H3C キャンパススイッチ
SmartMC ベスト プラクティス

内容

SmartMCとは

背景

ネットワークの拡張には、ネットワークエッジでのアクセスデバイスの数が増加する必要があります。このようなアクセスデバイスの管理と維持は非常に困難で時間がかかります。

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の豊富な管理機能とメンテナンス機能を統合するネットワーク管理プラットフォームを提供し、デバイスの一括管理を簡素化します。

SmartMCが設定されている場合は、SmartMC管理プラットフォームにログインし、Webインターフェイスからネットワークエッジに分散しているネットワークデバイスを一括して集中管理およびメンテナンスできます。

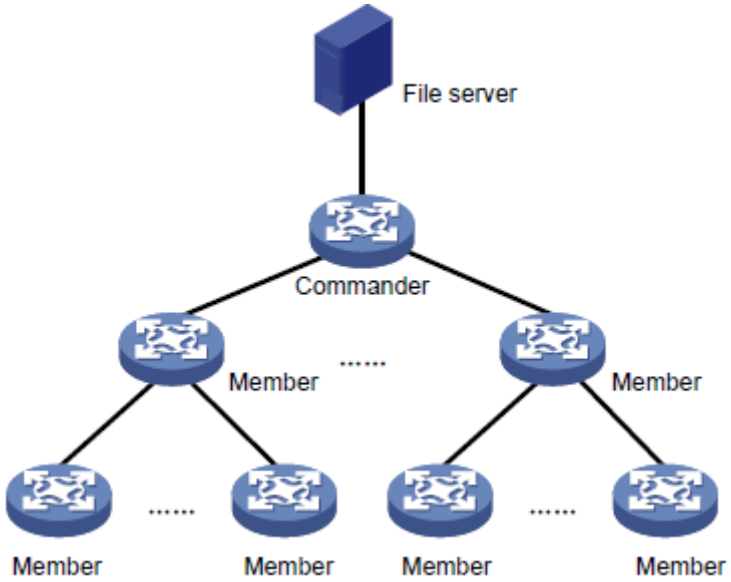
作動機構

ネットワークフレームワーク

基本的な枠組みを図1に示します。SmartMCネットワークには次の要素が含まれます。SmartMC

- **Commander(コマンダー)**: SmartMCネットワークのすべてのメンバーを管理します。SmartMCネットワークでは、1つのデバイスだけが**Commander**として機能し、残りのデバイスはすべて**Member**として機能します。
- **Member(メンバー)**: **Commander**によって管理されます。SmartMCネットワークには、最大64のメンバーを含めることができます。
- **File server**: **Commander**および**Member**の起動ソフトウェアイメージおよび構成ファイルを格納します。**Member**は、**Commander**が発行したコマンドに従って、サーバーから必要なファイルを取得します。**File server**は、独立したサーバーであるか、**Commander**または**Member**と同じ場所に配置できます。**Commander**または**Member**のワークロードを削減するためのベストプラクティスとして、独立したファイルサーバーを配置します。

図1 SmartMCネットワークのフレームワーク



管理プラットフォーム

SmartMC管理プラットフォームは、次の機能を統合しています。

- **インテリジェントな管理**: デバイスロールの変更、ネットワークトポロジーの収集、**Outgoing**(発信)インターフェイスの設定、および自動イーサネットリンク集約が含まれます。
- **インテリジェントな運用とメンテナンス**: **Member**のアップグレード、コンフィギュレーションファイルの一括バックアップ、ワンキーVLANの導入、スマートポートの識別、リソースのモニタリング、障害のあるデバイスの交換などが含まれます。
- **可視性**: ネットワークトポロジー管理、**Member**追加、デバイスリスト表示、およびデバイス状態表示が含まれます。
- **インテリジェントサービス**: ユーザーの作成とアクティブ化が含まれます。

SmartMC管理プラットフォームを使用すると、SmartMCネットワークトポロジーを管理し、**Member**を一括管理できます。

図2から図5は、Webインターフェイスの例を示しています。

図2 インテリジェントな管理

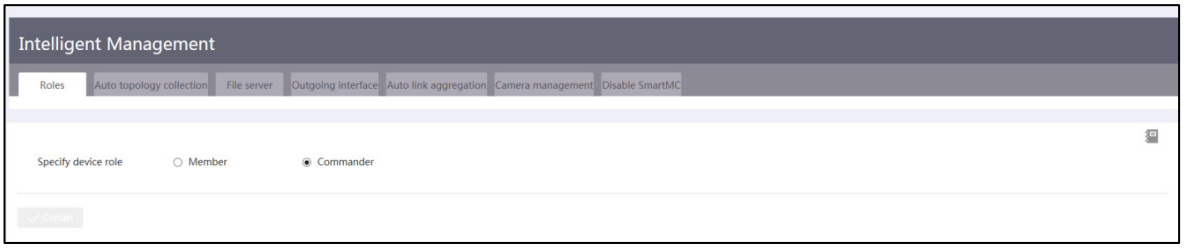


図3 インテリジェントな操作とメンテナンス

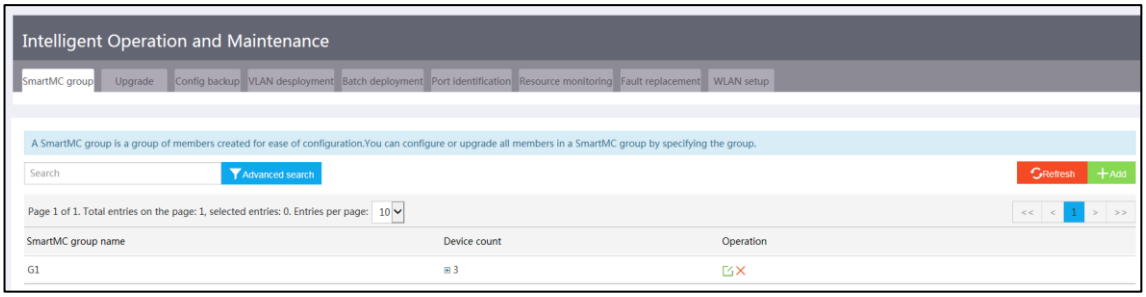


図4 可視性

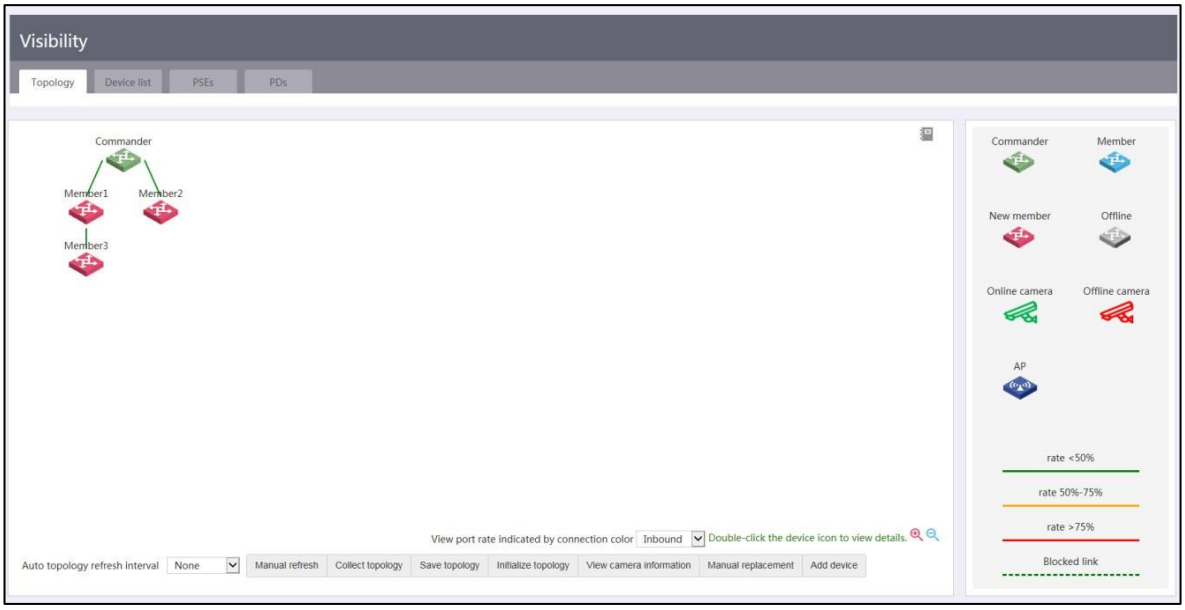
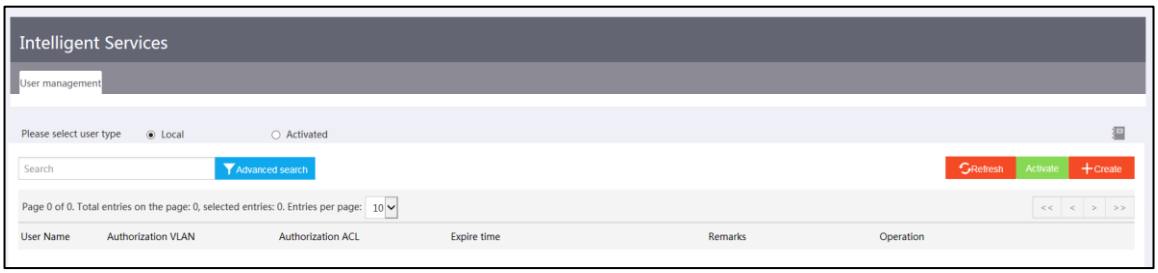


図5 インテリジェントサービス



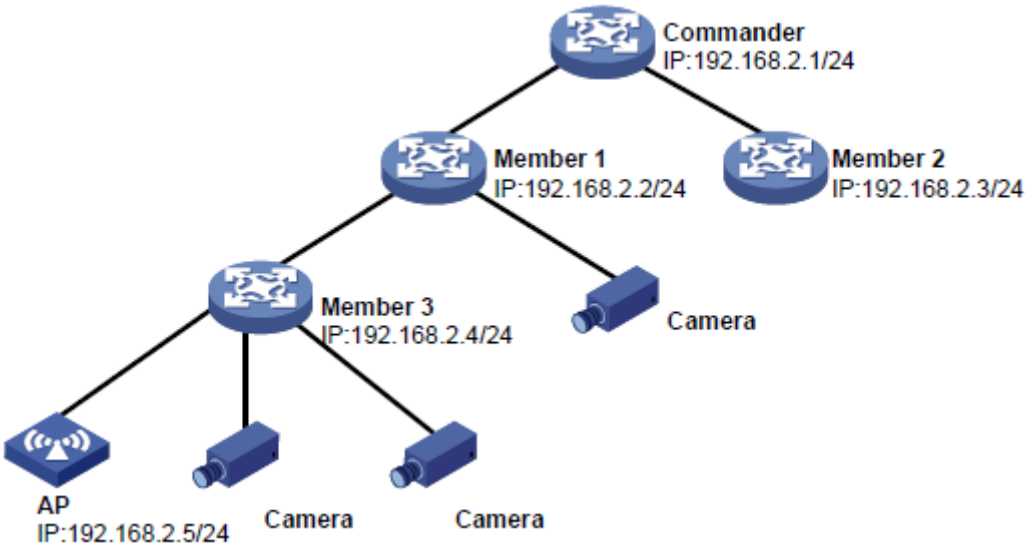
ベストプラクティス構成

ネットワーク要件

図6に示すように、APがメンバー3に接続され、2つのカメラがメンバー3に接続され、1つのカメラがメンバー1に接続されています。SmartMC設定ウィザードで**Commander**を設定します。

- SmartMCネットワークに自動的に参加するようにメンバーを設定するか、**Member**をネットワークに手動で追加します。
- VLAN 1で相互に通信するようにAP、**Commander**、および**Member**を設定します。
- **Commander**でAC機能をイネーブルにし、PoEを介してAPおよびカメラに電力を供給するようにメンバー3を設定します。
- モニターオーディオおよびビデオセッションのすべてのメンバーで、SIPベースのSQAをイネーブルにします。

図6 ネットワーク図



SmartMCネットワークの展開

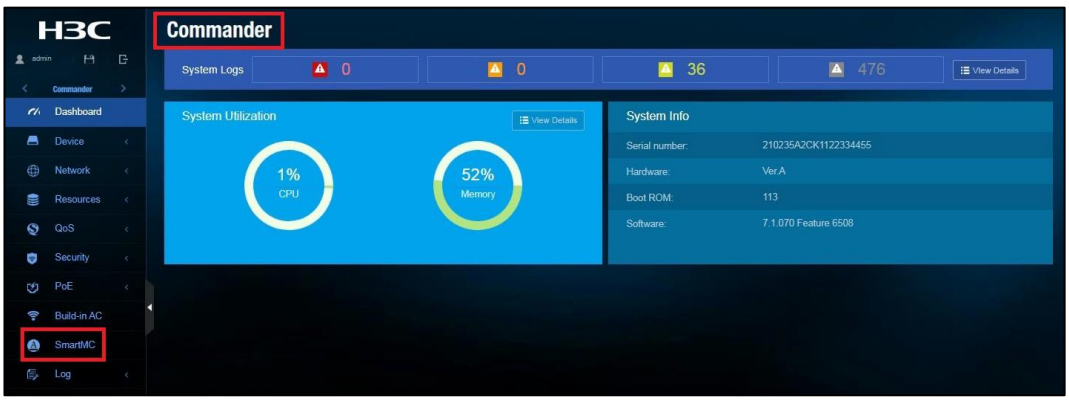
ネットワークに自動的に参加するように**Member**を設定することも、手動で追加することもできます。

自動配置の設定

手順

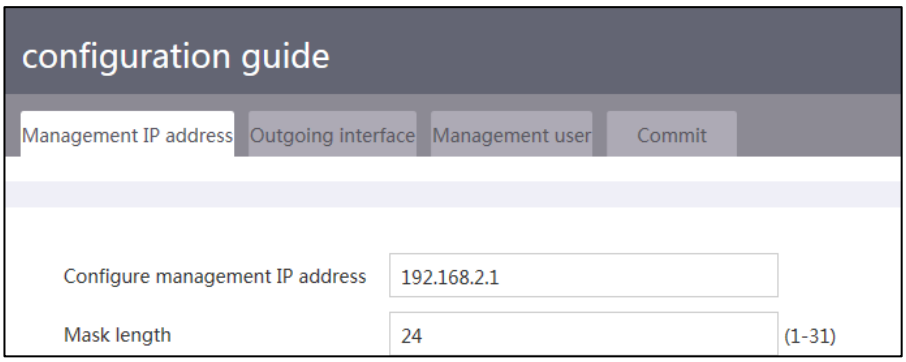
1. **Commander**を次のように設定します。
   a. **Commander**にログインし、左側のナビゲーションペインで**SmartMC**をクリックします。

