管理

この章は、次の項で構成されています。

システム設定

システム設定ページでは、スイッチの設定をカスタマイズできます。次の設定を行えます。

手順

ステップ 1 [Administration] > [System Settings] の順に選択します。

ステップ 2 システム設定を表示または変更します。

- [System Description]：デバイスの説明が表示されます。
- [System Location]：デバイスの物理的な場所を入力します。
- [System Contact]：担当者の名前を入力します。
- [Host Name]：デバイスのホスト名を選択します。これは CLI コマンドのプロンプトで使用されます。
  - [Use Default]：これらのスイッチのデフォルト ホスト名（System Name）は switch123456 であり、123456 はデバイスの MAC アドレスの最後の 3 バイトを 16 進形式で表しています。
  - [User Defined]：ホスト名を入力します。文字、数字、ハイフンだけが使用できます。ホスト名の開始または終了はハイフンにできません。（RFC1033、1034、1035 で指定されているように）他の記号、区切り文字、または空白スペースは使用できません。

カスタムバナー設定

以下のバナーを設定できます。

- [Login Banner]：ログイン前のログイン ページに表示するテキストを入力します。[Preview] をクリックして結果を表示します。
- [Welcome Banner]：ログイン後のログイン ページを表示するテキストを入力します。[Preview] をクリックして結果を表示します。

（注）
Web ベースの設定ユーティリティからログイン バナーを定義すると、CLI インターフェイス（コンソール、Telnet、SSH）のバナーも有効化されます。

バナーには最大で 1000 文字を含めることができます。510 文字より後は、<Enter> を押して続行してください。

ステップ 3 [Apply] をクリックして新しい設定を保存します。

コンソール設定

（注） コンソール設定は、[Advanced Mode] ビューでのみ使用できます。

コンソールポートの速度は、9600、19200、38400、57600、115200 または自動検出に設定できます。[Auto Detection] を選択すると、デバイスがコンソール速度を自動的に検出します。自動検出が有効ではない場合、コンソール ポートの速度は最後に手動で設定された速度（デフォルトは 115,200）に自動的に設定されます。自動検出が有効になっているがコンソールのボー レートが検出されていない場合、115,200 の速度が使用されてテキスト（ブートアップ情報など）

が表示されます。[Console Settings] ページで自動検出を有効にした後に、コンソールをデバイスに接続して Enter キーを 2 回押すと自動検出が有効化されます。デバイスは、ボー レートを自動的に検出します。

[Auto Detection] を有効にする、またはコンソールのボーレートを手動で設定するには、次のようにします。

手順

ステップ 1 [Administration] > [Console Settings] の順にクリックします。

ステップ 2 [Console Port Baud Rate]フィールドで、次のいずれかのオプションを選択します。

- [Auto Detection]：コンソール ボーレートが自動的に検出されます。
- [Static]：使用可能ないずれかの速度を選択します。

ステップ 3 [Apply] をクリックします。

スタック管理

（注） 特定のモデルのみがスタッキング機能を備えています。

スタックを管理するには、次の手順を実行します。

手順

ステップ 1 [Administration] > [Stack Management] をクリックします。

- [Stack Topology]：スタックのトポロジがチェーンまたはリングであるかどうかが表示されます。
- [Stack Active]：スタックのアクティブユニットのユニット ID が表示されます。

Stack Topology View

この表示は、デバイスのグラフィカルビューを提供します。この上にマウスカーソルを移動すると、ユニット番号、スタック内での機能、スタック内で接続されているデバイス、および経由しているスタッキングポートが表示されます。

Unit View and Stack Port Configuration

[Stack Topology View] で特定のデバイスをクリックすると、デバイスのグラフィカルビューが表示されます。

ステップ 2 デバイスのスタック ポートを選択するには、次の手順を実行します。

1. [Stack Topology View] でデバイスをクリックします。このデバイスのポートが、[Unit View and Stack Port Configuration] に表示されます。
2. ポートをマウスオーバーすると、ツールヒントにスタック構成ポート番号、接続しているユニット（1つの場合）、ポート速度、およぶ接続ステータスが表示されます。

ステップ 3 スタック内のデバイスのリセット後にユニット ID を設定するには、[Stack Topology View] でデバイスをクリックして、次のフィールドに入力します。

- [Unit ID After Reset]：ユニット ID を選択するか、システムによってユニット ID が指定されるように [Auto] を選択します。
- [Unit x Stack Connection Speed]：スタック接続の速度が表示されます。

ステップ 4 [Apply and Reboot] をクリックします。パラメータは実行コンフィギュレーション ファイルにコピーされ、スタックはリブートされます。

Bluetooth 設定

Bluetooth を使用すると、デバイスはワイヤレス接続し、短距離で相互に通信できます。これは、多くのアプリケーションで使用されている、便利で用途が広く、信頼性の高いテクノロジーです。

Bluetooth のサポートは、Bluetooth（BT）ドングルをデバイスの USB ポートに接続することによって実現されます。デバイスは、サポートされている BT ドングルがデバイスの USB ポートに挿入されたことを自動的に検出し、BT 操作を可能にする Bluetooth サポートを提供します。デバイス管理インターフェイスの Bluetooth インターフェイスにより、ユーザーは関連する Bluetooth 設定を適用できます。CLI およびテキスト構成ファイルでは、Bluetooth インターフェイスは「interface bluetooth 0」と表されます。BT ドングルが USB ポートに挿入されていなくても、BT インターフェイスを構成できます。

サポートされているドングルのリスト：

- BTD-400 Bluetooth 4.0 アダプタ（Kinivo 社製）
- Bluetooth 4.0 USB アダプタ（ASUS 社製）
- Bluetooth 4.0 USB アダプタ（Insignia 社製）
- Philips 4.0 Bluetooth アダプタ
- Lenovo LX1815 Bluetooth 5.0 USB アダプタ
- Lenovo LX1812 Bluetooth 4.0 USB アダプタ

スタックでは、BT ドングルの検出と操作はスタックアクティブユニットでのみサポートされます。デバイスは、USB ポートに挿入されている単一の USB デバイスの検出をサポートします。つまり、デバイスは、同じ USB インターフェイス上の複数の USB ドングルまたは USB ドングル + メモリスティックをサポートしません。

通知 syslog メッセージには、次のように、BT ドングルの検出と取り外しが成功したことが示されます。

- ドングルの挿入：「Bluetooth ドングルが USB ポートに挿入されました（Bluetooth Dongle inserted into USB port）」
- ドングルの取り外し：「Bluetooth ドングルが USB ポートから削除されました（Bluetooth Dongle removed from USB port）」

Bluetooth 設定を行うには、次の手順を実行します。

手順

ステップ 1 [Administration] > [Bluetooth Settings] をクリックします。

ステップ 2 次の設定を行います。

Bluetooth サービス	デバイスで Bluetooth サービスを有効にする場合は、[Enable] をオンにします。デフォルトは有効です。
PIN	次の中から選択します。 • [Encrypted]：暗号化された PIN を入力します • [Plaintext]：プレーンテキストの PIN（4 桁）を入力します デフォルトの PIN は 9999 です
Bluetooth デバイス名	デバイスが Bluetooth 経由で自身をアドバタイズするための文字列。次の中から選択します。 • [Switch Host Name]（デフォルト） • [User Defined]：ユーザー定義の名前を入力します（最大 20 文字）
BT インターフェイスの説明	Bluetooth インターフェイスの説明を入力します。（0 ～ 64 文字）

BT IP インターフェイス	Bluetooth インターフェイスを介してデバイスを管理するために使用される IP インターフェイス。次の中から選択します。 • [None]：Bluetooth インターフェイスで IP アドレスが構成されません。 • [User Defined]：Bluetooth インターフェイスで IP アドレスとマスクを構成します。 （注） [BT IP Address] フィールドと [BT IP Mask] フィールドは両方とも、BT IP インターフェイスの前の項目に関連付けられていて、ユーザーが [BT IP Interface] で [User Defined] を選択した場合にのみアクティブになります。
BT IP アドレス	Bluetooth インターフェイスの IP アドレスを入力します。
BT IP マスク	IP アドレスの IP マスク/プレフィックス長。このコントロールは、IPインターフェイスがユーザー定義の場合にのみ有効です。次の中から選択します。 • Network Mask • Prefix Length
ドングルあり	ドングルが存在する場合に表示されます。
状態	Bluetooth 接続の状態を表示します。利用可能な状態は次のとおりです。 • [Not Ready]（ドングルが挿入されていない） • [Discoverable]（ドングルが挿入されていて検出可能） • [Connected]（Bluetooth パートナーに接続済み） • [Disabled]（Bluetoothインターフェイスが無効になっている）
コネクテッドデバイス名	接続されている Bluetooth デバイスの表示名。このフィールドは、スイッチとリモート Bluetooth デバイス間で Bluetooth 接続が確立されている場合にのみ表示されます。

ステップ 3 [Apply] をクリックして設定を保存します。

ステップ 4 [Display Sensitive Data as Plaintext] をクリックすると機密データがプレーンテキスト形式で表示されます。

ユーザ アカウント

[User Accounts] ページでは、デバイスへのアクセス（読み取り専用または読み取り/書き込み）が許可されている追加ユーザの入力、および既存のユーザのパスワードの変更が可能です。デバイスに初めてアクセスするユーザーは、ユーザー名およびパスワードとして cisco と cisco を使用します。デフォルトのログイン情報を入力すると、デフォルトのレベル 15 のユーザー名およびパスワードを変更するよう求められます。このときに、新しいユーザー名とパスワードを設定する必要があります。新しいパスワードは、パスワードの複雑性ルールを満たす必要があります。

新規ユーザを追加する手順は、次のとおりです。

手順

ステップ 1 [Administration] > [User Accounts] の順にクリックします。

ステップ 2 [Password Recovery Service] で、[Enable] チェックボックスをオンにして、パスワードの復旧を有効にします。

ステップ 3 [Add] をクリックして新しいユーザーを追加するか、[Edit] をクリックしてユーザーおよび/またはパスワードを変更します。

ステップ 4 パラメータを入力します。

- [User Name]：1 ～ 20 文字の新しいユーザー名を入力します。UTF-8 文字は使用できません。
- [Current Password]：現在のパスワードを入力します。（このフィールドは編集モードでのみ表示されます。）
- [Suggest Password]：クリックするとパスワードを自動生成します。次に、[Copy to Clipboard] をクリックしてパスワードをコピーし、このアカウントのパスワードを使用する場合は [Yes] をクリックします。
- [Password]：パスワードを入力します（UTF-8 文字は使用できません）。

  （注）
  パスワードを作成する前に、ログイン設定のパスワードの複雑さのルールに関するセクションを参照してください。

  （注）
  ユーザーが入力したパスワードは、よくある一般的なパスワードのリストと比較されます。パスワードにこのリストの単語が含まれている場合、パスワードは拒否され、新しいパスワードを入力する必要があります。

- [Confirm Password]：パスワードを再度入力します。
- [Password Strength Meter]：パスワードの強度が表示されます。
- [User Level]：ユーザーの権限レベルを選択します。

- [Read-Only CLI Access (1)]：ユーザーは GUI にアクセスできません。デバイス構成を変更しない CLI コマンドだけにアクセスできます。
- [Read/Limited Write CLI Access (7)]：ユーザーは GUI にアクセスできません。デバイス構成を変更する一部の CLI コマンドだけにアクセスできます。詳細については、*CLI* のリファレンス ガイドを参照してください。
- [Read/Write Management Access (15)]：ユーザーは GUI にアクセスしてデバイスを設定できます。

ステップ 5 [Apply] をクリックします。ユーザは、デバイスの実行コンフィギュレーション ファイルに追加されます。

（注）
パスワードは、パスワードベースキー派生関数 2（PBKDF2）を使用して、回復不能なハッシュとしてコンフィギュレーション ファイルに保存されます。このとき、ハッシュアルゴリズムとしてセキュア ハッシュ アルゴリズムおよび SHA-512 が使用されます。

アイドルセッションタイムアウト

アイドル セッション タイムアウトは、管理セッションがタイムアウトする前にアイドル状態を維持できる時間間隔を設定します。

さまざまなタイプのセッションのアイドル セッション タイムアウトを設定するには、次の手順を実行します。

手順

ステップ 1 [Administration] > [Idle Session Timeout] の順にクリックします。

ステップ 2 リストから各セッションタイプのタイムアウトを選択します。

- HTTP セッション タイムアウト
- HTTPS セッション タイムアウト
- コンソール セッション タイムアウト
- Telnet セッション タイムアウト
- SSH セッション タイムアウト

デフォルトのタイムアウト値は 10 分です。選択したセッションのいずれかを再確立するには、もう一度ログインする必要があります。

ステップ 3 [Apply] をクリックして、構成時の設定をデバイスに設定します。

時刻設定

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

ネットワーク上のすべてのデバイスでの基準時間の枠組みが、システム クロックの同期により提供されます。ネットワークの管理、セキュリティ、計画、デバッグといったすべての局面でイベントの発生時刻の判定が行われるため、ネットワーク時間の同期は重要です。クロックを同期しない場合、セキュリティ侵害またはネットワーク使用量の追跡時にデバイス間でログファイルを正確に関連付けることが不可能になります。また、ファイル システムがどこに格納されているかにかかわらず、共有されたファイル システムでの競合を削減するには変更時間を一定にすることが重要であるため、時刻の同期により競合も削減することができます。これらの理由から、ネットワーク上のすべてのデバイスで、設定された時間が正確であることが重要です。

リアルタイム クロック

一部のデバイスには、デバイスがシャットダウンされて電源に接続されていない場合でも正確な時刻を維持する、自己完結型リアルタイムクロック（RTC）コンポーネントが内蔵されています。この内部クロックは製造中に初期化され、ソフトウェアクロックの設定時に、デバイスの時刻機能によって更新されます。RTC コンポーネントを搭載したデバイスが起動すると、システムクロックは RTC の時刻と日付に設定されます。システムクロックが Simple Network Time Protocol（SNTP）により動的に、または手動で変更されるたびに、RTC コンポーネントは更新されます。

（注） このデバイスは SNTP に対応しています。このプロトコルを有効にすると、デバイスは、SNTP サーバーから取得した時刻でデバイス時刻を動的に同期します。デバイスは SNTP クライアントとしてのみ動作し、他のデバイスに時間に関するサービスを提供することはできません。

システム時刻

システム時刻ページを使用して、システム時刻のソースを選択します。ソースが手動の場合には、ここで時刻を入力できます。

注意 システム時刻を手動で設定し、デバイスをリブートした場合、時刻設定を手動で再入力する必要があります。

システム時刻を定義するには、次の手順を実行します。

手順

ステップ 1 [Administration] > [Time Settings] > [System Time] をクリックします。

次のフィールドが表示されます。

- [Actual Time (From SNTP Server)]：デバイスの実際のシステム時刻。
- [Last Synchronized Server]：最後にシステム時刻が取得されたアドレス、ストラタム、およびSNTPサーバの種類。

ステップ 2 次のパラメータを入力します。

- [Clock Source Settings]：システム クロックの設定に使用するソースを選択します。
  - [Main Clock Source (SNTP Servers)]：これが有効な場合、システム時刻が SNTP サーバから取得されます。この機能を使用するには、SNTPマルチキャスト/エニーキャスト （14 ページ）で SNTP サーバーへの接続も設定する必要があります。
  - [Alternate Clock Source (PC via active HTTP/HTTPS sessions)]：HTTP プロトコルを使用した設定コンピュータからの日付と時刻の設定を有効にする場合に、[Enable] にチェックを入れます。

    （注）
    RIP MD5 認証を機能させるには、[Clock Source Setting] を上記のいずれかに設定する必要があります。

- [Manual Settings]：日付と時刻を手動で設定します。SNTP サーバーなどの代替時刻ソースがない場合は、現地時間が使用されます。
  - [Date]：システムの日付を入力します。
  - [Local Time]：システムの時刻を入力します。
- [Time Zone Settings]：DHCP サーバまたはタイムゾーン オフセットによるローカル時刻が使用されます。
  - [Get Time Zone from DHCP]：DHCP サーバからのタイムゾーンと DST の動的設定を有効にする場合に選択します。これらのパラメータの一方が設定されるのか両方が設定されるのかは、DHCP パケットに含まれる情報により変わります。このオプションが有効な場合、DHCP クライアントをデバイスで有効にする必要があります。
  - [Time Zone from DHCP]：DHCP サーバから設定されたタイムゾーンの略語が表示されます。この略語は [Actual Time] フィールドに表示されます。
  - [Time Zone Offset]：Greenwich Mean Time （GMT; グリニッジ標準時）と現 地時間との差を選択します。たとえば、パリのタイムゾーン オフセットは GMT +1、ニューヨークのタイムゾーン オフセットは GMT - 5 です。

- [Time Zone Acronym]：このタイムゾーンを表す名前を入力します。この略語は [Actual Time] フィールドに表示されます。

- [Daylight Savings Settings]：DST の定義方法を選択します。
  - [Daylight Savings]：サマータイムを有効にする場合に選択します。
  - [Time Set Offset]：GMT からのオフセットの分数を 1 ～ 1440 の範囲で入力します。デフォルトは 60 です。
  - [Daylight Savings Type]：次のいずれかをクリックします。

    [USA]：米国で使用されている日付に基づいて DST が設定されます。

    [European]：欧州連合およびこの規格を採用しているその他の国で使用されている日付に基づいて DST が設定されます。

    [By dates]：DST は手動で設定されます。通常は、米国とヨーロッパ諸国以外の国用です。以下のパラメータを入力します。

    [Recurring]：DST を毎年同じ日付に発生させます。

    [By Dates] を選択すると、DST の開始と終了をカスタマイズできるようになります。

- [From]：DST が開始する日付と時刻。
- [To]：DST が終了する日付と時刻。

ステップ 3 [Recurring] を選択すると、DST の開始と終了を個別にカスタマイズできるようになります。

- [From]：毎年 DST が開始する日付。
  - [Day]：毎年 DST が開始する曜日。
  - [Week]：毎年 DST が開始する月の週。
  - [Month]：毎年 DST が開始する月。
  - [Time]：毎年 DST が開始する時刻。

