Cisco Configuration Assistant 1.6/1.7 ガイド

この文書はお客様の便宜のために、オンラインヘルプから抽出したハンドブックになります。

目次

新機能

Configuration Assistant の最近のリリースでの機能拡張については、次のリンクをクリックしてください。

リリース 1.6
リリース 1.5
リリース 1.1

リリース 1.6

Configuration Assistant リリース 1.6 で新たにサポートされるデバイスは次のとおりです。

機能	説明
デバイスのサポート	Cisco Unified IP Phone 500 シリーズの、次に示すモデルを管理します。 521G 524G

リリース 1.5

Configuration Assistant リリース 1.5 の新機能および拡張機能は次のとおりです。

機能	説明
[デバイスの設定ウィザード]（新規）	Catalyst Express 520 スイッチ、Cisco Unified Communications 500 シリーズ プラットフォーム、Cisco 526 Wireless Express モビリティ コントローラ、および自律型 Cisco 521 Wireless Express アクセスポイントを設定します。
[無線コントローラダッシュボード]（新規）	コミュニティ内のすべての無線 LAN コントローラの情報を表示します。
[LAPに変換]（新規）	自律型アクセスポイントをライトウェイト アクセスポイントに変換します。
[WLANユーザ]（新規）	無線 LAN コントローラでの無線ユーザの追加と、WLAN ユーザ用の Web ログイン ページのコンテンツと概観のカスタマイズを行います。
[ライセンス管理]（新規）	追加のテレフォニー ユーザをサポートするためにライセンスを修正します。
[音声]（拡張）	SIP 電話および SIP トランクを設定します。
[VLAN]（拡張）	無線 LAN コントローラで VLAN を作成します。
[WLAN（SSID）]、旧[無線ネットワーク]（拡張）	4.2 イメージを実行する無線 LAN コントローラで WLAN（データ、ゲスト、または音声）を作成します。

[再起動/リセット]（拡張）	以前のリリースと同様にデバイスを再起動したり、工場出荷時の設定を回復します。
[トポロジビュー]（拡張）	トポロジ マップにネットワーク クラウドを追加したり、マップ上のノード間のリンクを手動で追加します。
[コミュニティ]（拡張）	[コミュニティの作成]ウィンドウまたは[コミュニティの修正]ウィンドウで、会社名または組織名をコミュニティと関連付けます。この名前がネットワークのデフォルトの SSID になります。
[設定の保存]（拡張）	類似するデバイスからバックアップされた設定を、選択されたデバイスに適用します。
デバイスのサポート	次に示す、Cisco Unified Communications 500 シリーズ プラットフォームの追加モデルを管理します。 UC520W-8/J-K9 UC520W-16/J-K9 UC520-24U-8FXO-K9 UC520-24U-4BRI-K9

リリース 1.1

Configuration Assistant リリース 1.1 の新機能および拡張機能は次のとおりです。

機能	説明
英語以外の GUI	フランス語、スペイン語、イタリア語、ドイツ語、ロシア語、日本語、および簡体字中国語バージョンの Configuration Assistant GUI をインストールします。
[音声]（拡張）	[音声]ウィンドウで T1/E1 音声ポート アダプタを設定します。
デバイスのサポート	次に示す、Cisco Unified Communications 500 シリーズ プラットフォームの追加モデルを管理します。 UC520-32U-8FXO-K9 UC520-32U-4BRI-K9 UC520-48U-12FXO-K9 UC520-48U-6BRI-K9 UC520-48U-T/E/F-K9 UC520-48U-T/E/B-K9
	次に示す、Catalyst Express 520 シリーズ スイッチの追加モデルを管理します。 WS-CE520-24PC-K9 WS-CE520-24LC-K9 WS-CE520-24TT-K9 WS-CE520G-24TC-K9

	次に示す、Cisco Unified IP Phone の追加モデルを管理します。 7942-G 7962-G 7945-G 7965-G 7975-G

ユーザ インターフェイス

概要

Configuration Assistant のユーザ インターフェイスを使用すると、ネットワーキング機能の管理および Configuration Assistant 自体からのサービス要求を容易に行うことができます。ユーザ インターフェイスの主要部は次のとおりです。

- **メニュー バー。**[Configuration Assistant]ウィンドウの上部に配置されているメニューの行です。アプリケーション サービス、開いているウィンドウのリスト、およびオンライン ヘルプを提供します。メニュー バーの詳細については、メニュー バーをクリックしてください。
- **ツールバー。**メニュー バーの真下にあるアイコンの行です。これらは、最もよく使用するアプリケーション サービスおよび最も頻繁に設定されるネットワーキング機能を表します。各アイコンが表す内容については、ツールバーをクリックしてください。
- **Configuration Assistant 作業スペース。**[Configuration Assistant]ウィンドウのメイン領域、つまりツールバーとステータス バーの間のすべての領域です。この領域は、機能バーと Configuration Assistant デスクトップの 2 つの部分で構成されます。
- **機能バー。**Configuration Assistant 作業スペースの左側にある、拡大縮小が可能なパネルです。ここでは、設定するネットワーキング機能を選択します。機能の名前がわからない場合は検索できます。機能バーの詳細については、機能バーをクリックしてください。
- **Configuration Assistant デスクトップ。**Configuration Assistant 作業スペースの右側の部分です。ここには、ウィンドウ、ウィザード、およびガイドモード手順が表示されます。レポートを表示したり、ネットワーキング機能を設定する情報を入力したりします。Configuration Assistant デスクトップの詳細については、Configuration Assistant デスクトップをクリックしてください。
- **ステータス バー。**[Configuration Assistant]ウィンドウの一番下にあるバーです。Configuration Assistant を起動すると、ステータス バーが表示され、ネットワーク上のデバイスが検出されるにつれてバーが右方向に進んでいきます。この処理が終了すると、Configuration Assistant は使用可能になります。この検出処理は、ネットワーク ポーリング間隔ごとに繰り返されます(コミュニティへの接続が切断された場合、ステータス バーには[No connectivity]と表示されます)。
- **[トポロジ]ビュー。**ネットワークのマップです。ビューで選択したオプションに応じて、他にさまざまな情報も表示されます。詳細については、[トポロジ]ビューをクリックしてください。
- **[前面パネル]ビュー。**ネットワーク上のデバイスの階層リスト、デバイスのワイヤリング クローゼットの図、および各デバイスとそのポートのステータスを示します。詳細については、[前面パネル]ビューをクリックしてください。

メニュー バー

メニュー バーには、Configuration Assistant を使用する際に役立つ複数の機能があります。各機能は、以下のように、いくつかのメニューにグループ分けされています。

メニュー	機能	説明

[アプリケーション]	[接続]	デバイスまたはコミュニティに接続します。
	[更新]	コミュニティ メンバをポーリングして、[前面パネル]ビューおよび[トポロジ]ビューを更新します。
	[コミュニティ]	コミュニティを作成および管理します。
	[アプリケーション更新]	アプリケーションの更新の有無を確認します。
	[システムメッセージ通知]	システムメッセージのメール通知を受け取ります。
	[ページ設定]、[印刷プレビュー]、[印刷]	標準の印刷オプションを使用して、ビュー、ウィンドウ、グラフ、およびヘルプ トピックを印刷します。
	[環境設定]	環境設定を行います。
	[機能バー]	機能バーの表示モードを設定します。
	[ガイド]、[エキスパート]	エキスパート モードとガイド モードを切り替えます。
[ウィンドウ]		開いているウィンドウのリストにある、特定のウィンドウに移動します。
[ヘルプ]	[概要]	Configuration Assistant を紹介するヘルプ トピックを表示します。
	[最新情報]	リリースの移行時に Configuration Assistant に追加された、新機能および拡張機能の一覧を表示します。
	[アクティブウィンドウのヘルプ]	アクティブなウィンドウまたはビューのヘルプ トピックを表示します。
	[コンテンツ]	Configuration Assistant を紹介するヘルプ トピックを表示します。
	[凡例]	ウィンドウおよびビュー内のすべてのアイコンについて説明する、ヘルプ トピックを表示します。
	[ヘルプの使い方]	オンライン ヘルプにおけるナビゲーションの表記規則および前提条件について説明する、ヘルプ トピックを表示します。
	[フィードバック]	シスコに Configuration Assistant のフィードバックを送信します。
	[サポート情報]	Cisco Technical Assistance Center（TAC）に問い合わせる方法、および TAC が必要とする情報を含むトラブルシューティ

		ング ログを生成する方法を表示します。
	[バージョン情報]	エンド ユーザのライセンス情報、および使用している Configuration Assistant リリースの識別情報を表示します。

ツールバー

ツールバーには、頻繁に実行するタスクのアイコンが表示されます。次の表は、これらのアイコンをクリックしたときに Configuration Assistant で実行される処理を示しています。

アイコン	処理
[接続]	Configuration Assistant で管理するコミュニティまたはスタンドアロン デバイスを指定する[接続]ウィンドウを開きます。
[更新]	コミュニティ メンバをポーリングして、[前面パネル]ビューおよび[トポロジ]ビューを更新します。デバイスおよびポートのステータスが更新され、新しいメンバがある場合はそれが表示されます。
[印刷]	グラフ、レポート、またはオンライン ヘルプで選択したものの印刷ファイルをプリンタに送信します。
[環境設定]	ユーザ環境設定を設定できる[環境設定]ウィンドウを開きます。
[設定の保存]	デバイス コンフィギュレーションに行った変更を固定の設定にします。つまり、デバイスの電源を切って、再び電源を入れたときに変更が有効なまま維持されます。
[音声]	音声通信のオプションを設定する[音声]ウィンドウを開きます。
[VPNサーバ]	セキュリティ ポリシーをデバイスに送信するように VPN サーバを設定する[VPNサーバ]ウィンドウを開きます。
[ファイアウォールとDMZ]	ファイアウォールの設定または DMZ の作成を実行する[ファイアウォールとDMZ]ウィンドウを開きます。
[無線ネットワーク]	WLAN コントローラおよびそれに関連付けられているアクセスポイントにセキュリティ機能を設定する[無線ネットワーク]ウィンドウを開きます。
[スマートポート]	ロールを適用することによってポートおよびデバイスを設定する[スマートポート]ウィンドウを開きます。
[ポート設定]	選択したデバイス上のポートのステータスを表示したり、ポート設定を変更したりできる[ポート設定]ウィンドウを開きます。
[インベントリ]	コミュニティのインベントリ(デバイスのタイプ、シリアル番号、IPアドレス、およびソフトウェア バージョン)、または単一デバイスのインベントリを表示する[インベントリ]ウィンドウを開きます。

[状態]	ダウンタイムを回避してネットワークが効率的に稼動するように、デバイスのさまざまな状態測定値を監視できる[状態]ウィンドウを開きます。
[イベント通知]	認識しておく必要があり、対処が必要な可能性のあるネットワーク状態を示す[イベント通知]ウィンドウを開きます。
[前面パネル]	コミュニティ内のデバイスの階層リスト、デバイスのワイヤリング クローゼットの図、および各デバイスとそのポートのステータスを示す[前面パネル]ビューを開きます。
[トポロジ]	コミュニティ メンバのネットワーク マップなど、選択したトポロジ オプションに応じた情報を表示する、[トポロジ]ビューを開きます。
[凡例]	Configuration Assistant で使用されている図の表記法を説明するオンライン ヘルプを開きます。
[アクティブウィンドウのヘルプ]	アクティブなウィンドウを説明するオンライン ヘルプを開きます。アクティブなウィンドウがない場合は、「概要」トピックが表示されます。
[フィードバック]	Configuration Assistant の使用に関するフィードバックを送信できるウェブページを開きます。

ツールバーの右にあるフィールドに用語を入力して[検索]をクリックすると、その用語が含まれるオンライン ヘルプ トピックを検索できます。詳細については、「情報の検索」を参照してください。

機能バー

機能バーは、Configuration Assistant デスクトップの左側に表示されます。機能バーに表示される機能の名前は、普段のタスクを識別する次のメニューに分類されています。

[セットアップ]。デバイスの使用の準備と、Configuration Assistant での管理のための準備
[設定]。デバイスとポートの設定
[モニタ]。ネットワークの監視
[トラブルシュート]。問題のトラブルシューティング
[メンテナンス]。ネットワークの管理

これらのいずれかのメニューから機能を選択すると、その機能のウィンドウ、つまりその機能の最初の手順を示すウィンドウが表示されます。

エキスパート モードとガイド モード

機能バー上の機能は、デフォルトでエキスパート モードで表示されます。つまり、ウィンドウから複数のオプションを選択することによって機能を使用します。機能名の横に アイコンが表示されている場合は、その機能をガイド モードで使用することもできます。この場合は、機能のオプションがガイド形式の手順で表示されます。エキスパート モードをガイド モードに切り替えるには、メニュー バーの[アプリケーション]をクリックして、[ガイド]を選択します。エキスパート モードに戻すには、[アプリケーション]メニューの[エキスパート]を選択します。

標準モードと自動非表示モード

機能バーが標準モードに設定されている場合は、機能バーの幅を狭くして、Configuration Assistant デスクトップ上のウィンドウ スペースを広げることができます。これを実行するには、機能バーの右端にカーソルを置き、そのカーソルを左にドラッグします。機能バーが自動非表示モードの場合、機能バーは、カーソルを Configuration Assistant 作業スペースの左端に移動したときにだけ表示されます。カーソルを機能バーの枠外の Configuration Assistant 作業スペースの任意の場所に移動すると、機能バーは再び非表示になります。モードを設定するには、**アプリケーション > 機能バー > 標準モード|自動非表示モード** を選択して、モードを選択します。

Configuration Assistant デスクトップ

Configuration Assistant デスクトップは、ユーザ インターフェイスの中心となる部分です。ここでは、次のタスクを実行できます。

- [トポロジ]ビュー（Configuration Assistant で管理しているコミュニティのネットワーク マップ）を表示する。このビューには、ノード情報、リンク情報、および隣接デバイスが表示されます。
- [前面パネル]ビュー（コミュニティ内のデバイスの前面パネルの図）を表示する。描画されたデバイスとポートをクリックすると、ポップアップ メニューから設定オプションを選択できます。

  注：Configuration Assistant がデバイスに接続されたときにデフォルトでどのビューを開くかは、環境設定として設定できます。どちらかのビューまたは両方のビューが開くように設定することも、両方とも開かないように設定することもできます。

- ネットワーキング機能を設定するための情報を入力する。このタスクは、機能ウィンドウまたはガイドモード手順を使用して実行します。

  注：Configuration Assistant では、入力した情報が有効な場合、入力値が有効であることを示す緑色の線で囲まれます。変更した情報は、ステータス バーに表示されます。変更を保存すると、緑色の線は消えます。入力した情報が無効な場合は、入力値が赤色の線で囲まれます。エラーを示すメッセージがステータス バーに表示されます。

- レポートとグラフを表示する。機能バーのメニューで、「レポート」および「グラフ」という語を探します。これらの語が含まれるさまざまなネットワーキング機能があります。

ボタン

ユーザ インターフェイスには、ほぼすべてのウィンドウ、ガイドモード手順、およびウィザード手順に表示されるボタンがあります。次の表は、これらのボタンをクリックしたときに実行される Configuration Assistant の動作を示しています。

ボタン	動作
[適用]	変更を有効にし、さらに他の項目を変更できるようにウィンドウを開いたままにします。
[OK]	親ウィンドウでは、変更を有効にしてウィンドウを閉じます。子ウィンドウでは、変更を記録してウィンドウを閉じます。親ウィンドウで[OK]または[適用]をクリックしない限り、変更は有効になりません。

[更新]	デバイス上で有効になっている設定を復元します。まだ適用されていない変更はすべて失われます。つまり、デバイス上の設定に置き換わります。
[キャンセル]	ウィンドウをクリアします。まだ適用されていない変更は破棄されます。
[ヘルプ]	対象のウィンドウに関するヘルプ トピックを表示します。
[前]	1 つ前の手順に戻ります。
[次]	次の手順に進みます。
[終了]	手順を完了し、入力された情報の処理を開始します。

情報の検索

ツールバーの検索フィールド、または[ヘルプ]ウィンドウの[検索]タブ上の検索フィールドを使用して、オンライン ヘルプ トピックで 1 つまたは複数の用語を検索できます。「用語」とは、英数字の文字列のことです。検索フィールドでは、スペースを使用して複数の用語を区切ります。

ツールバー検索で[検索]をクリックすると、フィールドに入力したすべての単語に該当するヘルプ トピックが Configuration Assistant によって検索されます。[検索]タブには、別の選択肢もあります。[部分一致]を選択すると、フィールドに入力した用語のいずれかに該当するヘルプ トピックが検索されます。

[検索]タブに、検索用語と一致するヘルプ トピックが一覧表示されます。ツールバーで検索を実行した場合、[ヘルプ]ウィンドウが開かれ、一致するトピックが表示されます。一致するトピックをクリックして、[ヘルプ]ウィンドウで表示します。

キーボードによるナビゲーション

Configuration Assistant の画面でマウスを使用して実行できる操作は、すべてキーボードでも実行できます。次の表は、画面操作とキーボードでの実行方法を示しています。

操作	**実行方法**
メニューバーのメニューを開く	**Alt** キーを押しながら、メニュー名の下線の付いた文字のキーを押します。
メニュー項目を選択する	目的の項目が強調表示されるまで、上下の矢印キーを押します。次に、**Enter** キーを押します。
機能バーのドロワーを開く	**Alt** キーを押しながら、メニュー名の下線の付いた文字のキーを押します。
機能バーから機能を選択する	上下の矢印キーを押して、項目を強調表示します。強調表示したタイトルを展開するには、右矢印キーを押します(左矢印キーを押すと、タイトルを折りたたむことができます)。目的の機能を強調表示したら、**Enter**

	キーを押します。
プロンプトへの応答	**Tab** キーを押して目的の応答に移動し、**Enter** キーを押します。
ウィンドウ内のタブ間の移動	任意のタブにフォーカスが置かれる（タブのラベルが点線で囲まれる）まで **Tab** キーを押します。次に、左右の矢印キーを使用して、他のタブに移動します。
ウィンドウのオプションを選択する（テーブルを除く）	目的のオプションにフォーカスが置かれるまで、**Tab** キーを押します。スペース バーを使用してラジオ ボタンを選択したり、チェックボックスのオンとオフを切り替えたりします。リスト項目の選択には、上下の矢印キーを使用します。
テーブルのセル内のオプションを編集する	テーブル内にフォーカスが移動するまで **Tab** キーを繰り返し押し、上下の矢印キーを使用して、特定の行に移動します。**Tab** キーまたは **Shift+Tab** キーを押して、編集するセルに移動します。 セルにチェックボックスが含まれる場合は、スペース バーを押してオンとオフを切り替えます。 テーブル内にフォーカスがある場合は、**Ctrl+Tab** キーを押すまで、フォーカスはテーブル内に維持されます。
開いているウィンドウ間を移動する	**Ctrl+F6** キーを押します。
[OK]、[適用]、[更新]、[キャンセル]、および[ヘルプ]ボタンを使用する	目的のボタンにフォーカスが置かれるまで **Tab** キーを押し、次に **Enter** キーを押します。
[ヘルプ]ウィンドウを閉じる	**Ctrl+F4** キーを押します。

アプリケーション サービス

キーボードによるナビゲーション

Configuration Assistant の画面でマウスを使用して実行できる操作は、すべてキーボードでも実行できます。次の表は、画面操作とキーボードでの実行方法を示しています。

操作	実行方法
メニューバーのメニューを開く	**Alt** キーを押しながら、メニュー名の下線の付いた文字のキーを押します。
メニュー項目を選択する	目的の項目が強調表示されるまで、上下の矢印キーを押します。次に、**Enter** キーを押します。
機能バーのドロワーを開く	**Alt** キーを押しながら、メニュー名の下線の付いた文字のキーを押します。
機能バーから機能を選択する	上下の矢印キーを押して、項目を強調表示します。強調表示したタイトルを展開するには、右矢印キーを押します（左矢印キーを押すと、タイトルを折りたたむことができます）。目的の機能を強調表示したら、**Enter** キーを押します。
プロンプトへの応答	**Tab** キーを押して目的の応答に移動し、**Enter** キーを押します。
ウィンドウ内のタブ間の移動	任意のタブにフォーカスが置かれる（タブのラベルが点線で囲まれる）まで **Tab** キーを押します。次に、左右の矢印キーを使用して、他のタブに移動します。
ウィンドウのオプションを選択する（テーブルを除く）	目的のオプションにフォーカスが置かれるまで、**Tab** キーを押します。スペース バーを使用してラジオ ボタンを選択したり、チェックボックスのオンとオフを切り替えたりします。リスト項目の選択には、上下の矢印キーを使用します。
テーブルのセル内のオプションを編集する	テーブル内にフォーカスが移動するまで **Tab** キーを繰り返し押し、上下の矢印キーを使用して、特定の行に移動します。**Tab** キーまたは **Shift+Tab** キーを押して、編集するセルに移動します。 セルにチェックボックスが含まれる場合は、スペース バーを押してオンとオフを切り替えます。 テーブル内にフォーカスがある場合は、**Ctrl+Tab** キーを押すまで、フォーカスはテーブル内に維持されます。
開いているウィンドウ間を移動する	**Ctrl+F6** キーを押します。
[OK]、[適用]、[更新]、[キャンセル]、および[ヘ	目的のボタンにフォーカスが置かれるまで **Tab** キーを押し、次に **Enter** キーを押します。

ルプ]ボタンを使用する	
[ヘルプ]ウィンドウを閉じる	**Ctrl+F4** キーを押します。

Configuration Assistant の更新

Cisco.com で更新を検索してインストールすることによって、Configuration Assistant を最新の状態に維持します。

Configuration Assistant では、次のような場合、更新の検索を求めるメッセージが表示されます。

- 管理対象のデバイスのうち、新しいデバイス タイプや、ソフトウェアがアップグレードされているデバイスが検出された場合
- [環境設定]ウィンドウで定期的な検索が設定されていて、次の検索時になった場合

アプリケーション > アプリケーション更新 を選択して、必要な時点で更新を検索することもできます。

Configuration Assistant で更新が検出された場合は、その内容の説明を読んで、インストールするかどうかを判断することができます。

コミュニティまたはスタンドアロン デバイスへの接続

Configuration Assistant を起動すると、2 つのウィンドウが表示されます。1 つは、ユーザ インターフェイスが含まれる[Configuration Assistant]ウィンドウ、もう 1 つは、[接続]ウィンドウです。

Configuration Assistant は、未接続モードで起動します。つまり、コミュニティにもスタンドアロン デバイスにも接続されていません。このモードでは、[Configuration Assistant]ウィンドウにメニュー バーは表示されますが、機能バーは表示されません。機能バーは、Configuration Assistant が接続されているときにだけ、デバイスの機能に基づく内容で作成および表示されます。

[接続]ウィンドウでは、次の処理を選択できます。

- 新しいコミュニティに接続する。まずコミュニティを作成してから接続します。
- 既存のコミュニティまたはスタンドアロン デバイスに接続する。

[OK]をクリックすると、Configuration Assistant のセッションが確立されます。1 台の PC では一度に 1 つのセッションのみ実行できます。

セッションを終了するには、[Configuration Assistant]ウィンドウを閉じるか、[アプリケーション]>[終了]の順に選択します。

コミュニティの管理

Configuration Assistant では、コミュニティと呼ばれるデバイス グループを管理します。コミュニティでは、各メンバに IP アドレスを割り当てる必要があります。Configuration Assistant は、すべてのメンバと直接通信するため、どのメンバとも HTTPS リンクでの接続が可能です。

注：HTTPS を使用する場合の要件については、「HTTPS の使用」を参照してください。

コミュニティの特徴

コミュニティには、HTTPS リンクのセキュリティを提供することのほかに、次のような特徴があります。

- Catalyst Express スイッチ、Cisco ルータ、Cisco WLAN コントローラ、Aironet 自律型アクセスポイント、および HWIC アクセスポイントからなる最大 25 個のデバイスで構成できます。

  注： Cisco ルータには、Unified Communications 500 シリーズ プラットフォームと 800 シリーズ アクセス ルータが含まれます。コミュニティのサイズおよび特定のデバイス タイプのデバイス数に関する制限事項は、「コミュニティに関する制限事項」を参照してください。

- すべてのメンバに IP アドレスが割り当てられるため、あるメンバとの通信が切断されても、他のメンバとは引き続き通信できます。
- ルータやアクセスポイントなどのコミュニティ メンバに対して、一連の基本的なネットワーキング タスクがサポートされます。サポートされるタスクは、次のとおりです。

  ユーザ アクセスの管理
  ソフトウェアのアップグレード
  実行中の設定の保存
  設定のバックアップと復元
  システムの時刻の管理
  システム メッセージ通知の受信
  HTTP ポート番号の変更
  インベントリ レポートの取得

コミュニティの作成

コミュニティは、次のいずれかの方法で作成できます。

- Configuration Assistant を起動すると、[接続]ウィンドウが表示されます。[新しいコミュニティに接続する]を選択して[接続]をクリックし、[コミュニティの作成]ウィンドウを使用します。
- メニュー バーから **アプリケーション > コミュニティ** を選択すると、[コミュニティ]ウィンドウが表示されます。[作成]をクリックして、[コミュニティの作成]ウィンドウを使用します。

ユーザ環境設定

Configuration Assistant での処理のほとんどはカスタマイズが可能です。たとえば、次の処理をカスタマイズできます。

- Configuration Assistant をネットワークに接続したときに、[トポロジ]ビューと[前面パネル]ビューのいずれかまたはその両方を表示するか。
- どれくらいの頻度で Configuration Assistant が管理対象デバイスをポーリングして最新の情報に更新するか。
- どれくらいの頻度で Cisco.com にアクセスして、Configuration Assistant の更新を検索するか。
- Configuration Assistant の更新を Cisco.com からダウンロードするためにプロキシ サーバを使用するか。ネットワークとの通信にプロキシ サーバを使用するか。

- 管理対象デバイス上の保存済み設定をのどの場所に保存するか。
- スタンドアロン デバイスまたはコミュニティの状態を監視できるように、Configuration Assistant でどの項目を定期的に測定するか。

このような質問への回答に合わせて設定するには、**アプリケーション > 環境設定** を選択して、[環境設定]ウィンドウを使用します。

環境設定は、Configuration Assistant を終了するときに、コンピュータの .user_preferences というファイルに保存されます。このファイルは、パス C:¥Documents and Settings¥*username*¥.configuration assistant に保存されます。このファイルを他の PC にコピーすることができます。

印刷

Configuration Assistant のウィンドウ、ビュー、グラフ、またはオンライン ヘルプ トピックを印刷するには、次の手順に従います。

1. 印刷するオブジェクトをアクティブにします。
2. [アプリケーション]>[印刷]の順に選択するか、ツールバーの  をクリックして、印刷ファイルをプリンタに送信します。

ウィンドウを印刷する場合、出力はレポート形式になります。この形式では、**Print Screen** キーを使用して画面を印刷するときのようにウィンドウの情報が切り捨てられることはありません。レポート形式では、タイムスタンプとページ番号も挿入されます。

注:

- ポップアップ エラー メッセージが表示されたために印刷するオブジェクトが非アクティブになった場合は、オブジェクトが再びアクティブになるまで印刷はできません。
- 子ウィンドウ(親ウィンドウでボタンをクリックしたときに開く 2 つ目のウィンドウ)を印刷するには、そのウィンドウが開いていてアクティブである必要があります。

[トポロジ]ビューまたは[前面パネル]ビューを印刷する場合、[印刷プレビュー]ウィンドウ([アプリケーション]>[印刷プレビュー])に[ページに合わせる]オプションが表示されます。ビューを 1 ページに印刷するには、このオプションをオンにします。

システム メッセージ通知の受信

詳細が必要なシステム メッセージのメール通知を受け取ることができます。システム メッセージとはコミュニティのイベントに関するもので、緊急事態やアラート(重大度 0 および 1)を示すものから、情報的なメッセージやデバッグ メッセージ(重大度 6 および 7)までが含まれます。

この機能を有効にするには、通知名を作成する必要があります。このタスクは、**アプリケーション > システムメッセージ通知** を選択し、[システムメッセージ通知]ウィンドウを使用して実行します。

デバイスの設定

ここでは、Configuration Assistant が管理するデバイス（スイッチ、Unified Communications 500 シリーズ プラットフォーム、無線 LAN コントローラ、自律型アクセスポイント）の設定方法について説明します。

デバイスの設定ウィザードの使用

デバイスの設定ウィザードでは、デバイスを使用する準備、および Configuration Assistant でデバイスを管理する準備の設定を順を追って行うことができます。

ウィザードを開くには、**セットアップ > デバイスの設定ウィザード** を選択します。

ネットワークの設定

ここでは、管理対象のネットワーク オブジェクト（デバイス、ポート、および VLAN）を設定する方法について説明します。

このセクションの内容は、次のとおりです。

- **ポートとデバイスのクイック設定**
  スマートポート機能について説明し、ポート接続およびデバイスの設定に使用するウィンドウへのリンクを示します。
- **ポートの管理**
  スマートポートの本来の機能に加えて、ポート設定をカスタマイズするためのタスクに関する情報を示します。
- **セキュリティの設定**
  管理対象デバイスへの安全なアクセスを確立するためのタスクに関する情報を示します。
- **テレフォニーの設定**
  音声システムの設定および管理を行うためのタスクに関する情報を示します。
- **LAN スイッチの設定**
  STP および VLAN の設定方法など、ローカル エリア ネットワークを管理するためのタスクに関する情報を示します。
- **無線アクセスの設定**
  無線セキュリティおよび無線インターフェイスを設定するためのタスクに関する情報を示します。
- **IP ルーティングの設定**
  静的ルーティングを設定するためのタスクに関する情報を示します。
- **デバイス プロパティの設定**
  管理するデバイスを設定するためのタスクに関する情報を示します。
- **実行中の設定の保存**
  [設定の保存]機能について説明し、個別またはすべての管理対象デバイスの実行中の設定の保存に使用するウィンドウへのリンクを示します。

ポートのクイック設定

CE520 スイッチを管理する場合

スマートポートは、ネットワークのポート接続に必要なセキュリティ、可用性、管理性の機能を確実に設定するためのソリューションです。

ポート接続を次のデバイスに設定できます。

デバイス	コメント
デスクトップ	インターネットおよび組織の内部サブネットにアクセスできる内部のエンドホスト。
IP Phone	PC のようなエンドホストは、IP Phone にカスケード接続することが可能です。

スイッチ	スイッチ間の接続。
ルータ	アクセス ルータまたは UC500 プラットフォーム。
アクセスポイント	モバイル エンドホストに接続できます。アクセスポイントの設定に応じて、モバイル エンドホストはゲスト エンドホストにもデスクトップ エンドホストにもなりえます。
サーバ	内部エンドホストおよびインターネット クライアントへサービスを提供するエンドホスト。サーバ エンドホストの例には、Exchange サーバ、コラボレーション サーバ、ターミナル サーバ、ファイル サーバ、および DHCP サーバがあります。
プリンタ	ネットワーク プリンタまたは外部プリント サーバ。
ゲスト	アクセスがインターネットに制限されたエンドホスト。組織の内部サブネットへのアクセス権はありません。
スニファ	トラブルシューティング時に支援するデバイス。
その他	ゲストに属するデスクトップ、IP Phone、サーバ、またはプリンタ。

ポート接続を設定するには、ロールをポートに適用します。このタスクを実行するには、機能バーで **設定 > スマートポート** を選択するか、ツールバー上の をクリックし、[スマートポート]ウィンドウを使用します。このウィンドウにデバイスの前面パネルが表示されるので、ポートを選択してロールを適用します。

UC500 を管理する場合

スマートポートは、ネットワークのポート接続に必要なセキュリティ、可用性、および管理性の機能の設定に役立つソリューションです。

ポート接続を次のデバイスに設定できます。

デバイス	**コメント**
デスクトップ	インターネットおよび組織の内部サブネットにアクセスできる内部エンドホスト。
IP Phone	PC のようなエンドホストは、IP Phone にカスケード接続することが可能です。
スイッチ	スイッチ間の接続。
ルータ	アクセス ルータまたは UC 500 プラットフォーム。
アクセスポイント	モバイル エンドホストに接続できます。アクセスポイントの設定に応じて、モバイル エンドホストはゲスト エンドホストにもデスクトップ エンドホストにもなりえます。

ポート接続を設定するには、ロールをポートに適用します。この作業を行うには、機能バーで **設定 > スマートポート** を選択するか、ツールバー上の をクリックし、[スマートポート]ウィンドウを使用します。このウィンドウにデバイスの前面パネルが表示されるので、ポートを選択してロールを適用します。

VLAN の設定

CE520 スイッチを管理する場合

VLAN は、ユーザの物理的な位置とは関係なく、機能、プロジェクト チーム、またはアプリケーションごとに論理的にセグメント化された、スイッチ ネットワークです。VLAN には物理的な LAN と同じ属性がありますが、物理的に同一 LAN セグメント上に配置されていないエンド ステーションでも、グループ化できます。どのスイッチ ポートも VLANに属し、ユニキャスト パケット、ブロードキャスト パケット、およびマルチキャスト パケットはその VLAN のエンドステーションにのみ転送されます。

VLAN ではレイヤ 2 ネットワークのブロードキャスト ドメインが定義されます。ブロードキャスト ドメインとは、セット内の任意のデバイスから発信されたブロードキャスト フレームを受信するすべてのデバイスのセットのことです。ブロードキャスト ドメインは、通常、ルータがブロードキャスト フレームを転送しないので、ルータにより分割されます。レイヤ 2 スイッチでは、スイッチのコンフィギュレーションに基づいてブロードキャスト ドメインが作成されます。スイッチは、複数のブロードキャスト ドメインを作成できるマルチポート ブリッジです。各ブロードキャスト ドメインは、スイッチ内で個別仮想ブリッジのような役割を果たします。

スイッチ内の 1 つまたは複数の仮想ブリッジを定義できます。スイッチ内に作成した各仮想ブリッジでは、新しいブロードキャスト ドメイン（VLAN）が定義されます。トラフィックは、スイッチ内または 2 つのスイッチ間で別の VLAN に（ブロードキャスト ドメインをまたがって）直接伝送できません。2 つの別々の VLAN を相互接続するには、ルータまたはレイヤ 3 スイッチを使用する必要があります。

デフォルトでは、スイッチは単一の VLAN （VLAN 1）で設定されています。追加の VLAN を作成する場合（IP Phone がポートに接続されている場合は推奨）、**設定 > VLAN** を選択し、[VLAN]ウィンドウを使用します。このウィンドウを使用して、VLAN の名前を変更したり、削除します。

WLC526 を管理する場合

WLAN コントローラにユーザ定義の VLAN を設定できます。VLAN を設定してから WLAN を作成する必要があります。1 つの WLAN コントローラで最大 8 つのユーザ定義 VLAN をサポートできます。これら 8 つの VLAN のうち、音声 VLAN とゲスト VLAN は 1 つずつしか設定できません。

1 つの VLAN には、VLAN ID、ポート、IP アドレス、サブネット マスク、デフォルト ゲートウェイ（IP サブネット用）、DHCP サーバなど複数のパラメータが関連付けられています。

ユーザ定義の VLAN を WLAN コントローラに設定するには、設定 > VLAN を選択して、[VLAN]ウィンドウを使用します。

セキュリティの設定

ファイアウォールと DMZ の設定

ネットワークのセキュリティは、ファイアウォールと Demilitarized Zone（DMZ; 非武装地帯）を設定して LAN を保護することで強化できます。

次の作業を行うことによって、ネットワークのセキュリティを管理してください。

- 選択したセキュリティ レベルに基づいて、ルータ上の着信パケットをフィルタするファイアウォールを設定します。基準を満たしているパケットは、インターフェイスを通過できます。セキュリティ パラメータで指定された基準を満たしていないパケットは破棄されます。
- パブリック アクセス サーバ用に DMZ を作成し、個別の独立したネットワークに配置します。これにより、内部ネットワークのセキュリティがいっそう強化されます。DMZ は、ウェブへのパブリック アクセス、およびインターネットからアクセス可能なサーバへのウェブ アクセスに使用できます。DMZ を作成するには、事前にファイアウォールを作成しておく必要があります。

これらの作業を行うには、**設定 > セキュリティ > ファイアウォールとDMZ** を選択します。

関連リンク

- *Cisco IOS Firewall:* Introduction

VPN の設定

Virtual Private Network（VPN; バーチャル プライベート ネットワーク）を使用すると、リモート クライアントから企業のネットワークにアクセスできるようになります。VPN による通信は、IEEE 802.1x に基づくユーザ認証の完了後に可能となります。

VPN は、次のような状況で必要になります。

- ネットワーク ファイアウォールの外部にあるリモート コンピュータから Cisco Unity Administrator のウェブ サイト（http://Cisco Unity サーバ名/web/sa）にアクセスする必要がある場合。
- Distributed Component Object Model（DCOM; 分散 COM）を使用してリモート コンピュータからファイアウォール越しに Cisco Unity サーバに接続し、Media Master コントロールバーを使用して音声名とメッセージを録音する必要がある場合。

VPN サーバから送信された IP Security（IPSec; IP セキュリティ）ポリシーを受け取れるように、リモートの VPN デバイスを認可することができます。また、IPSec ポリシーをリモートの VPN デバイスに送信するように VPN サーバを設定することも可能です。

VPN サーバからポリシーを受け取れるようにリモートの VPN クライアントを認可すると、エンド ユーザは、パスワードを入力して、VPN トンネル経由での自社ネットワークへの接続を要求できるようになります。接続が要求され、リモートのエンド ユーザが認証されると、VPN サーバからリモートのクライアントにパラメータが転送されます。パラメータが転送されない場合、ユーザは、IPSec パラメータを手動で入力して VPN トンネルを設定しなければなりません。リモートの VPN デバイスには、Cisco IOS ルータ、Cisco PIX セキュリティ アプライアンス、Cisco VPN 3002 ハードウェア クライアント、Cisco VPN クライアントなどがあります。

リモート クライアントを認証する事前共有鍵を設定することもできます。事前共有鍵は、IPSec ポリシーを受け取るリモート デバイスとサーバ間の通信のセキュリティを強化します。リモート デバイス上の事前共有鍵と VPN サーバ上の事前共有鍵は、一致している必要があります。

リモート ネットワークでスプリット トンネリングを有効にすると、ローカル デバイスとの通信やインターネット越えでの他のネットワークとの通信が暗号化されなくなります。データが暗号化されるのは、エンド ユーザが保護されたサブネットワーク（一般的には、企業ネットワーク）と通信するときだけになります。そのため、デバイスの処理時間が短縮され、ネットワークのパフォーマンスがよくなります。

例として、在宅勤務者が VPN クライアント PC を使用して企業ネットワークにアクセスする場合を考えてみます。途中にはルータがあり、在宅勤務者の自宅から企業ネットワークに、インターネット上の VPN トンネル経由で接続できるようになっています。ただし、在宅勤務者の自宅には、企業ネットワークに組み込まれておらず、VPN へのアクセスが許可されていない他の PC が存在する可能性があります。在宅勤務者の配偶者や子供の使用する PC などが、その一般的な例です。このような PC もインターネットへのアクセスを必要とするため、家庭内でブロードバンド接続を別に設定しなくてすむよう、在宅勤務者のルータが使用される可能性があります。IPSec トンネルは常時稼動し、リモート サイトからアクセスしようとする企業のユーザを IEEE 802.1x に基づいて認証します。企業の本社にある RADIUS サーバには、企業のユーザのデータベースが格納されています。このような場合、トンネルが常に利用可能な状態になっているため、リモート ルータからデータベースにクエリーを送信して在宅勤務者の 802.1x クレデンシャル（ユーザ名とパスワード）を確認し、在宅勤務者については VPN へのアクセスを許可する一方、その他のユーザについてはすべて排除することができます。

注 : スプリット トンネリングの設定には、セキュリティ上のリスクが伴います。VPN クライアントからインターネットへのアクセスは保護されないため、VPN クライアントは攻撃の標的となるおそれがあります。VPN クライアントを攻撃したユーザは、そのクライアントの ID を使用し、IPSec トンネル経由で企業 LAN にアクセスする可能性があります。

セキュリティ ポリシーをデバイスに送るように VPN サーバを設定するには、**設定 > セキュリティ > VPNサーバ** を選択します。

サーバから送られたセキュリティ ポリシーを受け取るようにデバイスを設定するには、**設定 > セキュリティ > VPNリモート** を選択します。

関連リンク

- *Cisco Easy VPN:* Introduction

ルータのセキュリティ設定の監査

ネットワーク上のネットワーキング サービスの安全性を高めるために、セキュリティ ポリシーを検査して、セキュリティ手順を有効にすることができます。ルータのセキュリティ設定を監査することで、ルータ設定における重要なセキュリティ機能を検査し、セキュリティ上の問題が潜んでいないかどうかを確認できます。推奨されるセキュリティ設定は、受け入れることも、拒否することもできます。

監査では、次の機能が検査されます。必要に応じて設定を変更し、ネットワークのセキュリティを調整してください。

- Finger サービスを無効にする。
- PAD サービスを無効にする。
- TCP スモール サーバ サービスを無効にする。
- UDP スモール サーバ サービスを無効にする。
- IP BOOTP サーバ サービスを無効にする。
- IP 識別サービスを無効にする。
- IP発信元ルートを無効にする。
- パスワード暗号化サービスを有効にする。

- インバウンド Telnet セッションの TCP キープアライブを有効にする。
- アウトバウンド Telnet セッションの TCP キープアライブを有効にする。
- デバッグのシーケンス番号とタイム スタンプを有効にする。
- IP Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）を有効にする。
- IP Gratuitous ARP を無効にする。
- パスワードの最小文字数を 6 文字以上に設定する。
- 認証が失敗する場合に許可される再試行の回数を 3 回未満に設定する。
- TCP synwait 時間を設定する。
- ロギングを有効にする。
- SNMP を無効にする。
- スケジューラ割り当てを設定する。
- IP リダイレクトを無効にする。
- IP プロキシ ARP を無効にする。
- IP ダイレクト ブロードキャストを無効にする。
- Maintenance Operation Protocol（MOP; メンテナンス オペレーション プロトコル）サービスを無効にする。
- IP 到達不能を無効にする。
- IP マスク応答を無効にする。
- ヌル インターフェイスに対して IP 到達不能を無効にする。
- 外部インターフェイスに対してユニキャスト RPF を有効にする。
- AAA を有効にする。

セキュリティ監査を実行するには、**設定 > セキュリティ > セキュリティ監査** を選択します。

関連リンク

- *Internetwork Design Guide:* Increasing Security on IP Networks

NAT の設定

インターフェイスで Network Address Translation（NAT; ネットワーク アドレス変換）を有効にすると、LAN 上のプライベート IP アドレスが、登録されているパブリック ネットワーク IP アドレスのグループ内の 1 つのパブリック ネットワーク IP アドレスにマッピングされます。

インターネットにアクセスするには、有効かつ登録済みであり、全体を通じて一意のパブリック IP アドレスが必要です。通常、組織は、十分なパブリック IP アドレスを所持していないため、インターネットへのアクセスを必要とする組織内の各クライアントに一意のパブリック IP アドレスを割り当てることができません。NAT を使用しなければ、パブリック IP アドレスのプールは使い果たされてしまいます。また、LAN の内部構造も、パブリック ネットワークのすべてのクライアントに表示されてしまいます。NAT を使用すると、1 つのパブリック IP アドレスを使用して、LAN 上の複数のクライアントにインターネット経由でアクセスできるようになります。

不正なクライアントは、ネットワーク IP アドレスを使用してネットワークのトポロジを特定できれば、簡単にネットワークを攻撃できます。NAT を使用すると、インターネットでプライベート IP アドレスを隠しておくことができます。IP アドレスを使用して LAN の構造を推測できなければ、攻撃者がネットワークに侵入することも困難になります。

注:NAT はレイヤ 3 イーサネット インターフェイスだけをサポートしています。レイヤ 2 スイッチ ポート インターフェイスはサポートしていません。(信頼できない)外部インターフェイスで NAT を有効にすると、他のすべての正規のインターフェイスが、(信頼できる)内部インターフェイスとして自動的に選択されます。

NAT を有効にするには、**設定 > セキュリティ > NAT** を選択します。

関連リンク

- *IP Addressing Services:* How NAT Works

無線アクセスの設定

無線セキュリティの設定

AP521 を管理する場合

自律型アクセスポイントのセキュリティ機能を設定できます。セキュリティ機能によって、自律型アクセスポイントとその他の無線デバイス間の無線通信が保護され、不正アクセスが阻止されます。自律型アクセスポイントには、さまざまなレベルのセキュリティおよび暗号化を設定できます。セキュリティを未適用にすることも、高度なセキュリティを適用することもできます。

自律型アクセスポイントにセキュリティを設定するには、**設定 > 無線 > WLAN(SSID)** を選択して、[WLAN(SSID)]ウィンドウを使用します。

UC500、Cisco 800シリーズルータを管理する場合

HWIC アクセスポイントには、セキュリティ機能を設定することができます。セキュリティ機能によって、HWIC アクセスポイントとその他の無線デバイス間の無線通信が保護され、不正アクセスが阻止されます。HWIC アクセスポイントには、さまざまなレベルのセキュリティおよび暗号化を設定可能です。セキュリティを未適用にすることも、高度なセキュリティを適用することもできます。

HWIC アクセスポイントにセキュリティを設定するには、**設定 > 無線 > WLAN(SSID)** を選択して、[WLAN (SSID)]ウィンドウを使用します。

WLC526 を管理する場合

WLAN コントローラおよびそれに関連付けられているアクセスポイントにセキュリティ機能を設定できます。セキュリティ機能によって、アクセスポイントとその他の無線デバイス間の無線通信が保護され、不正アクセスが阻止されます。アクセスポイントには、さまざまなレベルのセキュリティおよび暗号化を設定できます。セキュリティを未適用にすることも、高度なセキュリティを適用することもできます。

WLAN コントローラに RADIUS サーバを設定することもできます。

注:RADIUS サーバは、次のセキュリティ タイプに設定する必要があります。

- ［EAP］
- ［WPA］
- ［WPA2］
- ［MAC］
- ［MAC & EAP］

アクセスポイントにセキュリティを設定するには、設定 > 無線 > WLAN(SSID) を選択して、［WLAN (SSID)］ウィンドウを使用します。

デバイス プロパティの設定

デバイス アクセスの設定

Telnet および SSH を使用すると、デバイスへのリモート アクセスやデバイスからのリモート アクセスが可能になります。使用しているデバイスが音声機能をサポートしている場合、Telnet は無効にできません。SSH は、Telnet よりもセキュリティ レベルが高いと見なされます。

この機能を有効にするには、**設定 > デバイスプロパティ > デバイスアクセス** を選択します。

IP アドレスの管理

CE520 スイッチを管理する場合

次の作業を行うことによって、IP アドレスを管理します。

- IP アドレスを VLAN に割り当てます。これにより、VLAN は SVI（スイッチ仮想インターフェイス）になります。SVI を作成すると、デバイスのルーティングが有効になりません。
- デフォルト ゲートウェイとドメイン名を指定します。
- ドメインネームサーバを指定します。

IP アドレスを管理するには、**設定 > デバイスプロパティ > IPアドレス**を選択して、［IPアドレス］ウィンドウを使用します。

UC500 を管理する場合

次の作業を行うことによって、IP アドレスを管理します。

- IP アドレスを VLAN に割り当てます。これにより、VLAN は SVI（スイッチ仮想インターフェイス）になります。SVI を作成すると、デバイスのルーティングが有効になりません。
- ドメイン名を指定します。
- ドメインネームサーバを指定します。

IP アドレスを管理するには、**設定 > デバイスプロパティ > IPアドレス**を選択して、［IPアドレス］ウィンドウを使用します。

ホスト名の変更

コミュニティ内の名前のないメンバにホスト名を付与できます。または、そのホスト名を変更できます。このタスクを実行するには 2 つの方法があります。

1. [トポロジ]ビューで、名前を付けるメンバ、または名前を変更するメンバを右クリックします。
   メンバの色が青に変わり、ポップアップ メニューが表示されます。
2. ポップアップ メニューで[ホスト名]を選択して、[ホスト名]ウィンドウを使用します。

または、次の手順に従います。

1. [トポロジ]ビューで、名前を変更するメンバをクリックします。
2. **設定 > デバイスプロパティ > ホスト名** を選択して、[ホスト名]ウィンドウを使用します。

名前の変更は直ちには反映されません。変更があったときは、ステータス バーにメッセージが表示されます。

システムの時刻の管理

CE520 スイッチを管理する場合

時刻および夏時間をネットワーク デバイス上で手動で設定したり、デバイスの時刻を PC の時刻または特定のデバイス上のシステムの時刻と同期させたりできます。これらの作業を実行するには、**設定 > デバイスプロパティ > システム時間** を選択して、[システム時間]ウィンドウを使用します。

UC500、Cisco 800シリーズルータを管理する場合

時刻および夏時間は、ネットワーク デバイス上で手動で設定することもできますが、NTP サーバからの時刻の更新をデバイスが要求するよう NTP を設定することも、デバイスの時刻を PC 時刻や特定のデバイス上のシステムの時刻と同期させることもできます。これらの作業を行うためには、**設定 > デバイスプロパティ > システム時間** を選択し、[システム時間]ウィンドウを使用します。

ユーザ アクセスの管理

パスワード単独、またはユーザ名とペアになったパスワードを設定することによって、Configuration Assistant へのアクセスを管理できます。また、パスワードとユーザ名に特権レベルを関連付けて、ユーザごとのアクセスを管理することもできます。

- 特権レベル 15 では、読み取り/書き込みアクセスが与えられます。このレベルのユーザは、Configuration Assistant 内のすべてのオプションを表示して設定することができます。
- 特権レベル 1 から 14 では、読み取り専用アクセスが与えられます。デバイスの設定を変更できる機能バー、ツールバー、ポップアップ メニュー、および機能ウィンドウのオプションは表示されません。

パスワードを設定してユーザ名と特権レベルに関連付けるには、**設定 > デバイスプロパティ > ユーザとパスワード** を選択して[ユーザとパスワード]ウィンドウを使用します。

HTTP ポート番号の変更

Configuration Assistant は、HTTP または HTTPS ポート経由でコミュニティ内の各デバイスに接続します。HTTP ポート番号は変更できますが、HTTPS ポートは変更できません。常にデフォルトの 443 が使用されます。

注：HTTPS を使用する場合の要件については、「HTTPS の使用」を参照してください。

コミュニティ内のすべてのデバイスの HTTP ポート番号を変更するには、**設定 > デバイスプロパティ > HTTPポート** を選択して、[HTTPポート]ウィンドウを使用します。

SNMP の管理

SNMP の管理には、次の作業が含まれます。

- スタンドアロン スイッチの SNMP の無効化または有効化
- システム オプションの設定
- コミュニティ ストリングの追加および削除
- トラップ マネージャの追加および削除
- ユーザのグループにアクセスできる MIB オブジェクトのビューの作成
- ビューとそれらにアクセスできるグループとの関連付け
- グループとそれらに属するユーザとの関連付け

これらの作業を行うには、**設定 > デバイスプロパティ > SNMP** を選択して [SNMP管理]ウィンドウを使用します。

実行中の設定の保存

ネットワーク デバイスが実行中の場合、コンフィギュレーション設定のセットが 2 つあります。1 つは起動用設定であり、フラッシュ メモリに保存されます。もう 1 つはネットワーク デバイスの実行中の設定であり、RAM に保存されます。デバイスでは、実行中の設定を使用して、デバイスの動作が指定されます。実行中の設定に変更を加えると、直ちに変更が有効になります。ところが、起動用設定に変更を加えたときは、デバイスを再起動した場合にだけ変更が有効になります。

Configuration Assistant を使用すると、実行中の設定を起動用設定として保存できます。これにより、実行中の設定に加えた変更が固定の設定になります。**設定 > 設定の保存** を選択するか、ツール バー上の　をクリックして、[設定の保存]ウィンドウを使用します。

注：実行中の設定を保存しても、[トポロジ]ビューで行った変更は保存されません。[トポロジ]ビューの設定は、**トポロジレイアウトの保存** を選択することによって保存できます。

DHCP サーバの設定

Dynamic Host Configuration Protocol（DHCP）IP アドレス プールは、DHCP サーバからクライアント デバイスに動的に発行される IP アドレスの範囲です（[設定]>[テレフォニー]>[音声]>[ネットワーク パラメータ]ウィンドウを使用して、音声用に DHCP IP アドレス プールを設定できます）。すべてのクラ

イアントが常時接続されているわけではないため、必要に応じて IP アドレスを提供するようにすれば、別の時間に別のクライアントで同じ IP アドレスを再利用できるようになり、1 つのクライアント グループに必要な IP アドレスの数を減らすことができます。

Internet Assigned Numbers Authority（IANA）では、プライベート インターネット用に次の IP アドレス範囲が予約されています。

10.0.0.0 から 10.255.255.255
172.16.0.0 から 172.31.255.255
169.254.0.0 から 169.254.255.255
192.168.0.0 から 192.168.255.255

DHCP IP アドレス プールを管理するには、次の操作を行います。

- プール内の IP アドレスの範囲を識別する DHCP IP アドレス プールを作成します。
- クライアント デバイスの静的 IP アドレスを作成して、プール内の特定の IP アドレスを特定の MAC アドレスにバインドします（クライアントによっては、アプリケーションの実行に必要な接続を維持するために、静的 IP アドレスを使用しなければならないことがあります）。
- プール内の特定の IP アドレスの例外を作成して、それらのアドレスが DHCP サーバによってクライアントに割り当てられないようにします（範囲内のいくつかの IP アドレスが他のプロセスで割り当てられている可能性があります。競合を避けるには、それらのアドレスをプールから除外します）。

プールの範囲は、ネットワーク番号とサブネット マスクから算出されます。すべての使用可能なノードレベルの IP アドレスがプールに含まれ、それらのアドレスは、MAC アドレスに明示的にバインドされたり、プールから除外されていない限り、サーバで使用できます。サーバでは、バインドされているアドレスと除外されているアドレスは無視されます。

これらの作業を行うには、**設定 > DHCPサーバ** を選択します。

関連リンク

- *Dynamic Address Allocation and Resolution*

インターネット接続の設定

このウィンドウでは、インターフェイスにインターネット接続を設定できます。

PPPoE を有効にすることができます。PPPoE は、共有イーサネット インターフェイス上の複数のホストが、1 つまたは複数のブリッジ モデムを経由して複数の宛先に PPP セッションを開く場合に使用できます。