      図7 SmartMCのWebインターフェイス



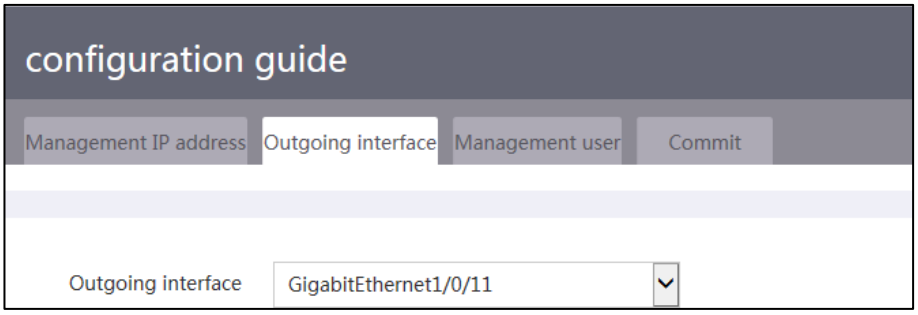
   b. 管理IPアドレス(コマンダー上のVLANインターフェイス1のIPアドレス)を指定します。

図8 管理IPアドレスの指定



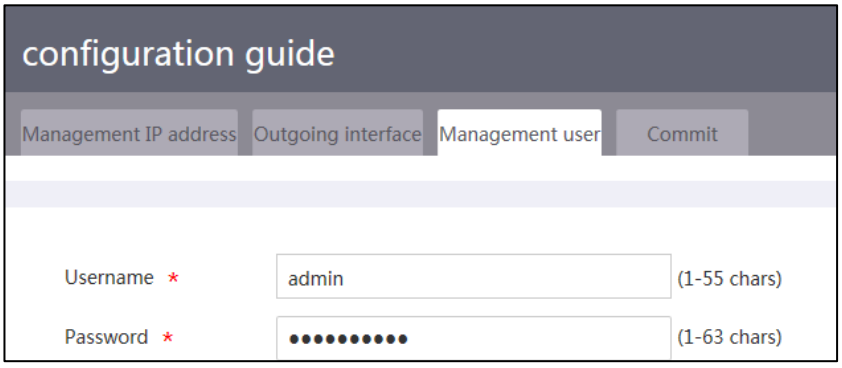
c. **Outgoing(**発信)インターフェイスを指定します。**Commander**を現在のPCに接続する**Commander**上のインターフェイスを発信インターフェイスとして指定します。

図9 発信インターフェイスの指定



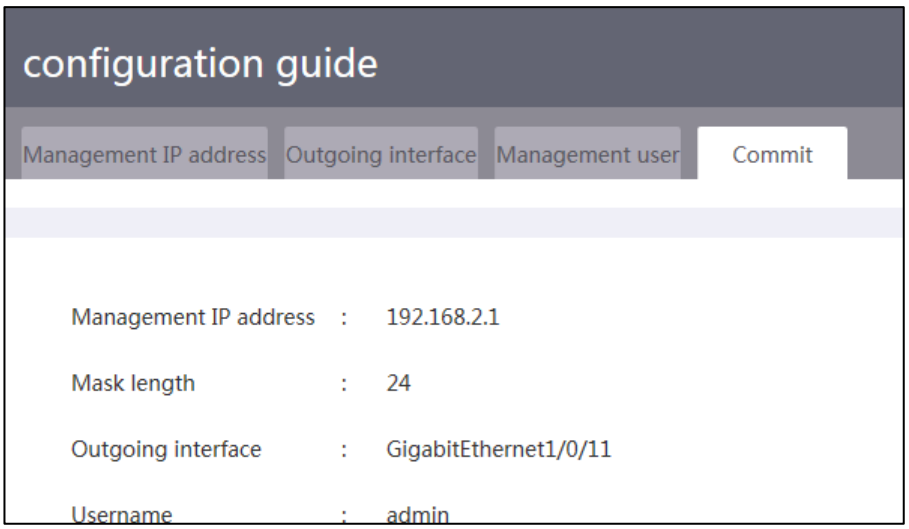
d. **Commander**のローカルユーザーを指定します。既存のローカルユーザーまたは新規のローカルユーザーを指定できます。新規ユーザーを指定すると、そのユーザーが自動的に作成されます。

図10 管理ユーザーの指定



e. **Commander**の設定を確認します。

図11 Commander**設定の確認**

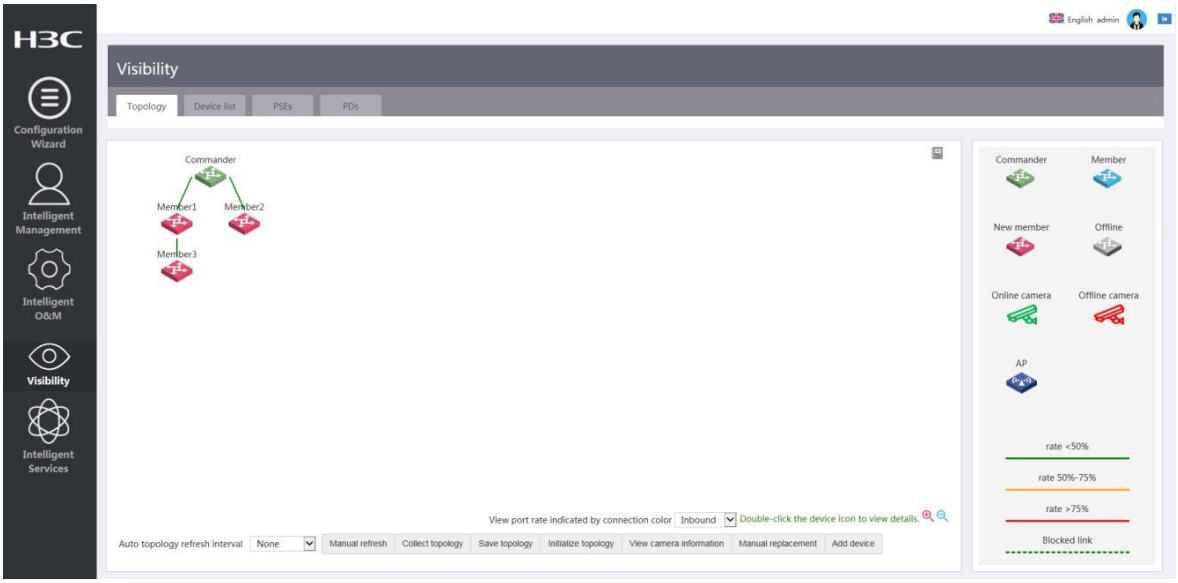


2. 構成をロードせずに**Member**の電源を入れます。メンバーは自動的にSmartMCネットワークに参加します。

設定の確認

Visibility > Topologyページにアクセスしtopologyページにアクセスし、ネットワークトポロジーを表示します。**Member**が予想どおりにネットワークに参加していることを確認します。

図12 ネットワークトポロジー



手動展開の設定

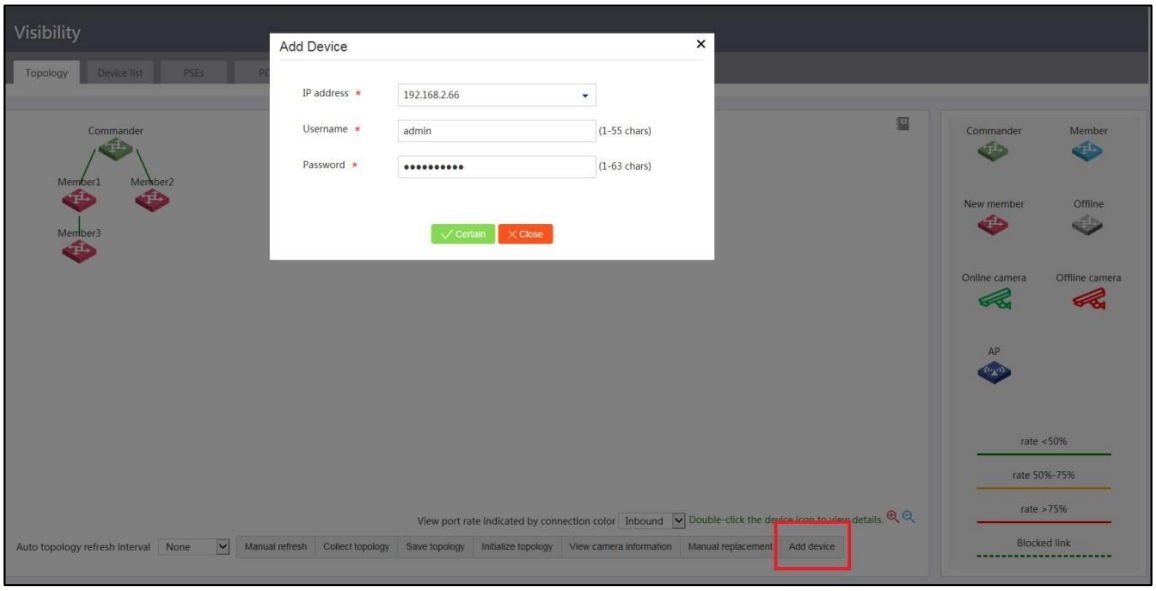
ネットワークに自動的に参加できないメンバーの場合は、**Visibility** > **Topology**にアクセスできます。ページでAdd deviceをクリックして、手動で1つずつ追加します。

手動で追加する前に、追加する**Member**に表1の設定が構成されていることを確認します。

表1手動で追加するMemberに必要な設定

項目	コマンド
VLAN-interface 1のIPアドレスを指定します。IPアドレスが、**Commander**上のVLAN-interface 1のIPアドレスと同じサブネットにあることを確認します。	• **interface vlan-interface 1** • **ip address** *ip-address* { *mask-length* | *mask* }
HTTPおよびHTTPSをイネーブルにします。	• **ip http enable** • **ip https enable**
Telnetサービスをイネーブルにします。	**telnet server enable**
NETCONF over SOAP over HTTPをイネーブルにします。	**netconf soap http enable**
LLDPをグローバルにイネーブルにします。	**lldp global enable**
パスワードの複雑さの要件が緩和されます。	• **password-control length 4** • **password-control composition type-number 1 type-length 1** • **undo password-control complexity user-name check**
ユーザーを作成します。ユーザー名とパスワードをadminに設定し、telnet、http、およびhttpsの各サービスタイプを追加して、ユーザーnetwork-adminユーザーロール。	• **local-user admin** • **password simple admin** • **service-type telnet http https** • **authorization-attribute user-role network-admin**
VTYユーザー回線0～63のスキーム認証を設定します。	• **line vty 0 63** • **authentication-mode scheme**
SNMPv2cをイネーブルにし、読み取り専用コミュニティパブリックを作成します。	• **snmp-agent sys-info version v2c** • **snmp-agent community read public**

図13 手動でのMemberの追加

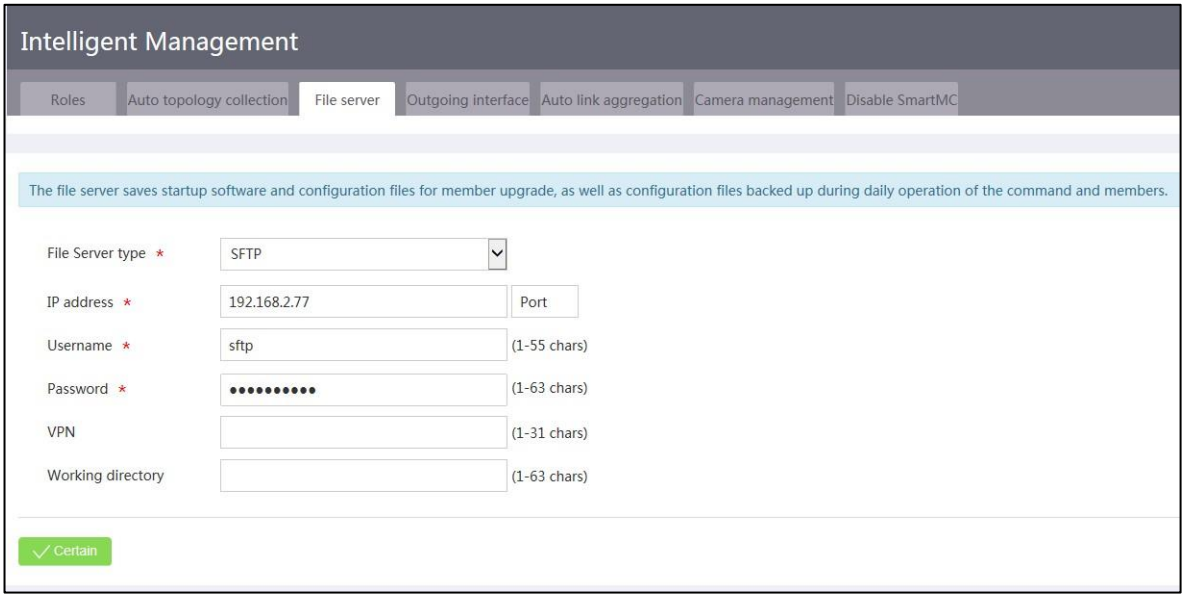


ファイルサーバーの指定

障害メンバーの交換、デバイスのアップグレード、一括のコンフィギュレーションファイルのバックアップ、および一括のコンフィギュレーションの展開には、ファイルサーバーが必要です。

ファイルサーバーを指定するには、**Intelligent Management > File Server**ページにアクセスし、必要に応じてファイルサーバーのパラメータを指定します。

図14 ファイルサーバーの指定



有線および無線の統合メンテナンスの設定

有線および無線の統合メンテナンスでは、有線ネットワーク管理機能、基本的な無線ネットワーク管理機能、およびPoE電力可視性機能が統合されているため、有線ネットワークと無線ネットワークの両方統合された管理と統計情報表示が可能になります。