- [To]：毎年 DST が終了する日付。たとえば、当地の DST を毎年 10 月の第 4 週目の金曜日 AM 5:00 に終了するとします。パラメータは次のとおりです。
  - [Day]：毎年 DST が終了する曜日。
  - [Week]：毎年 DST が終了する月の週。
  - [Month]：毎年 DST が終了する月。
  - [Time]：毎年 DST が終了する時刻。

ステップ 4 [Apply] をクリックします。システム時刻値が実行コンフィギュレーション ファイルに書き込まれます。

SNTPユニキャスト

SNTPは、サテライト受信機やモデムなどの送信元によってすでに同期されているサーバーと、コンピュータのシステム時刻を同期します。SNTP では、ユニキャスト、マルチキャスト、およびエニーキャスト オペレーティング モードがサポートされます。ユニキャストモードでは、クライアントはユニキャストアドレスを参照することで、専用サーバーに要求を送信します。最大 16 台のユニキャスト SNTP サーバを設定できます。

（注） SNTP クライアントユニキャストを機能させるには、システム時刻 （9 ページ）に記載されているメインクロックソース（SNTP サーバー）を有効にする必要があります。

ユニキャスト SNTP サーバーを追加するには、次の手順を実行します。

手順

ステップ 1 [Administration] > [Time Settings] > [SNTP Unicast] をクリックします。

ステップ 2 次のフィールドを設定します。

SNTPクライアントユニキャスト	[Enable] を選択すると、SNTP で事前定義されたユニキャストクライアントをユニキャスト SNTP サーバーとともにデバイスで使用できます。
IPv4送信元インターフェイス	ドロップダウンリストから SNTP サーバーとの通信に使用する IPv4 インターフェイスを選択します。
IPv6送信元インターフェイス	ドロップダウンリストから SNTP サーバーとの通信に使用する IPv6 インターフェイスを選択します。 （注） 自動（Auto）オプションを選択すると、システムは発信インターフェイスで定義されている IP アドレスから送信元 IP アドレスを取得します。

このページでは、ユニキャスト SNTP サーバごとに次の情報が表示されます。

- [SNTP Server]：SNTP サーバーの IP アドレス。ストラタム レベルに応じて、優先サーバまたはホスト名が選択されます。
- [Poll Interval]：ポーリングが有効か無効かを示します。
- [Authentication Key ID]：SNTP サーバとデバイス間の通信に使用するキー ID。
- [Stratum Level]：参照クロックからの距離を数値で示します。ポーリング間隔が有効になっていない限り、SNTP サーバーをプライマリサーバー（ストラタムレベル 1）にすることはできません。
- [Status]：SNTP サーバーのステータス。設定可能な値は次のとおりです。
  - [Up]：SNTP サーバーは現在正常に動作しています

- [Down]：SNTP サーバーは現在使用できません。
- [Unknown]：SNTP サーバのステータスは不明です。
- [In Process]：SNTP サーバーへの接続は現在処理中です。

- [Last Response]：SNTP サーバから最後に応答を受信した日時。
- [Offset]：ローカル クロックに対するサーバ クロックの概算オフセット（ミリ秒単位）。ホストは、RFC 2030 に記述されているアルゴリズムを使用してこのオフセットの値を決定します。
- [Delay]：サーバ クロックとローカル クロック間のネットワーク パス全体での、ローカル クロックに対するサーバ クロックの概算ラウンドトリップ遅延（ミリ秒単位）。ホストは、RFC 2030 に記述されているアルゴリズムを使用してこの遅延の値を決定します。
- [Source]：SNTP サーバの定義方法。たとえば、手動や DHCPv6 サーバからなど。
- [Interface]：パケットを受信するインターフェイス。

ステップ 3 ユニキャスト SNTP サーバーを追加するには、[Add] をクリックします。

（注）
ユーザ定義の SNTP サーバをすべて削除するには、[Restore Default Servers] をクリックします。

ステップ 4 次のパラメータを入力します。

サーバー指定方法	SNTP サーバーを選択します。IP アドレスまたはリスト内の名前で指定します。
IP バージョン	IP アドレスのバージョン（バージョン 6 またはバージョン 4）を選択します。
IPv6 アドレス タイプ	IPv6 アドレスタイプを選択します（IPv6 が使用されている場合）。次のオプションがあります。 • [Link Local]：IPv6 アドレスによって、同一ネットワーク リンク上のホストが一意に識別されます。リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。 • [Global]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
Link Local Interface	リストからリンク ローカル インターフェイスを選択します（IPv6 アドレスタイプとしてリンクローカルが選択されている場合）。
SNTPサーバーのIPアドレス/名前	SNTP サーバーの IP アドレスまたは名前を入力します。形式は、選択したアドレス タイプにより異なります。

ポーリング間隔	選択すると、システムの時刻情報を取得するためにSNTPサーバーのポーリングが有効になります。ポーリング対象のすべてのNTPサーバーがポーリングされ、クロックは、ストラタムレベルが一番低い、アクセス可能なサーバーから選択されます。最も低いストラタムのサーバはプライマリ サーバと見なされます。次に低いストラタムのサーバはセカンダリ サーバとなり、以下同様です。プライマリ サーバがダウンした場合、デバイスはポーリング設定が有効なすべてのサーバをポーリングし、最も低いストラタムの新しいプライマリ サーバを選択します。
認証	認証を有効にする場合、このチェックボックスをオンにします。
認証キーID	認証が有効な場合、キー IDの値を選択します。

ステップ5 [Apply] をクリックします。SNTP サーバを追加すると、メインページに戻ります。

SNTPマルチキャスト/エニーキャスト

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

（注） SNTPクライアントマルチキャスト/エニーキャストを機能させるには、メインクロックソース（SNTP サーバー）システム時刻 （9 ページ） を有効にする必要があります。

サブネット上のすべてのサーバーから SNTP パケットを受信したり、SNTP サーバーへの時刻要求を送信したりできるようにするには、次の手順を実行します。

手順

ステップ1 [Administration] > [Time Settings] > [SNTP Multicast/Anycast] をクリックします。

次のオプションから有効にするものを選択します。

オプション	説明
SNTP IPv4マルチキャストクライアントモード(クライアントブロードキャスト受信)	サブネット上の任意のSNTPサーバーから、システム時刻のIPv4マルチキャスト伝送を受信する場合に、[Enable] をオンにします。
SNTP IPv6マルチキャストクライアントモード(クライアントブロードキャスト受信)	サブネット上の任意のSNTPサーバーから、システム時刻のIPv6マルチキャスト伝送を受信する場合に、[Enable] をオンにします。

オプション	説明
SNTP IPv4エニーキャストクライアントモード(クライアントブロードキャスト送信)	システム時刻情報を要求する SNTP IPv4 同期パケットを送信する場合に、[Enable] をオンにします。パケットは、サブネット上のすべての SNTP サーバに送信されます。
SNTP IPv6エニーキャストクライアントモード(クライアントブロードキャスト送信)	システム時刻情報を要求する SNTP IPv6 同期パケットを送信する場合に、[Enable] をオンにします。パケットは、サブネット上のすべての SNTP サーバに送信されます。

ステップ 2 [Add] をクリックして、SNTP のインターフェイスを選択します。

インターフェイス（ポート、LAG、または VLAN）を選択し、ドロップダウンメニューからオプションを選択して構成します。

ステップ 3 [Apply] をクリックし、実行コンフィギュレーション ファイルに設定を保存します。

SNTP認証

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

SNTP クライアントは、HMAC-MD5 を使用して応答を認証できます。SNTP サーバーはキーに関連付けられています。このキーは応答自体とともにMD5関数への入力として使用されます。MD5 の結果も応答パケットに組み込まれます。[SNTP Authentication] ページでは、SNTP サーバーとの通信に使用する認証キーを設定できます。

認証キーは、SNTP サーバーのタイプに応じて、独立したプロセスで SNTP サーバーに作成されます。詳細については、SNTP サーバのシステム管理者にお尋ねください。

手順

ステップ 1 [Administration] > [Time Settings] > [SNTP Authentication] をクリックします。

ステップ 2 [Enable] をオンにすると、デバイスと SNTP サーバー間の SNTP セッションの SNTP 認証が有効になります。

ステップ 3 [Apply] をクリックして、デバイスを更新します。

ステップ 4 [Add] をクリックします。

ステップ 5 次のパラメータを入力します。

- [Authentication Key ID]：この SNTP 認証キーを内部的に識別するための番号を入力します。
- [Authentication Key]：次のオプションから選択します。

- [User Defined (Encrypted)]：認証に使用するキーを暗号化形式で入力します。SNTP サーバは、デバイスを自身と同期させるためにこのキーを送信する必要があります。
- [User Defined (Plaintext)]：認証に使用するキーをプレーンテキスト形式で入力します（最大 8 文字）。SNTP サーバは、デバイスを自身と同期させるためにこのキーを送信する必要があります。

- [Trusted Key]：デバイスが、この認証キーを使って、SNTP サーバーからのみ同期情報を受信できるようにする場合にオンにします。

ステップ 6 [Apply] をクリックします。SNTP 認証パラメータが、実行コンフィギュレーション ファイルに書き込まれます。

ステップ 7 SNTP 認証キーを削除するには、目的の認証キー ID のチェックボックスをオンにして、[Delete] アイコンをクリックします。

ステップ 8 ページでプレーン テキスト形式でセンシティブ データを表示するには、[Display Sensitive Data As Plaintext] をクリックします。

Time Range

時間範囲を定義し、以下の種類のコマンドと関連付けて、それらのコマンドが定義した時間範囲でのみ適用されるようにできます。

- ポート状態
- 時間ベースの PoE

時間範囲には 2 つの種類があります。

- [Absolute]：このタイプの時間範囲は、特定の日付または即時に開始し、特定の日付で終了するか、無制限に実行されます。これは時間範囲ページで作成されます。定期的な要素をここに追加することができます。
- [Periodic]：このタイプの時間範囲には、絶対範囲に追加される時間範囲要素が含まれており、定期的に開始および終了します。これは、[Periodic Range] ページで定義されます。

時間範囲に絶対範囲と周期範囲の両方が含まれる場合、それに関連したプロセスは、絶対開始時間と周期時間範囲の両方に達した場合にのみアクティブ化されます。このプロセスは、いずれかの時間範囲に達した時点で非アクティブ化されます。デバイスは最大 20 個の絶対時間範囲をサポートします。

時間範囲エントリが目的の時刻に有効になるようにするには、システム時刻を設定する必要があります。時間範囲機能は次の目的で使用できます。

- ネットワークへのコンピュータのアクセスを（たとえば）業務時間内のみに制限し、業務時間後はネットワークポートをロックし、残りのネットワークのアクセスをブロックします（「ポートの設定」および「LAG 情報の設定」を参照してください）。
- 指定した期間に PoE 操作を制限します。

時間範囲の説明を追加

手順

ステップ 1 [Administration] > [Time Settings] > [Time Range] の順にクリックします。

ステップ 2 [Time Range] テーブルで、[Add] をクリックして新しい時間範囲を追加するか、[Edit] または [Delete] をクリックして既存の時間範囲を編集または削除します。

ステップ 3 新しい時間範囲を追加するには、[Add] をクリックし、次のように設定します。

- [Time Range Name]：時間範囲の名前を入力します。
- [Absolute Starting Time]：[Immediate] を選択するか、日付と時刻を入力します。
- [Absolute Ending Time]：[Infinite] を選択するか、日付と時刻を入力します。

ステップ 4 新しい時間範囲設定を適用するには、[Apply] をクリックします。

繰り返し時間範囲

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

定期的な時間要素を絶対時間範囲に追加できます。これにより、絶対範囲内の特定の期間に動作が制限されます。

絶対時間範囲に定期時間範囲要素を追加するには、次の手順を実行します。

手順

ステップ 1 [Administration] > [Time Settings] > [Recurring Range] をクリックします。

既存の定期時間範囲が表示されます（特定の絶対時間範囲ごとにフィルタ処理されます）。

ステップ 2 定期範囲を追加する絶対時間範囲を選択します。

ステップ 3 新しい定期時間範囲を追加するには、[Add] をクリックします。

ステップ 4 次のフィールドに入力します。

- [Recurring Starting Time]：時間範囲の開始点とする曜日と時刻を入力します。
- [Recurring Ending Time]：時間範囲の終了点とする曜日と時刻を入力します。

ステップ 5 [Apply] をクリックします。

システム ログ

ここでは、システム ロギングについて説明します。システム ロギングは、デバイスが複数の独立したログを生成することを可能にします。各ログは、システムイベントが示された一連のメッセージで構成されます。

デバイスでは、次のローカル ログが生成されます。

- コンソール インターフェイスに送信されるログ
- イベントが記録された RAM 内の循環リストに書き込まれるログ。デバイスのリブート時に消去されます。
- フラッシュ メモリに保存される循環ログ ファイルに書き込まれるログ。リブート後も保持されます。

さらに、SNMP トラップ形式および SYSLOG メッセージ形式で、リモートの SYSLOG サーバにメッセージを送信できます。

ログ設定

シビラティ（重大度）レベル別に、ログに記録するイベントを選択できます。各ログメッセージにはシビラティ（重大度）レベルが設定され、シビラティ（重大度）レベルの最初の文字の両側にダッシュ（-）が付けられてマーキングされています（例外として緊急（Emergency）は文字 F で表されます）。たとえば、ログ メッセージ「%INIT-I-InitCompleted: …」のシビラティ（重大度）レベルは I であり、情報（Informational）を意味します。

イベントのシビラティ（重大度）レベルを、最も高いシビラティ（重大度）から最も低いシビラティ（重大度）まで、以下に順に示します。

- 緊急（Emergency）：システムを使用できません。
- アラート（Alert）：処置が必要です。
- 重大（Critical）：システムに重大な問題があります。
- エラー（Error）：システムにエラーがあります。
- 警告（Warning）：システム警告が発生しました。
- 注意（Notice）：システムは正しく機能していますが、システムの注意事項が発生しました。
- 情報（Informational）：デバイス情報です。
- デバッグ（Debug）：イベントに関する詳細応報です。

RAMおよびフラッシュのログに対して、異なるシビラティ（重大度）レベルを選択できます。これらのログはそれぞれRAMメモリとフラッシュ メモリに表示されます。

ログに保存されるシビラティ（重大度）レベルを選択すると、それより高いシビラティ（重大度）のすべてのイベントが自動的にそのログに保存されます。それより低いシビラティ（重大度）のイベントは、ログに保存されません。たとえば、[Warning] を選択すると、[Warning] およびそれより高いすべてのシビラティ（重大度）レベル（緊急、アラート、重大、エラー、および警告）がログに保存されます。[Warning] より低いシビラティ（重大度）レベル（注意、情報）は保存されません。

グローバルログパラメータを設定するには、次の手順を実行します。

手順

ステップ 1 [Administration] > [System Log] > [Log Settings] の順にクリックします。

ステップ 2 パラメータを入力します。

Logging	これを選択するとメッセージロギングが有効になります。
Syslog Aggregator	これを選択すると SYSLOG メッセージとトラップの集約が有効になります。有効な場合、同一および連続した SYSLOG メッセージとトラップが、指定された最大集約時間にわたって集約され、単一のメッセージで送信されます。集約されたメッセージは、その到着順で送信されます。各メッセージには、集約された回数が示されています。
Max. Aggregation Time	SYSLOG メッセージが集約される間隔を入力します。
Originator Identifier	この設定により、SYSLOG メッセージに発信元 ID を追加できます。次のオプションがあります。 • [None]：SYSLOG メッセージに発生元識別子を含めません。 • [HostName]：SYSLOG メッセージにシステム ホスト名を含めます。 • [IPv4 Address]：送信元インターフェイスの IPv4 アドレスを SYSLOG メッセージに含めます。 • [IPv6 Address]：送信元インターフェイスの IPv6 アドレスを SYSLOG メッセージに含めます。 • [User Defined]：SYSLOG メッセージに含まれる説明を入力します。
RAM Memory Logging	RAM に記録するメッセージのシビラティ（重大度）を選択します。
Flash Memory Logging	フラッシュメモリに記録するメッセージのシビラティ（重大度）を選択します。

ステップ 3 [Apply] をクリックします。実行コンフィギュレーション ファイルが更新されます。

リモートログサーバー

[Remote Log Servers] ページでは、ログ メッセージの送信先となるリモート SYSLOG サーバを定義できます。各サーバに対して、受信メッセージのシビラティ（重大度）を設定できます。

SYSLOG サーバーを定義するには、次の手順を実行します。

手順

ステップ 1 [Administration] > [System Log] > [Remote Log Servers] をクリックします。

ステップ 2 （注）
この設定は、[Advanced Mode] ビューでのみ使用できます。

次のフィールドに入力します。

- IPv4 送信元インターフェイス（IPv4 Source Interface）：送信元インターフェイスを選択します。このインターフェイスの IpV4 アドレスが、SYSLOG サーバに送信される SYSLOG メッセージの送信元 IPv4 アドレスとして使用されます。
- IPv6 送信元インターフェイス（IPv6 Source Interface）：送信元インターフェイスを選択します。このインターフェイスの IpV4 アドレスが、SYSLOG サーバに送信される SYSLOG メッセージの送信元 IPv6 アドレスとして使用されます。