インターフェイスは、静的 IP アドレス、DHCP サーバから取得したアドレス、またはネゴシエートされた IP アドレスを使用するように設定することもできます。ネゴシエートされた IP アドレスを選択した場合、ルータでは、Point-to-Point Protocol/IP Control Protocol（PPP/IPCP; ポイントツーポイント プロトコル/IP コントロール プロトコル）アドレス ネゴシエーションを通じて IP アドレスが取得されます。

これらの作業を行うには、**設定 > インターネット接続** を選択します。

ポートの管理

ポートの設定

デフォルトでは、スイッチ上のすべてのポートは有効になっており、ポートのパラメータは初期値に設定されています。[ポート設定]ウィンドウにはこれらの値が表示され、このウィンドウでこれらの値を変更できます。[ポート設定]ウィンドウを表示するには、**設定 > ポート > ポート設定** を選択します。

一部のポート タイプでは、コンフィギュレーション設定が自動的にネゴシエートされます。自動ネゴシエーションの不一致は、次の状況下で発生します。

- 手動で設定したデュプレックスのパラメータが接続ポート上の設定と異なる場合
- ポートが自動ネゴシエーションに設定されており、接続ポートが自動ネゴシエーションなしで全二重に設定されている場合

ファスト イーサネット ポート上の不一致の結果として、パフォーマンスの低下またはリンク エラーが発生します。ギガビット イーサネット ポート上の場合はリンクが立ち上がらず、統計が報告されません。

不一致状態のポート設定を修正するには、次のいずれかの操作を実行します。

- スピードとデュプレックスの両方に対して自動ネゴシエートするように両方のポートを設定します。
- 接続の両端のポートにスピードとデュプレックスのパラメータを手動で設定します。

注：自動ネゴシエートしないリモートのファスト イーサネット デバイスに接続する場合は、ローカル デバイス上のデュプレックスを[自動]以外の値に明示的に設定する必要があります。スピードのネゴシエーションは、他方のデバイスが自動ネゴシエートしない場合でも機能します。自動ネゴシエートしないリモートのギガビット イーサネット デバイスに接続する場合は、ローカル デバイス上で自動ネゴシエーションを無効にし、デュプレックスおよびフロー制御のパラメータをリモート デバイスに対応するように設定します。

テレフォニーの設定

音声の設定

音声は、Internet Protocol（IP; インターネット プロトコル）のテレフォニー通信や、コールのルーティングとシグナリングなどの、一連のコンポーネントで構成されます。

以下の音声機能を設定できます。

- [デバイス]
- [システム]
- [ネットワーク]
- [自動音声応答とボイスメール]
- [SIPトランク]
- [音声機能]
- [ダイヤルプラン]
- [ユーザ]

ハードウェア デバイスの設定が検出され、表示されます。アプリケーションでは、修正可能な設定パラメータが、ルータのハードウェア設定に基づいて制限されます。

[デバイス]

[デバイス]タブを使用して、次の設定を行います。

- 音声システムのタイプ。PBX またはキーシステム。
- 接続のタイプおよび PSTN のチャネル シグナリング。

[システム]

[システム]タブを使用して、市内電話の次の設定を行います。地域、電話の言語、ボイス メールの言語、言語ファイルの場所、日時の形式、およびシステム メッセージ。[システム]タブを使用して、市内短縮ダイヤル番号も設定します。

頻繁に呼び出される番号のリストを、すべての電話に対して作成できます。電話のユーザは、短縮ダイヤル番号のリストを使用して、番号をすばやくダイヤルできます。短縮ダイヤルのエントリは、追加、編集、削除できます。リストのエントリを上下に移動して、リストされた順に電話のディスプレイに表示できます。最大 32 の頻繁に呼び出される番号を、リスト内で定義できます。

[ネットワーク]

[ネットワーク]タブを使用して、次の設定を行います。

- 音声 VLAN の番号
- 音声用 DHCP プールの情報
- CME（Cisco Unified Communications Manager Express）の IP アドレス

[自動音声応答とボイスメール]

[自動音声応答とボイスメール]タブを使用して、PSTN から UC 500 シリーズ システムに着信する通話処理を設定します。

AA（自動音声応答）の内線番号を設定し、スクリプトを選択できます。スクリプトを使用して Cisco Unity Express の自動音声応答をカスタマイズします。スクリプトは入力内容を受け取り、タスクを実行します。デフォルトの自動音声応答スクリプトは、Cisco Unity Express で使用されるものと同じです。これは、システム ディレクトリ内にあり、ダウンロード、コピー、アップロードできません。このデフォルトの自動音声応答スクリプトは、システム スクリプトまたはシステム AA とも呼ばれます。デフォルトのスクリプトは、内線番号によるダイヤル、ユーザ名によるダイヤル、および呼び出しオペレータ機能などの基本的な機能をサポートしています。スクリプトは、休日リストおよび営業時間のスケジュールをサポートしています。呼び出しが自動音声応答に切り替わると、今日現在が休日かどうかが確認されます。休日の場合、AAHolidayPrompt.wav と呼ばれる休日プロンプトが再生されます。そのプロンプトでは「本日は営業しておりません。恐れ入りますが、おかけ直しください」と伝えられます。今日が休日でない場合、営業時間内かどうかが確認されます。営業時間内の場合、AABusinessOpen.wav プロンプトが再生されます。このファイルには、何も入っていません。営業時間外の場合、

AABusinessClosed.wav プロンプトが再生されます。そのプロンプトでは、「本日の営業は終了しました。恐れ入りますが、おかけ直しください」と伝えられます。

別の選択肢として、aa_transfer.aef スクリプトがあります。このスクリプトを選択した場合、スクリプト パラメータを設定して通話を転送します。

このタブを使用して、ボイス メールを内線および PSTN 番号につなげるよう設定します。

[SIPトランク]

トランク インターフェイスでは、ゲートウェイが時分割多重信号方式によって PSTN や他の外部装置とどのように通信するかを指定します。[SIPトランク]タブを使用して、次の設定を行います。

- SIP パラメータ:サービス プロバイダ、レジストラ サーバ、プロキシ サーバおよび MWI サーバ
- ダイジェスト認証
- DNS

[音声機能]

[音声機能]タブを使用して、次の設定を行います。

- 保留音
- インターコム
- 一斉同報
- ハント グループ
- ピックアップ グループ
- 発信者の ID ブロック
- コール パーク
- マルチパーティの会議

[ダイヤルプラン]

[ダイヤルプラン]タブを使用して、次の設定を行います。

- 国際通話および国内通話の発信通話ダイヤル プラン
- すべてのシステムの内線番号の桁数
- 緊急電話番号
- 着信通話がアナログの FXO で受信された際の処理
- PSTN および DID コールを内線番号と照合するダイヤルイン サービス
- すべての着信 FXO コールのリダイレクト先:
    - 自動音声応答
    - 基本自動着信呼分配(B-ACD)アプリケーション
    - オペレータ
    - ハント グループ
    - カスタム設定の作成
- DID 番号

[ユーザ]

各電話に対して、[ユーザ]タブを使用して次の設定を行います。

- ユーザ名
- ユーザ ID
- パスワード
- 電話ごとの複数の内線番号
- 共有回線
- オーバーレイ
- 内線の監視

シスコ電話サポート

Cisco Configuration Assistant は、SIP（セッション開始プロトコル）を実行する 3951 電話または 3911 電話の設定をサポートします。3951 電話および 3911 電話は同一です。ただし、3951 電話はディレクトリ回線を 2 つサポートし、3911 電話はディレクトリ回線を 1 つサポートします。（Cisco Configuration Assistant はサードパーティ製の SIP 電話をサポートしません。）

Cisco Configuration Assistant でサポートされるその他の IP 電話は、シスコ専用のプロトコル SCCP（Skinny Client Control Protocol）を使用します。Cisco Configuration Assistant 1.5 では、SCCP 電話での SIP の実行をサポートしていません。どちらの電話のタイプも同じ方法で管理されますが、これらの機能は SIP の次の操作を実行する際にはサポートされません。

- 自動登録
- 二重回線
- キーシステム

電話ユーザのパスワード

[音声]ウィンドウの[ユーザ]タブでは、パスワード フィールドが次の項目に適用されます。

- SCCP 電話：CME、Cisco Unity Express GUI、および IMAP（Internet Message Access Protocol）
- SIP 電話：CUE GUI および IMAP

パスワード フィールドはオプションです。パスワードの長さは、3 ～32 文字です。スペースは使用できません。パスワードに使用できる文字は、小文字の a ～ z、大文字の A ～ Z、数字の 0 ～ 9 および次の記号です。- , . + = _ ! @ # $ ^ * ( ) ? / ~ < > & %。パスワードを忘れた場合、ユーザ ID フィールドを編集すると、古いユーザ ID が削除され、新しいユーザ ID が新しい値で作成されます。（CUE は、ユーザ ID の変更をサポートしません。）すでにパスワードを指定してあるユーザが、自分のユーザ ID を修正した場合、新しいユーザ ID のパスワードの設定は行われません。

SCCP 電話のパスワード フィールドには、既に設定済みの場合、実際のパスワードが自動的に表示されます。SIP 電話のパスワード フィールドは常に空白ですが、これはパスワードが設定されていないということではありません。

電話のロード

Cisco 3951 および 3911 SIP 電話の電話ロード ファイルは、ソフトウェア アップグレード TAR 書庫に含まれていないことがあります。この場合には、ファイルを Cisco.com からダウンロードして、デバイスにアップロードできます。IP Phone をデバイスに登録する際に、電話がロード ファイルを要求するように設定されている場合、電話ロード ファイルが電話にダウンロードされます。電話ロード（ファームウェア）ファイルをアップロードするには、ファイルをトポロジ マップのデバイス アイコンにドラッグします。電話ロード ファイルはデバイスのフラッシュ メモリにアップロードされます。

これらのいずれかの作業を行うには、**設定 > テレフォニー > 音声** を選択します。

推奨される参考資料：『Cisco CallManager Fundamentals』SBN-10:1-58705-008-0; ISBN-13: 978-1-58705-008-4.

関連リンク

- *Telephony Signaling*

IP ルーティングの設定

静的ルーティング

ルータの静的ルーティング テーブルには、静的ルートを追加できます。静的ルートは、デバイスの静的ルーティング テーブルに固定的に登録されるため、設定する静的ルートはいずれも、削除または置換するまでルーティング テーブルに保持されます。静的ルートはすべての動的ルートより優先されます。また、パケットのパスが即時に確定されるため、処理時間も短縮されます。動的ルートは、デバイスで RIP などの IP ルーティング プロトコルを使用して認識されます。静的ルートより処理に時間がかかり、リフレッシュされない場合は、期限切れとなってルーティング テーブルから削除されます。

静的ルーティング テーブルでは、静的ルート情報を追加または削除して管理します。

これらの作業を行うには、**設定 > ルーティング > 静的ルーティング** を選択します。

ネットワークの監視

ここでは、ネットワーク上のデバイスを監視する方法について説明します。

このセクションの内容は、次のとおりです。

- **レポートとグラフの表示**
  管理対象デバイスのインベントリ、無線および無線クライアントに関するレポート、帯域幅のグラフ、リンクのグラフなど、さまざまな種類のレポートおよびグラフを表示するためのタスクに関する情報を示します。
- **ネットワークの表示**
  ネットワーク上のデバイスを[前面パネル]ビューおよび[トポロジ]ビューに表示するためのタスクに関する情報を示します。
- **ネットワークの状態の確認**
  [状態]機能について説明し、ネットワーク上のデバイスの状態の測定値を表示するウィンドウへのリンクを示します。
- **ネットワーク イベントの管理**
  [イベント通知]機能について説明し、Configuration Assistant からユーザに通知されるイベントを表示するウィンドウへのリンクを示します。
- **システム メッセージの表示**
  [システムメッセージ]機能について説明し、ネットワーク上のデバイスから発行されたシステム メッセージを表示するウィンドウへのリンクを示します。

レポートとグラフの表示

インベントリ

コミュニティのインベントリ(デバイス タイプ、シリアル ナンバー、IP アドレス、およびソフトウェア リリース)、または 1 つのデバイスのインベントリを表示するには、**モニタ > レポート > インベントリ** を選択します。[インベントリ]ウィンドウ(読み取り専用)にインベントリが表示されます。

デバイスのインベントリを変更するには、**設定 > デバイスプロパティ > SNMP** を選択し、[システム オプション]タブで変更を行います。

VPN のステータス

Virtual Private Network(VPN; バーチャル プライベート ネットワーク)トンネルのリモート エンドのデバイスを監視できます。

在宅勤務者が企業のネットワークにアクセスできるようにして、他のクライアントからはインターネットだけにアクセスできるように制限することを、「スプリット トンネリング」と言います。この場合、特定の PC だけが VPN トンネル経由で企業のネットワークにアクセスでき、トンネル経由で企業のネットワークにアクセスできて、他の PC はインターネットにしかアクセスできません。このソリューションは企業の営業所でも使用されます。その場合、インターネットにはすべての PC がアクセスできますが、各ユーザが VPN を使用するときには IEEE 802.1x に基づく認証が要求されます。

IP Security（IPSec; IP セキュリティ）トンネルは常時稼動し、802.1x に基づいて、リモート サイトから企業のネットワークにアクセスしようとする企業ユーザを認証します。リモート ルータでは、Port Address Translation（PAT; ポート アドレス変換）機能を使用してリモート サイトのすべての PC のアドレスが変換されます。VPN クライアント モードでは、企業のネットワークへのアクセスが試みられると、IPSec トンネルの接続時に VPN サーバから IPSec ポリシーが「プッシュ」され、企業ネットワーク上の単一のアドレスがリモート ルータに渡されます。リモートの企業 PC が VPN トンネル上で中央サイトにアクセスすると、その IP アドレスが「プッシュされた」企業アドレスにポート アドレス変換されます。同様に、インターネット アクセス専用に使用される PC の IP アドレスも、リモート ルータのパブリック インターフェイス IP アドレスにポート アドレス変換されます。パブリック インターフェイス IP アドレスは、インターネット サービス プロバイダから動的に割り当てられます。

リモートの VPN トンネルのステータスを表示するには、**モニタ > レポート > VPNステータス** を選択します。

ネットワークの表示

[前面パネル]ビュー

このビューは、次のいずれかの操作により表示されます

- Configuration Assistant に接続したときに[前面パネル]ビューが開くよう、[環境設定]ウィンドウで指定する。
- 機能バー上で **モニタ > ビュー > 前面パネル** を選択する。
- ツールバー上で  を選択する。

このビューには、相互に関連する次の 2 つの部分があります。左フレームと右フレームです。これらを使用してデバイスの選択およびポートの選択を実行することにより、設定を確認したり変更したりできます。ビュー内のデバイスの配列が適切でない場合は、これを変更できます。変更が適用されたことを確認するには、ビューを更新します。

左フレーム

左フレームは、ツリー構造になっており、コミュニティ名の下にメンバ デバイスがインデントされて表示されます。各デバイス名の横にはチェックボックスが付いています。このチェックボックスをオンにすると、右フレームに、そのデバイスの前面パネルが表示されます。

注：ルータ、アクセスポイント、および不明デバイスの前面パネルを表示することはできません。

ツリー構造では、デバイスのステータスが次の色で示されます。

- 緑 — デバイスは接続され、動作しています。
- 黄色 — 障害状態が検出されています（デバイスのアイコンにマウス ポインタを置くと、障害状態に関するメッセージが表示されます）。
- 赤 — デバイスがダウンしているか、接続されていません。

右フレーム

右フレームには、左フレームで選択したデバイスが表示されます。ワイヤリング クローゼット内にいるかのように、デバイスのポートおよびモジュール スロットを確認できます。

表示される情報の種類は、前面パネルの左端にあるモード ボタンをクリックすると制御できます。クリックするたびに、ポートまたはデバイスについてのさまざまな情報が、ポートの色と状態（点滅しているか、いないか）によって示されます。

各モードでのポートの色の意味については、凡例をクリックして、凡例を参照してください（凡例は、ツールバー上の  をクリックするか、[ヘルプ]ウィンドウの[目次]タブで[凡例]トピックをクリックすると参照できます）。

デバイスの選択

次の 2 つの方法でデバイスを選択できます。

- 選択するデバイスの前面パネルをクリックする。
- ツリー構造からデバイスのアイコンを選択する。

デバイスをクリックすると、そのデバイスの周囲が黄色の線で囲まれます。これは、そのデバイスが選択されていることを示します。複数のデバイスを選択するには、**Ctrl** キーを押したまま、選択するデバイスをクリックしていきます。デバイスの選択を解除するには、**Ctrl** キーを押したまま、選択を解除するデバイスをクリックします。

デバイスのグループを選択してから、そのうちの 1 つのデバイスを右クリックすると、ポップアップ メニューを表示できます。このポップアップ メニューを使用して、デバイスの設定を確認したり変更したりします。ポップアップ メニューのオプションは、選択したデバイスだけに適用されます。機能バーのオプションを使用して、デバイスの設定の確認または変更を実行することもできます。機能バーのオプションを、選択したデバイスに適用できない場合は、選択は無視されます。

ポートの選択

次の表は、ポートの選択方法を示しています。

目的	操作
単一ポートの選択	ポートをクリック、または右クリックします。右クリックした場合は、ポップアップ メニューが表示されます。
デバイス上のすべてのポートの選択	任意のポートを右クリックして、ポップアップ メニューから[すべてのポートを選択]を選択します。
同一デバイスまたは異なるデバイス上の複数のポートの選択	次のいずれかの方法を使用します。 • **Ctrl** キーを押しながら、選択するポートをクリックします。 • ラバーバンドを使用してポートを選択します。つまり、マウス ボタンを押したままドラッグして、選択するポートのグループを四角形で囲みます。**Ctrl** キーを押したまま実行すると、隣接していないポートのグループをラバーバンドで選択できます。

注：WLAN コントローラ上のポートは選択できません。

ポートの選択を解除するには、**Ctrl** キーを押しながら、選択を解除するポートをクリックします。

単一ポートの選択時に右クリックを使用すると、ポップアップ メニューが表示されます。複数のポートを選択するときにポップアップ メニューを表示するには、ポートの 1 つを右クリックする必要があります。このポップアップ メニューを使用して、ポートの設定を確認したり変更したりします。ポップアップ メニューの項目は、選択したポートだけに適用されます。機能バーの項目からも、ポートの設定を確認したり変更したりできます。機能バーの項目を、選択したポートに適用できない場合は、選択は無視されます。

[前面パネル]ビューの調整

デバイスの順序を変更して、ワイヤリング クローゼット内の物理的な設定を反映させることができます。デバイスの配置を変更するには、ツリー構造内のデバイスのアイコンを新しい位置にドラッグします。

ビューの更新

[前面パネル]ビューを更新するには、ツールバー上の[更新]アイコン をクリックします。この操作は、コミュニティ内に変更が加えられたことがわかっていて、その変更を直ちに確認する場合に便利です。

[トポロジ]ビュー

このビューは、次のいずれかの操作により表示されます

- Configuration Assistant を管理対象のデバイスに接続する。
- 機能バー上で **モニタ > ビュー > トポロジ** を選択する。
- ツールバー上で をクリックする。

このビューでは、管理対象デバイスのトポロジおよび接続を確認できます。このビューの ツールバー、左フレーム、および右フレームを使用して、ビューを処理したり、ビューを保存したり、デバイスに関する情報をビューに表示したりする作業を実行します。

ツールバー

このビューには固有のツールバーがあります。次の表は、ツールバーのオプションの使用時に、Configuration Assistant によって実行される処理を示しています。

オプション	使用方法
[自動レイアウト]	クリックすると、ビュー内のスペースおよび情報のレイアウトが再調整されます。
[レイアウトの保存]	クリックすると、トポロジ マップ内のデバイスの位置が保存されます。
[トポロジオプション]	クリックすると、[トポロジオプション]ウィンドウが開きます。このウィンドウでは、ビューの表示内容を制御できます。たとえば、[情報の表示]タブのチェックボックスを使用することにより、リンクおよびノードに関して表示する情報量を制御できます。
ズーム調整	ビューの起動時は常に、右フレームは 100% の倍率で表示されます。縮小

	表示するには、次の手順に従います。 • [-]拡大縮小アイコンをクリックするか、適切な倍率になるまで押し続けます。 • キーボード上の「-」を押します。 • ドロップダウン リストから低い倍率を選択します。 • テキスト フィールドに 100 未満の数値を入力します。 拡大表示するには、次の手順に従います。 • [+]拡大縮小アイコンをクリックするか、適切な倍率になるまで押し続けます。 • キーボード上の「+」を押します。 • ドロップダウン リストから高い倍率を選択します。 • テキスト フィールドに大きな数値（最大 100）を入力します。

注：最初の 3 つのオプションは、右フレームの灰色の領域を右クリックすると表示されるメニューから選択できます。

左フレーム

左フレームはツリー構造になっています。このツリーでは、コミュニティの名前を持つノードと、各コミュニティ メンバの下位ノードが展開表示されます。コミュニティ メンバの隣接デバイスのノードも表示されます。

スタンドアロン デバイスの場合、ツリーには、そのデバイスのノードおよび隣接デバイスのノードが表示されます。

マウスを使用せずに操作する場合は、**Tab** キーを使用してツリーを選択し、上下の矢印キーでツリー内を移動します。

ツリー ビュー内でデバイスを選択すると、対応するデバイスが右フレーム内で選択され、そのデバイスが表示されるように自動的にフレームがスクロールされます。

デバイスの色

ツリーには、デバイスのステータスが次の色で示されます。

	接続され、動作しています。
	ダウンしているか、接続されていません。
	不明。

ポップアップ ウィンドウの使用

デバイスを右クリックするか、Shift キーを押しながら F10 キーを押すと、ポップアップ ウィンドウが表示されます。ポップアップ メニューは、ホスト名の変更や、帯域幅グラフの表示など、デバイスで実行できる作業のリストです。このポップアップ ウィンドウは、右フレーム内でデバイスを右クリックすると表示されるものと同じです。

右フレーム

右フレームはトポロジ マップになっています。デバイス間のリンクおよびリンク情報が示されます。右フレームにも、左フレームと同じ次のルールが適用されます。

- 表示される内容は、コミュニティとスタンドアロン デバイスのどちらを管理しているか、および[トポロジオプション]ウィンドウで隣接デバイスを表示するようにしているかどうかで異なります。
- ポップアップ ウィンドウを使用して、選択したデバイスに作業を実行できます。このフレームでは、ビューを処理するデバイス固有の作業も実行できます。
- デバイスのステータスも左フレームと同じ色で示されます。

作業

次の表は、このビューから開始できる作業と、その実行方法を示しています。

作業	実行方法
レイアウトの再配置	ビュー内のデバイス、リンク、および情報を見やすくするには、次の手順を実行します。 • デバイスを任意の位置までドラッグします。 • ラバーバンドを使用して、移動するデバイスをグループとして選択します。つまり、マウス ボタンを押したままドラッグして、移動するデバイスのグループを四角形で囲みます。1 つのデバイスをドラッグすると、すべてのデバイスがドラッグされます。
デバイスおよびリンク情報の表示	デバイスまたはリンクのプロパティを表示するには、デバイスまたはリンクを右クリックまたはダブルクリックして、ポップアップ メニューから[プロパティ]を選択します。デバイスのプロパティとしては、デバイス名、タイプ、IP アドレス、MAC アドレス、およびデバイス上で実行されている Cisco IOS リリースが表示されます。リンクのプロパティとしては、接続されているポートの識別情報、およびリンクの状態が表示されます。 デバイスで使用されている帯域幅を監視するには、デバイスを右クリックまたはダブルクリックして、ポップアップ メニューから[帯域幅グラフ]を選択します。リンクの使用状況を監視するには、リンクを右クリックまたはダブルクリックして、ポップアップ メニューから[リンク グラフ]を選択する。
VLAN の表示	コミュニティを管理している場合は、トポロジ マップ上に VLAN リンクを表示できます。 をクリックして[トポロジオプション]ウィンドウを開き、[VLANの表示]タブを使用します。
コミュニティメンバの追加および削除	コミュニティにメンバを追加するには、任意の候補を右クリックまたはダブルクリックして、ポップアップ メニューから[コミュニティに追加]を選択します。次に、表示されたウィ

	ンドウを使用します。 コミュニティからメンバを削除するには、任意のデバイスを右クリックして、ポップアップ メニューから[コミュニティから削除]を選択します。次に、表示されたウィンドウを使用します。
ビューの更新	Configuration Assistant は、管理対象のデバイスを定期的にポーリングして、デバイスが削除または追加された場合に、ネットワーク マップを再表示します。変更が加えられたことがわかっていて、次のポーリングの前にその変更を確認する場合は、ツールバーの  をクリックします。 **注**:ポーリング間隔を変更するには、[環境設定]ウィンドウを使用します。
ホスト名の変更	デバイスを右クリックして、ポップアップ ウィンドウから[ホスト名]を選択し、[ホスト名]ウィンドウを使用します。
オブジェクトとリンクへの注釈付け	「注釈」と呼ばれるテキスト フィールドを、デバイスとネットワーク クラウドの下や、リンクのエンド ポイントに追加できます。注釈は、トポロジ マップ上に表示されない説明的な情報を表示するために役立ちます。 ネットワーク クラウドやリンクを追加すると、[注釈]ウィンドウが開きます。マップ上にすでに存在するデバイスに注釈を付けるには、そのデバイスを右クリックして、ポップアップ ウィンドウから[注釈]を選択し、[注釈]ウィンドウを使用します。 [トポロジ]ビューの注釈を非表示にする場合は、[トポロジオプション]ウィンドウを開き、[情報の表示]タブの[注釈]チェックボックスをオフにします。
ソフトウェアのアップグレード	ソフトウェアイメージ ファイルを、PC からドラッグして、デバイスのアイコンにドロップします(デバイスはコミュニティ メンバであることが必要です)。このファイルは、マップされたドライブ、ネットワーク ドライブ、またはローカル ドライブ上に保存しておきます。 複数のデバイスで一度にソフトウェアをアップグレードするには、**メンテナンス > ソフトウェアアップグレード** を選択し、[ソフトウェアアップグレード]ウィンドウを使用します。
ネットワーククラウドの追加	トポロジ マップの背景を右クリックし、ポップアップ ウィンドウから[ネットワーククラウドの追加]を選択します。表示された[注釈]ウィンドウでクラウドにラベルを付け、任意のマップ領域にドラッグします。 ラベルを変更したり、クラウドを削除するには、対象を右クリックして、メニューから操作を選択します。
リンクの追加	手動でリンクをマップに追加できます。リンク元のノードをポイントして **Ctrl** キーを押しながらクリックし、リンク先のノードをポイントして **Ctrl** キーを押しながら再度クリックします。いずれかのノードを右クリックして、ポップアップ ウィンドウから[リンクの追加]を選択します。ノード間にリンクが作成され、[注釈]ウィンドウが表示されます。そのウィンドウのフィールドで、リンクのエンド ポイント用のラベルを入力します。

ネットワークの状態の確認

ダウンタイムが発生しないように、またネットワークが効率よく稼働するように、さまざまなデバイスの状態測定値を監視できます。これらの測定値によって、帯域幅、PoE（Power over Ethernet）、CPU、およびメモリの使用状況、およびデバイスの温度とパケット エラーの割合がわかります。

状態の測定値を確認するには、**モニタ > 状態** を選択して、[状態]ウィンドウを使用します。

Configuration Assistant には、状態の測定値以外に、次のような特定のリソースの使用に焦点を置く機能があります。

- PoE使用率についての詳細は、**設定 > ポート > ポート設定** を選択し、[ポート設定]ウィンドウを使用します。
- 帯域幅使用率についての情報は、**モニタ > レポート > 帯域幅グラフ** を選択し、[帯域幅グラフ]ウィンドウを使用します。
- リンクの使用状況についての情報は、**モニタ > レポート > リンクグラフ** を選択して、[リンクグラフ]ウィンドウを使用します。
- パケット エラーについての情報は、**モニタ > レポート > ポート統計情報** を選択して、[ポート統計情報]ウィンドウを使用します。

ネットワーク イベントの管理

イベントは、Configuration Assistant によって検出されて、ユーザに通知される状態です。イベントの例は、次のとおりです。

- 高いデバイス温度
- ファンが故障しているデバイス
- 管理上無効なポート
- デュプレックスの不一致があるポート
- スマートポートを使用して設定できるポート
- ネットワーク内の不明なデバイス

ユーザにイベントを認識させるために、Configuration Assistant からポップアップ メッセージが表示されます。また、ステータス バーと[トポロジ]ビューでは、イベントが発生したデバイスの横に、クリック可能なイベント アイコンが表示されます。[トポロジ]ビュー内のイベント アイコンにマウスのポインタを置くと、そのイベントの要約が表示されます。

アイコンの外観はイベントのタイプによって異なります。イベントのタイプは番号によって区別されます。タイプ番号が小さいほど、処置を施す必要性が高まります。次の表は、すべてのイベント アイコンと、それらのアイコンが表すタイプ番号を示しています。

アイコン				
タイプ	0 および 1	2 および 3	4	5、6、および 7

Configuration Assistant で複数のイベントが検出された場合、[トポロジ]ビューにすべてのイベントのアイコンが表示されます。ステータス バーには、最も緊急性の高いイベントのアイコンだけが表示されます。

イベント アイコンをクリックすると、[イベント通知]ウィンドウが表示されます。**モニタ > イベント通知**を選択して、このウィンドウを直接開くこともできます。

[イベント通知]ウィンドウには、ネットワークで検出されたイベントの詳細が表示されます。このウィンドウを使用する目的は、次のとおりです。

- イベントを認識したことを Configuration Assistant に伝達する。
- 可能な場合、Configuration Assistant を使用して処理を実行する。
- スイッチのアラート LED をオフにする。

システム メッセージの表示

[システムメッセージ]ウィンドウでシステム メッセージを表示できます。機能バーから **モニタ > システムメッセージ** を選択してウィンドウを開きます。システム エラー メッセージを表示する前に、このウィンドウ内のボタンを使用して、これらのメッセージをフィルタリングする条件を設定できます。

ネットワークの管理

ここでは、ネットワーク上のデバイスの管理方法について説明します。

このセクションの内容は、次のとおりです。

- **ソフトウェアのアップグレード**
  [ソフトウェアアップグレード]機能について説明し、個別またはすべての管理対象デバイスのアップグレードに使用するウィンドウへのリンクを示します。
- **ファイルシステムの管理**
  [ファイル管理]機能について説明し、デバイス上のファイルシステムの詳細を表示したり、必要に応じてファイルまたはディレクトリを削除して必要な領域を確保したりする場合に使用するウィンドウへのリンクを示します。
- **コンフィギュレーションの保存**
  [設定の保存]機能について説明し、個別またはすべての管理対象デバイスの起動用設定のバックアップおよび復元に使用するウィンドウへのリンクを示します。
- **デバイスのリロード**
  [システムのリロード]機能について説明し、個別またはすべての管理対象デバイスの再起動に使用するウィンドウへのリンクを示します。

ソフトウェアのアップグレード

CE520 スイッチを管理する場合

次のいずれかの方法で、コミュニティ内のデバイス上のソフトウェアをアップグレードできます。

- ソフトウェアイメージ ファイルをローカル ドライブ、マップ ドライブ、またはネットワーク ドライブからドラッグし、[トポロジ]ビューのスイッチ アイコン上にドロップします。この手順によって、一度に 1 つのデバイス上のソフトウェアがアップグレードされます。
- **メンテナンス > ソフトウェアアップグレード** を選択して、[ソフトウェアアップグレード]ウィンドウ を使用します。複数のデバイスを選択して、選択したデバイスすべてを一度にアップグレードできます。

いずれの場合でも、tar バージョンのアップグレード イメージを使用してください。これらのファイルには、アップグレードに必要なソフトウェア イメージと管理コードが含まれています。

Cisco.com からソフトウェアをダウンロードするには、このトピックの下にある[関連リンク]の下に表示されているリンクを使用します。

関連リンク

- *Download Software, Support*

UC500 を管理する場合

次のいずれかの方法を使用して、デバイスのソフトウェアをアップグレードします。

- Cisco IOS イメージ、音声ファイル（拡張子は .wav または au）、または電話ファームウェア ファイルをローカル ドライブ、マップ ドライブ、またはネットワーク ドライブからドラッグして、[トポロジ]ビューのコミュニティ メンバ上にドロップします。TFTP サーバは必要ありません。
- **メンテナンス > ソフトウェアアップグレード** を選択して、[ソフトウェアアップグレード]ウィンドウ を使用します。複数のコミュニティ メンバを選択して、それらの Cisco IOS イメージまたは CUE ソフトウェアをアップグレードできます。

注：CUE ソフトウェアの場合は、Cisco IOS イメージの tar バージョンおよび CUE パッケージ ファイルを使用します。

[ソフトウェアアップグレード]ウィンドウを使用して Cisco IOS イメージをアップグレードする場合、アップグレード イメージがローカルに保存されている場合は、標準モードでアップグレードします。アップグレード イメージがリモートに保存されている場合は、リモート TFTP サーバ モードでアップグレードします。

標準モードでのアップグレード

標準モードでは、TFTP サーバは必要ではありません。標準モードを使用するには、まずイメージを Cisco.com からお使いの PC またはワークステーションにダウンロードする必要があります。ダウンロードするには、次の手順に従います。

1. Cisco.com にログインします。
2. Cisco.com の手順に従って tar ファイル（Cisco IOS イメージおよび管理ソフトウェアの組み合わせ）をダウンロードします。

注：ドラッグ アンド ドロップによるアップグレードおよび標準モードの両方で、Configuration Assistant に埋め込まれている TFTP サーバが使用されます。アップグレードしようとするときにお使いの PC でサードパーティ製の TFTP サーバが実行されている場合、埋め込み TFTP サーバは TFTP ポートにアクセスできません。ポートにアクセスできる TFTP サーバは一度に 1 つだけです。

リモート TFTP サーバ モードでのアップグレード

UNIX ワークステーションまたは別の PC 上に専用の TFTP サーバを用意する必要があります。TFTP サーバでは、任意のサードパーティ製 TFTP アプリケーションを実行できます。

次の手順に従います。

1. TFTP サーバとして機能するワークステーションまたは PC の IP アドレスを取得します。Windows NT システムの場合は、DOS コマンド プロンプトに **ipconfig** と入力します。ワークステーションの場合は、プロンプトに **ifconfig -a** と入力するか、/etc/hosts ファイルで検索します。
2. Cisco.com にログインします。
3. Cisco.com の手順に従って tar ファイル（Cisco IOS イメージおよび管理ソフトウェアの組み合わせ）をダウンロードします。

ファイルシステムの管理

UC500、Cisco 800シリーズルータを管理する場合

デバイスが稼働中のネットワークに接続されている間、デバイスのファイルシステムを表示できます。表示されたファイルシステム上で、基本的なファイル管理操作を実行できます。

対象デバイスで使用されているファイルシステムの種類によって操作は異なります。クラス B ファイルシステムでは、ファイルの復元または削除ファイルが使用していたメモリの再利用ができます（これを圧縮 と言います）。クラス B ファイルシステムは、ごみ箱機能を持つ GUI オペレーティング システムにやや似ており、削除ファイルは、消去されるまでメモリから完全に削除されません。

クラス C ファイルシステムでは、メモリを再利用する必要がなく、ファイルを削除するとそれで終わりです。ソフトウェアのアップグレードを実行するには、新しいイメージ用に十分なメモリが必要なので、ファイルの削除またはメモリの圧縮が必要な場合があります。

ファイルシステムの詳細を表示するには、**メンテナンス > ファイル管理** を選択して、[ファイル管理] ウィンドウを使用します。

UC500 を管理する場合

いずれのデバイスも、ライブ ネットワークに接続したままの状態で、ファイルシステムを表示できます。これらのファイルシステムでは、基本的なファイル管理操作を実行できます。ソフトウェアのアップグレードを実行する際に、新しいイメージのインストールに十分な空き容量がない場合は、古いイメージを削除して、新しいイメージのための空き容量を確保する必要があることがあります。

ファイルシステムの詳細を表示するには、**メンテナンス > ファイル管理** を選択し、[ファイル管理] ウィンドウを使用します。

設定の保存

異なるネットワーク条件で使用するなどの目的で、デバイス上に起動用設定を保存することがあります。この場合、デバイスまたはコミュニティ内の類似するデバイスに簡単に復元できるバックアップ コピーを作成します。

設定を保存するか保存した設定を復元するには、**メンテナンス > 設定の保存** を選択し、[設定の保存]ウィンドウを使用します。

デバイスの再起動とリセット

コミュニティ内のデバイスを再起動したり、工場出荷時のデフォルトの設定にリセットすることができます。

デバイスを再起動すると、アクティブな設定ファイルが保存され、再起動されます。再起動中はデバイスにアクセスできなくなり、デバイスとそのエンド ステーションとの間の接続が一時的に中断されます。

デバイスをリセットすると、工場出荷時の設定が復元されます。デバイスをリセットしたら、Configuration Assistant を使用して管理する前に再度設定する必要があります。この作業には、デバイスの設定ウィザードを使用できます。

デバイスを再起動またはリセットするには、**メンテナンス > 再起動/リセット** を選択して、[再起動/リセット]ウィンドウを使用します。

ライセンスの管理

UC 500 シリーズ プラットフォームでは、Cisco Software Licensing がサポートされており、フィールドの変更が可能です。物理的に 16 ユーザをサポートする 8 ユーザ用のライセンスを付与されたシステムは、16 ユーザのライセンスにアップグレードできます。物理的に 48 ユーザをサポートする 32 ユーザ用のライセンスを付与されたシステムは、48 ユーザのライセンスにアップグレードできます。ライセンスをダウングレードすることもできます。

IP Phone は、各電話のライセンスの有効性に基づき、登録されます。ライセンスの期限満了またはユーザ設定によりシステム ライセンスがダウングレードされ、登録された電話の数がユーザ ライセンス数を超過すると、システムがリロードされます。

次のソフトウェア ライセンス機能が導入されています。

- 評価ライセンス、拡張ライセンス、永久ライセンス、および猶予期間ライセンスがサポートされています。
- インストールおよび期限満了のイベントは、Software Licensing インフラストラクチャで管理されます。
- ライセンス情報を表示するには、**show license**、**show platform software license**、および **show version** という Cisco IOS CLI コマンドを使用します。
- UC 500 システムをアップグレードするには、**uc500-16u-upgrade** および **uc500-48u-upgrade** という Cisco IOS CLI コマンドを使用します。これらのコマンドのどのバージョンを使用しても、ライセンスが付与された設定をダウングレードすることはできません。
- 拡張ライセンスおよび永久ライセンスをインストールするには、**license install** *license_file* という Cisco IOS CLI コマンドを使用します。

ライセンス タイプの説明

Cisco Configuration Assistant では、以下で説明する 4 つのタイプのライセンスをサポートしています。

評価ライセンス

評価ライセンスは、Cisco IOS イメージにバンドルされた、特定のノードに限定されない従量制のライセンスで、期間限定で有効です。このライセンスは、機能に対して、永久ライセンス、拡張ライセンス、または猶予期間ライセンスがない場合にのみ、使用されます。このライセンスを使用するには、End User License Agreement（EULA; 使用許諾契約書）に同意する必要があります。

拡張ライセンス

拡張ライセンスは、特定のノードに限定された従量制のライセンスで、Cisco Licensing ポータルを介して発行されます。このライセンスのインストールの一部として、EULA に同意する必要があります。

猶予期間ライセンス

猶予期間ライセンスは、特定のノードに限定された従量制のライセンスで、ライセンスを再ホストする許可チケットの一部として、Cisco Licensing ポータルを介して発行されます。これらのライセンスは、再ホスト操作の一部として、デバイスにインストールされます。このタイプのライセンスでは、再ホストの操作の一部として、EULA に同意する必要があります。

永久ライセンス

永久ライセンスは、特定のノードに限定されるライセンスで、関連付けられた使用期間がなく、Cisco Licensing ポータルを介して発行されます。このライセンスのインストールの一部として、EULA に同意する必要があります。

ライセンスを管理するには、**メンテナンス > ライセンス管理** を選択します。

参照トピック

SBCS の概要

Smart Business Communications System（SBCS）では、顧客に対するアクセス、サービス、および維持を包括的に行うことができます。これは、Cisco Unified Communications を小規模企業向けに拡張した、音声、データ、ビデオ、および無線ネットワーク製品のシステムで、24 時間体制での情報への安全なアクセスを含め、顧客および社員間の効率的な通信を実現しています。

フル システムは、次のコンポーネントで構成されています。

- **Cisco Configuration Assistant**：現在使用しているネットワーク管理アプリケーションです。
- **Cisco Monitor Manager および Cisco Monitor Director**：Cisco Monitor Manager は顧客の主要サイトに展開され、5 ～ 250 人のユーザにサービスを提供する、音声およびデータのネットワークに関する重要なデバイス パラメータをアクティブに監視します。Cisco Monitor Director は、お使いのサイト（パートナー サイト）に展開される包括的な管理アプリケーションで、Cisco Monitor Manager と連動して、24 時間体制のアクティブな音声およびデータのネットワーク管理サポートを顧客に提供することができます。
- **Cisco Unified Communications 500 シリーズ プラットフォーム**：統合された音声メッセージング システムと自動音声応答、Cisco Unified IP Phone と PC の有線接続用の 8 つの PoE（Power-over-Ethernet）ポートを提供し、さらに、統合された無線アクセスポイント オプションを通して無線接続を提供する、IP テレフォニー ソリューションです。公衆電話交換網（PSTN）トランク、IP トランク、およびローカル アナログ デバイスをサポートしています。最大 2 人の在宅勤務者に対して、データ、セキュリティ、および無線サービスを提供します。
- **Cisco Catalyst Express 520 スイッチ**：有線および無線のシスコ電話、Wireless Express アクセスポイント、および PC に、追加の PoE ポートを提供することによって、音声およびデータのユーザ数を増やすことを可能にするデバイスです。デスクトップモデルでは 8 つの追加の PoE ポートを提供し、ラックマウント モデルでは最大 24 個の追加 PoE ポートを提供します。
- **Cisco 500 Series Wireless Express アクセスポイント**：2 つの操作モード（スタンドアロン モードおよびコントローラモードの Cisco 521 Wireless アクセスポイント（AP521））で使用可能な、無線 802.11g アクセスポイントです。コントローラモードの AP521 は、Cisco 526 Wireless Express Mobility Controller（WLC526）とのみ連携します。
- **Cisco 500 Series Wireless Express Mobility Controller**：コントローラモードの AP521 を制御および自動設定します。セキュアなゲスト アクセス、Voice over WLAN、最適化された無線カバレッジなど、モビリティ サービスのプラットフォームを提供します。

SBCS コンポーネントの詳細については、次の［関連リンク］を参照してください。

関連リンク

- *Cisco Unified Communications 500 Series for Small Business:* Introduction
- *Cisco Unified Communications Manager Express:* Introduction
- *Cisco Unity Express*: Introduction
- *Cisco Catalyst Express 520 Series:* Introduction
- *Cisco 500 Series Wireless Express Mobility Controllers:* Introduction
- *Cisco 500 Series Wireless Express Access Points:* Introduction

- *Cisco Unified IP Phones 7900 Series:* Introduction

コミュニティに関する制限事項

コミュニティ内のデバイス（Catalyst Express スイッチ、Cisco ルータ、Cisco WLAN コントローラ、および Aironet 自律型アクセスポイント）の合計数は、25 以内である必要があります。

注： Cisco ルータには、Unified Communications 500 シリーズ プラットフォームと 800 シリーズ アクセス ルータが含まれます。

次の表は、デバイスのタイプ別の制限数を示しています。

デバイスのタイプ	制限数
Catalyst Express スイッチ	15
Cisco ルータ	5
Cisco WLAN コントローラ	2
Aironet自律型アクセスポイントと HWIC アクセスポイント	3

注：

- Catalyst Express スイッチは、コミュニティ内のデバイス数の制限値 25 を超えなければ、いくつでも使用できます。
- IP Phone は、コミュニティ内のデバイス数の制限値である 25 には加算されません。コミュニティ内のスイッチ ポートの数だけ IP Phone を接続できます。

デバイス数が制限値を超えると、制限範囲内になるまでデバイスを削除しないかぎり、コミュニティを管理できなくなります。

Configuration Assistant で管理できるコミュニティの数には、制限はありません。

HTTPS の使用

HTTPS によって、Configuration Assistant と管理対象デバイスとの間の通信が暗号化されます。HTTPS は Cisco IOS の crypto イメージだけに使用できます。

HTTPS で最初に接続する際には、アラートが表示されます。アラートでは、接続先のデバイスが信頼できるサイトであることを示す証明書を受け入れるかどうかが尋ねられます。[はい]、[いいえ]、[常に]、および[証明書を見る]の選択肢があります。続行するには、[はい]または[常に]と回答します。[常に]と回答した場合は、後の Configuration Assistant セッションでアラートは表示されなくなります。

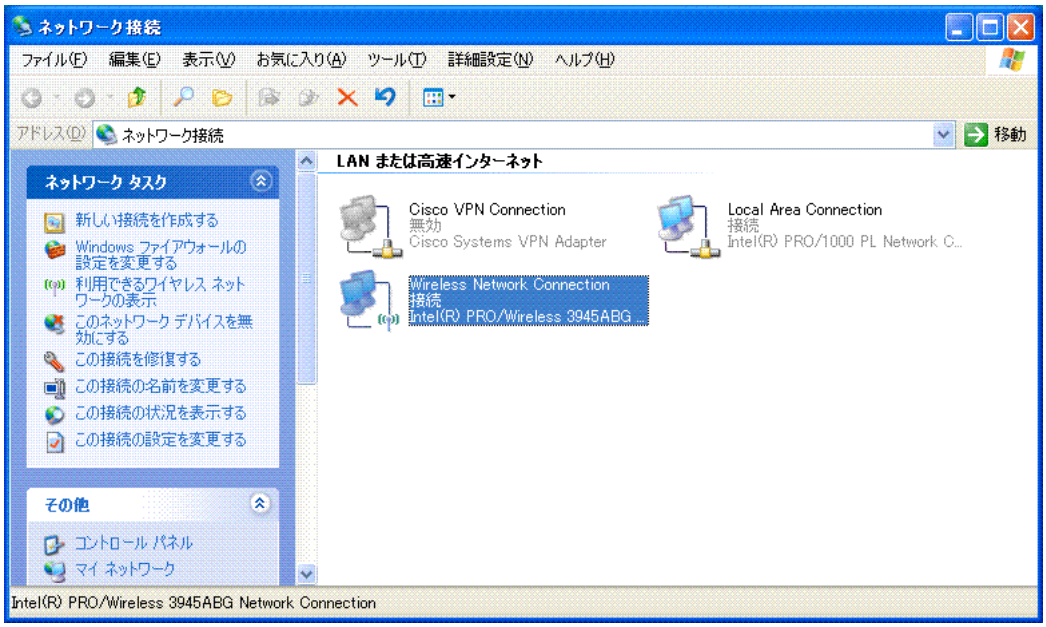
HTTPS が使用されているときは、ステータス バーに アイコンが表示されます。

無線クライアントの設定

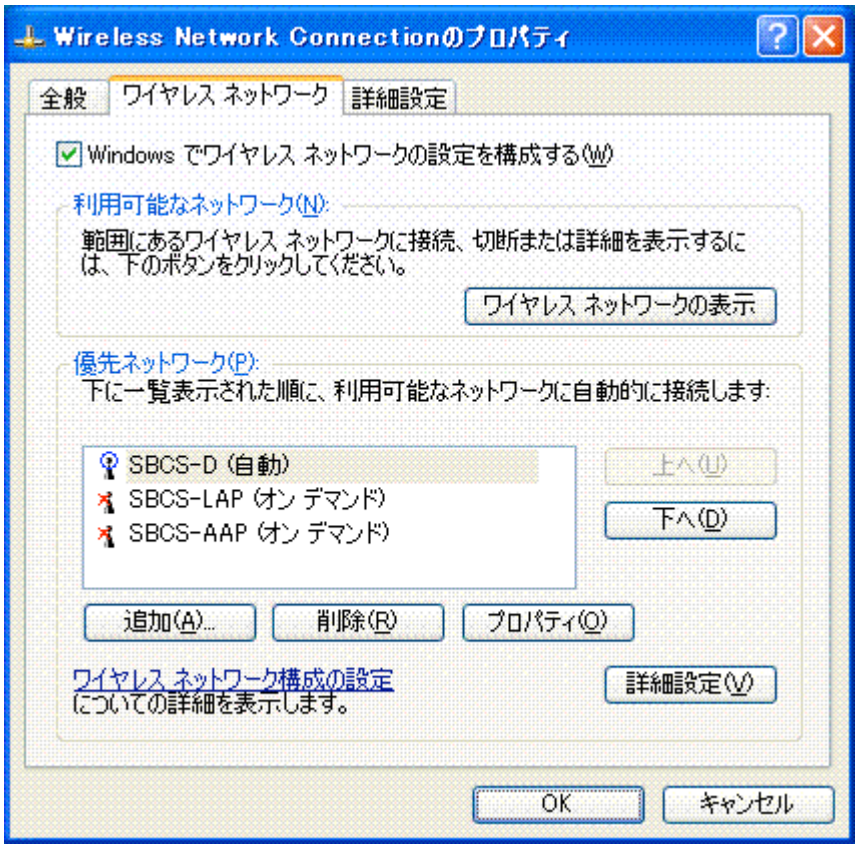
ネットワークにデータ WLAN を設定する前に、使用する可能性のあるすべての無線クライアント、アクセスポイント、WLAN コントローラに共通する認証および暗号化方式を調べます。また、SSID をブロードキャストするかどうかを決定します。[WLAN(SSID)]ウィンドウを開き、[作成]または[修正]をクリックし、共通の802.11セキュリティ オプションを使用してデータ WLAN を設定します。データ WLAN が稼動すると、無線クライアントを設定できます。

次の例では、Windows XP を実行する PC で無線クライアントを設定する方法を示します。

1. クライアント PC のコントロール パネルを開き、[ネットワーク接続]をダブルクリックします。[ワイヤレス ネットワーク接続]を右クリックし、[プロパティ]を選択します。



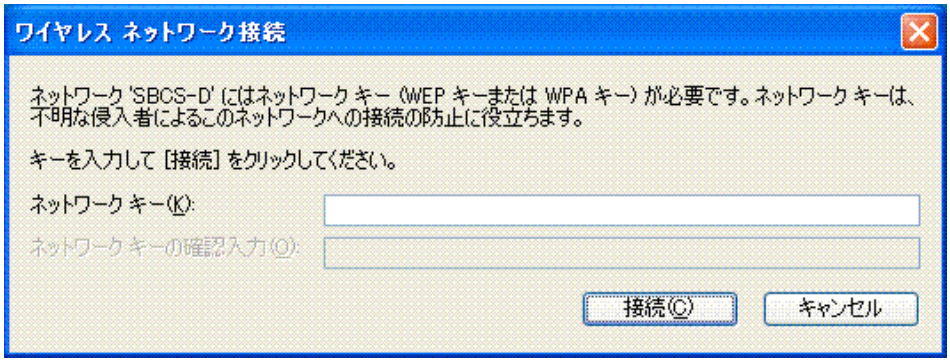
2. [プロパティ]ウィンドウで、[ワイヤレス ネットワーク]タブをクリックします。



3. SSID をブロードキャストする場合は、次を実行します。

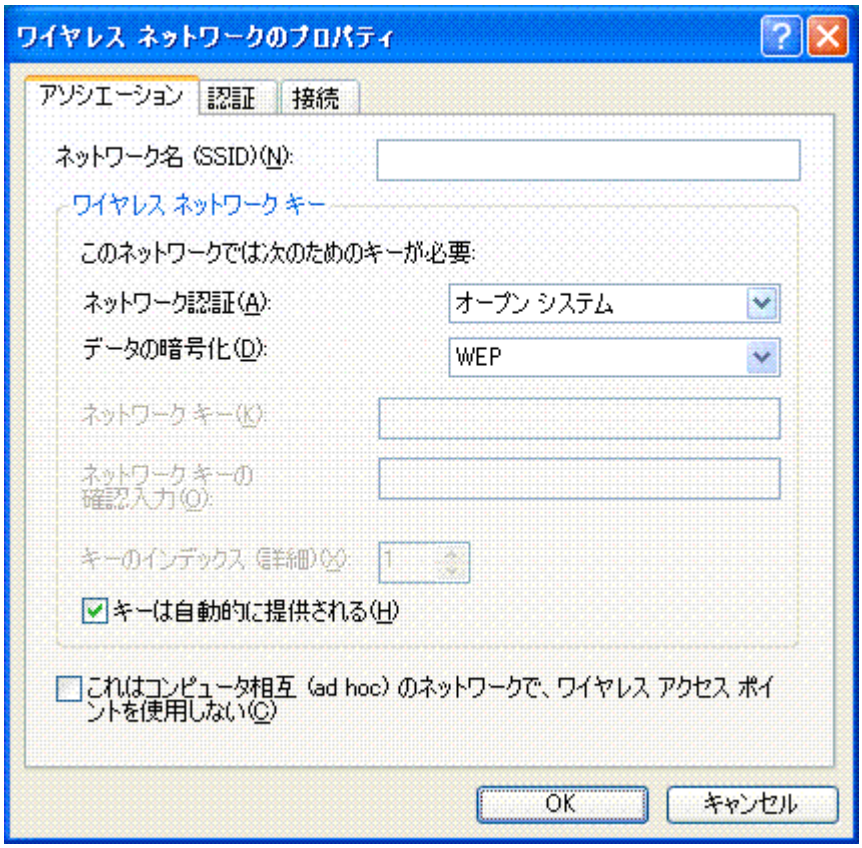
   a. [ワイヤレス ネットワークの表示]をクリックし、目的の SSID を参照します。

   b. 目的の SSID を選択し、[接続]をクリックします。データ WLAN の認証および暗号化方式を選択した場合は、クレデンシャルを求められます。



c. クレデンシャルを入力すると、クライアントはアクセスポイントに関連付けられ、クライアントに IP アドレスが割り当てられます。

4. SSID をブロードキャストする場合、[Windows でワイヤレス ネットワークの設定を構成する] がオンになっていることを確認して、[追加]をクリックします。[ワイヤレス ネットワークのプロパティ]ダイアログボックスが表示されたら、SSID と WLAN のクレデンシャルを入力します。