基本的なWLAN設定

無線サービスの追加、削除、または変更、AP間レイヤ2分離の設定、およびSmartMCネットワーク内のすべてのデバイス上のPoE電源の管理を行うには、次の作業を実行します。

前提条件

CommanderでAC機能がイネーブルになっていることを確認します。

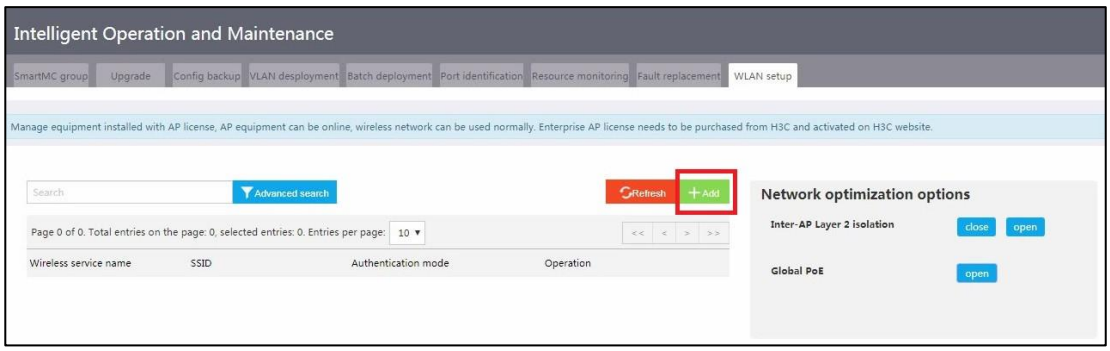
制限事項とガイドライン

デフォルトでは、作成された無線サービスの認証モードはPSKです。

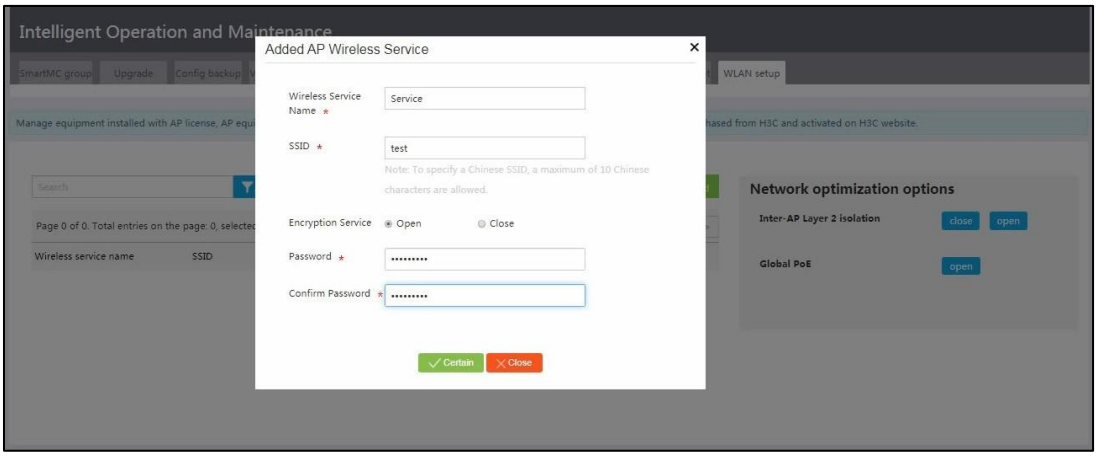
手順

1. **Intelligent O&M > WLAN setup**ページにアクセスします。
2. **Add**をクリックします。

図15 ワイヤレスサービスの追加

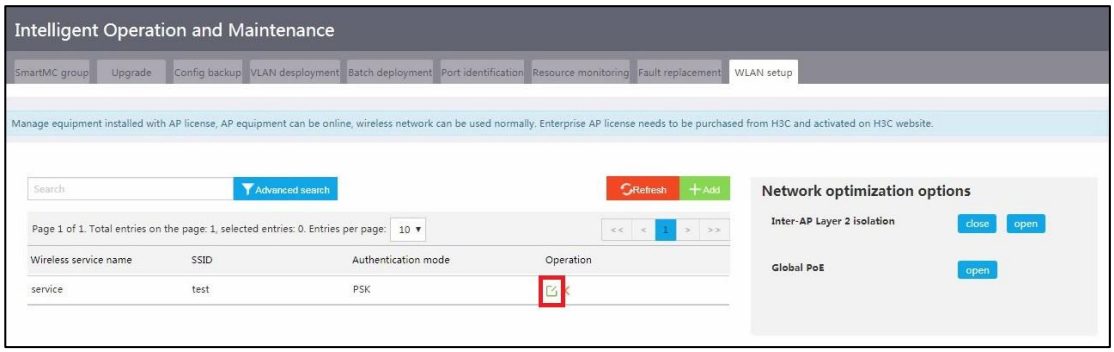


3. ワイヤレスサービスパラメータを設定し、**Confirm**をクリックします。図16 ワイヤレスサービスパラメータの設定



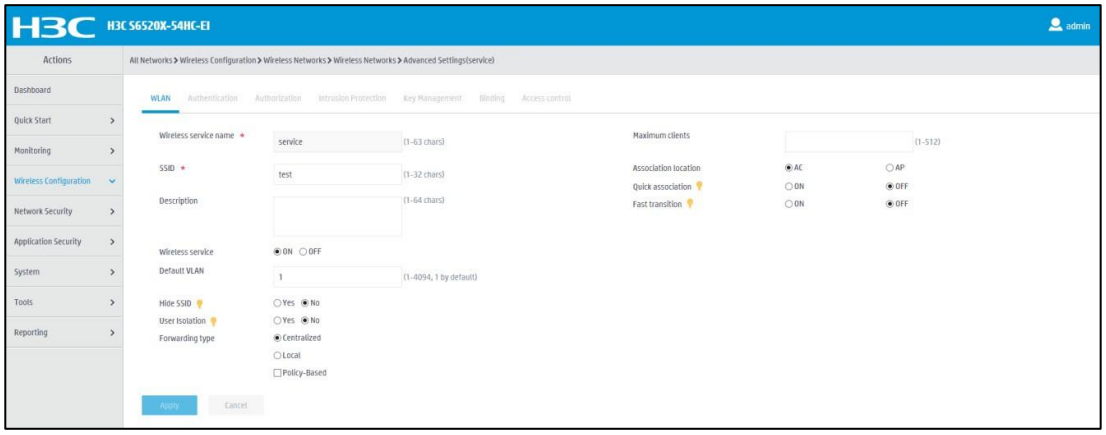
4. ワイヤレスサービスの**Edit**アイコンをクリックします。

図17 ワイヤレスサービスの編集



5. 必要に応じて、ワイヤレスサービスの詳細設定を構成します。

図18 ワイヤレスサービスの詳細設定



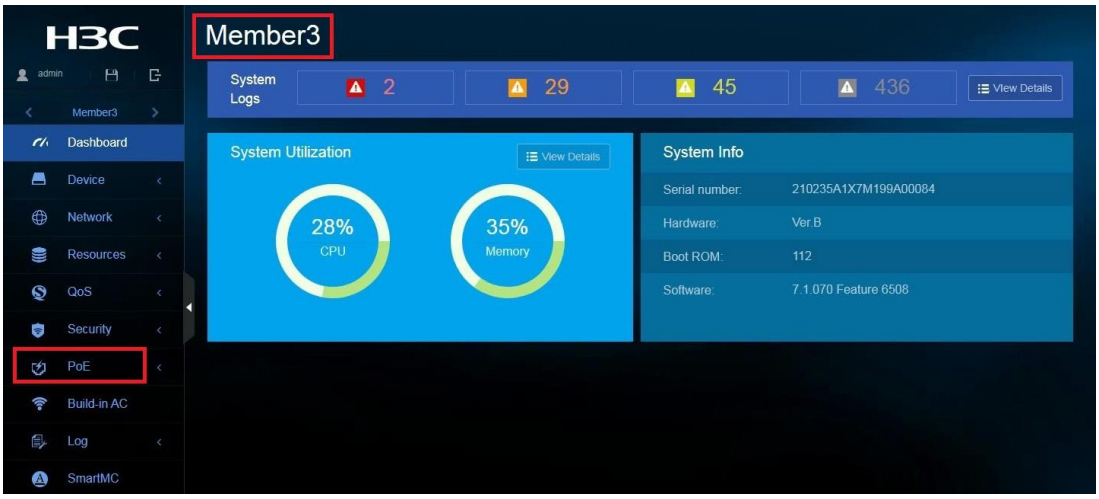
PoE電源の設定

1. 左側のナビゲーションペインで、**Visibility**をクリックします。
2. PSE 情報を表示するには、PSE タブをクリックします。**Action**列のアクション リンクをクリックして、PSE の詳細または PD を表示したり、PoE 電源を構成したりできます。

図19 PSE情報の表示

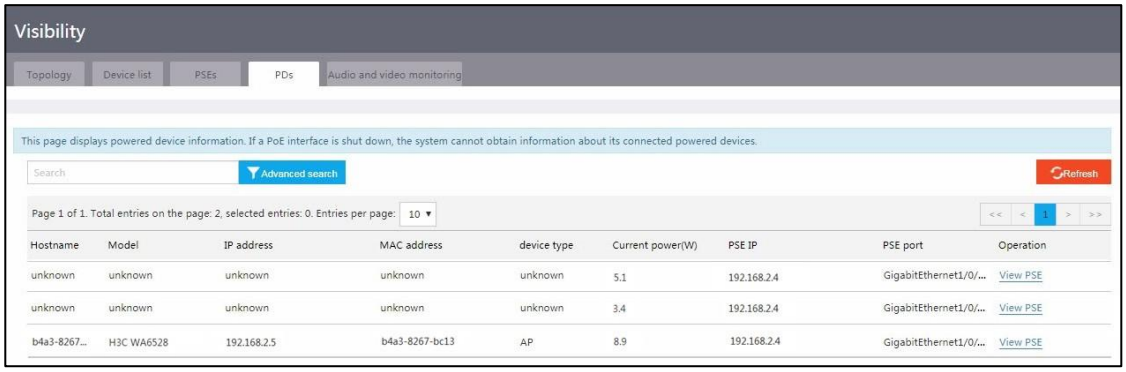
図20 PSEの詳細の表示

図21 PoE電源の設定



3. PD情報を表示するには、PDタブをクリックします。

図22 PD情報の表示



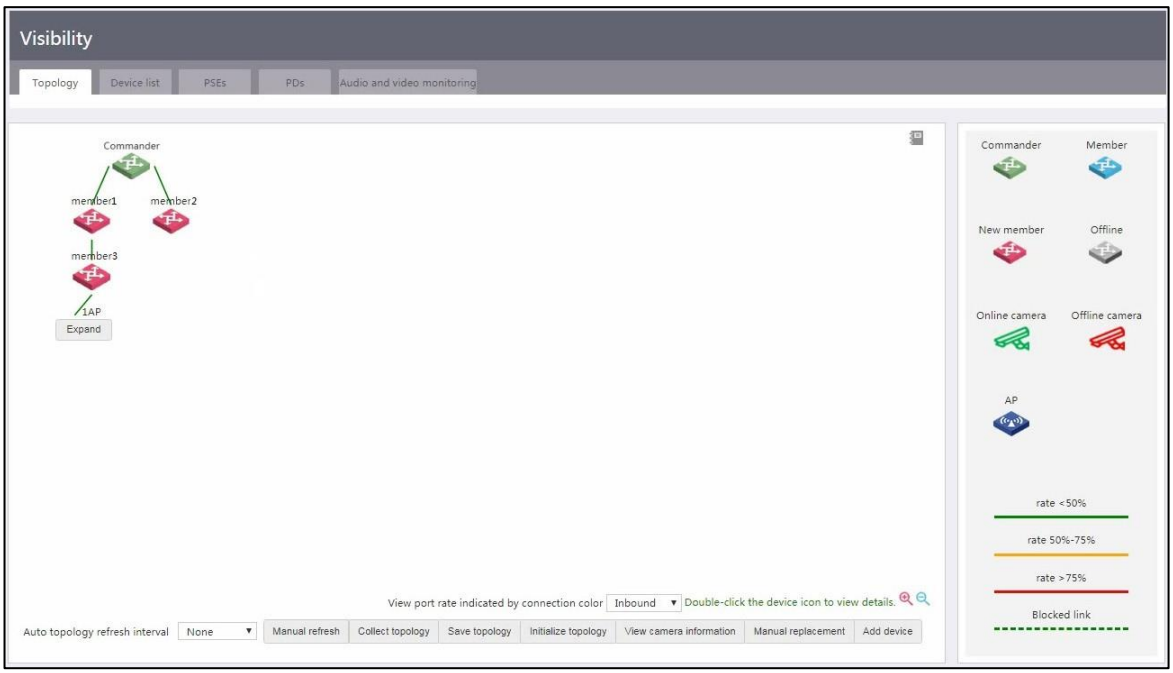
ネットワークトポロジーおよびデバイスの詳細の表示

Visibility > Topologyページでネットワークトポロジーを表示できます。

APの詳細情報を表示するには、**Expand**をクリックします。

デバイスに関するネイバー情報を表示するには、デバイスアイコンをダブルクリックします。

図23 ネットワークトポロジーおよびデバイスの詳細の表示



カメラモニタリングの設定

VLAN内のカメラのアソシエーションおよびアソシエーション解除をモニタするには、次の作業を実行します。この機能を設定すると、**Visibility > Topology**ページに監視対象カメラが表示され、カメラのステータスがリアルタイムでリフレッシュされます。