（注）
自動（Auto）オプションを選択すると、システムは発信インターフェイスで定義されている IP アドレスから送信元 IP アドレスを取得します。

以前に設定したログサーバーごとに情報が記載されています。フィールドについては、後述の [Add] ページで説明します。

ステップ 3 [Add] をクリックします。

ステップ 4 パラメータを入力します。

Server Definition	リモートログサーバーを IP アドレスで識別するか、名前で指定するかを選択します。
IP Version	サポートする IP 形式を選択します。

IPv6 Address Type	IPv6 アドレスタイプを選択します（IPv6 が使用されている場合）。次のオプションがあります。 • [Link Local]：IPv6 アドレスによって、同一ネットワーク リンク上のホストが一意に識別されます。リンクローカルアドレスのプレフィックス部は FE80::/10 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。 • [Global]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
Link Local Interface	リストからリンク ローカル インターフェイスを選択します（IPv6 アドレスタイプとしてリンクローカルが選択されている場合）。
Log Server IP Address/Name	ログサーバーの IP アドレスまたはドメイン名を入力します。
UDP ポート	ログメッセージの送信先となる UDP ポートを入力します。
ファシリティ	リモートサーバーに送信されるシステムログの出力元のファシリティ値を選択します。サーバに割り当てることができるファシリティ値は 1 つだけです。2 番目のファシリティ コードが割り当てられている場合は、最初のファシリティ値がオーバーライドされます。
説明	サーバーの説明を入力します。
シビラティ（重大度）の最小値	サーバーに送信されるシステムログメッセージの最小シビラティ（重大度）を選択します。

ステップ 5 [Apply] をクリックします。[Add Remote Log Server] ページが閉じて、SYSLOG サーバが追加され、実行コンフィギュレーション ファイルが更新されます。

ファイル管理

ファイル管理システムは、デバイス上のファイルを保存、整理、およびアクセスするために使用されるアプリケーションです。システムファイルとは、コンフィギュレーション情報やファームウェアイメージなどの情報を格納したファイルです。一般に、flash://system/ フォルダの下にあるすべてのファイルがシステム ファイルです。これらのファイルを使用してさまざまな処理を実行できます。たとえば、デバイスのブート元となるファームウェアファイルの選択、デバイス内部でのさまざまなタイプのコンフィギュレーションファイルの変更、外部デバイス（外部サーバーなど）との間のファイルのコピーなどです。

次に、デバイスに存在するファイルのタイプの一部を示します。

- 実行コンフィギュレーション：デバイスが動作するために現在使用されているパラメータが含まれています。このファイルは、デバイス上のパラメータ値を変更したときに変更されます。デバイスをリブートすると、実行コンフィギュレーションは失われます。デバイスに加えた変更内容を保持するには、スタートアップ コンフィギュレーション、または別のファイル タイプに実行コンフィギュレーションを保存する必要があります。
- スタートアップ コンフィギュレーション：別の設定（通常は実行コンフィギュレーション）をスタートアップ コンフィギュレーションにコピーすることで保存されるパラメータ値です。スタートアップ コンフィギュレーションはフラッシュに保持され、デバイスがリブートした場合でも保持されます。現時点では、スタートアップ コンフィギュレーションは RAM にコピーされ、実行コンフィギュレーションとして識別されます。
- ミラー コンフィギュレーション：次の条件が存在する場合、デバイスによって作成されるスタートアップ コンフィギュレーションのコピーです。
  - デバイスが継続的に 24 時間にわたって動作している。
  - 過去 24 時間に実行コンフィギュレーションに設定変更が加えられていない。
  - スタートアップ コンフィギュレーションが実行コンフィギュレーションと同一である。

  ミラー コンフィギュレーションにスタートアップ コンフィギュレーションをコピーできるのはシステムだけです。ただし、ユーザはミラー コンフィギュレーションから他のファイル タイプまたは別のデバイスにコピーできます。
- バックアップ ファイル：システム シャットダウンに対する保護のため、または特定の動作状態の保持のために使用されるファイルの手動コピーです。たとえば、ミラー コンフィギュレーション、スタートアップ コンフィギュレーション、または実行コンフィギュレーションをバックアップ ファイルにコピーすることができます。バックアップはフラッシュ、PC または USB ドライブに存在し、デバイスがリブートした場合でも保持されます。
- ファームウェア：デバイスの動作と機能を制御するプログラムです。一般に、イメージと呼ばれています。
- 言語ファイル：選択した言語で Web ベースの設定ユーティリティ ウィンドウを表示できるようにするディクショナリです。
- ログ ファイル：フラッシュ メモリに保存される SYSLOG メッセージです。

ファームウェア操作

[Firmware Operations] ページは、次のために使用できます。

- ファームウェア イメージの更新またはバックアップ
- アクティブイメージのスワップ

スタックの適切な動作を保証するために、スタック内のユニットのソフトウェアイメージは同一である必要があります。スタックのユニットは、次のいずれかの方法でアップグレードできます。

手順

ステップ 1 [Administration] > [File Management] > [Firmware Operations] をクリックします。

次のフィールドが表示されます。

- アクティブなファームウェア ファイル（Active Firmware File）：最新のアクティブなファームウェア ファイルが表示されます。
- アクティブなファームウェア バージョン（Active Firmware Version）：最新のアクティブなファームウェア ファイルのバージョンが表示されます。

ステップ 2 次のオプションから、[Operation Type] を選択します。

- ファームウェアの更新
- ファームウェアのバックアップ
- イメージの切り替え

ステップ 3 次のオプションから、[Copy Method] を選択します。

HTTP/HTTPS	HTTP/HTTPS の場合は、[File Name] フィールドにファイル名を入力するか、[browse] をクリックしてファイルを探して選択します。
USB	USB の場合は、[File Name] フィールドにファイル名を入力するか、[browse] をクリックしてファイルを探して選択します。
TFTP	TFTP については、以下の TFTP の手順に従ってください。
SCP (SSH経由のファイル転送)	SCP については、以下の SCP の手順に従ってください。

TFTP の手順

（注）
この設定は、[Advanced Mode] ビューでのみ使用できます。

ファームウェア操作のコピー方式として TFTP を選択した場合は、次のように設定します。

Server Definition	次のオプションから選択します。 • IPアドレス別 • 名前別

IP Version	次のオプションから選択します。 • IP Version 6 • IP Version 4
IPv6 Address Type	次のオプションから選択します。 • [Link Local]：リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。 • [Global]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
Link Local Interface	IPv6 アドレスタイプで [Link Local] を選択した場合は、ドロップダウンリストからインターフェイスを選択します。
サーバーのIPアドレス/名前	サーバーの IP アドレス/名前を入力します。
送信元（ファームウェアの更新時に表示されます）	送信元の名前を入力します（0 ～ 62 文字を使用）
接続先（ファームウェアのバックアップ時に表示されます）	宛先を入力します（0 ～ 62 文字を使用）

SCP の手順

（注）
この設定は、[Advanced Mode] ビューでのみ使用できます。

ファームウェア操作のコピー方式として SCP を選択した場合は、次のように設定します。

リモートSSHサーバー認証	SSH サーバー認証（デフォルトでは無効）を有効にするには、[Edit] をクリックします。
SSHクライアント認証	次の中から選択します。 • [Use SSH Client System Credentials] を使用します。 • [SSH Client One-Time Credentials] を使用します。
Username	[SSH Client One-Time Credentials] オプションを使用する場合、ユーザー名を入力します。
Password	[SSH Client One-Time Credentials] オプションを使用する場合、パスワードを入力します。

Server Definition	次のオプションから選択します。 • IPアドレス別 • 名前別
IP Version	次のオプションから選択します。 • バージョン 6 • バージョン 4
IPv6 Address Type	次のオプションから選択します。 • [Link Local]：リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。 • [Global]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
Link Local Interface	IPv6 アドレスタイプで [Link Local] を選択した場合は、ドロップダウンリストからインターフェイスを選択します。
サーバーのIPアドレス/名前	サーバーの IP アドレス/名前を入力します。
送信元（ファームウェアの更新時に表示されます）	送信元の名前を入力します（0 ～ 62 文字を使用）
接続先（ファームウェアのバックアップ時に表示されます）	宛先を入力します（0 ～ 62 文字を使用）

ステップ 4 [Apply] をクリックして設定値を保存します。

ファイル操作

手順

ステップ 1 [Administration] > [File Management] > [File Operations] をクリックします。

ステップ 2 次のオプションから、[Operation Type] を選択します。

- 更新ファイル

- バックアップファイル
- 重複

ステップ 3 次のオプションから、[Destination] または [Source File Type] を選択します。

- 実行コンフィギュレーション
- スタートアップ コンフィギュレーション
- ミラーコンフィギュレーション
- ロギングファイル
- 言語ファイル
- ダッシュボード情報ファイル

ステップ 4 次のオプションから、[Copy Method] を選択します。

HTTP/HTTPS	HTTP/HTTPS の場合は、[File Name] フィールドにファイル名を入力するか、[browse] をクリックしてファイルを探して選択します。
USB	USB の場合は、[File Name] フィールドにファイル名を入力するか、[browse] をクリックしてファイルを探して選択します。
内部フラッシュ	内部ファイルの場合は、[File Name] フィールドにファイル名を入力するか、[File Directory] をクリックして参照します。[Sensitive Data Handling]：データの処理方法を選択します。ファイルのバックアップにのみ適用されます。 • [Exclude]：機密データを除外します • [Encrypt]：機密データを暗号化します • [Plaintext]：プレーンテキストで機密データを表示します。
TFTP	TFTP については、以下の TFTP の手順に従ってください。
SCP (SSH経由のファイル転送)	SCP については、以下の SCP の手順に従ってください。

TFTP の手順

ファイル操作の更新方式またはバックアップ方式としてTFTPを選択した場合は、次のように設定します。

サーバー指定方法	次のオプションから選択します。 • IPアドレス別 • 名前別

IP バージョン	次のオプションから選択します。 • IP Version 6 • IP Version 4
IPv6 アドレス タイプ	次のオプションから選択します。 • [Link Local]：リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。 • [Global]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
Link Local Interface	IPv6 アドレスタイプで [Link Local] を選択した場合は、ドロップダウンリストからインターフェイスを選択します。
サーバーのIPアドレス/名前	サーバーの IP アドレス/名前を入力します。
送信元	送信元の名前を入力します（0 ～ 62 文字を使用）
機密データの処理	（注） このオプションは、SCP またはTFTP のバックアップファイルモードの場合にのみ表示されます。 バックアップファイルに機密データを含める方法を、次のいずれかのオプションから選択します。 • 除外（Exclude）：機密データはバックアップに含めません。 • 暗号化（Encrypt）：暗号化された形式で機密データをバックアップに含めます。 • プレーン テキスト（Plaintext）：プレーン テキスト形式で機密データをバックアップに含めます。

SCP の手順

ファイル操作のコピー方式として SCP を選択した場合は、次のように設定します。

リモートSSHサーバー認証	SSH サーバー認証（デフォルトでは無効）を有効にするには、[Edit] をクリックします。
SSHクライアント認証	次の中から選択します。 • [Use SSH Client System Credentials] を使用します。 • [SSH Client One-Time Credentials] を使用します。

ユーザー名	[SSH Client One-Time Credentials] オプションを使用する場合、ユーザー名を入力します。
パスワード	[SSH Client One-Time Credentials] オプションを使用する場合、パスワードを入力します。
サーバー指定方法	次のオプションから選択します。 • IPアドレス別 • 名前別
IP バージョン	次のオプションから選択します。 • IP Version 6 • IP Version 4
IPv6 アドレス タイプ	次のオプションから選択します。 • [Link Local]：リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。 • [Global]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
Link Local Interface	IPv6 アドレスタイプで [Link Local] を選択した場合は、ドロップダウンリストからインターフェイスを選択します。
サーバーのIPアドレス/名前	サーバーの IP アドレス/名前を入力します。
送信元	送信元の名前を入力します（0 ～ 62 文字を使用）

ステップ 5 コピー方法として [HTTP/HTTPS] を選択した場合は、[File name] セクションで [Browse] ボタンをクリックし、ファイルを探して選択します。

ステップ 6 [Apply] をクリックして設定を保存します。

設定のバックアップ

設定ファイルのバックアップは、製品に障害が発生した場合のダウンタイムを最小限に抑えるために不可欠です。さらに、実稼働またはテスト機器で新しい設定をテストする前に、正常に動作することがわかっている設定ファイルをバックアップすることをお勧めします。設定の変更が期待どおりに機能していることを確認したら、必ず変更を適用し、新しいバックアップ設定ファイルを作成します。

スイッチの設定をバックアップおよび復元するために、デバイスの Web ベースのグラフィカル ユーザー インターフェイス（GUI）を使用できます。スイッチの設定をバックアップおよび復元する手順は次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	スイッチの Web ベースの GUI にログインします。	
ステップ 2	[Administration] > [File Management] > [File Operations] に移動します。	
ステップ 3	[Operation Type] で [Backup File] を選択します。	
ステップ 4	次に、[Source File Type] で [Running Configuration] を選択します。	
ステップ 5	[Copy Method] については、次のいずれかのオプションを選択します。	• HTTP/HTTPS • USB • 内部フラッシュ
ステップ 6	次に、以下から [Sensitive Data Handling] オプションを選択します。	• Exclude • Encrypt • Plaintext
ステップ 7	[Apply] をクリックします。	

設定の復元

手順

	コマンドまたはアクション	目的
ステップ 1	スイッチの Web ベースの GUI にログインします。	
ステップ 2	[Administration] > [File Management] > [File Operations] に移動します。	
ステップ 3	[Operation Type] で [Update File] を選択します。	
ステップ 4	次に、次のオプションから、[Destination File Type] を選択します。	• 実行コンフィギュレーション • スタートアップ コンフィギュレーション
ステップ 5	[Copy Method] については、次のいずれかのオプションを選択します。	• HTTP/HTTPS • USB

	コマンドまたはアクション	目的
		• 内部フラッシュ
ステップ 6	次に、[File Name] セクションで [Browse] ボタンをクリックし、設定ファイルを探して選択します。	設定が実行コンフィギュレーションに直接適用された場合、スイッチは設定の変更をすぐに適用します。 設定がスタートアップ コンフィギュレーションに適用されている場合は、スイッチをリブートして設定の変更を反映させる必要があります。 設定ファイルを復元すると、スイッチの現在の設定が上書きされることに注意してください。設定ファイルを復元する前に、現在の設定をバックアップして、バックアップ後に行われた変更が失われないようにしてください。

ファイルディレクトリ

[File Directory] ページには、システムに存在するシステム ファイルが表示されます。

手順

ステップ 1 [Administration] > [File Management] > [File Directory] をクリックします。

ステップ 2 必要な場合、[Auto Mirror Configuration] を有効にします。これにより、ミラー コンフィギュレーション ファイルの自動作成が有効になります。この機能を無効にした場合、ミラーコンフィギュレーションファイルが削除されます（存在する場合）。

ステップ 3 ファイルおよびディレクトリを表示するドライブを選択します。次のオプションを使用できます。

- フラッシュ（Flash）：管理ステーションのルート ディレクトリにあるすべてのファイルを表示します。
- USB：USB ドライブ上のファイルを表示します。

ステップ 4 [Go] をクリックすると、次のフィールドが表示されます。

- ファイル名（File Name）：ファイルタイプに応じてシステム ファイル タイプまたは実際のファイル名。
- 権限（Permissions）：ファイルに対するユーザの読み取り/書き込み権限。
- サイズ（Size）：ファイルサイズ。
- 最終更新日時（Last Modified）：ファイルが変更された日付と時刻。
- フル パス（Full Path）：ファイルのパス。

ステップ 5 [Refresh] アイコンをクリックしてデータを更新します。ファイルを削除する場合は、ファイルを選択して [Delete] アイコンをクリックします。

ステップ 6 [Apply] をクリックして設定を保存します。

DHCP 自動更新

自動設定/イメージ更新機能は、自動的にネットワーク内のスイッチを設定し、ファームウェアをアップグレードする便利な方法を提供します。管理者はこのプロセスを使用して、ネットワーク内のこれらのデバイスの設定とファームウェアをリモートから最新の状態に保つことができます。

手順

ステップ 1 [Administration] > [File Management] > [DHCP Auto Update] の順にクリックします。

ステップ 2 次を設定します。

DHCP経由の自動コンフィギュレーション	DHCP による自動設定を有効にするには、[Enable] にチェックを付けます。自動設定機能により、ネットワーク内のスイッチの設定と、そのファームウェアのアップグレードを自動で行うことができます。
ダウンロードプロトコル	次のオプションから、ダウンロードプロトコルを選択します。 • [Auto By File Extension]：（デフォルト）この拡張子を持つファイルは SCP を使用して（SSH 経由で）ダウンロードされ、その他の拡張子を持つファイルは TFTP を使用してダウンロードされます。 • [TFTP Only]：設定ファイル名のファイル拡張子に関係なく、ダウンロードは TFTP で行われます。 • [SCP Only]：設定ファイル名のファイル拡張子に関係なく、ダウンロードは SCP（SSH 経由）で行われます。
DHCP によるイメージ自動更新	[Enable] チェックボックスをオンにすると、DHCP によるイメージの自動更新が有効になります。イメージの自動更新機能により、ネットワーク内のスイッチの更新と、そのファームウェアのアップグレードを自動で行うことができます。

ダウンロードプロトコル	次のオプションから、ダウンロードプロトコルを選択します。 • [Auto By File Extension]：（デフォルト）この拡張子を持つファイルは SCP を使用して（SSH 経由で）ダウンロードされ、その他の拡張子を持つファイルは TFTP を使用してダウンロードされます。 • [TFTP Only]：設定ファイル名のファイル拡張子に関係なく、ダウンロードは TFTP で行われます。 • [SCP Only]：設定ファイル名のファイル拡張子に関係なく、ダウンロードは SCP（SSH 経由）で行われます。

