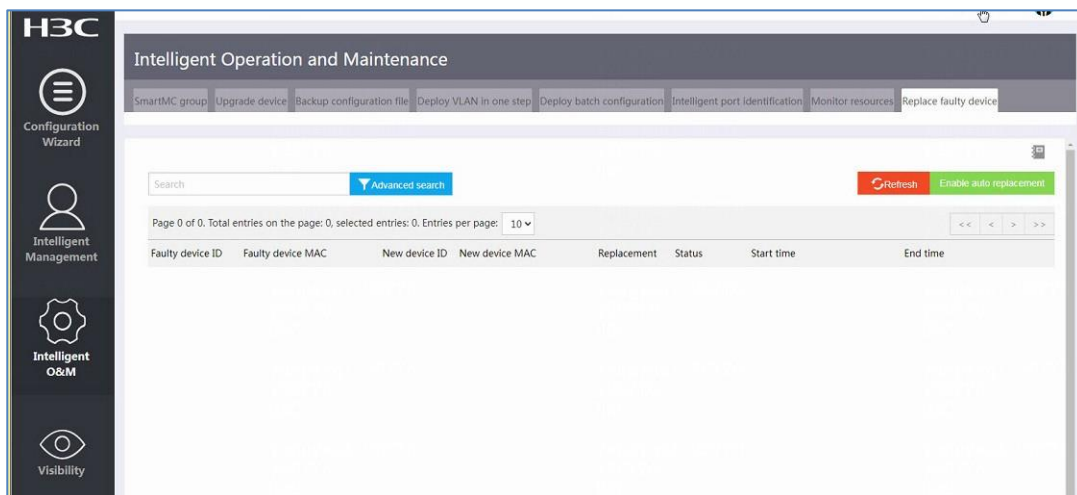
制限事項およびガイドライン

- 1つ以上のデバイスに障害がある場合、コマンダーは自動交換を実行できず、手動交換が必要になります。
- 新しいメンバーのスタックスプリットを回避するには、スタックデバイスを交換するときに、新しいメンバーと障害のあるメンバーのスタック設定と物理接続が同じであることを確認します。

障害のあるデバイスを自動的に交換する

1. ナビゲーションペインで、**Intelligent O&M**を選択します。
2. **Replace faulty device**タブをクリックします。
3. **Enable auto replacement**をクリックします。
4. 障害のあるメンバーがインストールされていた場所に新しいメンバーをインストールし、デバイスを起動します。

図176 障害のあるメンバーの自動置換



障害のあるメンバーを手動で交換する

1. ナビゲーションペインで、**Intelligent O&M**を選択します。
2. **Replace faulty device**タブをクリックします。
3. 障害のあるメンバーがインストールされていた場所に新しいメンバーをインストールし、デバイスを起動します。
4. ナビゲーションペインで、**Visibility**をクリックします。
5. **Typology**タブをクリックします。
6. **Manual replacement**をクリックします。
7. 開いたページで、デバイスモデル、障害のあるデバイス、および新しいデバイスを指定します。
8. **Certain**をクリックします。

図177 障害のあるメンバーの手動での交換








The image shows a 'Manual Replacement' dialog box with a close button (X) in the top right corner. It contains three dropdown menus, each with a red asterisk indicating a required field: 'Device model *', 'Faulty device *', and 'Replacement device *'. At the bottom, there are two buttons: a green '✓ Certain' button and a red '✗ Close' button.

可視性

類型を保存

類型保存の概要

SmartMCのネットワークトポロジーは自動的に描画されます。すべてのデバイスがネットワークに参加した後、管理者はWebモニターからトポロジーを表示し、メンバーデバイスアイコンをドラッグして位置を調整し、調整されたトポロジーをローカルPCに保存できます。ネットワークが変更されるまで、同じPCからのその後のログイン時に、保存されたトポロジーが表示されます。

-  コマンドーを示します。
-  メンバーが正常に動作していることを示します。
-  トポロジーの保存後にネットワークに追加されたメンバーを示します。
-  トポロジーの保存後にメンバーがオフラインになることを示します。
-  は、SmartMCネットワーク内のAPを示します。

制限事項およびガイドライン

- 類型マップは現在のブラウザに保存され、ブラウザを変更しても保存された類型は有効になりません。
- 類型を保存した後、SmartMCのネットワークが変更された場合、たとえば、一部のメンバーが追加または削除された場合、システムは自動的に新しい類型を描画します。保存された類型は有効になりません。