カメラを管理する

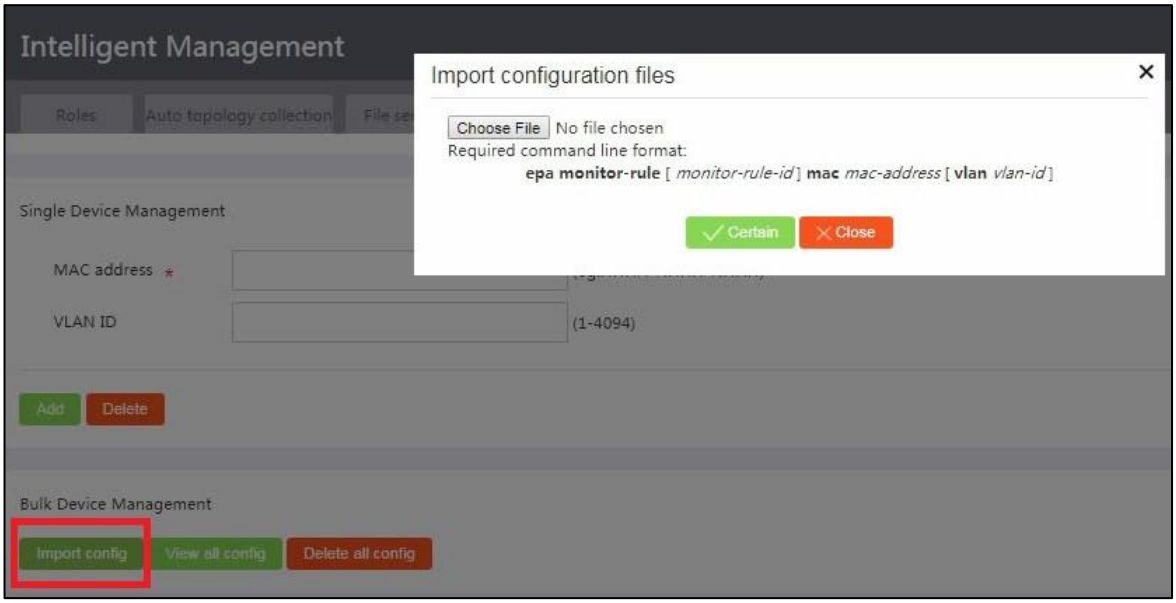
1つのカメラを管理することも、複数のカメラを1回の操作で管理することもできます。

モニタにカメラを追加する

単一のカメラを追加するには、カメラのMACアドレスとカメラを監視するVLANを指定し、Addをクリックします。

複数のカメラを一括して追加するには、**Import config**をクリックし、カメラ情報を含むコンフィギュレーションファイルをインポートします。

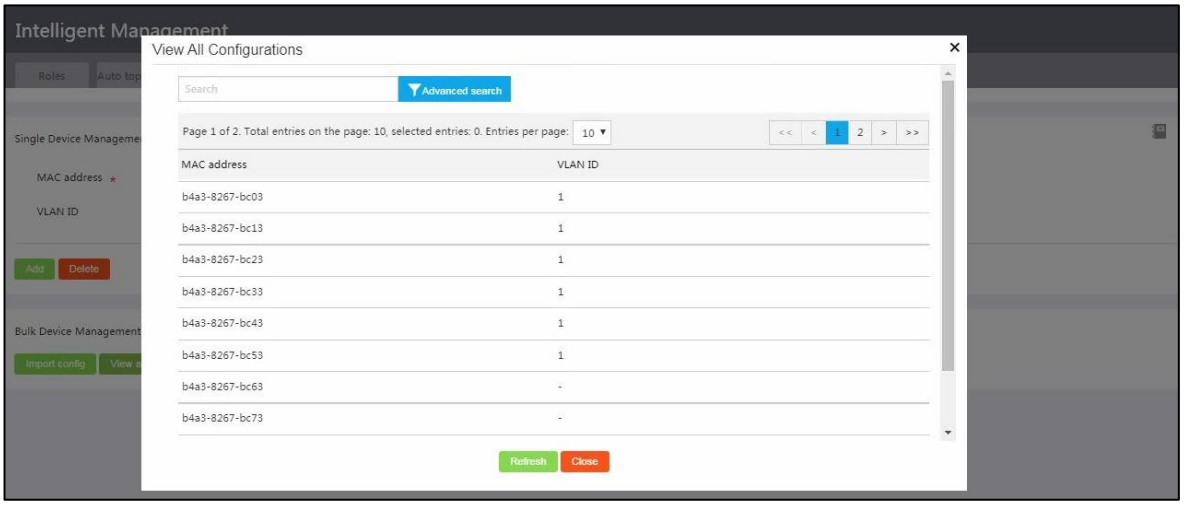
図24 監視するカメラのインポート



すべての監視対象カメラの表示

すべてのカメラ監視構成を表示するには、**View all config**をクリックします。

図25 すべてのカメラ監視構成の表示



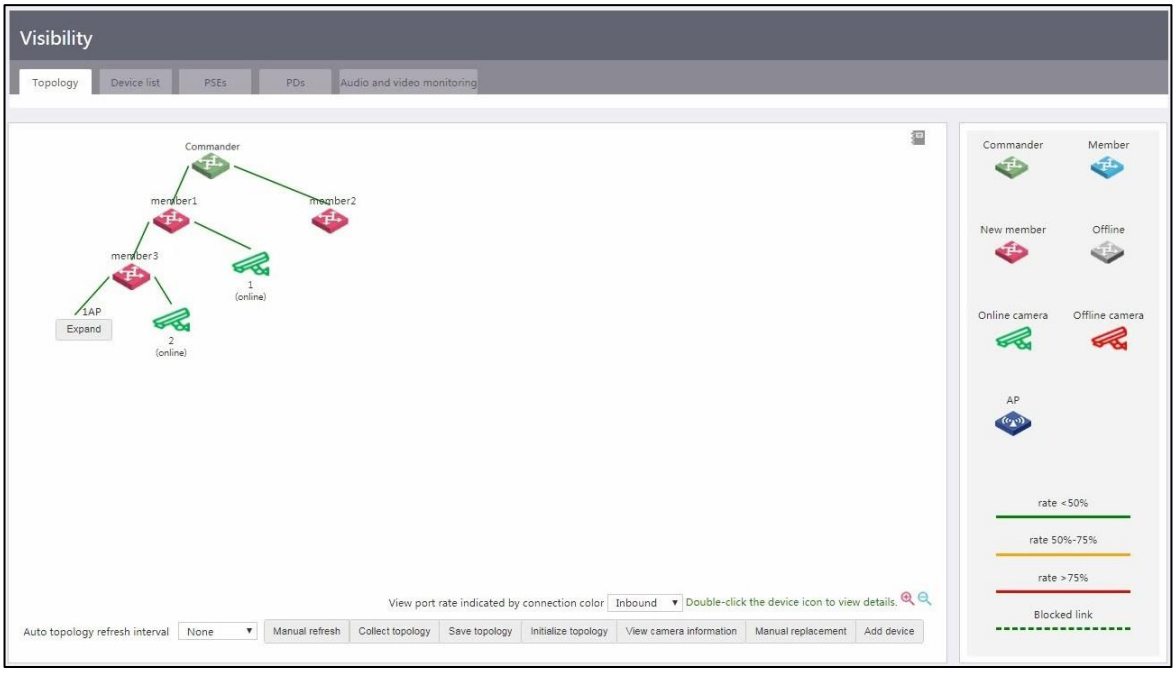
カメラを削除する

1台または複数台のカメラを一括して削除できます(詳細は省略)。

トポロジー内のカメラの表示

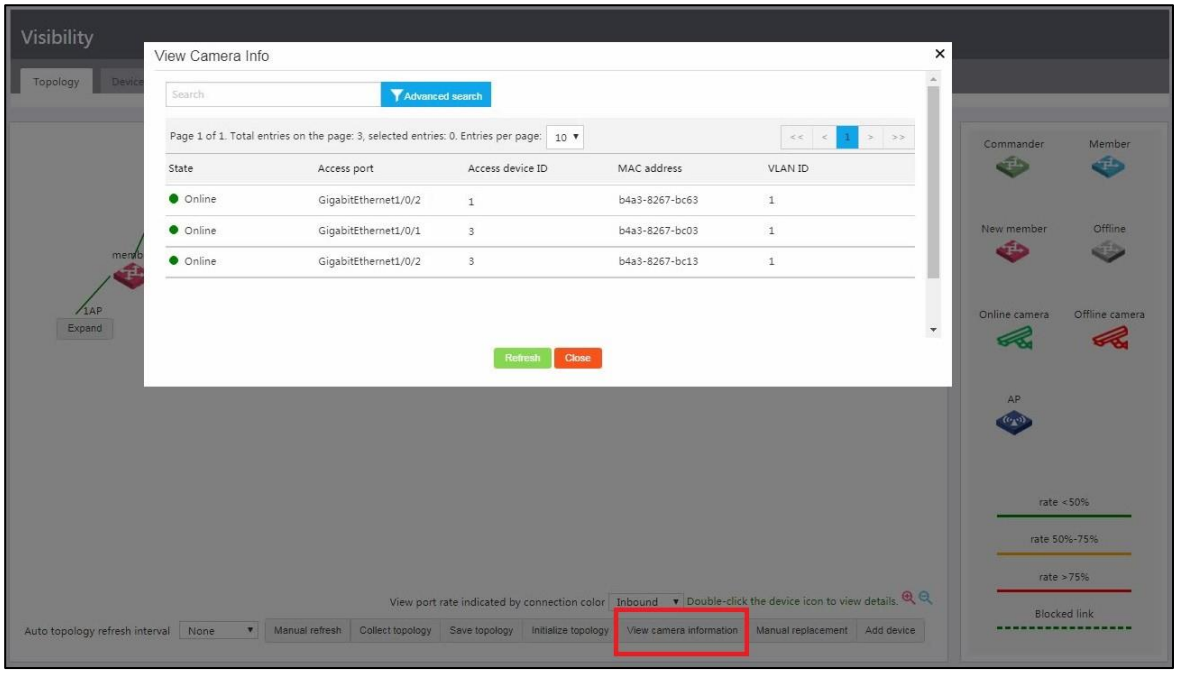
Visibility > Topologyページにアクセスして、トポロジー内の監視対象カメラを表示できます。

図26 トポロジー内のカメラの表示



監視対象カメラの詳細情報を表示するには、**View camera information**をクリックします。

図27 カメラの詳細情報の表示



オーディオおよびビデオモニタリングの設定

マルチメディアトラフィックのモニターオーディオおよびビデオセッションに対して、この作業を実行します。CLIからデバイスにSIPベースのService Quality Analysis(SQA)を1つずつ設定することも、Webインターフェイスから複数のデバイスにSIPベースのSQAを一括して設定することもできます。

SQAの設定

CLIからの単一デバイスでのSQAの設定

この作業は、**Commander**と**Member**の両方で実行する必要があります。単一のデバイスにSQAを設定するには、次の手順を実行します。

1. システムビューに入ります。
   System-view
2. SQAビューに入ります。
   sqa
3. SIPベースのSQAをイネーブルにします。
   sqa-sip enable
   デフォルトでは、SIPベースSQAはディセーブルになっています。
4. (任意)SIPリスニングポート番号を指定します。
5. **sqa-sip port** *port-number*
   デフォルトでは、SIPリスニングポート番号は5060です。
   デバイスのSIPリスニングポート番号が、SIPサーバーのポート番号と同じであることを確認します。
6. (任意)SIPベースのSQAのIPアドレス範囲を指定します。
7. **sqa-sip filter address** *start-address end-address*
   デフォルトでは、SIPベースのSQAにはIPアドレス範囲は指定されていません。デバイスはすべてのSIPパケットに対してSQAを実行します。
   このコマンドの実行後、デバイスは指定されたIPアドレス範囲内のSIPコールに対してだけSQAを実行します。

Webインターフェイスからの複数のデバイスでのSQAの設定

1. 構成ファイルConfig.cfgを作成し、ファイルをファイルサーバーに保存します。構成ファイルの内容には、次のコマンドが含まれている必要があります。

   <FTP Server>more Config.cfg

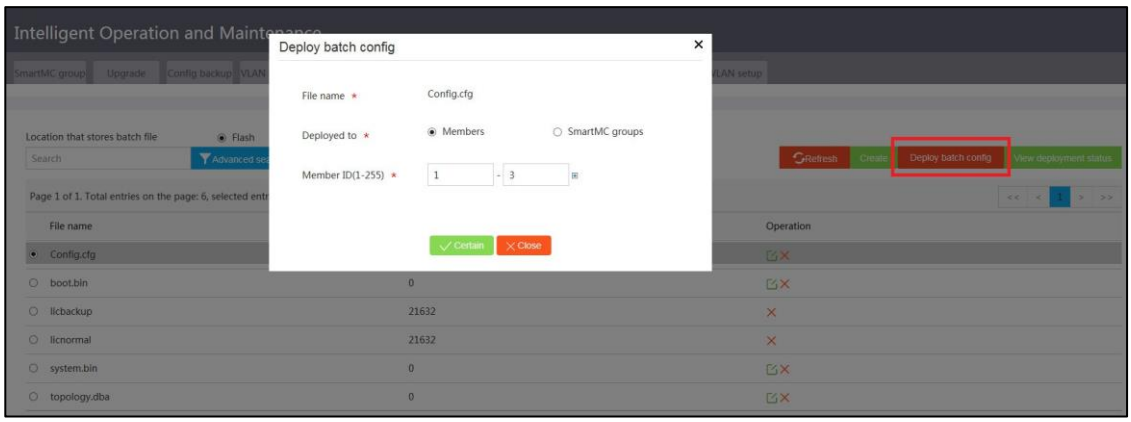
   system-view
   sqa

   sqa-sip enable

   sqa-sip port 5066
   sqa-sip filter address 192.168.56.1 192.168.56.244

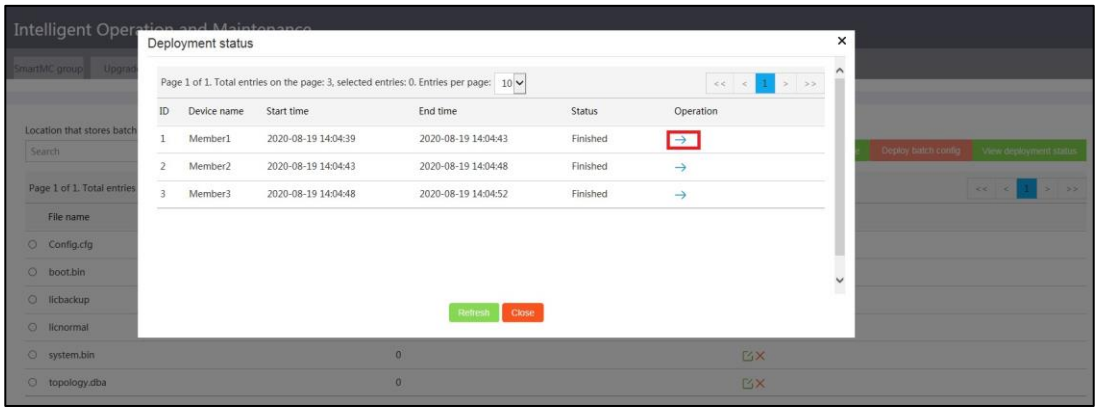
2. **Intelligent O&M > Batch deployment**ページにアクセスし、ファイルサーバーをバッチファイルの保存場所として選択し、ファイルリストからConfig.cfgを選択します。
3. **Deploy batch config**をクリックします。
4. 配置オブジェクトとして**Members**を選択し、メンバーIDの範囲を指定してConfirmします。