ステップ 3 SCP の SSH 設定を選択します。

リモート SSH サーバー認証	リンクをクリックすると、[SSH Server Authentication] ページに移動します。このページでは、ダウンロードに使用する SSH サーバの認証を有効にし、必要な場合は信頼できる SSH サーバを入力できます。
SSHクライアント認証	• [SSH User Authentication] ページで [System Credentials] をクリックしてユーザーログイン情報を入力します。
バックアップサーバー定義	次のオプションから選択します。 • IPアドレス別 • 名前別
IP Version	次のオプションから選択します。 • バージョン 6 • バージョン 4
IPv6 Address Type	次のオプションから選択します。 • [Link Local]：リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。 • [Global]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
Link Local Interface	IPv6 アドレスタイプで [Link Local] を選択した場合は、ドロップダウンリストからインターフェイスを選択します。
バックアップサーバーの IP アドレス/名前	バックアップ設定ファイルの名前を入力します。

バックアップコンフィギュレーションファイル名	バックアップ設定ファイルの名前を入力します（0 ～ 160 文字を使用）。
バックアップ間接イメージファイル名	バックアップ間接イメージファイルの名前を入力します（0 ～ 160 文字を使用）。
前回の自動設定サーバーのIPアドレス	前回の自動設定サーバーの IP アドレスのアドレスが表示されます。
最後に自動コンフィギュレーションで使用したファイル名	前回の自動設定ファイルの名前が表示されます。

（注）
DHCP自動コンフィギュレーション/イメージは、IPアドレスが動的に設定される場合にのみ機能します。

ステップ 4 [Apply] をクリックして設定値を保存します。

Cisco Business ダッシュボードの設定

Cisco Business ダッシュボードは、Cisco Business ダッシュボードマネージャを使用して、Cisco 100 ー 500 シリーズのネットワークを監視および管理するために役立ちます。Cisco Business ダッシュボードマネージャは、ネットワークを自動的に検出し、シスコのスイッチ、ルータ、ワイヤレスアクセスポイントなど、サポートされているすべての Cisco 100 ～ 500 シリーズのデバイスを設定および監視することを可能にするアドオンです。

Cisco Business ダッシュボードを表示するには、[Request a Demo] をクリックします。

Cisco Business ダッシュボードマネージャは、2 つの個別のコンポーネントまたはアプリケーション（Cisco Business ダッシュボードプローブと呼ばれる 1 つ以上のプローブと、Cisco Business ダッシュボードマネージャと呼ばれる 1 つのマネージャ）から構成される分散アプリケーションです。Cisco Business ダッシュボードプローブのインスタンスは、ネットワークの各サイトにインストールされ、ネットワークを検出し各シスコデバイスと直接通信します。

（注） Cisco Business ダッシュボードマネージャおよびプローブのセットアップ方法の詳細については、Cisco Business ダッシュボードのクイックスタートガイドを参照してください。

https://cisco.com/go/cbd-docs

スイッチのグラフィカルユーザーインターフェイス（GUI）で次の手順を実行して、ダッシュボードへのプローブ接続を有効にし、ダッシュボードへの接続を許可するために必要な組織名、ネットワーク名、およびその他の情報を設定します。

手順

ステップ 1 [Administration] > [Cisco Business Dashboard Settings] の順にクリックします。

ステップ 2 次を設定します。

[Probe Operation]	Cisco Business ダッシュボードプローブの動作を有効にする場合はチェックを入れます。
[Probe Status]	CBD プローブのステータスが表示されます。可能な値は、[Active]、[Inactive]、または [Fault] です。 プローブステータスが [Active] の場合、プローブステータス [Active] とともにプローブモードも次のように表示されます。 • [Active (Probe Managed)]：プローブはネットワーク検出を実行し、ダッシュボードに代わって各管理対象デバイスと直接通信します。 1 つのネットワークでは、1 つの Probe のみを有効にする必要があります。 • [Active (Direct Managed)]：直接管理対象デバイスは、広範囲のネットワーク内にある他のデバイスを検出すると、ダッシュボードにそれらのデバイスを自動的に接続し、それらのデバイスを管理可能にします。必要に応じて、ダッシュボードで IP アドレス範囲を明示的に検索し、他の VLAN やサブネットにあるネットワークデバイスを検出することができます。 すべてのデバイスが直接管理をサポートしている場合は、直接管理ネットワークが推奨されます。
[Probe Version]	Cisco Business ダッシュボードプローブのバージョンが表示されます。
[Logging Threshold]	ドロップダウンリストからオプション（[Information]、[Debug]、[Warning]、または [Error]）を選択して、Cisco Business Dashboard プローブエージェントがログに記録するメッセージのレベルを制限します。指定したレベル以上のメッセージのみがログに記録されます。
[All Module Logging]	有効にする場合はオンにします。これにより、すべてのモジュール間のすべての通信とイベントがログに記録されます。
[Call Home Logging]	有効にする場合はオンにします。これにより、プローブとマネージャの間のすべての通信がログに記録されます。
[Discovery Logging]	有効にする場合はオンにします。これにより、デバイス検出イベントとトポロジ検出がログに記録されます。
[Services Logging]	有効にする場合はオンにします。これにより、ノースバウンドとサウスバウンドの間のメッセージ変換がログに記録されます。

[System Logging]	有効にする場合はオンにします。これにより、他のログの対象になっていないコアシステムプロセスがログに記録されます。
[Northbound Logging]	有効にする場合はオンにします。これにより、マネージャとプローブの間の通信がログに記録されます。
[Southbound Logging]	有効にする場合はオンにします。これにより、プローブとデバイスの間の低レベルの通信がログに記録されます。
[Dashboard Connection]	オンにすると接続が有効になります。
[Dashboard Status]	Cisco Business ダッシュボードマネージャのステータス（[Connected] または [Disconnected]）が表示されます。 ダッシュボードのステータスが [Disconnected] の場合、エラーの理由が表示されます。次に例を示します。 • Certificate-error：未指定の証明書検証エラー • Certificate-error：証明書はまだ有効ではありません • Certificate-error：証明書の有効期限が切れました • Certificate-error：証明書の確認に失敗しました • Connection-error：ホストが見つかりません（権限あり） • Connection-error：ホストへのルートがありません
[Dashboard Definition]	Cisco Business ダッシュボードのアドレスを定義します。次のいずれかを選択します。 • [By IP address]：このオプションでは、[IP Address/Name] フィールドに有効な IP アドレスを入力する必要があります。 • [By Name]：このオプションでは、[IP Address/Name] フィールドにホスト名を入力する必要があります。
[IP Address/Name]	Cisco Business ダッシュボードの名前または IP アドレスを入力します。
[Dashboard Port]	ダッシュボードに接続するには、次のいずれかの TCP ポートを指定します。 • デフォルト（443）の使用。 • ユーザー定義（範囲：1～65535）。このオプションは、[Dashboard Address] フィールドに有効なアドレスが入力されている場合にのみ使用できます。
[Connection Setup]	次のいずれかの接続設定を指定します。 • [Online with Web Browser] • [Offline with Access Key]

[Access Key ID]	[Access Key ID] フィールドは、24 桁の 16 進数で構成されています。このフィールドには 16 進数文字以外は入力できないことに注意してください。
[Access Key Secret]	認証に使用するシークレットを指定します。暗号化またはプレーンテキストのいずれかの形式で指定できます。プレーンテキスト形式は、ホワイトスペースなしで、最大 160 文字の英数字文字列として指定されます。キー ID とシークレットの設定は、同時に設定する必要があります。 （注） 適用時に、[Key ID] フィールドが空で [Secret] フィールドが空でない場合、または [Secret] フィールドが空で [Key ID] フィールドが空でない場合、「Key ID and Secret must be set together」というエラーメッセージが表示されます。

ステップ 3 [Apply] をクリックし、実行コンフィギュレーションに設定を保存します。

（注）
[Dashboard Connection] 設定が有効になっている場合、フィールドの [Organization Name]、[Network Name]、[Dashboard Address]、[Key ID] は変更できません。これらの設定を変更するには、[Dashboard Connection] チェックボックスをオフにし、[Apply] をクリックして、上記の手順 2 ～ 4 をやり直します。

[Display Sensitive Data as Plaintext]：クリックすると機密データがプレーンテキスト形式で表示されます。

[Reset Connection]：クリックすると、ダッシュボードとの現在の接続を切断し、Cisco Business ダッシュボードプローブのキャッシュデータをフラッシュしてから、ダッシュボードへの再接続を試みます操作の開始前に確認メッセージが表示されます。このコントロールは、[Dashboard Connection] と [Probe Operation] が有効になっている場合にのみ有効になります。

（注）
[Reset Connection] は、[Dashboard Connection] チェックボックスと [Probe Operation] チェックボックスがオンになっている場合にのみ有効になります。

[Clear Probe Database]：クリックすると、プローブデータをクリアします。これは、[Probe Operation] チェックボックスがオフになっている（および画面がロードされて以降オフである）場合にのみ有効になります。それ以外の場合、ボタンは無効になり、「Probe Operation must be disabled prior to clearing probe database」というツールチップが表示されます。

（注）
スイッチ上の Cisco Business Dashboard プローブが管理できるネットワークデバイスとクライアントの数には、多くの要因が影響します。スイッチ上のプローブでは、15 台以下のネットワークデバイス（スイッチ、ルータ、およびワイヤレスアクセスポイント）と、150 台以下の接続クライアントを管理することを推奨します。ネットワークがより複雑な場合は、Cisco Business Dashboard プローブに他のプラットフォームを使用することをお勧めします。Cisco Business Dashboard の詳細については、https://www.cisco.com/c/en/us/products/cloud-systems-management/business-dashboard/index.html を参照してください。

プラグアンドプレイ（PNP）

新しいネットワーク デバイスの設置やデバイスの交換を手作業で行うと、費用と時間がかかり、誤りが発生しやすくなります。通常、新しいデバイスは最初に中心的な準備施設に送られ、そこでデバイスを開梱し、ステージング ネットワークに接続し、適切なライセンス、設定、イメージを使って更新します。その後、デバイスを梱包して実際の設置場所に運びます。これらの手順が完了した後、専門的な担当者が設置場所まで出向いて設置作業を行う必要があります。デバイスがNOC/データ センター自体に設置される場合でも、デバイスの数が非常に多くて専門家が不足する可能性があります。このすべての問題のために、デプロイが遅れ、運用コストがさらに増えます。

PNP サーバーへの接続

スイッチがPnPサーバーに接続できるように、スイッチがPNPサーバーのアドレス/URLを検出するプロセスが実行されます。検出方法には複数の方法があります。スイッチでは以下に示すシーケンスに従って実行されます。PnPサーバーが特定の方法で検出された場合、検出プロセスは完了し、残りの方法は実行されません。

1. ユーザー設定のアドレス：PnP サーバーの URL または IP アドレスはユーザーが指定します。
2. DHCP 応答オプション 43 から受信したアドレス：PnP サーバーの URL または IP アドレスは、DHCP 応答のオプション 43 の一部として受信されます
3. ホスト名「pnpserver」の DNS 解決：ホスト名「pnpserver」の DNS サーバー解決によって、アドレス指定された PnP サーバー IP が取得されます。
4. Cisco プラグアンドプレイ接続：HTTP を介して実行される完全な PNP サーバー検出を「すぐに使用可能」にするリダイレクションサービス。

スイッチは、FQDN「devicehelper.cisco.com」を使用してリダイレクションサービスに接続します。

Cisco PnP 接続の前提条件

Cisco プラグアンドプレイ接続動作を可能にするには、ユーザーが、プラグアンドプレイ接続でデバイスとコントローラプロファイルを作成する必要があります（https://software.cisco.com に移動し、[Plug and Play Connect] リンクをクリック）。PnP 接続を使用するには Cisco スマートアカウントが必要です。スマートアカウントを作成または更新するには、https://software.cisco.com の [Administration] セクションを参照してください。

さらに、スイッチ自体で次の前提条件が満たされている必要があります。

- PNP サーバーが他の検出方法で検出されていない。
- デバイスが devicehelper.cisco.com という名前を正常に解決できる（静的設定または DNS サーバーを使用）。
- システム時刻が次のいずれかの方式で設定されている。

- 時刻が SNTP サーバーによって更新されている。
- クロックがユーザーによって手動で設定されている。
- リアルタイムクロック（RTC）により、リセット後も時間が保持されている。

CA 署名付き証明書ベースの認証

シスコでは、署名機関によって署名された証明書を .tar ファイル形式で配布し、シスコの認証局（CA）署名を使用してバンドルに署名します。この証明書バンドルは、cisco.com でのパブリックダウンロード向けに Cisco infoSec によって提供されます。

（注） シスコ PnP 接続情報に基づいて PNP サーバーを検出する場合、トラストプールは http://www.cisco.com/security/pki/trs/ios_core.p7b からダウンロードされます。

DHCP オプション 43 に基づいて PNP サーバーを検出する場合は、DHCP オプション 43 の「T<Trust pool CA bundle URL>;」パラメータを使用して、トラストプールをダウンロードするための URL を指定します。このバンドルの証明書は、SSL ハンドシェイク時にサーバー側の検証用シスコデバイスにインストールできます。サーバでは、バンドルで使用可能な CA のいずれかによって署名された証明書を使用するものとします。

PnP エージェントは、組み込み PKI 機能を使用して証明書バンドルを検証します。バンドルはシスコの CA によって署名されるため、エージェントはデバイスに証明書をインストールする前に、改ざんされたバンドルを特定できます。エージェントによってバンドルの整合性が確認されると、デバイスに証明書がインストールされます。証明書がデバイスにインストールされると、サーバから追加手順を実行しなくても PnP エージェントがサーバへの HTTPS 接続を開始します。

（注） デバイスでは、組み込み証明書バンドルをブートアッププロセスの一環としてインストールすることもできます。このバンドルは、PNP サーバーの検証に使用できます。バンドルがシスコ PnP 接続情報に基づいてダウンロードされると、ダウンロードされたバンドルから証明書がインストールされ、組み込みバンドルに基づく証明書はアンインストールされます。

（注） PNP エージェントは、インストールされた CA 証明書に基づいて PNP 証明書を検証するだけでなく、証明書の共通名/サブジェクト代替名（CN/SAN）が PNP サーバーのホスト名/IP アドレスと一致するかも検証します。一致しない場合、証明書の検証は拒否されます。

Cisco PnP DHCP オプション 43 使用上のガイドライン

DHCP オプション 43 はベンダー固有の識別子です。これは、PnP エージェントが PnP サーバーを見つけて接続するために使用できる方法の一つです（詳細については、Cisco プラグアンドプレイを参照）。

DHCP サーバーでの適切な設定を可能にするオプション 43 の設定については、以下を参照してください。

オプション 43 には次のフィールド/パラメータが含まれています。

<DHCP-typecode><feature-opcode><version><debug-option>;<arglist>

<arglist> パラメータでは次の構文を使用する必要があります。

B<IP address type>;I<IP address>;J<Port>;K<Transport protocol>;T<Trust pool CA bundle URL>;Z<SNTP server IP address>

次の表に、オプション 43 のフィールドの説明と使用方法の詳細を示します。

パラメータ	説明
DHCP-typecode	DHCP サブオプションタイプ。PnP の DHCP サブオプションタイプは 5 です。
feature-opcode	機能動作コード：アクティブ（A）またはパッシブ（P）のいずれかにできます。PnP の機能動作コードはアクティブ（A）です。これにより、PnP エージェントが PnP サーバーへの接続を開始します。PnP サーバーに到達できない場合、PnP エージェントは接続を確立するまで再試行します。
version	PnP エージェントが使用するテンプレートのバージョン。1 にする必要があります。
debug-option	DHCP オプション 43 の処理時のデバッグメッセージをオンまたはオフにします。 D：デバッグオプションはオンです。N：デバッグオプションはオフです。
K	PnP エージェントと PnP サーバーの間で使用されるトランスポートプロトコル。 4：HTTP または 5：HTTPS。
B	文字コード「I」で指定される PnP サーバーの IP アドレスの タイプ。 1：ホスト、2：IPv4、3：IPv6

パラメータ	説明
I	PnP サーバーの IP アドレスまたはホスト名。ホスト名を指定する場合は、ホスト名を正常に使用できるように、DHCP サーバーに DNS 関連のオプションが存在している必要があります。
T	トラストプールの CA バンドルの URL。CA バンドルは、Cisco Business ダッシュボードまたは TFTP サーバーから取得できます。 • Cisco Business ダッシュボードを使用する場合は、次の URL 形式を使用します。 http://*CBD IP address or domain name/ca/trustpool/CA_bundle_name* • TFTP サーバーを使用する場合は、次の URL 形式を使用します。tftp://*tftp server IP/CA_bundle_name*
Z	SNTP サーバー IP アドレス。トラストプールを設定する前に、クロックを同期させる必要があります。 （注） スイッチのクロックは、スイッチでサポートされている SNTP サーバーによって更新された場合（デフォルトで、ユーザー設定により、または Z パラメータで）またはユーザーが手動で設定した場合に同期していると見なされます。このパラメータは、スイッチが他の SNTP サーバーに到達できないときにトラストプールセキュリティを使用する場合に必要です。たとえば、初期状態のスイッチで工場出荷時にデフォルト設定が行われているものの、デフォルトの SNTP サーバーに到達するためのインターネット接続がない場合などです。
J	ポート番号 HTTP=80 HTTPS=443

オプション 43 の使用例：

- 次の形式は、HTTP を使用した PnP 接続のセットアップに使用されます。

```
option 43 ascii 5A1N;K4;B2;I10.10.10.3;J80
```