Cisco 7920 IP Phone の設定

次のガイドラインに従います。

- Cisco 7920 IP Phone で使用可能なセキュリティ オプションは、[EAP]、[WPA]、または[なし]です。

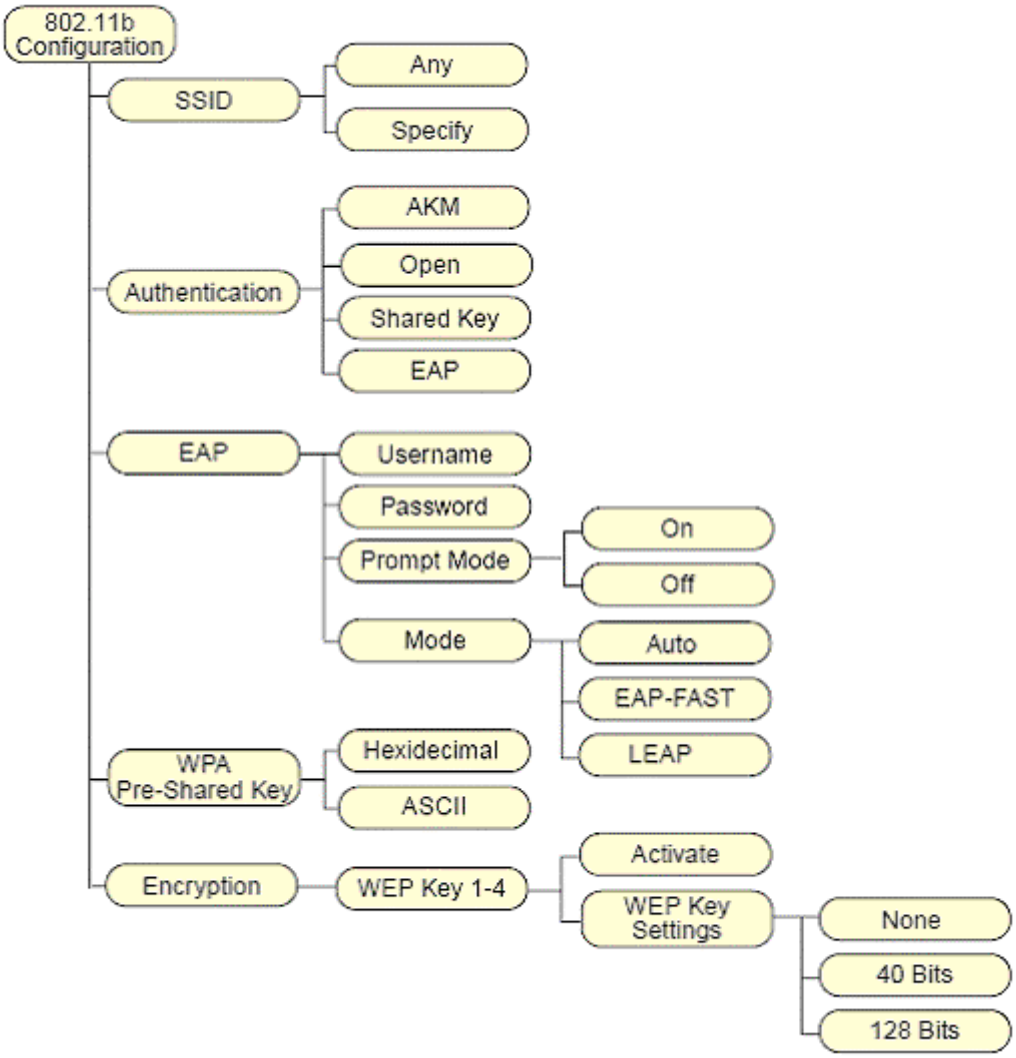
- WLAN コントローラで、別の音声 WLAN を作成します。これにより、使用している音声 WLAN と異なるセキュリティ設定を使用して、データ WLAN を設定することができます。
- 音声 WLAN で[7920 CAC]を選択します。CACは Cisco 7920 IP Phone をサポートします。
- Cisco 7920 IP Phone に音声 WLAN の SSID を手動で入力する必要があります。音声 WLAN の SSID をブロードキャストしないよう、WLAN コントローラを設定することをお勧めします。

WLAN コントローラで音声 WLAN を設定後、Cisco 7920 IP Phone に電源を投入します。

Cisco 7920 IP Phone を設定するには、次の手順に従います。

1. [メニュー]>[プロファイル]を押し、[センタク]を押します。
2. [ネットワーク プロファイル]にスクロールし、[センタク]を押します。
3. 目的のプロファイルにスクロールし、[センタク]を押します。
4. [DHCPユウコウ/ムコウ]にスクロールし、[ユウコウ]を選択します。
5. [モドル]を押し、メニューを終了します。
6. [TFTPオプション]にスクロールし、[センタク]を押します。
7. [DHCPシヨウ]にスクロールし、[センタク]を押します。.
8. [モドル]を押し、メニューを終了します。
9. [802.11bセッテイ]にスクロールし、[センタク]を押します。

   次の図は、[802.11bセッテイ]の下のメニューのレイアウトです。



10. [SSID]にスクロールし、[センタク]を押します。
11. [シテイ]を選択し、音声 WLAN SSID の名前を入力します。

    注: 大文字と小文字を切り替えるには、* キーを使用します。任意の記号を入力するには、# キーを使用します。

12. ネットワーク セキュリティに応じて、[ニンショウ]および[アンゴウカ]の値を入力します。
13. 802.11bのオプションの入力が完了したら、[モドル]を押し、メニューを終了します。
14. [ヘンコウノテキヨウ]にスクロールし、[センタク]を押して変更を有効にします。

    SSID、認証タイプ、および暗号化データが有効になります。

Cisco 7920 IP Phone を音声 WLAN で使用する準備が整いました。電話機はネットワークと関連付けられ、WLAN コントローラに登録され、内線を受けることができます。

よくある質問

Configuration Assistant の概要

Configuration Assistant のシステム要件は何ですか。

Configuration Assistant は他のオペレーティングシステム（UNIX、Linux、Mac OS）で実行できますか。

Configuration Assistant はどのようなデバイスをサポートしていますか。

Configuration Assistant はデバイスをいくつサポートしていますか。

Configuration Assistant でマルチベンダ ネットワークを管理することはできますか。

Configuration Assistant を使用して、Cisco デバイスの Cisco IOS ソフトウェア イメージをアップグレードするには、どうすればいいですか。

同時に複数のデバイスでソフトウェアをアップグレードできますか。

読み書きモードはありますか。

コミュニティ内のデバイスで HTTPS が有効になっていることを Configuration Assistant に認識させるには、どうすればいいですか。

トポロジをファイルに保存できますか。

IP テレフォニー

Configuration Assistant を使用して、エンド ユーザに対して VT Advantage を有効にするには、どうすればいいですか。

Configuration Assistant を使用して、マルチサイトの Voice-over-IP（VoIP）展開を設定するには、どうすればいいですか。

サービス プロバイダへの Session Initiation Protocol（SIP; セッション開始プロトコル）トランク接続を失った場合にアナログ（たとえば、ファックス ポート（FXO））にフェールオーバーするよう、パートナーが Cisco Unified Communications 500 シリーズ プラットフォームを設定することはできますか。

Configuration Assistantを使用して、Cisco Unified Communications 500 シリーズ プラットフォームの自動着信呼分配（ACD）機能を設定できますか。

特定の地域の顧客ネットワークにおいて、ボイスメール（CUE）およびコール制御（CUCME）言語をカスタマイズするには、どうすればいいですか。

無線 LAN 設定

Configuration Assistant では、WLAN–WAN リンク上にデバイスを設定できますか。

Configuration Assistant では、どのような無線デバイスをサポートしていますか。AP1131、1242、および 350 はサポートされていますか。

Configuration Assistant を使用して、無線 LAN コントローラ用に Cisco Centralized Key Management を設定するには、どうすればいいですか。

Configuration Assistant のシステム要件は何ですか。

Configuration Assistant の最低要件は、次の通りです。

- Pentium IV ベースの IBM PC または互換コンピュータ
- メモリ:512MB DRAM
- Windows XP（Service Pack 1以降）または Windows Vista

Configuration Assistant は他のオペレーティングシステム（UNIX、Linux、Mac OS）で実行できますか。

いいえ、Configuration Assistant は Microsoft Windows 上でしか実行できません。

Configuration Assistant はどのようなデバイスをサポートしていますか。

Configuration Assistant では、次の表のすべてのデバイスをサポートしています。

製品番号	製品の説明
Cisco Catalyst Express 500 シリーズ スイッチ	
WS-CE500-24TT-K9	10/100 アクセス ポート x 24、10/100/1000BASE-T アップリンク x 2
WS-CE500-24LC-K9	10/100 アクセス ポート x 20、PoE ポート付き 10/100 アクセスポート x 4、10/100/1000BASE-T アップリンクまたは Small Form-Factor Pluggable（SFP）アップリンク x 2
WS-CE500-24PC-K9	PoE 付き 10/100 アクセス ポート x 24、10/100/1000BASE-T アップリンクまたは SFP アップリンク x 2
WS-CE500G-12TC-K9	10/100/1000BASE-T ポート x 8、10/100/1000BASE-T アップリンクまたは SFP アップリンク x 4
Cisco Catalyst Express 520 シリーズ スイッチ	
WS-CE520-8PC-K9	PoE 付き 10/100 アクセス ポート x 8、10/100/1000BASE-T アップリンクまたは SFP アップリンク x 1
WS-CE520-24TT-K9	10/100 アクセス ポート x 24、10/100/1000BASE-T アップリンク x 2
WS-CE520-24LC-K9	10/100 アクセス ポート x 20、PoE ポート付き 10/100 アクセス ポート x 4、10/100/1000BASE-T アップリンクまたは SFP アップリンク x 2

WS-CE520-24PC-K9	PoE 付き 10/100 アクセス ポート x 24、10/100/1000BASE-T アップリンクまたは SFP アップリンク x 2
WS-CE520G-24TC-K9	10/100/1000BASE-T ポート x 24、10/100/1000BASE-T アップリンクまたは SFP アップリンク x 2
小規模企業向け Cisco Unified Communications 500 シリーズ	
UC520-8U-4FXO-K9	8 ユーザ構成、PSTN トランク（FXO）x 4、アナログ ポート（FXS）x 4、PoE ポート x 8、拡張用 VIC スロット x 1 コール制御、ボイスメール、Cisco Unified IP Phone 用の機能ライセンス
UC520W-8U-2BRI-K9 UC520W-8/J-K9	8 ユーザ構成、BRI トランク（BRI）x 2、アナログ ポート（FXS）x 4、PoE ポートx 8、拡張用 VIC スロット x 1 コール制御、ボイスメール、Cisco Unified IP Phone 用の機能ライセンス
UC520-16U-4FXO-K9	16 ユーザ構成、PSTN トランク（FXO）x 4、アナログ ポート（FXS）x 4、PoE ポート x 8、拡張用 VIC スロット x 1 コール制御、ボイスメール、Cisco Unified IP Phone 用の機能ライセンス **注：** 8 ユーザ用のコール制御機能ライセンスを備えた、8 ポートの Cisco Catalyst Express 520 スイッチが必要です。
UC520W-16U-2BRI-K9 UC520W-16/J-K9	16 ユーザ構成、BRI トランク（BRI）x 2、アナログ ポート（FXS）x 4、PoE ポートx 8、拡張用 VIC スロット x 1 コール制御、ボイスメール、Cisco Unified IP Phone 用の機能ライセンス **注：** 8 ユーザ用のコール制御機能ライセンスを備えた、8 ポートの Cisco Catalyst Express 520 スイッチが必要です。
UC520W-8U-4FXO-K9	8 ユーザ構成、PSTN トランク（FXO）x 4、アナログ ポート（FXS）x 4、PoE ポート x 8、拡張用 VIC スロット x 1 コール制御、ボイスメール、Cisco Unified IP Phone 用の統合 Wi-Fi アクセスポイント機能ライセンス
UC520W-8U-2BRI-K9	8 ユーザ構成、BRI トランク（BRI）x 2、アナログ ポート（FXS）x 4、PoE ポートx 8、拡張用 VIC スロット x 1 コール制御、ボイスメール、Cisco Unified IP Phone 用の統合 Wi-Fi アクセスポイント機能ライセンス
UC520W-16U-4FXO-K9	16 ユーザ構成、PSTN トランク（FXO）x 4、アナログ ポート（FXS）x 4、PoE ポート x 8、拡張用 VIC スロット x 1 コール制御、ボイスメール、Cisco Unified IP Phone 用の統合 Wi-Fi アクセスポイント機能ライセンス

UC520W-16U-2BRI-K9	16 ユーザ構成、BRI トランク（BRI）x 2、アナログ ポート（FXS）x 4、PoE ポートx 8、拡張用 VIC スロット x 1 コール制御、ボイスメール、Cisco Unified IP Phone 用の統合 Wi-Fi アクセスポイント機能ライセンス
UC520-24U-8FXO-K9	24 ユーザ構成、PSTN トランク（FXO）x 8、PoE ポート x 8、拡張用 VIC スロット x 1 コール制御、ボイスメール、Cisco Unified IP Phone 用の機能ライセンス **注**：24 ポートの Cisco Catalyst Express 520 スイッチ（WS-CE520-24PC-K9）が必要です。
UC520-24U-4BRI-K9	24 ユーザ構成、BRI トランク（BRI）x 4、PoE ポート x 8、拡張用 VIC スロット x 1 コール制御、ボイスメール、Cisco Unified IP Phone 用の機能ライセンス **注**：24 ポートの Cisco Catalyst Express 520 スイッチ（WS-CE520-24PC-K9）が必要です。
UC520-32U-8FXO-K9	32 ユーザ構成、PSTN トランク（FXO）x 8、アナログ ポート（FXS）x 4、PoE ポート x 8、拡張用 VIC スロット x 1 コール制御、ボイスメール、Cisco Unified IP Phone 用の機能ライセンス **注**：24 ポートの Cisco Catalyst Express 520 スイッチ（WS-CE520-24PC-K9）が必要です。
UC520-32U-4BRI-K9	32 ユーザ構成、BRI トランク（BRI）x 4、アナログ ポート（FXS）x 4、PoE ポートx 8、拡張用 VIC スロット x 1 コール制御、ボイスメール、Cisco Unified IP Phone 用の機能ライセンス **注**：24 ポートの Cisco Catalyst Express 520 スイッチ（WS-CE520-24PC-K9）が必要です。
UC520-48U-12FXO-K9	48 ユーザ構成、PSTN トランク（FXO）x 12、アナログ ポート（FXS）x 4、PoE ポート x 8、拡張用 VIC スロット x 1 コール制御、ボイスメール、Cisco Unified IP Phone 用の機能ライセンス **注**：24 ポートの Cisco Catalyst Express 520 スイッチ（WS-CE520-24PC-K9）が 2 つ必要です。
UC520-48U-6BRI-K9	48 ユーザ構成、BRI トランク（BRI）x 6、アナログ ポート（FXS）x 4、PoE ポートx 8、拡張用 VIC スロット x 1 コール制御、ボイスメール、Cisco Unified IP Phone 用の機能ライセンス **注**：24 ポートの Cisco Catalyst Express 520 スイッチ（WS-CE520-24PC-K9）

	が 2 つ必要です。
UC520-48U-T/E/F-K9	48 ユーザ構成、T1/E1 音声インターフェイス、PSTN トランク（FXO）x 4、アナログ ポート（FXS）x 4、PoE ポート x 8、拡張用 VIC スロット x 1 コール制御、ボイスメール、Cisco Unified IP Phone 用の機能ライセンス **注：** 24 ポートの Cisco Catalyst Express 520 スイッチ（WS-CE520-24PC-K9）が必要です。
UC520-48U-T/E/B-K9	48 ユーザ構成、T1/E1 音声インターフェイス、BRI トランク（BRI）x 2、アナログ ポート（FXS）x 4、PoE ポート x 8、拡張用 VIC スロット x 1 コール制御、ボイスメール、Cisco Unified IP Phone 用の機能ライセンス **注：** 24 ポートの Cisco Catalyst Express 520 スイッチ（WS-CE520-24PC-K9）が 2 つ必要です。
521G	Cisco Unified IP Phone 1 回線、単一の 10/100 PoE ポート、DC アダプタ ポート（DC5V）（オプション）、ヘッドセット ポート、ハンドセット ポート
524G	Cisco Unified IP Phone 4 回線、単一の 10/100 PoE ポート、DC アダプタ ポート（DC5V）（オプション）、ヘッドセット ポート、ハンドセット ポート
Cisco 850 シリーズ サービス統合型ルータ	
CISCO851-K9	Cisco 851 イーサネット/イーサネット ルータ
CISCO851W-G-A-K9	Cisco 851 イーサネット/イーサネット無線ルータ（南アメリカ、北アメリカ、中央アメリカ ）
CISCO851W-G-E-K9	Cisco 851 イーサネット/イーサネット無線ルータ（ヨーロッパ）
CISCO851W-G-J-K9	Cisco 851 イーサネット/イーサネット無線ルータ（日本）
CISCO857-K9	Cisco 857 ADSL ルータ
CISCO857W-G-A-K9	Cisco 857 ADSL 無線ルータ（米国および南アメリカ、北アメリカ、中央アメリカ）
CISCO857W-G-E-K9	Cisco 857 ADSL 無線ルータ（ヨーロッパ）
Cisco 870 シリーズ サービス統合型ルータ	
CISCO871-K9	Cisco 871 イーサネット/イーサネット ルータ
CISCO871W-G-A-K9	Cisco 871 イーサネット/イーサネット無線ルータ（米国および南アメリカ、北アメリカ、中央アメリカ ）
CISCO871W-G-E-K9	Cisco 871 イーサネット/イーサネット無線ルータ（ヨーロッパ）
CISCO871W-G-J-K9	Cisco 871 イーサネット/イーサネット無線ルータ（日本）

CISCO876-K9	Cisco 876 ADSL over ISDN ルータ
CISCO876W-G-E-K9	Cisco 876 ADSL over ISDN 無線ルータ
CISCO877-K9	Cisco 877 ADSL ルータ
CISCO877W-G-A-K9	Cisco 877 ADSL 無線ルータ（米国および南アメリカ、北アメリカ、中央アメリカ）
CISCO877W-G-E-K9	Cisco 877 ADSL 無線ルータ（ヨーロッパ）
CISCO878-K9	Cisco 878 G.SHDSL ルータ
CISCO878W-G-A-K9	Cisco 878 G.SHDSL 無線ルータ（米国および南アメリカ、北アメリカ、中央アメリカ）
CISCO878W-G-E-K9	Cisco 878 G.SHDSL 無線ルータ（ヨーロッパ）
音声インターフェイス カード	
VIC3-2FXS/DID	2 ポートの FXS 音声/ファックス インターフェイス カード
VIC-4FXS/DID	4 ポートの FXS 音声/ファックス インターフェイス カード
VIC3-4FXS/DID	4 ポートの FXS 音声/ファックス インターフェイス カード
VIC2-2FXO	2 ポートの FXO 音声/ファックス インターフェイス カード
VIC2-4FXO	4 ポートの FXO 音声/ファックス インターフェイス カード
VIC2-2BRI-NT/TE	2 ポートの BRI 音声/ファックス インターフェイス カード
Cisco Mobility Express ソリューション	
AIR-AP521G-A-K9 AIR-AP521G-E-K9 AIR-AP521G-P-K9	Cisco 521 Wireless Express アクセスポイント（Cisco IOS ソフトウェア）
AIR-LAP521G-A-K9 AIR-LAP521G-E-K9 AIR-LAP521G-P-K9	Cisco 521 Wireless Express アクセスポイント（Cisco Unified Wireless Network ソフトウェア）
AIR-WLC526-K9	Cisco 526 Wireless Express モビリティ コントローラ

Configuration Assistant はデバイスをいくつサポートしていますか。

Configuration Assistant では、最大 25 のデバイスから成るコミュニティを管理できます。デバイスに対しては次の制限があります。

- Catalyst Express スイッチ x 15。
- ルータ x 5（在宅勤務者は含まず）。（（ルータには、Unified Communications 500 シリーズ プラットフォームと 800 シリーズ アクセス ルータが含まれます。）
- 無線コントローラ x 2。
- 自律型アクセスポイント x 3。

コミュニティ内のデバイス数の詳細については、コミュニティに関する制限事項をクリックしてください。

Configuration Assistant でマルチベンダ ネットワークを管理することはできますか。

いいえ。Configuration Assistant では、Cisco のデバイスしか管理できません。

Configuration Assistant を使用して、Cisco デバイスの Cisco IOS ソフトウェア イメージをアップグレードするには、どうすればいいですか。

PC に保存されている Cisco IOS ソフトウェア イメージを、トポロジ マップ内のデバイス アイコンにドラッグアンドドロップします。Cisco Unified Communications 500 シリーズ プラットフォームで、Cisco Unity Express ソフトウェアをアップグレードする際もこの方法を使用できます。

同時に複数のデバイスでソフトウェアをアップグレードできますか。

はい。機能バーで **メンテナンス > ソフトウェアアップグレード** を選択して、[ソフトウェアアップグレード]ウィンドウを使用します。

読み書きモードはありますか。

はい。ユーザごとに異なるアクセス権を割り当てるには、**設定 > デバイスプロパティ > ユーザとパスワード** を選択し、[ユーザとパスワード]ウィンドウを使用します。

コミュニティ内のデバイスで HTTPS が有効になっていることを Configuration Assistant に認識させるには、どうすればいいですか。

デバイスをコミュニティに追加する前に、CLI を使用して、デバイスで HTTPS を有効にします。デバイスをコミュニティに追加してから、デバイスで HTTPS を有効にした場合、Configuration Assistant では HTTPS ではなく HTTP が通信プロトコルとして認識されます。この問題を修正するには、コミュニティからデバイスを削除し、再度追加します。

トポロジをファイルに保存できますか。

いいえ。[レイアウトの保存]オプションでは、トポロジ マップ内のデバイスの場所は保存されますが、マップ自体は保存されません。

Configuration Assistant を使用して、エンド ユーザに対して VT Advantage を有効にするには、どうすればいいですか。

Configuration Assistant では、ユーザの IP Phone の内線を設定する際に、Cisco Unified Communications 500 シリーズ プラットフォームで自動的に VT Advantage が設定されます。

Configuration Assistant を使用して、マルチサイトの Voice-over-IP（VoIP）展開を設定するには、どうすればいいですか。

Configuration Assistant では、マルチサイトでの音声設定はサポートされていません。Cisco Unified Communications 500 シリーズ プラットフォームで CLI を使用した場合のみ、サポートされます。

サービス プロバイダへの Session Initiation Protocol（SIP; セッション開始プロトコル）トランク接続を失った場合にアナログ（たとえば、ファックス ポート（FXO））にフェールオーバーするよう、パートナーが Cisco Unified Communications 500 シリーズ プラットフォームを設定することはできますか。

Configuration Assistant では、SIP トランクのフェールオーバー先として、存在する任意のアナログ トランクが自動で設定されます。つまり、アナログ トランクは、SIP トランクより優先度が低く設定されています。

Configuration Assistantを使用して、Cisco Unified Communications 500 シリーズ プラットフォームの自動着信呼分配（ACD）機能を設定できますか。

Configuration Assistant では、Cisco CallManager Express の基本 ACD 機能の設定はサポートされていません。（Cisco CallManager Express の一部として）この機能に精通しているパートナーは、Cisco Unified Communications 500 シリーズ プラットフォーム上の CLI/コンソール アクセスを使用して、この機能（Tclスクリプトなど）を設定できます。

特定の地域の顧客ネットワークにおいて、ボイスメール（CUE）およびコール制御（CUCME）言語をカスタマイズするには、どうすればいいですか。

以下の事前設定手順に従います。

1. Cisco.com から CUCME 言語ファイルをダウンロードします。
2. Cisco.com から CUE 言語パックをダウンロードします。
3. ［言語ファイルの場所］フィールドに表示されているフォルダに、CME および CUE 言語ファイルをコピーします。

次に、以下の事前設定手順に従います。

1. ［地域］リストから、CUCME の地域を選択します。それによって、電話のトーンと鳴り方が設定されます。
2. ［電話の言語］リストから、ユーザの電話に表示される言語を選択します。
3. ［ボイスメールの言語］リストから、ユーザに聞かせるボイス メール プロンプトの言語を選択します。
4. ［日付書式］リストから、日付形式を選択します。
5. ［時間制］リストから、時刻形式を選択します。

   ［地域/電話の言語］の設定は、CME のローカライズ用です。CME 用の言語ファイルは、Cisco.com からダウンロードできる tar ファイルです。［ボイスメールの言語］の設定は、CUE のローカライズに関するものです。

Configuration Assistant では、WLAN–WAN リンク上にデバイスを設定できますか。

はい。Configuration Assistant では WLAN 上にデバイスを設定できます。WAN リンク上のデバイスについては、パートナーが顧客サイトへの VPN を設定して、Configuration Assistant で顧客ネットワークと通信できるようにする必要があります。

Configuration Assistant では、どのような無線デバイスをサポートしていますか。AP1131、1242、および 350 はサポートされていますか。

いいえ。これらのアクセスポイントはサポートされていません。この表に列挙されていないデバイスは、トポロジ マップではサポートされないデバイスとして表示されます。

Configuration Assistant を使用して、無線 LAN コントローラ用に Cisco Centralized Key Management を設定するには、どうすればいいですか。

Cisco Centralized Key Management を設定するには、無線 LAN コントローラの Web ユーザ インターフェイスから行う必要があります。Configuration Assistant では、Cisco Centralized Key Management の設定はサポートしていません。

ヘルプの使い方

ここでは、オンライン ヘルプの使い方について説明します。

ヘルプ トピックを表示する方法

[ヘルプ]ウィンドウの左側の枠で、[コンテンツ]、[インデックス]、または[検索]タブにあるトピックをクリックすると、そのトピックが右側の枠に表示されます。

トピックに表示される情報は、デバイスによって異なる場合があります。このような場合は、右側の枠にそのトピックのすべてのバージョンが表示され、バージョンごとに、そのバージョンが適用されているコミュニティ メンバのホスト名が示されます。

機能ウィンドウの表示

多くのヘルプ トピックには、紫色のリンクが含まれます。これらのリンクのテキストは、機能ウィンドウのタイトルである場合もあれば、「ここ」と記されている場合もあります。このリンクをクリックすると、機能ウィンドウが開きます。

ウィンドウに関するヘルプを表示するには、[ヘルプ]ボタンをクリックします。次の方法でもヘルプを表示できます。

1. [コンテンツ]タブで、[ウィンドウリスト]トピックをクリックします。
2. [ヘルプ]ウィンドウの右側の枠で、ウィンドウのタイトルをクリックします。

Cisco IOS リリースに関する前提条件

オンライン ヘルプは、すべてのデバイスが最新の Cisco IOS リリースを実行していることを前提としています。デバイスで最新の Cisco IOS リリースを実行していない場合は、オンライン ヘルプに記載されている機能のオプションが、ユーザ インターフェイスに表示されるものと一致しない場合があります。

凡例

この凡例では、[トポロジ]ビュー、[前面パネル]ビュー、各設定ウィンドウ、およびオンライン ヘルプ トピックに表示される図と色について説明します。次のカテゴリに分けて説明します。

- デバイスのアイコン
- デバイスのステータス
- ポートのタイプ
- ポートのステータスとプロパティ
- リンクのタイプ
- リンクのステータス
- 冗長電源のステータス
- 全般

デバイスのアイコン

以下のデバイス アイコンは、Configuration Assistant のビューおよびウィンドウに共通して表示されます。

以下のアイコンが、トポロジ マップに表示される場合もあります。

注：

- デバイスがダウンしている場合、デバイスのアイコンは赤色になります。
- 不明なデバイスのアイコンは、Configuration Assistant がそのデバイスをサポートしていない場合、またはそのデバイスで実行している Cisco IOS バージョンをサポートしていない場合に表示されます。

デバイスのステータス

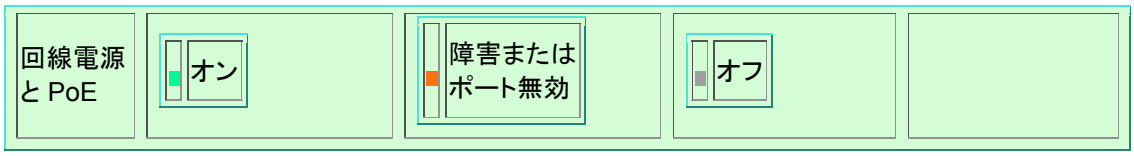
アイコンの色	アップ	ダウン	不明
ラベルの色	メンバまたはスタンドアロン デバイス	候補	エッジ デバイス

ポートのタイプ

	RJ-45
	RJ-45
	RJ-45
	着脱可能小型フォーム ファクタ（SFP）モジュール（空）
	SFP 光ファイバ モジュール（LX、SX、ZX、CWDM、100BASE-FX）

ポートのステータスとプロパティ

システム	正常	デバイス障害	無線コントローラ不良	
ステータス	リンク正常	リンク不良またはポート無効	リンクなし	リンクなし、ポート無効
スピード	100Mbps（10/100）または 155Mbps（ATM）	10Gbps または 1000Mbps（固定）、または 1000Mbps（10/100/1000）	10Mbs	不明
デュプレックス	全二重		半二重	不明

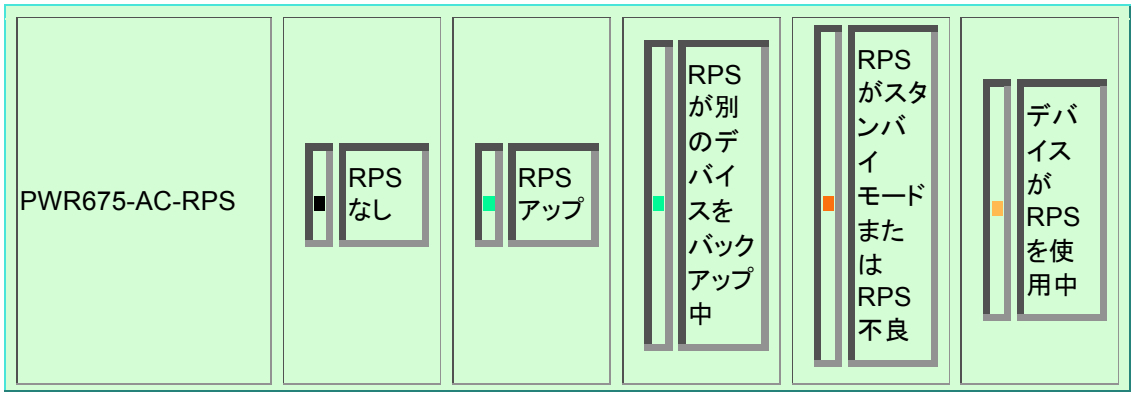


リンクのタイプ

注：2 本のパイプは複数のリンクを表します。1 つのパイプがグレーで、もう 1 つのパイプが緑の場合、1 つ以上のリンクがブロックされ、1 つ以上のリンクが正常である（アップしている）ことを示します。

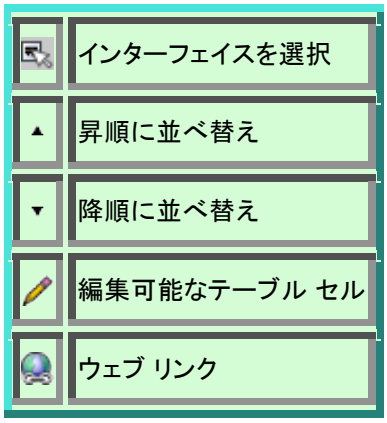
リンクのステータス

冗長電源のステータス



PWR600-AC-RPS	RPS なし	デバイスが RPS を使用中	RPS アップ	RPS 不良	
PWR300-AC-RPS	RPS なし	RPS アップ	RPS が別のデバイスをバックアップ中	RPS がスタンバイ モードまたは RPS 不良	デバイスが RPS を使用中

全般



ウインドウリスト

UC500、Cisco 800シリーズルータを管理する場合

[DHCP IP 除外対象範囲の追加]ウィンドウ

このウィンドウは、[DHCPサーバ]ウィンドウの[DHCP IP 除外対象]タブで[作成]をクリックした場合に表示されます。

このウィンドウを使用すると、DHCP IP アドレスの除外範囲を追加できます。

次の手順に従います。

1. [開始IPアドレス]フィールドに、DHCP サーバによって DHCP クライアントに割り当てられないようにする DHCP IP アドレスの範囲を示す最初の IP アドレスを入力します。
2. [終了IPアドレス]フィールドに、DHCP サーバによって DHCP クライアントに割り当てられないようにする DHCP IP アドレスの範囲を示す最後の IP アドレスを入力します。
3. ウィンドウを閉じるには、[OK]をクリックします。

UC500、Cisco 800シリーズルータを管理する場合

[DHCPサーバ]ウィンドウ

このウィンドウは、**設定 > DHCPサーバ** を選択した場合に表示されます。

まず、設定するデバイスを[ホスト名]リストから選択します。

このウィンドウには、次のタブがあります。

- [DHCPプール]。IP アドレスの DHCP プールの表示、作成、変更、または削除に使用します。
- [DHCPバインディング]。DHCP プール内の IP アドレスをクライアントの MAC アドレスに手動でマップする場合に使用します。
- [DHCP IP 除外対象]。DHCP サーバによってクライアントに割り当てられない(除外される)ようにするIP アドレスの指定に使用します。

[DHCPプール]

DHCP プールのプロパティおよび値を表示するには、表示する DHCP プールの名前を選択します。

新しい DHCP プールを作成するには、[作成]をクリックして、[DHCPプールの作成]ウィンドウを使用します。

既存の DHCP プールを変更するには、変更する DHCP プールを選択して、[修正]をクリックし、[DHCPプールの修正]ウィンドウを使用します。

DHCP プールを削除するには、次の手順に従います。

1. 削除する DHCP プールの名前を選択します。
2. [削除]をクリックします。このまま処理を続行すると DHCP プールが削除されることを警告するウィンドウが表示されます。
3. ウィンドウを閉じるには、[OK]をクリックします。

[DHCPバインディング]

新しい DHCP バインディングを作成するには、[作成]をクリックして、[DHCPバインディングの作成]ウィンドウを使用します。

既存の DHCP バインディングを変更するには、変更するバインディングの名前を選択して、[修正]をクリックし、[DHCPバインディングの修正]ウィンドウを使用します。

DHCP バインディングを削除するには、次の手順に従います。

1. 削除する DHCP バインディングの名前を選択します。
2. [削除]をクリックします。このまま処理を続行すると DHCP バインディングが削除されることを警告するウィンドウが表示されます。
3. ウィンドウを閉じるには、[OK]をクリックします。

[DHCP IP 除外対象]

DHCP で除外される IP アドレスを新たに指定するには、[作成]をクリックして、[DHCP除外対象の作成]ウィンドウを使用します。

DHCP で除外される IP アドレスを削除するには、IP アドレスを選択して、[削除]をクリックします。

UC500、Cisco 800シリーズルータを管理する場合

[DHCPバインディングの作成]ウィンドウ

このウィンドウは、[DHCPサーバ]ウィンドウの[DHCPバインディング]タブで[作成]をクリックした場合に表示されます。

このウィンドウを使用すると、DHCP バインディングを作成できます。

次の手順に従います。

1. [名前]フィールドに、DHCP サーバ アドレス プールの名前を入力します。
2. [ホストIPアドレス]フィールドに、ホスト IP アドレスを入力します。
3. [ネットマスク]フィールドに、ホスト サブネット ネットワーク マスクを入力します。
4. [ID]メニューから識別子を選択します。識別子は、MAC アドレスがハードウェア識別子またはクライアント識別子であることを意味します。

5. [MACアドレス]フィールドに、MAC アドレスを入力します。MAC アドレスでは、クライアントのハードウェア アドレスまたは識別子を小数点付き 16 進表記法で指定します。たとえば、01b7.0813.8811.66 です。
6. [クライアント名]フィールドに、標準 ASCII 文字でクライアント名を入力します。クライアント名はドメイン名であってはいけません。たとえば、「mars」という名前を「mars.cisco.com」と指定しないでください。
7. ウィンドウを閉じるには、[OK]をクリックします。

UC500、Cisco 800シリーズルータを管理する場合

[DHCPバインディングの修正]ウィンドウ

このウィンドウは、[DHCPサーバ]ウィンドウの[DHCPバインディング]タブで[修正]をクリックした場合に表示されます。

このウィンドウを使用すると、DHCP バインディングを変更できます。

次の手順に従います。

1. [名前]フィールドに、DHCP サーバ アドレス プールの名前を入力します。
2. [ホストIPアドレス]フィールドに、ホスト IP アドレスを入力します。
3. [ネットマスク]フィールドに、ホスト サブネット ネットワーク マスクを入力します。
4. [ID]メニューから識別子を選択します。識別子は、MAC アドレスがハードウェア識別子またはクライアント識別子であることを示します。
5. [MACアドレス]フィールドに、MAC アドレスを入力します。MAC アドレスでは、クライアントのハードウェア アドレスまたは識別子を小数点付き 16 進表記法で指定します。たとえば、01b7.0813.8811.66 です。
6. [クライアント名]フィールドに、標準 ASCII 文字でクライアント名を入力します。クライアント名はドメイン名であってはいけません。たとえば、「mars」という名前を「mars.cisco.com」と指定しないでください。
7. ウィンドウを閉じるには、[OK]をクリックします。

UC500、Cisco 800シリーズルータを管理する場合

[DHCPプールの作成]ウィンドウ

このウィンドウは、[DHCPサーバ]ウィンドウの[DHCPバインディング]タブで[作成]をクリックした場合に表示されます。

このウィンドウを使用すると、DHCP プールを作成したり、任意で DNS サーバ、ドメイン名、デフォルトのルータ、および Windows Internet Naming Service（WINS）サーバを指定したりできます。

次の手順に従います。

1. [名前]フィールドに、DHCP プール名を入力します。
2. [ネットワーク]フィールドに、サブネット ネットワーク番号を入力します。
3. [サブネットマスク]フィールドにサブネット ネットワーク マスクを入力します。
4. [DNSサーバ1]フィールドに、DNS サーバの IP アドレスを入力します。DHCP クライアントから DNS サーバに対して、IP アドレスとホスト名を関連付けるためのクエリが実行されます。
5. オプション:[DNSサーバ2]フィールドに、セカンド DNS サーバの IP アドレスを入力します。
6. [ドメイン名]フィールドに、ドメインの名前を入力します。DHCP クライアントのドメイン名を指定すると、クライアントがそのドメインに配置されます。
7. オプション:[デフォルトルータ]フィールドに、デフォルトのルータの IP アドレスを入力します。DHCP クライアントの起動時に、クライアントはデフォルトのルータ宛てにパケットの送信を開始します。デフォルトのルータの IP アドレスは、クライアントと同じサブネット上にある必要があります。
8. オプション:[WINSサーバ1]フィールドおよび[WINSサーバ2]フィールドに、WINS サーバの IP アドレスを入力します。これらのフィールドで、Microsoft DHCP クライアントで使用可能な WINS サーバを指定します。
9. ウィンドウを閉じるには、[OK]をクリックします。

UC500、Cisco 800シリーズルータを管理する場合

[DHCPプールの修正]ウィンドウ

このウィンドウは、[DHCPサーバ]ウィンドウの[DHCPプール]タブで[修正]をクリックした場合に表示されます。

このウィンドウを使用すると、DNS サーバ、ドメイン名、デフォルトのルータ、WINS サーバなど、既存の DHCP プールを変更できます。

次の手順に従います。

1. [名前]フィールドに、DHCP プール名を入力します。
2. [ネットワーク]フィールドに、サブネット ネットワーク番号を入力します。
3. [サブネットマスク]フィールドにサブネット ネットワーク マスクを入力します。
4. [開始IP]フィールドに、DHCP プールの最初の IP アドレスを入力します。
5. [終了IP]フィールドに、DHCP プールの最後の IP アドレスを入力します。
6. [DNSサーバ1]フィールドに、DNS サーバの IP アドレスを入力します。DHCP クライアントは、ホスト名と IP アドレスを照合する必要がある場合に、DNS IP サーバに対してクエリを実行します。
7. オプション:[DNSサーバ2]フィールドに、セカンド DNS サーバの IP アドレスを入力します。
8. [ドメイン名]フィールドに、ドメインの名前を入力します。DHCP クライアントのドメイン名を指定すると、クライアントがそのドメインに配置されます。
9. オプション:[デフォルトルータ]フィールドに、デフォルトのルータの IP アドレスを入力します。DHCP クライアントの起動時に、クライアントはデフォルトのルータ宛てにパケットの送信を開

始します。デフォルトのルータの IP アドレスは、クライアントと同じサブネット上にある必要があります。

10. オプション：[WINSサーバ1]フィールドおよび[WINSサーバ2]フィールドに、WINS サーバの IP アドレスを入力します。これらのフィールドで、Microsoft DHCP クライアントで使用可能な WINS サーバを指定します。
11. [OK]をクリックしてウィンドウを閉じます。

UC500、Cisco 800シリーズルータを管理する場合

[DMZサービスの作成]ウィンドウ

このウィンドウは、[ファイアウォールとDMZ]ウィンドウの[DMZ]タブで[作成]をクリックした場合に表示されます。

このダイアログでは、インターフェイスに Demilitarized Zone（DMZ; 非武装地帯）を追加できます。事前にファイアウォールを設定しておく必要があります。

次の手順に従います。

1. 指定した TCP または UDP サービスのトラフィックの宛先を指定するには、[IPアドレス]フィールドに IP アドレスを入力します。Network Address Translation（NAT; ネットワーク アドレス変換）が有効になっている場合は、NAT 変換されたアドレス（内部グローバル アドレス）を入力します。
2. [サーバタイプ]リストから、サポートされているサーバの種類を選択します。サポートされているサーバの種類は、[FTP]、[ウェブサーバ]、[セキュア ウェブサーバ]、[メールサーバ]、[SSH]、および [SFTP]です。
3. ウィンドウを閉じるには、[OK]をクリックします。

UC500、Cisco 800シリーズルータを管理する場合

[FXOカスタム設定]ウィンドウ

このウィンドウは、[音声]ウィンドウの[ダイヤルプラン]タブで、FXO トランクの[カスタム設定]を選択して[設定]をクリックした場合に表示されます。

1対1 DID 変換を設定するには、次の手順に従います。

1. 設定を追加するには、[作成]をクリックします。
2. [説明]フィールドに、設定の説明を入力します。
3. [トランク]メニューで、音声のエンドポイントを選択します。使用できる選択肢は、デバイスで検出された FXO ポートに対応します。
4. [宛先番号]フィールドに、呼び出しのリダイレクト先の番号を入力します。

CE520 スイッチを管理する場合

[HTTPポート]ウィンドウ

このウィンドウは、機能バーで **設定 > デバイスプロパティ > HTTPポート** を選択した場合に表示されます。このウィンドウを使用すると、コミュニティ内のすべてのデバイスの HTTP ポート番号を変更できます。

注：一部のデバイスとの通信に、HTTP の代わりにセキュア HTTP（HTTPS）を使用できます。ただし、Configuration Assistant を使用してデフォルトの HTTPS ポート番号を変更することはできません。HTTPS を使用する場合の要件については、「HTTPS の使用」を参照してください。

次の手順に従います。

1. [HTTPポート]フィールドに別のポート番号を入力します。

   デフォルトのポート番号は 80 です。有効な別のポート番号の範囲は 1025 から 65535 です。

2. [OK]をクリックします。

新しい HTTP ポート番号がコミュニティのすべてのメンバに伝達されます。

CE520 スイッチを管理する場合

[IGMPスヌーピング]ウィンドウ

このウィンドウには次のタブがあります。

- [設定]。ほとんどの場合 IGMP スヌーピングが個々の VLAN で有効になります。
- [マルチキャストグループ]。マルチキャスト グループが表示されます。
- [マルチキャストルータポート]。マルチキャスト ルータのポートが表示されます。

[設定]タブで選択する前に、[ホスト名]リストでデバイスを選択します。このタブ上で選択したすべての項目は、選択したデバイスに適用されます。

設定を変更するには、次の手順に従います。

1. [IGMPスヌーピングを有効にする]は、デフォルトでオンになっています。デバイス全体で IGMP スヌーピングを無効にする場合に限り、オフにします。
2. スイッチ　ポートが所属する VLAN と、その VLAN に対する設定はテーブル上に示されています。デフォルトでは、IGMP スヌーピングが VLAN 上で有効になっています。これらのデフォルトを変更するには、[修正]をクリックし、[IGMPスヌーピング設定の修正]ウィンドウを使用します。
3. [IGMPスヌーピング]ウィンドウに戻ったら、[OK]をクリックします。

注：[マルチキャストグループ]タブおよび[マルチキャストルータポート]タブに記載された情報は、読み取り専用で変更できません。

CE520 スイッチを管理する場合

[IGMPスヌーピング設定の修正]ウィンドウ

このウィンドウは、[IGMPスヌーピング]ウィンドウで[設定]タブを表示している際に、[VLAN]を選択して[修正]をクリックした場合に表示されます。このウィンドウを使用して、選択した VLAN の IGMP スヌーピングを有効または無効にします。

次の手順に従います。

- [ステータス]リストで[有効]または[無効]のいずれかを選択します。
- 変更したら、[OK]をクリックします。[IGMPスヌーピング]ウィンドウが表示されます。

CE520 スイッチを管理する場合

[IPアドレス]ウィンドウ

このウィンドウは、機能バーで **設定 > デバイスプロパティ > IPアドレス** を選択した場合に表示されます。

このウィンドウを使用して、IP アドレスをデバイス上に設定された VLAN に割り当てます。デバイスには 1 つの IP アドレスしか割り当てることができないので、実際には 1 つの IP アドレスをデバイスに割り当てます。

まず、[ホスト名]リストでデバイスおよび IP アドレスのタイプ([静的IP]または[DHCP])を選択します。[静的IP]を選択した場合、相手先静的 IP アドレスを割り当て、[DHCP]を選択した場合 DHCP により動的 IP アドレスが割り当てられます。

注: [DHCP]を選択した場合、デバイスの MAC アドレスによる IP アドレスのバインディングでデバイスを再起動するたびに、DHCP によって同じ IP アドレスが割り当てられたことを確認してください。支援が必要な場合には、DHCP サーバ管理者に問い合わせてください。

次のタブを使用します。

- [インターフェイス設定]。IP アドレスおよびサブネット マスクを VLAN に割り当てます。
- [デバイス設定]。デフォルト ゲートウェイとドメイン名を、選択したデバイスに関連付けます。

完了したら、[OK]をクリックします。

[インターフェイス設定]

[インターフェイス名]カラムに、選択したデバイス上に設定された VLAN の名前が表示されます。これらの VLAN の 1 つには、すでに IP アドレスとサブネット マスクが指定されています。別の VLAN、IP アドレス、およびサブネット マスクを選択するには、[静的IP]をクリックします。これをクリックしないのは、別の VLAN を選択する場合のみです。DHCP により IP アドレスおよびサブネット マスクが割り当てられます。

別の VLAN を選択するには、[インターフェイス名]カラムで VLAN 名をクリックし、ドロップダウン リストで別の VLAN を選択します。

静的 IP アドレスを割り当てるには、[IPアドレス]カラムにそのアドレスを入力します。

新規サブネット マスクを割り当てるには、[サブネットマスク]カラムでサブネット マスクをクリックし、ドロップダウン リストで別のサブネットマスクを選択します。

[デバイス設定]

1. [デフォルト ゲートウェイ]フィールドに、デバイスから不明なアドレスを含むトラフィックが送信される送信先の IP アドレスを入力します。
2. [ドメイン名]フィールドに、IP ネットワーク内で管理地域を識別する名前を入力します(この情報は、ネットワーク管理者に問い合わせる必要がある場合があります)。ネットワーク トラフィックにドメイン名が無い場合には、入力した名前がデバイスの名前に追加され、完全修飾ドメイン名がデバイスのホスト名テーブルに追加されます。
3. [ドメイン検索を有効にする]チェックボックスをオンにして、サーバでデバイス名を IP アドレスに変換できるようにします。
4. [新しいサーバ]フィールドに、ドメインネームサーバとして使用するデバイスの名前を入力して、[追加]をクリックします。このデバイスは、[現在のサーバ]リストに追加されます。
5. デバイスをサーバとして使用することを停止するには、[現在のサーバ]リストからそのデバイスを選択して、[削除]をクリックします。

UC500 を管理する場合

[IPアドレス]ウィンドウ

このウィンドウは、機能バーで **設定 > デバイスプロパティ > IPアドレス** を選択した場合に表示されます。

このウィンドウを使用すると、[VLAN]ウィンドウを使用して作成した VLAN に IP アドレスを割り当てることができます。デバイスには 1 つの IP アドレスしか割り当てることができないので、実際には 1 つの IP アドレスをデバイスに割り当てます。

まず、[ホスト名]リストからデバイスを選択します。

次のタブを使用します。

- [インターフェイス設定]。IP アドレスおよびサブネット マスクを VLAN に割り当てます。
- [デバイス設定]。選択したデバイスにドメイン名を関連付けます。

完了したら、[OK]をクリックします。

[インターフェイス設定]

[インターフェイス名]カラムに、選択したデバイス上に設定された VLAN の名前が表示されます。これらの VLAN の 1 つには、すでに IP アドレスとサブネット マスクが指定されています。別の VLAN、IP アドレス、およびサブネット マスクを選択できます。

別の VLAN を選択するには、[インターフェイス名]カラムで VLAN 名をクリックし、ドロップダウン リストで別の VLAN を選択します。

新規サブネット マスクを割り当てるには、[サブネットマスク]カラムでサブネット マスクをクリックし、ドロップダウン リストで別のサブネットマスクを選択します。

[デバイス設定]

1. [ドメイン名]フィールドに、IP ネットワーク内で管理地域を識別する名前を入力します(この情報は、ネットワーク管理者に問い合わせる必要がある場合があります)。ネットワーク トラフィックにドメイン名が無い場合には、入力した名前がデバイスの名前に追加され、完全修飾ドメイン名がデバイスのホスト名テーブルに追加されます。
2. [ドメイン検索を有効にする]チェックボックスをオンにして、サーバでデバイス名を IP アドレスに変換できるようにします。
3. [新しいサーバ]フィールドに、ドメインネームサーバとして使用するデバイスの名前を入力して、[追加]をクリックします。このデバイスは、[現在のサーバ]リストに追加されます。
4. デバイスをサーバとして使用することを停止するには、[現在のサーバ]リストからそのデバイスを選択して、[削除]をクリックします。

AP521 を管理する場合

[LAPに変換]ウィンドウ

このウィンドウを使用して、自律型アクセスポイントをライトウェイト アクセスポイントにアップグレードします。

自律型アクセスポイントのライトウェイト アクセスポイントへの変換

次の表は、[LAPに変換]ウィンドウのカラムについて説明しています。

カラム	説明
[デバイス]	デバイスのアイコンとホスト名が表示されます。
[変換]	デバイスが**変換**用に選択されているかどうかを示します。
[デバイスタイプ]	デバイスのタイプを示します。
[現在のバージョン]	現在の Cisco IOS のバージョンを示します。
[復旧イメージ名]	[変換の設定]ウィンドウに入力した Cisco IOS tar ファイルの名前が表示されます。ファイル名だけが表示され、パスは表示されません。
[変換ステータス]	変換のステータスおよび進捗状況のメッセージが表示されます。詳細については、[変換ステータス]ウィンドウを参照してください。
[IPアドレス]	[変換の設定]ウィンドウに入力した、静的または DHCP のどちらかの IP アドレス設

	定が表示されます。
[ホスト名]	[変換の設定]ウィンドウに入力した、[保持する]または[保持しない]のどちらかのホスト名設定が表示されます。

自律型アクセスポイントをライトウェイト アクセスポイントへ変換するには、次の手順に従います。

1. 自律型アクセスポイントの変換に使用する Cisco IOS tar ファイルをダウンロードします。
2. 1 つまたは複数の自律型アクセスポイントを選択します。
3. [変換の設定]をクリックします。
4. [変換の設定]ウィンドウを完了したら、[OK]をクリックし入力内容を保存します。
5. 変換対象デバイスの横にある[変換]チェックボックスをオンにします。
6. [変換]をクリックして変換処理を開始します。

   注:現在のイメージは削除され、新しいイメージがダウンロードされます。コマンドライン インターフェイス(CLI)を使用して、現在のイメージを保存できます。

7. [ステータス]をクリックすると、[変換ステータス]ウィンドウが表示されます。このウィンドウには、変換の進捗状況が表示されます。
8. 変換処理が完了すると、確認のダイアログが表示されます。ステータスのメッセージに、正常に変換されたアクセスポイントと正常に変換されなかったアクセスポイントが一覧表示されます。
9. 設定に加えた変更はすべて自動的にフラッシュ メモリに保存されます。1 分後、デバイスはリロードされ、新しいイメージの実行が開始します。その後に[LAPに変換]ウィンドウを閉じることができます。

   注:デバイスをリロードすると、そのデバイスへの接続は失われます。

CE520 スイッチを管理する場合

[MACアドレス]ウィンドウ

このウィンドウでは、MAC アドレス テーブルを表示したり、クリアしたりできます。

次の手順に従います。

1. [ホスト名]リストから、保存されている MAC アドレスを表示するスイッチを選択します。
2. *オプション:*アドレスを削除して、テーブルをクリアするには、[すべてを削除]をクリックします。
3. [OK]をクリックしてウィンドウを閉じます。

次の表では、テーブルのカラムについて説明しています。

カラム	**意味**
MACアドレス	接続されているデバイスの MAC アドレス

VLAN ID	送信側インターフェイス上で設定されている VLAN ID
出力インターフェイス	送信側 MAC アドレスが MAC アドレス カラム内の 1 つと一致した場合の、受信パケットの転送先インターフェイス

CE520 スイッチを管理する場合

[MACアドレスの修正]ウィンドウ

このウィンドウは、[ネットワークセキュリティの設定]ウィンドウで 1 つまたは複数の MAC アドレスを選択して[修正]をクリックした場合に表示されます。

単一の MAC アドレスを選択した場合には、アドレスはウィンドウ内に表示され、複数の MAC アドレスを選択した場合には、[MACアドレス: 複数]が表示されます。

[承認]リストで、[はい]または[いいえ]を選択し、[OK]をクリックします。選択した MAC アドレスのステータスは、それぞれのステータスに応じて変わります。

CE520 スイッチを管理する場合

[MACアドレスの追加]ウィンドウ

このウィンドウは、[ネットワークセキュリティの設定]ウィンドウを[中]セキュリティ レベルに設定して[事前承認されたMACアドレスの追加]をクリックした場合に表示されます。