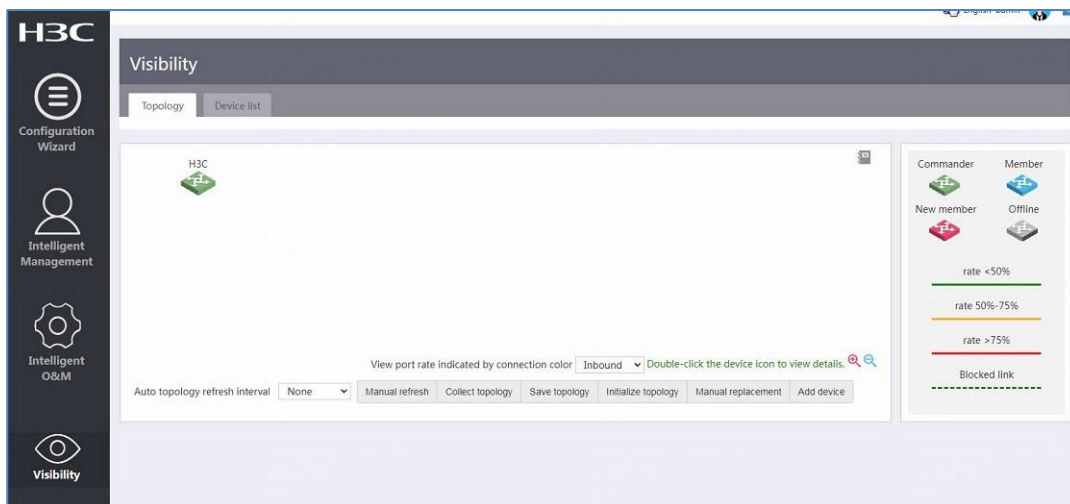
手順

1. ナビゲーションペインで、**Visibility**をクリックします。
2. **Typology**タブをクリックします。
3. **Collect typology**をクリックします。システムは、SmartMCネットワーク内のデバイス、ネイバー、

およびポート情報を収集します。

4. **Manual refresh**をクリックします。システムは、ネイバーおよびデバイス情報に基づいて、現在の類型マップを更新します。
5. メンバーアイコンをドラッグして、SmartMCネットワークの類型を最適化します。
6. **Save typology** をクリックします。

図178 手動による類型論の更新



トポロジーの初期化

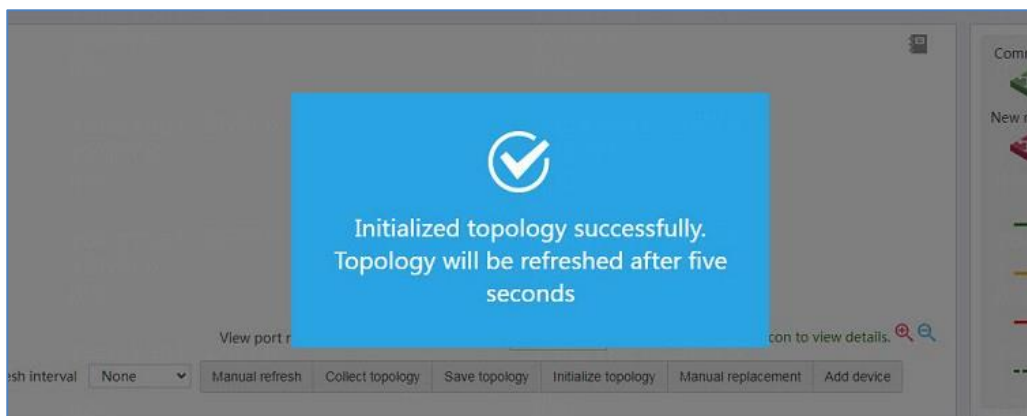
トポロジーの初期化の概要

SmartMCネットワーク内のオフラインデバイスを削除し、元のメンバー状態を復元するには、次の作業を実行します。

手順

1. ナビゲーションペインで、**Visibility**をクリックします。
2. **Typology**タブをクリックします。
3. **Initialize typology**をクリックします。