- 次の形式は、トラストプールを直接使用する HTTPS 上での PnP 接続のセットアップに使用されます。HTTPS は、トラストプールの CA バンドルが Cisco Business ダッシュボードからダウンロードされ、Cisco Business ダッシュボードサーバー証明書がサードパーティによって発行されている（自己署名ではない）場合に使用できます。次の例で「10.10.10.3」は Cisco Business ダッシュボードの IP アドレスです。ドメイン名を指定することもできます。

```
option 43 ascii
5A1N;K5;B2;I10.10.10.3;Thttp://10.10.10.3/ca/trustpool/ios.p7b;Z10.75.166.1
```

PNP設定

PNP 設定を行うには、次の手順に従ってください。

手順

ステップ 1 [Administration] > [PNP] > [PNP Settings] の順にクリックします。

ステップ 2 次のフィールドに情報を入力して、PNP を設定します。

PNP状態	有効にする場合はオンにします。
PNP トランスポート/設定の定義	使用するトランスポートプロトコル、PNP サーバーアドレス、および使用する TCP ポートに関する設定情報を取得するためのオプションとして、次のいずれかを選択します。 • [Default Settings]：このオプションを選択すると、DHCP オプション 43 から PNP 設定が取得されます。DHCP オプション 43 から設定が得られない場合、デフォルト値（デフォルト トランスポート プロトコルの HTTP、PNP サーバーの DNS 名として「pnpserver」、HTTP に関連するポート）が使用されます。「pnpserver」の名前が DNS によって解決されない場合は、DNS 名「devicehelper.cisco.com」を使用して Cisco プラグアンドプレイ接続サービスが使用されます。[Default Settings] オプションを選択すると、[PNP Transport] セクションのすべてのフィールドがグレー表示になります。デバイス上で PNP エージェントと [DHCP Auto Configuration/Image Update] の両方が有効になっている場合、オプション 43 に加えて、コンフィギュレーションまたはイメージファイル名に関連するオプションが DHCP 応答に含まれていると、デバイスは、受信したオプション 43 を無視します。 • [Manual Settings]：PNP トランスポートに使用する TCP ポートとサーバーを手動で設定します。
トランスポートプロトコル	トランスポートプロトコル（HTTP または HTTPS）を選択します。
TCP ポート	TCP ポートの番号。これはシステムによって自動的に入力されます。HTTP の場合は 80 です。
サーバー指定方法	PNP サーバーを IP アドレスで指定するか、名前で指定するかを選択します。

IP バージョン	サポートする IP 形式を選択します。 • [Version 6]：IPv6 • [Version 4]：IPv4
サーバーIPv6アドレスタイプ	IP バージョンタイプが IPv6 である場合は、次のいずれかのオプションを選択します。 • [Link Local]：IPv6 アドレスによって、同一ネットワーク リンク上のホストが一意に識別されます。リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカル ネットワーク内で通信する場合にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカルアドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。 • [Global]：IPv6 アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
Link Local Interface	送信元 IPv6 アドレスタイプが [Link Local] である場合は、どこから IPv6 アドレスを受け取るかを選択します。
サーバーのIPアドレス/名前	PNP サーバーの IP アドレスまたはドメイン名を入力します。
PNPユーザー/ユーザー定義	サーバーに送られる PNP パケットに含まれるユーザー情報。次のオプションのいずれかを選択します。 • [Default Settings]：このオプションを選択すると、PNP ユーザー名とパスワードの設定が DHCP オプション 43 から取得されます。このオプションを選択すると、ユーザー名とパスワードのフィールドがグレー表示になります。 • [Manual Settings]：PNP ユーザー名とパスワードを手動で設定するにはこれを選択します。
ユーザー名	PNP パケットに含めるユーザー名。
パスワード	暗号化形式またはプレーンテキスト形式のパスワード。
PNP動作設定/再接続間隔	[User Defined] を選択した場合に、接続が失われてからセッションの再接続が試行されるまでの間隔（秒数）を設定します。
ディスカバリタイムアウト	PNP サーバーの検出に失敗した後、検出を再試行するまでの待機時間（秒数）を指定します。

タイムアウト指数因子	指数を使って検出の試行をトリガーする値。前のタイムアウト値を指数で乗算し、その結果をタイムアウトとして適用します（値がタイムアウト最大値より小さい場合）。
最大ディスカバリタイムアウト	タイムアウトの最大値。[Discovery Timeout] 値よりも大きくなければなりません。
ウォッチドッグタイムアウト	アクティブなPNPセッション中（ファイルのダウンロード処理中など）にPnPまたはファイルサーバーからの応答を待つ間隔。

ステップ3 [Apply] をクリックします。パラメータが実行コンフィギュレーション ファイルにコピーされます。

暗号化されたパスワードを表示するには、[Display Sensitive Data as Plaintext] をクリックします。

PNPセッション

PNP セッション画面には、現在有効になっている PNP パラメータの値が表示されます。該当する場合、パラメータのソースが括弧で示されます。

PNP パラメータに関する情報を表示するには、次の手順を実行します。

手順

[Administration] > [PNP] > [PNP Session] をクリックします。

次のフィールドが表示されます。

- [Administrative Status]：PNP が有効になっているかどうか。
- [Operational Status]：PNP が動作中かどうか。
- [PNP Agent State]：アクティブなPNPセッションが存在するかどうかを示します。可能な値は、[Discovery Wait]、[Discovery]、[Not Ready]、[Disabled]、[Session]、[Session Wait] です。
- [Transport Protocol]：PNP エージェント セッション情報を表示します。
- [TCP Port]：PNP セッションの TCP ポート。
- [Server IP Address]：PNP サーバーの IP アドレス。
- [Username]：PNP パケットで送信されるユーザー名。
- [Password MD5]：PNP パケットで送信されるパスワード。
- [Session Interval Timeout]：設定済みのセッション間隔タイムアウト（PNP エージェント状態が「待機中」の場合にのみ表示されます）。

• [Remaining Timeout]：残っているタイムアウトの値。

（注） [Resume] ボタンをクリックすると、ただちに PnP エージェントが次のように待機状態を終了します。

- エージェントがディスカバリ待機中状態の場合は、ディスカバリ状態に設定されます。
- エージェントが PnP セッション待機中状態の場合は、PnP セッション状態に設定されます。

リブート

ジャンボ フレームのサポートの有効化などの一部の設定変更では、システムのリブートが必要です。ただし、デバイスをリブートすると、実行コンフィギュレーションが削除されるので、デバイスをリブートする前に、実行コンフィギュレーションをスタートアップ コンフィギュレーションとして保存しておくことが重要です。[Apply] をクリックしても、コンフィギュレーションはスタートアップ コンフィギュレーションに保存されません。

デバイスをリブートするには、次の手順を実行します。

手順

ステップ 1 [Administration] > [Reboot] の順にクリックします。

ステップ 2 [Reboot] をクリックし、デバイスをリブートします。再起動を確認するポップアップが表示されます。[OK] をクリックします。

リブート時に実行コンフィギュレーション内の保存されていない情報は破棄されてしまうので、[Save] をクリックして、ブート中に現在のコンフィギュレーションが保持されるようにする必要があります。[Save] オプションが表示されない場合は、実行コンフィギュレーションがスタートアップ コンフィギュレーションと一致していて、保存する必要がないことを意味しています。

ステップ 3 次のいずれかの再起動オプションから選択します。

- • [Immediate]：すぐにリブートします。
  - [Date]：スケジュール リブートの日付（月/日）と時刻（時間と分）を入力します。指定した時刻（24 時間形式を使用）にソフトウェアがリロードされるように、スケジュールが設定されます。

  （注）
  このオプションは、システム時刻か手動で設定されているか SNTP によって設定されている場合にのみ使用できます。

- [In]：デバイスが再起動するまでの日数、時間、分を入力します。経過可能な時間は、最大 24日です。

ステップ 4 [Restore to Factory Defaults] をオンにして、再起動プロセス中に工場出荷時のデフォルト設定を復元します。

ステップ 5 構成ファイルをクリアするには、[Clear Startup Configuration File] をオンにします。

ステップ 6 [Cancel Reboot] をクリックすると、スケジュール済みのリブートがキャンセルされます。

ハードウェアリソース

[Hardware Resources] ページでは、ポリシーベースのルーティング（IPv4 および IPv6）と VLAN マッピングのルールに関してルータ TCAM 割り当てを調整できます。また、ステータスを確認し、ハードウェアベースのルーティングを再アクティブ化できます。

ルータ TCAM 割り当ての変更が正しくない場合、エラーメッセージが表示されます。ルータ TCAM 割り当てが適切な場合、新しい設定で自動リブートが実行されることを知らせるメッセージが表示されます。

ルーティングリソースは、変更が正しく行われない場合があります。次のいずれかの状態が該当します。

- 特定のエントリ タイプに対して割り当てたルータ TCAM エントリ数が、現在使用中のエントリ数より少ない場合。
- 割り当てたルータ TCAM エントリの総数が、使用可能な最大数よりも多い場合。

ルーティングリソースを表示および変更するには、次のようにします。

手順

ステップ 1 [Administration] > [Hardware Resources] の順にクリックします。

次のフィールドが表示されます。

- [Maximum IPv4 Policy-Based Routes]
  - [Use Default]：デフォルト値を使用します。
  - [User Defined]：値を入力します（範囲 0 ～ 32、デフォルト 12）。

    （注）
    [User Defined] の範囲は、スイッチのモデルによって異なる場合があります。

- [Maximum IPv6 Policy-Based Routes]
  - [Use Default]：デフォルト値を使用します。

- [User Defined]：値を入力します（範囲 0 ～ 32、デフォルト 12）。

  （注）
  [User Defined] の範囲は、スイッチのモデルによって異なる場合があります。

- [Maximum VLAN—Mapping entries]：次のいずれかを選択します。
  - [Use Default]：デフォルト値を使用します。
  - [User Defined]：値を入力します（範囲 0 ～ 228、デフォルト 0）。

    （注）
    [User Defined] の範囲は、スイッチのモデルによって異なる場合があります。

- [Hardware-Based Routing]：ハードウェアベースのルーティングがアクティブであるか、非アクティブであるかを表示します。

ステップ 2 [Apply] をクリックして新しい設定を保存します。

（注） ハードウェアベースのルーティングがアクティブではない場合には、[Reactivate Hardware Based Routing] ボタンが表示されます。ハードウェア ベースのルーティングを有効にするには、このボタンをクリックします。ハードウェア ベースのルーティングのアクティブ化は、現在のルーティング コンフィギュレーションをサポートするのに使用可能なハードウェア リソースに応じて決まります。デバイス設定をサポートできる十分なルータリソースがない場合は、操作が失敗し、エラーメッセージがユーザーに対して表示されます。

ディスカバリ - Bonjour

Bonjour クライアントとして、デバイスはディスカバリ - Bonjour プロトコルのパケットを、直接接続された IP サブネットにブロードキャストします。このデバイスは、ネットワーク管理システムまたはその他のサードパーティ製アプリケーションから検出できます。デフォルトでは、管理 VLAN で Bonjour が有効になっています。

Bonjour 設定を行うには、次の手順に従ってください。

手順

ステップ 1 [Administration] > [Discovery - Bonjour] をクリックします。
ステップ 2 [Enable] をオンにし、ディスカバリ - Bonjour をグローバルに有効にします。
ステップ 3 特定のインターフェイスで Bonjour を有効にするには、[Add] をクリックします。
ステップ 4 インターフェイス（ポート、LAG、または VLAN）を選択し、インターフェイスを構成します。

ステップ 5 [Apply] をクリックして実行コンフィギュレーション ファイルを更新します。

（注）
Bonjourが有効な場合、デバイスはBonjourディスカバリ インターフェイス コントロール テーブルでBonjourに関連付けられている IP アドレスを持つインターフェイスに、ディスカバリ - Bonjour パケットを送信します。

ステップ 6 [Delete] をクリックして、インターフェイスの Bonjour を無効にします。

ディスカバリ - LLDP

LLDPは、ネットワーク マネージャによるマルチベンダー環境でのネットワーク管理のトラブルシューティングや強化を可能にするプロトコルです。LLDP では、ネットワーク デバイスが、それ自体を他のデバイスにアドバタイズする手法と、検出された情報を保存する手法が標準化されています。LLDPにより、デバイスは、そのID、設定、および機能を近接するデバイスにアドバタイズできます。その後、受信側のデバイスは、それらのデータを管理情報ベース（MIB）に保存します。

LLDP はリンク層プロトコルです。デフォルトで、デバイスは、プロトコルの要求に従ってすべての着信 LLDP パケットの終了し、処理します。ここでは、LLDP の設定方法について説明します。内容は次のとおりです。

プロパティ

[Properties]ページでは、LLDPの一般パラメータを入力して、機能をグローバルに有効/無効にしたり、タイマーを設定したりすることができます。LLDP のプロパティを入力するには、次の手順を実行します。

手順

ステップ 1 [Administration] > [Discovery - LLDP] > [Properties] をクリックします。

ステップ 2 パラメータを入力します。

LLDP Status	選択するとデバイス上の LLDP が有効になります（デフォルトで有効）。
LLDP Frames Handling	[LLDP] が有効になっていない場合は、次のいずれかのオプションを選択します。 • [Filtering]：パケットを削除します。 • [Flooding]：VLAN メンバーすべてにパケットを転送します。

TLV Advertise Interval	次のオプションのいずれかを選択します。 • [Use Default]：デフォルト値を使用します。 • [User Defined]：値を入力します。
Topology Change SNMP Notification Interval	次のオプションのいずれかを選択します。 • [Use Default]：デフォルト値を使用します。 • [User Defined]：値を入力します。
Hold Multiplier	次のオプションのいずれかを選択します。 • [Use Default]：デフォルト値を使用します。 • [User Defined]：値を入力します。
Reinitializing Delay	次のオプションのいずれかを選択します。 • [Use Default]：デフォルトの時間を使用します。 • [User Defined]：時間を入力します
Transmit Delay	次のオプションのいずれかを選択します。 • [Use Default]：デフォルトの時間を使用します。 • [User Defined]：時間を入力します
Chassis ID Advertisement	LLDP メッセージのアドバタイズメントに関して、次のオプションのいずれかを選択します。 • [MAC Address]：デバイスの MAC アドレスをアドバタイズします。 • [Host Name]：デバイスのホスト名をアドバタイズします。

ステップ 3 LED-MED の [Properties] の [Fast Start Repeat Count] フィールドに、LLDP-MED Fast Start 機能の初期化時に LLDP パケットを送信する回数を入力します。LLDP-MED FastStart メカニズムは、新しいエンドポイントデバイスがデバイスにリンクしたときに初期化されます。LLDP MED の詳細については、「LLDP MED ネットワーク ポリシー」セクションを参照してください。

ステップ 4 [Apply] をクリックします。LLDP プロパティが実行コンフィギュレーション ファイルに追加されます。

ポート設定

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

[LLDP Port Settings] ページで、ポートごとに LLDP と SNMP の通知を有効にできます。LLDP-MED TLV は、LLDP MEDポート設定 （52 ページ）で設定できます。

LLDP ポート設定を定義するには、次の手順を実行します。

手順

ステップ 1 [Administration] > [Discovery - LLDP] > [Port Settings] をクリックします。

このページには、ポートの LLDP 情報が表示されます。

ステップ 2 ポートを選択して [Edit] をクリックします。

ステップ 3 次のフィールドを設定します。

Interface	編集するポートを選択します。
Administrative Status	このポートの LLDP 発行オプションを選択します。 • [Tx Only]：発行はしますが検出はしません。 • [Rx Only]：検出はしますが発行はしません。 • [Tx & Rx]：送信も検出も行います。 • [Disable]：このポート上で LLDP を無効にします。
SNMP 通知	[Enable] を選択すると、SNMP 通知の受信者に通知が送信されます。

使用可能な、または選択されたオプションの TLV	デバイスが発行する情報のオプションを選択します。 • [Port Description]：ポートに関する情報。 • [System Name]：システムに割り当てられた名前。 • [System Description]：ネットワークエンティティの説明。 • [System Capabilities]：デバイスの主な機能、およびそれらの機能がデバイス上で有効になっているかどうか。 • [802.3 MAC-PHY]：送信元デバイスの、設定可能な通信方式（全二重 / 半二重） およびビット レート、ならびに、現在の通信方式およびビット レート。 • [802.3 Power via MDI]：MDI 経由で伝送される最大電力。 • [802.3 Link Aggregation]：LLDP PDU 送信元ポートに関連付けられてい るリンクを集約できるかどうかを示します。 • [802.3 Maximum Frame Size]：MAC/PHY の実装における許容最大フレームサイズ。 • [4-Wire Power via MDI]：（60W PoE をサポートする PoE ポートに関連）60 ワットの電力を可能にする Power over Ethernet をサポートするために定義されたシスコ独自の TLV（標準サポートは最大 30 ワット）。 管理アドレスのオプション TLV
アドバタイズメントモード	デバイスの IP 管理アドレスをアドバタイズする方法を次の中から 1 つ選択します。 • [Auto Advertise]：アドバタイズする管理アドレスをデバイスのすべての IP アドレスからソフトウェアが自動的に選択するように指定します。複数の IP アドレスがある場合、ソフトウェアはダイナミック IP アドレスの中から最下位の IP アドレスを選択します。ダイナミック アドレスがない場合、ソフトウェアはスタティック IP アドレスの中から最下位の IP アドレスを選択します。 • [None]：アドバタイズメントモードが不要な場合、このオプションを選択します。 • [Manual Advertise]：アドバタイズする管理 IP アドレスを選択します。
IP Address	[Manual Advertise] を選択した場合、表示される IP アドレスの中から管理 IP アドレスを選択します。
PVID	TLV で PVID をアドバタイズする場合に選択します。