図28 バッチ構成ファイルのデプロイ



5. デプロイステータスの表示をクリックして、デプロイ結果を確認します。デプロイの詳細を表示するには、右の山形のアイコンをクリックします。

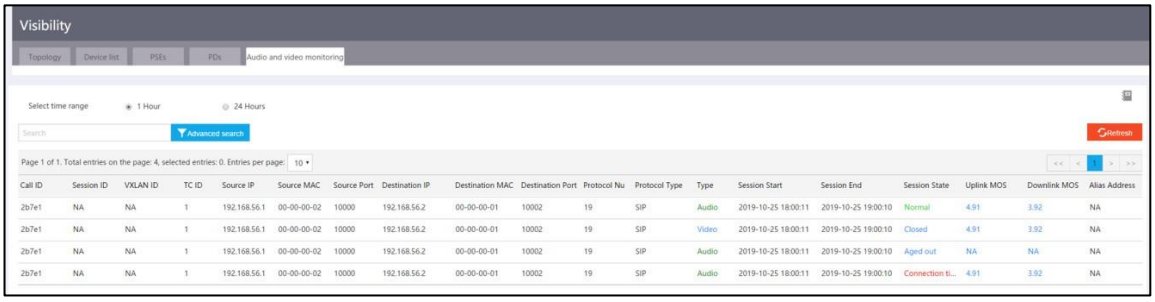
図29 デプロイステータスの表示



オーディオおよびビデオの監視情報の表示

Visibility > Audio and Video Monitoringページにアクセスして、オーディオおよびビデオモニタリングに関する詳細情報を表示し、アップリンクおよびダウンリンクMOS値に基づいてセッション品質を識別できます。

図30 オーディオおよびビデオの監視情報の表示



注:

TC IDが0のデバイスがコマンダーです。

MOS値が大きいほど、セッション品質が高いことを表します。MOS値の範囲は0～5です。

- **0～1**: セッション品質が非常に低い。
- **1～2**: セッション品質が低い。
- **2～3**: 平均的なセッション品質
- **3～4**: 好なセッション品質。
- **4～5**: 優れたセッション品質。
- **N/A**: システムはMOS値を取得できません。

SmartMC機能仕様

項目	値
サポートされるメンバーの最大数	64
サポートされるAPの最大数	**Commander**の統合有線および無線ACでサポートされている数と同じ
サポートされるカメラ監視ルールの最大数	512
Commanderまたはメンバー上でサポートされるSIPセッションの最大数	1000

SmartMCの制約とガイドライン

ベストプラクティスとして、自動方式を使用してSmartMCネットワークを展開します。S5130Sシリーズスイッチは、オーディオおよびビデオモニタリングをサポートしていません。

PoEを使用するには、配置されたデバイスがPoE対応であることを確認します。

SmartMCネットワークがVLAN 1に確立されます。ネットワークが正常に動作するためには、VLAN 1でセキュリティ設定を行わないでください。

SmartMCに推奨されるデバイス

装置モデル	TM	TC	推奨されるバージョン	備考
S6520-SI	サポート対象	サポート対象	F6509L01 以上	• 動的カメラ監視 (ONVIF) は F6615 以降のバージョンでのみサポートされています.
S6520X-SI	サポート対象	サポート対象		
S6520X-EI	サポート対象	サポート対象		
S6520X-HI	サポート対象	サポート対象		• 統合された有線および無線 AC と基本的な WLAN 設定は、R6522 以降のバージョンでのみサポートされます。
S5560X-30F-HI S5560X-54F-HI	サポート対象	サポート対象	R6530P01 以上	
S5560X-34C-HI S5560X-58C-HI	サポート対象	サポート対象	R6615P03 以上	
MS4600	サポート対象	サポート対象	F6509L01 以上	• 動的カメラ監視 (ONVIF) と自動エンドポイント識別は、R6615P03 以降のバージョンでのみサポートされています。 • 統合された有線および無線 AC と基本的な WLAN 設定は、R6522 以降のバージョンでのみサポートされます。
S5000-EI	サポート対象	サポート対象	F6509L01 以上	
S5560X-EI	サポート対象	サポート対象	F6509L01 以上	• 動的カメラ監視 (ONVIF) と自動エンドポイント識別は、F6615 以降のバージョンでのみサポートされます。 • 動的カメラ監視 (ONVIF) と自動エンドポイント識別は、F6615 以降のバージョンでのみサポートされます。
MS4520V2-30F	サポート対象	サポート対象	F6509L01 以上	• 動的カメラ監視 (ONVIF) と自動エンドポイント識別は、R6615P03 以降のバージョンでのみサポートされています。 • 統合された有線および無線 AC と基本的な WLAN 設定は、F6512P01 以降のバージョンでのみサポートされます。
MS4520V2-30C MS4520V2-54C	サポート対象	サポート対象	R6510P01 以上	
S5500V2-EI	サポート対象	サポート対象	F6509L01 以上	
S5560S-EI	サポート対象	サポート対象		• これらのシリーズのデバイスは SIP ベースの SQA をサポートしていません. • これらのシリーズのデ
S5560S-SI	サポート対象	サポート対象		
S5500V3-SI	サポート対象	サポート対象		
MS4520V2	サポート対象	サポート対象		

S5130S-HI	サポートせず	サポート対象	R6318P01 以上	バイスは、統合された有線および無線 AC と基本的な WLAN 設定をサポートしていません。 • 静的カメラ管理と自動エンドポイント識別は、R6328 以降のバージョンでのみサポートされています。 • ダイナミック カメラ モニタリング (ONVIF) は、R6338 以降のバージョンの S5130S-EI シリーズ スイッチでのみサポートされます。 • これらのシリーズのデバイスは TM として機能できます。 ベスト プラクティスとして、デバイスの役割を推奨どおりに構成します。
S5130S-EI	サポートせず	サポート対象		
S5130S-SI	サポートせず	サポート対象		
MS4320V2	サポートせず	サポート対象		
MS4320	サポートせず	サポート対象		
MS4300V2	サポートせず	サポート対象		
MS4200	サポートせず	サポート対象		
S5130S-LI	サポートせず	サポート対象		
S5120V2-SI	サポートせず	サポート対象		
S5120V2-LI	サポートせず	サポート対象		
E100C	サポートせず	サポート対象		
E500C	サポートせず	サポート対象		
E500D	サポートせず	サポート対象		
S5110V2	サポートせず	サポート対象		
S5110V2-SI	サポートせず	サポート対象		
S5000V3-EI	サポートせず	サポート対象		
S5000E-X	サポートせず	サポート対象		
S3100V3-EI	サポートせず	サポート対象		
S3100V3-SI	サポートせず	サポート対象		
S1850-X	サポートせず	サポート対象		
S5000V5-EI	サポートせず	サポート対象	Release 6319P01 以上	
S5120V3-SI	サポートせず	サポート対象	R6329 以上	
S5120V3-LI	サポートせず	サポート対象	R6329 以上	
S5000X-EI	サポートせず	サポート対象	R6329 以上	
S1850V2-X	サポートせず	サポート対象	R6329 以上	
MS4320V3	サポートせず	サポート対象	R6329 以上	
S1850V2-EI	サポートせず	サポート対象	R6330 以上	
E500C-F	サポートせず	サポート対象	R6338 以上	

SmartMCの設定

SmartMCとは

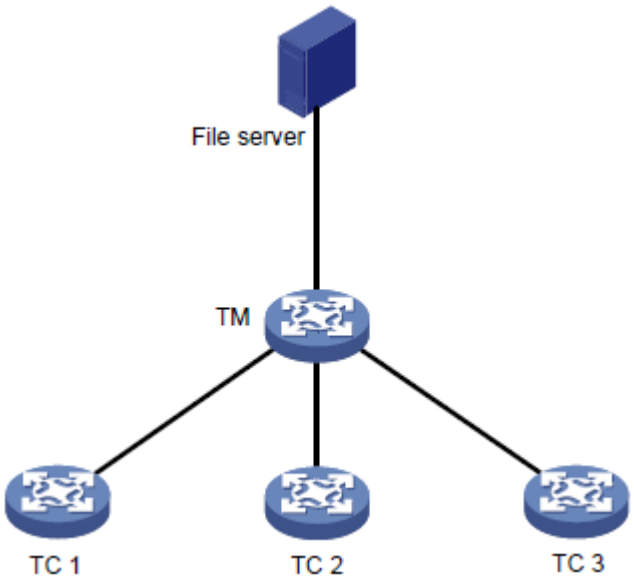
Smart Management Center(SmartMC)は、分散したネットワークデバイスをネットワークエッジで一元的に管理および維持します。SmartMCネットワークでは、1つのデバイスのみがコマンダーとして機能し、残りのデバイスはすべてメンバーとして機能します。SmartMCには、コマンダーからメンバーを管理するための次の機能が用意されています。

- コンフィギュレーションファイルのバックアップとダウンロード
- ソフトウェアのアップグレード。
- 設定の適用。
- 不良メンバー交換

SmartMCネットワークフレームワーク

図1は、SmartMCネットワークの基本的な枠組みを示しています。

図1 SmartMCネットワークのフレームワーク



SmartMCネットワークには、次の要素が含まれます。

- **Commander**: トポロジーマスター(TM)とも呼ばれ、SmartMCネットワーク内のすべてのメンバーを管理します。
- **Member**: トポロジークライアント(TC)とも呼ばれ、コマンダーによって管理されます。
- **File server**: コマンダーとメンバーのスタートアップソフトウェアイメージとコンフィギュレーションファイルを保存します。

SmartMCネットワークの構築

SmartMCネットワークは、自動または手動で確立できます。自動で確立されたSmartMCネットワークでは、コマンダーはNETCONFセッションを通じてメンバー情報を取得し、ネットワークトポロジーを形成します。メンバー情報には、ポート情報、LLDPネイバー情報、STP情報、デバイスタイプ、およびソフトウェアバージョンが含まれます。手動で確立されたSmartMCネットワークでは、コマンダーはNETCONFセッションを通じてメンバーのLLDPネイバー情報を取得し、SNMP Get操作を通じてメンバーのハードウェア情報を取得します。

自動SmartMCネットワーク構築

コマンダーとメンバーは、次の手順を使用してSmartMCネットワークを確立します。

1. SmartMCがイネーブルになると、コマンダーは15秒間隔でSmartMCパケットをブロードキャストして、ネットワーク内のメンバーを検出します。SmartMCパケットには、コマンダーのブリッジMACアドレスやVLANインターフェイス1のIPアドレスなど、コマンダーの情報が含まれます。
2. メンバーはパケットを受信すると、コマンダー情報を記録し、応答パケットをコマンダーに返します。応答パケットには、メンバーのブリッジMACアドレスやVLANインターフェイス1のIPアドレスなど、メンバーの情報が含まれています。
3. コマンダーは応答パケットを受信すると、デフォルトのユーザー名adminとパスワードadminを使用して、メンバーへのNETCONFセッションを開始します。コマンダーは、セッションを通じて、ポート情報、LLDPネイバー情報、STP情報、デバイスタイプ、ソフトウェアバージョンなど、メンバーに関する詳細情報を取得します。
4. コマンダーは、メンバーの活性を追跡するためにメンバーへの接続を確立し、SmartMCネットワークにメンバーを追加します。
5. コマンダーは、すべてのメンバーから取得したLLDPネイバー情報に基づいて、SmartMCトポロジーを形成します。

SmartMCネットワークが確立された後、指揮官とメンバーはSmartMCパケットを交換することによって互いの存在を確認する。

- メンバーは、コマンダーからSmartMCブロードキャストパケットを受信すると、パケット内のブリッジMACアドレスと記録されたブリッジMACアドレスを比較します。2つのブリッジMACアドレスが同じ場合、メンバーはコマンダーに応答パケットを返します。メンバーが制限時間内にコマンダーからブロードキャストパケットを受信しない場合、メンバーはコマンダーがネットワークに存在しなくなったと判断します。その後、メンバーはコマンダー情報をクリアします。制限時間は、60～120秒の範囲のランダムな値です。
- コマンダーは、メンバーからの応答パケットを受信すると、パケット内のブリッジMACアドレスを、記録されているブリッジMACアドレスと比較します。2つのブリッジMACアドレスが同じ場合、コマンダーはそのメンバーがまだネットワーク内に存在すると判断します。コマンダーが150秒以内にメンバーからの応答パケットを受信しない場合、コマンダーはそのメンバーがオフラインであると判断します。次に、コマンダーはそのメンバーのステータスをオフラインに設定します。

SmartMCネットワークの手動設定

コマンダーのWebインターフェイスにログインし、メンバーのIPアドレス、ユーザー名、およびパスワードを入力して、ネットワークに手動で追加できます。メンバーは、コマンダーとSmartMCパケットを交換せずにネットワークに参加できます。詳細については、『Comware 7 Webベース製品ユーザーガイド』を参照してください。

コマンダーでメンバーの情報を指定すると、コマンダーは次の操作を実行してメンバーをネットワークに追加します。

- Telnetを使用してメンバーにアクセスできることを確認します。
- NETCONFを介して、LLDPネイバー情報を含む基本メンバー情報を取得します。
- SNMP Get操作を通じてハードウェア情報を取得します。

SmartMCの機能

メンバーの一括設定の展開

この機能を使用すると、コマンダーから複数のコマンドラインをメンバーに展開できるため、メンバーにログインしてコマンドを1つずつ設定する必要がなくなります。
一括設定展開の手順は次のとおりです。