[MACアドレス]フィールドに MAC アドレスを入力して、[OK]をクリックします。MAC アドレスが[ネットワークセキュリティの設定]ウィンドウに[はい]という承認ステータスで表示されます。

UC500、Cisco 800シリーズルータを管理する場合

[NAT]ウィンドウ

[ホスト名]リストから、NAT を有効にするデバイスを選択します。

NAT を有効にするには、[外部インターフェイス]リストから、(信頼できない)外部インターフェイスを選択します。

NAT の設定全体を削除するには、次の手順に従います。

1. [外部インターフェイス]リストから[インターフェイスの削除]を選択します。
2. [外部インターフェイス]リストから[インターフェイスの削除]を選択します。ウィンドウが開き、このまま処理を続行すると NAT の設定が削除されるという警告が表示されます。

3. NAT を削除してダイアログを閉じるには、[OK]をクリックします。
4. ウィンドウを閉じて変更を保存するには、[OK]をクリックします。

各ポート マッピングのエントリを作成するには、次の手順に従います。

1. エントリを[NAT]ウィンドウに追加するには、[追加]をクリックします。
2. [サービスタイプ]メニューからサーバの種類を選択します。
3. [プライベートIPアドレス]フィールドに、サーバが内部ネットワーク上で使用する IP アドレスを入力します。これは、インターネット経由で外部から使用することのできない IP アドレスです。
4. [オリジナルポート]フィールドに、内部デバイスのポート番号を入力します。これは、サーバが内部ネットワークからのサービス リクエストを受け入れる場合に使用するポート番号です。
5. [変換後ポート]フィールドに、NAT がこの変換に使用するポート番号を入力します。このポート番号は、サーバが、インターネットからのサービス リクエストを受け入れる際に使用します。
6. ウィンドウを閉じて変更を保存するには、[OK]をクリックします。

ポート マッピングを削除するには、次の手順に従います。

1. ウィンドウからエントリを選択します。
2. [削除]をクリックします。
3. ウィンドウを閉じて変更を保存するには、[OK]をクリックします。

ファイアウォールを追加することによってセキュリティを強化するには、[ファイアウォール サービス]をクリックし、[ファイアウォール]ウィンドウを使用します。

UC500、Cisco 800シリーズルータを管理する場合

[NAT]ウィンドウ

このウィンドウは、**設定 > セキュリティ > NAT** を選択した場合に表示されます。

まず、[ホスト名]リストから、NAT を有効にするデバイスを選択します。

NAT を有効にするには、[外部インターフェイス]リストから、(信頼できない)外部インターフェイスを選択します。

各ポート マッピングのエントリを作成するには、次の手順に従います。

1. エントリを[NAT]ウィンドウに追加するには、[追加]をクリックします。
2. [サービスタイプ]メニューからサーバの種類を選択します。
   - [ウェブサーバ]
   - [セキュア ウェブ サーバ]
   - [メール サーバ]
   - [FTP]
   - [SSH]

- [SFTP]
- [その他(TCP)]
- [その他(UDP)]

3. [プライベートIPアドレス]フィールドに、サーバが内部ネットワーク上で使用する IP アドレスを入力します。これは、インターネット経由で外部から使用することのできない IP アドレスです。
4. [オリジナルポート]フィールドに、内部デバイスのポート番号を入力します。これは、サーバが内部ネットワークからのサービス リクエストを受け入れる場合に使用するポート番号です。
5. [変換後ポート]フィールドに、NAT がこの変換に使用するポート番号を入力します。このポート番号は、サーバが、インターネットからのサービス リクエストを受け入れる際に使用します。
6. ウィンドウを閉じて変更を保存するには、[OK]をクリックします。

ポート マッピングを削除するには、次の手順に従います。

1. ウィンドウからエントリを選択します。
2. [削除]をクリックします。
3. ウィンドウを閉じて変更を保存するには、[OK]をクリックします。

NAT の設定全体を削除するには、次の手順に従います。

1. [外部インターフェイス]リストから[インターフェイスの削除]を選択します。ウィンドウが開き、このまま処理を続行すると NAT の設定が削除されるという警告が表示されます。
2. NAT を削除してダイアログを閉じるには、[OK]をクリックします。
3. ウィンドウを閉じて変更を保存するには、[OK]をクリックします。

ファイアウォールを追加することによってセキュリティを強化するには、[ファイアウォール サービス]をクリックし、[ファイアウォール]ウィンドウを使用します。

WLC526 を管理する場合

[RADIUSサーバ]ウィンドウ

このウィンドウは、[無線ネットワーク]ウィンドウの[RADIUSサーバ]領域の[設定] をクリックした場合に表示されます。

このウィンドウを使用すると、WLAN コントローラの RADIUS サーバ設定を表示したり、WLAN コントローラに最大 2 つの RADIUS サーバを設定したりできます。

次の表は、このウィンドウのカラムについて説明しています。

カラム	説明
IPアドレス	RADIUS サーバの IP アドレス。
認証	RADIUS 認証ポート番号。

ポート	
優先順位	RADIUS サーバの優先順位。これによって、いずれかのサーバにアクセスできない場合に、サーバが使用される順序が指定されます。
ステータス	RADIUS サーバのステータス。[有効にされた]または[無効にされた]のいずれかです。

WLAN コントローラに RADIUS サーバを設定する手順は、次のとおりです。

1. [ホスト名] リストから対象の WLAN コントローラを選択します。
2. RADIUS サーバを設定するには、[作成] をクリックして、[RADIUSサーバの作成]ウィンドウに入力します。

設定を変更するには、RADIUS サーバの IP アドレスを選択して、[修正]をクリックし、[RADIUSサーバの修正]ウィンドウを使用します。

設定されている RADIUS サーバを削除するには、削除する RADIUS サーバの IP アドレスを選択して、[削除] をクリックします。

変更を保存してウィンドウを閉じるには、[RADIUSサーバ]ウィンドウで[OK] をクリックします。

WLC526 を管理する場合

[RADIUSサーバの作成]ウィンドウ

このウィンドウは、[RADIUSサーバの設定]ウィンドウで[作成] をクリックした場合に表示されます。このウィンドウを使用すると、RADIUS サーバ設定を指定できます。

次の手順に従います。

1. [IPアドレス] フィールドに、RADIUS サーバの IP アドレスを入力します。
2. [認証ポート] フィールドに、RADIUS 認証ポート番号を入力します。デフォルトの認証ポート番号は 1812 です。
3. [秘密鍵(ASCII)] フィールドに、WLAN コントローラで RADIUS サーバとの通信に使用する共有秘密を入力します。
4. [秘密鍵の確認] フィールドに、共有秘密をもう一度入力します。
5. サーバの優先順位キー リストから、サーバの優先順位を選択します。

   注:各 RADIUS サーバで、異なる優先順位を使用する必要があります。

6. [管理ステータス] リストから、[有効]または[無効]を選択します。
7. [OK] をクリックして、変更を保存し、ウィンドウを閉じます。

WLC526 を管理する場合

[RADIUSサーバの修正]ウィンドウ

このウィンドウは、[RADIUSサーバの設定]ウィンドウで[修正]をクリックした場合に表示されます。このウィンドウを使用すると、RADIUS サーバのステータスを変更できます。

次の手順に従います。

1. [管理ステータス] リストから、[有効にされた]または[無効にされた]を選択します。
2. [OK] をクリックして、変更を保存し、ウィンドウを閉じます。

CE520 スイッチを管理する場合

[SNMP管理]ウィンドウ

このウィンドウは、機能バーで **設定 > デバイスプロパティ > SNMP** を選択した場合に表示されます。

このウィンドウには次のタブがあります。

- [システムオプション]。管理情報をデバイスに割り当て、それによりデバイスを識別します。
- [コミュニティストリング]。コミュニティ ストリングを追加および削除します。
- [トラップマネージャ]。トラップ マネージャを追加および削除します。
- [ビュー]。ユーザのグループにアクセスできる MIB オブジェクトのビューを作成します。
- [グループ]。ビューをビューにアクセスできるグループに関連付けます。
- [ユーザ]。グループをそのグループに属するユーザに関連付けます。

まず、次の操作を実行します。

- [ホスト名]リストからデバイスを選択します。タブとその設定は、選択したデバイスに適用されます。デバイスが SNMP バージョン 3 以降をサポートしている場合にのみ、[ビュー]タブ、[グループ]タブ、および[ユーザ]タブが表示されます。
- [SNMPを有効にする]がオンになっていることを確認します。

タブにすべての設定を入力したら、[OK]をクリックします。

[システムオプション]

SNMP によりこのタブの各フィールドには最大 255 文字の入力が許可されますが、Configuration Assistant でこの情報は短縮されます。このため、入力は短くするようお勧めします（個々の手順については、下記のガイドラインを参照してください）。

システム オプションを割り当てるには、次の手順に従います。

1. [システムの場所]フィールドに、デバイスの物理的な場所を入力します。

   [システムの場所]フィールドには、最大 129 文字を入力できます。

2. [システム担当者の連絡先]フィールドに、デバイスを管理する組織名を入力します。

［システム担当者の連絡先］フィールドには、最大129 文字を入力できます。

［コミュニティストリング］

コミュニティ ストリングは、SNMP メッセージを認証するパスワードとして機能します。各コミュニティ ストリングは、MIB オブジェクトの情報の表示を許可する読み取り専用（RO）か、MIB オブジェクトの情報の表示および変更を許可する読み取りと書き込み（RW）のいずれかです。

最初の読み取り専用コミュニティ ストリングおよび最初の読み取りと書き込みコミュニティ ストリングは、［SNMP管理］ウィンドウに一覧表示されます。これらのコミュニティ ストリングは SNMP パケット ルーティングに必要なので、どのデバイス上からも削除しないでください。

SNMP 設定には、ユーザ定義のコミュニティ ストリングも追加できます。

コミュニティ ストリングの追加

選択したデバイスは、任意の長さのコミュニティ ストリングを無制限の数にわたってサポートします。

新規コミュニティ ストリングをデバイスに追加するには、次の手順に従います。

1. ［新規ストリング］フィールドに、文字列を入力します。
2. ［RO］（読み取り専用）または［RW］（読み取りと書き込み）を選択して、ストリングのタイプを指定します。
3. ［追加］をクリックして新規コミュニティ ストリングを［現在のストリング］リストに移動します。

   注： アクセス モードが読み取り専用の場合、このリストにコミュニティ ストリングは表示されません。

コミュニティ ストリングの削除

最初の読み取り専用コミュニティ ストリングまたは読み取りと書き込みコミュニティ ストリングを削除しないでください。これらのストリングは、SNMP 機能に必要です。

既存のコミュニティ ストリングを削除するには、次の手順に従います。

1. ［現在のストリング］リストで、削除するコミュニティ ストリングを選択します。

   すべてのコミュニティ ストリングを削除するには、［すべて選択］をクリックします。

2. ［削除］をクリックします。

［トラップマネージャ］

トラップ マネージャは、デバイスで生成されるシステム アラートであるトラップを受信する管理ステーションです。デフォルトでは、トラップ マネージャは定義されていません。また、トラップは送信されません。

選択したデバイスでトラップの送信を有効にするには、［トラップを有効にする］をオンにします。次に、各 IP 送信先で有効にするトラップ タイプのチェック ボックスをオンにします。

新規トラップ マネージャを追加するには、次の手順に従います。

1. [IP アドレス]フィールドに、新規トラップ マネージャの IP アドレスを入力します。
2. [コミュニティストリング]フィールドに、新規トラップ マネージャのコミュニティ ストリングを入力します。
3. [UDP ポート]フィールドに、トラップの送信先のトラップ マネージャの UDP ポートを入力します。
4. すべてのトラップ タイプをトラップ マネージャに送信するには、[全トラップの送信]をオンにします。そうでない場合には、送信するトラップ タイプのみをオンにします。

   トラップ タイプの説明については、選択したデバイスのマニュアルを参照してください。

5. [追加]をクリックして、入力内容を[現在のマネージャ]リストに移動します。

   注: アクセス モードが読み取り専用の場合、このリストにトラップ マネージャおよびそのコミュニティ ストリングは表示されません。

トラップ マネージャを削除するには、次の手順に従います。

1. [現在のマネージャ]リストで、削除するトラップ マネージャを選択します。

   すべての既存トラップ マネージャを削除するには、[すべて選択]をクリックします。

2. [削除]をクリックします。

[ビュー]

このタブには、ビューの名前、すなわち次のようなアクセス権のユーザ グループに対する MIB オブジェクトの収集が表示されます。

- 読み取りアクセス権
- 書き込みアクセス権
- 通知権限

ビューを作成してこのタブにその名前を追加するには、[作成]をクリックして[SNMPビューの作成]ウィンドウを使用します。

ビューを変更するには、変更するビューを選択して、[修正]をクリックし、[SNMPビュー修正]ウィンドウを使用します。

ビューを削除するには、削除するビューを選択して、[削除]をクリックします。

注: [v1default]ビューを削除または変更することはできません。

[グループ]

このタブのカラムの意味は、次のとおりです。

カラム	意味
[グループ]	ユーザのグループ名

[セキュリティレベル]	ユーザはパスワードの入力を要求される([認証する])かどうか、およびそのパスワードは暗号化されている([プライバシー])かどうか
[読み取りビュー]	グループが読み取りアクセス権を持っている場合のビュー
[書き込みビュー]	グループが書き込みアクセス権を持っている場合のビュー
[通知ビュー]	グループが通知権限を持っている場合のビュー

グループを作成してこのタブにその属性を追加するには、[作成]をクリックして[SNMPグループの作成]ウィンドウを使用します。

グループを変更するには、変更するグループを選択して、[修正]をクリックし、[SNMPグループの修正]ウィンドウを使用します。

グループを削除するには、削除するグループを選択して、[削除]をクリックします。

注:[v1default]グループを削除または変更することはできません。

[ユーザ]

次の表は、このタブのカラムの内容について説明しています。

カラム	内容
[ユーザ]	ユーザ名
[グループ]	隣接するユーザが属するグループ
[認証アルゴリズム]	認証用パスワードの暗号化に使用されるアルゴリズムのタイプ

ユーザをグループに割り当てて、このタブにそのユーザを追加するには、[作成]をクリックして[SNMPユーザの作成]ウィンドウを使用します。

ユーザが属するグループも含めたユーザの属性を変更するには、ユーザのエントリを選択して[修正]をクリックし、[SNMPユーザの修正]ウィンドウを使用します。

ユーザを削除するには、そのユーザのエントリを選択して[削除]をクリックします。

UC500 を管理する場合

[SNMP管理]ウィンドウ

このウィンドウは、機能バーで **設定 > デバイスプロパティ > SNMP** を選択した場合に表示されます。

このウィンドウには、次のタブがあります。

- [システムオプション]。管理情報をデバイスに割り当て、それによりデバイスを識別します。
- [コミュニティストリング]。コミュニティ ストリングを追加および削除します。
- [トラップマネージャ]。トラップ マネージャを追加および削除します。
- [ビュー]。ユーザのグループにアクセスできる MIB オブジェクトのビューを作成します。
- [グループ]。ビューをビューにアクセスできるグループに関連付けます。
- [ユーザ]。グループをそのグループに属するユーザに関連付けます。

まず、次の操作を実行します。

- [ホスト名]リストからデバイスを選択します。タブとその設定は、選択したデバイスに適用されます。デバイスが SNMP バージョン 3 以降をサポートしている場合にのみ、[ビュー]タブ、[グループ]タブ、および[ユーザ]タブが表示されます。
- [SNMPを有効にする]がオンになっていることを確認します。

タブにすべての設定を入力したら、[OK]をクリックします。

[システムオプション]

SNMP によりこのタブの各フィールドには最大 255 文字の入力が許可されますが、Configuration Assistant でこの情報は短縮されます。このため、入力は短くするようお勧めします（個々の手順については、下記のガイドラインを参照してください）。

システム オプションを割り当てるには、次の手順に従います。

1. [システムの場所]フィールドに、デバイスの物理的な場所を入力します。

   [システムの場所]フィールドには、最大 129 文字を入力できます。

2. [システム担当者の連絡先]フィールドに、デバイスを管理する組織名を入力します。

   [システム担当者の連絡先]フィールドには、最大129 文字を入力できます。

[コミュニティストリング]

コミュニティ ストリングは、SNMP メッセージを認証するパスワードとして機能します。各コミュニティ ストリングは、MIB オブジェクトの情報の表示を許可する読み取り専用（RO）か、MIB オブジェクトの情報の表示および変更を許可する読み取りと書き込み（RW）のいずれかです。

最初の読み取り専用コミュニティ ストリングおよび最初の読み取りと書き込みコミュニティ ストリングは、[SNMP管理]ウィンドウに一覧表示されます。これらのコミュニティ ストリングは SNMP パケット ルーティングに必要なので、どのデバイス上からも削除しないでください。

SNMP 設定には、ユーザ定義のコミュニティ ストリングも追加できます。

コミュニティ ストリングの追加

選択したデバイスは、任意の長さのコミュニティ ストリングを無制限の数にわたってサポートします。

新規コミュニティ ストリングをデバイスに追加するには、次の手順に従います。

1. [新規ストリング]フィールドに、文字列を入力します。
2. [RO](読み取り専用)または[RW](読み取りと書き込み)を選択して、ストリングのタイプを指定します。
3. [追加]をクリックして新規コミュニティ ストリングを[現在のストリング]リストに移動します。

   注:アクセス モードが読み取り専用の場合は、このリストにコミュニティ ストリングは表示されません。

コミュニティ ストリングの削除

最初の読み取り専用コミュニティ ストリングまたは最初の読み取りと書き込みコミュニティ ストリングを削除しないでください。これらのストリングは、SNMP 機能に必要です。

既存のコミュニティ ストリングを削除するには、次の手順に従います。

1. [現在のストリング]リストで、削除するコミュニティ ストリングを選択します。

   すべてのコミュニティ ストリングを削除するには、[すべて選択]をクリックします。

2. [削除]をクリックします。

[トラップマネージャ]

トラップ マネージャは、デバイスで生成されるシステム アラートであるトラップを受信する管理ステーションです。デフォルトでは、トラップ マネージャは定義されていません。また、トラップは送信されません。

新規トラップ マネージャを追加するには、次の手順に従います。

1. [IPアドレス]フィールドに、新規トラップ マネージャの IP アドレスを入力します。
2. [コミュニティストリング]フィールドに、新規トラップ マネージャのコミュニティ ストリングを入力します。
3. [UDP ポート]フィールドに、トラップの送信先のトラップ マネージャの UDP ポートを入力します。
4. 送信するトラップ タイプに対応するチェック ボックスをオンにします。

   トラップ タイプの説明については、選択したデバイスのマニュアルを参照してください。

5. [追加]をクリックして、入力内容を[現在のマネージャ]リストに移動します。

   注: アクセス モードが読み取り専用の場合、このリストにトラップ マネージャおよびそのコミュニティ ストリングは表示されません。

トラップ マネージャを削除するには、次の手順に従います。

1. [現在のマネージャ]リストで、削除するトラップ マネージャを選択します。

   すべての既存トラップ マネージャを削除するには、[すべて選択]をクリックします。

2. [削除]をクリックします。

[ビュー]

このタブには、ビューの名前、すなわち次のようなアクセス権のユーザ グループに対する MIB オブジェクトの収集が表示されます。

- 読み取りアクセス権
- 書き込みアクセス権
- 通知権限

ビューを作成してこのタブにその名前を追加するには、[作成]をクリックして[SNMPビューの作成]ウィンドウを使用します。

ビューを変更するには、変更するビューを選択して、[修正]をクリックし、[SNMPビュー修正]ウィンドウを使用します。

ビューを削除するには、削除するビューを選択して、[削除]をクリックします。

注 : [v1default]ビューを削除または変更することはできません。

[グループ]

このタブのカラムの意味は、次のとおりです。

カラム	**意味**
グループ	ユーザのグループ名
セキュリティ レベル	ユーザはパスワードの入力を要求される([認証する])かどうか、およびそのパスワードは暗号化されている([プライバシー])かどうか
読み取り ビュー	グループが読み取りアクセス権を持っている場合のビュー
書き込み ビュー	グループが書き込みアクセス権を持っている場合のビュー
通知ビュー	グループが通知権限を持っている場合のビュー

グループを作成してこのタブにその属性を追加するには、[作成]をクリックして[SNMPグループの作成]ウィンドウを使用します。

グループを変更するには、変更するグループを選択して、[修正]をクリックし、[SNMPグループの修正]ウィンドウを使用します。

グループを削除するには、削除するグループを選択して、[削除]をクリックします。

注 : [v1default]グループを削除または変更することはできません。

[ユーザ]

次の表は、このタブのカラムの内容について説明しています。

カラム	内容
ユーザ	ユーザ名
グループ	隣接するユーザが属するグループ
認証アルゴリズム	認証用パスワードの暗号化に使用されるアルゴリズムのタイプ

ユーザをグループに割り当てて、このタブにそのユーザを追加するには、[作成]をクリックして[SNMPユーザの作成]ウィンドウを使用します。

ユーザが属するグループも含めたユーザの属性を変更するには、ユーザのエントリを選択して[修正]をクリックし、[SNMPユーザの修正]ウィンドウを使用します。

ユーザを削除するには、そのユーザのエントリを選択して[削除]をクリックします。

CE520 スイッチを管理する場合

[SNMPグループの作成]ウィンドウ

このウィンドウは、[SNMP]ウィンドウの[ユーザ]タブで[作成]をクリックした場合に表示されます。このウィンドウを使用して、SNMP ユーザの属性を指定します。

次の手順に従います。

1. [ユーザ名]フィールドに、ユーザの名前を入力します。
2. [グループ名]リストで、ユーザが属するグループを選択します(グループは最初に[グループ]タブで定義する必要があります)。
3. *オプション:* 認証用パスワードが必要なユーザの場合、[認証]領域で次の操作を実行します。
    1. [認証アルゴリズム]リストで認証アルゴリズムを選択します。
    2. ユーザが認証に対して入力する[パスワード]フィールドにパスワードを入力します。
    3. [パスワード確認]フィールドにパスワードをもう一度入力します。
4. [OK]をクリックします。[SNMP]ウィンドウに戻ると、[ユーザ]タブに新規エントリが表示されます。

CE520 スイッチを管理する場合

[SNMPグループの作成]ウィンドウ

このウィンドウは、[SNMP]ウィンドウの[グループ]タブで[作成]をクリックした場合に表示されます。このウィンドウを使用して、SNMP ユーザのグループの属性を指定します。

次の手順に従います。

1. [グループ名]フィールドに、新規グループの名前を入力します。

   別のセキュリティ レベルを選択すると、既存のグループ名を入力できます。グループ名およびセキュリティ レベルは、グループを一意に識別します。

2. [セキュリティレベル]リストで、セキュリティ レベルを選択します。

   [NoAuthenticate]は、パケットの認証が要求されないことを意味します。

   [認証する]は、パケットの認証を要求されることを意味します。

   [プライバシー]は、パケットの暗号化が要求されることを意味します。このオプションは、暗号ソフトウェア イメージがインストールされている場合に限り有効になります。

3. *オプション:* [読み取りビュー]リストで、読み取りアクセス権を取得するグループのビューを選択します。
4. オプション: [書き込みビュー]リストで、書き込みアクセス権を取得するグループのビューを選択します。
5. オプション: [通知ビュー]リストで、通知を送信するグループのビューを選択します。
6. [OK]をクリックします。[SNMP]ウィンドウに戻ると、[グループ]タブに新規エントリが表示されます。

CE520 スイッチを管理する場合

[SNMPグループの修正]ウィンドウ

このウィンドウは、グループを選択して、[SNMP]ウィンドウの[グループ]タブで[修正]をクリックした場合に表示されます。

変更できるグループの属性は、次のとおりです。

- 読み取りアクセス権のあるグループに対する MIB オブジェクトのビュー
- 書き込みアクセス権のあるグループに対する MIB オブジェクトのビュー
- 通知と共にグループに送信する MIB オブジェクトのビュー

これらのウィンドウのオプションの詳細については、「[SNMPグループの作成]ウィンドウのヘルプ トピック」を参照してください。

完了したら、[OK]をクリックします。

CE520 スイッチを管理する場合

[SNMPビュー修正]ウィンドウ

このウィンドウは、ビューを選択して、[SNMP]ウィンドウの[ビュー]タブで[修正]をクリックした場合に表示されます。

SNMP ビューを変更するには、次の手順に従います。

1. [OID]リストで、ビューに追加する OID を選択します。次に[追加]をクリックします。
2. [選択済み]リストで、ビューから削除する OID を選択します。次に[削除]をクリックします。
3. [OK]をクリックします。

CE520 スイッチを管理する場合

[SNMPビューの作成]ウィンドウ

このウィンドウは、[SNMP]ウィンドウの[ビュー]タブで[作成]をクリックした場合に表示されます。

[SNMP]ビューを作成するには、次の手順に従います。

1. [ビュー名]フィールドにビューの名前を入力します。
2. [OID]リストで 1 つまたは複数の OID（MIB オブジェクトの ID）を選択します。すべての OID を選択するには、[すべて選択]をクリックします。
3. [追加]をクリックして、選択した OID を[選択済み]リストに移動します。

   これらが、新規ビューを作成する OID となります。

   注：OID を[選択済み]リストに戻すには、目的の OID を選択して[削除]をクリックします。

4. [OK]をクリックします。作成したビューの名前が、[SNMP]ウィンドウの[ビュー]タブに表示されます。

CE520 スイッチを管理する場合

[SNMPユーザの修正]ウィンドウ

このウィンドウは、ユーザを選択して、[SNMP]ウィンドウの[ユーザ]タブで[修正]をクリックした場合に表示されます。

変更できるユーザの属性は、次のとおりです。

- ユーザが属するグループ。変更するには、異なるグループ名を選択します。
- 認証アルゴリズム（ある場合）。
- 認証用パスワードおよび確認用パスワード（ある場合）。

これらのウィンドウのオプションの詳細については、「[SNMPユーザの作成]ウィンドウのヘルプ トピック」を参照してください。

完了したら、[OK]をクリックします。

WLC526 を管理する場合

[SSIDの追加]ウィンドウ

このウィンドウは、[WLANユーザの作成]ウィンドウの[SSID]領域で[SSIDの追加]をクリックした場合に表示されます。このウィンドウを使用して、事前定義された SSID 設定を WLAN コントローラに適用します。

Cisco Configuration Assistant により、定められているセキュリティ タイプに対応する VLAN と SSID が設定されます。事前定義された SSID 設定を WLAN コントローラに適用すると、対応する WLAN を [WLAN (SSID)]ウィンドウから変更または削除できるようになります。また、対応する VLAN を [VLAN]ウィンドウから変更または削除できます。

SSID を追加するには、次の手順に従います。

1. [WLANの選択]領域から無線ネットワークのタイプを選択します。選択肢は次のとおりです。
   - [データ(Web認証、WPA1-PSKを使用)]
   - [音声(Web認証、WPA2-PSKを使用)]

     注: ゲスト ユーザを設定している場合は、[ゲスト(Web認証を使用)]オプションが選択されます。

2. [WLANの選択]での選択内容に応じて、次の情報を入力します。
   1. [VLAN ID (2-1000)]:VLAN の ID を入力します。
   2. [VLAN名]:データ ネットワークの場合は、事前定義された名前をそのまま使用するか、VLAN 用の別の名前を入力します。音声ネットワークまたはゲスト ネットワークの場合は、このフィールドには、WLAN の選択内容に基づいた事前定義された VLAN 名が設定されます。
   3. [IPアドレス]:VLAN の IP アドレスを入力します。
   4. [サブネットマスク]:VLAN のサブネット マスクを選択します。
   5. [ゲートウェイIPアドレス]:デフォルト ゲートウェイの IP アドレスを入力します。
   6. [DHCPサーバIPアドレス]:DHCP サーバの IP アドレスを入力します。
   7. [SSID]:会社名および WLAN の選択内容に基づいたデフォルトの SSID をそのまま使用するか、最大 32 文字の英数字からなる別の SSID を入力します。
   8. [WPA1事前共有キー](データ ネットワーク用)または[WPA2事前共有キー](音声ネットワーク用):8 ～ 63 文字の長さのキーを入力します。
3. このウィンドウに必要な情報を入力したら、[OK] をクリックして、変更を保存し、ウィンドウを閉じます。

CE520 スイッチを管理する場合

[STP]ウィンドウ

このウィンドウには、次のタブがあります。

- [STPステータス]。1 つまたは複数の VLAN 上のスパニング ツリー プロトコル(STP)を無効または有効にします。
- [現在のルート]。現在のスパニング ツリー のルート設定が表示されます。

まず、スイッチを[ホスト名]リストから選択します。タブの情報は、選択したスイッチに適用されます。

タブのポート情報のサブセットを表示するには、[フィルタ]をクリックして[フィルタエディタ]ウィンドウを使用します。[更新]をクリックし、デバイスをポーリングして最新データを表示します。

STP の設定が完了したら、[OK]をクリックします。

[STPステータス]

このタブには、スイッチ上の各 VLAN に対して STP が有効であるかどうかが示されます。デフォルトでは、STP は有効になっています。ただし、STP を無効にすると、スイッチを再設定する際にポートからのパケット転送で 30 秒の遅延を避けることができます。

このスイッチは、Per-VLAN Spanning-Tree plus (PVST+)プロトコルのみをサポートします。このプロトコルは、[スパニングツリー モード]リストの[pvst]で示されます。

注:STP の無効化は、ネットワーク トポロジにループがないことを確信している場合にのみ行ってください。STP を無効にしたトポロジにループが存在すると、過剰なトラフィックと無限のパケット重複によりネットワーク パフォーマンスが低下します。

STP を無効または有効にするには、次の手順に従います。

1. [VLAN ID]カラムで、STP を無効または有効にする VLAN を 1 つまたは複数選択します。
2. [スパニングツリー ステータス]カラムで、ドロップダウン リストから[有効]を選択し、選択した各 VLAN の STP を有効にします。[無効]を選択して、選択した各 VLAN の STP を無効にします。

[現在のルート]

各 VLAN に対して、[現在のルート]タブ(読み取り専用タブ)に現在のルート スイッチ上の STP 設定が表示されます。これらの設定は、別のスイッチで定義されている場合もあり、スイッチが VLAN ルートとして機能する際に有効になるパラメータを定義します。

[現在のルート]タブで説明される設定は、次のとおりです。

フィールド	説明
[VLAN ID]	スイッチがルートとして機能する際にこれらの設定が適用される VLAN。
[MAC アドレス]	ルート スイッチの MAC アドレス。
[優先順位]	ルート ブリッジを識別します。最低値を持つスイッチは最も優先度が高く、ルートとして選択されます。デフォルトは 32768 です。

[待機時間]	スイッチが再設定を試行する前に STP 設定メッセージを受信せずに待機する秒数を設定します。IEEE のデフォルトは 20 秒、IBM のデフォルトは 10 秒です。
[ハロータイム]	STP 設定メッセージ間の秒数を設定します。IEEE および IBM には 1 から 10 の数を入力します。デフォルトは 2 秒です。
[転送遅延]	ポートの STP ラーニングおよびリスニング ステートからフォワーディング ステートに変わる前に、ポートが待機する秒数を設定します。この遅延時間によって、スイッチがパケットをフォワードする前にループが形成されていないことが確認されます。IEEE のデフォルトは 15 秒、IBM のデフォルトは 4 秒です。
[ルートパスコスト]	送信先への最適なパスを判断するのに使用される相対的な基準。詳細については、「[パス コスト テーブル]」を参照してください。
[ルートポート]	これらの設定が適用されるポート。
[ルートブリッジ]	スイッチが実際にその VLAN の STP のルートの場合、フィールドに[はい]と表示されます。そうでない場合には、フィールドに[いいえ]と表示され、デバイスのルート ポートが[ルートポート]カラムに表示されます。

注： スパニング ツリー インスタンスの各スイッチは、設定方法とは関係なく、ルート ブリッジの hello、delay、および max age パラメータを採用します。

パス コスト テーブル

次の表は、異なる速度に対するデフォルトのパス コストの設定について説明しています。

パス コスト	スピード
100	10 Mbps
19	100 Mbps
14	155 Mbps
4	1 Gbps
2	10 Gbps
1	10 Gbps を超える速度

CE520 スイッチを管理する場合

[VLAN] ウィンドウ

[ホスト名]リストからデバイスを選択します。

次の操作を実行すると、テーブルの情報が更新されます。

- [作成]をクリックして VLAN を追加する。
- 情報の行を選択して[修正]をクリックし、VLAN を変更する。
- 情報の行を選択して[削除]をクリックし、VLAN を削除する。

CE520 スイッチを管理する場合

[VLAN]ウィンドウ

このウィンドウは、機能バーで **設定 > VLAN** を選択した場合に表示されます。

[ホスト名]リストからデバイスを選択すると、そのデバイスに関連付けられている VLAN の ID と名前が表示されます。1 つのデバイスに最大 15 の VLAN を関連付けることができます。

すべてのデバイスが、デフォルトで VLAN 1 に関連付けらます。VLAN をさらに作成しない限り、スマートポートを使用してポートの接続を設定する際にはこの VLAN を選択します（スマートポートに関する詳細については、ポートのクイック設定をクリックしてください）。IP Phone に接続されたポートがある場合には、それらのポートに対して音声 VLAN を作成することをお勧めします。

VLAN を作成するには、[作成]をクリックして、[VLANの作成]ウィンドウを使用します。

VLAN の名前を変更するには、このウィンドウで変更対象の VLAN を選択し、[修正]をクリックして[VLANの変更]ウィンドウでその名前を変更します。VLAN 1 は、Configuration Assistant で使用するために予約されているので、その名前を変更することはできません。

VLAN を削除するには、削除する VLAN を選択して、[削除]をクリックします。

注： Catalyst Express スイッチまたは Unified Communications 500 シリーズ プラットフォームで VLAN を作成、変更、または削除すると、それらの操作がコミュニティ内のこれらのタイプのすべてのデバイスに自動的に反映されます。これにより、デバイス間の VLAN の整合性が維持されます。もしも、コミュニティに追加しようとしているデバイスが VLAN に関連付けられている場合、その VLAN に関連付けられていないデバイスとの間で VLAN の競合が発生します。このような場合には、[VLAN競合解決]ウィンドウを使用して VLAN の整合性を復元するようにプロンプトが表示されます。

このウィンドウでの作業が完了したら、[OK]をクリックします。

UC500、Cisco 800シリーズルータを管理する場合

[VLAN]ウィンドウ

このウィンドウは、機能バーで **設定 > VLAN** を選択した場合に表示されます。

[ホスト名]リストからデバイスを選択すると、そのデバイスに関連付けられている VLAN の ID と名前が表示されます。1 つのデバイスに最大 15 の VLAN を関連付けることができます。すべてのデバイスが、デフォルトで VLAN 1 に関連付けられます。

VLAN を作成するには、[作成]をクリックして、[VLANの作成]ウィンドウを使用します。

VLAN の名前を変更するには、このウィンドウで変更対象の VLAN を選択し、[修正]をクリックして[VLANの修正]ウィンドウでその名前を変更します。VLAN 1 は、Configuration Assistant で使用するために予約されているので、その名前を変更することはできません。

VLAN を削除するには、削除する VLAN を選択して、[削除]をクリックします。

このウィンドウでの操作が完了したら、[OK]をクリックします。

WLC526 を管理する場合

[VLAN]ウィンドウ

このウィンドウは、機能バー上で **設定 > VLAN** を選択した場合に表示されます。

このウィンドウを使用すると、WLAN コントローラ上のすべての VLAN 設定を表示したり、WLAN コントローラにユーザ定義 VLAN を設定したりできます。

次の表は、このウィンドウのカラムについて説明しています。

カラム	説明
名前	読み取り専用 VLAN(management、ap-manager、および virtual)および読み取り/書き込み(ユーザ定義)VLANなどの VLAN 名
VLAN	VLAN に関連付けられている ID
IPアドレス	無線インターフェイスの IP アドレス。
タイプ	VLAN の種類。読み取り専用(management、ap-manager、および virtual)または読み取り/書き込み(ユーザ定義)のどちらかです。

WLAN コントローラにユーザ定義 VLAN を設定する手順は、次のとおりです。

1. [ホスト名] リストから対象の WLAN コントローラを選択します。
2. VLAN を作成するには、[作成]をクリックして、[VLANの作成]ウィンドウに必要な情報を入力します。

   注: 1 つのコントローラで最大 8 つのユーザ定義 VLAN をサポートできます。

設定を変更するには、VLAN 名を選択して[修正]をクリックし、[VLANの変更]ウィンドウを使用します。

設定を削除するには、VLAN 名を選択して[削除]をクリックします。

注: 変更したり削除したりできるのは、ユーザ定義 VLAN だけです。読み取り専用 VLAN の変更や削除はできません。

注: WLAN コントローラで VLAN を作成または変更すると、それらの操作がコミュニティ内のすべての Catalyst Express スイッチまたは Unified Communications 500 シリーズ プラットフォーム デバイスに自動的に反映されます。これにより、デバイス間の VLAN の整合性が維持されます。もしも、コミュニティに追加しようとしているデバイスが VLAN に関連付けられている場合、その VLAN に関連付けられていないデバイスとの間で VLAN の競合が発生します。このような場合には、[VLAN競合解決]ウィンドウを使用して VLAN の整合性を復元するようにプロンプトが表示されます。

変更を保存してウィンドウを閉じるには、[VLAN]ウィンドウで[OK]をクリックします。

CE520 スイッチを管理する場合

[VLAN競合解決]ウィンドウ

コミュニティ内のデバイスには、同一の VLAN を設定しておく必要があります。同一の VLAN が設定されていない場合、Configuration Assistant ではステータス バーにイベント アイコンが表示され、[イベント通知]ウィンドウに競合が記録されます。そのウィンドウでイベントを確認して[解決]をクリックした場合、[VLAN競合解決]ウィンドウが表示されます。このウィンドウで、VLAN の競合を解決します。

次の表は、このウィンドウのカラムについて説明しています。

カラム	説明
VLAN ID	競合する VLAN の ID。
競合	競合の説明。 • [存在しません]:VLAN がすべてのデバイス上で設定されていません。 • [別の名前で存在します]:すべてのデバイスで VLAN ID は一致していますが、VLAN 名が一致していません。
解決策	競合を解決するアクションのドロップダウン リスト。必要なアクションを選択します。

VLAN の各競合に対するアクションを選択したら、[解決]をクリックします。開いている[VLAN]ウィンドウで選択したアクションが反映されていることを確認します。

注:VLAN の各競合に対してアクションを選択するまでは、[解決]をクリックできません。

[VLAN]ウィンドウで[適用]をクリックしてアクションを保存し、別の作業を行うか、[OK]をクリックしてアクションを保存し、ウィンドウを閉じます。

CE520 スイッチを管理する場合

[VLANの作成]ウィンドウ

このウィンドウは、[VLAN]ウィンドウで[作成]をクリックした場合に表示されます。

VLAN を作成するには、次の手順に従います。

1. [VLAN ID]フィールドに VLAN の ID を入力します。

   2 から 1000の範囲の ID を使用します。1 は入力しないでください。この ID は予約されています。

2. [VLAN名]フィールドでは、デフォルト名は VLAN*xxxx* となります。この *xxxx* は VLAN ID 番号と等しい 4 桁(先頭のゼロを含む)を表します。デフォルト名をそのまま使用するか、データ VLAN タイプ用の 1 から 32 文字の VLAN 名を入力します。この名前は、管理ドメイン内で一意でなければなりません。

   音声 VLAN タイプとゲスト VLAN タイプの場合、このフィールドには、選択した VLAN タイプに基づいた事前定義された VLAN 名が設定されます。

3. [OK]をクリックします。

WLC526 を管理する場合

[VLANの作成]ウィンドウ

このウィンドウは、[VLAN]ウィンドウで[作成]をクリックした場合に表示されます。

VLAN を作成するには、次の手順に従います。

1. [VLANタイプ]選択領域で、データ、音声、ゲストのいずれかの VLAN タイプを選択します。

   注: 音声 VLAN とゲスト VLAN を 1 つずつだけ作成できます。音声 VLAN またはゲスト VLAN がすでに存在している場合は、このオプションはグレー表示になります。

2. [VLAN ID]フィールドに、VLAN に関連付ける VLAN ID を入力します。2 から 1000の範囲の ID を使用します。1 は入力しないでください。この ID は予約されています。
3. [VLAN名]フィールドにデータ VLAN タイプ用の別の VLAN 名を入力するか、デフォルトの VLAN 名をそのまま使用します。音声 VLAN タイプとゲスト VLAN タイプの場合、[VLAN名]フィールドには、選択した VLAN タイプに基づいた事前定義された VLAN 名が設定されます。
4. [ポート]リストから、VLAN のポートを選択します。
5. [IPアドレス]フィールドに、VLAN の IP アドレスを入力します。
6. [サブネットマスク]リストから、VLAN のサブネット マスクを選択します。
7. [ゲートウェイIPアドレス] フィールドに、デフォルト ゲートウェイの IP アドレスを入力します。
8. [DHCPサーバIPアドレス] フィールドに、DHCP サーバの IP アドレスを入力します。
9. このウィンドウに必要な情報を入力したら、[OK] をクリックして、変更を保存し、ウィンドウを閉じます。

CE520 スイッチを管理する場合

[VLANの作成]ウィンドウ

[VLAN ID]フィールドに VLAN の ID を入力します。2 から 1000 の範囲の ID を使用します。

注： VLAN ID 1 は予約されています。

[VLAN名]フィールドに、VLAN 名を入力します。これは 1 から 32 文字で、管理ドメイン内で一意のものにします。

デフォルト名は VLAN*nnnn* となります。この *nnnn* は VLAN ID 番号と等しい 4 桁（先頭のゼロを含む）を表します。

[VLANタイプ]選択領域で、データ、音声、ゲストのいずれかの VLAN タイプを選択します。

注: 音声 VLAN とゲスト VLAN を 1 つずつだけ作成できます。音声 VLAN またはゲスト VLAN がすでに存在している場合は、このオプションはグレー表示になります。

[VLANタイプ]は変更できません。[次へ]をクリックして続行します。

[VLAN名]フィールドにデータ VLAN タイプ用の別の VLAN 名を入力するか、デフォルトの VLAN 名をそのまま使用します。音声 VLAN タイプとゲスト VLAN タイプの場合、[VLAN名]フィールドには、選択した VLAN タイプに基づいた事前定義された VLAN 名が設定されます。

[VLAN名]は変更できません。[次へ]をクリックして続行します。

[ポート]リストから、VLAN のポートを選択します。

[IPアドレス]フィールドに、VLAN の IP アドレスを入力します。

[サブネットマスク]リストから、VLAN のサブネット マスクを選択します。

[ゲートウェイIPアドレス] フィールドに、デフォルト ゲートウェイの IP アドレスを入力します。

[DHCPサーバIPアドレス] フィールドに、DHCP サーバの IP アドレスを入力します。

CE520 スイッチを管理する場合

[VLANの作成] ウィンドウ

このウィンドウは、[VLAN]ウィンドウで VLAN を選択して[修正]をクリックした場合に表示されます。

VLAN ID を変更することはできません。VLAN 名を変更するには、次の手順に従います。

1. [VLAN名]フィールドに、新しい VLAN 名を入力します。
2. [OK]をクリックします。

WLC526 を管理する場合

[VLANの追加]ウィンドウ

このウィンドウは、[WLANの作成]ウィンドウで[VLANの追加]をクリックした場合に表示されます。

VLAN を追加するには、次の手順に従います。

1. [VLAN ID]フィールドに、VLAN に関連付ける VLAN ID を入力します。
2. [VLAN名]フィールドにデータ VLAN タイプ用の別の VLAN 名を入力するか、デフォルトの VLAN 名をそのまま使用します。音声 VLAN タイプとゲスト VLAN タイプの場合、[VLAN名] フィールドには、選択した VLAN タイプに基づいた事前定義された VLAN 名が設定されます。
3. [ポート]リストから、VLAN のポートを選択します。
4. [IPアドレス]フィールドに、VLAN の IP アドレスを入力します。
5. [サブネットマスク]リストから、VLAN のサブネット マスクを選択します。
6. [ゲートウェイIPアドレス] フィールドに、デフォルト ゲートウェイの IP アドレスを入力します。
7. [DHCPサーバIPアドレス] フィールドに、DHCP サーバの IP アドレスを入力します。
8. このウィンドウに必要な情報を入力したら、[OK] をクリックして、変更を保存し、ウィンドウを閉じます。

WLC526 を管理する場合

[VLANの変更]ウィンドウ

このウィンドウは、[VLAN]ウィンドウで[修正]をクリックした場合に表示されます。

VLAN を変更するには、次の手順に従います。

1. [VLAN ID] フィールドに、無線インターフェイスに関連付ける VLAN ID を入力します。
2. [ポート] リストから、無線インターフェイスのポートを選択します。
3. [IP アドレス] フィールドに、無線インターフェイスの IP アドレスを入力します。
4. [サブネットマスク] リストから、無線インターフェイスのサブネット マスクを選択します。
5. [ゲートウェイIPアドレス] フィールドに、デフォルト ゲートウェイの IP アドレスを入力します。
6. [DHCPサーバIPアドレス] フィールドに、DHCP サーバの IP アドレスを入力します。
7. このウィンドウに必要な情報を入力したら、[OK] をクリックして、変更を保存し、ウィンドウを閉じます。

UC500、Cisco 800シリーズルータを管理する場合

[VPNサーバ]ウィンドウ

このウィンドウは、**設定 > セキュリティ > VPNサーバ** を選択した場合に表示されます。

まず、設定するデバイスを[ホスト名]リストから選択します。

Virtual Private Network(VPN; バーチャル プライベート ネットワーク)サーバを起動するには、[インターフェイス]リストからインターフェイスを選択します。デバイスで VPN サーバがすでに設定されている場合は、[インターフェイス]リストが淡色表示され、[削除]ボタンがアクティブになります。

VPN サーバを削除するには、次の手順に従います。

1. [削除]をクリックします。このまま処理を続行すると VPN サーバの設定が削除されることを警告するウィンドウが表示されます。
2. VPN サーバを削除してウィンドウを閉じるには、[はい]をクリックします。
3. 変更を保存してウィンドウを閉じるには、[OK]をクリックします。

ユーザ アカウント

VPN トンネル経由での接続を要求するユーザのユーザ アカウントを作成し、パスワードを設定するには、[作成]をクリックして[アカウントの追加]ウィンドウを使用します。

ユーザ アカウントを削除するには、対象のユーザ アカウントを選択して[削除]をクリックします。

許可されるユーザ接続数を制限するには、[使用可能な最大接続数]フィールドに接続数を入力します。最大接続数は 10 です。

事前共有鍵

事前共有鍵は、リモートの VPN デバイスに設定されている事前共有鍵と一致している必要があります。

暗号化トンネルを認証するには、次の手順に従います。

1. [新しい事前共有鍵の入力]フィールドに、事前共有鍵を入力します。事前共有鍵には、1 から 127 文字の英数字を使用できます。スペースと疑問符(?)は使用できません。
2. [新しい事前共有鍵の再入力]フィールドに、事前共有鍵を再入力します。

VPN リモート IP アドレスの範囲

IP アドレス プールとは、ユーザに割り当てることのできる IP アドレスの範囲のことです。接続数は 10 個の IP アドレスに制限されます。

IP アドレスの範囲を指定するには、次の手順に従います。

1. [開始IPアドレス]フィールドに、範囲の最初の IP アドレスを入力します。
2. [終了IPアドレス]フィールドに、範囲の最後の IP アドレスを入力します。

スプリット トンネリング

スプリット トンネリングを有効にし、暗号化によって保護するネットワークを指定するには、次の手順に従います。

1. [スプリットトンネリングを有効にする]チェックボックスをオンにします。
2. [作成]をクリックして[ネットワークの追加]ウィンドウを使用します。保護されたサブネットを宛先とするトラフィックだけが暗号化され、VPN トンネル経由でホーム ネットワークに送信されます。他のトラフィックはいずれも宛先のサブネットに送られますが、暗号化されず、VPN トンネルにより保護されることもありません。

保護されたサブネットを削除するには、次の手順に従います。

1. ネットワークとマスクを選択します。
2. [削除]をクリックします。

UC500、Cisco 800シリーズルータを管理する場合

[VPNサーバ]ウィンドウ

VPN サーバを設定するデバイスを[ホスト名]リストから選択します。

[インターフェイス]リストからインターフェイスを選択します。

デバイスで VPN サーバがすでに設定されている場合は、既存の VPN サーバを編集するか削除するかを選択できます。

VPN サーバを編集するには、[VPNサーバの編集]オプション ボタンを選択して[VPNサーバ]ウィンドウを使用します。

VPN サーバを削除するには、次の手順に従います。

1. [削除]オプション ボタンをクリックします。
2. [終了]をクリックします。このまま処理を続行すると VPN サーバの設定が削除されることを警告するウィンドウが表示されます。
3. VPN サーバを削除してウィンドウを閉じるには、[はい]をクリックします。

VPN トンネル経由での接続を要求するユーザのユーザ アカウントを作成し、パスワードを設定するには、[追加]をクリックして[アカウントの追加]ウィンドウを使用します。

ユーザ アカウントを削除するには、対象のユーザ アカウントを選択して[削除]をクリックします。

許可されるユーザ接続数を制限するには、[使用可能な最大接続数]フィールドに接続数を入力します。最大接続数は 10 です。

事前共有鍵は、リモートの VPN デバイスに設定されている事前共有鍵と一致している必要があります。

暗号化トンネルを認証するには、次の手順に従います。

1. [新しい事前共有鍵の入力]フィールドに、事前共有鍵を入力します。事前共有鍵には、1 から 127 文字の英数字を使用できます。スペースと疑問符(?)は使用できません。
2. [新しい事前共有鍵の再入力]フィールドに、事前共有鍵を再入力します。

IP アドレス プールとは、ユーザに割り当てることのできる IP アドレスの範囲のことです。

IP アドレスの範囲を指定するには、次の手順に従います。

1. [開始IPアドレス]フィールドに、範囲の最初の IP アドレスを入力します。
2. [終了IPアドレス]フィールドに、範囲の最後の IP アドレスを入力します。

スプリット トンネリングを有効にし、暗号化によって保護するネットワークを指定するには、次の手順に従います。

1. [スプリットトンネリングを有効にする]チェックボックスをオンにします。
2. [追加]をクリックして[ネットワークの追加]ウィンドウを使用します。保護されたサブネットを宛先とするトラフィックだけが暗号化され、VPN トンネル経由でホーム ネットワークに送信されます。他のトラフィックはいずれも宛先のサブネットに送られますが、暗号化されず、VPN トンネルにより保護されることもありません。

保護されたサブネットを削除するには、次の手順に従います。

1. ネットワークとマスクを選択します。
2. [削除]をクリックします。

UC500、Cisco 800シリーズルータを管理する場合

[VPNリモート]ウィンドウ

このウィンドウは、**設定 > セキュリティ > VPNリモート** を選択した場合に表示されます。

注:VPN サーバとの Virtual Private Network(VPN; バーチャル プライベート ネットワーク)接続を確立する唯一の方法は、ブラウズ時に PC から XAuth クレデンシャルを入力することです。ユーザが VPN トンネルを使用して中央サイト ネットワークに接続する手順は、次のとおりです。

まず、設定するデバイスを[ホスト名]リストから選択します。

音声サービスを有効にするには、[リモート接続で音声サービスを有効にする]チェック ボックスをオンにします。

VPN リモート サービスを有効にするには、次の手順に従います。

1. [CME IPアドレス]フィールドに、CME(Cisco Unified CallManager Express)IP アドレスを入力します。
2. [VPNサーバ]フィールドに、VPN サーバまたはコンセントレータの IP アドレスまたはホスト名を入力します。

3. オプション：[新しい事前共有鍵の入力]フィールドに、暗号化トンネルの認証に使用する事前共有鍵を入力します。共有鍵には 1 から 127 文字の英数字を使用できます。スペースと疑問符（?）は使用できません。リモート VPN デバイス上に事前共有鍵が設定されている場合、その共有鍵が VPN サーバ上に設定された事前共有鍵と一致している必要があります。
4. [新しい事前共有鍵の再入力]フィールドに、事前共有鍵を再入力します。
5. 変更を保存してウィンドウを閉じるには、[OK]をクリックします。

IPSec ポリシーを受け取るためのリモート デバイスに対する許可を解除するには、次の手順に従います。

1. [削除]をクリックします。このまま処理を続行すると VPN リモート設定が削除されることを警告するウィンドウが表示されます。
2. 変更を保存してウィンドウを閉じるには、[OK]をクリックします。

リモート ユーザと中央サイト ネットワーク間の VPN トンネルを確立するには、次の手順に従います。

1. Internet Explorer などの Web ブラウザ ウィンドウを起動します。
2. ブラウザの[アドレス]フィールドに、VPN サーバの IP アドレスを入力します。[VPN tunnel Activation Tool]ウィンドウが開き、VPN を使用して中央サイト ネットワークに接続するか、またはインターネットに接続するオプションが表示されます。
3. 中央サイト ネットワークに接続するには、[Connect Now]をクリックします。[Authentication for VPN tunnel Activation]ウィンドウが開きます。
4. UserName フィールドにユーザ名を入力します。
5. Password フィールドにパスワードを入力します。
6. [Continue]をクリックします。VPN トンネルが確立されます。

注：これらの手順は、Cisco 800 シリーズ ルータを使用してサービス プロバイダに接続しているエンド ユーザが、中央サイト ネットワークへの VPN トンネルを確立する方法について説明しています。（これらの手順は、システム管理者の便宜を図るために提供されています）。

UC500、Cisco 800シリーズルータを管理する場合

[VPN リモート]ウィンドウ

Virtual Private Network（VPN; バーチャル プライベート ネットワーク）を有効にするリモート デバイスを[ホスト名]リストから選択します。

VPN サーバとの VPN 接続を確立する唯一の方法は、ブラウズ時に PC から XAuth クレデンシャルを入力することです。VPN サーバの IP アドレスまたはホスト名、IP Security（IPSec; IP セキュリティ）グループ名、および事前共有鍵を知っている必要があります。

デバイスで VPN リモート接続がすでに設定されている場合は、既存の接続を編集するか削除するかを選択できます。

VPN リモート設定を編集するには、[VPNリモート接続の編集]オプション ボタンを選択して[VPNリモート]ウィンドウを使用します。

VPN リモート接続を削除するには、次の手順に従います。

1. すべての VPN リモート接続の削除オプション ボタンをクリックします。
2. [終了]をクリックします。このまま処理を続行すると VPN リモート設定が削除されることを警告するウィンドウが表示されます。
3. VPN リモート設定を削除してウィンドウを閉じるには、[はい]をクリックします。