VLAN ID	アドバタイズする VLAN を選択します。
プロトコルID	アドバタイズするプロトコルを選択します。
選択されたプロトコルID	[Protocols IDs] ボックスで使用するプロトコルを選択して、それらを [Selected Protocols ID] ボックスに移動します。

ステップ 4 関連情報を入力し、[Apply] をクリックします。ポート設定は、実行コンフィギュレーション ファイルに書き込まれます。

LLDP MED ネットワークポリシー

LLDP-MED ネットワークポリシーは、音声やビデオなどの特定のリアルタイムアプリケーションに関連する設定のセットです。ネットワーク ポリシーが設定されている場合は、接続された LLDP メディア エンドポイント デバイスへの発信 LLDP パケットにそのポリシーを含めることができます。メディア エンドポイント デバイスは、受信したネットワーク ポリシーの指定に従ってトラフィックを送信する必要があります。たとえば、VoIP フォンに対して VoIP トラフィックの次の処理を指示するネットワーク ポリシーを作成できます。

- VLAN 10 の音声トラフィックをタグ付きパケットとして 802.1p プライオリティ 5 で送信する。
- DSCP 46 で音声トラフィックを送信する。

ネットワークポリシーをポートにバインドするには、LLDP MEDポート設定 （52 ページ）を使用します。管理者は、1 つ以上のネットワーク ポリシーと、ポリシーの宛先インターフェイスを手動で設定できます。VLAN を手動で作成することと、ネットワーク ポリシーおよびそれに関連付けられるインターフェイスに従って VLAN のポート メンバーシップを指定することは、管理者が担当します。

また、管理者は、デバイスによって維持されている音声 VLAN に基づいて音声アプリケーションのネットワーク ポリシーを自動的に生成してアドバタイズするようにデバイスを設定することもできます。デバイスが音声 VLAN を維持する方法の詳細については、自動音声 VLAN に関するセクションを参照してください。

LLDP MED ネットワークポリシーを定義するには、次の手順を実行します。

手順

ステップ 1 [Administration] > [Discovery - LLDP] > [LLDP MED Network Policy] をクリックします。

このページには、作成済みのネットワーク ポリシーが表示されます。

ステップ 2 デバイスによって維持されている音声VLANに基づいて音声アプリケーションのネットワーク ポリシーを自動的に生成してアドバタイズするようにデバイスを設定する場合は、[LLDP-MED Network Policy for Voice Application] で [Auto] を選択します。

（注）
このボックスがオンの場合、手動で音声ネットワーク ポリシーを設定できません。

ステップ 3 [Apply] をクリックし、この設定を実行コンフィギュレーション ファイルに追加します。

ステップ 4 新しいポリシーを定義するには、[Add] をクリックします。

ステップ 5 値を入力します。

- [Network Policy Number]：作成するネットワーク ポリシーの番号を選択します。
- [Application]：定義されるネットワーク ポリシーの対象となるアプリケーションのタイプ（トラフィックのタイプ）を選択します。
- [VLAN ID]：トラフィックの宛先 VLAN ID を入力します。（範囲 0 ～ 4095）
- [VLAN Type]：トラフィックをタグ付きにするかタグなしにするかを選択します。
- [User Priority]：このネットワーク ポリシーで設定したトラフィックに適 用するプライオリティを選択します。これは CoS 値です。
- [DSCP Value]：ネイバーから送信されるアプリケーションデータに割り当てるDSCP値を選択します。この値により、ネイバーからデバイスに送信するアプリケーション トラフィックにマークする方法をネイバーに通知できます。

ステップ 6 [Apply] をクリックします。ネットワーク ポリシーが定義されます。

（注）
[LLDP MED Port Settings] ページを使用して、発信 LLDP パケットに必要な手動定義ネットワーク ポリシーを含めるようにインターフェイスを手動で設定する必要があります。

LLDP MEDポート設定

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

[LLDP MED Port Settings] ページでは、LLDP-MED TLV の設定を有効にします。ネットワーク ポリシーは、[LLDP MED Network Policy] ページを使用して設定します。

（注） [LLDP-MED Network Policy for Voice Application] が [Auto] で、自動音声 VLAN が動作している場合、デバイスは、すべてのLLDPポートについて、音声アプリケーションのLLDP-MEDネットワークポリシーを自動的に生成します。LLDP-MEDは有効で、音声VLANのメンバーです。

各ポートで LLDP MED を設定するには、次の手順を実行します。

手順

ステップ 1 [Administration] > [Discovery - LLDP] > [LLDP MED Port Settings] をクリックします。

ステップ 2 ページ上部のメッセージは、音声アプリケーションのLLDP MEDネットワークポリシーが自動的に生成されるかどうかを示しています。モードを変更するリンクをクリックします。

ステップ 3 追加の LLDP MED TLV や 1 つ以上のユーザ定義 LLDP MED ネットワーク ポリシーをポートに関連付けるには、目的のものを選択して、[Edit] をクリックします。

ステップ 4 パラメータを入力します。

- [Interface]：設定するインターフェイスを選択します。
- [LLDP MED Status]：このポート上で LLDP-MED を有効にするか無効にするかを選択します。
- [SNMP Notification]：MED をサポートするエンドステーションが検出されたときに、ポートごとに SNMP 通知を送信するかどうかを選択します。
- [Selected Optional TLVs]：デバイスが発行できる TLV を選択するには、目的の TLV を [Available Optional TLVs] リストから [Selected Optional TLVs] リストに移動させます。
- [Selected Network Policies]：LLDP が発行する LLDP MED ポリシーを選択するには、目的のポリシーを [Available Network Policies] リストから [Selected Network Policies] リストに移動させます。1 つ以上のユーザー定義のネットワークポリシーをアドバタイズメントに含めるには、[Available Optional TLVs] から [Network Policy] を選択する必要があります。

  （注）
  次のフィールドの値は、LLDP-MED 規格（ANSI-TIA-1057_final_for_publication.pdf）で定義されているデータ形式に従い、16 進数で正確に入力する必要があります。

  - [Location Coordinate]：LLDP を使用して送信する座標を入力します。
  - [Location Civic Address]：LLDP を使用して送信する住所を入力します。
  - [Location ECS ELIN]：LLDP を使用して発行する緊急通報サービス（ECS）の ELIN ロケーションを入力します。

ステップ 5 [Apply] をクリックします。LLDP MED ポート設定は、実行コンフィギュレーション ファイルに書き込まれます。

ステップ 6 [LLDP Local Information Detail] をクリックして、LLDP ローカル情報を表示します。

LLDPポートステータス

[LLDP Port Status] ページには、各ポートの LLDP グローバル情報が表示されます。

手順

ステップ 1 LLDP ポート ステータスを表示するには、[Administration] > [Discovery - LLDP] > [LLDP Port Status] をクリックします。

すべてのポートの情報が表示されます。

ステップ 2 特定のポートに送信される LLDP および LLDP-MED の TLV の詳細情報を表示するには、ポートを選択して、[LLDP Local Information Detail] をクリックします。

ステップ 3 特定のポートから受信する LLDP および LLDP-MED の TLV の詳細情報を表示するには、ポートを選択して、[LLDP Neighbor Information Detail] をクリックします。

LLDP ポート ステータス グローバル情報

- [Chassis ID Subtype]：シャーシ ID のタイプ（例：MAC アドレス）。
- [Chassis ID]：シャーシの ID。シャーシ ID サブタイプが MAC アドレスである場合、デバイスの MAC アドレスが表示されます。
- [System Name]：デバイスの名前。
- [System Description]：デバイスの説明（英数字形式）。
- [Supported System Capabilities]：スイッチでサポートされている主要機能（例：ブリッジ、WLAN AP、ルータ）。
- [Enabled System Capabilities]：スイッチで有効になっている主要機能。
- [Port ID Subtype]：表示されるポート ID のタイプ。

LLDP ポート ステータス テーブル

- [Interface]：ポート ID。
- [LLDP Status]：有効または無効。
- [LLDP MED Status]：有効または無効。
- [Local PoE ((Power Type, Power Source, Power Priority, Power Value)]：アドバタイズされるローカル PoE 情報。
- [Remote PoE (Power Type, Power Source, Power Priority, Power Value)]：ネイバーによってアドバタイズされる PoE 情報。

- [# of neighbors]：検出されたネイバーの数。
- [Neighbor capability of 1st device]：ネイバーの主要機能（ブリッジ、ルータなど）が表示されます。

LLDPローカル情報

ポートからアドバタイズされているLLDPローカルポートステータスを表示するには、次のようにします。

手順

ステップ1 [Administration] > [Discovery - LLDP] > [LLDP Local Information] をクリックします。

ステップ2 LLDP ローカル情報を表示するインターフェイスを選択します。

[LLDP Local Information] ページには、次のフィールドが含まれています。

[Global]

- [Chassis ID Subtype]：シャーシ ID のタイプ。（MAC アドレスなど）。
- [Chassis ID]：シャーシの ID。シャーシ ID サブタイプが MAC アドレスである場合、デバイスの MAC アドレスが表示されます。
- [System Name]：デバイスの名前。
- [System Description]：デバイスの説明（英数字形式）。
- [Supported System Capabilities]：スイッチでサポートされている主要機能（例：ブリッジ、WLAN AP、ルータ）。
- [Enabled System Capabilities]：スイッチで有効になっている主要機能。
- [Port ID Subtype]：表示されるポート ID のタイプ。
- [ポート ID]：ポートの ID。
- [Port Description]：ポートに関する情報（例：製造元、製品名、ハードウェア バージョン、ソフトウェア バージョン）。

[Management Address]

- [IPv4 Address]：管理用途に最も適した IPv4 戻りアドレス。
- [IPv6 Global Address]：管理用途に最も適した IPv6 戻りグローバル アドレス。
- [IPv6 Link Local Address]：管理用途に最も適した IPv6 戻りリンク ローカル アドレス。

[MAC/PHY Details]

- [自動ネゴシエーション対応] : ポート速度のオートネゴシエーションがサポートされ ているかどうか。表示される値は [True] または [False] です。
- [自動ネゴシエーション有効] : ポート速度のオートネゴシエーションが有効になっているかどうか。表示される値は [True] または [False] です。
- [自動ネゴシエーションアドバタイズ機能] : オートネゴシエーションが可能なポート 速度のタイプ（例：1000BASE-T 半二重モード、100BASE-TX 全二重モード）。
- [動作 MAU タイプ] : Medium Attachment Unit（MAU）のタイプ。MAU では物理層の機能が実行されます。たとえば、イーサネット インターフェイスのコリジョン検出から入ってきたデータに対するデジタル データ変換、ネットワーク（100BASE-TX 全二重モードなど）へのビット挿入などの処理が実行されます。

[802.3 Details]

- [802.3 Maximum Frame Size] : サポートされている IEEE 802.3 フレームサイズの最大値。

[802.3 Link Aggregation]

- [Aggregation Capability] : インターフェイスを集約できるかどうか。
- [Aggregation Status] : 現在、インターフェイスが集約されているかどうか。
- [Aggregation Port ID] : アドバタイズされている集約インターフェイス ID。

[802.3 Energy Efficient Ethernet (EEE)]

- [Local Tx] : リモートリンクパートナーの Tx 値に対するローカルリンクパートナーのリフレクションを示します。
- [Local Rx] : リモートリンクパートナーの Rx 値に対するローカルリンクパートナーのリフレクションを示します。
- [Remote Tx Echo] : 低電力アイドル（LPI モード）を抜けた後、データの送信を開始するまで、送信リンクパートナーが待機する時間（単位：マイクロ秒）を示します。
- [Remote Rx Echo] : 受信リンクパートナーが要求する、低電力アイドル（LPI モード）後にデータを送信するまでに、送信リンクパートナーが待機する時間（単位：マイクロ秒）を示します。

[802.3 Power via MDI]

- [MDI 電源対応ポートクラス] : アドバタイズされている電力サポート ポート クラス。
- [PSE MDI 電源対応] : ポートで MDI 電力がサポートされているかどうか。
- [PSE MDI 電源状態] : ポートで MDI 電力が有効になっているかどうか。
- [PSE 電源ペア制御機能] : ポートで電力線制御がサポートされているかどうか。
- [PSE 電源ペア] : ポートで電力線制御タイプがサポートされているかどうか。
- [PSE 電力クラス] : アドバタイズされている、ポートの電力クラス。
- [電源タイプ] : ポートに接続されたポッド デバイスのタイプ。

- [Power Source]：ポートの電源。
- [Power Priority]：ポートの電力のプライオリティ。
- [PD Requested Power Value]：PSE から PD に割り当てられた電力量。
- [PSE Allocated Power Value]：給電側機器（PSE）に割り当てられた電力量。

[4-Wire Power via MDI]

- [4-Pair PoE Supported]：システムとポートが 4 ペア線の有効化をサポートしていることを示します（この HW 能力を持っている特定のポートにのみ当てはまる）。
- [Spare Pair Detection/Classification Required]：4 ペア線が必要であることを示します。
- [PD Spare Pair Desired State]：POD デバイスが 4 ペア能力を有効にするように要求していることを示します。
- [PD Spare Pair Operational State]：4 ペア能力が有効か無効かを示します。

[MED Details]

- [サポートされている機能]：ポート上で有効になっている MED 機能。
- [現在の機能]：ポートからアドバタイズされている MED TLV。
- [デバイスクラス]：LLDP-MED エンドポイント デバイス クラス。表示されるデバイス クラスは次のとおりです。
  - [Endpoint Class 1]：汎用エンドポイント クラス（基本的な LLDP サービスを提供）を示します。
  - [Endpoint Class 2]：メディア エンドポイント クラス（クラス 1 のすべての機能に加え、メディア ストリーミング機能を提供）を示します。
  - [Endpoint Class 3]：通信デバイス クラス（クラス 1 およびクラス 2 のすべての機能に加え、場所、911、レイヤ 2 スイッチ サポート、およびデバイス情報管理の各機能を提供）を示します。

[Extended PSE Information]

- [PoE デバイスタイプ]：ポートの PoE タイプ（PD/PSE など）。
- [PoE 電源]：ポートの電源。
- [PoE 電力プライオリティ]：ポートの電力のプライオリティ。
- [PoE Power Value]：ポートの電力の値。

[Inventory Information]

- [ハードウェアリビジョン]：ハードウェアのバージョン。
- [ファームウェアリビジョン]：ファームウェアのバージョン。
- [ソフトウェアリビジョン]：ソフトウェアのバージョン。
- [シリアル番号]：デバイスのシリアル番号。

- [製造業者名]：デバイスの製造元名。
- [モデル名]：デバイスのモデル名。
- [Asset ID]：アセット ID。

[Location Information]

ANSI-TIA-1057 規格の 10.2.4 項に従って、次のデータ構造を 16 進数で入力します。

- [住所]：住所。
- [座標]：位置マップ座標（緯度、経度、および標高）。
- [ECS ELIN]：デバイスの ECS の ELIN。

[Network Policy Table]

- [Application Type]：ネットワーク ポリシーのアプリケーション タイプ（例：音声）。
- [VLAN ID]：ネットワーク ポリシーがバインドされている VLAN の ID。
- [VLAN Type]：ネットワーク ポリシーがバインドされている VLAN のタイプ（タ グ付きまたはタグなし）。
- [User Priority]：ネットワーク ポリシーのユーザー プライオリティ。
- [DSCP]：ネットワーク ポリシーの DSCP。

LLDPネイバー情報

[LLDP Neighbor Information] ページには、ネイバーデバイスから受信した情報が表示されます。タイムアウト（ネイバーから受信した値（ネイバーから LLDP PDU を受信しなかったパケット存続時間 TLV の値）に基づく）後に、情報が削除されます。

LLDP ネイバー情報を表示するには、次の手順を実行します。

手順

ステップ 1 [Administration] > [Discovery - LLDP] > [LLDP Neighbor Information] をクリックします。

ステップ 2 LLDP ネイバー情報を表示するインターフェイスを選択します。

このページには、選択したインターフェイスに関する次のフィールドが表示されます。

- [ローカルポート]：ネイバーが接続されているローカル ポートの番号。
- [シャーシ ID サブタイプ]：シャーシ ID のタイプ（例：MAC アドレス）。
- [シャーシ ID]：802 LAN 近隣デバイスのシャーシの ID。

- [Port ID Subtype]：表示されるポート ID のタイプ。
- [ポート ID]：ポートの ID。
- [システム名]：発行されたデバイスの名前。
- [存続可能時間]：タイムアウト時間（単位：秒）。この時間内にこのネイバーからLLDP PDU が 1 件も受信されなかった場合、このネイバーの情報は削除されます。

ステップ 3 ローカル ポートを選択し、[Details] をクリックします。

[LLDP Neighbor Information] ページには、次のフィールドが含まれています。

[Port Details]

- [ローカルポート]：ポート番号。
- [MSAP エントリ]：デバイスの Media Service Access Point（MSAP）エントリ 番号。

[Basic Details]

- [シャーシ ID サブタイプ]：シャーシ ID のタイプ（例：MAC アドレス）。
- [シャーシ ID]：802 LAN 近隣デバイスのシャーシの ID。
- [Port ID Subtype]：表示されるポート ID のタイプ。
- [ポート ID]：ポートの ID。
- [Port Description]：ポートに関する情報（例：製造元、製品名、ハードウェア バージョン、ソフトウェア バージョン）。
- [システム名]：公開されているシステム名。
- [システムの説明]：ネットワーク エンティティの説明（英数字）。これには、システムの名前と、このデバイスでサポートされているハードウェア、オペレーティング システム、およびネットワーキング ソフトウェアのバージョンが含まれます。値は、sysDescr オブジェクトと同一です。
- [サポートされているシステム機能]：このデバイスでサポートされている主要機能。機能は 2 オクテットで示されます。ビット 0 ～ 7 はそれぞれ、その他、リピータ、ブリッジ、WLAN AP、ルータ、電話、DOCSIS ケーブル デバイス、およびステーションを示します。ビット 8 ～ 15 は予約されています。
- [有効なシステム機能]：スイッチで有効になっている主要機能。