1. コマンダーはTelnetクライアントとして機能し、メンバーへのTelnet接続を確立します。
2. コマンダーは、Telnet接続を介してバッチファイルをメンバーに展開します。バッチファイルはコマンダー上に作成され、展開されるコマンドラインを含みます。
3. メンバーは、ファイル内のコマンドラインを実行します。

APとIP Phoneを接続するポートの一括設定展開

バッチファイル展開をイネーブルにすると、コマンダーは指定されたバッチファイル内の設定をAPまたはIP Phoneに接続しているポートに自動的に展開し、アクセスポートの設定を簡素化します。

コマンダーは、LLDPを介してポート上でAPまたはIP電話のアソシエーションを最初に検出すると、指定されたバッチファイル内のコマンドラインをポートに展開します。デバイスタイプにバッチファイルが指定されていない場合、ポート上の設定は変更されません。
APまたはIP Phoneがポートから切断されても、ポートの設定は残ります。新しいデバイスがポートからオンラインになると、ポートで使用される設定は新しいデバイスタイプに依存します。

- 新しいデバイスがAPまたはIP Phoneで、切断されたデバイスと同じタイプの場合、ポートの設定は変更されません。
- 新しいデバイスがAPまたはIP Phoneで、接続解除されたデバイスとタイプが異なる場合、コマンダーは指定されたバッチファイルのコマンドラインをポートに展開します。デバイスタイプにバッチファイルが指定されていない場合、ポートの設定は変更されません。
- 新しいデバイスがAPでもIP電話でもない場合、ポートの設定は変更されません。

コマンダーによるバッチファイルのSmartMCへの展開をディセーブルにするには、指定されたバッチファイルを削除するか、**undo port batch-file-apply enable**コマンドを実行してバッチファイル展開をディセーブルにします。

設定ファイルのバックアップ

次の方法を使用して、コマンダーおよびメンバーのnext-startupコンフィギュレーションファイルをバックアップできます。

- 自動バックアップコマンダーとネットワーク内のすべてのメンバーがすぐにバックアップを実行できるように、この機能を有効にします。その後、コマンダーとメンバーは、ユーザーが指定した間隔で設定ファイルをバックアップします。
- 手動バックアップコマンダー、指定されたメンバー、またはSmartMCグループのバックアップを手動でトリガーします。

メンバーのコンフィギュレーションファイルをバックアップするために、コマンダーはSmartMCパケットをユニキャストしてメンバーに指示します。メンバーがパケットを受信すると、コマンダーは実行コンフィギュレーションをnext-startupコンフィギュレーションファイルに保存し、そのファイルをファイルサーバーにアップロードします。

スタートアップソフトウェアと設定ファイルのアップグレード

この機能を使用すると、コマンダーからメンバーデバイスのスタートアップソフトウェアとコンフィギュレーションファイルをアップグレードできます。
アップグレードの前に、コマンダーからファイルサーバーにアップグレードファイルをアップロードし、メンバーがダウンロードするファイルサーバー上のアップグレードファイルを指定する必要があります。

スタートアップソフトウェアおよびコンフィギュレーションファイルのアップグレード手順は次のとおりです。

1. コマンダーは、メンバー(またはSmartMCグループ)に、ファイルサーバーからアップグレードファイルをダウンロードするように指示します。
2. メンバーは、ファイル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ます。
3. メンバーは、スタートアップソフトウェアと設定ファイルを次のようにアップグレードします。
    - **Startup software upgrade**: アップグレードスタートアップソフトウェアファイルを使用してISSUを実行します。メンバーはアップグレードプロセス中に再起動される場合があります。
    - **Configuration file upgrade**: 現在の構成ファイルをアップグレード構成ファイルに置き換えます。メンバーはアップグレードプロセス中に再起動されません。

不良メンバー交換

次の方法を使用して、障害のあるメンバーを置換できます。

- **Automatic replacement**: コマンダーは、トポロジー内のすべてのメンバーの位置を記録して置換できます。コマンダーは、新しいメンバーが障害のあるメンバーを物理的に置換したことを検出すると、新しいメンバーと障害のあるメンバーを比較します。コマンダーは、次の要件が満たされている場合に置換を実行します:
    - 新しいメンバーは、障害のあるメンバーと同じトポロジー上の位置に配置されます。
    - 新しいメンバーと障害のあるメンバーのモデルは同じです。

    コマンダーは、新しいメンバーに対して、障害のあるメンバーの構成ファイルをファイルサーバーからダウンロードするように指示します。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。
- **Manual replacement**: 障害のあるメンバーが物理的に置換された後、構成の置換を手動でトリガーします。新しいメンバーは、ファイルサーバーから障害のあるメンバーの構成ファイルをダウンロードし、ファイルを実行して置換を完了します。

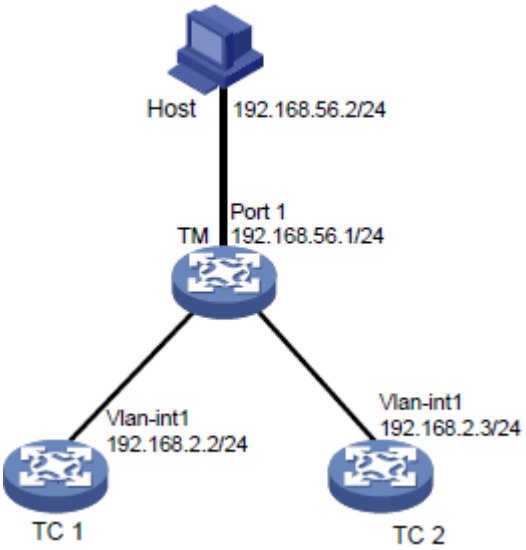
SmartMCネットワークのOutgoing(発信)インターフェイス

発信インターフェイス機能を使用すると、発信インターフェイスに接続するホストは、SmartMCネットワーク内のすべてのメンバーにアクセスできます。SmartMCネットワークには、複数の発信インターフェイスを設定できます。

図2に示すように、ホストはTMのポート1に接続されており、TC 1とTC 2はホストとは異なるネットワークセグメントにあります。ホストはTMのWebインターフェイスにアクセスできますが、どのメンバーのWebインターフェイスにもアクセスできません。
TMのポート1が発信インターフェイスとして設定されている場合、システムは各メンバーのIPアドレスを新しいアドレスにミラーリングします。新しいアドレスには、発信インターフェイスのIPアドレスと、コマンダーによってメンバーに割り当てられたポート番号がIPアドレス:ポート番号の形式で含まれます。これにより、ホストはTMのWebインターフェイスからメンバーのWebインターフェイスにアクセスできます。

メンバーのWebインターフェイスにアクセスするには、コマンダーのWebインターフェイスに入り、ナビゲーションペインで**Visibility**をクリックします。次に、**Topology**タブをクリックし、ターゲットメンバーを選択して、**Login to Web interface**をクリックします。

図2 SmartMCネットワーク



自動リンクアグリゲーション

自動リンクアグリゲーションは、2つのメンバー間の複数の物理イーサネットリンクを、アグリゲーションリンクと呼ばれる1つの論理リンクに自動的にバンドルします。この機能により、リンク帯域幅が増加し、リンクの信頼性が向上します。

注:

- コマンダーとメンバー間、またはメンバーとSmartMCネットワーク外のデバイス間では、自動リンク集約を実行できません。コマンダーとメンバー間のリンクは手動で集約できます。手動リンク集約の詳細については、『Layer 2 LAN Switching Configuration Guide』の「Ethernet Link Aggregation」を参照してください。
- 自動リンクアグリゲーションが有効になっているメンバーが、コマンダーがアグリゲーション機能で無効になっているSmartMCネットワークに参加すると、そのメンバーの機能も無効になります。これは、メンバーのサービストラフィックフォワーディングに影響を与える可能性があります。

メンバーのVLAN作成

設定と管理を簡素化するために、メンバー用のVLANを作成できます。その後、他のメンバーまたはコマンダーに接続されていないメンバー上のすべてのアクセスポートがVLANに割り当てられます。
メンバーのアクセスポートがオフラインデバイスに接続されている場合は、メンバーのVLANを作成する前にオフラインデバイスを削除する必要があります。
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。

リソースの監視

リソースモニタリングを使用すると、コマンダーおよびコマンダー上のメンバーのCPU使用率、メモリ使用率、温度情報、およびパケット廃棄情報を表示できます。パケット廃棄モニタリングは、メンバーおよびインターフェイス上のパケット廃棄を監視します。

コマンダーのWebインターフェイスの**SmartMC > Intelligent O&M > Resource monitoring**ページから、コマンダーの使用状況と温度情報、およびパケット廃棄情報を表示できます。

制約事項およびガイドライン:SmartMCの設定

SmartMCは、デフォルトのMDCでのみサポートされます。

SmartMCを設定できるのは、ネットワーク管理者ロールを持つユーザーだけです。ユーザーロールの詳細については、『Fundamentals Configuration Guide』の「RBAC」を参照してください。

SmartMCネットワークがVLAN 1で確立されています。ネットワークが正常に動作するためには、VLAN 1でセキュリティ設定を行わないでください。
コマンダーとメンバーの両方でSmartMCを有効にし、他のすべてのSmartMCタスクはコマンダーでのみ実行する必要があります。
次の機能は、SmartMCネットワークに自動的に追加されたメンバーに対してのみ有効です。

- 設定ファイルのバックアップ。
- 不良メンバーの交換
- スタートアップソフトウェアと設定ファイルのアップグレード
- 自動リンクアグリゲーション。

SmartMCタスク一覧

SmartMCを設定するには、次のタスクを実行します。

1. SmartMCの有効化
2. ファイルサーバーの指定

   この作業は、自動コンフィギュレーションファイルバックアップの設定、障害のあるメンバーの交換、およびメンバー上のスタートアップソフトウェアとコンフィギュレーションファイルのアップグレードに必要です。
3. (オプション)SmartMCネットワークの発信インターフェイスの設定
4. (任意)自動イーサネットリンク集約のイネーブル化
5. (オプション)メンバーのデフォルトユーザーのパスワードの変更
6. SmartMCグループの作成

   このタスクは、メンバーのスタートアップソフトウェアと設定ファイルをアップグレードし、SmartMCグループにバッチファイルを展開するために必要です。
7. (省略可能)構成の展開と管理
   - メンバーのVLANの作成
   - メンバーへのバッチファイルの配置
   - APまたはIP Phoneを接続するポートのバッチファイルの設定
   - 設定ファイルのバックアップ
8. (省略可能)SmartMCネットワークの監視と保守
   - リソース監視の設定
   - メンバーのスタートアップソフトウェアと構成ファイルのアップグレード
   - ネットワークトポロジーの管理
   - 障害のあるメンバーの置換

SmartMCの前提条件

SmartMCを設定する前に、コマンダーとメンバーに対して次のタスクを実行します。

- Telnetサービスをイネーブルにし、VTYユーザー回線のスキーム認証を設定します。Telnetサービスおよび VTYユーザー回線の詳細については、『Fundamentals Configuration Guide』の「CLI login configuration」を参照してください。
- ローカルユーザーを設定します。
  - ユーザー名とパスワードを指定します。
    - コマンダーで、ユーザー名とパスワードが、**smartmc tm username** *username* **password** { **cipher** | **simple** } *string* **enable**コマンドを使用して設定されたユーザー名とパスワードと同じであることを確認します。
    - メンバーで、ユーザー名とパスワードの両方を**admin**に設定し**password-control length 4**, **password-control composition type-number 1 type-length 1**, そして **undo password-control complexity user-name check**コマンドを使用して、パスワードの複雑さの要件を下げます。

      これは、SmartMCでは、コマンダーがユーザー名adminとパスワードadminを使用してメンバーと通信する必要があり、デフォルトのパスワードの複雑さの要件を満たしていないためです。これらのコマンドの詳細については、『Security Command Reference』の**password control**コマンドを参照してください。

      SmartMCネットワークが確立されたら、パスワードの複雑さの要件を増やし、**SmartMC tc password**コマンドを使用してユーザー名とパスワードを変更できます。
  - ユーザーのTelnet、HTTP、およびHTTPSサービスを指定します。
  - ローカルユーザーのRBACロールをnetwork-adminに設定します。

  ローカルユーザーの詳細については、『Security Configuration Guide』の「AAA configuration」を参照してください。ユーザーロールの詳細については、『Fundamentals Configuration Guide』の「RBAC configuration」を参照してください。
- NETCONF over SOAP over HTTPを有効にします。NETCONF over SOAPの詳細は、『Network Management and Monitoring Configuration Guide』のNETCONF configurationを参照してください。
- LLDPをグローバルにイネーブルにします。LLDPの詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。
- Webインターフェイスを介してコマンダーとメンバーを管理するには、HTTPサービスとHTTPSサービスを有効にし、ローカルユーザーのサービスタイプをHTTPとHTTPSに設定する必要があります。Webログイン、HTTP、およびHTTPSの詳細については、『Fundamentals Configuration Guide』を参照してください。
- SmartMCネットワークを手動で確立するには、メンバーに**snmp-agent community read public**コマンドおよび**snmp-agent sys-info version v2c**コマンドを設定する必要があります。SNMPの詳細については、『Network Management and Monitoring Configuration Guide』を参照してください。

SmartMCの有効化

このタスクについて

コマンダーからメンバーを管理できるようにするには、コマンダーとメンバーの両方でこの機能を有効にします。

制限事項およびガイドライン

SmartMCネットワークには、コマンダーが1つだけ必要です。
コマンダーのロールをメンバーに変更するか、コマンダーのSmartMCをディセーブルにすると、実行コンフィギュレーションのすべてのSmartMC設定がクリアされます。

ACLリソースが不足していると、SmartMCを有効にできません。ACLリソースが不足している場合は、**undo acl**コマンドを使用して不要なACLを削除してから、SmartMCを有効にしてください。**display acl**コマンドを実行すると、ACLの構成と試合の統計を表示できます。ACLの詳細については、『ACL and QoS Configuration Guide』を参照してください。