音声サービスを有効にするには、次の手順に従います。

1. 音声サービスを有効にするには、[リモート接続で音声サービスを有効にする]チェックボックスをオンにします。
2. [CME IP アドレス]フィールドに、CME（Cisco Unified CallManager Express）IP アドレスを入力します。

[VPN サーバ]フィールドに、VPN サーバまたはコンセントレータの IP アドレスまたはホスト名を入力します。

オプション：[新しい事前共有鍵の入力]フィールドに、暗号化トンネルの認証に使用する事前共有鍵を入力し、[新しい事前共有鍵の再入力]フィールドに事前共有鍵を再入力します。共有鍵には 1 から 127 文字の英数字を使用できます。スペースと疑問符（?）は使用できません。リモート VPN デバイス上に事前共有鍵が設定されている場合、その共有鍵が VPN サーバ上に設定された事前共有鍵と一致している必要があります。

VPN トンネル経由でホーム ネットワークに接続されるリモート ネットワークが表示されます。

VPN トンネル経由で VPN サーバに接続される外部インターフェイスが表示されます。通常、これは、インターネットに接続された WAN インターフェイスです。

WLC526 を管理する場合

[Webログイン]ウィンドウ

このウィンドウは、[WLANユーザ]ウィンドウの[Webログイン]領域の[設定]をクリックした場合に表示されます。このウィンドウを使用して、WLAN ユーザ用の Web ログイン ページのコンテンツと概観をカスタマイズします。

ログイン ページは、Web 認証が有効になっている WLAN に Web ユーザが初めてアクセスする際に表示されます。シスコでは、テキスト ベースの HTML エディタを使用して変更が可能な、デフォルトの Web ログイン ページを提供しています。ただし、[ユーザ名]フィールドと[パスワード]フィールドは変更できません。また、Submit メソッドはそのまま残す必要があります。カスタマイズした Web ログイン ページを作成したら、それをページ コードと必要なイメージを含む tar ファイルにする必要があります。

ログイン ページを設定するには、次の手順に従います。

1. [ホスト名]リストから、対象の WLAN コントローラを選択します。
2. [Web認証]領域で、[内部]または[カスタマイズ]を選択します。

   [内部]を選択した場合は、次の手順を実行します。

1. [シスコのロゴ]領域で、[表示]を選択してログイン ページ上で シスコのロゴを表示するか、[非表示]を選択してロゴを非表示にします。デフォルトは[表示]です。
2. [ログイン後のリダイレクト先URL]フィールドに、ログインした後の移動先の URL を入力します。www.companyname.com の形式で、最大 254 文字の URL を入力します(「http://」は入力しないでください)。
3. [ヘッドライン]フィールドに、最大 127 文字でログイン ページの見出しまたは概要を入力します。デフォルトのヘッドラインは「Welcome to the Cisco wireless network.」です。
4. [メッセージ]フィールドに、最大 2047 文字でメッセージのテキストを入力します。デフォルトのメッセージは「Cisco is pleased to provide the wireless LAN infrastructure for your network. Please login and put your air space to work.」です。

   注 : デフォルトの設定を使用するには、[デフォルトに設定]をクリックします。

[カスタマイズ]を選択した場合は、次の手順を実行します。

5. [TFTPサーバIPアドレス]フィールドに、カスタマイズした Web 認証バンドル ファイルが存在する TFTP サーバの IP アドレスを入力します。

   注 : Cisco WCS と TFTP サーバは同じ通信ポートを使用するため、TFTP サーバを Cisco WCS と同じコンピュータ上で実行することはできません。

6. [最大試行回数]フィールドに、WLAN コントローラが TFTP サーバからの Web 認証ファイルのロードを失敗と判断するまでの試行回数を入力します。デフォルト値は 3 です。
7. [タイムアウト(秒)]フィールドに、タイムアウト期間を秒単位で入力します。この期間内に WLAN コンロトーラでファイルのダウンロードが開始できなかった場合は、ロードは実行されません。
8. [ファイルパス]フィールドに、TFTP サーバ上の Web 認証ファイルのパスを入力します。デフォルト値はスラッシュ(/)です。
9. [ファイル名]フィールドに、転送するファイルの名前を入力します。
10. [ダウンロード]をクリックして、カスタマイズしたログイン ファイルをダウンロードします。

    注 : [OK]または[適用]をクリックした場合は、ダウンロードが開始され、カスタマイズしたログイン ファイルがデバイスに適用されます。

    注 : ダウンロード処理には少なくとも 3 分はかかります。また、この処理により既存のログイン ファイルが上書きされます。

3. このウィンドウに必要な情報を入力したら、[OK] をクリックして、変更を保存し、ウィンドウを閉じます。

AP521 を管理する場合

[WLAN (SSID)]ウィンドウ

このウィンドウは、機能バー上で **設定 > 無線 > WLAN(SSID)** を選択した場合に表示されます。

このウィンドウを使用すると、自律型アクセスポイントのセキュリティを設定したり、自律型アクセスポイントに設定されているセキュリティ設定を表示したりできます。

次の表は、このウィンドウのカラムについて説明しています。

カラム	説明
SSID	アクセスポイントに設定されている SSID
VLAN	SSID に関連付けられている VLAN
セキュリティ	セキュリティ設定 • ［セキュリティなし］ • ［WEP］ • ［EAP］ • ［LEAP］ • ［WPA］ • ［WPA-PSK］ • ［WPA2］ • ［WPA2-PSK］ • ［MAC］ • ［MAC & EAP］ • ［不明］：これは、セキュリティ設定が、コマンドライン インターフェイスを使用して設定されており、Configuration Assistant ではサポートされていない場合に表示されます。
暗号化	暗号化タイプ • ［なし］ • ［WEP］ • ［動的 WEP］ • ［TKIP］ • ［AES CCMP］
認証	認証タイプ（複数も可） • ［Open］ • ［Open EAP］ • ［Network EAP］ • ［WPA-PSK］

自律型アクセスポイントにセキュリティを設定するには、次の手順に従います。

1. ［ホスト名］リストからアクセスポイントを選択します。
2. WLAN を作成してセキュリティ設定を選択するには、［作成］をクリックして、［WLANの作成］ウィンドウに必要な情報を入力します。

   注：1 つのアクセスポイントに最大 8 つの WLAN を作成できます。複数の WLAN を使用すると、ユーザは 1 つの自律型アクセスポイントから複数のネットワークにアクセスできるようになります。

設定を変更するには、WLAN を選択して［修正］をクリックし、［WLANの修正］ウィンドウを使用します。

設定を削除するには、WLAN を選択して［削除］をクリックします。

変更を保存してウィンドウを閉じるには、［OK］をクリックします。

WLC526 を管理する場合

［WLAN (SSID)］ウィンドウ

このウィンドウは、機能バー上で **設定 > 無線 > WLAN(SSID)** を選択した場合に表示されます。

このウィンドウを使用すると、WLAN コントローラおよびそれに関連付けられているアクセスポイントにセキュリティを設定したり、WLAN コントローラおよびそれに関連付けられているアクセスポイントに設定されているセキュリティ設定を表示したりできます。

次の表は、［無線ネットワーク名（SSID）］領域のカラムについて説明しています。

カラム	説明
SSID	関連付けられているアクセスポイントに設定されている SSID
VLAN	SSID に関連付けられている VLAN
セキュリティ	セキュリティ設定 • ［セキュリティなし］ • ［WEP］ • ［EAP］ • ［WPA］ • ［WPA-PSK］ • ［WPA2］ • ［WPA2-PSK］ • ［MAC］

	• [MAC & EAP] • [不明]:これは、セキュリティ設定が、コマンドライン インターフェイスを使用して設定されており、Configuration Assistant ではサポートされていない場合に表示されます。
暗号化	暗号化タイプ • [なし] • [WEP] • [TKIP] • [AES]
認証	認証タイプ • [Open] • [Shared key] • [802.1x] • [WPA-PSK]

WLAN コントローラにセキュリティを設定する手順は、次のとおりです。

1. [ホスト名] リストから対象の WLAN コントローラを選択します。
2. WLAN を作成してセキュリティ設定を選択するには、[作成]をクリックして、[WLANの作成]ウィンドウに必要な情報を入力します。

   注:1 つのアクセスポイントに最大 8 つの WLAN を作成でき、音声 WLAN と ゲスト WLAN を 1 つずつだけ作成可能です。VLAN ごとに 1 つの WLAN を設定できます。複数の WLAN を使用すると、ユーザは 1 つのアクセスポイントから複数のネットワークにアクセスできるようになります。

設定を変更するには、WLAN を選択して、[修正]をクリックし、[WLANの修正]ウィンドウを使用します。

設定を削除するには、WLAN を選択して[削除]をクリックします。

WLAN コントローラに RADIUS サーバを設定するには、[RADIUSサーバ]領域の[設定] をクリックします。

変更を保存してウィンドウを閉じるには、[無線ネットワーク]ウィンドウで[OK] をクリックします。

UC500、Cisco 800シリーズルータを管理する場合

[WLAN (SSID)]ウィンドウ

このウィンドウは、機能バーで **設定 > 無線 > WLAN(SSID)** を選択した場合に表示されます。

このウィンドウを使用すると、HWIC アクセスポイントにセキュリティを設定したり、HWIC アクセスポイントに設定されているセキュリティ設定を表示したりできます。

このウィンドウには、次の領域があります。

- ［無線ネットワーク名（SSID）］
- ［外部RADIUSサーバ］
- ［ローカルRADIUSサーバ］

次の表は、［無線ネットワーク名（SSID）］領域のカラムについて説明しています。

カラム	説明
SSID	アクセスポイントに設定されている SSID
VLAN	SSID に関連付けられている VLAN
セキュリティ	セキュリティ設定 • ［セキュリティなし］ • ［WEP］ • ［EAP］ • ［WPA］ • ［WPA-PSK］ • ［WPA2］ • ［WPA2-PSK］ • ［MAC & EAP］ • ［不明］：これは、セキュリティ設定が、コマンドライン インターフェイスを使用して設定されており、Configuration Assistant ではサポートされていない場合に表示されます。
暗号化	暗号化タイプ • ［なし］ • ［WEP］ • ［動的 WEP］ • ［TKIP］ • ［AES CCMP］
認証	認証タイプ（複数も可） • ［Open］ • ［Shared］

	• ［Open EAP］ • ［Network EAP］ • ［WPA-PSK］

次の表は、［外部RADIUSサーバ］領域のパラメータについて説明しています。

パラメータ	説明
［外部RADIUSサーバを有効にする］	外部 RADIUS サーバを有効または無効にします。EAP、WPA、WPA2、MAC、および MAC & EAP セキュリティ タイプで外部 RADIUS 認証を使用できるようになります。
［IPアドレス］	外部 RADIUS サーバの IP アドレスを入力します。
［秘密鍵］	HWIC アクセスポイントが外部 RADIUS サーバとの通信に使用する共有秘密を入力します。
［認証ポート］	RADIUS 認証ポート番号を入力します。デフォルトの認証ポート番号は 1812 です。
［課金ポート］	RADIUS アカウンティング ポート番号を入力します。デフォルトのアカウンティング ポート番号は 1813 です。

次の表では、［ローカルRADIUSサーバ］領域のパラメータについて説明してします。

パラメータ	説明
［ローカルRADIUSサーバを有効にする］	ローカル RADIUS サーバを有効または無効にします。EAP、WPA、WPA2、MAC、および MAC & EAP セキュリティ タイプでローカル RADIUS 認証を使用できるようになります。
［秘密鍵］	HWIC アクセスポイントが外部 RADIUS サーバとの通信に使用する共有秘密を入力します。
ユーザのユーザ名	ローカル RADIUS サーバを使用して認証を実行できるクライアントのユーザ名です。
ユーザのパスワード	ローカル RADIUS サーバを使用して認証を実行できるクライアントのパスワードです。
［MACアドレス］	ローカル RADIUS サーバを使用して認証を実行できるクライアントの MAC アドレスです。

HWIC アクセスポイントのセキュリティを設定するには、次の手順に従います。

1. ［ホスト名］リストから HWIC アクセスポイントを選択します。
2. WLAN を作成してセキュリティ設定を選択するには、［作成］をクリックして、［WLANの作成］ウィンドウに必要な情報を入力します。

注:1 つの HWIC アクセスポイントに最大 16 の WLAN を作成できます。複数の WLAN を使用すると、ユーザは 1 つの HWIC アクセスポイントから複数のネットワークにアクセスできるようになります。

無線設定を変更するには、WLAN を選択して、[修正]をクリックし、[WLANの修正]ウィンドウを使用します。

無線設定を削除するには、WLAN を選択して、[削除]をクリックします。

HWIC アクセスポイントに外部 RADIUS サーバを設定するには、次の手順に従います。

1. 外部 RADIUS サーバを設定するには、[外部RADIUSサーバを有効にする]をオンにします。
2. 外部 RADIUS サーバの IP アドレス、秘密鍵、認証ポート、およびアカウンティング ポートを入力します。

HWIC アクセスポイントにローカル RADIUS サーバを設定するには、次の手順に従います。

1. ローカル RADIUS サーバを設定するには、[ローカルRADIUSサーバを有効にする]をオンにして、ローカル RADIUS サーバの秘密鍵を入力します。
2. [追加]をクリックして、[ユーザ]または[MACアドレス]の表に新しい行を追加します。
3. 空白行をクリックして、ローカル認証に使用するクライアントのユーザ名とパスワード、またはクライアントの MAC アドレスを追加します。
4. エントリを変更するには、既存のユーザ名、パスワード、または MAC アドレス エントリをクリックします。
5. ユーザまたは MAC アドレスを削除するには、その行を選択して[削除]をクリックします。

変更を保存してウィンドウを閉じるには、[OK]をクリックします。

AP521 を管理する場合

[WLANの作成]ウィンドウ

このウィンドウは、[WLAN (SSID)]ウィンドウで[作成]をクリックした場合に表示されます。このウィンドウを使用すると、新しい SSID を作成したり、セキュリティ設定を指定したりできます。

次の手順に従います。

1. [SSID]フィールドに SSID を入力します。SSID には、最大 32 文字の英数字を使用できます。
2. SSID を指定しないデバイスが自律型アクセスポイントに関連付けられる(無線接続を確立できる)ように SSID をブロードキャストする場合は、[ビーコンのブロードキャスト]をオンにします。ビーコンには、1 つの SSID だけを含めることができます(guest SSID)。
3. [VLAN]フィールドで、SSID に関連付ける VLAN ID を入力するか、選択します。

   注:VLAN を SSID に割り当てる場合は、VLAN をすべての SSID に割り当てる必要があります。一部の SSID に VLAN を割り当て、それ以外の SSID には割り当てないようにすることはできません。

4. この VLAN をネイティブ VLAN にする場合は、[ネイティブ VLAN]ボックスをオンにします。
5. [セキュリティ設定]領域で、[セキュリティ]リストからセキュリティ設定を選択します。このウィンドウの他のオプションは、選択内容によって異なります。[セキュリティなし]、[WEP]、[EAP]、[LEAP]、[WPA]、[WPA-PSK]、[WPA2]、[WPA2-PSK]、[MAC]または[MAC & EAP]を選択できます。選択したセキュリティ設定に応じて、Configuration Assistant によって暗号化および認証タイプが自動的に選択されます。
6. このウィンドウに必要な情報を入力したら、[OK]をクリックして、変更を保存し、ウィンドウを閉じます。

[セキュリティなし]

これは最もセキュリティ レベルの低いオプションです。このオプションは、公共の場で使用されている SSID（guest SSID）に対してだけ選択し、ネットワークへのアクセスを制限する VLAN に関連付けます。暗号化は行われず、認証タイプはオープン認証です。

[WEP]

このセキュリティ設定では、自律型アクセスポイントとクライアント デバイス（ラップトップや PC など、無線デバイスに接続されているデバイス）で、同一の WEP キーを共有してプライベートな通信を維持することが必要です。暗号化タイプは WEP で、認証タイプはオープン認証です。

この種類のセキュリティを設定するには、次の手順に従います。

1. [パスフレーズ]フィールドにパスフレーズを入力し、リストからビット暗号化を選択します。
2. [生成]をクリックします。[キー]リストの横にある[キー]フィールドに自動的に値が入力されます。[キー]リストで 1、2、3、または 4 を選択することによって、キー番号を変更できます。デフォルトのキー番号は 1 です。

[EAP]

このセキュリティ設定では、IEEE 802.1X 認証が有効になり、RADIUS サーバの IP アドレスおよび共有秘密を入力する必要があります。暗号化タイプは動的 WEP で、認証タイプは EAP でのオープン認証です。

注：EAP セキュリティ タイプを選択する場合、無線クライアントは、EAP 設定（EAP-TLS、EAP-FAST、PEAP など）を使用する必要があります。無線クライアントは、LEAP 設定を使用できません。

この種類のセキュリティを設定するには、次の手順に従います。

1. RADIUS サーバの IP アドレスを入力します。
2. 自律型アクセスポイントで RADIUS サーバとの通信に使用する共有秘密を入力します。

[LEAP]

このセキュリティ設定では、IEEE 802.1X 認証が有効になり、RADIUS サーバの IP アドレスおよび共有秘密を入力する必要があります。暗号化タイプは動的 WEP で、認証タイプは EAP でのオープン認証、およびネットワーク EAP です。

注：

- LEAP セキュリティ タイプを選択する場合、無線クライアントは、LEAP 設定を使用する必要があります。
- Configuration Assistant では、EAP でのオープン認証とネットワーク EAP の両方の認証が有効になります。これにより、Cisco のクライアント デバイスも、Cisco 以外のクライアント デバイスも、同じ SSID で自律型アクセスポイントに関連付けられ、IEEE 802.1x 認証を実行できるようになります。

この種類のセキュリティを設定するには、次の手順に従います。

1. RADIUS サーバの IP アドレスを入力します。
2. 自律型アクセスポイントで RADIUS サーバとの通信に使用する共有秘密を入力します。

［WPA］

このセキュリティ設定では、EAP 設定よりも高いセキュリティを確保できます。この設定では、WPA 認証が有効になり、RADIUS サーバの IP アドレスと共有秘密を入力する必要があります。この SSID を使用して自律型アクセスポイントに関連付けられるクライアント デバイスは、WPA 対応である必要があります。暗号化タイプは TKIP で、認証タイプは EAP でのオープン認証、およびネットワーク EAP です。

注：Configuration Assistant では、EAP でのオープン認証とネットワーク EAP の両方の認証が有効になります。これにより、Cisco のクライアント デバイスも、Cisco 以外のクライアント デバイスも、同じ SSID で自律型アクセスポイントに関連付けられ、IEEE 802.1x 認証を実行できるようになります。

この種類のセキュリティを設定するには、次の手順に従います。

1. RADIUS サーバの IP アドレスを入力します。
2. 自律型アクセスポイントで RADIUS サーバとの通信に使用する共有秘密を入力します。

［WPA-PSK］

WPA 暗号化を使用する場合に RADIUS サーバにアクセスできないときは、このセキュリティ設定を選択します。この設定では、自律型アクセスポイントとクライアント デバイスで同一の WPA-PSK を共有する必要があります。キーは、8 から 63 文字の長さで指定できます。暗号化タイプは TKIP で、認証タイプは WPA-PSK です。

この種類のセキュリティを設定するには、［WPA 事前共有キー］フィールドにキーを入力します。

［WPA2］

このセキュリティ設定は、WPA 設定よりもセキュリティ レベルが高くなります。この設定では、WPA2 認証が有効になり、RADIUS サーバの IP アドレスと共有秘密を入力する必要があります。この SSID を使用して自律型アクセスポイントに関連付けられるクライアント デバイスは、WPA2 対応である必要があります。暗号化タイプは AES CCMP で、認証タイプは EAP でのオープン認証、およびネットワーク EAP です。

注：Configuration Assistant では、EAP でのオープン認証とネットワーク EAP の両方の認証が有効になります。これにより、Cisco のクライアント デバイスも、Cisco 以外のクライアント デバイスも、同じ SSID で自律型アクセスポイントに関連付けられ、IEEE 802.1x 認証を実行できるようになります。

この種類のセキュリティを設定するには、次の手順に従います。

1. RADIUS サーバの IP アドレスを入力します。
2. 自律型アクセスポイントで RADIUS サーバとの通信に使用する共有秘密を入力します。

［WPA2-PSK］

WPA2 暗号化を使用する場合に RADIUS サーバにアクセスできないときは、このセキュリティ設定を選択します。この設定では、自律型アクセスポイントとクライアント デバイスで同一の WPA2-PSK を共有する必要があります。キーは、8 から 63 文字の長さで指定できます。暗号化タイプは AES CCMP で、認証タイプは WPA-PSK です。

この種類のセキュリティを設定するには、[WPA2事前共有キー]フィールドにキーを入力します。

［MAC］

MAC ベースの認証を使用してクライアント デバイスを認証する場合にこのセキュリティ設定を選択します。

暗号化はなく、認証タイプはオープン認証です。

この種類のセキュリティを設定するには、次の手順に従います。

1. RADIUS サーバの IP アドレスを入力します。
2. 自律型アクセスポイントで RADIUS サーバとの通信に使用する共有秘密を入力します。

［MAC & EAP］

MAC ベースの認証と EAP 認証を組み合わせて使用してクライアント デバイスを認証する場合にこのセキュリティ設定を選択します。IEEE 802.11 オープン認証を使用してアクセスポイントに関連付けられるクライアント デバイスは、まず MAC 認証を試みます。MAC 認証に成功すると、このクライアント デバイスはネットワークに接続されます。クライアントで EAP 認証も使用されている場合は、EAP を使用して認証が行われます。MAC 認証に失敗すると、アクセスポイントは、クライアント デバイスによる EAP 認証を待機します。

暗号化タイプは動的 WEP で、認証タイプは EAP でのオープン認証、およびネットワーク EAP です。

注 : Configuration Assistant では、EAP でのオープン認証とネットワーク EAP の両方の認証が有効になります。これにより、Cisco のクライアント デバイスも、Cisco 以外のクライアント デバイスも、同じ SSID で自律型アクセスポイントに関連付けられ、802.1x 認証を実行できるようになります。

この種類のセキュリティを設定するには、次の手順に従います。

1. RADIUS サーバの IP アドレスを入力します。
2. 自律型アクセスポイントで RADIUS サーバとの通信に使用する共有秘密を入力します。

WLC526 を管理する場合

[WLANの作成]ウィンドウ

このウィンドウは、[WLAN (SSID)]ウィンドウで[作成]をクリックした場合に表示されます。このウィンドウを使用すると、新しい SSID を作成したり、セキュリティ設定を指定したりできます。

次の手順に従います。

1. [WLANタイプ]領域で、データ、音声、ゲストのいずれかの WLAN タイプを選択します。

   注:音声またはゲストを選択すると、VLAN が自動的に選択されます。

   注:ゲストを選択すると、[Web認証]が自動的に有効になり、セキュリティが[セキュリティなし]に設定されます。

2. [SSID]フィールドで、会社名および選択した WLAN タイプに基づいたデフォルトの SSID をそのまま使用するか、別の SSID を入力します。SSID には、最大 32 文字の英数字を使用できます。
3. SSID を指定しないデバイスがアクセスポイントに関連付けられる(無線接続を確立できる)ように SSID をブロードキャストする場合は、[ビーコンのブロードキャスト]をオンにします。ビーコンには、1 つの SSID だけを含めることができます(guest SSID)。
4. [VLAN]リストで、SSID に関連付けるデータ VLAN ID を選択します。

   注:[VLANの追加]をクリックして、VLAN をドロップダウン リストに追加します。

5. ゲストまたは従業員のユーザ リストを作成した場合は、[セキュリティ設定]領域で[Web認証]を有効にします。このオプションは、ゲスト WLAN ではデフォルトで有効になっています。
6. [セキュリティ]リストから、セキュリティ設定を選択します。リストでの選択についての説明や、それにより有効になる暗号化オプションおよび認証オプションについては、「セキュリティ設定」を参照してください。
7. (音声 WLAN のみ)[音声CACタイプ]領域で、クライアント デバイスで WMM の使用が必要となる[無線マルチメディアポリシー]を選択するか、ネットワーク上の Cisco 7920 IP Phone をサポートする[7920 CAC]を選択します。デフォルトの設定は[無線マルチメディアポリシー]です。

   注:ネットワーク上で Cisco 7920 IP Phone を使用する場合は、[無線マルチメディアポリシー]を選択しないでください。

8. このウィンドウに必要な情報を入力したら、[OK]をクリックして、変更を保存し、ウィンドウを閉じます。

セキュリティ設定

注:[Web認証]が有効になっている場合は、セキュリティ設定は[セキュリティなし]、[WEP]、[WPA-PSK]、または[WPA2-PSK]に制限されます。

次のセキュリティ設定から選択します。

[セキュリティなし]

これは最もセキュリティ レベルの低いオプションです。このオプションは、公共の場で使用されている SSID（guest SSID）に対してのみ選択し、各自のネットワークへのアクセスを制限する VLAN に関連付けます。暗号化は行われず、認証タイプはオープン認証です。

［WEP］

このセキュリティ設定では、アクセスポイントとクライアント デバイス（ラップトップや PC など、無線デバイスに接続されているデバイス）で、同一の WEP キーを共有して通信をプライベートに維持することが必要です。暗号化タイプは WEP です。

この種類のセキュリティを設定するには、次の手順に従います。

1. ［認証］リストから認証タイプを選択します。［オープン］または［共有鍵］を選択できます。
2. ［鍵形式］リストから鍵形式を選択します。［16進］または［ASCII］を選択できます。
3. ［鍵形式］リストで［16進］を選択した場合は、次の手順を実行します。
    a. リストからビット暗号化（40 ビットまたは 104 ビット）を選択します。
    b. ［パスフレーズ］フィールドにパスフレーズを入力します。
    c. ［生成］をクリックします。［キー］リストの横にある［キー］フィールドに自動的に値が入力されます。
4. ［鍵形式］リストで［ASCII］を選択した場合は、次の手順を実行します。
. リストからビット暗号化（40 ビットまたは 104 ビット）を選択します。
    a. 5 文字のキー(40 ビット）または 13 文字のキー（104 ビット）をキー フィールドに入力します。
5. ［キー］リストで 1、2、3、または 4 を選択することによって、キー番号を変更できます。デフォルトのキー番号は 1 です。

［EAP］

このセキュリティ設定では、IEEE 802.1X 認証が有効になり、RADIUS サーバの IP アドレスを選択する必要があります。暗号化タイプは WEP で、認証タイプは IEEE 802.1x です。

［WPA］

このセキュリティ設定では、EAP 設定よりも高いセキュリティを確保できます。この設定では、WPA 認証が有効になり、RADIUS サーバの IP アドレスを選択する必要があります。この SSID を使用してアクセスポイントに関連付けられるクライアント デバイスは、WPA 対応である必要があります。

この種類のセキュリティを設定するには、次の手順に従います。

1. ［暗号化］リストから暗号化タイプを選択します。［aes］または［tkip］を選択できます。

2. ［認証］リストから認証タイプを選択します。［802.1x］、［高速ローミング(CCKM)］、または［802.1x、高速ローミング(CCKM)］を選択できます。高速ローミングにより、クライアントがアクセスポイント間でローミングできるようになります。

［WPA-PSK］

WPA 暗号化を使用する場合に RADIUS サーバにアクセスできないときは、このセキュリティ設定を選択します。この設定では、アクセスポイントとクライアント デバイスで同一の WPA-PSK を共有する必要があります。キーは、8 から 63 文字の長さで指定できます。認証タイプは WPA-PSK です。

この種類のセキュリティを設定するには、次の手順に従います。

1. ［暗号化］リストから暗号化タイプを選択します。［aes］または［tkip］を選択できます。
2. ［WPA事前共有キー］ フィールドにキーを入力します。

［WPA2］

このセキュリティ設定は、WPA 設定よりもセキュリティ レベルが高くなります。この設定では、WPA2 認証が有効になり、RADIUS サーバの IP アドレスを選択する必要があります。この SSID を使用してアクセスポイントに関連付けられるクライアント デバイスは、WPA2 対応である必要があります。

この種類のセキュリティを設定するには、次の手順に従います。

1. ［暗号化］リストから暗号化タイプを選択します。［aes］または［tkip］を選択できます。
2. ［認証］リストから認証タイプを選択します。［802.1x］、［高速ローミング(CCKM)］、または［802.1x、高速ローミング(CCKM)］を選択できます。高速ローミングにより、クライアントがアクセスポイント間でローミングできるようになります。

［WPA2-PSK］

WPA2 暗号化を使用する場合に RADIUS サーバにアクセスできないときは、このセキュリティ設定を選択します。この設定では、アクセスポイントとクライアント デバイスで同一の WPA2-PSK を共有する必要があります。キーは、8 から 63 文字の長さで指定できます。認証タイプは WPA2-PSK です。

この種類のセキュリティを設定するには、次の手順に従います。

1. ［暗号化］リストから暗号化タイプを選択します。［aes］または［tkip］を選択できます。
2. ［WPA2事前共有キー］フィールドにキーを入力します。

［MAC］

MAC ベースの認証を使用してクライアント デバイスを認証する場合にこのセキュリティ設定を選択します。

暗号化はなく、認証タイプは IEEE 802.1x です。

この種類のセキュリティを設定するには、次の手順に従います。

1. RADIUS サーバの IP アドレスを入力します。
2. 自律型アクセスポイントで RADIUS サーバとの通信に使用する共有秘密を入力します。

[MAC & EAP]

MAC ベースの認証と EAP 認証を組み合わせて使用してクライアント デバイスを認証する場合にこのセキュリティ設定を選択します。IEEE 802.11 オープン認証を使用してアクセスポイントに関連付けられるクライアント デバイスは、まず MAC 認証を試みます。MAC 認証に成功すると、このクライアント デバイスはネットワークに接続されます。クライアントで EAP 認証も使用されている場合は、EAP を使用して認証が行われます。MAC 認証に失敗すると、アクセスポイントは、クライアント デバイスによる EAP 認証を待機します。

暗号化タイプは WEP で、認証タイプは IEEE 802.1x および Open MAC です。

この種類のセキュリティを設定するには、[暗号化]リストから暗号化タイプを選択します。[aes]または[tkip]を選択できます。

WLC526 を管理する場合

[WLANの作成]ウィンドウ

このウィンドウは、[WLAN (SSID)]ウィンドウで[作成]をクリックした場合に表示されます。このウィンドウを使用すると、新しい SSID を作成したり、セキュリティ設定を指定したりできます。

次の手順に従います。

1. [SSID]フィールドに SSID を入力します。SSID には、最大 32 文字の英数字を使用できます。
2. SSID を指定しないデバイスがアクセスポイントに関連付けられる(無線接続を確立できる)ように SSID をブロードキャストする場合は、[ビーコンのブロードキャスト]をオンにします。ビーコンには、1 つの SSID だけを含めることができます(guest SSID)。
3. [VLAN]リストで、SSID に関連付ける VLAN ID を選択します。
4. 次の中から QoS のレベルを選択します。
   - [音声]:この設定によって、無線接続上の音声トラフィックに対して高度な QoS が確保されます。
   - [データ]:この設定では、クライアントに対して通常の帯域幅がサポートされます。

5. ［セキュリティ設定］領域で、［セキュリティ］リストからセキュリティ設定を選択します。リストでの選択についての説明や、それにより有効になる暗号化オプションおよび認証オプションについては、「セキュリティ設定」を参照してください。
6. このウィンドウに必要な情報を入力したら、［OK］をクリックして、変更を保存し、ウィンドウを閉じます。

［セキュリティ設定］

次のセキュリティ設定から選択します。

［セキュリティなし］

これは最もセキュリティ レベルの低いオプションです。このオプションは、公共の場で使用されている SSID（guest SSID）に対してのみ選択し、各自のネットワークへのアクセスを制限する VLAN に関連付けます。暗号化は行われず、認証タイプはオープン認証です。

［WEP］

このセキュリティ設定では、アクセスポイントとクライアント デバイス（ラップトップや PC など、無線デバイスに接続されているデバイス）で、同一の WEP キーを共有して通信をプライベートに維持することが必要です。暗号化タイプは WEP です。

この種類のセキュリティを設定するには、次の手順に従います。

1. ［認証］リストから認証タイプを選択します。［オープン］または［共有鍵］を選択できます。
2. ［鍵形式］リストから鍵形式を選択します。［16進］または［ASCII］を選択できます。
3. ［鍵形式］リストで［16進］を選択した場合は、次の手順を実行します。
    a. リストからビット暗号化（40 ビットまたは 104 ビット）を選択します。
    b. ［パスフレーズ］フィールドにパスフレーズを入力します。
    c. ［生成］をクリックします。［キー］リストの横にある［キー］フィールドに自動的に値が入力されます。
4. ［鍵形式］リストで［ASCII］を選択した場合は、次の手順を実行します。
    . リストからビット暗号化（40 ビットまたは 104 ビット）を選択します。
        a. 5 文字のキー(40 ビット）または 13 文字のキー（104 ビット）をキー フィールドに入力します。
5. ［キー］リストで 1、2、3、または 4 を選択することによって、キー番号を変更できます。デフォルトのキー番号は 1 です。

［EAP］

このセキュリティ設定では、IEEE 802.1X 認証が有効になり、RADIUS サーバの IP アドレスを選択する必要があります。暗号化タイプは WEP で、認証タイプは IEEE 802.1x です。

［WPA］

このセキュリティ設定では、EAP 設定よりも高いセキュリティを確保できます。この設定では、WPA 認証が有効になり、RADIUS サーバの IP アドレスを選択する必要があります。この SSID を使用してアクセスポイントに関連付けられるクライアント デバイスは、WPA 対応である必要があります。認証タイプは IEEE 802.1x です。

この種類のセキュリティを設定するには、[暗号化]フィールドから暗号化タイプを選択します。[aes]または[tkip]を選択できます。

[WPA-PSK]

WPA 暗号化を使用する場合に RADIUS サーバにアクセスできないときは、このセキュリティ設定を選択します。この設定では、アクセスポイントとクライアント デバイスで同一の WPA-PSK を共有する必要があります。キーは、8 から 63 文字の長さで指定できます。認証タイプは WPA-PSK です。

この種類のセキュリティを設定するには、次の手順に従います。

1. [暗号化]フィールドから暗号化タイプを選択します。[aes]または[tkip]を選択できます。
2. [WPA事前共有キー] フィールドにキーを入力します。

[WPA2]

このセキュリティ設定は、WPA 設定よりもセキュリティ レベルが高くなります。この設定では、WPA2 認証が有効になり、RADIUS サーバの IP アドレスを選択する必要があります。この SSID を使用してアクセスポイントに関連付けられるクライアント デバイスは、WPA2 対応である必要があります。認証タイプは IEEE 802.1x です。

この種類のセキュリティを設定するには、[暗号化]フィールドから暗号化タイプを選択します。[aes]または[tkip]を選択できます。

[WPA2-PSK]

WPA2 暗号化を使用する場合に RADIUS サーバにアクセスできないときは、このセキュリティ設定を選択します。この設定では、アクセスポイントとクライアント デバイスで同一の WPA2-PSK を共有する必要があります。キーは、8 から 63 文字の長さで指定できます。認証タイプは WPA2-PSK です。

この種類のセキュリティを設定するには、次の手順に従います。

1. [暗号化]フィールドから暗号化タイプを選択します。[aes]または[tkip]を選択できます。
2. [WPA2事前共有キー]フィールドにキーを入力します。

[MAC]

MAC ベースの認証を使用してクライアント デバイスを認証する場合にこのセキュリティ設定を選択します。

暗号化はなく、認証タイプは IEEE 802.1x です。

この種類のセキュリティを設定するには、次の手順に従います。

1. RADIUS サーバの IP アドレスを入力します。
2. 自律型アクセスポイントで RADIUS サーバとの通信に使用する共有秘密を入力します。

[MAC & EAP]

MAC ベースの認証と EAP 認証を組み合わせて使用してクライアント デバイスを認証する場合にこのセキュリティ設定を選択します。IEEE 802.11 オープン認証を使用してアクセスポイントに関連付けられるクライアント デバイスは、まず MAC 認証を試みます。MAC 認証に成功すると、このクライアント デバイスはネットワークに接続されます。クライアントで EAP 認証も使用されている場合は、EAP を使用して認証が行われます。MAC 認証に失敗すると、アクセスポイントは、クライアント デバイスによる EAP 認証を待機します。

暗号化タイプは WEP で、認証タイプは IEEE 802.1x および Open MAC です。

この種類のセキュリティを設定するには、[暗号化]フィールドから暗号化タイプを選択します。[aes]または[tkip]を選択できます。

UC500、Cisco 800シリーズルータを管理する場合

[WLANの作成]ウィンドウ

このウィンドウは、[WLAN (SSID)]ウィンドウで[作成]をクリックした場合に表示されます。このウィンドウを使用すると、新しい SSID を作成したり、セキュリティ設定を指定したりできます。

次の手順に従います。

1. [SSID]フィールドに SSID を入力します。SSID には、最大 32 文字の英数字を使用できます。
2. SSID を指定しないデバイスが HWIC アクセスポイントに関連付けられる(無線接続を確立できる)ように SSID をブロードキャストする場合は、[ビーコンのブロードキャスト]をオンにします。ビーコンには、1 つの SSID だけを含めることができます(guest SSID)。
3. [VLAN]フィールドで、SSID に関連付ける VLAN ID を入力するか、選択します。

   注:VLAN を SSID に割り当てる場合は、VLAN をすべての SSID に割り当てる必要があります。一部の SSID に VLAN を割り当て、それ以外の SSID には割り当てないようにすることはできません。

4. この VLAN をネイティブ VLAN にする場合は、[ネイティブVLAN]ボックスをオンにします。
5. [セキュリティ設定]領域で、[セキュリティ]リストからセキュリティ設定を選択します。このウィンドウの他のオプションは、選択内容によって異なります。[セキュリティなし]、[WEP]、[EAP]、[WPA]、[WPA-PSK]、[WPA2]、[WPA2-PSK]、または[MAC & EAP]を選択で

きます。選択したセキュリティ設定に応じて、Configuration Assistant によって暗号化および認証タイプが自動的に選択されます。

6. このウィンドウに必要な情報を入力したら、[OK]をクリックして、変更を保存し、ウィンドウを閉じます。

[セキュリティなし]

これは最もセキュリティ レベルの低いオプションです。このオプションは、公共の場で使用されている SSID(guest SSID)に対してのみ選択し、各自のネットワークへのアクセスを制限する VLAN に関連付けます。暗号化は行われず、認証タイプはオープン認証です。

[WEP]

このセキュリティ設定では、HWIC アクセスポイントとクライアント デバイス(ラップトップや PC など、無線デバイスに接続されているデバイス)で、同一の WEP キーを共有してプライベートな通信を維持することが必要です。暗号化タイプは WEP で、認証タイプはオープン認証です。

この種類のセキュリティを設定するには、次の手順に従います。

1. [パスフレーズ]フィールドにパスフレーズを入力し、リストからビット暗号化を選択します。
2. [生成]をクリックします。[キー]リストの横にある[キー]フィールドに自動的に値が入力されます。[キー]リストで 1、2、3、または 4 を選択することによって、キー番号を変更できます。デフォルトのキー番号は 1 です。

[EAP]

このセキュリティ設定では、IEEE 802.1X 認証が有効になり、RADIUS サーバの IP アドレスおよび共有秘密を入力する必要があります。暗号化タイプは動的 WEP で、認証タイプは EAPでのオープン認証、およびネットワーク EAP です。

注:Configuration Assistant では、EAPでのオープン認証とネットワーク EAP の両方の認証が有効になります。これにより、Cisco のクライアント デバイスも、Cisco 以外のクライアント デバイスも、同じ SSID で HWIC アクセスポイントに関連付けられ、IEEE 802.1x 認証を実行できるようになります。

この種類のセキュリティを設定するには、次の手順に従います。

1. 外部 RADIUS サーバを使用するには、[外部RADIUSサーバを使用する]をオンにします。
2. ローカル RADIUS サーバを使用するには、[ローカルRADIUSサーバを使用する]をオンにします。

   注:外部とローカルの両方の RADIUS 認証をオンにした場合、HWIC アクセスポイントは、最初に外部 RADIUS サーバへの認証を試みます。この認証に失敗した場合、HWIC アクセスポイントはローカル RADIUS サーバを使用します。

[WPA]

このセキュリティ設定では、EAP よりも高いセキュリティを確保できます。この設定では、WPA 認証が有効になり、外部 RADIUS サーバ、ローカル RADIUS サーバ、またはその両方を使用することができます。この SSID を使用して HWIC アクセスポイントに関連付けられるクライアント デバイスは、WPA 対応である必要があります。暗号化タイプは TKIP で、認証タイプは EAPでのオープン認証、およびネットワーク EAP です。

注：Configuration Assistant では、EAPでのオープン認証とネットワーク EAP の両方の認証が有効になります。これにより、Cisco のクライアント デバイスも、Cisco 以外のクライアント デバイスも、同じ SSID で HWIC アクセスポイントに関連付けられ、IEEE 802.1x 認証を実行できるようになります。

この種類のセキュリティを設定するには、次の手順に従います。

1. 外部 RADIUS サーバを使用するには、[外部RADIUSサーバを使用する]をオンにします。
2. ローカル RADIUS サーバを使用するには、[ローカルRADIUSサーバを使用する]をオンにします。

   注：外部とローカルの両方の RADIUS 認証をオンにした場合、HWIC アクセスポイントは、最初に外部 RADIUS サーバへの認証を試みます。この認証に失敗した場合、HWIC アクセスポイントはローカル RADIUS サーバを使用します。

[WPA-PSK]

WPA 暗号化を使用する場合に RADIUS サーバにアクセスできないときは、このセキュリティ設定を選択します。この設定では、HWIC アクセスポイントとクライアント デバイスで同一の WPA-PSK を共有する必要があります。キーは、8 から 63 文字の長さで指定できます。暗号化タイプは TKIP で、認証タイプは WPA-PSK です。

この種類のセキュリティを設定するには、[WPA事前共有キー]フィールドにキーを入力します。

[WPA2]

このセキュリティ設定は、WPA 設定よりもセキュリティ レベルが高くなります。この設定では WPA2 認証が有効になり、外部 RADIUS サーバ、ローカル RADIUS サーバ、またはその両方を使用することができます。この SSID を使用して HWIC アクセスポイントに関連付けられるクライアント デバイスは、WPA2 対応である必要があります。暗号化タイプは AES CCMP で、認証タイプは EAP でのオープン認証、およびネットワーク EAP です。

注：Configuration Assistant では、EAPでのオープン認証とネットワーク EAP の両方の認証が有効になります。これにより、Cisco のクライアント デバイスも、Cisco 以外のクライアント デバイスも、同じ SSID で HWIC アクセスポイントに関連付けられ、IEEE 802.1x 認証を実行できるようになります。

この種類のセキュリティを設定するには、次の手順に従います。

1. 外部 RADIUS サーバを使用するには、[外部RADIUSサーバを使用する]をオンにします。
2. ローカル RADIUS サーバを使用するには、[ローカルRADIUSサーバを使用する]をオンにします。

   注：外部とローカルの両方の RADIUS 認証をオンにした場合、HWIC アクセスポイントは、最初に外部 RADIUS サーバへの認証を試みます。この認証に失敗した場合、HWIC アクセスポイントはローカル RADIUS サーバを使用します。

[WPA2-PSK]

WPA2 暗号化を使用する場合に RADIUS サーバにアクセスできないときは、このセキュリティ設定を選択します。この設定では、HWIC アクセスポイントとクライアント デバイスで同一の WPA2-PSK を共有する必要があります。キーは、8 から 63 文字の長さで指定できます。暗号化タイプは AES CCMP で、認証タイプは WPA-PSK です。

この種類のセキュリティを設定するには、[WPA2事前共有キー]フィールドにキーを入力します。

[MAC & EAP]

MAC ベースの認証と EAP 認証を組み合わせて使用してクライアント デバイスを認証する場合にこのセキュリティ設定を選択します。IEEE 802.11 オープン認証を使用してアクセスポイントに関連付けられるクライアント デバイスは、まず MAC 認証を試みます。MAC 認証に成功すると、このクライアント デバイスはネットワークに接続されます。クライアントで EAP 認証も使用されている場合は、EAP を使用して認証が行われます。MAC 認証に失敗すると、アクセスポイントは、クライアント デバイスによる EAP 認証を待機します。

この設定では、外部 RADIUS サーバ、ローカル RADIUS サーバ、またはその両方を使用することができます。暗号化タイプは動的 WEP で、認証タイプは EAPでのオープン認証、およびネットワーク EAP です。

注: Configuration Assistant では、EAPでのオープン認証とネットワーク EAP の両方の認証が有効になります。これにより、Cisco のクライアント デバイスも、Cisco 以外のクライアント デバイスも、同じ SSID で HWIC アクセスポイントに関連付けられ、IEEE 802.1x 認証を実行できるようになります。

この種類のセキュリティを設定するには、次の手順に従います。

1. 外部 RADIUS サーバを使用するには、[外部RADIUSサーバを使用する]をオンにします。
2. ローカル RADIUS サーバを使用するには、[ローカルRADIUSサーバを使用する]をオンにします。

   注: 外部とローカルの両方の RADIUS 認証をオンにした場合、HWIC アクセスポイントは、最初に外部 RADIUS サーバへの認証を試みます。この認証に失敗した場合、HWIC アクセスポイントはローカル RADIUS サーバを使用します。

AP521 を管理する場合

[WLANの修正]ウィンドウ

このウィンドウは、[WLAN (SSID)]ウィンドウで[修正]をクリックした場合に表示されます。このウィンドウを使用すると、SSID のセキュリティ設定を変更できます。

次の手順に従います。

1. SSID を指定しないデバイスが自律型アクセスポイントに関連付けられる(無線接続を確立できる)ように SSID をブロードキャストする場合は、[ビーコンのブロードキャスト]をオンにします。ビーコンには、1 つの SSID だけを含めることができます(guest SSID)。

   注:SSID を変更することはできません。

2. [VLAN]フィールドで、SSID に関連付ける VLAN ID を入力するか、選択します。

   注: VLAN を SSID に割り当てる場合は、VLAN をすべての SSID に割り当てる必要があります。一部の SSID に VLAN を割り当て、それ以外の SSID には割り当てないようにすることはできません。

3. この VLAN をネイティブ VLAN にする場合は、[ネイティブ VLAN]ボックスをオンにします。
4. [セキュリティ設定]領域で、[セキュリティ]リストからセキュリティ設定を選択します。このウィンドウの他のオプションは、選択内容によって異なります。[セキュリティなし]、[WEP]、[EAP]、[LEAP]、[WPA]、[WPA-PSK]、[WPA2]、[WPA2-PSK]、[MAC]または[MAC & EAP]を選択できます。選択したセキュリティ設定に応じて、Configuration Assistant によって暗号化および認証タイプが自動的に選択されます。
5. このウィンドウに必要な情報を入力したら、[OK] をクリックして、変更を保存し、ウィンドウを閉じます。

[セキュリティなし]

これは最もセキュリティ レベルの低いオプションです。このオプションは、公共の場で使用されている SSID（guest SSID）に対してだけ選択し、ネットワークへのアクセスを制限する VLAN に関連付けます。暗号化は行われず、認証タイプはオープン認証です。

[WEP]

このセキュリティ設定では、自律型アクセスポイントとクライアント デバイス（ラップトップや PC など、無線デバイスに接続されているデバイス）で、同一の WEP キーを共有してプライベートな通信を維持することが必要です。暗号化タイプは WEP で、認証タイプはオープン認証です。

この種類のセキュリティを設定するには、次の手順に従います。

1. [パスフレーズ]フィールドにパスフレーズを入力し、リストからビット暗号化を選択します。
2. [生成]をクリックします。[キー]リストの横にある[キー]フィールドに自動的に値が入力されます。[キー]リストで 1、2、3、または 4 を選択することによって、キー番号を変更できます。デフォルトのキー番号は 1 です。

[EAP]

このセキュリティ設定では、IEEE 802.1X 認証が有効になり、RADIUS サーバの IP アドレスおよび共有秘密を入力する必要があります。暗号化タイプは WEP で、認証タイプは EAP でのオープン認証です。

注：EAP セキュリティ タイプを選択する場合、無線クライアントは、EAP 設定（EAP-TLS、EAP-FAST、PEAP など）を使用する必要があります。無線クライアントは、LEAP 設定を使用できません。

この種類のセキュリティを設定するには、次の手順に従います。

1. RADIUS サーバの IP アドレスを入力します。
2. 自律型アクセスポイントで RADIUS サーバとの通信に使用する共有秘密を入力します。

[LEAP]

このセキュリティ設定では、IEEE 802.1X 認証が有効になり、RADIUS サーバの IP アドレスおよび共有秘密を入力する必要があります。暗号化タイプは WEP で、認証タイプは EAP でのオープン認証、およびネットワーク EAP です。

注：LEAP セキュリティ タイプを選択する場合、無線クライアントは、LEAP 設定を使用する必要があります。

注：Configuration Assistant では、EAP でのオープン認証とネットワーク EAP の両方の認証が有効になります。これにより、Cisco のクライアント デバイスも、Cisco 以外のクライアント デバイスも、同じ SSID で自律型アクセスポイントに関連付けられ、IEEE 802.1x 認証を実行できるようになります。

この種類のセキュリティを設定するには、次の手順に従います。

1. RADIUS サーバの IP アドレスを入力します。
2. 自律型アクセスポイントで RADIUS サーバとの通信に使用する共有秘密を入力します。

［WPA］

このセキュリティ設定では、EAP 設定よりも高いセキュリティを確保できます。この設定では、WPA 認証が有効になり、RADIUS サーバの IP アドレスと共有秘密を入力する必要があります。この SSID を使用して自律型アクセスポイントに関連付けられるクライアント デバイスは、WPA 対応である必要があります。暗号化タイプは TKIP で、認証タイプは EAP でのオープン認証、およびネットワーク EAP です。

注：Configuration Assistant では、EAP でのオープン認証とネットワーク EAP の両方の認証が有効になります。これにより、Cisco のクライアント デバイスも、Cisco 以外のクライアント デバイスも、同じ SSID で自律型アクセスポイントに関連付けられ、IEEE 802.1x 認証を実行できるようになります。

この種類のセキュリティを設定するには、次の手順に従います。

1. RADIUS サーバの IP アドレスを入力します。
2. 自律型アクセスポイントで RADIUS サーバとの通信に使用する共有秘密を入力します。

［WPA-PSK］

WPA 暗号化を使用する場合に RADIUS サーバにアクセスできないときは、このセキュリティ設定を選択します。この設定では、自律型アクセスポイントとクライアント デバイスで同一の WPA-PSK を共有する必要があります。キーは、8 から 63 文字の長さで指定できます。暗号化タイプは TKIP で、認証タイプは WPA-PSK です。

この種類のセキュリティを設定するには、[WPA事前共有キー]フィールドにキーを入力します。

［WPA2］

このセキュリティ設定は、WPA 設定よりもセキュリティ レベルが高くなります。この設定では、WPA2 認証が有効になり、RADIUS サーバの IP アドレスと共有秘密を入力する必要があります。この SSID を使用して自律型アクセスポイントに関連付けられるクライアント デバイスは、WPA2 対応である必要があります。暗号化タイプは AES CCMP で、認証タイプは EAP でのオープン認証、およびネットワーク EAP です。

注：Configuration Assistant では、EAP でのオープン認証とネットワーク EAP の両方の認証が有効になります。これにより、Cisco のクライアント デバイスも、Cisco 以外のクライアント デバイスも、同じ SSID で自律型アクセスポイントに関連付けられ、802.1x 認証を実行できるようになります。

この種類のセキュリティを設定するには、次の手順に従います。

1. RADIUS サーバの IP アドレスを入力します。

2. 自律型アクセスポイントで RADIUS サーバとの通信に使用する共有秘密を入力します。

［WPA2-PSK］

WPA2 暗号化を使用する場合に RADIUS サーバにアクセスできないときは、このセキュリティ設定を選択します。この設定では、自律型アクセスポイントとクライアント デバイスで同一の WPA2-PSK を共有する必要があります。キーは、8 から 63 文字の長さで指定できます。暗号化タイプは AES CCMP で、認証タイプは WPA-PSK です。

この種類のセキュリティを設定するには、［WPA2 事前共有キー］フィールドにキーを入力します。

［MAC］

MAC ベースの認証を使用してクライアント デバイスを認証する場合にこのセキュリティ設定を選択します。

暗号化はなく、認証タイプはオープン認証です。

この種類のセキュリティを設定するには、次の手順に従います。

1. RADIUS サーバの IP アドレスを入力します。
2. 自律型アクセスポイントで RADIUS サーバとの通信に使用する共有秘密を入力します。

［MAC & EAP］

MAC ベースの認証と EAP 認証を組み合わせて使用してクライアント デバイスを認証する場合にこのセキュリティ設定を選択します。IEEE 802.11 オープン認証を使用してアクセスポイントに関連付けられるクライアント デバイスは、まず MAC 認証を試みます。MAC 認証に成功すると、このクライアント デバイスはネットワークに接続されます。クライアントで EAP 認証も使用されている場合は、EAP を使用して認証が行われます。MAC 認証に失敗すると、アクセスポイントは、クライアント デバイスによる EAP 認証を待機します。

暗号化タイプは動的 WEP で、認証タイプは EAP でのオープン認証、およびネットワーク EAP です。

注 : Configuration Assistant では、EAP でのオープン認証とネットワーク EAP の両方の認証が有効になります。これにより、Cisco のクライアント デバイスも、Cisco 以外のクライアント デバイスも、同じ SSID で自律型アクセスポイントに関連付けられ、802.1x 認証を実行できるようになります。

この種類のセキュリティを設定するには、次の手順に従います。

1. RADIUS サーバの IP アドレスを入力します。
2. 自律型アクセスポイントで RADIUS サーバとの通信に使用する共有秘密を入力します。

UC500、Cisco 800シリーズルータを管理する場合

［WLANの修正］ウィンドウ

このウィンドウは、［WLAN (SSID)］ウィンドウで［修正］をクリックした場合に表示されます。このウィンドウを使用すると、SSID のセキュリティ設定を変更できます。

次の手順に従います。

1. SSID を指定しないデバイスが HWIC アクセスポイントに関連付けられる（無線接続を確立できる）ように SSID をブロードキャストする場合は、[ビーコンのブロードキャスト]をオンにします。ビーコンには、1 つの SSID だけを含めることができます（guest SSID）。