[Management Address Table]

- [アドレスサブタイプ]：管理アドレスのサブタイプ（MAC、IPv4 など）。
- [アドレス]：管理アドレス。
- [インターフェイスサブタイプ]：ポートのサブタイプ。
- [インターフェイス番号]：ポート番号。

[MAC/PHY Details]

- [自動ネゴシエーション対応] : ポート速度のオートネゴシエーションがサポートされ ているかどうか。表示される値は [True] または [False] です。
- [自動ネゴシエーション有効] : ポート速度のオートネゴシエーションが有効になっているかどうか。表示される値は [True] または [False] です。
- [自動ネゴシエーションアドバタイズ機能] : オートネゴシエーションが可能なポート 速度のタイプ（例：1000BASE-T 半二重モード、100BASE-TX 全二重モード）。
- [動作 MAU タイプ] : Medium Attachment Unit（MAU）のタイプ。MAU では物理層の機能が実行されます。たとえば、イーサネットインターフェイスのコリジョン検出から入ってきたデータに対するデジタル データ変換、ネットワーク（100BASE-TX 全二重モードなど）へのビット挿入などの処理が実行されます。

[802.3 Power via MDI]

- [MDI 電源対応ポートクラス] : アドバタイズされている電力サポート ポート クラス。
- [PSE MDI 電源対応] : ポートで MDI 電力がサポートされているかどうか。
- [PSE MDI 電源状態] : ポートで MDI 電力が有効になっているかどうか。
- [PSE 電源ペア制御機能] : ポートで電力線制御がサポートされているかどうか。
- [PSE 電源ペア] : ポートで電力線制御タイプがサポートされているかどうか。
- [PSE 電力クラス] : アドバタイズされている、ポートの電力クラス。
- [電源タイプ] : ポートに接続されたポッド デバイスのタイプ。
- [電源] : ポートの電源。
- [電源優先度] : ポートの電源の優先順位。
- [PD 要求電力値] : POD デバイスから要求された電力量。
- [PSE 割り当て電力値] : PSE から PD に割り当てられた電力量。

[4-Wire Power via MDI]

- [4-Pair PoE Supported] : システムとポートが 4 ペア線の有効化をサポートしていることを示します（この HW 能力を持っている特定のポートにのみ当てはまる）。
- [Spare Pair Detection/Classification Required] : 4 ペア線が必要であることを示します。
- [PD Spare Pair Desired State] : POD デバイスが 4 ペア能力を有効にするように要求していることを示します。
- [PD Spare Pair Operational State] : 4 ペア能力が有効か無効かを示します。

[802.3 Details]

- [802.3 最大フレームサイズ] : アドバタイズされている、ポートの最大フレーム サ イズ。

[802.3 Link Aggregation]

- [アグリゲーション機能] : ポートを集約できるかどうか。
- [アグリゲーションステータス] : 現在、ポートが集約されているかどうか。
- [アグリゲーションポート ID] : アドバタイズされている集約ポート ID。

[802.3 Energy Efficient Ethernet (EEE)]

- [Remote Tx] : 低電力アイドル（LPI モード）を抜けてからデータ送信を開始するまでに送信リンク パートナーが待機する時間（マイクロ秒単位）。
- [Remote Rx] : 受信リンク パートナーが要求する、低電力アイドル（LPI モード）を抜けてからデータ送信を開始するまでに送信リンク パートナーが待機する時間（マイクロ秒単位）。
- [Local Tx Echo] : リモート リンク パートナーの Tx 値に対するローカル リンク パートナーのリフレクションを示します。
- [Local Rx Echo] : リモート リンク パートナーの Rx 値に対するローカル リンク パートナーのリフレクションを示します。

[MED Details]

- [サポートされている機能] : ポート上で有効になっている MED 機能。
- [現在の機能] : ポートからアドバタイズされている MED TLV。
- [デバイスクラス] : LLDP-MED エンドポイント デバイス クラス。表示されるデバイス クラスは次のとおりです。
  - [Endpoint Class 1] : 汎用エンドポイント クラス（基本的な LLDP サービスを提供）を示します。
  - [Endpoint Class 2] : メディア エンドポイント クラス（クラス 1 のすべての機能に加え、メディア ストリーミング機能を提供）を示します。
  - [Endpoint Class 3] : 通信デバイス クラス（クラス 1 およびクラス 2 のすべての機能に加え、場所、911、レイヤ 2 スイッチ サポート、およびデバイス情報管理の各機能を提供）を示します。
- [PoE デバイスタイプ] : ポートの PoE タイプ（PD/PSE など）。
- [PoE 電源] : ポートの電源。
- [PoE 電力プライオリティ] : ポートの電力のプライオリティ。
- [PoE Power Value] : ポートの電力の値。
- [ハードウェアリビジョン] : ハードウェアのバージョン。
- [ファームウェアリビジョン] : ファームウェアのバージョン。
- [ソフトウェアリビジョン] : ソフトウェアのバージョン。
- [シリアル番号] : デバイスのシリアル番号。
- [製造業者名] : デバイスの製造元名。

- [モデル名]：デバイスのモデル名。
- [Asset ID]：アセット ID。

[802.1 VLAN and Protocol]

- [PVID]：アドバタイズされている、ポートの VLAN ID。

[PPVID Table]

- [VID]：プロトコルの VLAN ID。
- [サポート済み]：サポートされている、ポートとプロトコルの VLAN ID。
- [有効]：有効になっている、ポートとプロトコルの VLAN ID。

[VLAN ID Table]

- [VID]：ポートとプロトコルの VLAN ID。
- [VLAN Name]：アドバタイズされている VLAN 名。

[Protocol ID Table]

- [Protocol ID]：アドバタイズされているプロトコル ID。

[Location Information]

ANSI-TIA-1057 規格の 10.2.4 項に従って、次のデータ構造を 16 進数で入力します。

- [住所]：住所。
- [座標]：位置マップ座標（緯度、経度、および標高）。
- [ECS ELIN]：デバイスの ECS の ELIN。
- [不明]：位置情報不明。

[Network Policy Table]

- [Application Type]：ネットワーク ポリシーのアプリケーション タイプ（例：音声）。
- [VLAN ID]：ネットワーク ポリシーがバインドされている VLAN の ID。
- [VLAN Type]：ネットワーク ポリシーがバインドされている VLAN のタイプ（タ グ付きまたはタグなし）。
- [User Priority]：ネットワーク ポリシーのユーザー プライオリティ。
- [DSCP]：ネットワーク ポリシーの DSCP。

ステップ 4 [LLDP Neighbor Table] のデータをフィルタ処理するには、[Filter] をオンにして、ドロップダウンリストからローカルポートを選択します。次に、[Go] をクリックして、選択したポートを表示します。

ステップ 5 [LLDP Neighbor Table] からポートを削除するには、ポートを選択して削除アイコンをクリックします。

LLDP の統計情報

[LLDP Statistics] ページには、ポートごとの LLDP 統計情報が表示されます。

LLDP 統計情報を表示するには、次の手順を実行します。

手順

ステップ 1 [Administration] > [Discovery - LLDP] > [LLDP Statistics] をクリックします。

各ポートについて、次のフィールドが表示されます。

- [Interface]：インターフェイス ID。
- [Tx Frames (Total)]：送信されたフレームの数。
- Rx フレーム
  - [Total]：受信したフレームの合計数。
  - [Discarded]：受信したフレームのうち、廃棄されたフレームの数。
  - [Errors]：受信したフレームのうち、エラーになったフレームの数。
- [Rx TLVs]
  - [Discarded]：受信した TLV のうち、廃棄された TLV の数。
  - [Unrecognized]：受信した TLV のうち、認識されなかった TLV の数。
- [Neighbor's Information Deletion Count]：このインターフェイスでネイバーがエージアウトされた回数。

ステップ 2 最新の統計情報を表示するには、[Refresh] をクリックします。

LLDP過負荷

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

LLDP では、情報が LLDP TLV および LLDP-MEDTLV として LLDP パケットに追加されます。LLDP 過負荷は、LLDP パケット内の総情報量がインターフェイスでサポートされている最大 PDU サイズを超えたときに発生します。

[LLDP Overloading] ページには、LLDP/LLDP-MED 情報のバイト数、使用可能なバイト数、および各インターフェイスの過負荷ステータスが表示されます。

LLDP 過負荷情報を表示するには、次の手順に従います。

手順

ステップ 1 [Administration] > [Discovery - LLDP] > [LLDP Overloading] をクリックします。

LLDP 過負荷テーブルでは、各ポートについて次の情報が表示されます。

- [Interface]：ポート ID。
- [Total Bytes In-Use]：各パケットの LLDP 情報の合計バイト数。
- [Available Bytes Left]：各パケットで追加の LLDP 情報用に残っている利用可能な合計バイト数。
- [Status]：TLV が送信されているか、それとも過負荷状態になっているか。

ステップ 2 特定のポートの過負荷状態を詳細表示するには、そのポートを選択して [Details] をクリックします。

このページには、ポートで送信された各 TLV に関する次の情報が表示されます。

- [Interface]：ドロップダウンリストからインターフェイスを選択します。
- [LLDP Mandatory TLVs]
  - [Size (Bytes)]：必須 TLV の合計バイト数。
  - [Status]：必須 TLV グループが送信されているか、それとも過負荷状態に なっているか。
- [LLDP MED Capabilities]
  - [Size (Bytes)]：LLDP MED 機能パケットの合計バイト数。
  - [Status]：LLDP MED 機能パケットが送信されたかかどうか、または過負荷状態であったかどうかが示されます。
- [LLDP MED Location]
  - [Size (Bytes)]：LLDP MED 位置パケットの合計バイト数。
  - [Status]：LLDP MED 位置パケットが送信されたかかどうか、または過負荷状態であったかどうかが示されます。
- [LLDP MED Network Policy]
  - [Size (Bytes)]：LLDP MED ネットワーク ポリシー パケットの合計バイト数。
  - [Status]：LLDP MED ネットワーク ポリシー パケットが送信されたかかどうか、または過負荷状態であったかどうかが示されます。
- [LLDP MED Extended Power via MDI]
  - [Size (Bytes)]：LLDP MED 拡張 Power via MDI パケットの合計バイト サイズ。
  - [Status]：LLDP MED 拡張 Power via MDI パケットが送信されたかかどうか、または過負荷状態であったかどうかが示されます。

- [802.1 TLV]
  - [Size (Bytes)]：LLDP MED 802.1 TLV パケットの合計バイト サイズ。
  - [Status]：LLDP MED 802.1 TLV パケットが送信されたかかどうか、または過負荷状態であったかどうかが示されます。
- [802.3 TLVs]
  - [Size (Bytes)]：LLDP MED 802.3 TLV パケットの合計バイト サイズ。
  - [Status]：LLDP MED 802.3 TLV パケットが送信されたかかどうか、または過負荷状態であったかどうかが示されます。
- [LLDP Optional TLVs]
  - [Size (Bytes)]：LLDP MED オプション TLV パケットの合計バイト サイズ。
  - [Status]：LLDP MED オプション TLV パケットが送信されたかかどうか、または過負荷状態であったかどうかが示されます。
- [LLDP MED Inventory]
  - [Size (Bytes)]：LLDP MED インベントリ TLV パケットの合計バイト サイズ。
  - [Status]：LLDP MED インベントリ パケットが送信されたかかどうか、または過負荷状態であったかどうかが示されます。
- Total
  - [Total (Bytes)]：各パケットの LLDP 情報の合計バイト数。
  - [Available Bytes Left]：各パケットで追加の LLDP 情報用に未送信のまま残っている利用可能な合計バイト数。

ディスカバリ - CDP

Cisco Discovery Protocol は、メディア独立型かつネットワーク独立型のレイヤ 2 プロトコルであり、ネットワーキングアプリケーションで、直接接続された付近のデバイスに関して学習するために使用されます。Cisco Discovery Protocol はデフォルトでイネーブルになっています。Cisco Discovery Protocol 用に設定された各デバイスは、メッセージを受信できるアドレスを 1 つ以上アドバタイズし、定期的なアドバタイズメント（メッセージ）を既知のマルチキャストアドレス 01:00:0C:CC:CC:CC に送信します。デバイスは、このアドレスをリッスンすることによって相互に検出します。また、メッセージをリッスンすることにより、他のデバイス上のインターフェイスがアップまたはダウン状態になった時期を認識します。

アドバタイズメントには、存続可能時間情報が含まれます。この情報は、受信デバイスが Cisco Discovery Protocol 情報を廃棄するまでの保持時間の長さを示します。デフォルトで、シスコ ソ

フトウェアでサポートされている設定済みアドバタイズメントは、サブネットワーク アクセス プロトコル（SNAP）ヘッダーをサポートするインターフェイス上で 60 秒ごとに送信されます。シスコ デバイスは、Cisco Discovery Protocol パケットを転送しません。Cisco Discovery Protocol をサポートしているシスコ デバイスは、受信した情報をテーブルに保存します。このテーブル内の情報はアドバタイズメントを受信するたびに更新されます。また、アドバタイズメントの送信に 3 回失敗したデバイスに関する情報は廃棄されます。

ここでは、CDP の設定方法について説明します。

プロパティ

LLDP と同様に、Cisco Discovery Protocol（CDP）は、直接接続されたネイバーが自身とそれぞれの機能を互いにアドバタイズするためのリンク層プロトコルです。LLDP とは異なり、CDP はシスコ独自のプロトコルです。CDP プロパティを設定するには、次の手順を実行します。

手順

ステップ 1 [Administration] > [Discovery - CDP] > [Properties] をクリックします。

ステップ 2 パラメータを入力します。

CDP Status	選択するとデバイス上の CDP が有効になります。
CDPフレーム処理	CDP が有効でない場合は、選択した基準に一致するパケットを受信したときに実行する処理を次の中から選択します。 • [Bridging]：VLAN に基づいてパケットを転送 • [Filtering]：パケットを削除 • [Flooding]：入力ポートを除くすべてのポートに着信 CDP パケットを転送する VLAN 非対応のフラッディング。
CDP音声VLANアドバタイズメント	選択すると、CDP が有効で、音声 VLAN のメンバーであるすべてのポートで、デバイスが CDP を使用して音声 VLAN をアドバタイズできるようになります。音声 VLAN の設定については、プロパティを参照してください。
CDP必須TLVの検証	選択すると、必須 TLV を含まない着信 CDP パケットは廃棄され、無効エラーカウンタが増加します。
CDPバージョン	使用する CDP のバージョンを選択します。

CDP保留時間	CDP パケットを廃棄するまで待機する時間を、[TLV Advertise Interval] の値の倍数で測定します。たとえば、[TLV Advertise Interval] の値が 30 秒であり、Hold Multiplier] の値が 4 である場合、LLDP パケットは 120 秒後に破棄されます。次のオプションがあります。 • [デフォルトを使用] : デフォルトの時間（180 秒）を使用します。 • [ユーザー定義] : 時間を入力します（単位：秒）。
CDP転送速度	CDPアドバタイズメント更新データの送信間隔を秒単位で入力します。次のオプションがあります。 • [デフォルトを使用] : デフォルト レート（60 秒）を使用します。 • [ユーザー定義] : レートを入力します（単位：秒）。
デバイスID形式	デバイス ID の形式を選択します（MAC アドレスまたはシリアル番号）。次のオプションがあります。 • [Mac Address] : デバイスの MAC アドレスをデバイス ID として使用します。 • [Serial Number] : デバイスのシリアル番号をデバイス ID として使用します。 • [Hostname] : デバイスのホスト名をデバイス ID として使用します。
送信元インターフェイス	フレームの TLV で使用される IP アドレス。次のオプションがあります。 • [デフォルトを使用] : 発信インターフェイスの IP アドレスを使用します。 • [ユーザー定義] : アドレス TLV 内のインターフェイス（[インターフェイス] フィー ルド）の IP アドレスを使用します。
インターフェイス	[Source Interface] で [User Defined] が選択された場合は、インターフェイスを選択します。
Syslog音声VLAN不一致	オンにすると、音声 VLAN の不一致が検出されたときに SYSLOG メッセージが送信されます。これは、着信フレーム内の音声 VLAN 情報が、ローカル デバイスがアドバタイズしている情報と一致していないことを示しています。
SyslogネイティブVLAN不一致	オンにすると、ネイティブ VLAN の不一致が検出されたときに SYSLOG メッセージが送信されます。これは、着信フレーム内のネイティブ VLAN 情報が、ローカルデバイスがアドバタイズしている情報と一致していないことを示しています。
Syslogデュプレックス不一致	オンにすると、デュプレックス情報が一致しないときに SYSLOG メッセージが送信されます。これは、着信フレーム内のデュプレックス情報が、ローカル デバイスがアドバタイズしている情報と一致していないことを示しています。

ステップ 3 [Apply] をクリックします。LLDP のプロパティが定義されます。

インターフェイスの設定

（注） この設定は、[Advanced Mode] ビューでのみ使用できます。

[Interface Settings] ページでは、ポートごとに CDP の有効/無効を設定できます。これらのプロパティ値を設定することにより、LLDP プロトコル対応デバイスに送信する情報のタイプを選択できます。