図179 トポロジーの初期化



構成を手動で置換

障害が発生したデバイスの設定交換の概要

障害のあるメンバーが物理的に交換された後、このタスクを実行して構成の交換をトリガーします。新しいメンバーは、障害のあるメンバーの構成ファイルをFTPサーバーからダウンロードし、ファイルを実行して交換を完了します。

制限事項およびガイドライン

- 交換用の新しいメンバーと障害のあるメンバーのデバイスモデルとIRFメンバーIDが同じであることを確認します。
- 故障した部材を交換する前に、故障した部材が取り付けられていた場所に新しい部材を取り付け、すべてのケーブルを新しい部材に接続します。

手順

1. ナビゲーションペインで、**Visibility**をクリックします。
2. **Typology**タブをクリックします。
3. **Manual replacement**をクリックします。
4. 開いたページで、デバイスモデル、障害のあるデバイス、および新しいデバイスを指定します。
5. **Certain**をクリックします。

図180 手動による構成の置換



The screenshot shows a dialog box titled "Manual Replacement" with a close button (X) in the top right corner. Inside the dialog, there are three dropdown menus, each with a red asterisk indicating a required field: "Device model", "Faulty device", and "Replacement device". At the bottom of the dialog, there are two buttons: a green button labeled "Certain" with a checkmark icon, and a red button labeled "Close" with an "X" icon.

デバイスを追加する

デバイス追加の概要

SmartMCネットワークにデバイスを手動で追加するには、次のタスクを実行します。Add Deviceボタンの右上隅に、追加に使用できないデバイスの数が表示されます。

制限事項およびガイドライン

SmartMCネットワークにデバイスを手動で追加する前に、必ず次の設定を行ってください。

- HTTPおよびHTTPSサービスをイネーブルにします。
- Telnetサービスをイネーブルにします。
- HTTPに基づいてNETCONF over SOAPをイネーブルにします。
- LLDP機能をグローバルにイネーブルにします。

- パスワードが**admin**、サービスタイプがTelnet、HTTP、およびHTTPS、RBACロールがnetwork-adminであるローカルユーザー**admin**を設定します。
- VTY回線認証方式**scheme**を指定します。
- SNMPv2cをサポートするようにデバイスを設定し、読み取り専用操作用にSNMPコミュニティ名publicを指定します。

手順

1. ナビゲーションペインで、**Visibility**を選択します。
2. **Typology**タブをクリックします。
3. **Add dev**をクリックします。
4. 開いたページで、IPアドレス、ユーザー名、およびパスワードを指定します。
5. **Certain**をクリックします。

図181 デバイスの追加

メンバー関連の機能

ポートの構成

1. ナビゲーションペインで、**Visibility**を選択します。
2. **Typology**タブをクリックします。
3. ターゲットデバイスのアイコンをクリックします。
4. デバイスペインで、モニターを選択します。
5. **Configure ports**をクリックします。
6. 表示されたページで、バッチ設定ファイルを選択します。
7. **Certain**をクリックします。ファイル内の設定が、対応するモニターに発行されます。
8. ナビゲーションペインで、**Intelligent O&M**を選択します。
9. **Intelligent port identification**タブをクリックします。
10. **View deployment status**をクリックして、モニターのステータスを表示します。

デバイスの名前を変更する

1. ナビゲーションペインで、**Visibility**を選択します。
2. **Typology**タブをクリックします。

3. ターゲットデバイスのアイコンをクリックします。
4. **Rename device**をクリックします。
5. 開いたページで、デバイス名を入力します。
6. **Certain**をクリックします。