ポート80および443が使用されている場合、SmartMCをイネーブルにできません。

smartmc enableコマンドを複数回実行すると、最新の設定が有効になります。このコマンドを実行して、デバイスロールまたはパスワードを変更できます。

手順

1. システムビューに入ります。
   system-view
2. SmartMCをイネーブルにし、デバイスロールを設定します。
   smartmc { **tc** | **tm username** *username* **password** { **cipher** | **simple** } *string* } **enable**
   デフォルトでは、SmartMCはディセーブルになっています。

ファイルサーバーの指定

このタスクについて

SmartMCのネットワークでは、次のファイルを保存するためにファイルサーバーが使用されます。

- スタートアップソフトウェアファイルをアップグレードし、メンバーの設定ファイルをアップグレードします。
- コマンダーとメンバーの設定ファイルをバックアップします。

システムは、ファイルサーバーとしてFTPまたはSFTPサーバーの使用をサポートしています。FTPサーバーの詳細については、『Fundamentals Configuration Guide』の「configuring FTP」を参照してください。SFTPサーバーの詳細については、『Security Configuration Guide』の「configuring SSH」を参照してください。

制限事項およびガイドライン

次の方法を使用して、ファイルサーバーを指定できます。

- ファイルサーバーのIPアドレスを指定します。
- コマンダーのIPアドレスを指定します。コマンダーはファイルサーバーとして機能します。

コマンダーをファイルサーバーとして動作するように設定するには、コマンダーに、メンバーが必要とするファイルを格納するための十分なストレージ領域があることを確認します。
独立したファイルサーバーを使用するには、メンバーではなくコマンダーにファイルサーバーを接続することをお勧めします。ファイルサーバーは、VLAN 1を使用してSmartMCネットワークと通信します。ファイルサーバーをメンバーに接続する場合、メンバーのVLANを作成すると、ファイルサーバーに接続しているメンバーインターフェイスが作成されたVLANに割り当てられるため、ファイルサーバーが切断されます。メンバーVLANの作成の詳細については、「メンバーのVLANの作成」を参照してください。

手順

1. システムビューに入ります。

   system-view

2. ファイルサーバーを指定します。
   smartmc { **ftp-server** | **sftp-server** } { *ipv4-address* | **ipv6** *ipv6-address* } [**port** *port*] [**vpn-instance** *vpn-instance-name*] [**directory** *directory*] **username** *username* **password** { **cipher** | **simple** } *string*
   デフォルトでは、ファイルサーバーは指定されていません。

SmartMCネットワーク用の**Outgoing(発信)**インターフェイスの設定

制限事項およびガイドライン

SmartMCネットワークがVLAN 1で確立されているため、VLAN-interface 1は発信インターフェイスとして使用できません。
レイヤ3集約グループのメンバーポートは、SmartMCの発信インターフェイスとして使用できません。その逆も同様です。設定された発信インターフェイスがレイヤ3集約グループのメンバーポートである場合、発信インターフェイスは有効になりません。レイヤ3集約グループの詳細については、『Layer 2 LAN Switching Configuration Guide』の「Ethernet Link Aggregation」を参照してください。

VLANインターフェイスを発信インターフェイスとして指定すると、service slot slot-numberコマンドが発信インターフェイスおよびVLAN-interface 1に対して発行されます。slot-number引数は、アクティブなMPUのスロット番号を表します。レイヤ3イーサネットインターフェイスを発信インターフェイスとして指定すると、VLAN-interface 1に対してだけコマンドが発行されます。発信インターフェイス設定を削除すると、service slot slot-number設定は残り、必要に応じて設定を手動で変更できます(スタンドアロンモードの場合)。

VLANインターフェイスを発信インターフェイスとして指定した場合、システムは**service chassis** *chassis-number* **slot** *slot-number*コマンドを発信インターフェイスおよびVLAN-interface 1に発行します。chassis-number引数はマスターデバイスのメンバーIDを表し、slot-number引数はグローバルアクティブMPUのスロット番号を表します。レイヤを指定した場合
3イーサネットインターフェイスを発信インターフェイスとして使用する場合、システムはVLAN-interface 1に対してだけコマンドを発行します。発信インターフェイス設定を削除しても、**service slot** *slot-number*設定は残り、必要に応じて設定を手動で変更できます(IRFモード)。

serviceコマンドの詳細については、『Layer 2 LAN Switching Command Reference』の「VLANコマンド」を参照してください。

手順

1. システムビューに入ります。

   system-view

2. VLANインターフェイスビューまたはレイヤ3イーサネットインターフェイスビューを開始します。
   - VLANインターフェイスビューを開始します。

     interface vlan *interface-number*
   - レイヤ3イーサネットインターフェイスビューを開始します。

     interface *interface-type interface-number*

3. インターフェイスを発信インターフェイスとして設定します。

   smartmc outbound

   デフォルトでは、発信インターフェイスとして使用されるインターフェイスはありません。

自動イーサネットリンク集約のイネーブル化

制限事項およびガイドライン

自動リンクアグリゲーションを有効または無効にすると、ネットワークのフラッピングが発生し、メンバーが短時間オフラインになる場合があります。

手順

1. システムビューに入ります。

   system-view
2. 自動イーサネットリンク集約をイネーブルにします。

   smartmc auto-link-aggregation enable

   デフォルトでは、自動イーサネットリンク集約はディセーブルになっています。

メンバーのデフォルトユーザーのパスワードの変更

このタスクについて

SmartMCネットワークの確立中、コマンダーはデフォルトのユーザー名とパスワードを使用して、ネットワークに自動的に追加されたメンバーに対してNETCONFセッションを確立します。NETCONFセッション確立用のメンバーのデフォルトのユーザー名とパスワードは、**admin**と**admin**です。

セキュリティを強化するには、コマンダーがメンバーをネットワークに追加した後で、このタスクを実行して、メンバーのデフォルトユーザー**admin**のパスワードを変更します。

制限事項およびガイドライン

SmartMCのネットワークに手動で追加されたメンバーのパスワードは変更しないでください。手動で追加されたメンバーのパスワードを変更すると、コマンダーからそのメンバーを管理できなくなります。

メンバーの追加に使用されたメソッドを識別するには、**display smartmc tc verbose**コマンドを使用します。

手順

1. システムビューに入ります。

   system-view
2. メンバーのデフォルトユーザーのパスワードを変更します。

   smartmc tc password [**cipher**] *string*

SmartMCグループの作成

このタスクについて

この機能を使用すると、コマンダーにSmartMCグループを作成し、そのグループにメンバーを追加できます。次の操作を実行するときに、SmartMCグループを指定して、グループ内のすべてのメンバーに操作を適用できます。

- スタートアップソフトウェアのアップグレード。
- 設定ファイルのアップグレード。
- 設定の展開。

手順

1. システムビューに入ります。

system-view

2. SmartMCグループを作成し、そのビューに入ります。

   smartmc group *group-name*

3. (任意)定義済みのデバイスタイプを表示します。

   match device-type ?

4. 一致基準を設定します。

   Match { **device-type** *device-type* | **ip-address** *ip-address* { *ip-mask-length* | *ip-mask* } | **mac-address** *mac-address mac-mask-length* }
   デフォルトでは、一致基準は設定されていません。

5. メンバーのデバイスタイプがコマンダーで事前に定義されていない場合は、次のタスクを実行して、コマンダーでデバイスタイプを手動で定義します。

   a. システムビューに戻ります。

      quit

   b. コマンダーでデバイスタイプを定義します。

      smartmc tc sysoid *sysoid* **device-type** *device-type*

      メンバーのSYSOIDを取得するには、**display smartmc tc verbose**を実行します。

      定義済のメンバータイプを別のタイプとして定義することはできません。

メンバーのVLANの作成

制限事項およびガイドライン

メンバーのVLANを作成するためにこのタスクを複数回実行すると、最新の設定が有効になります。

手順

1. システムビューに入ります。

   system-view

2. メンバーのVLANを作成し、メンバーのアクセスポートをVLANに割り当てます。

   smartmc vlan *vlan-id* { **group** *group-name-list* | **tc** *tc-id-list* }

メンバーへのバッチファイルの配置

1. ユーザービューで次のコマンドを実行して、バッチファイルを作成し、メンバーに展開するコマンド行を編集します。

   create batch-file *cmd-filename*

   各コマンドは、バッチファイル内の1行を占めます。編集が終了したら、パーセント記号(%)を入力してユーザービューに戻ります。

   システムはコマンドラインが正しいかどうかを検証しないため、入力するコマンドラインが正しいことを確認してください。

2. システムビューに入ります。

   system-view

3. メンバーまたはSmartMCグループのリストにバッチファイルを配布します。

   smartmc batch-file *cmd-filename* **deploy** { **group** *group-name-list* | **tc** *tc-id-list* }

APまたはIP Phoneを接続するポートのバッチファイルの設定

制限事項およびガイドライン

バッチファイル内のすべてのコマンドは、インターフェイスビューで使用されるコマンドである必要があります。バッチファイルのサイズは8190文字を超えることはできません。

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。

手順

1. (任意)ユーザービューで次のコマンドを実行して、バッチファイルを作成し、メンバーに展開するコマンドラインを編集します。

   create batch-file *cmd-filename*

   各コマンドは、バッチファイル内の1行を占めます。編集が終了したら、パーセント記号(%)を入力してユーザービューに戻ります。

   システムはコマンドラインが正しいかどうかを検証しないため、入力するコマンドラインが正しいことを確認してください。
2. システムビューに入ります。

   system-view
3. APまたはIP Phoneを接続するポートのバッチファイルを指定します。

   smartmc batch-file *batch-file-name* **apply** { **ap**| **phone**}
4. (任意)バッチファイル展開をディセーブルにします。

   undo smartmc batch-file-apply enable

   デフォルトでは、バッチファイル展開は有効になっています。

設定ファイルのバックアップ

このタスクについて

コマンダーまたは指定したメンバーのコンフィギュレーションファイルをバックアップするには、次の作業を実行します。ファイルサーバーに自動的にバックアップされるコンフィギュレーションファイルには、*device_bridge_MAC_address*_**backup.cfg**の形式で名前が付けられます。

制限事項およびガイドライン

SmartMCのネットワークでコマンダーを変更するときは、ファイルサーバー上の元のコマンダーのバックアップ設定ファイルが削除されていることを確認してください。ファイルがまだ存在する場合は、新しいコマンダーがファイルをダウンロードして設定を実行する可能性があります。これにより、ネットワークで競合が発生します。

自動構成を同時に実行できるメンバーの最大数は、ファイルサーバーのパフォーマンスによって制限されます。自動構成バックアップが失敗した場合は、メンバーの最大数をより小さい値に設定します。

前提条件

このタスクを実行する前に、ファイルサーバーを指定する必要があります(「ファイルサーバーの指定」を参照)。

手順

1. システムビューに入ります。
   system-view
2. 構成ファイルのバックアップを同時に実行できるメンバーの最大数を設定します。
   smartmc backup configuration max-number *max-number*
   デフォルトでは、最大5つのメンバーが同時に自動設定バックアップを実行できます。
3. 構成ファイルをバックアップします。必要に応じて、次のいずれかのオプションを選択します。
   - 自動構成ファイルバックアップを有効にし、バックアップ間隔を設定します。
     smartmc backup startup-configuration interval *interval-time*
     デフォルトでは、自動構成ファイルバックアップは無効になっています。
   - コマンダーまたは指定したメンバーの設定ファイルを手動でバックアップします。
     smartmc backup configuration { **group** *group-name-list* | **tc**[*tc-id-list*] }
     TC ID 0はコマンダーを表します。

リソース監視の設定

1. システムビューに入ります。
   system-view
2. コマンダーがリソース監視情報を取得する間隔を設定します。
   smartmc resource-monitor interval *interval*
   デフォルト設定は1分です。
3. リソース監視情報のエージングタイムを設定します。
   smartmc resource-monitor max-age *max-age*
   デフォルト設定は24時間です。
4. リソース監視を有効にします。
   smartmc resource-monitor [**cpu** | **memory** | **packet-drop** | **temperature**] * [**group** *group-name-list* | **tc** { *tc-id-list* | **mac-address**s *mac-address* } | **tm**]
   デフォルトでは、リソースモニタリングはディセーブルです。
   リソースタイプを指定しない場合、このコマンドはすべてのリソースタイプのリソースモニタリングをイネーブルにします。
   監視するデバイス(メンバーまたはコマンダー)を指定しない場合、このコマンドはコマンダーおよびすべてのメンバーのリソース監視をイネーブルにします。

メンバーのスタートアップソフトウェアと構成ファイルのアップグレード

メンバーのスタートアップソフトウェアと設定ファイルのアップグレードについて

次の方法を使用して、メンバーのスタートアップソフトウェアと設定ファイルをアップグレードできます。

- アップグレード時間またはアップグレード遅延を指定して、アップグレードをスケジュールします。
- アップグレード時間またはアップグレード遅延を指定しないで、ただちにアップグレードします。

スタートアップソフトウェアおよびコンフィギュレーションファイルのアップグレードに関する制約事項およびガイドライン

メンバーは、一度に1つのアップグレードタスクしか実行できません。

即時アップグレードは取り消すことができません。遅延時間またはアップグレード時間を指定してスケジュール済アップグレードを実行する場合、アップグレード操作は、開始前に**undo smartmc upgrade**コマンドを使用して取り消すことができます。

前提条件

このタスクを実行する前に、ファイルサーバーを指定する必要があります(「ファイルサーバーの指定」を参照)。

メンバーのスタートアップソフトウェアと構成ファイルのアップグレード

1ステップでのスタートアップソフトウェアと設定ファイルのアップグレード

1. システムビューに入ります。

   system-view

2. メンバーのスタートアップソフトウェアを1つの手順でアップグレードします。
   smartmc upgrade boot-loader tc { *tc-id-list* { **boot** *boot-filename* **system** *system-filename* | **file** *ipe-filename* } } &<1-40> [**delay** *delay-time* | **time** *in-time*]

3. メンバーの構成ファイルを1つの手順でアップグレードします。

   smartmc upgrade startup-configuration tc { *tc-id-list cfg-filename* }&<1-40> [**delay** *delay-time* | **time** *in-time*]