アドバタイズする LLDP-MED TLV は、LLDP MEDポート設定 （52 ページ）で選択できます。

CDP インターフェイス設定を定義するには、次の手順に従います。

手順

ステップ 1 [Administration] > [Discovery - CDP] > [Interface Settings] をクリックします。

このページには、各インターフェイスの次の CDP 情報が表示されます。

- [Entry No.]：CDP エントリ。
- [Interface]：CDP エントリに使用されるインターフェイス。
- [CDP Status]：ポートに対する CDP 発行オプション。
- [Reporting Conflicts with CDP Neighbors]：[Edit] ページで有効/無効になっているレポート オプション（音声 VLAN/ネイティブ VLAN/デュプレックス）のステータス。
- [No. of Neighbors]：検出されたネイバーの数。

  ページ下部に次の 4 つのボタンがあります。
- [Copy Settings]：選択すると、ポート間でコンフィギュレーションがコピーされます。
- [Edit]：フィールドは後述のステップ 2 で説明されています。
- [CDP Local Information Details]：CDPローカル情報 （69 ページ）に移動します。
- [CDP Neighbor Information Details]：CDP ネイバー情報 （71 ページ）に移動します。

ステップ 2 ポートを選択して [Edit] をクリックします。

このページには、次のフィールドがあります。

- [インターフェイス]：定義するインターフェイスを選択します。
- [CDP ステータス]：ポートで CDP を有効または無効にします。

（注）
次の 3 つのフィールドは、デバイスが管理ステーションにトラップを送信するように設定されている場合のオプションです。

- [Syslog Voice VLAN Mismatch]：選択すると、音声 VLAN の不一致が検出されたときに SYSLOG メッセージが送信されます。これは、着信フレーム内の音声 VLAN 情報が、ローカルデバイスがアドバタイズしている情報と一致していないことを示しています。
- [Syslog Native VLAN Mismatch]：選択すると、ネイティブ VLAN の不一致が検出されたときに SYSLOG メッセージが送信されます。これは、着信フレーム内のネイティブ VLAN 情報が、ローカルデバイスがアドバタイズしている情報と一致していないことを示しています。
- [Syslog Duplex Mismatch]：選択すると、デュプレックス情報の不一致が検出されたときに SYSLOG メッセージが送信されます。これは、着信フレーム内のデュプレックス情報が、ローカルデバイスがアドバタイズしている情報と一致していないことを示しています。

ステップ 3 関連情報を入力し、[Apply] をクリックします。ポート設定は、実行コンフィギュレーションに書き込まれます。

CDPローカル情報

ローカルデバイスに関して CDP プロトコルによってアドバタイズされる情報を表示するには、次の手順に従います。

手順

[Administration] > [Discovery - CDP] > [CDP Local Information] の順にクリックします。次のフィールドが表示されます。

Interface	ローカルポート数。
CDP State	CDP が有効かどうかを表示します。
Device ID TLV	• [Device ID Type]：デバイス ID TLV でアドバタイズされるデバイス ID のタイプ。 • [Device ID]：デバイス ID TLV でアドバタイズされるデバイス ID。
System Name TLV	[System Name TLV]：デバイスのシステム名。
Address TLV	[Address1-3]：デバイス アドレス TLV でアドバタイズされる IP アドレス。
[Port TLV]	[Port ID]：ポート TLV でアドバタイズされるポートの ID。
Capabilities TLV	[Capabilities]：ポート TLV でアドバタイズされる機能。

Version TLV	[Version]：デバイスが稼動しているソフトウェアのリリースに関する情報。
Platform TLV	[Platform]：プラットフォーム TLV でアドバタイズされるプラットフォー ムの ID。
Native VLAN TLV	[Native VLAN TLV]：ネイティブ VLAN TLV でアドバタイズされるネイティブ VLAN ID。
Full/Half Duplex TLV	[Duplex]：全二重 TLV または半二重 TLV でアドバタイズされるポートのデュプレックスが半二重か全二重か。
Appliance TLV	• [Appliance ID]：アプライアンス TLV でアドバタイズされる、ポートに接続されたデバイスのタイプ。 • [Appliance VLAN ID]：アプライアンスによって使用されるデバイス上の VLAN。たとえば、アプライアンスが IP 電話の場合は、これは音声 VLAN になります。
Extended Trust TLV	[Extended Trust]：有効になっている場合、ポートが信頼され、受信されたパケットがマーキングされます。この場合、このようなポートで受信されたパケットは、再度マーキングされることはありません。無効な場合は、ポートが信頼できないことを示しています。この場合、次のフィールドが該当します。
CoS for Untrusted Ports TLV	[CoS for Untrusted Ports]：ポートの [Extended Trust] が無効な場合、このフィールドにはレイヤ 2 CoS 値、つまり 802.1D/802.1p プライオリティ値が表示されます。これは、信頼できないポートで受信されたすべてのパケットに、デバイスが再度マーキングする CoS 値です。
Power Available TLV	• [Request ID]：最新の電力要求 ID が、電力要求 TLV で最後に受信した [要求 ID] フィール ドに反映されます。インターフェイスが最後にアップした時点以降に電力要求 TLV を受信しなかった場合は、0 になります。 • [Power Management ID]：次のイベントのいずれかが発生するたびに、値が 1（または、0 を避けるため 2）増加します。 [Available Power] または [Management Power Level] が変化した。 最後に受信した設定値と異なる要求 ID を持つ電力要求 TLV を受信した。 インターフェイスがダウンした。 • [Available Power]：ポートが消費する電力量。 • [Management Power Level]：電力消費量 TLV についての、POD デバイスに対するサプライヤの要求が表示されます。デバイスはこのフィールドに常に [No Preference] と表示します。

4-Wire Power via MDI (UPOE) TLV）	この TLV がサポートされているかどうかが表示されます。 • [4-Pair PoE Supported]：PoE がサポートされているかどうかが表示されます。 • [Spare Pair Detection/Classification Required]：この分類が必要かどうかが表示されます。 • [PD Spare Pair Desired State]：PD 予備ペアが必要な状態が表示されます。 • [PD Spare Pair Operational State]：PSE 予備ペアの状態が表示されます。

CDP ネイバー情報

[CDP Neighbors Information] ページには、ネイバー デバイスから受信した CDP 情報が表示されます。

タイムアウトになると、情報は削除されます。タイムアウトは、CDP PDU が 1 件も受信されなかった場合、存続可能時間 TLV から取得した値に基づきます。

CDP ネイバー情報を表示するには、次のようにします。

手順

ステップ 1 [Administration] > [Discovery - CDP] > [CDP Neighbor Information] をクリックします。

ステップ 2 新しいインスタンスを開始するには、[Clear Table] をクリックして、CDP ネイバー情報テーブルの以前のデータをクリアします。

ステップ 3 フィルタを選択するには、[Filter] チェックボックスをオンにし、ローカルインターフェイスを選択して、[Go] をクリックします。

リスト上でフィルタが適用されます。[Clear Filter] がアクティブになって、フィルタの停止が有効になります。

[CDP Neighbor Information] ページには、リンク パートナー（ネイバー）に関する次のフィールドが表示されます。

Device ID	ネイバーデバイス ID。
System Name	ネイバーシステム名。
Local Interface	ネイバーが接続されているローカルポートの番号。
Advertisement Version	CDP プロトコルのバージョン。
Time to Live (sec)	このネイバーの情報が削除されるまでの時間間隔（単位：秒）。

Capabilities	ネイバーによってアドバタイズされる機能。
Platform	ネイバーのプラットフォーム TLV からの情報。
Neighbor Interface	ネイバーの発信インターフェイス。

ステップ 4 デバイスを選択し、[Details] をクリックします。

このページには、ネイバーに関する次のフィールドが含まれています（実際のフィールドの表示は、ネイバーによるアドバタイズの内容によって異なります）。

Device ID	ネイバーデバイス ID。
System Name	ネイバーシステム名。
Local Interface	ネイバーが接続されているローカルポートの番号。
Advertisement Version	CDP プロトコルのバージョン。
Time to Live	このネイバーの情報が削除されるまでの時間間隔（単位：秒）。
Capabilities	ネイバーによってアドバタイズされる機能。
Platform	ネイバーのプラットフォーム TLV からの情報。
Neighbor Interface	ネイバーの発信インターフェイス。
Native VLAN	ネイバーのネイティブ VLAN。
Application	ネイバーのアプリケーション。
Duplex	ネイバーインターフェイスが半二重か全二重か。
Addresses	ネイバーアドレス。
Power Drawn	インターフェイスでネイバーによって消費される電力量。
Version	ネイバーのソフトウェアのバージョン。
Power Request	ポートに接続された PD によって要求される電力。 • [電力要求リスト]：各 PD は、サポートされる電力レベル（最大 3 つ）からなるリストを送信できます。

4-Wire Power via MDI	• [4-Pair PoE Supported]：システムとポートが 4 ペア線の有効化をサポートしていることを示します。 • [Spare Pair Detection/Classification Required]：4 ペア線が必要であることを示します。 • [PD Spare Pair Desired State]：POD デバイスが 4 ペア能力を有効にするように要求していることを示します。 • [PD 予備ペア動作状態（PD Spare Pair Operational State）]：4 ペア能力が有効か無効かを示します。

（注） [Clear Table] ボタンをクリックすると、CDP からの場合は、接続されていたデバイスがすべて切断され、Auto Smartport が有効な場合は、すべてのポートタイプがデフォルトに変更されます。

CDP統計情報

[CDP Statistics] ページには、ポートとの間で送受信された CDP フレームに関する情報が表示されます。CDP パケットは、スイッチ インターフェイスに接続されたデバイスから受信され、Smartport 機能用に使用されます。

CDP 統計情報を表示するには、次の手順を実行します。

手順

ステップ 1 [Administration] > [Discovery - CDP] > [CDP Statistics] をクリックします。

各インターフェイスについて、次のフィールドが表示されます。

[Packets Received/Packets Transmitted]：

- [Version 1]：受信または送信した CDP バージョン 1 のパケットの数。
- [Version 2]：受信または送信した CDP バージョン 2 のパケットの数。
- [Total]：受信または送信した CDP パケットの合計数。

[CDP Error Statistics]

- [Illegal Checksum]：無効なチェックサム値とともに受信したパケットの数。
- [Other Errors]：無効なチェックサム以外のエラーとともに受信したパケットの数。
- [Neighbors Over Maximum]：空き容量がないためパケット情報をキャッシュに格納できなかった回数。

ステップ 2 すべてのインターフェイスのカウンタを完全にクリアするには、[Clear All Interface Counters] をクリックします。インターフェイス上のすべてのカウンタをクリアするには、選択して [Clear Interface Counters] をクリックします。

デバイスの特定

この機能は、ネットワーク内の特定のデバイスのすべてのネットワーク ポート LED を点滅させて、デバイスの物理的な場所を特定できます。この機能は、相互接続された多数のデバイスがある部屋で1つのデバイスを特定する場合に役立ちます。この機能をアクティブにすると、該当するデバイス上のすべてのネットワーク ポート LED が、設定された期間（デフォルトでは 1 分）点滅します。

手順

ステップ 1 [Administration] > [Locate Device] の順にクリックします。

ステップ 2 次のフィールドに値を入力します。

- [Duration]：ポートの LED を点滅させる時間（秒単位）を入力します。
- [Remaining Time]：このフィールドは、この機能が現在アクティブな場合にのみ表示されます。ここには、LED が点滅する残り時間が表示されます。
- [Unit ID]：このフィールドは、デバイスがスタック構成のときにのみ表示されます。ネットワークポート LED を点滅させるユニットを指定するか、すべてのユニットを対象とする場合は [All] を選択します。

ステップ 3 [Start] をクリックして、機能を開始します。

機能が開始されると [Start] ボタンが [Stop] ボタンに置き換わります。このボタンを使用して、定義されたタイマーが終了する前に LED の点滅を停止できます。

ping

pingユーティリティは、リモートホストに到達できるかどうかをテストし、送信したパケットが往復に要した時間を計測します。

ping は、ICMP（Internet Control Message Protocol）のエコー要求パケットをターゲット ホストに送信して ICMP 応答を待つことによって動作します。ラウンド トリップ時間を計測し、パケット損失がある場合はそれを記録します。

ホストに ping を実行するには、次の手順を実行します。

手順

ステップ 1 [Administration] > [Ping] の順にクリックします。

ステップ 2 次のフィールドに入力して、ping を設定します。

オプション	説明
Host Definition	送信元インターフェイスをIPアドレスで指定するか、名前で指定するかを選択します。このフィールドは、以下に説明するように [Source IP] フィールドに表示されるインターフェイスに影響します。
IP Version	送信元インターフェイスを IP アドレスで識別する場合は、IPv4 または IPv6 を選択し、選択した形式で入力することを示します。
Source IP	宛先との通信用送信元IPv4アドレスとして送信元インターフェイスを選択します。[Host Definition] フィールドに [By Name] を指定した場合、すべての IPv4 および IPv6 アドレスが表示されます。[Host Definition] フィールドに [IP Address] を指定した場合、[IP Version] フィールドで指定したタイプの既存の IP アドレスのみが表示されます。 （注） [Auto] オプションを選択すると、システムは宛先アドレスに基づいて送信元アドレスを計算します。
Destination IPv6 Address Type	次のオプションのいずれかを選択します。 • [Link Local]：IPv6アドレスによって、同一ネットワーク リンク上のホストが一意に識別されます。リンクローカルアドレスのプレフィックス部は FE80 です。このタイプのアドレスはルーティング不能であり、ローカルネットワーク内で通信する場合にのみ使用できます。1 つのリンク ローカル アドレスのみがサポートされます。リンク ローカル アドレスがインターフェイス上に存在する場合、このエントリは構成内のアドレスを置き換えます。 • [Global]：IPv6アドレスは、他のネットワークからも認識かつアクセス可能 なグローバル ユニキャスト IPv6 タイプになります。
Link Local Interface	IPv6 アドレスタイプが [Link Local] である場合は、どこから IPv6 アドレスを受け取るかを選択します。
Destination IP Address/Name	Ping対象デバイスのアドレスまたはホスト名。これがIPアドレスとホスト名のどちらであるかは、ホスト定義によって異なります。
Ping Interval （注）	システムがPingパケット間で待機する時間。Pingは、成功したかどうかにかかわらず、[Number of Pings] フィールドで設定した回数繰り返されます。デフォルトの間隔を使用するか、独自の値を指定するかを選択します。

オプション	説明
この設定は、[Advanced Mode] ビューでのみ使用できます。	
Number of Pings （注） この設定は、[Advanced Mode] ビューでのみ使用できます。	Ping 操作を実行する回数。デフォルトを使用するか、独自の値を指定するかを選択します。
Status	Ping が正常に実行されたかどうかが表示されます。

ステップ 3 [Activate Ping] をクリックして、ホストに ping を実行します。ping のステータスが表示され、メッセージのリストにメッセージが追加されて ping 操作の結果が示されます。

ステップ 4 このページの [Ping Counters and Status] セクションに ping の結果が表示されます。

- [Number of Sent Packets]：ping で送信されたパケットの数
- [Number of Received Packets]：ping で受信されたパケットの数
- [Packet Loss]：Ping プロセス中に損失したパケットの割合
- [Minimum Round Trip Time]：パケットが戻った最短の時間
- [Maximum Round Trip Time]：パケットが戻った最長の時間
- [Average Round Trip Time]：パケットが戻った時間の平均
- [Status]：失敗か成功か

traceroute

トレースルートは、IPパケットをターゲットホストに送信し、デバイスに戻すことにより、転送される IP ルートを検出します。traceroute ページには、デバイスとターゲット ホスト間の各ホップが表示され、このような各ホップへのラウンド トリップ時間が表示されます。

手順

ステップ 1 [Administration] > [Traceroute] の順にクリックします。

ステップ 2 次のフィールドに情報を入力して、トレースルートを設定します。

- [Host Definition]：ホストがその IP アドレスまたは名前で識別されるどうかを選択します。

- [IP Version]：ホストがその IP アドレスで識別される場合、IPv4 または IPv6 のどちらかを選択して、IP アドレスを選択した形式で入力することを示します。
- [Source IP]：送信元インターフェイスを選択します。このインターフェイスの IPv4 アドレスが、通信メッセージの送信元 Ipv4 アドレスとして使用されます。[Host Definition] フィールドに [By Name] を指定した場合、ドロップダウンフィールドにはすべての IPv4 および IPv6 アドレスが表示されます。[Host Definition] フィールドが [By IP Address] の場合は、[IP Version] フィールドで指定したタイプの既存の IP アドレスのみが表示されます。
- [Host IP Address/Name]：ホストのアドレスまたは名前を入力します。
- [TTL]：traceroute で許容されるホップの最大数を入力します。これは、送信されたフレームが無限ループに陥る状態を防ぐために使用されます。traceroute コマンドは、宛先に到達した場合、またはこの値に到達した場合に終了します。デフォルト値（30）を使用するには、[Use Default] を選択します。

  （注）
  この設定は、[Advanced Mode] ビューでのみ使用できます。

- [Timeout]：システムがフレームの損失を宣言する前に、フレームが戻るのを待機する時間を入力するか、[Use Default] を選択します。

  （注）
  この設定は、[Advanced Mode] ビューでのみ使用できます。

ステップ 3 [Activate Traceroute] をクリックします。操作が実行されます。

（注）
トレースルートを停止するかどうかを示すポップアップが表示されます。[Stop Traceroute] をクリックして、プロセスを停止します。

ページが表示され、ラウンドトリップ時間（RTT）、および各トリップのステータスが次のフィールドに表示されます。

- [Index]：ホップ数が表示されます。
- [Host]：宛先までのルートに沿ったストップが表示されます。

  [Round Trip Time (1-3)]：ラウンドトリップ時間（ミリ秒）とステータスが表示されます。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。