   注：SSID を変更することはできません。

2. [VLAN]フィールドで、SSID に関連付ける VLAN ID を入力するか、選択します。

   注：VLAN を SSID に割り当てる場合は、VLAN をすべての SSID に割り当てる必要があります。一部の SSID に VLAN を割り当て、それ以外の SSID には割り当てないようにすることはできません。

3. この VLAN をネイティブ VLAN にする場合は、[ネイティブVLAN]ボックスをオンにします。
4. [セキュリティ設定]領域で、[セキュリティ]リストからセキュリティ設定を選択します。このウィンドウの他のオプションは、選択内容によって異なります。[セキュリティなし]、[WEP]、[EAP]、[WPA]、[WPA-PSK]、[WPA2]、[WPA2-PSK]、または[MAC & EAP]を選択できます。選択したセキュリティ設定に応じて、Configuration Assistant によって暗号化および認証タイプが自動的に選択されます。
5. このウィンドウに必要な情報を入力したら、[OK]をクリックして、変更を保存し、ウィンドウを閉じます。

［セキュリティなし］

これは最もセキュリティ レベルの低いオプションです。このオプションは、公共の場で使用されている SSID（guest SSID）に対してのみ選択し、各自のネットワークへのアクセスを制限する VLAN に関連付けます。暗号化は行われず、認証タイプはオープン認証です。

［WEP］

このセキュリティ設定では、HWIC アクセスポイントとクライアント デバイス（ラップトップや PC など、無線デバイスに接続されているデバイス）で、同一の WEP キーを共有してプライベートな通信を維持することが必要です。暗号化タイプは WEP で、認証タイプはオープン認証です。

この種類のセキュリティを設定するには、次の手順に従います。

1. [パスフレーズ]フィールドにパスフレーズを入力し、リストからビット暗号化を選択します。
2. [生成]をクリックします。[キー]リストの横にある[キー]フィールドに自動的に値が入力されます。[キー]リストで 1、2、3、または 4 を選択することによって、キー番号を変更できます。デフォルトのキー番号は 1 です。

［EAP］

このセキュリティ設定では、IEEE 802.1X 認証が有効になり、外部 RADIUS サーバ、ローカル RADIUS サーバ、またはその両方を使用することができます。暗号化タイプは動的 WEP で、認証タイプは EAPでのオープン認証、およびネットワーク EAP です。

注：Configuration Assistant では、EAPでのオープン認証とネットワーク EAP の両方の認証が有効になります。これにより、Cisco のクライアント デバイスも、Cisco 以外のクライアント デバイスも、同じ SSID で HWIC アクセスポイントに関連付けられ、IEEE 802.1x 認証を実行できるようになります。

この種類のセキュリティを設定するには、次の手順に従います。

1. 外部 RADIUS サーバを使用するには、[外部RADIUSサーバを使用する]をオンにします。
2. ローカル RADIUS サーバを使用するには、[ローカルRADIUSサーバを使用する]をオンにします。

   注：外部とローカルの両方の RADIUS 認証をオンにした場合、HWIC アクセスポイントは、最初に外部 RADIUS サーバへの認証を試みます。この認証に失敗した場合、HWIC アクセスポイントはローカル RADIUS サーバを使用します。

［WPA］

このセキュリティ設定では、EAP よりも高いセキュリティを確保できます。この設定では、WPA 認証が有効になり、外部 RADIUS サーバ、ローカル RADIUS サーバ、またはその両方を使用することができます。この SSID を使用して HWIC アクセスポイントに関連付けられるクライアント デバイスは、WPA 対応である必要があります。暗号化タイプは TKIP で、認証タイプは EAPでのオープン認証、およびネットワーク EAP です。

注：Configuration Assistant では、EAPでのオープン認証とネットワーク EAP の両方の認証が有効になります。これにより、Cisco のクライアント デバイスも、Cisco 以外のクライアント デバイスも、同じ SSID で HWIC アクセスポイントに関連付けられ、IEEE 802.1x 認証を実行できるようになります。

この種類のセキュリティを設定するには、次の手順に従います。

1. 外部 RADIUS サーバを使用するには、[外部RADIUSサーバを使用する]をオンにします。
2. ローカル RADIUS サーバを使用するには、[ローカルRADIUSサーバを使用する]をオンにします。

   注：外部とローカルの両方の RADIUS 認証をオンにした場合、HWIC アクセスポイントは、最初に外部 RADIUS サーバへの認証を試みます。この認証に失敗した場合、HWIC アクセスポイントはローカル RADIUS サーバを使用します。

［WPA-PSK］

WPA 暗号化を使用する場合に RADIUS サーバにアクセスできないときは、このセキュリティ設定を選択します。この設定では、HWIC アクセスポイントとクライアント デバイスで同一の WPA-PSK（WPA-Pre-shared key）を共有する必要があります。キーは、8 から 63 文字の長さで指定できます。暗号化タイプは TKIP で、認証タイプは WPA-PSK です。

この種類のセキュリティを設定するには、[WPA事前共有キー]フィールドにキーを入力します。

［WPA2］

このセキュリティ設定は、WPA 設定よりもセキュリティ レベルが高くなります。この設定では、WPA2 認証が有効になり、外部 RADIUS サーバ、ローカル RADIUS サーバ、またはその両方を使用することができます。この SSID を使用して HWIC アクセスポイントに関連付けられるクライアント デバイスは、WPA2 対応である必要があります。暗号化タイプは AES CCMP で、認証タイプは EAPでのオープン認証、およびネットワーク EAP です。

注 : Configuration Assistant では、EAPでのオープン認証とネットワーク EAP の両方の認証が有効になります。これにより、Cisco のクライアント デバイスも、Cisco 以外のクライアント デバイスも、同じ SSID で HWIC アクセスポイントに関連付けられ、IEEE 802.1x 認証を実行できるようになります。

この種類のセキュリティを設定するには、次の手順に従います。

1. 外部 RADIUS サーバを使用するには、[外部RADIUSサーバを使用する]をオンにします。
2. ローカル RADIUS サーバを使用するには、[ローカルRADIUSサーバを使用する]をオンにします。

   注 : 外部とローカルの両方の RADIUS 認証をオンにした場合、HWIC アクセスポイントは、最初に外部 RADIUS サーバへの認証を試みます。この認証に失敗した場合、HWIC アクセスポイントはローカル RADIUS サーバを使用します。

[WPA2-PSK]

WPA2 暗号化を使用する場合に RADIUS サーバにアクセスできないときは、このセキュリティ設定を選択します。この設定では、HWIC アクセスポイントとクライアント デバイスで同一の WPA2-PSK を共有する必要があります。キーは、8 から 63 文字の長さで指定できます。暗号化タイプは AES CCMP で、認証タイプは WPA-PSK です。

この種類のセキュリティを設定するには、[WPA2事前共有キー]フィールドにキーを入力します。

[MAC & EAP]

MAC ベースの認証と EAP 認証を組み合わせて使用してクライアント デバイスを認証する場合にこのセキュリティ設定を選択します。IEEE 802.11 オープン認証を使用してアクセスポイントに関連付けられるクライアント デバイスは、まず MAC 認証を試みます。MAC 認証に成功すると、このクライアント デバイスはネットワークに接続されます。クライアントで EAP 認証も使用されている場合は、EAP を使用して認証が行われます。MAC 認証に失敗すると、アクセスポイントは、クライアント デバイスによる EAP 認証を待機します。

この設定では、外部 RADIUS サーバ、ローカル RADIUS サーバ、またはその両方を使用することができます。暗号化タイプは動的 WEP で、認証タイプは EAPでのオープン認証、およびネットワーク EAP です。

注 : Configuration Assistant では、EAPでのオープン認証とネットワーク EAP の両方の認証が有効になります。これにより、Cisco のクライアント デバイスも、Cisco 以外のクライアント デバイスも、同じ SSID で HWIC アクセスポイントに関連付けられ、IEEE 802.1x 認証を実行できるようになります。

この種類のセキュリティを設定するには、次の手順に従います。

1. 外部 RADIUS サーバを使用するには、[外部RADIUSサーバを使用する]をオンにします。
2. ローカル RADIUS サーバを使用するには、[ローカルRADIUSサーバを使用する]をオンにします。

   注 : 外部とローカルの両方の RADIUS 認証をオンにした場合、HWIC アクセスポイントは、最初に外部 RADIUS サーバへの認証を試みます。この認証に失敗した場合、HWIC アクセスポイントはローカル RADIUS サーバを使用します。

WLC526 を管理する場合

[WLANの修正]ウィンドウ

このウィンドウは、[WLAN (SSID)]ウィンドウで[修正]をクリックした場合に表示されます。このウィンドウを使用すると、SSID のセキュリティ設定を変更できます。

次の手順に従います。

1. SSID を指定しないデバイスがアクセスポイントに関連付けられる(無線接続を確立できる)ように SSID をブロードキャストする場合は、[ビーコンのブロードキャスト]をオンにします。ビーコンには、1 つの SSID だけを含めることができます(guest SSID)。

   注:SSID を変更することはできません。

2. [VLAN]リストで、SSID に関連付けるデータ VLAN ID を選択します。

   注:WLAN タイプが音声またはゲストの場合、VLAN が自動的に選択され、変更できません。

3. [セキュリティ]リストから、セキュリティ設定を選択します。リストでの選択についての説明や、それにより有効になる暗号化オプションおよび認証オプションについては、「セキュリティ設定」を参照してください。

   注:WLAN タイプがゲストの場合、[Web認証]が自動的に有効になり、セキュリティが[セキュリティなし]に設定されます。

4. (音声 WLAN のみ)[音声CACタイプ]領域で、クライアント デバイスで WMM の使用が必要となる[無線マルチメディアポリシー]を選択するか、ネットワーク上の Cisco 7920 IP Phone をサポートする[7920 CAC]を選択します。デフォルトの設定は[無線マルチメディアポリシー]です。

   注:ネットワーク上で Cisco 7920 IP Phone を使用する場合は、[無線マルチメディアポリシー]を選択しないでください。

5. このウィンドウに必要な情報を入力したら、[OK] をクリックして、変更を保存し、ウィンドウを閉じます。

セキュリティ設定

注:[Web認証]が有効になっている場合は、セキュリティ設定は[セキュリティなし]、[WEP]、[WPA-PSK]、または[WPA2-PSK]に制限されます。

次のセキュリティ設定から選択します。

[セキュリティなし]

これは最もセキュリティ レベルの低いオプションです。このオプションは、公共の場で使用されている SSID(guest SSID)に対してのみ選択し、各自のネットワークへのアクセスを制限する VLAN に関連付けます。暗号化は行われず、認証タイプはオープン認証です。

[WEP]

このセキュリティ設定では、アクセスポイントとクライアント デバイス（ラップトップや PC など、無線デバイスに接続されているデバイス）で、同一の WEP キーを共有して通信をプライベートに維持することが必要です。暗号化タイプは WEP です。

この種類のセキュリティを設定するには、次の手順に従います。

1. ［認証］リストから認証タイプを選択します。［オープン］または［共有鍵］を選択できます。
2. ［鍵形式］リストから鍵形式を選択します。［16進］または［ASCII］を選択できます。
3. ［鍵形式］リストで［16進］を選択した場合は、次の手順を実行します。

a. リストからビット暗号化（40 ビットまたは 104 ビット）を選択します。

b. ［パスフレーズ］フィールドにパスフレーズを入力します。

c. ［生成］をクリックします。［キー］リストの横にある［キー］フィールドに自動的に値が入力されます。

4. ［鍵形式］リストで［ASCII］を選択した場合は、次の手順を実行します。

. リストからビット暗号化（40 ビットまたは 104 ビット）を選択します。

a. 5 文字のキー(40 ビット）または 13 文字のキー（104 ビット）をキー フィールドに入力します。

5. ［キー］リストで 1、2、3、または 4 を選択することによって、キー番号を変更できます。デフォルトのキー番号は 1 です。

［EAP］

このセキュリティ設定では、IEEE 802.1X 認証が有効になり、RADIUS サーバの IP アドレスを選択する必要があります。暗号化タイプは WEP で、認証タイプは IEEE 802.1x です。

［WPA］

このセキュリティ設定では、EAP 設定よりも高いセキュリティを確保できます。この設定では、WPA 認証が有効になり、RADIUS サーバの IP アドレスを選択する必要があります。この SSID を使用してアクセスポイントに関連付けられるクライアント デバイスは、WPA 対応である必要があります。認証タイプは IEEE 802.1x です。

この種類のセキュリティを設定するには、次の手順に従います。

1. ［暗号化］リストから暗号化タイプを選択します。［aes］または［tkip］を選択できます。
2. ［認証］リストから認証タイプを選択します。［802.1x］、［高速ローミング(CCKM)］、または［802.1x、高速ローミング(CCKM)］を選択できます。高速ローミングにより、クライアントがアクセスポイント間でローミングできるようになります。

［WPA-PSK］

WPA 暗号化を使用する場合に RADIUS サーバにアクセスできないときは、このセキュリティ設定を選択します。この設定では、アクセスポイントとクライアント デバイスで同一の

WPA-PSK を共有する必要があります。キーは、8 から 63 文字の長さで指定できます。認証タイプは WPA-PSK です。

この種類のセキュリティを設定するには、次の手順に従います。

1. ［暗号化］リストから暗号化タイプを選択します。［aes］または［tkip］を選択できます。
2. ［WPA事前共有キー］フィールドにキーを入力します。

［WPA2］

このセキュリティ設定は、WPA 設定よりもセキュリティ レベルが高くなります。この設定では、WPA2 認証が有効になり、RADIUS サーバの IP アドレスを選択する必要があります。この SSID を使用してアクセスポイントに関連付けられるクライアント デバイスは、WPA2 対応である必要があります。認証タイプは IEEE 802.1x です。

この種類のセキュリティを設定するには、次の手順に従います。

1. ［暗号化］リストから暗号化タイプを選択します。［aes］または［tkip］を選択できます。
2. ［認証］リストから認証タイプを選択します。［802.1x］、［高速ローミング(CCKM)］、または［802.1x、高速ローミング(CCKM)］を選択できます。高速ローミングにより、クライアントがアクセスポイント間でローミングできるようになります。

［WPA2-PSK］

WPA2 暗号化を使用する場合に RADIUS サーバにアクセスできないときは、このセキュリティ設定を選択します。この設定では、アクセスポイントとクライアント デバイスで同一の WPA2-PSK を共有する必要があります。キーは、8 から 63 文字の長さで指定できます。認証タイプは WPA2-PSK です。

この種類のセキュリティを設定するには、次の手順に従います。

1. ［暗号化］リストから暗号化タイプを選択します。［aes］または［tkip］を選択できます。
2. ［WPA2事前共有キー］フィールドにキーを入力します。

［MAC］

MAC ベースの認証を使用してクライアント デバイスを認証する場合にこのセキュリティ設定を選択します。

暗号化はなく、認証タイプは IEEE 802.1x です。

この種類のセキュリティを設定するには、次の手順に従います。

1. RADIUS サーバの IP アドレスを入力します。
2. 自律型アクセスポイントで RADIUS サーバとの通信に使用する共有秘密を入力します。

［MAC & EAP］

MAC ベースの認証と EAP 認証を組み合わせて使用してクライアント デバイスを認証する場合にこのセキュリティ設定を選択します。IEEE 802.11 オープン認証を使用してアクセスポイントに関連付けられるクライアント デバイスは、まず MAC 認証を試みます。MAC 認証に成功すると、このクライアント デバイスはネットワークに接続されます。クライアントで EAP 認証も使用されている場合は、EAP を使用して認証が行われます。MAC 認証に失敗すると、アクセスポイントは、クライアント デバイスによる EAP 認証を待機します。

暗号化タイプは WEP で、認証タイプは IEEE 802.1x および Open MAC です。

この種類のセキュリティを設定するには、［暗号化］リストから暗号化タイプを選択します。［aes］または［tkip］を選択できます。

WLC526 を管理する場合

［WLANの修正］ウィンドウ

このウィンドウは、［WLAN (SSID)］ウィンドウで［修正］をクリックした場合に表示されます。このウィンドウを使用すると、SSID のセキュリティ設定を変更できます。

次の手順に従います。

1. SSID を指定しないデバイスがアクセスポイントに関連付けられる（無線接続を確立できる）ように SSID をブロードキャストする場合は、［ビーコンのブロードキャスト］をオンにします。ビーコンには、1 つの SSID だけを含めることができます（guest SSID）。

   注：SSID を変更することはできません。

2. ［VLAN］リストで、SSID に関連付ける VLAN ID を選択します。
3. 次の中から QoS のレベルを選択します。
   - ［音声］：この設定によって、無線接続上の音声トラフィックに対して高度な QoS が確保されます。
   - ［データ］：この設定では、クライアントに対して通常の帯域幅がサポートされます。
4. ［セキュリティ設定］領域で、［セキュリティ］リストからセキュリティ設定を選択します。リストでの選択についての説明や、それにより有効になる暗号化オプションおよび認証オプションについては、「セキュリティ設定」を参照してください。
5. このウィンドウに必要な情報を入力したら、［OK］をクリックして、変更を保存し、ウィンドウを閉じます。

［セキュリティ設定］

次のセキュリティ設定から選択します。

［セキュリティなし］

これは最もセキュリティ レベルの低いオプションです。このオプションは、公共の場で使用されている SSID（guest SSID）に対してのみ選択し、各自のネットワークへのアクセスを制限する VLAN に関連付けます。暗号化は行われず、認証タイプはオープン認証です。

［WEP］

このセキュリティ設定では、アクセスポイントとクライアント デバイス（ラップトップや PC など、無線デバイスに接続されているデバイス）で、同一の WEP キーを共有して通信をプライベートに維持することが必要です。暗号化タイプは WEP です。

この種類のセキュリティを設定するには、次の手順に従います。

1. ［認証］リストから認証タイプを選択します。［オープン］または［共有鍵］を選択できます。
2. ［鍵形式］リストから鍵形式を選択します。［16進］または［ASCII］を選択できます。
3. ［鍵形式］リストで［16進］を選択した場合は、次の手順を実行します。
    a. リストからビット暗号化（40 ビットまたは 104 ビット）を選択します。
    b. ［パスフレーズ］フィールドにパスフレーズを入力します。
    c. ［生成］をクリックします。［キー］リストの横にある［キー］フィールドに自動的に値が入力されます。
4. ［鍵形式］リストで［ASCII］を選択した場合は、次の手順を実行します。
    . リストからビット暗号化（40 ビットまたは 104 ビット）を選択します。
    a. 5 文字のキー(40 ビット）または 13 文字のキー（104 ビット）をキー フィールドに入力します。
5. ［キー］リストで 1、2、3、または 4 を選択することによって、キー番号を変更できます。デフォルトのキー番号は 1 です。

［EAP］

このセキュリティ設定では、IEEE 802.1X 認証が有効になり、RADIUS サーバの IP アドレスを選択する必要があります。暗号化タイプは WEP で、認証タイプは IEEE 802.1x です。

［WPA］

このセキュリティ設定では、EAP 設定よりも高いセキュリティを確保できます。この設定では、WPA 認証が有効になり、RADIUS サーバの IP アドレスを選択する必要があります。この SSID を使用してアクセスポイントに関連付けられるクライアント デバイスは、WPA 対応である必要があります。認証タイプは IEEE 802.1x です。

この種類のセキュリティを設定するには、［暗号化］フィールドから暗号化タイプを選択します。［aes］または［tkip］を選択できます。

［WPA-PSK］

WPA 暗号化を使用する場合に RADIUS サーバにアクセスできないときは、このセキュリティ設定を選択します。この設定では、アクセスポイントとクライアント デバイスで同一の WPA-PSK を共有する必要があります。キーは、8 から 63 文字の長さで指定できます。認証タイプは WPA-PSK です。

この種類のセキュリティを設定するには、次の手順に従います。

1. [暗号化]フィールドから暗号化タイプを選択します。[aes]または[tkip]を選択できます。
2. [WPA事前共有キー] フィールドにキーを入力します。

[WPA2]

このセキュリティ設定は、WPA 設定よりもセキュリティ レベルが高くなります。この設定では、WPA2 認証が有効になり、RADIUS サーバの IP アドレスを選択する必要があります。この SSID を使用してアクセスポイントに関連付けられるクライアント デバイスは、WPA2 対応である必要があります。認証タイプは IEEE 802.1x です。

この種類のセキュリティを設定するには、[暗号化]フィールドから暗号化タイプを選択します。[aes]または[tkip]を選択できます。

[WPA2-PSK]

WPA2 暗号化を使用する場合に RADIUS サーバにアクセスできないときは、このセキュリティ設定を選択します。この設定では、アクセスポイントとクライアント デバイスで同一の WPA2-PSK を共有する必要があります。キーは、8 から 63 文字の長さで指定できます。認証タイプは WPA2-PSK です。

この種類のセキュリティを設定するには、次の手順に従います。

1. [暗号化]フィールドから暗号化タイプを選択します。[aes]または[tkip]を選択できます。
2. [WPA2事前共有キー]フィールドにキーを入力します。

[MAC]

MAC ベースの認証を使用してクライアント デバイスを認証する場合にこのセキュリティ設定を選択します。

暗号化はなく、認証タイプは IEEE 802.1x です。

この種類のセキュリティを設定するには、次の手順に従います。

1. RADIUS サーバの IP アドレスを入力します。
2. 自律型アクセスポイントで RADIUS サーバとの通信に使用する共有秘密を入力します。

[MAC & EAP]

MAC ベースの認証と EAP 認証を組み合わせて使用してクライアント デバイスを認証する場合にこのセキュリティ設定を選択します。IEEE 802.11 オープン認証を使用してアクセスポイントに関連付けられるクライアント デバイスは、まず MAC 認証を試みます。MAC 認証に成功すると、このクライアント デバイスはネットワークに接続されます。クライアントで EAP 認証も使用されている場合は、EAP を使用して認証が行われます。MAC 認証に失敗すると、アクセスポイントは、クライアント デバイスによる EAP 認証を待機します。

暗号化タイプは WEP で、認証タイプは IEEE 802.1x および Open MAC です。

この種類のセキュリティを設定するには、[暗号化]フィールドから暗号化タイプを選択します。[aes]または[tkip]を選択できます。

WLC526 を管理する場合

[WLANユーザ]ウィンドウ

このウィンドウを使用すると、WLAN コントローラに無線ユーザを設定したり、WLAN コントローラに設定されている無線ユーザ設定を表示したりできます。

次の表は、[無線ネットワークユーザ]領域のカラムについて説明しています。

カラム	説明
ユーザ名	無線ユーザの名前
ゲストユーザ	ゲスト ユーザのステータス([はい]または[いいえ])
SSID	SSID の名前
終了時間	ゲスト ユーザのアクセスの有効期限
説明	無線ユーザの説明

WLAN コントローラの無線ユーザを設定する手順は、次のとおりです。

1. [ホスト名] リストから対象の WLAN コントローラを選択します。
2. ゲスト ユーザやゲスト以外のユーザを作成するには、[作成]をクリックして、[WLANユーザの作成]ウィンドウに必要な情報を入力します。

無線ユーザを変更するには、対象のユーザ名を選択して[修正]をクリックし、[WLANユーザの修正]ウィンドウを使用します。

無線ユーザを削除するには、対象のユーザ名を選択して[削除]をクリックします。

注: [WLANユーザ]ウィンドウを開く際にゲスト ユーザのアクセス期限が切れていた場合は、自動的に[無線ネットワークユーザ]リストからそのゲスト ユーザが削除されます。ゲスト ユーザ のアクセス期限が切れるときにすでに[WLANユーザ]ウィンドウが開いており、そのゲスト ユーザを変更しようとし

た場合は、そのゲスト ユーザは[無線ネットワークユーザ]リストから削除されます。新しいゲスト ユーザを作成するには、[作成]をクリックします。

無線ユーザ用のログイン ページを設定するには、[Webログイン]領域で[設定]をクリックします。

変更を保存してウィンドウを閉じるには、[WLANユーザ]ウィンドウで[OK]をクリックします。

WLC526 を管理する場合

[WLANユーザの作成]ウィンドウ

このウィンドウは、[WLANユーザ]ウィンドウで[作成]をクリックした場合に表示されます。このウィンドウを使用すると、新しい無線ユーザを作成できます。

次の手順に従います。

1. [ユーザ名]フィールドに、無線ユーザの名前を入力します。最大 24 文字の英数字を入力できます。
2. [パスワード]フィールドに、無線ユーザのパスワードを入力します。最大 24 文字の英数字を入力できます。
3. [パスワード確認]フィールドにパスワードをもう一度入力します。
4. [説明]フィールドに、無線ユーザについての説明を入力します。
5. 無線ユーザがゲスト ユーザではない場合は、次の手順を実行します。
    1. [ゲストユーザ]チェックボックスをオフにします。
    2. [SSID]リストから SSID を選択します。セキュリティが[Web認証]、[WEP]、[WPA1-PSK]、または[WPA2-PSK]に設定されている SSID のみが表示されます。

        注:SSID を作成する必要がある場合は、[SSIDの追加] (事前定義済み)をクリックして[SSIDの追加] (事前定義済み)ウィンドウを開きます。
6. 無線ユーザがゲスト ユーザの場合は、次の手順を実行します。
    1. [ゲストユーザ]チェックボックスをオンにします。
    2. [SSID]リストから SSID を選択します。セキュリティが[Web認証]に設定されている SSID のみが表示されます。

        注:SSID を作成する必要がある場合は、[SSIDの追加](事前定義済み)をクリックして[SSIDの追加](事前定義済み)ウィンドウを開きます。
    3. [終了時間]領域で、年、月、日、時、および分を選択して有効期限を入力します。ゲスト ユーザ用の最長有効期限は、現時点から 30 日間です。
7. このウィンドウに必要な情報を入力したら、[OK] をクリックして、変更を保存し、ウィンドウを閉じます。

WLC526 を管理する場合

[WLANユーザの修正]ウィンドウ

このウィンドウは、[WLANユーザ]ウィンドウで[修正]をクリックした場合に表示されます。このウィンドウを使用すると、無線ユーザ設定を変更できます。

次の手順に従います。

1. [パスワード]フィールドに、無線ユーザのパスワードを入力します。最大 24 文字の英数字を入力できます。
2. [パスワード確認]フィールドにパスワードをもう一度入力します。
3. [説明]フィールドに、無線ユーザについての説明を入力します。
4. [SSID]リストから SSID を選択します。
5. 無線ユーザがゲスト ユーザの場合は、[終了時間]領域で、年、月、日、時、および分を選択して有効期限を変更します。ゲスト ユーザ用の最長有効期限は、現時点から 30 日間です。
6. このウィンドウに必要な情報を入力したら、[OK] をクリックして、変更を保存し、ウィンドウを閉じます。

UC500、Cisco 800シリーズルータを管理する場合

[アカウントの追加]ウィンドウ

このウィンドウは、[VPNサーバ]ウィンドウで[作成]([ユーザアカウント])をクリックした場合に表示されます。

このウィンドウでは、ユーザの認証情報をローカル データベースに追加できます。

アカウントを追加するには、次の手順に従います。

1. [ユーザ名]フィールドにユーザ名を入力します。ユーザ名には最大 64 文字の英数字を使用できます。次の文字は使用できません。(スペース)、+、#、%、/、¥、?、;、<、>、{、}、|、^、~、[、]、`、および "
2. [パスワード]フィールドにパスワードを入力し、その後[パスワード確認]フィールドに同じパスワードを再入力します。パスワードには、最大 25 文字の英数字を使用できます。パスワードの最小文字数は 6 文字です。次の文字は使用できません。(スペース)、+、?、/、¥、<、>、#、%、{、}、|、^、~、[、]、`、および "
3. ウィンドウを閉じるには、[OK]をクリックします。

CE520 スイッチを管理する場合

[アップグレード設定]ウィンドウ

このウィンドウは、[ソフトウェアアップグレード]ウィンドウで 1 つまたは複数のデバイスを選択して、[アップグレード設定]をクリックした場合に表示されます。

[IOSイメージTarファイル]フィールドに、アップグレード先の IOS イメージ tar ファイルのフル パスとファイル名を入力します。[参照]をクリックすると、ファイルを参照できます。

[OK]をクリックして、入力したファイル名を保存します。[ソフトウェアアップグレード]ウィンドウに、新しい設定が表示されます。

UC500、Cisco 800シリーズルータを管理する場合

[アップグレード設定]ウィンドウ

このウィンドウは、[ソフトウェアアップグレード]ウィンドウで 1 つまたは複数のデバイスを選択して、[アップグレード設定]をクリックした場合に表示されます。このウィンドウを使用して、同一プラットフォーム上のデバイスのアップグレード設定を入力します。

まず、[モード]リストの項目を選択します。ローカルに保存されている Cisco IOS イメージを使用する場合は[標準]を選択し、それ以外の場合は[リモートTFTPサーバ]を選択します。

[標準]を選択した場合は、[IOSイメージ]フィールドに、Cisco IOS イメージのファイル名を入力します。[参照]をクリックすると、ファイルを参照できます。

[リモートTFTPサーバ]を選択した場合:

1. [IOSイメージ]フィールドに、Cisco IOS イメージのフル パスとファイル名を入力します。
2. [TFTPサーバIPアドレス]フィールドに、TFTP サーバの IP アドレスを入力します。

   注: グループでのアップグレードを実行するには、TFTP サーバで複数の要求およびセッションが同時に処理される必要があります。

[OK]をクリックして設定を保存します。[ソフトウェアアップグレード]に設定が表示されます。

UC500 を管理する場合

[アップグレード設定]ウィンドウ

このウィンドウは、[ソフトウェアアップグレード]ウィンドウで 1 つまたは複数のデバイスを選択して、[アップグレード設定]をクリックした場合に表示されます。このウィンドウを使用して、同一プラットフォーム上のデバイスのアップグレード設定を入力します。

Cisco IOS をアップグレードするには[IOS]をクリックし、CUE ソフトウェアをアップグレードするには[CUE]をクリックし、Cisco IOS、CUE、関連する CME 電話機用ファームウェア、およびサポート ファイルを含めたすべてのソフトウェアをアップグレードするには[すべて]をクリックします。

設定を入力したら[OK]をクリックします。[ソフトウェアアップグレード]に設定が表示されます。

Cisco IOS のアップグレード

[モード]リストから、ローカルに保存されている Cisco IOS イメージを使用する場合は[標準]を選択し、それ以外の場合は[リモートTFTPサーバ]を選択します。

[標準]を選択した場合は、[IOSイメージファイル]フィールドに、Cisco IOS イメージのファイル名を入力します。[参照]をクリックすると、ファイルを参照できます。

[リモートTFTPサーバ]を選択した場合:

1. [IOSイメージファイル]フィールドに、Cisco IOS イメージのフル パスとファイル名を入力します。
2. [TFTPサーバIPアドレス]フィールドに、TFTP サーバの IP アドレスを入力します。

   注: グループでのアップグレードを実行するには、TFTP サーバで複数の要求およびセッションが同時に処理される必要があります。

CUE ソフトウェアのアップグレード

次の手順に従います。

· [IOSイメージファイル]フィールドに、アップグレードした CUE ソフトウェアを含むパッケージ ファイルのフル パスとファイル名を入力します。
· [言語]リストで、対象の CUE ソフトウェアの言語を選択します。

すべてのソフトウェアのアップグレード

モードが[標準]に、および言語が[英語(米国)]にデフォルト設定されます。[IOSイメージファイル]フィールドに、Cisco.com からダウンロードした必要なソフトウェアすべてが含まれる zip ファイルのフル パスとファイル名を入力します。

CE520 スイッチを管理する場合

[イーサチャネル]ウィンドウ

このウィンドウを使用して、イーサチャネル ポート グループを表示して次の作業を行います。

- ポート グループの作成
- ポート グループの変更
- ポート グループの削除

まず、ローカル デバイスを[ホスト名]リストから選択します。[チャネルグループ]領域の情報は、選択したデバイスに適用されます。

[ロードバランス]フィールドは、デフォルトで[発信元/宛先IPアドレス]に設定されています。このフィールドは変更できません。

選択内容は、スイッチ上に作成するポート グループごとに適用されます。

次の表は、[チャネルグループ]領域のカラムについて説明しています。

カラム	説明
グループ	ポート グループに割り当てられた数。
ポート	グループに属するポート。
ステータス	[down]または[In use]のいずれか。グループに[レイヤ2]インターフェイスが存在することも表示されます。

ポート グループの作成

最大 6 つのポート グループを作成できます。グループを形成するポートは、同じタイプのものでなければなりません。

LACP モードの場合、ポート グループには最大 16 のメンバを入れることができます。そうでない場合には、最大 8 つのメンバを入れることができます。

注: この手順を使用する前に、ポート グループの制限を確認してください。

ポート グループを作成するには、次の手順に従います。

1. [作成]をクリックし、[イーサチャネルの作成]ウィンドウを使用します。

   選択したローカル デバイスでも、またオプションでリモート デバイスでもポート グループを作成できます。

2. [OK]をクリックして、変更を適用し、ウィンドウを閉じます。
3. [OK]をクリックして、[イーサチャネル]ウィンドウを閉じます。

注: デフォルトでは、スイッチはパケット送信元アドレスに基づいてトラフィックをポート グループに転送します。ポート グループの静的アドレスを設定する場合、パケットを静的アドレスからグループのすべてのポートに転送し、パケットの損失を防ぐようにスイッチを設定します。送信先アドレスに基づいてパケットを転送するようにポート グループを設定した場合、静的アドレスの送信先パケットをポート グループの 1 つのポートにのみ転送するようにスイッチを設定します。そうしないと、送信先アドレスは重複パケットを受信します。

ポート グループの変更

ポート グループを変更するには、次の作業を行います。

- メンバ ポートの追加
- メンバ ポートの削除
- メンバ ポートの LACP モードの変更

これらの作業のいずれかを行うには、次の手順に従います。

1. [チャネルグループ]領域で、変更するグループの行を選択します。
2. [修正]をクリックし、[イーサチャネルの修正]ウィンドウを使用します。

   選択したローカル デバイスでも、またオプションでリモート デバイスでもポート グループを変更できます。

3. [OK]をクリックして、変更内容を確定し、ウィンドウを閉じます。
4. [OK]をクリックして、[イーサチャネル]ウィンドウを閉じます。

ポート グループの削除

ポート グループを削除するには、次の手順に従います。

1. [チャネルグループ]領域で、削除するグループの行を選択します。
2. [削除]をクリックします。
3. [OK]をクリックしてウィンドウを閉じます。

ポート グループの制限

どのポートもポート グループに属することができますが、次の制限が適用されます。

- ポート グループ メンバには、[スイッチ]ロールを適用する必要があります。
- どのポート グループ メンバもポート モニタリングを設定できません。
- どのポート グループ メンバもポート セキュリティを有効にできません。
- ポート グループ メンバは同じセットの VLAN に属する必要があり、すべて静的アクセス、すべてマルチ VLAN、またはすべてトランク ポートである必要があります。
- 動的アクセス ポートは、他の動的アクセス ポートとも、他のいかなるポートともグループ化できません。
- ネットワーク ポートは送信先ベースのポート グループに属することはできません。

CE520 スイッチを管理する場合

[イーサチャネルの作成]ウィンドウ

このウィンドウは、[イーサチャネル]ウィンドウで[作成]をクリックした場合に表示されます。これを使用して、ローカル ポートを選択したデバイスのポート グループに割り当て、リモート ポートをリモート デバイスのポート グループに割り当てます。

注： スイッチ ポートのロールを割り当てたポートのみがこのウィンドウに表示されます。

次の手順に従います。

1. ローカル デバイスおよびリモート デバイスの両方にポート グループを作成する場合には、[リモートデバイス]リストからリモート デバイスを選択します。リモート ポート側のウィンドウに、ローカル デバイスのポートに接続されているリモート ポートが表示されます。

   リモート デバイスのオプションは、ローカル デバイスのオプションと同じです。ローカル デバイスのオプションを選択する際には、リモート デバイスと同一にしてください。

2. [グループ]フィールドに、作成するポート グループの番号を入力します。
3. [グループ]のチェック ボックスでグループ メンバに加える各ポートをオンにします。

4. [ステータス]カラムは無視します。ここには、[イーサチャネルの変更]ウィンドウのポートのステータスのみが表示されます。
5. 選択したポートの[モード]セルをクリックして、次の値のいずれかを選択します。
   - [LACP]:ポートではリンク集約を形成し、チャネルを開始できます。他端で LACP がアクティブ モードで稼動している場合、集約が形成されます。
   - [On (No LACP)]:ポートでは LACP は使用されません。ポート グループがこのモードで別のグループに接続されている場合にのみ、使用可能な イーサチャネル が存在します。
6. 選択したポートの[優先順位]セルをクリックして、デフォルト(LACP の場合 32768)以外の LACP 優先度を指定する場合にはその値を入力します。

   優先度が最も高いポートがパケットを送信します。

7. [OK]をクリックしてウィンドウを閉じます。

   新規ポート グループが[イーサチャネル]ウィンドウに表示されます。

CE520 スイッチを管理する場合

[イベント通知]ウィンドウ

このウィンドウは、次のいずれかの操作を実行した場合に表示されます。

- ステータス バー上または[トポロジ]ビュー内でアイコン、、、またはをクリックする(アイコンの説明は、ネットワーク イベントの管理をクリックする)。
- 機能バー上で **モニタ > イベント通知** を選択する。
- ツールバー上で を選択する。

このウィンドウには、次のタブがあります。

- [イベント]。ネットワーク内のすべてのイベントの説明が表示されます。イベントを認識し、可能な場合は Configuration Assistant を使用してイベントを解決します。
- [LEDアラート]。アラート LED をオンにしたイベントの説明が表示されます。

イベント情報のサブセットを表示するには、[フィルタ]をクリックして[通知フィルタ]ウィンドウを使用します。

ウィンドウでの作業が完了したら、[OK]をクリックします。

[イベント]

次の表は、このタブに表示される情報について説明しています。

カラム	説明
タイ	イベントを解決する緊急性を示します。タイプ番号が小さいほど、イベントを解決する必要性が

プ	緊急になります。
デバイス	イベントに関係しているデバイスです。
時間	イベントが発生した時刻です。
イベント説明	発生した内容の簡単な説明です。イベントを選択すると、イベントのリストの下に詳細が表示されます。
解決可能	Configuration Assistant でイベントを解決できる場合は[はい]が表示され、イベントを解決できない場合は[いいえ]が表示されます。Configuration Assistant を使用してイベントを解決するには、対象のイベントを強調表示して[解決]をクリックします。イベントの解決に使用するウィンドウが開きます。
認識済み	イベントの認識を示すためのチェックボックスです。[すべてを認識済みに設定]をクリックすると、一度にすべてのイベントを認識できます。認識されたイベントのアイコンは、ぼかし表示になります。

[LEDアラート]

このタブに表示されるイベント情報は、次の点においてネットワーク イベントのタブに表示される情報と異なります。

- 表示されるイベントは LED アラートだけです。つまり、デバイスのアラート LED をオンにするイベントだけです。
- Configuration Assistant を使用して LED アラートを解決することはできません。
- LED アラートを強調表示して[クリア]をクリックすることにより、LED アラートを削除できます。ただし、原因となっている問題を修正するまで、アラートは繰り返し発生します。

UC500、Cisco 800シリーズルータを管理する場合

[インターネット接続]ウィンドウ

このウィンドウは、**設定 > インターネット接続** を選択した場合に表示されます。

インターネット接続を有効にするには、次の手順に従います。

1. [ホスト名]リストから、設定するデバイスを選択します。
2. [WANインターフェイス]リストからインターフェイスを選択します。
3. [修正]をクリックし、[インターネット接続の修正]ウィンドウを使用します。
4. 変更を保存してウィンドウを閉じるには、[OK]をクリックします。

UC500、Cisco 800シリーズルータを管理する場合

[インターネット接続の修正]ウィンドウ

このウィンドウは、[インターネット接続]ウィンドウで[修正]をクリックした場合に表示されます。

インターフェイスにインターネット接続を設定するには、次の手順に従います。

1. インターネット接続を有効にするには、[WANインターフェイスを有効にする]チェックボックスをオンにします。
2. オプション：サービス プロバイダから PPPoE の使用を義務付けられており、これを有効にする必要がある場合は、[PPPoE]チェックボックスをオンにします。
3. [ユーザ名]フィールドにユーザー名を入力します。
4. PPPoE を有効にした場合は、[パスワード]フィールドに CHAP/PAP 認証用のパスワードを入力し、[パスワードの再入力]フィールドに同じパスワードをもう一度入力します。
5. [静的IP]、[DHCP]、または[IPネゴシエート]ボタンを選択します。[静的IP]を選択した場合は、下記の手順に示すように、IP アドレス情報を入力します。[DHCP]を選択した場合は、ルータによってリモート DHCP サーバから IP アドレスがリースされます。PPPoE カプセル化を使用する場合だけ有効になる[IPネゴシエート]を選択した場合は、ルータにより、PPP/IPCP アドレス ネゴシエーションを通じて IP アドレスが取得されます。
6. 静的 IP アドレスを設定する場合は、次の手順に従います。
    1. [インターネットIPアドレス]フィールドに、静的 IP アドレスを入力します。
    2. [サブネットマスク]フィールドに、サブネット マスクを入力します。
    3. [デフォルトゲートウェイ]フィールドに、デフォルト ゲートウェイの IP アドレスを入力します。
    4. ウィンドウを閉じるには、[OK]をクリックします。

CE520 スイッチを管理する場合

[インターフェイスの選択]ウィンドウ

このウィンドウは、[Configuration Assistant]ウィンドウで　アイコンをクリックした場合に表示されます。ここには、選択したスイッチのフロント パネルが表示されます。このウィンドウを使用して、スイッチのインターフェイスを選択します。

次の手順に従います。

1. 使用するインターフェイスをクリックします（選択できないインターフェイスはグレー表示になっています）。
2. [OK]をクリックします。使用していた[Configuration Assistant]ウィンドウに戻ります。[インターフェイス]フィールドに選択したインターフェイスの数が表示されます。

CE520 スイッチを管理する場合

[インベントリ]ウィンドウ

この読み取り専用ウィンドウには、コミュニティ内のデバイスのインベントリが表示されます。このウィンドウは、次のいずれかの操作を実行した場合に表示されます。

- 機能バー上で **モニタ > レポート > インベントリ** を選択する。
- ツールバー上で をクリックする。

インベントリでは、コミュニティ内の各デバイスについて、次の項目が表示されます。

- ホスト名
- タイプ
- MAC アドレス
- ハードウェアのバージョン番号（バージョン ID）
- シリアル ナンバー
- IP アドレス
- インストールされているソフトウェアのリビジョン
- 場所
- デバイスが動作し始めてからの時間

コミュニティ内のスイッチにホスト名が割り当てられていない場合、「switch-」の後に数値が続くホスト名が自動的に割り当てられます。その数値は、対象のスイッチがコミュニティに追加された順番を示します。

UC500、Cisco 800シリーズルータを管理する場合

[インベントリ詳細]ウィンドウ

このウィンドウは、[インベントリ]ウィンドウでルーティング機能のあるデバイスを選択して、[詳細]をクリックした場合に表示されます。

このウィンドウには、コンポーネントごとのデバイス情報、モデルの説明、部品番号、ハードウェアのリビジョン、Printed Circuit Board（PCB; プリント基板）のシリアル番号、および製品番号が表示されます。モデルの説明は、コンポーネントの詳細です。部品番号は、コンポーネントの製造番号です。

変更が加えられたことがわかっていて、その変更を確認する場合、[更新]をクリックします。コンポーネントが削除または追加されたときは、Configuration Assistant によってそのコンポーネントが再度サンプリングされ、詳細が再表示されます。

UC500、Cisco 800シリーズルータを管理する場合

[音声]ウィンドウ

このウィンドウは、機能バー上で **設定 > テレフォニー > 音声** を選択した場合に表示されます。

注:

- Telnet が無効になっている場合、音声機能は設定できません。[デバイスアクセス]ウィンドウを使用して Telnet を有効にしてください。
- ユーザ パラメータのバルク インポートを実行する前に、すべての音声機能を設定してください。

このウィンドウには、次のタブがあります。

- [デバイス]
- [システム]
- [ネットワーク]
- [自動音声応答とボイスメール]
- [SIPトランク]
- [音声機能]
- [ダイヤルプラン]
- [ユーザ]

[デバイス]

ハードウェア デバイスの設定が検出され、表示されます。アプリケーションでは、修正可能な設定パラメータが、ルータのハードウェア設定に基づいて制限されます。

通話処理を PBX の通話処理と同じようにするか、それともキーシステムの通話処理と同じようにするかを設定するには、[PBX]オプション ボタンまたは[キーシステム]オプション ボタンをクリックします。**注意**:このパラメータは初期設定の際にのみ使用できます。このパラメータを設定すると、このフィールドは読み取り専用となります。

公衆電話交換網(PSTN)を設定するには、次の手順に従います。

1. 接続タイプを選択するには、[音声システムのタイプ]オプション ボタンをクリックします。このパラメータは初期設定の際にのみ使用できます。このパラメータを設定すると、このフィールドは読み取り専用となります。デバイスに T1/E1 ボイス ポートが内蔵されている場合には、T1/E1 オプションが表示されます。(VIC スロットに取り付ける T1/E1 ボイス カードはサポートされません。)
2. ボイス ポート アダプタを設定するには、[チャネルシグナリング]メニューでチャネル シグナリング タイプを選択します。
    - [チャネルシグナリング]メニューから[ISDN PRI]を選択した場合は、次の手順に従います。
        1. [スイッチタイプ]メニューで、設定するスイッチのタイプを選択します。このパラメータを使用して、グローバル ISDN スイッチのタイプおよびインターフェイス レベルのスイッチのタイプを指定します。

2. [PRIグループのタイムスロット]フィールドで、ISDN PRI グループのタイム スロットの範囲を指定します。デフォルトの T1 の範囲は、1 タイム スロットから 24 タイム スロットです。タイム スロット 24（D チャネル）は常に含まれます。タイム スロット 24 からタイム スロット 24 の範囲は無効です。デフォルトの E1 の範囲は、1 タイム スロットから 31 タイム スロットです。タイム スロット 16（D チャネル）は常に含まれます。タイム スロット 16 からタイム スロット 16 の範囲は無効です。

- [チャネルシグナリング]メニューから[FGD]を選択した場合は、次の手順に従います。
    1. シグナリングのタイプを選択するには、[EANA]または[OS]（オペレータのサービス）をクリックします。
    2. 着信および発信コールに個別のタイム スロットを使用するには、[発信と受信には異なるグループを使用]チェックボックスをオンにします。
    3. [グループのタイムスロット]フィールドに、タイム スロットの範囲を入力します。[発信と受信には異なるグループを使用]チェックボックスをオンにした場合には、[着信グループのタイムスロット]フィールドに着信タイム スロットの範囲を、[発信グループのタイムスロット]フィールドに発信タイム スロットの範囲を入力します。
- [チャネルシグナリング]メニューから[R2]を選択した場合は、次の手順に従います。
    1. シグナリングのタイプを選択するには、次のいずれかをクリックします。
        - [アナログ]：R2 回線のシグナリングのタイプ ITU-U Q.411 です。通常、キャリア システムに使用されます（Tone/A ビットが使用されている場合）。
        - [デジタル]：R2 回線のシグナリングのタイプ ITU-U Q0.421 です。通常、PCM システムに使用されます（A および B ビットが使用されている場合）。
        - [パルス]：R2 回線のシグナリングのタイプ ITU-U Supplement 7 です。通常、衛星リンクを展開するシステムに使用されます（Tone/A ビットがパルス化されている場合）。
    2. 着信および発信コールに個別のタイム スロットを使用するには、[発信と受信には異なるグループを使用]チェックボックスをオンにします。
    3. [タイムスロット]フィールドに、タイム スロットの範囲を入力します。または、[発信と受信には異なるグループを使用]チェックボックスをオンにした場合には、[着信グループのタイムスロット]フィールドに着信タイム スロットの範囲を、[発信グループのタイムスロット]フィールドに発信タイム スロットの範囲を入力します。デフォルトの E1 の範囲は、1 タイム スロットから 31 タイム スロットです。タイム スロット 16（D チャネル）は常に含まれます。タイム スロット 16 からタイム スロット 16 の範囲は無効です。
- [チャネルシグナリング]メニューから[FXO]、[FXS]、または[E&M]を選択した場合には、次の手順に従います。
    1. [シグナル]メニューからシグナリングのタイプを選択します。
    2. 着信および発信コールに個別のタイム スロットを使用するには、[発信と受信には異なるグループを使用]チェックボックスをオンにします。
    3. [グループのタイムスロット]フィールドに、タイム スロットの範囲を入力します。[発信と受信には異なるグループを使用]チェックボックスをオンにした場合には、[着信グループのタイムスロット]フィールドに着信タイム スロットの範

囲を、[発信グループのタイムスロット]フィールドに発信タイム スロットの範囲を入力します。デフォルトの T1 の範囲は、1 タイム スロットから 24 タイム スロットです。タイム スロット 24（D チャネル）は常に含まれます。タイム スロット 24 からタイム スロット 24 の範囲は無効です。デフォルトの E1 の範囲は、1 タイム スロットから 31 タイム スロットです。タイム スロット 16（D チャネル）は常に含まれます。タイム スロット 16 からタイム スロット 16 の範囲は無効です。

ISDN PRI が PBX モードに設定されている場合、ボイス ポートのダイヤル ピアが自動的にルータ上で設定されます。キーシステム モードを選択した場合には、ダイヤル ピアは設定されません。

注：UC520 VIC スロットに VIC-FXS または VIC-FXS/DID が取り付けられている場合には、Configuration Assistant により 0/2/0、0/2/1、0/2/2、および 0/2/3 のポートにそれぞれ 1100、1101、1102、および 1103 のダイヤルピア タグ番号が予約されます。アウトオブバンドで、2500 から 2999 までのユーザ定義のダイアル ピア タグを設定できます。

ISDN PRI が存在して選択されており、さらに BRI インターフェイスが 1 つ以上存在する場合、BRI スイッチのタイプを設定する必要があります。[スイッチタイプ]パラメータを使用して BRI インターフェイス上の ISDN スイッチのタイプを設定し、競合を避けます。

デバイスに 1 つまたは複数の BRI ボイス ポートが内蔵されている場合には、BRI オプションが表示されます。スイッチのタイプを設定するには、[スイッチタイプ]メニューからスイッチのタイプを選択します。

FXS/DID（VIC 専用）カードがある場合には、次の手順に従います。

1. [モード]メニューから、[FXS]モードまたは[DID]モードを選択します。
2. [シグナル]メニューから、FSX モードのポートには[ループスタート]または[グラウンドスタート]を、DID モードのポートには[遅延ダイヤル]、[即時スタート]、または[ウィンクスタート]を選択します。
3. [発信者ID]フィールドに、着信先の電話に表示される発信者 ID を入力します。
4. [内線番号]フィールドに、内線番号を入力します。
5. [権限]フィールドに、権限を入力します。
6. [ブロック制限番号]チェックボックスをオンにして、制限された番号をブロックします。

注：8 ユーザ システムまたは 16 ユーザ システムに VIC が存在する場合、アドホック会議の参加者は 3 名までに制限されます。4 名以上の参加者をサポートできるだけのデジタル シグナル プロセッサ（DSP）を用意できないことがあるためです。

[システム]

ローカル設定を行うには、次の手順に従います。

1. [地域]メニューから、Cisco Unified Communications Manager Express の地域を選択します。それによって、電話のトーンと鳴り方が設定されます。
2. [電話の言語]メニューから、ユーザの電話に表示される言語を選択します。
3. [ボイスメールの言語]メニューから、ボイスメールのユーザに聞かせるボイス メール プロンプトの言語を選択します。言語パックをインストールするには、次の手順に従います。

1. Cisco Unified Communications Manager Express の、必要な言語の tar ファイルをダウンロードします。
2. Cisco Unity Express の、必要な言語のパッケージ ファイルをダウンロードします。
3. [言語ファイルの場所]フィールドに表示されているフォルダにファイルをコピーします。
4. [適用]をクリックします。

4. [日付書式]メニューから、日付形式を選択します。
5. [時間制]メニューから、時刻形式を選択します。
6. オプション:[システムメッセージ]フィールドに、システム メッセージを入力します。

注:ロケール、時間帯、または日付形式のパラメータを変更すると、IP Phone はリブートします。

市内の短縮ダイヤル メニューをすべての電話、Skinny Call Control Protocol(SCCP)および SIP に対して有効にするには、次の手順を実行します。

1. [追加]をクリックします。
2. [名前]フィールドに、短縮ダイヤルの名前を入力します。
3. [電話番号]フィールドに、短縮ダイヤルの番号を入力します。

リストの市内短縮ダイヤル番号を並べ替えるには、エントリを選択して、上下の矢印をクリックします。これによって、エントリが電話に表示される順序が示されます。

メニューから市内短縮ダイヤル番号を削除するには、メニューでエントリを選択して[システムスピードダイヤル]ボックスで[削除]をクリックします。

リストのエントリが許可された最大数に達した場合には、[追加]ボタンが無効になります。

[ネットワーク]

ネットワーク パラメータを設定するには、次の手順に従います。

1. [VLAN番号]メニューから、音声ネットワークのサブインターフェイス番号を選択します。選択値の範囲は、1 から 1001 です。音声 VLAN は、デフォルトでは VLAN 100 です。別の音声 VLAN を設定するには、次の手順に従います。
   - [設定]>[VLAN]の順に選択して、新しい VLAN を作成します。
   - [音声]画面をリフレッシュして、新しい VLAN を読み込みます。ドロップダウン メニューに新しい VLAN が表示されます。
   - スマート ポートを使用し、各スイッチ ポートから新しい音声 VLAN に接続できるように設定します。
2. [DHCP IPアドレスプール]フィールドと[サブネットマスク]フィールドに、IP アドレスと、サブネット マスクの範囲内の最初の IP アドレスを入力します。このパラメータを変更すると、IP Phone はリブートします。
3. [除外対象アドレス]フィールドに、音声ネットワークの DHCP アドレス指定から除外する IP アドレスの範囲を入力します。

4. [CME IPアドレス]フィールドと[サブネットマスク]フィールドに、設定するルータの Cisco Unified Communications Manager Express(CME)IP アドレスとサブネット マスクを入力します。この IP アドレスとサブネット マスクは、DHCP による割り当てから除外されます。

[自動音声応答とボイスメール]