Webモニターにログインする

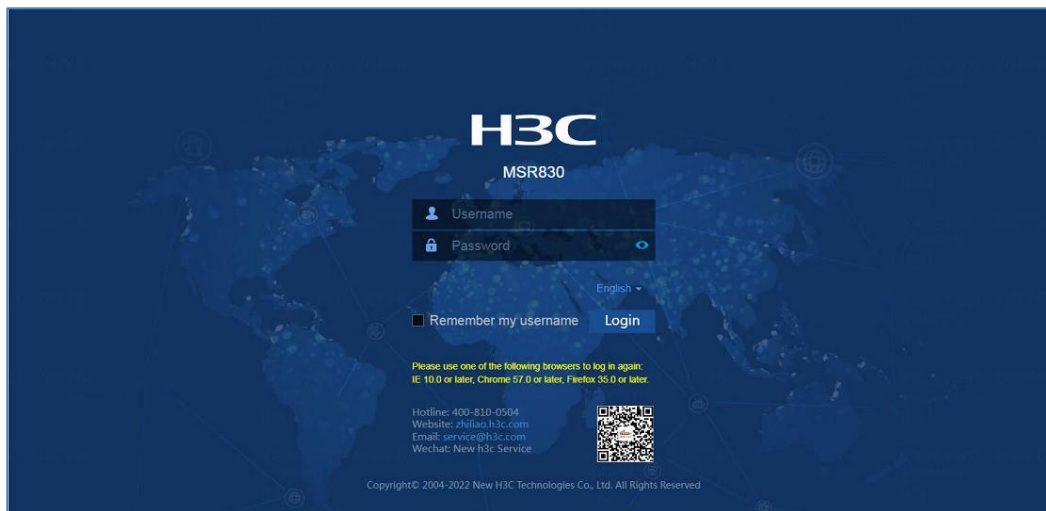
Webモニターログインの概要

メンバーの管理Webモニターにログインするには、次のタスクを実行します。

手順

1. ナビゲーションペインで、**Visibility**を選択します。
2. **Typology**タブをクリックします。
3. ターゲットメンバーのアイコンをクリックします。
4. **Log in to Web interface**をクリックします。
5. 開いたページで、メンバーのユーザー名とパスワードを入力します。

図182 Webモニターへのログイン



デバイスを再起動する

デバイスリブートの概要

メンバーを再起動するには、次のタスクを実行します。サポートされている再起動方法は次のとおりです：

- 設定を保存して再起動します。
- 強制的に再起動します。
- 工場出荷時のデフォルト設定で再起動します。

制限事項およびガイドライン

サービスの中断を避けるために、注意してデバイスを再起動してください。

自動設定をサポートしているデバイスでは、再起動後に工場出荷時のデフォルト設定で自動設定が開始されます。

手順

1. ナビゲーションペインで、**Visibility**を選択します。
2. **Typology**タブをクリックします。
3. ターゲットメンバーのアイコンをクリックします。
4. **Reboot device**をクリックします。
5. 開いたページで、再起動方法を指定します。
6. **Certain**をクリックします。

メンバーログ

メンバーログの概要

メンバーのキャッシュログと再起動ログ、およびAP再起動ログを表示するには、次の作業を実行します。

制限事項およびガイドライン

コマンドーは、メンバーごとに最大10個の再起動ログを保存できます。

手順

1. ナビゲーションペインで、**Visibility**を選択します。
2. **Typology**タブをクリックします。
3. ターゲットメンバーのアイコンをクリックします。
4. **Member logs**をクリックします。

情報の監視

情報の監視の概要


CPU使用率、メモリ使用率、温度情報、パケット損失情報など、メンバーのモニタリング情報を表示するには、次の作業を実行します。

手順


1. ナビゲーションペインで、**Visibility**を選択します。
2. **Typology**タブをクリックします。
3. ターゲットメンバーのアイコンをクリックします。
4. **Monitoring information**をクリックします。

デバイスリスト

デバイスリストの概要

デバイスリストには、コマンドーおよびメンバーの基本情報が表示されます。デバイスの詳細情報を表示するには、デバイスの**Operation**列のアイコンをクリックします。カスタムデバイスタイプを表示および構成できます。

カスタムデバイスタイプを設定する

1. ナビゲーションペインで、**Visibility**を選択します。
2. **Device list**タブをクリックします。
3. ターゲットデバイスを選択し、そのデバイスの**Operation**列にあるアイコンをクリックします。
4. 開いたデバイスの詳細ページで、デバイスのSYSOID値を検索し、その値をコピーします。
5. **Close**をクリックして、ページを閉じます。

6. **Customize device type**をクリックします。
7. 開いたページで、SYSOID値を貼り付け、デバイスタイプを指定します。
8. **Certain**をクリックします。

図183 デバイスタイプのカスタマイズ

カスタマイズされたデバイスタイプの表示

1. ナビゲーションペインで、**Visibility**を選択します。
2. **Device list**タブをクリックします。
3. **View customized device type**をクリックします。

図184 カスタマイズされたデバイスタイプの表示

SYSOID	Device type	Operation