スタートアップソフトウェアと設定ファイルのアップグレードの段階的な設定

1. システムビューに入ります。

   system-view

2. メンバーのスタートアップソフトウェアのアップグレードを段階的に設定します。

   a. アップグレードスタートアップソフトウェアファイルを指定します。

      smartmc tc *tc-id* **boot-loader** { *ipe-filename* | **boot** *boot-filename* **system** *system-filename* }

b. メンバーのスタートアップソフトウェアをアップグレードします。

smartmc upgrade boot-loader tc *tc-id-list*

3. メンバーのコンフィギュレーションファイルのアップグレードをステップごとに設定します。

a. アップグレードコンフィギュレーションファイルを指定します。

smartmc tc*tc-id***startup-configuration***cfg-filename*

b. メンバーの構成ファイルをアップグレードします。

smartmc upgrade startup-configuration tc *tc-id-list*

SmartMCグループのすべてのメンバーでのスタートアップソフトウェアと設定ファイルのアップグレード

1ステップでのスタートアップソフトウェアと設定ファイルのアップグレード

1. システムビューに入ります。

system-view

2. SmartMCグループのすべてのメンバーのスタートアップソフトウェアを1つの手順でアップグレードします。

smartmc upgrade boot-loader group { *group-name-list* [**boot** *boot-filename* **system** *system-filename* | **file** *ipe-filename*] } &<1-40> [**delay** *minutes* | **time** *in-time*]

3. SmartMCグループ内のすべてのメンバーのコンフィギュレーションファイルを1つの手順でアップグレードします。

smartmc upgrade startup-configuration group { *group-name-list cfg-filename*} &<1-40> [**delay** *minutes*| **time** *in-time*]

スタートアップソフトウェアと設定ファイルのアップグレードの段階的な設定

1. システムビューに入ります。

system-view

2. SmartMCグループビューに入ります。

smartmc group *group-name*

3. SmartMCグループのアップグレードスタートアップソフトウェアファイルを指定します。
boot-loader file { *ipe-filename* | **boot** *boot-filename* **system** *system-filename*}

デフォルトでは、SmartMCグループにアップグレードスタートアップソフトウェアファイルは指定されていません。

4. SmartMCグループのアップグレードコンフィギュレーションファイルを指定します。

startup-configuration *cfgfil*

デフォルトでは、SmartMCグループにアップグレードコンフィギュレーションファイルは指定されていません。

5. システムビューに戻ります。

quit

6. SmartMCグループのすべてのメンバーで、スタートアップソフトウェアと設定ファイルをアップグレードします。必要に応じて、次のいずれかのオプションを選択します。

- スタートアップソフトウェアをアップグレードします。
smartmc upgrade boot-loader group *group-name-list* [**delay** *minutes*| **time** *in-time*]
- 設定ファイルをアップグレードします。
smartmc upgrade startup-configuration group *group-name-list* [**delay** *minutes* | **time** *in-time*]

ネットワークトポロジーの管理

ネットワークトポロジーの更新

このタスクについて

次の方法を使用して、ネットワークトポロジーを更新できます。

- **Automatic topology refresh**: 更新間隔を指定して、コマンダーがネットワークトポロジーを定期的に更新できるようにします。
- **Manual topology refresh**: ネットワークトポロジーを手動で更新するには、smartmc topology-refreshコマンドを実行します。

制限事項およびガイドライン

トポロジーのリフレッシュ時間は、ネットワーク内のメンバーの数によって異なります。

手順

必要に応じて、次のいずれかのオプションを選択します。

- いずれかのビューでネットワークトポロジーを手動で更新します。

  smartmc topology-refresh
- ネットワークトポロジーの自動更新を設定します。
  a. システムビューに入ります。

     system-view
  b. トポロジーの自動更新間隔を設定します。

     smartmc topology-refresh interval *interval*

     デフォルトでは、トポロジーの自動更新間隔は60秒です。

ネットワークトポロジーの保存

このタスクについて

このタスクでは、現在のネットワークトポロジーをフラッシュメモリ内の**topology.dba**ファイルに保存できます。コマンダーは再起動後、**topology.dba**ファイルを使用してネットワークトポロジーを復元します。

手順

1. システムビューに入ります。

   system-view
2. ネットワークトポロジーを保存します。

   smartmc topology-save

障害のあるメンバーの交換

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ネイバー関係とデバイスモデルが同じであることを確認します。

新しいメンバーのメンバーIDが、オフラインのメンバーを含むSmartMCのネットワーク内のすべてのメンバーと異なることを確認します。障害のあるメンバーはオフラインと見なされます。
故障した部材を自動的に交換するには、まず自動交換を有効にしてから、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接続します。

故障したメンバーを手動で交換するには、まず故障したメンバーが取り付けられていた場所に新しいメンバーを取り付け、すべてのケーブルを接続してから、手動交換コマンドを実行します。

前提条件

障害のあるメンバーを交換する前に、ファイルサーバーを指定します(「ファイルサーバーの指定」を参照)。

手順

1. システムビューに入ります。

   system-view
2. 障害のあるメンバーを置換します。

   必要に応じて、次のいずれかのオプションを選択します:

   - 障害のあるメンバーの自動置換を有効にします。
     smartmc auto-replace enable
     デフォルトでは、障害のあるメンバーの自動置換は無効になっています。
   - 障害のあるメンバーを手動で交換します。
     smartmc replace tc *tc-id1* **faulty-tc** *tc-id2*

SmartMCの表示およびメンテナンスコマンド

任意のビューで表示コマンドを実行します。

タスク	コマンド
メンバーのバックアップステータスを表示します。	**display smartmc backup configuration status**
バッチファイルの実行結果を表示します。	**display smartmc batch-file status** [**ap** | **last** *number* | **phone**]
SmartMC 構成を表示します。	**display smartmc configuration**
SmartMC ネットワーク内のデバイス間の接続を表示します。	**display smartmc device-link**
SmartMCグループ情報を表示します。	**display smartmc group**[*group-name*] [**verbose**]
不良メンバーの交換状況を表示します。	**display smartmc replace status**
リソース監視情報の表示.	**display smartmc resource-monitor** [**cpu** | **memory** | **temperature**] * [**tc** *tc-id* | **tm**]
リソース監視設定を表示します。	**display smartmc resource-monitor configuration**
メンバー情報を表示します。	**display smartmc tc** [*tc-id*] [**verbose**]
メンバーのログ バッファー内のログ情報を表示します。	**display smartmc tc** *tc-id* **log buffer** [**module** *module-name* [**mnemonic** *mnemonic-value*]]

メンバーの再起動ログ情報を表示します。	**display smartmc tc***tc-id***log restart**
メンバーのVLAN作成結果を表示します。	**display smartmc vlan**
メンバーのアップグレードステータスを表示します。	**display smartmc upgrade status**

SmartMCの設定例

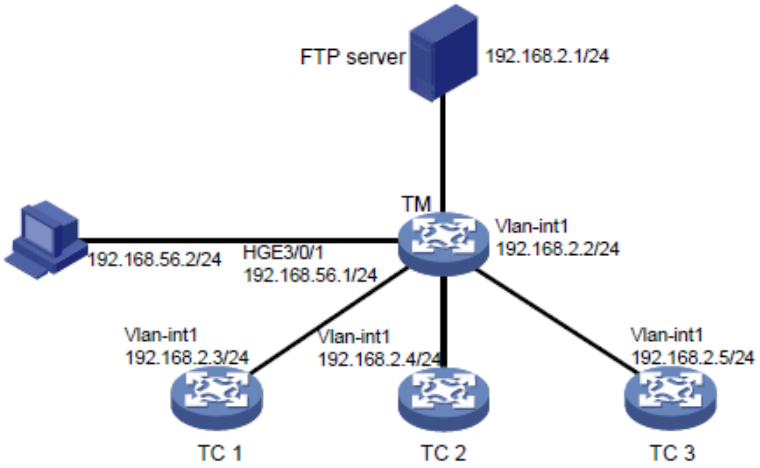
例:SmartMCの設定

ネットワーク構成

図3に示すように、メンバー1、メンバー2、およびメンバー3は同じデバイスタイプ(S12500G-AFシリーズ)に属しています。ファイルサーバーのIPアドレスは192.168.2.1です。ファイルサーバーにアクセスするためのユーザー名とパスワードは、それぞれ**admin**と**hello12345**です。
SmartMCネットワークを確立し、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。

1. SmartMCネットワークを自動的に確立するように、コマンダーとメンバーを設定します。
2. インターフェイスHundredGigE 3/0/1をSmartMCネットワークの発信インターフェイスとして設定します。
3. SmartMCグループを作成し、そのグループにメンバーを追加します。
4. SmartMCグループのすべての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します。
5. コンフィギュレーションファイル**startup.cfg**をファイルサーバーに保存します。

図3ネットワークダイアグラム



手順

1. TC 1を設定します。
   #VLAN-interface 1を設定します。
   <TC1> system-view
   [TC1] interface vlan-interface 1
   [TC1-Vlan-interface1] ip address 192.168.2.3 24
   [TC1-Vlan-interface1] quit
   # HTTP と HTTPSを有効にします
   [TC1] ip http enable
   [TC1] ip https enable
   # Telnetサービスを有効にします
   [TC1] telnet server enable
   # NETCONF over SOAP over HTTPを有効にします
   [TC1] netconf soap http enable
   # LLDPをグローバルに有効にします
   [TC1] lldp global enable
   # パスワードの複雑さの要件が緩和されます。これらのコマンドの詳細については、『セキュリティ コマンド リファレンス』の「パスワード制御コマンド」を参照してください。

[TC1] password-control length 4
[TC1] password-control composition type-number 1 type-length 1
[TC1] undo password-control complexity user-name check
ユーザーを作成します。ユーザー名とパスワードを **admin** に設定し、**telnet**、**http**、および **https** サービス タイプを追加し、ユーザーに **network-admin** ユーザー ロールの使用を許可します。
[TC1] local-user admin
[TC1-luser-manage-admin] password simple admin
[TC1-luser-manage-admin] service-type telnet http https
[TC1-luser-manage-admin] authorization-attribute user-role network-admin
[TC1-luser-manage-admin] quit
VTY ユーザー行 0 ～ 63 のスキーム認証を設定します。
[TC1] line vty 0 63
[TC1-line-vty0-63] authentication-mode scheme
[TC1-line-vty0-63] quit
SmartMC を有効にし、デバイスの役割を tc に設定します。
[TC1] smartmc tc enable

2. 2. TC 1 と同じ方法で TC 2 と TC 3 を設定します。(詳細は省略)

3. TM を構成します:
HundredGigE 3/0/1を設定します
<TM> system-view
[TM] interface hundredgige 3/0/1
[TM-HundredGigE3/0/1] port link-mode route
[TM-HundredGigE3/0/1] ip address 192.168.52.2 24
[TM-HundredGigE3/0/1] quit
VLAN-interface 1を設定します
[TM] interface vlan-interface 1
[TM-Vlan-interface1] ip address 192.168.2.2 24
[TM-Vlan-interface1] quit
HTTP と HTTPSを有効にします
[TM] ip http enable
[TM] ip https enable
Telnetサービスを有効にします
[TM] telnet server enable
NETCONF over SOAP over HTTPを有効にします
[TM] netconf soap http enable
LLDP をグローバルに有効にします
[TM] lldp global enable
パスワードの複雑さの要件が緩和されます。これらのコマンドの詳細については、『セキュリティ コマンド リファレンス』の「パスワード制御コマンド」を参照してください。
[TC1] password-control length 4
[TC1] password-control composition type-number 1 type-length 1
[TC1] undo password-control complexity user-name check
ユーザーを作成します。ユーザー名を **admin**、パスワードを **hello12345** に設定し、**telnet**、**http**、および **https** サービス タイプを追加して、ユーザーに **network-admin** ユーザー ロールの使用を許可します。
[TM] local-user admin
[TM-luser-manage-admin] password simple hello12345
[TM-luser-manage-admin] service-type telnet http https
[TM-luser-manage-admin] authorization-attribute user-role network-admin
[TM-luser-manage-admin] quit
VTY ユーザー行 0 ～ 63 のスキーム認証を設定します。
[TM] line vty 0 63
[TM-line-vty0-63] authentication-mode scheme
[TM-line-vty0-63] quit

SmartMC を有効にし、デバイスの役割をコマンダーに設定し、ユーザー名を **admin** に、パスワード (プレーンテキスト) を **hello12345** に設定します。.
[TM] smartmc tm username admin password simple hello12345 enable
HundredGigE 3/0/1 を発信インターフェースに設定します
[TM] interface hundredgige 3/0/1
[TM-HundredGigE3/0/1] smartmc outbound
[TM-HundredGigE3/0/1] quit
ファイル サーバーの IP アドレス、ユーザー名、平文パスワードをそれぞれ 192.168.2.1、**admin**、および **hello12345** に設定します。
[TM] smartmc ftp-server 192.168.2.1 username admin password simple hello12345
SmartMC グループ **S1** を作成し、そのビューに入ります。
[TM] smartmc group S1
IP アドレス一致基準を作成して、指定されたネットワーク セグメント内のすべてのメンバーを SmartMC グループ **S1** に追加します.
[TM-smartmc-group-S1] match ip-address 192.168.2.0 24
SmartMCグループ**S1**のアップグレード構成ファイル**startup.cfg**を指定します。.
[TM-smartmc-group-S1] startup-configuration startup.cfg
[TM-smartmc-group-S1] quit
SmartMC グループ **S1** のすべてのメンバーの構成ファイルをアップグレードします。
[TM] smartmc upgrade startup-configuration group S1 startup.cfg

設定の確認

Display brief information about all members after the SmartMC network is established.

[TM] display smartmc tc

TCID	DeviceType	Sysname	IpAddress	MacAddress	Status	Version		
1	S12508G-AF	TC1	192.168.2.3	201c-e7c3-0300	Normal	7.1.070	ESS	7593
2	S12508G-AF	TC2	192.168.2.4	201c-e7c3-0301	Normal	7.1.070	ESS	7593
3	S12508G-AF	TC3	192.168.2.5	201c-e7c3-0302	Normal	7.1.070	ESS	7593

Display the configuration file upgrade status on the members.

<TM> display smartmc upgrade status

ID	IpAddress	MacAddress	Status	UpdateTime	UpdateFile
1	192.168.2.3	201c-e7c3-0300	Finished	Immediately	startup.cfg
2	192.168.2.4	201c-e7c3-0301	Finished	Immediately	startup.cfg
3	192.168.2.5	201c-e7c3-0302	Finished	Immediately	startup.cfg