自動音声応答(AA)パラメータを設定するには、次の手順に従います。

1. [自動音声応答の内線番号]フィールドに、企業向けの一般的な自動音声応答機能を使用する内線番号を入力します。これは通常、オフィスの代表電話の内線番号です。発信者がこの内線番号をダイヤルすると、自動音声応答スクリプトが稼動します。
2. [自動音声応答のPSTN番号]フィールドに、企業向けの一般的な自動音声応答機能を使用する PSTN 番号を入力します。
3. [自動音声応答スクリプト]メニューから、トリガー イベントが発生する際に実行するスクリプトを選択します。デフォルトのスクリプト以外のスクリプトを選択すると、次のスクリプト パラメータを設定できます。
    - [メニュープロンプト]:自動音声応答を起動すると再生される WAV ファイル。現在の WAV ファイルがフィールドに表示されます。別の WAV ファイルを選択するには、[参照]をクリックして[プロンプトファイルのアップロード]ウィンドウを使用します。
    - [オプション *n*](この場合 *n* はユーザがダイヤルしたオプションの番号):プライマリ ユーザ内線番号のリストを表示します。各リストから内線番号を選択するか、フィールドに内線番号を入力します。自動音声応答をキーシステム モードで設定している場合、メニューには各交換局の回線とすべての交換局の回線を呼び出すオプションのリストが表示されます。

ボイスメール パラメータを設定するには、次の手順に従います。

1. [ボイスメールの内線番号]フィールドに、着信に対する応答メッセージを流す電話機の内線番号を入力します。これは、着信コールに完全自動対応するフロント エンドの電話機に使用する内線番号です。
2. [ボイスメールのPSTN番号]フィールドに、着信に対する応答メッセージを流す PSTN 番号を入力します。

[SIPトランク]

キーシステム通話処理では、SIP トランクをサポートしていません。

SIP トランク パラメータを設定するには、次の手順に従います。

1. [サービス プロバイダ]メニューで、このルータから PSTN にアクセスするときに接続する SIP トランク サービス プロバイダを選択します。このルータから SIP トランクに接続しない場合は、[なし]を選択し、残りの手順は省略します。
2. オプション:[レジストラサーバ]フィールドに、プライマリ SIP レジストラ サーバの IP アドレスを入力します。
3. [プロキシサーバ]フィールドに、外部 SIP レジストラ サーバの IP アドレスを入力します。
4. オプション:[MWIサーバ]フィールドに、外部の SIP ベース MWI サーバの IP アドレスを入力します。

5. オプション:ダイジェスト認証の[ユーザ名]フィールドに、SIP 電話登録の認証クレデンシャルとして使用する名前を入力します。この名前は 一語にする必要があります。また、疑問符やスペースを含むことはできません。
6. オプション:ダイジェスト認証の[パスワード]フィールドに、このユーザ名のパスワードを入力します。パスワードの長さは 1 から 25 文字にする必要があります。スペースを含めることもできます。
7. オプション:ドメイン ネーム サービスの[SIPドメイン名]フィールドに、プライマリ SIP レジストラ サーバの DNS 名を入力します。
8. オプション:ドメイン ネーム サービスの[DNSサーバアドレス]フィールドに、プライマリ SIP レジストラ サーバの DNS アドレスを入力します。

[音声機能]

注: 通話処理をキーシステムとして設定した場合、一斉同報とインターコムのみ設定できます。

保留音を設定するには、[保留音]メニューから音楽を選択します。

一斉同報のパラメータを設定するには、次の手順に従います。

1. [有効にする]チェックボックスをオンにします。
2. [一斉同報グループ数]メニューから、設定する一斉同報 グループの数を選択します。
3. [一斉同報グループの内線番号]フィールドに、設定する各一斉同報 グループの内線番号を入力します。

グループ ピックアップ パラメータを設定するには、[有効にする]チェックボックスをオンにして、[ピックアップグループ数]メニューからピックアップ グループ数を選択します。

発信者 ID ブロック コードを設定するには、次の手順に従います。

1. [有効にする]チェックボックスをオンにし、[発信者IDブロックコード]フィールドにブロック コードを入力します。
2. 発信者の ID コードを入力します。発信者 ID ブロック コードは、電話のユーザが電話をかける前にダイヤルすることができる 4 桁のコードです。呼び出される側の電話に自分の番号を表示させたくない場合、ユーザはこのコードをダイヤルしてから、電話をかけます。発信者 ID は送信されますが、その表示パラメータは「制限」に設定されているので、発信者 ID は表示されません。このコードはアスタリスク(*)と 3 桁の数字で構成されます。最初の文字はアスタリスク(*)にする必要があります。使用可能な番号の範囲は 000 から 999 です。
3. [追加]をクリックします。

発信ブロック番号リストを設定するには、次の手順に従います。

1. [発信ブロック番号リスト]フィールドに、ブロックする番号を入力します。コール ブロッキングは、ダイヤルされた番号を、指定した桁数のパターンと照合して、電話の不正使用を防止します。コール ブロッキングは、IP 電話でのみサポートされ、アナログ FXS 電話ではサポートされていません。ユーザが、コール ブロッキングに指定したパターンで照合する桁数を呼び出そうとすると、高速の話中音が約 10 秒間聞こえます。その時点で呼び出しは終了し、回線は受話器が下ろされた状態に戻ります。

- 特定のパターンで始まるすべての番号をブロックするには、その番号のパターンを入力します。たとえば、5550000 から 5559999 までの番号をブロックするには、「555」と入力します。このパターンを含む番号のうち、このパターンで始まっていない番号はブロックされません。たとえば、15550000411 はブロックされません。
- 市外局番や国コードを含む長距離番号をブロックするには、その長距離ダイヤルコードも一緒に入力します。たとえば、900 の市外局番を持つ番号をブロックするには、「1900」と入力します。
- 411 のような特殊な市内電話番号をブロックするには、その番号を入力します。パターンは、最初の桁で照合されます。番号にパターンが含まれていても、たとえば 15555550411 はブロックされません。

2. [追加]をクリックします。

リストから**発信コール ブロック**の番号を削除するには、リストから削除する番号を選択して[削除]をクリックします。

インターコムを有効にして、プッシュ ツー トーク インターコム回線を使用して IP Phone 同士で対話できるようにするには、[インターコムを有効にする]チェックボックスをオンにします。

ハント グループ パラメータを設定し、順次選択またはラウンドロビン選択を使用して IP Phone グループ内でコールを分配するには、次の手順に従います。

1. [ハントグループ数]メニューで、[有効にする]チェックボックスをオンにします。
2. [ハントグループ数]メニューから、ハント グループ数を選択します。
3. [ハントのタイムアウト]フィールドに、まだ応答を受けていないコールをボイス ハント グループ リストの次の番号にリダイレクトするまでの秒数を入力します。入力値の範囲は、5 から 20 です。
4. [パイロット]フィールドに、設定する各ハント グループの番号を入力します。これは、ハント グループの最初の内線番号と、発信者がボイス ハント グループに接続するためにダイヤルする内線番号です。
5. メニューから[ハントタイプ]を選択します。設定する各ハント グループのタイプを選択します。
    - [順次]:コール ハントは常にグループのパイロット番号から開始され、その後、グループ内の各番号に対して、リストされている順(左から右)に続けられます。
    - [最長のアイドル時間]:コールは、その内線番号での最後の応答時刻に基づき、最も長い間アイドル状態になっていると判断されたディレクトリ番号に送信されます。その内線番号が使用不可の場合は、検索が続行され、グループ内の次の内線番号が検出されます。
    - [ピア]:このタイプのハント グループでは、最初に呼び出す番号がリストからラウンドロビン方式で選択されます。
6. [VMに転送]チェックボックスでは、未応答のコールを、最初に呼び出した内線番号のボイスメールボックスに、ボイス ハント グループから転送するかどうかを設定します。

パーク スロット数を設定するには、次の手順に従います。

1. [有効にする]チェックボックスをオンにします。
2. [パークスロット数]メニューから、設定するパーク スロット数を選択します。

3. [パークスロットの内線番号]フィールドに、各パーク スロットの番号を入力します。この機能では、着信コールの一時的な保管場所が確保されます。コールがパークされると、コールはパーク スロット番号に転送され、パークされたコールのパーク スロット番号で呼び出された別の従業員がその電話に応答するまで保留状態に置かれます。

アドホック会議を設定するには、次の手順に従います。

1. [参加者]メニューから、許可する参加者の最大数を選択します。
2. 混在モード(ハードウェアベースのアドホック会議)を有効にするには、[混在モード]チェックボックスをオンにします。このチェックボックスをオフにすると、デバイスは、シングル モードのアドホック会議用に設定されます。

[セッション]メニューには、許可するセッションの最大数が表示されます。許可するセッションの最大数は、選択した参加者数および使用するデバイスの制約に応じて変わります。このパラメータは設定できません。

注:

シングル モード(G711 コーデックを持つ参加者のみ)では、最大 3 名の参加者を設定できます。4 名以上の参加者を選択した場合、フリーの DSP リソースを備えたハードウェアベースのアドホック会議が必要になります。ハードウェアベースのアドホック会議は、シングル モードでも混在モード(G711 コーデックおよび G729 コーデックを持つ参加者)でも設定できます。

8 ユーザ システムまたは 16 ユーザ システムを VIC で設定している場合、ハードウェアベースのアドホック会議が VIC カードを CCA から設定する前にデバイス上で設定済みであれば、アドホック会議をソフトウェアベースの会議に戻す必要があります。それには、3 名の参加者を選択して[適用]をクリックします。トランスコーディングなどの DSP 関連の設定が、アウトオブバンドで任意のシステムで実行された場合、アドホック会議は使用できません。アウトオブバンドのアドホック会議を作成するか、アウトオブバンド用に修正する必要があります。

[ダイヤルプラン]

システムの内線番号を設定するには、[内線番号の桁数]フィールドに、その場所の内線番号の桁数を入力します。

注: 通話処理をキーシステムとして設定した場合、国際ダイヤル プランや国内ダイヤル プランは設定できません。

発信コール処理を設定するには、次の手順に従います。

1. オプション ボタンを使用して、[発信コール処理 番号計画のロケール]を選択します。
2. [市外局番の桁数]フィールドに、ルータの設置場所の国の市外局番の長さを入力します。長さが一定でない場合、このフィールドは空白のままにします。入力値の範囲は、1 から 10 です。
3. [市内番号の桁数]フィールドに、市内通話地域内の電話番号の長さを入力します。長さが一定でない場合、このフィールドは空白のままにします。入力値の範囲は、0 から 99 です。
4. [長距離電話発信番号]フィールドに、市内通話地域外の電話を呼び出す場合に(国内長距離呼び出し)、電話のユーザが(必要に応じて)発信コールのダイアル トーン番号を押した後に押す必要がある数字列を入力します。数字列の長さは 1 から 7 文字で、使用可能な数字

は 0 から 9 です。米国の場合、デフォルトは 1 です。ダイヤル トーン番号は、電話のユーザが PSTN 接続にアクセスするときに押す必要がある数字です。

5. [国際電話発信番号]フィールドに、ルータが設置された国以外の電話を呼び出す場合に、ユーザが押す必要がある数字列を入力します。数字列の長さは 1 から 7 文字で、使用可能な数字は 0 から 9 です。米国内から米国外への通話の場合、デフォルトは 011 です。
6. [外線発信番号]フィールドに、発信コールのダイヤル番号を入力します。

緊急番号を設定するには、[緊急電話番号]フィールドに緊急番号を入力します。北米のダイヤル プランでは、通常、緊急番号は 911 のように 3 桁です。ただし、10 桁の緊急番号も使用できます。10 桁の番号には、長距離のダイヤル コードを 10 桁の番号に追加する必要があります。たとえば、緊急番号として 408 522 4000 を使用したい場合には、「14085264000」と入力します。

個々のポートにカスタム設定を作成する場合には、[設定]をクリックして、[カスタムFXOポート]ウィンドウを使用します。

着信コール処理を設定するには、次の手順に従います。

1. [FXOトランク]メニューで、FXO ポート用の着信コールの宛先を選択します。
2. ダイヤルインの[設定]をクリックし、[DID設定]ウィンドウで 1 つの着信トランクの DID および柔軟な内線番号計画を持った各着信トランクのカスタム DID を指定します。

[ユーザ]

電話をデータベースに追加するには、次の手順に従います。

1. データベースにエントリを作成するには、[新規]をクリックします。
2. SIP 電話の場合、自動登録はサポートされていません。[MACアドレス]フィールドに、設定する各 IP Phone の MAC アドレスを入力します。
3. [電話タイプ]メニューから、設定する各 IP Phone の電話タイプを選択します。
4. [プライマリ内線番号]フィールドに、この IP Phone の内線番号を入力します。この内線番号には、実際の電話番号、この IP Phone 番号に割り当てられた内線番号、または Message Waiting Indication（MWI; メッセージ ウェイティング インジケータ）などの特別な機能の仮想電話番号を指定できます。
5. [姓]フィールドに、この IP Phone のユーザの姓を入力します。
6. [名]フィールドに、この IP Phone のユーザの名を入力します。
7. [ユーザID]フィールドに、この電話ユーザのユーザ ID を入力します。ユーザが電話の設定を変更するときには、このパラメータを使用します。
8. （オプション）[パスワード]フィールドに、この IP Phone に対して設定するユーザ ID のパスワードを入力します。このパラメータは、電話ユーザがこの IP Phone にログインして電話の設定を変更するときに使用します。パスワード フィールドは、Cisco Unity Express の GUI およびインターネット メッセージ アクセス プロトコル（IMAP; Internet Message Access Protocol）にのみ適用されます。SCCP 電話の場合、このフィールドは CME（Cisco Unified Communications Manager Express）の GUI にも適用されます。
9. その他の設定を変更するには、[詳細]をクリックして、[詳細]ウィンドウを使用します。

外部ファイルから電話またはユーザのデータをインポートするには、[インポート]をクリックして、電話とユーザのデータが入った外部ファイルを選択します。注:外部ファイルからのユーザ パラメータのバルク インポートを実行するには、あらかじめ[音声システムの機能]タブを設定しておく必要があります。

IP Phone を削除するには、次の手順に従います。

1. デバイスから IP Phone を取り外します。
2. ウィンドウで、削除する電話を選択します。
3. [削除]ボタンをクリックすると、電話が削除されます。

UC500、Cisco 800シリーズルータを管理する場合

[音声]ウィンドウ

[自動音声応答とボイスメール]タブで、[アップロード]**設定 > テレフォニー > 音声** の順にクリックすると、このウィンドウが表示されます。

ボイス プロンプト ファイルをアップロードするには、[プロンプトファイル名]フィールドにプロンプト ファイルのフル パスとファイル名を入力するか、[参照]をクリックしてファイルを選択します。

UC500、Cisco 800シリーズルータを管理する場合

[音声]ウィンドウ

[ホスト名]リストから、音声を設定するデバイスを選択します。

設定する機能のチェック ボックスをオンにします。

- [ファイルから読み取る]。テンプレート ファイルからパラメータをロードします。
- [デバイス]。ホスト名、時刻、ロケールなどのデバイス パラメータを設定します。
- [システム]。ローカル設定を行います。
- [ネットワーク]。VLAN 番号や DHCP プール情報などのネットワーク パラメータを設定します。
- [自動音声応答とボイスメール]。自動音声応答に使用する内線番号と、ボイス メール パラメータを設定します。
- [SIPトランク]。サービス プロバイダ、ドメイン名などの SIP トランク パラメータを設定します。
- [音声機能]。一斉同報 グループ、ハント グループ、緊急番号などのグループ機能を設定します。
- [ダイヤルプラン]。発信コール処理を設定します。
- [ユーザ]。MAC アドレス、内線番号、ユーザ名などのユーザ パラメータを設定します。

設定テンプレートをインポートするには、[テンプレートのインポート]をクリックします。

ハードウェア デバイスの設定が検出され、表示されます。アプリケーションでは、修正可能な設定パラメータが、ルータのハードウェア設定に基づいて制限されます。

通話処理を PBX の通話処理と同じようにするか、それともキーシステムの通話処理と同じようにするかを設定するには、[PBX]オプション ボタンまたは[キーシステム]オプション ボタンをクリックします。
注意:このパラメータは初期設定の際にのみ使用できます。このパラメータを設定すると、このフィールドは読み取り専用となります。

公衆電話交換網(PSTN)を設定するには、次の手順に従います。

1. 接続タイプを選択するには、[音声システムのタイプ]オプション ボタンをクリックします。このパラメータは初期設定の際にのみ使用できます。このパラメータを設定すると、このフィールドは読み取り専用となります。デバイスに T1/E1 ボイス ポートが内蔵されている場合には、T1/E1 オプションが表示されます。(VIC スロットに取り付ける T1/E1 ボイス カードはサポートされません。)
2. ボイス ポート アダプタを設定するには、[チャネルシグナリング]メニューでチャネル シグナリング タイプを選択します。
    - [チャネルシグナリング]メニューから[ISDN PRI]を選択した場合は、次の手順に従います。
        1. [スイッチタイプ]メニューで、設定するスイッチのタイプを選択します。このパラメータを使用して、グローバル ISDN スイッチのタイプおよびインターフェイスレベルのスイッチのタイプを指定します。
        2. [PRIグループのタイムスロット]フィールドで、ISDN PRI グループのタイムスロットの範囲を指定します。デフォルトの T1 の範囲は、1 タイム スロットから 24 タイム スロットです。タイム スロット 24(D チャネル)は常に含まれます。タイム スロット 24 からタイム スロット 24 の範囲は無効です。デフォルトの E1 の範囲は、1 タイム スロットから 31 タイム スロットです。タイム スロット 16(D チャネル)は常に含まれます。タイム スロット 16 からタイム スロット 16 の範囲は無効です。
    - [チャネルシグナリング]メニューから[FXO]、[FXS]、または[E&M]を選択した場合には、次の手順に従います。
        1. [シグナル]メニューからシグナリングのタイプを選択します。
        2. 着信および発信コールに個別のタイム スロットを使用するには、[発信と受信には異なるグループを使用]チェックボックスをオンにします。
        3. [グループのタイムスロット]フィールドに、タイム スロットの範囲を入力します。[発信と受信には異なるグループを使用]チェックボックスをオンにした場合には、[着信グループのタイムスロット]フィールドに着信タイム スロットの範囲を、[発信グループのタイムスロット]フィールドに発信タイム スロットの範囲を入力します。デフォルトの T1 の範囲は、1 タイム スロットから 24 タイム スロットです。タイム スロット 24(D チャネル)は常に含まれます。タイム スロット 24 からタイム スロット 24 の範囲は無効です。デフォルトの E1 の範囲は、1 タイム スロットから 31 タイム スロットです。タイム スロット 16(D チャネル)は常に含まれます。タイム スロット 16 からタイム スロット 16 の範囲は無効です。
    - [チャネルシグナリング]メニューから[FGD]を選択した場合は、次の手順に従います。

1. シグナリングのタイプを選択するには、[EANA]または[OS]（オペレータのサービス）をクリックします。
2. 着信および発信コールに個別のタイム スロットを使用するには、[発信と受信には異なるグループを使用]チェックボックスをオンにします。
3. [グループのタイムスロット]フィールドに、タイム スロットの範囲を入力します。[発信と受信には異なるグループを使用]チェックボックスをオンにした場合には、[着信グループのタイムスロット]フィールドに着信タイム スロットの範囲を、[発信グループのタイムスロット]フィールドに発信タイム スロットの範囲を入力します。

- [チャネルシグナリング]メニューから[R2]を選択した場合は、次の手順に従います。
  1. シグナリングのタイプを選択するには、次のいずれかをクリックします。
     - [アナログ]：R2 回線のシグナリングのタイプ ITU-U Q.411 です。通常、キャリア システムに使用されます（Tone/A ビットが使用されている場合）。
     - [デジタル]：R2 回線のシグナリングのタイプ ITU-U Q0.421 です。通常、PCM システムに使用されます（A および B ビットが使用されている場合）。
     - [パルス]：R2 回線のシグナリングのタイプ ITU-U Supplement 7 です。通常、衛星リンクを展開するシステムに使用されます（Tone/A ビットがパルス化されている場合）。
  2. 着信および発信コールに個別のタイム スロットを使用するには、[発信と受信には異なるグループを使用]チェックボックスをオンにします。
  3. [タイムスロット]フィールドに、タイム スロットの範囲を入力します。または、[発信と受信には異なるグループを使用]チェックボックスをオンにした場合には、[着信グループのタイムスロット]フィールドに着信タイム スロットの範囲を、[発信グループのタイムスロット]フィールドに発信タイム スロットの範囲を入力します。デフォルトの E1 の範囲は、1 タイム スロットから 31 タイム スロットです。タイム スロット 16（D チャネル）は常に含まれます。タイム スロット 16 からタイム スロット 16 の範囲は無効です。

FXS/DID（VIC 専用）を設定するには、次の手順に従います。

1. [モード]メニューから、[FXS]モードまたは[DID]モードを選択します。
2. [シグナル]メニューから、FSX モードのポートには[ループスタート]または[グラウンドスタート]を、DID モードのポートには[遅延ダイヤル]、[即時スタート]、または[ウィンクスタート]を選択します。
3. [発信者ID]フィールドに、着信先の電話に表示される発信者 ID を入力します。
4. [内線番号]フィールドに、内線番号を入力します。
5. [権限]フィールドに、権限を入力します。
6. [ブロック制限番号]チェックボックスをオンにして、制限された番号をブロックします。

注：8 ユーザ システムまたは 16 ユーザ システムに VIC が存在する場合、アドホック会議の参加者は 3 名までに制限されます。4 名以上の参加者をサポートできるだけのデジタル シグナル プロセッサ（DSP）を用意できないことがあるためです。

ISDN PRI が PBX モードに設定されている場合、ボイス ポートのダイヤル ピアが自動的にルータ上で設定されます。キーシステム モードを選択した場合には、ダイヤル ピアは設定されません。

注：UC520 VIC スロットに VIC-FXS または VIC-FXS/DID が取り付けられている場合には、Configuration Assistant により 0/2/0、0/2/1、0/2/2、および 0/2/3 のポートにそれぞれ 1100、1101、1102、および 1103 のダイヤルピア タグ番号が予約されます。アウトオブバンドで、2500 から 2999 までのユーザ定義のダイアル ピア タグを設定できます。

ISDN PRI が存在して選択されており、さらに BRI インターフェイスが 1 つ以上存在する場合、BRI スイッチのタイプを設定する必要があります。[スイッチタイプ]パラメータを使用して BRI インターフェイス上の ISDN スイッチのタイプを設定し、競合を避けます。

デバイスに 1 つまたは複数の BRI ボイス ポートが内蔵されている場合には、BRI オプションが表示されます。スイッチのタイプを設定するには、[スイッチタイプ]メニューからスイッチのタイプを選択します。

ローカル設定を行うには、次の手順に従います。

1. [地域]メニューから、Cisco Unified Communications Manager Express の地域を選択します。それによって、電話のトーンと鳴り方が設定されます。
2. [電話の言語]メニューから、ユーザの電話に表示される言語を選択します。
3. [ボイスメールの言語]メニューから、ボイスメールのユーザに聞かせるボイス メール プロンプトの言語を選択します。言語パックをインストールするには、次の手順に従います。
    1. Cisco Unified Communications Manager Express の、必要な言語の tar ファイルをダウンロードします。
    2. Cisco Unity Express の、必要な言語のパッケージ ファイルをダウンロードします。
    3. [言語ファイルの場所]フィールドに表示されているフォルダにファイルをコピーします。
    4. [適用]をクリックします。
4. [日付書式]メニューから、日付形式を選択します。
5. [時間制]メニューから、時刻形式を選択します。
6. オプション：[システムメッセージ]フィールドに、システム メッセージを入力します。

注：ロケール、時間帯、または日付形式のパラメータを変更すると、IP Phone はリブートします。

市内の短縮ダイヤル メニューをすべての電話、Skinny Call Control Protocol（SCCP）および SIP に対して有効にするには、次の手順を実行します。

1. [追加]をクリックします。
2. [名前]フィールドに、短縮ダイヤルの名前を入力します。
3. [電話番号]フィールドに、短縮ダイヤルの番号を入力します。

リストの市内短縮ダイヤル番号を並べ替えるには、エントリを選択して、上下の矢印をクリックします。これによって、エントリが電話に表示される順序が示されます。

メニューから市内短縮ダイヤル番号を削除するには、メニューでエントリを選択して[システムスピードダイヤル]ボックスで[削除]をクリックします。

リストのエントリが許可された最大数に達した場合には、[追加]ボタンが無効になります。

ネットワーク パラメータを設定するには、次の手順に従います。

1. [VLAN番号]メニューから、音声ネットワークのサブインターフェイス番号を選択します。選択値の範囲は、1 から 1001 です。音声 VLAN は、デフォルトでは VLAN 100 です。別の音声 VLAN を設定するには、次の手順に従います。
    - [設定]>[VLAN]の順に選択して、新しい VLAN を作成します。
    - [音声]画面をリフレッシュして、新しい VLAN を読み込みます。ドロップダウン メニューに新しい VLAN が表示されます。
    - スマート ポートを使用し、各スイッチ ポートから新しい音声 VLAN に接続できるように設定します。
2. [DHCP IPアドレスプール]フィールドと[サブネットマスク]フィールドに、IP アドレスと、サブネット マスクの範囲内の最初の IP アドレスを入力します。このパラメータを変更すると、IP Phone はリブートします。
3. [除外対象アドレス]フィールドに、音声ネットワークの DHCP アドレス指定から除外する IP アドレスの範囲を入力します。
4. [CME IPアドレス]フィールドと[サブネットマスク]フィールドに、設定するルータの Cisco Unified Communications Manager Express(CME)IP アドレスとサブネット マスクを入力します。この IP アドレスとサブネット マスクは、DHCP による割り当てから除外されます。

自動音声応答(AA)パラメータを設定するには、次の手順に従います。

1. [自動音声応答の内線番号]フィールドに、企業向けの一般的な自動音声応答機能を使用する内線番号を入力します。これは通常、オフィスの代表電話の内線番号です。発信者がこの内線番号をダイヤルすると、自動音声応答スクリプトが稼動します。
2. [自動音声応答のPSTN番号]フィールドに、企業向けの一般的な自動音声応答機能を使用する PSTN 番号を入力します。
3. [自動音声応答スクリプト]メニューから、トリガー イベントが発生する際に実行するスクリプトを選択します。デフォルトのスクリプト以外のスクリプトを選択すると、次のスクリプト パラメータを設定できます。
    - [メニュープロンプト]:自動音声応答を起動すると再生される WAV ファイル。現在の WAV ファイルがフィールドに表示されます。別の WAV ファイルを選択するには、[参照]をクリックして[プロンプトファイルのアップロード]ウィンドウを使用します。
    - [オプション *n*](この場合 *n* はユーザがダイヤルしたオプションの番号):プライマリ ユーザ内線番号のリストを表示します。各リストから内線番号を選択するか、フィールドに内線番号を入力します。自動音声応答をキーシステム モードで設定している場合、メニューには各交換局の回線とすべての交換局の回線を呼び出すオプションのリストが表示されます。

ボイスメール パラメータを設定するには、次の手順に従います。

1. [ボイスメールの内線番号]フィールドに、着信に対する応答メッセージを流す電話機の内線番号を入力します。これは、着信コールに完全自動対応するフロント エンドの電話機に使用する内線番号です。
2. [ボイスメールのPSTN番号]フィールドに、着信に対する応答メッセージを流す PSTN 番号を入力します。

キーシステム通話処理では、SIP トランクをサポートしていません。

SIP トランク パラメータを設定するには、次の手順に従います。

1. [サービス プロバイダ]メニューで、このルータから PSTN にアクセスするときに接続する SIP トランク サービス プロバイダを選択します。このルータから SIP トランクに接続しない場合は、[なし]を選択し、残りの手順は省略します。
2. オプション:[レジストラサーバ]フィールドに、プライマリ SIP レジストラ サーバの IP アドレスを入力します。
3. [プロキシサーバ]フィールドに、外部 SIP レジストラ サーバの IP アドレスを入力します。
4. オプション:[MWIサーバ]フィールドに、外部の SIP ベース MWI サーバの IP アドレスを入力します。
5. オプション:ダイジェスト認証の[ユーザ名]フィールドに、SIP 電話登録の認証クレデンシャルとして使用する名前を入力します。この名前は 一語にする必要があります。また、疑問符やスペースを含むことはできません。
6. オプション:ダイジェスト認証の[パスワード]フィールドに、このユーザ名のパスワードを入力します。パスワードの長さは 1 から 25 文字にする必要があります。スペースを含めることもできます。
7. オプション:ドメイン ネーム サービスの[SIPドメイン名]フィールドに、プライマリ SIP レジストラ サーバの DNS 名を入力します。
8. オプション:ドメイン ネーム サービスの[DNSサーバアドレス]フィールドに、プライマリ SIP レジストラ サーバの DNS アドレスを入力します。

注: 通話処理をキーシステムとして設定した場合、一斉同報とインターコムのみ設定できます。

保留音を設定するには、[保留音]メニューから音楽を選択します。

一斉同報のパラメータを設定するには、次の手順に従います。

1. [有効にする]チェックボックスをオンにします。
2. [一斉同報グループ数]メニューから、設定する一斉同報 グループの数を選択します。
3. [一斉同報グループの内線番号]フィールドに、設定する各一斉同報 グループの内線番号を入力します。

グループ ピックアップ パラメータを設定するには、[有効にする]チェックボックスをオンにして、[ピックアップグループ数]メニューからピックアップ グループ数を選択します。

発信者 ID ブロック コードを設定するには、次の手順に従います。

1. [有効にする]チェックボックスをオンにし、[発信者IDブロックコード]フィールドにブロック コードを入力します。
2. 発信者の ID コードを入力します。発信者 ID ブロック コードは、電話のユーザが電話をかける前にダイヤルすることができる 4 桁のコードです。呼び出される側の電話に自分の番号を表示させたくない場合、ユーザはこのコードをダイヤルしてから、電話をかけます。発信者 ID は送信されますが、その表示パラメータは「制限」に設定されているので、発信者 ID は表示されません。このコードはアスタリスク(*)と 3 桁の数字で構成されます。最初の文字はアスタリスク(*)にする必要があります。使用可能な番号の範囲は 000 から 999 です。
3. [追加]をクリックします。

発信ブロック番号リストを設定するには、次の手順に従います。

1. ［発信ブロック番号リスト］フィールドに、ブロックする番号を入力します。コール ブロッキングは、ダイヤルされた番号を、指定した桁数のパターンと照合して、電話の不正使用を防止します。コール ブロッキングは、IP 電話でのみサポートされ、アナログ FXS 電話ではサポートされていません。ユーザが、コール ブロッキングに指定したパターンで照合する桁数を呼び出そうとすると、高速の話中音が約 10 秒間聞こえます。その時点で呼び出しは終了し、回線は受話器が下ろされた状態に戻ります。
    - 特定のパターンで始まるすべての番号をブロックするには、その番号のパターンを入力します。たとえば、5550000 から 5559999 までの番号をブロックするには、「555」と入力します。このパターンを含む番号のうち、このパターンで始まっていない番号はブロックされません。たとえば、15550000411 はブロックされません。
    - 市外局番や国コードを含む長距離番号をブロックするには、その長距離ダイヤル コードも一緒に入力します。たとえば、900 の市外局番を持つ番号をブロックするには、「1900」と入力します。
    - 411 のような特殊な市内電話番号をブロックするには、その番号を入力します。パターンは、最初の桁で照合されます。番号にパターンが含まれていても、たとえば 15555550411 はブロックされません。
2. ［追加］をクリックします。

リストから**発信コール ブロック**の番号を削除するには、リストから削除する番号を選択して［削除］をクリックします。

インターコムを有効にして、プッシュ ツー トーク インターコム回線を使用して IP Phone 同士で対話できるようにするには、［インターコムを有効にする］チェックボックスをオンにします。

ハント グループ パラメータを設定し、順次選択またはラウンドロビン選択を使用して IP Phone グループ内でコールを分配するには、次の手順に従います。

1. ［ハントグループ数］メニューで、［有効にする］チェックボックスをオンにします。
2. ［ハントグループ数］メニューから、ハント グループ数を選択します。
3. ［ハントのタイムアウト］フィールドに、まだ応答を受けていないコールをボイス ハント グループ リストの次の番号にリダイレクトするまでの秒数を入力します。入力値の範囲は、5 から 20 です。
4. ［パイロット］フィールドに、設定する各ハント グループの番号を入力します。これは、ハント グループの最初の内線番号と、発信者がボイス ハント グループに接続するためにダイヤルする内線番号です。
5. メニューから［ハントタイプ］を選択します。設定する各ハント グループのタイプを選択します。
    - ［順次］：コール ハントは常にグループのパイロット番号から開始され、その後、グループ内の各番号に対して、リストされている順（左から右）に続けられます。
    - ［最長のアイドル時間］：コールは、その内線番号での最後の応答時刻に基づき、最も長い間アイドル状態になっていると判断されたディレクトリ番号に送信されます。その内線番号が使用不可の場合は、検索が続行され、グループ内の次の内線番号が検出されます。
    - ［ピア］：このタイプのハント グループでは、最初に呼び出す番号がリストからラウンドロビン方式で選択されます。
6. ［VMに転送］チェックボックスでは、未応答のコールを、最初に呼び出した内線番号のボイス メールボックスに、ボイス ハント グループから転送するかどうかを設定します。

パーク スロット数を設定するには、次の手順に従います。

1. [有効にする]チェックボックスをオンにします。
2. [パークスロット数]メニューから、設定するパーク スロット数を選択します。
3. [パークスロットの内線番号]フィールドに、各パーク スロットの番号を入力します。この機能では、着信コールの一時的な保管場所が確保されます。コールがパークされると、コールはパーク スロット番号に転送され、パークされたコールのパーク スロット番号で呼び出された別の従業員がその電話に応答するまで保留状態に置かれます。

アドホック会議を設定するには、次の手順に従います。

1. [参加者]メニューから、許可する参加者の最大数を選択します。
2. 混在モード(ハードウェアベースのアドホック会議)を有効にするには、[混在モード]チェックボックスをオンにします。このチェックボックスをオフにすると、デバイスは、シングル モードのアドホック会議用に設定されます。

[セッション]メニューには、許可するセッションの最大数が表示されます。許可するセッションの最大数は、選択した参加者数および使用するデバイスの制約に応じて変わります。このパラメータは設定できません。

注:

シングル モード(G711 コーデックを持つ参加者のみ)では、最大 3 名の参加者を設定できます。4 名以上の参加者を選択した場合、フリーの DSP リソースを備えたハードウェアベースのアドホック会議が必要になります。ハードウェアベースのアドホック会議は、シングル モードでも混在モード(G711 コーデックおよび G729 コーデックを持つ参加者)でも設定できます。

8 ユーザ システムまたは 16 ユーザ システムを VIC で設定している場合、ハードウェアベースのアドホック会議が VIC カードを CCA から設定する前にデバイス上で設定済みであれば、アドホック会議をソフトウェアベースの会議に戻す必要があります。それには、3 名の参加者を選択して[適用]をクリックします。トランスコーディングなどの DSP 関連の設定が、アウトオブバンドで任意のシステムで実行された場合、アドホック会議は使用できません。アウトオブバンドのアドホック会議を作成するか、アウトオブバンド用に修正する必要があります。

システムの内線番号を設定するには、[内線番号の桁数]フィールドに、その場所の内線番号の桁数を入力します。

注:通話処理をキーシステムとして設定した場合、国際ダイヤル プランや国内ダイヤル プランは設定できません。

発信コール処理を設定するには、次の手順に従います。

1. オプション ボタンを使用して、[発信コール処理 番号計画のロケール]を選択します。
2. [市外局番の桁数]フィールドに、ルータの設置場所の国の市外局番の長さを入力します。長さが一定でない場合、このフィールドは空白のままにします。入力値の範囲は、1 から 10 です。
3. [市内番号の桁数]フィールドに、市内通話地域内の電話番号の長さを入力します。長さが一定でない場合、このフィールドは空白のままにします。入力値の範囲は、0 から 99 です。

4. [長距離電話発信番号]フィールドに、市内通話地域外の電話を呼び出す場合に(国内長距離呼び出し)、電話のユーザが(必要に応じて)発信コールのダイアル トーン番号を押した後に押す必要がある数字列を入力します。数字列の長さは 1 から 7 文字で、使用可能な数字は 0 から 9 です。米国の場合、デフォルトは 1 です。ダイヤル トーン番号は、電話のユーザが PSTN 接続にアクセスするときに押す必要がある数字です。
5. [国際電話発信番号]フィールドに、ルータが設置された国以外の電話を呼び出す場合に、ユーザが押す必要がある数字列を入力します。数字列の長さは 1 から 7 文字で、使用可能な数字は 0 から 9 です。米国内から米国外への通話の場合、デフォルトは 011 です。
6. [外線発信番号]フィールドに、発信コールのダイヤル番号を入力します。

緊急番号を設定するには、[緊急電話番号]フィールドに緊急番号を入力します。北米のダイヤル プランでは、通常、緊急番号は 911 のように 3 桁です。ただし、10 桁の緊急番号も使用できます。10 桁の番号には、長距離のダイヤル コードを 10 桁の番号に追加する必要があります。たとえば、緊急番号として 408 522 4000 を使用したい場合には、「14085264000」と入力します。

個々のポートにカスタム設定を作成する場合には、[設定]をクリックして、[カスタムFXOポート]ウィンドウを使用します。

着信コール処理を設定するには、次の手順に従います。

1. [FXOトランク]メニューで、FXO ポート用の着信コールの宛先を選択します。
2. ダイヤルインの[設定]をクリックし、[DID設定]ウィンドウで 1 つの着信トランクの DID および柔軟な内線番号計画を持った各着信トランクのカスタム DID を指定します。

電話をデータベースに追加するには、次の手順に従います。

1. データベースにエントリを作成するには、[新規]をクリックします。
2. SIP 電話の場合、自動登録はサポートされていません。[MACアドレス]フィールドに、設定する各 IP Phone の MAC アドレスを入力します。
3. [電話タイプ]メニューから、設定する各 IP Phone の電話タイプを選択します。
4. [プライマリ内線番号]フィールドに、この IP Phone の内線番号を入力します。この内線番号には、実際の電話番号、この IP Phone 番号に割り当てられた内線番号、または Message Waiting Indication(MWI; メッセージ ウェイティング インジケータ)などの特別な機能の仮想電話番号を指定できます。
5. [姓]フィールドに、この IP Phone のユーザの姓を入力します。
6. [名]フィールドに、この IP Phone のユーザの名を入力します。
7. [ユーザID]フィールドに、この電話ユーザのユーザ ID を入力します。ユーザが電話の設定を変更するときには、このパラメータを使用します。
8. (オプション)[パスワード]フィールドに、この IP Phone に対して設定するユーザ ID のパスワードを入力します。このパラメータは、電話ユーザがこの IP Phone にログインして電話の設定を変更するときに使用します。パスワード フィールドは、Cisco Unity Express の GUI およびインターネット メッセージ アクセス プロトコル(IMAP; Internet Message Access Protocol)にのみ適用されます。SCCP 電話の場合、このフィールドは CME(Cisco Unified Communications Manager Express)の GUI にも適用されます。
9. その他の設定を変更するには、[詳細]をクリックして、[詳細]ウィンドウを使用します。

外部ファイルから電話またはユーザのデータをインポートするには、[インポート]をクリックして、電話とユーザのデータが入った外部ファイルを選択します。注:ユーザ パラメータを外部ファイルから一括インポートするには、あらかじめ[音声システムの機能]タブを設定しておく必要があります。

IP Phone を削除するには、次の手順に従います。

1. デバイスから IP Phone を取り外します。
2. ウィンドウで、削除する電話を選択します。
3. [削除]ボタンをクリックすると、電話が削除されます。

[終了]をクリックして、デバイスにパラメータをロードします。

[環境設定]ウィンドウ

このウィンドウは、次のいずれかの処理を実行した場合に表示されます。

- メニューバー上で **アプリケーション > 環境設定** を選択する。
- ツールバー上で  を選択する。

このウィンドウには、次のタブがあります。

- [全般]。ポーリングおよび起動に関する環境設定を選択します。
- [アプリケーション更新]。新規更新の検索頻度を Configuration Assistant に指定します。
- [プロキシサーバ]。Cisco.com およびネットワークとの通信にプロキシ サーバを使用します。
- [設定の保存]。デバイス上の保存済み設定のバックアップに関する環境設定を設定します。
- [状態]。スタンドアロン デバイスまたはコミュニティの状態の監視に使用するカテゴリを選択します。

次に、これらのタブで設定する環境設定の説明とデフォルト値を示します。デフォルト値を変更した場合は、[デフォルトに設定]をクリックすると元に戻すことができます。

[全般]

次の環境設定を設定できます。

[ネットワークポーリング間隔]。Configuration Assistant が管理対象デバイスのステータスと新しいメンバの存在を確認するために管理対象デバイスをポーリングする頻度を指定します。このポーリング情報は、[トポロジ]ビュー、[前面パネル]ビュー、および多くの機能ウィンドウのリフレッシュに使用されます。デフォルトは 5 分です。

[LEDポーリング間隔]。Configuration Assistant が管理対象デバイスの LED をポーリングする頻度を指定します。ポーリングごとに、[前面パネル]ビューにインターフェイスと RPS の情報が LED の色と共に表示されます。ビューの左側にあるボタンをクリックすると、それぞれの色が示す情報の種類(リンクのステータス、ポートの速度、デュプレックスの状態、または電源の状態)を選択できます。デフォルトは 3 分です。

[グラフポーリング間隔]。Configuration Assistant がデバイス利用率データおよびリンク利用率データを取得するためのクエリを管理対象デバイスに実行する頻度を指定します。この情報は、リンクおよび帯域幅のグラフの更新に使用されます。デフォルトは 5 秒です。

[ネットワーク接続時にトポロジビューを表示する]。Configuration Assistant がデバイスに接続されたときに、[トポロジ]ビューを表示するかどうかを指定します。デフォルトはオンです。

[ネットワーク接続時に前面パネルビューを表示する]。Configuration Assistant がデバイスに接続されたときに、[前面パネル]ビューを表示するかどうかを指定します。デフォルトはオフです。

[アプリケーション更新]

[アプリケーション更新の確認頻度]リストで、[毎月]、[毎週]、または[しない]を選択します。[しない]を選択した場合、Configuration Assistant では定期確認は実行されません。ただし、メニュー バーの **アプリケーション > アプリケーション更新** を選択すれば、必要なときに確認を実行できます。

[プロキシサーバ]

このタブでは、次の通信にプロキシ サーバを使用するかどうかを指定します。

- インターネットとの通信（特に、Configuration Assistant の更新に使用する Cisco.com）
- ネットワークとの通信

次の手順に従います。

1. プロキシ サーバ経由の通信を有効にするには、[プロキシサーバを有効にする]をオンにします。このチェックボックスをオンにすると、タブ内の他のフィールドが使用できるようになります。
2. プロキシ サーバ経由でネットワークと通信するには、[プロキシサーバを使用してデバイスを管理する]をオンにします。
3. HTTP トラフィックでプロキシ サーバを使用するよう指定するには、次の値を[HTTP]フィールドに入力します。
    - プロキシ サーバの IP アドレスまたはホスト名
    - HTTP ポートの番号
4. HTTPS トラフィックでプロキシ サーバを使用するよう指定する場合は、適切な値を[HTTPS]フィールドに入力します。

注:プロキシ サーバの識別にホスト名を使用できるのは、DNS サーバがホスト名を解決するよう設定されている場合だけです。

[設定の保存]

次の手順に従います。

1. Configuration Assistant を使用してデバイスに実行中の設定を保存してから、それを保存済み設定としてバックアップするには、[バックアップ前にデバイスの設定を保存する]をオンにします。
2. 設定を別のパスにバックアップする場合は、[バックアップディレクトリ]フィールドで、設定のバックアップに使用されるパスを置き換えます。

[状態]

Configuration Assistant で監視する状態のカテゴリに対応するチェックボックスをオンにします。

[状態ポーリング間隔]を設定して、[状態]ウィンドウおよび[状態の詳細]ウィンドウの測定値の更新頻度を指定します。

CE520 スイッチを管理する場合

[基本的なポートの説明]ウィンドウ

このウィンドウは、[ポート設定]ウィンドウで 1 つのポートを選択して、[説明の記入]をクリックした場合に表示されます。

[ポート設定]ウィンドウにポートの説明を追加するには、次の手順に従います。

1. [説明]フィールドに、テキストの説明を入力します。
2. [OK]をクリックします。

CE520 スイッチを管理する場合

[検索]ウィンドウ

このウィンドウを使用して、ポートに関連付けられたキーワードやフレーズを持つポートを検索します。また、指定したデバイスの IP アドレスや MAC アドレスを入力して、特定のデバイスに接続されたデバイスを検索することもできます。

次の手順に従います。

1. [ポートの検索(キー: 説明/IPアドレス/MACアドレス)]フィールドに、キーワードやフレーズ、MAC アドレスや IP アドレスを入力します。入力内容は、コミュニティまたはクラスタ内のすべてのデバイスに対して照合されます。

   注: 入力する MAC アドレスの形式は、**xxxx.xxxx.xxxx.xxxx** または **xx:xx:xx:xx:xx:xx** です。この場合、x は 16 進文字(0 から 9、a から f、A から F)です。

2. [検索]をクリックします。

ポートの説明を[検索]フィールドに入力した場合、その説明と一致するポートが[検索結果]領域に表示されます。この情報は、次のようにテーブルに表示されます。

カラム	説明
ポート	説明と一致するポートのデバイス名およびポート番号。
説明	ポートの説明。

注：[検索]フィールドに何も入力しないで[検索]をクリックすると、Configuration Assistant には WLAN コントローラとそのポートを除くすべてのコミュニティ メンバのリストが表示されます。

[検索]フィールドに IP アドレスまたは MAC アドレスを入力した場合、この情報が次のようにテーブルに表示されます。

カラム	説明
ホスト	[検索]フィールドに入力された IP アドレスまたは Mac アドレスを持つデバイスの名前。
MAC アドレス	デバイスの MAC アドレス。
IP アドレス	デバイスの IP アドレス。
説明	デバイスのタイプ。

このウィンドウでの操作が完了したら、[OK]をクリックします。

[コミュニティ]ウィンドウ

このウィンドウは、メニュー バーで **アプリケーション > コミュニティ** を選択した場合に表示されます。

このウィンドウを使用すると、既存のコミュニティのリストの表示、コミュニティの作成、コミュニティの変更、およびコミュニティの削除を実行できます。

コミュニティを作成するには、[作成]をクリックします。次に、[コミュニティの作成]ウィンドウを使用します。

コミュニティを変更するには、リストからコミュニティを選択して[修正]をクリックします。次に、[コミュニティの修正]ウィンドウを使用します。

コミュニティを削除するには、リストから削除するコミュニティを選択し、[削除]をクリックします。

このウィンドウでの作業が完了したら、[OK]をクリックします。

[コミュニティ詳細設定]ウィンドウ

このウィンドウは、[コミュニティの作成]ウィンドウまたは[コミュニティの修正]ウィンドウで[詳細]をクリックした場合に表示されます。

[HTTPポート]フィールドは、コミュニティの作成時にだけ変更できます。このフィールドには、Configuration Assistant がコミュニティ内のデバイスとの通信に使用する HTTP ポートの番号を入力する必要があります。

デフォルトの 80 以外の HTTP ポート番号を入力する場合は、その番号を入力してからコミュニティにデバイスを追加してください。後にポート番号を変更するには、**設定 > デバイスプロパティ > HTTP ポート** を選択して、[HTTPポート]ウィンドウを使用します。

HTTPS 接続に使用するポート番号は変更できません。このポートは 443 である必要があります。HTTPS を使用する場合の要件については、「HTTPS の使用」を参照してください。

注：Configuration Assistant はまず HTTPS を使用してデバイスへの接続を試行します。これに失敗すると、HTTP を使用した接続を試行します。

コミュニティを作成する場合だけ、アクセス モードと特権レベルを選択できます。選択した設定は、デバイスを検出したり、コミュニティに初めて接続したりするときに使用されます。

ウィンドウでの作業が完了したら、[OK]をクリックします。

[コミュニティ制限]ウィンドウ

このウィンドウは、次のいずれかのイベントが発生した場合に表示されます。

- デバイス数がコミュニティの制限値である 25 を超過した。
- 特定のデバイス タイプのデバイス数がそのタイプに設定されている制限値を超過した。

[カウント]カラムは、コミュニティ内のデバイス数およびデバイス タイプ別のデバイス数を示します。[制限]カラムは、コミュニティのデバイスの制限数、およびデバイス タイプ別のデバイスの制限数を示します。[カウント]カラムの数値は、対応する[制限]カラムの制限値を超過している場合、赤い縁取りで表示されます。

コミュニティを管理するには、すべての数値が制限範囲内になるまでデバイスを削除する必要があります。デバイスを削除するには、次の手順に従います。

1. 削除するデバイスが属するデバイス タイプのフォルダを展開します。
2. 展開したフォルダからデバイスを選択します。
3. [削除]をクリックします。

完了したら、[OK]をクリックします。

[コミュニティの作成]ウィンドウ

このウィンドウは、次の場合に表示されます。

- ［コミュニティ］ウィンドウで［作成］をクリックしたとき
- ［接続］ウィンドウで、［新しいコミュニティに接続する］をクリックして［接続］をクリックしたとき

このウィンドウを使用すると、デバイスを検出して、それをコミュニティに追加できます。

次の手順に従います。

1. ［名前］フィールドに、コミュニティの名前を入力します。名前には最大 64 文字の英数字を使用できます。

   使用できる文字は、A から Z、a から z、0 から 9、-（ハイフン）、および _（アンダースコア）です。

2. オプション：次の場合は、［詳細］クリックします。

   - HTTP ポート番号を入力する（コミュニティ内のデバイスでデフォルトのポート番号 80 が使用されてない場合）。
   - デバイスを検出したり、コミュニティに初めて接続したりするためのアクセスモードを指定する。アクセス モードが**読み取り専用**であるコミュニティにすでに接続している場合のデフォルトは、**読み取り専用**です。それ以外の場合のデフォルトは、**読み書き**です。

3. オプション：［会社名］フィールドに、会社名、組織名、またはその他の識別用のテキストを入力します。ネットワークの SSID を作成する際、このテキストが、推奨される SSID（サービス セット ID）の一部として表示されます。

4. ［検索］リストからオプションを選択します。リストの下のフィールドに必要な情報を入力し、［スタート］をクリックします。

   次の表は、［検索］リスト内のオプション、リストの下のフィールドに入力する情報、および Configuration Assistant によって［デバイス］テーブルに入力される情報を示しています。

オプション	入力する情報	Configuration Assistant によって入力される情報
［IPアドレスの指定］	Configuration Assistant を使用して検出するデバイスの IP アドレス	検出されたデバイスに関する情報
［起点IPアドレスを使用しているデバイス］	起点 IP アドレス（コミュニティに追加する、隣接デバイスを持つデバイスの IP アドレス）	指定したデバイスに関する情報および Cisco Discovery Protocol がホップ カウント 4 を使用して検出した隣接デバイスに関する情報
［サブネットのデバイス］	コミュニティに追加するデバイスが属するサブネットを識別する IP アドレスとサブネット マスク	サブネット上で検出されたデバイスに関する情報
［IPアドレス範囲にあるデバイス］	コミュニティに追加するデバイスの IP アドレス範囲を示す開始 IP アドレスと終了 IP アドレス	その IP アドレス範囲内で検出されたデバイスに関する情報

5. 検出が開始されると、[スタート]ボタンが[停止]ボタンに変わります。これをクリックすれば、いつでも検出処理を中断できます。

6. Configuration Assistant で、コミュニティに追加するデバイスが検出されない場合は、[検索]リストの別のオプションを使用して、手順 3 をもう一度実行します。

7. [デバイス]テーブルで、コミュニティに追加しないデバイスの行を見つけて、それらのチェックボックスをオフにします。1 つのコミュニティには最大 25 個のデバイスを選択できます。また、特定のデバイス タイプでは、コミュニティに追加できる数に制限があります。詳細については、「コミュニティに関する制限事項」を参照してください。

8. [OK]をクリックして選択したデバイスをコミュニティに追加し、ウィンドウを閉じます。

[コミュニティの修正]ウィンドウ

このウィンドウは、[コミュニティ]ウィンドウでコミュニティを選択し、[修正]をクリックした場合に表示されます。このウィンドウを使用すると、コミュニティにデバイスを追加したり、コミュニティからデバイスを削除したりできます。次の操作を行うこともできます。

- コミュニティ内のデバイスに使用する HTTP ポートを変更する場合に、[詳細]をクリックして新しい HTTP ポート番号を入力することができます。
- [会社名]フィールドで、会社名、組織名、またはその他の識別用のテキストを入力または修正することができます。ネットワークの SSID を作成する際、このテキストが、推奨される SSID（サービス セット ID）の一部として表示されます。

コミュニティにデバイスを追加するには、次の手順に従います。

1. [検索]リストからオプションを選択します。リストの下のフィールドに必要な情報を入力し、[開始] をクリックします。

   次の表は、[検索]リスト内のオプション、リストの下のフィールドに入力する情報、および Configuration Assistant によって[デバイス]テーブルに入力される情報を示しています。

オプション	入力する情報	Configuration Assistant によって入力される情報
[IPアドレスによる1つのデバイス]	Configuration Assistant を使用して検出するデバイスの IP アドレス	検出されたデバイスに関する情報
[起点IPアドレスを使用しているデバイス]	起点 IP アドレス（コミュニティに追加する、隣接デバイスを持つデバイスの IP アドレス）	指定したデバイスおよび検出された各隣接デバイスに関する情報
[サブネットのデバイス]	コミュニティに追加するデバイスが属するサブネットを識別する IP アドレスとサブネットマスク	サブネット上で検出されたデバイスに関する情報

[IPアドレス範囲のデバイス]	コミュニティに追加するデバイスの IP アドレス範囲を示す開始 IP アドレスと終了 IP アドレス	その IP アドレス範囲内で検出されたデバイスに関する情報

2. 検出が開始されると、[スタート]ボタンが[停止]ボタンに変わります。これをクリックすれば、いつでも検出処理を中断できます。

3. Configuration Assistant で、コミュニティに追加するデバイスが検出されない場合は、[検索]リストの別のオプションを使用して、手順 1 をもう一度実行します。

4. [デバイス]テーブルで、すでに追加されているデバイスのうち、コミュニティには追加しないデバイスの行を見つけて、それらのチェックボックスをオフにします。1 つのコミュニティには最大 25 個のデバイスを追加できます。また、特定のデバイス タイプでは、コミュニティに追加できる数に制限があります。詳細については、「コミュニティに関する制限事項」を参照してください。

コミュニティ内に既存のデバイスを削除するには、[デバイス]テーブルで削除するエントリのチェックボックスをオフにします。

[OK]をクリックして変更を保存し、ウィンドウを閉じます。

CE520 スイッチを管理する場合

[再起動/リセット]ウィンドウ

このウィンドウは、機能バーで **メンテナンス > 再起動/リセット** を選択した場合に表示されます。

このウィンドウを使用すると、1 つまたは複数のデバイスの再起動やリセットが可能です。再起動を選択すると、アクティブな設定が保存されデバイスが再起動されます。リセットを選択すると、アクティブな設定が削除され工場出荷時の設定がロードされます。

注：DHCP サーバによって、リセットしたデバイスに新しい IP アドレスが割り当てられる場合があります。この場合、デバイスが到達不能であることが[トポロジ]ビューに表示されます。新しい IP アドレスを使用して、コミュニティにデバイスを追加する必要があります。

次の表は、このウィンドウのカラムとオプションについて説明しています。

カラム	説明
デバイス	コミュニティ内のデバイスのホスト名
デバイスタイプ	コミュニティ内のデバイスのモデル名
再起動	再起動するデバイスのチェックボックスをオンにする
リセット	リセットするデバイスのチェックボックスをオンにする

ステータス	選択した各デバイスの再起動ステータスまたはリセット ステータスに関するメッセージ

ウィンドウでの操作が終了したら、[OK]をクリックします。

CE520 スイッチを管理する場合

[システム時間]ウィンドウ

このウィンドウは、機能バーで **設定 > デバイスプロパティ > システム時間** を選択した場合に表示されます。

このウィンドウを使用する目的は、次のとおりです。

- 現在の時刻の表示
- システムの時刻の設定

現在の時刻の表示

[システム時間]ウィンドウには、コミュニティ内のすべてのデバイスで使用する現在の時刻の、時(24 時間形式)、分、時間帯、月、日、および年が自動的に表示されます。

次に、この情報の表示形式の例を示します。

- 月、日、および年は、**August/2/2005** のように表示されます。
- 時、分は、**9:00**(午前 9 時)や **13:00**(午後 1 時)のように表示されます。
- 時間帯は、**(GMT -10:00) Hawaii** のように表示されます。これは、Greenwich Mean Time (GMT; グリニッジ標準時)より 10 時間遅れているという意味です。

システムの時刻の設定

このウィンドウを使用する目的は、次のとおりです。

- 1 つまたは複数のデバイスでの、時刻の手動設定または変更
- コミュニティ内のデバイス間での時刻の同期

デバイス上のシステムの時刻を手動で設定または変更するには、次の手順に従います。

1. デバイスの行を選択します。
2. 行のセル内で、ドロップダウン リストから月、日、年、時、および分を選択します。時の選択は 24 時間形式にする必要があります。たとえば、午前 9 時は **09**、午後 1 時の場合は **13** と入力し、真夜中は **24** と入力します。
3. ドロップダウン リストから、適切な時間帯を選択します。Universal Time Coordinated(UTC; 協定世界時)補正値はすべてサポートされています。UTC はグリニッジ標準時と同じです。補正値(UTC と、スイッチの時間帯の差異)は、正または負の数値となります。たとえば、太平洋標準時の補正値は -8 時間ですが、これは UTC から 8 時間遅れているという意味です。各時間帯は、UTC 補正値と、その地域の主要な都市や国の名前と共に表示されます。

4. 夏時間を自動的に設定するには、[自動夏時間調整]を選択します。自動夏時間調整は、米国、オーストラリア、カナダ、およびヨーロッパだけでサポートされており、各地で設定されている日時に夏時間が開始します。
5. [OK]をクリックします。

複数のデバイス上のシステムの時刻を手動で設定または変更するには、次の手順に従います。

1. 対象デバイスの行を選択します。
2. [修正]をクリックします。
3. [システム時間の修正]ウィンドウに情報を入力し、[OK]をクリックして変更内容を保存します。
4. [システム時間]ウィンドウの[適用]をクリックして変更内容を有効にします。
5. [更新]をクリックしてウィンドウを更新します。

コミュニティ内のデバイス間で時刻の設定を同期するには、次の手順に従います。

1. コミュニティ内のすべてのデバイスで同期を取るには、[同期]をクリックします。特定のデバイスと同期を取るには、デバイスの行を選択して、[同期]をクリックします。
2. [システム時間の同期]ウィンドウに情報を入力し、[OK]をクリックして変更内容を保存します。
3. [システム時間]ウィンドウの[適用]をクリックして変更内容を有効にします。
4. [更新]をクリックしてウィンドウを更新します。

UC500、Cisco 800シリーズルータを管理する場合

[システム時間]ウィンドウ

このウィンドウは、機能バーで **設定 > デバイスプロパティ > システム時間** を選択した場合に表示されます。

このウィンドウを使用する目的は、次のとおりです。

- 現在の時刻の表示
- システムの時刻の設定

現在の時刻の表示

[システム時間]ウィンドウには、コミュニティ内のすべてのデバイスで使用する現在の時刻の、時（24時間形式）、分、時間帯、月、日、および年が自動的に表示されます。

次に、この情報の表示形式の例を示します。

- 月、日、および年は、August/2/2005 のように表示されます。
- 時、分は、**9:00**（午前 9 時）や **13:00**（午後 1 時）のように表示されます。
- 時間帯は、（GMT -10:00） Hawaii のように表示されます。これは、Greenwich Mean Time（GMT; グリニッジ標準時）より 10 時間遅れているという意味です。

システムの時刻の設定

このウィンドウを使用する目的は、次のとおりです。

- 複数のデバイスでの、時刻の手動設定または変更
- コミュニティ内のデバイス間での時刻の同期
- NTP サーバの設定

注：一般的にいって、システムが NTP のような外部のタイミング メカニズムと同期している場合は、システム クロックを設定する必要はありません。時刻に関する発信元が利用できない場合は、手動で時刻を設定します。設定時刻は、設定された時間帯に準拠します。

デバイス上のシステムの時刻を手動で設定または変更するには、次の手順に従います。

1. デバイスの行を選択します。
2. 行のセル内で、ドロップダウン リストから月、日、年、時、および分を選択します。時の選択は 24 時間形式にする必要があります。たとえば、午前 9 時は **09**、午後 1 時の場合は **13** と入力し、真夜中は **24** と入力します。
3. ドロップダウン リストから、適切な時間帯を選択します。Universal Time Coordinated（UTC; 協定世界時）補正値はすべてサポートされています。UTC はグリニッジ標準時と同じです。補正値（UTC と、スイッチの時間帯の差異）は、正または負の数値となります。たとえば、太平洋標準時の補正値は -8 時間ですが、これは UTC から 8 時間遅れているという意味です。各時間帯は、UTC 補正値と、その地域の主要な都市や国の名前と共に表示されます。
4. 夏時間を自動的に設定するためには、[自動夏時間調整]を選択します。夏時間は、米国、オーストラリア、カナダおよびヨーロッパで採用されており、各地で決められた日付、時刻から夏時間になります。
5. [OK]をクリックします。

複数のデバイス上のシステムの時刻を手動で設定または変更するには、次の手順に従います。

1. 対象デバイスの行を選択します。
2. [修正]をクリックします。
3. [システム時間の修正]ウィンドウに情報を入力し、[OK]をクリックして変更内容を保存します。
4. [システム時間]ウィンドウの[適用]をクリックして変更内容を有効にします。
5. [更新]をクリックしてウィンドウをリフレッシュします。

コミュニティ内のデバイス間で時刻の設定を同期するには、次の手順に従います。

1. コミュニティ内のすべてのデバイスで同期を取るには、[同期]をクリックします。特定のデバイスと同期を取るには、デバイスの行を選択して、[同期]をクリックします。
2. [システム時間の同期]ウィンドウに情報を入力し、[OK]をクリックして変更内容を保存します。
3. [システム時間]ウィンドウの[適用]をクリックして変更内容を有効にします。
4. [更新]をクリックしてウィンドウをリフレッシュします。

NTP サーバを設定するには、次の手順に従います。

1. NTP サーバを設定するには、[NTP]をクリックします。
2. [ネットワークタイムサーバ]ウィンドウを終了します。

3. ［適用］をクリックして変更内容を有効にします。
4. ［更新］をクリックして、［システム時間］ウィンドウを閉じます。

CE520 スイッチを管理する場合

［システム時間の修正］ウィンドウ

このウィンドウは、［システム時間］ウィンドウで 1 つまたは複数のデバイスを選択して、［修正］をクリックしたときに表示されます。

注: 設定が異なるデバイスを複数選択した場合、これらの設定のフィールドは空白で表示されます。選択した複数のデバイスの設定が同じ場合は、設定が表示されます。

1. ［日付と時間］領域で、ドロップダウン リストから適切な月、日、年を選択します。
2. ドロップダウン リストから、適切な時、分を選択します。時の選択は 24 時間形式にする必要があります。たとえば、午前 9 時の場合は「**09**」と入力し、午後 1 時の場合は、「**13**」と入力します。
3. ドロップダウン リストから、適切な時間帯を選択します。Universal Time Coordinated（UTC; 協定世界時）補正値はすべてサポートされています。UTC はグリニッジ標準時と同じです。補正値（UTC と、スイッチの時間帯の差異）は、正または負の数値となります。たとえば、太平洋標準時の補正値は -8 時間ですが、これは UTC から 8 時間遅れているという意味です。各時間帯は、UTC 補正値と、その地域の主要な都市や国の名前と共に表示されます。
4. 自動夏時間調整を設定するには、ドロップダウン リストから［有効にする］を選択します。自動夏時間調整を無効にするには、［無効にする］を選択します。自動夏時間調整は、米国、カナダ、オーストラリア、およびヨーロッパだけでサポートされており、各地で設定されている日時に夏時間が開始します。
5. 変更したら、［OK］をクリックします。［システム時間］ウィンドウが表示されます。

CE520 スイッチを管理する場合

［システム時間の同期］ウィンドウ

このウィンドウは、［システム時間］ウィンドウで、［同期］をクリックしたとき、または 1 つまたは複数のデバイスを選択して［同期］をクリックしたときに表示されます。このウィンドウには、PC の現在の時刻が表示されます。

選択したデバイスのシステムの時刻を PC の現在の時刻に同期したり、特定のデバイスのシステムの時刻に同期したりできます。選択したデバイスの時間帯の設定を上書きすることもできます。たとえば、ニューヨークにあるデバイスのシステムの時刻を、時刻が午後 1 時（太平洋標準時）のサンノゼのデバイスの時刻設定と同期させると、同期の実行後、ニューヨークのデバイスには、午後 4 時（東部標準時）という新しい時刻設定が表示されます。ただし、［ローカルタイムゾーンを上書き］チェックボックスをオンにした場合は、ニューヨークのデバイスには新しい設定として太平洋標準時午後 1 時（サンノゼのデバイスと同じ）が表示されます。現地時間が上書きされたためです。

選択したデバイスのシステムの時刻を PC の現在の時刻に同期するには、次の手順に従います。

1. [PCと同期]を選択します。
2. 選択したデバイスの現地時間帯設定を上書きする場合は、[ローカルタイムゾーンを上書き]設定をオンにします。
3. [OK]をクリックして、変更内容を保存し、[システム時間]ウィンドウに戻ります。

選択したデバイスのシステムの時刻を特定のデバイスのシステムの時刻に同期するには、次の手順に従います。

1. [デバイスと同期]を選択します。
2. プルダウン リストからデバイス(同期先)を選択します。
3. 選択したデバイスの現地時間帯設定を上書きする場合は、[ローカルタイムゾーンを上書き]設定をオンにします。
4. [OK]をクリックして、変更内容を保存し、[システム時間]ウィンドウに戻ります。

CE520 スイッチを管理する場合

[システムメッセージ]ウィンドウ

このウィンドウは、機能バーで **モニタ > システムメッセージ** を選択した場合に表示されます。このウィンドウを使用すると、コミュニティ内のデバイスから発行されたメッセージを表示できます。

次の手順に従います。

1. [ホスト名]リストから、メッセージを表示するデバイスを選択するか、[全デバイス]を選択してコミュニティ内のすべてのデバイスから発行されたメッセージを表示します。
2. テーブルのカラム ヘッダをクリックし、必要に応じてメッセージをソートします。デフォルトでは、メッセージは重大度でソートされます。
3. 特定のメッセージの詳細を表示するには、テーブル内のその行を選択します。メッセージの詳細がテーブルの下の領域に表示されます。
4. *オプション:*[フィルタ]をクリックして[システムメッセージフィルタ]ウィンドウを開きます。このウィンドウでは、表示されるメッセージを制限する条件を指定できます。
5. オプション:[レポートの保存]をクリックして、ファイルにカンマ区切り形式でウィンドウの内容を保存します。デフォルトのファイル名には、ファイル名を一意にするためにタイム スタンプが含まれます。
6. ウィンドウでの作業が完了したら、[OK]をクリックします。

[システムメッセージ通知]ウィンドウ

このウィンドウは、機能バーで **アプリケーション > システムメッセージ通知** を選択した場合に表示されます。

このウィンドウを使用する目的は、次のとおりです。

- SMTP サーバからのシステム メッセージのメール通知の送信を有効にする。
- 通知名を作成、変更、または削除する。

システム メッセージ通知を設定するには、次の手順に従います。

1. [メールサーバ(SMTP)]フィールドに、通知を送信する SMTP サーバの名前を入力します。
2. [送信者のメールアドレス]フィールドに、通知の送信者として SMTP に指定するメールアドレスを入力します。

   注: SMTP 用語では、このアドレスを「返信アドレス」といいます。

3. [メールテスト]をクリックして、SMTP サーバと送信者のメール アドレス間の接続をテストします。送信者がテスト用のメールを受信すれば、接続は確認されます。
4. [作成]をクリックして、[通知の作成]ウィンドウを使用します。

   以上の手順を完了すると、[通知リスト]に新しい通知名が表示され、その通知名の[アクティブ]ボックスがオンになります。

通知名の情報を変更するには、その名前を選択して、[修正]をクリックし、[通知の修正]ウィンドウを使用します。

注: Configuration Assistant 5.0 より前のリリースで作成された通知名の情報は、変更できません。

通知名を削除するには、削除する通知名を選択して、[削除]をクリックします。

ウィンドウでの作業が完了したら、[OK]をクリックします。

CE520 スイッチを管理する場合

[システムメッセージフィルタ]ウィンドウ

このウィンドウは、[システムメッセージ]ウィンドウで[フィルタ]をクリックした場合に表示されます。このウィンドウを使用すると、このウィンドウに表示されるメッセージを制限できます。

次の手順に従います。

1. [重要度レベル]の下で、フィルタリングして除外する重大度レベルのチェックボックスをオフにします。オフにした重大度レベルのメッセージは、[システムメッセージ]ウィンドウに表示されなくなります。
2. オフになっているチェックボックスがあり、すべてのチェックボックスを再度オンにする場合は、[デフォルトに設定]をクリックします。
3. ウィンドウでの作業が完了したら、[OK]をクリックします。

CE520 スイッチを管理する場合

[状態]ウィンドウ

このウィンドウは、次のいずれかの処理を実行した場合に表示されます。

- 機能バー上で **モニタ > 状態** を選択する。
- ツールバー上で  を選択する。

このウィンドウでは、監視用に選択したカテゴリで最も高い測定値を持つデバイスを最大 5 つ表示できます。ウィンドウのバーにマウス ポインタを当てると、詳細が表示されます。さらに詳細を表示するには、[詳細]をクリックして[状態の詳細]ウィンドウを開きます。

注：Configuration Assistant には、次のような特定のリソースの使用に焦点を置く機能も含まれています。

- PoE使用率についての詳細は、**設定 > ポート > ポート設定** を選択し、[ポート設定]ウィンドウを使用します。
- 帯域幅使用率についての情報は、**モニタ > レポート > 帯域幅グラフ** を選択し、[帯域幅グラフ]ウィンドウを使用します。
- リンクの使用状況についての情報は、**モニタ > レポート > リンクグラフ** を選択して、[リンクグラフ]ウィンドウを使用します。
- パケット エラーについての情報は、**モニタ > レポート > ポート統計情報** を選択して、[ポート統計情報]ウィンドウを使用します。

[状態]ウィンドウ内の測定値は、状態のポーリングが実行されるたびに更新されます。ウィンドウの右上の角に、ポーリング間隔の残り時間が表示されます。

デフォルトで表示される測定カテゴリ以外の測定カテゴリを選択するには、[環境設定]をクリックして、[環境設定]ウィンドウを表示し、[状態]タブで選択します。ここで状態のポーリング間隔を変更することもできます。

CE520 スイッチを管理する場合

[状態の詳細]ウィンドウ

このウィンドウは、[状態]ウィンドウ内の[詳細]をクリックした場合に表示されます。監視する測定カテゴリの詳細を表示する際に使用します。

ウィンドウでの作業が完了したら、[OK]をクリックします。

このウィンドウ内のタブについての説明は次のとおりです。

[概要]

このタブには、カテゴリが適用されているネットワーク内のすべてのデバイス上で監視する各カテゴリの測定概要（詳細なし）が示されます。

次の表は、タブの各カラムを示しています。

カラム	説明
ホスト名	スタンドアロンのデバイスのホスト名、またはコミュニティ内のデバイスのホスト名
帯域幅使用率	パケットの送受信で使用された平均的な帯域幅（最新のポーリング時点）
パケット エラー	全体のパケットの入力および出力エラー率
PoE使用率	PoE で使用中のワット数の割合
CPU使用率	直近 5 秒間の CPU 使用率
メモリ使用率	使用中のメモリの使用率
温度	温度（摂氏）

［帯域幅使用率］

このタブには、パケットの受信と送信に使用されているそれぞれの帯域幅の割合、およびこれらの平均が表示されます。

［帯域幅グラフ］ウィンドウを表示すると、デバイスの帯域幅の長期的な使用状況を確認できます。［リンク グラフ］ウィンドウには、トラフィックが最大のポートが表示されます。

［パケット エラー］

このタブには、デバイスの入力および出力パケット エラーの比率と、全体のエラー比率が示されます。

［PoE使用率］

PoE（Power over Ethernet）をサポートするデバイスの場合、このタブには、使用中の PoE ワット数の割合、合計ワット数、使用されたワット数、および使用可能なワット数が表示されます。

ネットワークにアクセスポイントと IP Phone を追加する場合は、PoE 使用率が低いデバイスに接続してください。

［CPU使用率］

このタブには、デバイスごとに、直近 5 秒間、1 分間および 5 分間の使用中の CPU 容量の使用率が示されます。

［メモリ使用率］

このタブには、使用中のメモリの割合と、メモリ合計、使用されたメモリ、および空きメモリのメガバイト数が表示されます。

［温度］

温度を正確に測定できるデバイスの場合、このタブには、現在の温度、オーバーヒートしきい値、および緊急しきい値が摂氏で表示されます。それ以外のデバイスの場合は、温度は［OK］、［Normal］、［Faulty］、または［N/A］と表示され、正確な現在の温度、オーバーヒートしきい値、および緊急しきい値が検知されていないことを示します。

UC500 を管理する場合

[推奨スマートポート]

このウィンドウは、次のいずれかの処理を実行した場合に表示されます。

- [スマートポート]ウィンドウで[推奨]をクリックする。
- [イベント通知]ウィンドウで[解決]をクリックしてスマートポートロールを適用する。

このウィンドウを使用する目的は、次のとおりです。

- VLAN を IP Phone 、スイッチ、ルータ、またはアクセスポイントの推奨ポート ロールに設定する。
- 誤って適用したロールを修正する。

ポートにロールを適用するには、次の手順に従います。

1. [推奨ロール]カラムに表示されているロールをそのまま受け入れるか、または推奨されているロールをクリックして、開いたリストから別のロールを選択します。

   注:

   - Configuration Assistant は、場合によっては、デバイス タイプがルータのときに接続されたデバイス タイプをスイッチとして検出したり、スイッチをルータとして検出することがあります。検出されたデバイス タイプが正しくない場合には、[推奨ロール]カラムから別のデバイス タイプを選択します。
   - 接続されているデバイスがアクセスポイントの場合は、推奨される[アクセスポイント]ロールを受け入れるか、またはリストをクリックして[ゲスト]を選択してください。

2. VLAN(IP Phone の場合は 2 つの VLAN)を選択します。次の表は、デバイスの各接続タイプに必要な VLAN を示しています。

接続先	選択する VLAN
IP Phone	[アクセス VLAN]および[音声VLAN]
スイッチ	[ネイティブ VLAN]
ルータ	[ネイティブ VLAN]
アクセスポイント	[ネイティブ VLAN]

   選択した VLAN は、設定している接続に対応している必要があります。必要な VLAN が表示されない場合、その VLAN は作成されていません。このウィンドウおよび[スマートポート]ウィンドウを閉じてから、[VLAN]ウィンドウを使用して VLAN を作成し、再度スマートポート機能を使用してください。

3. 完了したら、[OK]をクリックします。[スマートポート]ウィンドウで[OK]をクリックして、VLAN を設定したロールを適用します。

CE520 スイッチを管理する場合

[推奨スマートポート]

このウィンドウは、次のいずれかの処理を実行した場合に表示されます。

- [スマートポート]ウィンドウで[推奨]をクリックする。
- [イベント通知]ウィンドウで[解決]をクリックして スマートポートロールを適用する。

このウィンドウを使用する目的は、次のとおりです。

- VLAN を IP Phone、スイッチ、ルータ、またはアクセスポイントの推奨ポート ロールに設定する。
- 誤って適用したロールを修正する。

ポートにロールを適用するには、次の手順に従います。

1. [推奨ロール]カラムに表示されているロールをそのまま受け入れるか、または推奨されているロールをクリックして、開いたリストから別のロールを選択します。

   注:

   - Configuration Assistant は、場合によっては、デバイス タイプがルータのときに接続されたデバイス タイプをスイッチとして検出したり、スイッチをルータとして検出することがあります。検出されたデバイス タイプが正しくない場合には、[推奨ロール]カラムから別のデバイス タイプを選択します。
   - 接続されているデバイスがアクセスポイントの場合は、推奨される[アクセスポイント]ロールを受け入れるか、またはリストをクリックして[ゲスト]を選択してください。
   - Configuration Assistant は、Cisco Express 500 スイッチ ポートに接続されたスイッチまたはスニファを検出できません。したがって、これらの接続の場合には推奨されるロールは表示されません。

2. VLAN(IP Phone の場合は 2 つの VLAN)を選択します。次の表は、デバイスの各接続タイプに必要な VLAN を示しています。

接続先	選択する VLAN
IP Phone	[アクセス VLAN]および[音声VLAN]
スイッチ	[ネイティブ VLAN]
ルータ	[ネイティブ VLAN]
アクセスポイント	[ネイティブ VLAN]

選択した VLAN は、設定している接続に対応している必要があります。必要な VLAN が表示されない場合、その VLAN は作成されていません。このウィンドウおよび[スマートポート]ウィ

ンドウを閉じてから、[VLAN]ウィンドウを使用して VLAN を作成し、再度スマートポート機能を使用してください。

3. 完了したら、[OK]をクリックします。[スマートポート]ウィンドウで[OK]をクリックして、VLAN を設定したロールを適用します。

CE520 スイッチを管理する場合

[スマートポート]ウィンドウ

このウィンドウは、次のいずれかを選択した場合に表示されます。

- 機能バー上で **設定 > スマートポート** を選択する。
- ツールバー上で  を選択する。
- [イベント通知]ウィンドウで[解決]を選択して、スマートポートイベントを解決する。

このウィンドウには、ネットワーク内のデバイスの前面パネルのビューが表示されます。ポートがデバイスに接続されてロールが適用されていると、そのポートに接続されたデバイスのアイコンが表示されます。マウス ポインタをアイコン上に移動すると、Configuration Assistant は接続されたデバイスのタイプを識別します。

ロールを別の接続されたポートに適用したり、誤って適用されたロール( アイコンにより示される)を修正するには、次の操作のいずれかを実行します。

- [推奨]をクリックします。接続デバイスのアイコンがポート上に点滅し、[推奨スマートポート]ウィンドウが表示されます。ウィンドウでは、ポートに適用するロールを推奨します。
- ポートを選択して、[修正]をクリックします。[ポートロールの修正]ウィンドウが表示されます。このウィンドウでは、スマートポートロールを削除したり、デバイスに接続していないポートにロールを適用したりすることもできます。

注:

- 複数のポートを選択するには、**Ctrl** キーを押しながら、必要なポートをクリックします。また、マウスのボタンを押しながら、ポートのグループを長方形にドラッグすることにより、ポートを ラバーバンドで選択することもできます。**Ctrl** キーを押しながら、隣接していないポートのグループをラバーバンドで選択できます。
- Configuration Assistant を使用してロールを適用する場合、そのロールは以前に適用されたロールと置き換わります。

[スマートポート]ウィンドウに戻ると、ロールの選択を設定した各ポートの上にデバイスのアイコンが表示されます。Configuration Assistant でロールを削除すると、以前に表示されていたアイコンがなくなります。

設定済みポートに関する詳細を確認するには、[詳細]をクリックして[ポートロールの詳細]ウィンドウを開きます。

UC500、Cisco 800シリーズルータを管理する場合

[静的ルーティング]ウィンドウ

このウィンドウは、**設定 > ルーティング > 静的ルーティング** を選択した場合に表示されます。

このウィンドウでは、ルータに対する静的ルートの追加または削除を行うことができます。

まず、設定するデバイスを[ホスト名]リストから選択します。

静的ルートを追加するには、[追加]をクリックして、[静的ルートの追加]ウィンドウを使用します。

静的ルートを削除するには、次の手順に従います。

1. [静的ルーティング]ウィンドウで、静的ルートを選択します。
2. 静的ルーティング テーブルからエントリを削除するには、[削除]をクリックします。
3. ウィンドウを閉じて変更を保存するには、[OK]をクリックします。

UC500、Cisco 800シリーズルータを管理する場合

[静的ルートの追加]ウィンドウ

このウィンドウは、[静的ルーティング]ウィンドウで[追加]をクリックした場合に表示されます。

このウィンドウでは、ルータに静的ルートを追加できます。

次の手順に従います。

1. [宛先/ネットワークIP]フィールドに、宛先ネットワークの IP アドレスを入力します。
2. [ネットワークマスク]フィールドに、宛先ネットワークのサブネット マスクを入力します。
3. [ネットワークマスク]フィールドの下のドロップダウン メニューから、インターフェイスを選択します。
4. [ゲートウェイIPまたは発信インターフェイス]リストからインターフェイスを選択します。[ゲートウェイIPまたは発信インターフェイス]リストから[ゲートウェイIPの入力]オプションを選択した場合は、[ゲートウェイIPまたは発信インターフェイス]フィールドの下で、ゲートウェイまたは発信インターフェイスの IP アドレスを入力します。
5. ウィンドウを閉じて変更を保存するには、[OK]をクリックします。

UC500、Cisco 800シリーズルータを管理する場合

[セキュリティ監査]ウィンドウ

このウィンドウは、を選択した場合に表示されます。

デバイスでセキュリティ監査を実行するには、次の手順に従います。

1. [セキュリティ]リストから[セキュリティ監査]を選択し、[セキュリティ監査]起動ボタンを表示します。
2. [ホスト名]リストから、監査するデバイスを選択します。
3. セキュリティ監査設定の一覧と推奨されるアクションを表示するには、[セキュリティ監査]をクリックします。セキュリティ監査のレポート ウィンドウが表示されます。
4. このウィンドウでは、ネットワークを保護するために実行するアクションを選択できます。

推奨値に設定されているセキュリティ設定と、推奨値に設定されていないセキュリティ設定が表に示されます。推奨値に設定されていないものは、セキュリティ上の問題が潜んでいることになります。

デバイスのセキュリティ設定を変更するには、次の手順に従います。

1. [ホスト名]リストから、監査するデバイスを選択します。
2. 推奨値に設定されていないパラメータのセキュリティ設定を推奨値に設定するには、[セキュリティに関する問題を修正する]ラジオ ボタンをクリックします。セキュリティ機能をデフォルト値に設定するには、[セキュリティ設定を元に戻す]ボタンをクリックします。
3. セキュリティ機能を推奨値に設定するには、セキュリティ監査にパスしなかったセキュリティ設定の横にある[修正]カラムのチェックボックスをオンにします。セキュリティ機能をデフォルト値に設定するには、セキュリティ監査にパスしたセキュリティ設定の横にある[元に戻す]カラムのチェックボックスをオンにします。すべてのチェックボックスをオンにするには、[すべて選択]をオンにします。
4. セキュリティの変更を有効にしてウィンドウを閉じるには、[OK]をクリックします。

[接続]ウィンドウ

このウィンドウは、次の場合に表示されます。

- Configuration Assistant を起動したとき
- **アプリケーション > 接続** を選択したとき

このウィンドウを使用すると、新しいコミュニティ、既存のコミュニティ、またはスタンドアロンデバイスに Configuration Assistant を接続できます。

[コミュニティの作成]を選択して[OK]をクリックすると、[コミュニティの作成]ウィンドウが開きます。このウィンドウに必要な情報を入力すると、Configuration Assistant が新しいコミュニティに接続されます。

[接続先]を選択して、既存のコミュニティに接続する場合は、次の手順に従います。

1. コミュニティ名を入力するか、リストから選択します。
2. Configuration Assistant でネットワーキング機能を設定する権限を持っている場合は、[オプション]を選択して[読み書き]をクリックします。権限を持っていない場合は、[読み取り専用]をクリックしてアクセスレベル番号を選択します。デフォルトは[読み書き]です。
3. [OK]をクリックします。

スタンドアロン デバイスに接続するには、そのデバイスの IP アドレスまたはホスト名を入力します。

注:

- Configuration Assistant では、アクセスポイントまたはルータの IP アドレスを入力すると、不明なデバイスとして処理されます。アクセスポイントとルータを管理するためのコミュニティを作成する必要があります。
- ホスト名は、DNS サーバがホスト名を解決するように設定されている場合にだけ使用できます。ホスト名がコミュニティ名と同じであれば、Configuration Assistant はそのコミュニティに接続されます。
- 接続できない場合は、HTTP が有効になっていることを確認してください。デバイスによっては、出荷時に HTTP が無効になっている場合があります。接続するにはこれを有効にする必要があります。

CE520 スイッチを管理する場合

[設定の保存]ウィンドウ

このウィンドウは、メニュー バーで **メンテナンス > 設定の保存** を選択した場合に表示されます。このウィンドウは、起動用設定のバックアップおよび復元に使用します。

このウィンドウには、次のタブがあります。

- [バックアップ]。管理対象デバイスの起動用設定のバックアップを PC またはネットワーク ドライブに作成します。
- [復元]。起動用設定を管理対象デバイスに復元します。

[バックアップ]

次の手順に従います。

1. [ホスト名]リストから、起動用設定のバックアップを作成するデバイスを 1 つまたは複数選択します。
2. [バックアップのメモ]テキスト領域に、バックアップした設定を後で復元する場合に識別できるように情報を入力します。
3. [バックアップ]をクリックします。[バックアップディレクトリ]フィールドに表示されているディレクトリに設定が保存され、このイベントが[復元]タブに記録されます。

   注:

   - バックアップ ディレクトリに保存した設定の保存を削除できます。
   - 別のディレクトリにバックアップを作成するには、[環境設定]をクリックして[環境設定]ウィンドウを開き、[設定の保存]タブで別のパスとディレクトリを入力します。このタブには、実行中の設定を自動で保存してからバックアップを作成するというオプションもあります。これを選択しないと、実行中の設定が起動用設定と異なる場合に、実行中の設定を保存するように指示するプロンプトが、Configuration Assistant に表示されます。
4. [OK]をクリックしてウィンドウを閉じます。

[復元]

次の手順に従います。

1. [ホスト名]リストから、復元先のデバイスを選択します。
2. ボタンをクリックして、[バックアップ済み設定]リストに表示されているバックアップ済み設定の範囲を指定します。

   上のボタンは、選択したデバイスからバックアップした設定のみを表示します。中央のボタンは、選択したデバイスからバックアップした設定と、同じデバイス タイプのコミュニティ内のその他のデバイスからバックアップした設定を表示します。下のボタンは、バックアップ ディレクトリにあるバックアップ済み設定をすべて表示します。

3. [バックアップ済み設定]リストから、復元する設定を選択します。

   [バックアップのメモ]テキスト領域の内容を見て、選択した設定が復元対象のファイルであることを確認します。

4. [復元]をクリックします。
5. [再起動]をクリックして、設定の復元後にデバイスを再起動します。[OK]をクリックした場合は、デバイスの再起動を求めるプロンプトが表示されます。

CE520 スイッチを管理する場合

[設定の保存]ウィンドウ

このウィンドウは、機能バーで **設定 > 設定の保存** を選択した場合に表示されます。

管理対象デバイスの実行中の設定を起動用設定に保存するには、[ホスト名]リストからデバイスを選択して[保存]をクリックします。

すべての管理対象デバイスの実行中の設定を保存するには、[全デバイス]を選択して[保存]をクリックします。

WLC526 を管理する場合

[設定の保存]ウィンドウ

このウィンドウは、メニュー バーで **メンテナンス > 設定の保存** を選択した場合に表示されます。このウィンドウは、起動用設定のバックアップおよび復元に使用します。

このウィンドウには、次のタブがあります。

- [バックアップ]。管理対象デバイスの起動用設定のバックアップを PC またはネットワーク ドライブに作成します。
- [復元]。起動用設定を管理対象デバイスに復元します。

[バックアップ]

次の手順に従います。

1. [ホスト名] リストから、起動用設定のバックアップを作成するデバイスを 1 つまたは複数選択します。
2. [バックアップのメモ] テキスト領域に、バックアップした設定を後に復元する場合に識別できるように情報を入力します。
3. [バックアップ] をクリックします。[バックアップディレクトリ]フィールドに表示されているディレクトリに、設定の保存が作成され、このイベントが[復元]タブに記録されます。

   注:

   - バックアップ ディレクトリに保存した設定の保存を削除できます。
   - 別のディレクトリにバックアップを作成するには、[環境設定] をクリックして[環境設定]ウィンドウを開き、[設定の保存] タブで別のパスとディレクトリを入力します。このタブには、実行中の設定を自動で保存してからバックアップを作成するというオプションもあります。これを選択しないと、実行中の設定が起動用設定と異なる場合に、実行中の設定を保存するように指示するプロンプトが、Configuration Assistant に表示されます。
4. [OK]をクリックしてウィンドウを閉じます。

[復元]

次の手順に従います。

1. [ホスト名] リストから、復元先のデバイスを選択します。
2. ボタンをクリックして、[バックアップ済み設定]リストに表示されているバックアップ済み設定の範囲を指定します。

   上のボタンは、選択したデバイスからバックアップした設定のみを表示します。中央のボタンは、選択したデバイスからバックアップした設定と、同じデバイス タイプのコミュニティ内のその他のデバイスからバックアップした設定を表示します。下のボタンは、バックアップ ディレクトリにあるバックアップ済み設定をすべて表示します。

3. [バックアップ済み設定] リストから、復元する設定を選択します。

   [バックアップのメモ] テキスト領域の内容を見て、選択した設定が復元対象のファイルであることを確認します。

4. [復元] をクリックします。
5. [再起動]をクリックして、設定の復元後にデバイスを再起動します。[OK]をクリックした場合は、デバイスの再起動を求めるプロンプトが表示されます。

UC500 を管理する場合

[ソフトウェアアップグレード]ウィンドウ

このウィンドウは、機能バーで **メンテナンス > ソフトウェアアップグレード** を選択した場合に表示されます。このウィンドウを使用する目的は、次のとおりです。

- Cisco IOS ソフトウェアを 1 つまたは複数のデバイス上でアップグレードする。
- CUE ソフトウェアを Unified Communications 500 シリーズ プラットフォーム上でアップグレードする。
- Cisco IOS ソフトウェアおよび CUE ソフトウェアの両方を同時に Unified Communications 500 シリーズ プラットフォーム上でアップグレードする。

このウィンドウでは、標準のまたはリモートの TFTP サーバ モードを使用したソフトウェアのアップグレードがサポートされます。このウィンドウをドラッグ アンド ドロップ モードに使用することはできません。

デバイスのアップグレード

デバイスをアップグレードするには、次の手順に従います。

1. デバイスのアップグレードに使用する Cisco IOS bin ファイルをダウンロードします。
2. 同一プラットフォームから 1 つまたは複数のデバイスを選択します。
3. [アップグレード設定]をクリックします。
4. [アップグレード設定]ウィンドウを完了したら、[OK]をクリックし入力内容を保存します。
5. 複数のデバイス タイプをアップグレードする場合は、デバイス タイプごとに手順 2 から 4 を繰り返します。
6. アップグレードする各デバイスの横の[アップグレード]ボックスをチェックします。
7. [アップグレード]をクリックしてアップグレード処理を開始します。
8. [ステータス]をクリックすると、[ソフトウェアアップグレードのステータス]ウィンドウが表示されます。このウィンドウには、アップグレードの進捗状況が表示されます。
9. 選択したすべてのデバイスについて、ソフトウェアのアップグレード処理が完了すると、確認を示すダイアログが表示されます。ステータスのメッセージに、正常にアップグレードされたデバイスと正常にアップグレードされなかったデバイスが一覧表示されます。
10. [OK]をクリックします。正常にアップグレードされたデバイスのリロードを求めるプロンプトが表示されます。これらのデバイスをリロードする場合は[はい]を選択し、リロードしない場合は[いいえ]を選択します。デバイスをリロードするまで、そのデバイスでは更新は使用されません。
11. [アップグレードしたデバイスのリロード]をクリックして、アップグレードしてから選択したデバイスをリロードすることもできます。

    設定に加えた変更はすべて自動的にフラッシュ メモリに保存されます。1 分後、デバイスはリロードされ、新しいイメージが実行されます。その後に[ソフトウェアアップグレード]ウィンドウを閉じることができます。

    注:

    - デバイスをリロードするとすぐにコミュニティでそれらのデバイスを管理できます。
    - デバイスをリロードするとそのデバイスへの接続は失われます。

次の表は、[ソフトウェアアップグレード]ウィンドウのカラムについて説明しています。

カラム	説明
デバイス	デバイスのアイコンとホスト名が表示されます。
アップグレード	[アップグレード]をクリックしたときにデバイスをアップグレードするかどうかを示します。
デバイスタイプ	デバイスのタイプを示します。
現在のバージョン	Cisco IOS のバージョンを示します。
新しいイメージ名	[アップグレード設定]ウィンドウに入力した Cisco IOS .bin ファイルの名前が表示されます。ファイル名だけが表示され、パスは表示されません。
アップグレードステータス	アップグレード ステータスおよび進捗状況のメッセージが表示されます。詳細については、「アップグレード ステータスのメッセージ」を参照してください。

アップグレード ステータスのメッセージ

次の表は、アップグレード ステータスのメッセージについて説明しています。

メッセージ	説明
[アップグレード設定]ボタンをクリックして続行します。]	デバイスをアップグレードするには、[アップグレード設定]ウィンドウに情報を入力する必要があります。
[デバイスをアップグレードする場合は、[アップグレード]ボタンをクリックします。]	デバイスのアップグレードに必要なすべてのパラメータがデバイスに設定されました。
[デバイスのリロードを開始しました。]	ソフトウェアが正常にアップグレードされた後にデバイスがリロードされています。リロードが完了した後でも、ウィンドウをリフレッシュするまでこのメッセージは表示されます。
[ソフトウェアアップグレードに成功しました。]	アップグレードは正常に完了しました。
[ソフトウェアのアップグレードに失敗しました。]	アップグレードが失敗しました。詳細は[ステータス]ウィンドウを参照してください。
[ソフトウェアのアップグレード中です。]	デバイスのアップグレードの実行中です。
[イメージをアップロードしています。]	イメージがデバイスにアップロードされています。
[Cisco IOSイメージを検証しています。]	デバイスでイメージを検証しています。

CE520 スイッチを管理する場合

[ソフトウェアアップグレード]ウィンドウ

このウィンドウは、機能バーで **メンテナンス > ソフトウェアアップグレード** を選択した場合に表示されます。このウィンドウを使用すると、デバイスのソフトウェアをアップグレードしたり、複数のデバイスのソフトウェアを同時にアップグレードしたりできます。

代替方法:1 つのデバイスでソフトウェアをアップグレードする場合は、アップグレードを含む Cisco IOS tar ファイルを[トポロジ]ビューにドラッグして、デバイスのアイコン上にドロップします。

デバイスのアップグレード

次の表は、[ソフトウェアアップグレード]ウィンドウのカラムについて説明しています。

カラム	説明
デバイス	デバイスのアイコンとホスト名が表示されます。
アップグレード	デバイスが**アップグレード**するために選択されているかどうかを示します。
デバイスタイプ	デバイスのタイプを示します。
現在のバージョン	現在の Cisco IOS のバージョンと、SMI、EMI などのイメージのタイプを表示します。
新しいイメージ名	[アップグレード設定]ウィンドウに入力した Cisco IOS tar ファイルの名前が表示されます。ファイル名だけが表示され、パスは表示されません。
アップグレードステータス	アップグレード ステータスおよび進捗状況のメッセージが表示されます。詳細については、「アップグレード ステータスのメッセージ」を参照してください。

デバイスをアップグレードするには、次の手順に従います。

1. デバイスのアップグレードに使用する Cisco IOS tar ファイルをダウンロードします。「ソフトウェアのアップグレード」トピックの下にあるリンクを使用して、Cisco.com からソフトウェアをダウンロードできます。
2. 同一プラットフォームの 1 つまたは複数のデバイスを選択します。
3. [アップグレード設定]をクリックします。
4. [アップグレード設定]ウィンドウを完了したら、[OK]をクリックし入力内容を保存します。
5. 複数のデバイス タイプをアップグレードする場合は、デバイス タイプごとに手順 2 から 4 を繰り返します。
6. 今すぐアップグレードする各デバイスの横の[アップグレード]チェックボックスをオンにします。
7. [アップグレード]をクリックしてアップグレード処理を開始します。

   注:現在のイメージは削除され、新しいイメージがダウンロードされます。コマンドライン インターフェイス(CLI)を使用して、現在のイメージを保存できます。

8. [ステータス]をクリックすると、[ソフトウェアアップグレードのステータス]ウィンドウが表示されます。このウィンドウには、アップグレードの進捗状況が表示されます。
9. 選択したすべてのデバイスについて、ソフトウェアのアップグレード処理が完了すると、確認を示すダイアログが表示されます。ステータスのメッセージに、正常にアップグレードされたデバイスと正常にアップグレードされなかったデバイスが一覧表示されます。正常にアップグレードされたデバイスのリロードを求めるプロンプトが表示されます。これらのデバイスをリロードする場合は[はい]を選択し、リロードしない場合は[いいえ]を選択します。
10. [アップグレードしたデバイスのリロード]をクリックして、アップグレードしてから選択したデバイスをリロードすることもできます。

    設定に加えた変更はすべて自動的にフラッシュ メモリに保存されます。1 分後、デバイスはリロードされ、新しいイメージの実行が開始します。その後に[ソフトウェアアップグレード]ウィンドウを閉じることができます。

    注 : デバイスをリロードすると、そのデバイスへの接続は失われます。

アップグレード ステータスのメッセージ

次の表は、アップグレード ステータスのメッセージについて説明しています。

メッセージ	説明
[[アップグレード設定]ボタンをクリックして続行します。]	デバイスをアップグレードするには、[アップグレード設定]ウィンドウに情報を入力する必要があります。
[デバイスをアップグレードする場合は、[アップグレード]ボタンをクリックします。]	デバイスのアップグレードに必要なすべてのパラメータがデバイスに設定されました。
[フラッシュの合計サイズを決定しています。]	デバイスのアップグレードに使用できる十分な空き容量があるかどうかを、アップグレードプロセスが確認しています。
[tarイメージファイルの情報ファイルを抽出しています。]	Cisco IOS イメージ tar ファイルから info ファイルが抽出されています。
[tarイメージファイルの情報ファイルを読み取っています。]	Cisco IOS イメージに関する詳細について、Cisco IOS イメージ tar ファイルの info ファイルが読み込まれています。
[デバイスのリロードを開始しました。]	ソフトウェアが正常にアップグレードされた後にデバイスがリロードされています。リロードが完了した後でも、ウィンドウをリフレッシュするまでこのメッセージは表示されます。
[ソフトウェアアップグレードに成功しました。]	アップグレードは正常に完了しました。
[ソフトウェアのアップグレードに失敗しました。]	アップグレードが失敗しました。詳細は[詳細]ウィンドウを参照してください。
[ソフトウェアのアップグレード中です。]	デバイスのアップグレードの実行中です。
[ソフトウェアのアップグレードはキャンセルされました。]	アップグレードがキャンセルされました。

[イメージをアップロードしています。]	イメージがデバイスにアップロードされています。
[Cisco IOSイメージを検証しています。]	デバイスでイメージを検証しています。

CE520 スイッチを管理する場合

[ソフトウェアアップグレードのステータス]ウィンドウ

このウィンドウは、[ソフトウェアアップグレード]ウィンドウでデバイスを選択して[ステータス]をクリックした場合に表示されます。詳細メッセージがアップグレードの間にデバイスから生成された場合、このウィンドウにそれらのメッセージが表示されます。

新しいイメージをインストールするための十分な容量がデバイスにない場合、[ファイル管理]ウィンドウへのリンクとともにメッセージが表示されます。[ファイル管理]ウィンドウを使用すると、ファイルシステムを管理できます。また、新しいイメージに使用する容量を確保するために必要に応じて古いイメージを削除できます。

ウィンドウでの作業が完了したら、[OK]をクリックします。

CE520 スイッチを管理する場合

[帯域幅グラフ]ウィンドウ

このウィンドウは、機能バーで モニタ > レポート > 帯域幅グラフ を選択した場合（またはビューでデバイスを右クリックしてポップアップ メニューから[帯域幅グラフ]を選択した場合）に表示されます。

このウィンドウを使用して、[ホスト名]リストから選択したデバイスを経由するトラフィック フローの予測を表示します。

このウィンドウには次のタブがあります。

- [時系列]。このタブには、ウィンドウが表示された時点からの、帯域幅利用率が表示されます。
- [トレンド]。このタブには、分、時間、日、または 2 週間単位で過去の帯域幅利用率が表示されます。

[時系列]

このタブのグラフは、次の方法で操作できます。

- 表示されるグラフのタイプの選択
- x 軸上の差分の変更
- ポーリング間隔の変更
- x 軸のスクロール

表示されるグラフのタイプの選択

[タイプ]リストで、[折れ線]または[棒]をクリックしてグラフのタイプを選択します。折れ線グラフでは、データ ポイントが線で結ばれます。棒グラフでは、データ ポイントが棒の高さで示されます。

x 軸上の差分の変更

デフォルトでは、x 軸上の時間の差分が 2 分間隔で表示されます。その差分の間隔を短くしたり、長くしたりするには、[拡大/縮小]ボタンをクリックします。

ポーリング間隔の変更

通常の間隔で、Configuration Assistant が管理対象デバイスにデバイス利用率データおよびリンク利用率データを収集するよう照会します。この間隔は、グラフ ポーリング間隔と呼ばれています。その間隔を設定するには、[環境設定]ウィンドウを開いて[全般]タブをクリックし、[グラフポーリング間隔]フィールドの値を選択します。

注: デバイス上のトラフィック レベルが急激に下がった場合には、グラフ ポーリング間隔の設定に関わらず、少なくとも 15 分間はグラフの変化が表示されません。

x 軸のスクロール

グラフの下にあるスクロール バーを使用し、左にスクロールしてグラフの外へ移動した過去のデータ ポイントを確認できます。その後で右にスクロールして最新のデータに戻ることができます。

注: グラフは、デバイスがポーリングされるたびに更新されます。ポーリング間隔(データ収集の頻度)を変更するには、**アプリケーション > 環境設定** を選択して [環境設定]ウィンドウを使用します。

[トレンド]

このタブ上のグラフは、過去の帯域幅利用率を示しています。したがって、このタブを開くとデータの履歴が表示されます。デフォルトでは、過去 60 秒間のデバイスの帯域幅データが表示されます。タブ上の[トレンド]ボタンをクリックすると、過去 60 分、24 時間、または 14 日間のデータも表示できます。データは必ず棒グラフとして表示されます。

x 軸上の間隔は[トレンド]グラフごとに固定されています。間隔を伸ばしたり縮めたりするには、別の[トレンド]ボタンをクリックします。

CE520 スイッチを管理する場合

[注釈]ウィンドウ

このウィンドウは、次の場合に表示されます。

- トポロジ マップ上のデバイスを右クリックし、ポップアップ メニューで[注釈]を選択した場合。
- ネットワーク クラウドを追加した場合。
- トポロジ マップ上のノード間にリンクを追加した場合(デバイスとネットワーク クラウドとの間、デバイス間など)。

ノードに注釈を付けている場合は、テキスト フィールドに説明的な情報（デバイスの場所など）を入力します。この情報は、ノード アイコンの下に表示されます。リンクに注釈を付けている場合は、リンクの各エンドポイントの識別用情報を入力します。完了したら、[OK]をクリックします。

注：[トポロジオプション]ウィンドウの[情報の表示]タブで[注釈]をオフにすると、トポロジ マップ上の注釈を非表示にできます。

[通知の作成]ウィンドウ

このウィンドウは、[システムメッセージ通知]ウィンドウで[作成]をクリックした場合に表示されます。このウィンドウでは、次の情報を指定します。

- 通知名
- 受信者のメール アドレス
- セキュリティ レベルごとの、受信者が詳細を必要とするメッセージの種類

次の手順に従います。

1. [通知名]フィールドに名前を入力します。
2. [メールアドレス]フィールドにメール アドレスを入力します。これは、受信者が通知を受け取るアドレスです。
3. メッセージのセキュリティ レベルの横にあるボックスをオンにして、受信者が詳細を必要とするメッセージの種類を指定します。

   4 以上のセキュリティ レベルをオンにすると、受信者に必要以上の通知が送信される可能性があります。

ウィンドウでの作業が完了したら、[OK]をクリックします。

[通知の修正]ウィンドウ

このウィンドウは、[システムメッセージ通知]ウィンドウで通知名を選択して、[修正]をクリックした場合に表示されます。このウィンドウでは、受信者のメール アドレス、および受信者が詳細を必要とするメッセージの種類を変更できます。

次の手順に従います。

1. 受信者の新しいメール アドレスに通知を送信する場合は、[メールアドレス]フィールドにそのアドレスを入力します。
2. メッセージのセキュリティ レベルの横にあるボックスをオンにして、受信者が詳細を必要とするメッセージの種類を指定します。

   4 以上のセキュリティ レベルをオンにすると、受信者に必要以上の通知が送信される可能性があります。

ウィンドウでの作業が完了したら、[OK]をクリックします。

CE520 スイッチを管理する場合

[通知フィルタ]ウィンドウ

このウィンドウは、[イベント通知]ウィンドウで[フィルタ]をクリックした場合に表示されます。このウィンドウを使用すると、このウィンドウに表示されるイベントのタイプを制限できます。

次の手順に従います。

1. [タイプ]の下で、フィルタリングして除外するイベント タイプのチェックボックスをオフにします。オフにしたタイプのイベントは[イベント通知]ウィンドウに表示されなくなります。
2. オフになっているチェックボックスがあり、すべてのチェックボックスを再度オンにする場合は、[デフォルトに設定]をクリックします。
3. ウィンドウでの作業が完了したら、[OK]をクリックします。

UC500、Cisco 800シリーズルータを管理する場合

[デバイスアクセス]ウィンドウ

このウィンドウは、**設定 > デバイスプロパティ > デバイスアクセス** を選択した場合に表示されます。

まず、設定するデバイスを[ホスト名]リストから選択します。

Telnet を有効にするには、[Telnet]ボックスをオンにします。

注：Telnet が無効になっている場合、音声機能は設定できません。

SSH を有効にするには、[SSH]ボックスをオンにします。

CE520 スイッチを管理する場合

[トポロジオプション]ウィンドウ

このウィンドウは、[トポロジ]ビューのツールバー上で  を選択した場合に表示されます。このウィンドウを使用すると、[トポロジ]ビューに表示する項目を指定できます。

このウィンドウには、次のタブがあります。

- [隣接デバイスの表示]。表示する隣接デバイスを選択します。
- [情報の表示]。リンクおよびノードについて表示する情報を選択します。

- [VLANの表示]。コミュニティ内に VLAN リンクを表示して、VLAN リンクを表す色を選択します。

ウィンドウでの作業が完了したら、[OK]をクリックします。

[隣接デバイスの表示]

次のチェックボックスにより、表示する隣接デバイスを制御します。

- [IP Phones]:オンにすると、IP ネットワークを介して音声通信を提供するフル機能の電話が表示されます。
- [その他の隣接デバイス]:オンにすると、CDP で検出された隣接デバイスが表示されます。たとえば、Configuration Assistant にコミュニティ メンバとしてサポートされていないアクセス ポイントやデバイスなどです。

[情報の表示]

次のチェックボックスにより、トポロジ マップ上に表示する、リンクおよびノードの情報を制御します。

- [インターフェイスID]:オンにすると、リンクの接続先インターフェイスの ID が表示されます。
- [実質スピード]:オンにすると、リンクの管理上のスピードに対するものとして、リンクのスピード情報が表示されます。
- [ホスト名]:オンにすると、ノードのホスト名が表示されます。
- [IPアドレス]:オンにすると、ノードの IP アドレスが表示されます。
- [MACアドレス]:オンにすると、ノードの MAC アドレスが表示されます。
- [注釈]:オンにすると、リンクおよびノードの注釈が表示されます。

[VLANの表示]

トポロジ マップ上に VLAN リンクを表示するには、次の手順に従います。

1. [VLAN]フォルダで、リンクを強調表示する VLAN に対応する[色の割り当て]をクリックします。
2. [色の選択]ウィンドウで、使用する強調表示の色をクリックして、[OK]をクリックします。VLAN 番号が[VLAN]フォルダの上から強調表示の色を持つ VLAN のリストに移動します。[色の割り当て]ボタンが[色の修正]ボタンに変わり、選択した色が表示されます。
3. [トポロジ]ビューで VLAN 番号の横のチェックボックスをオンにして、強調表示の色をオンにします。後でチェックボックスをオフにすると、強調表示はオフになります。

注:

- VLAN の強調表示の色を変更するには、[色の修正]ボタンをクリックして[色の選択]ウィンドウで別の色を選択します。
- VLAN の強調表示を削除するには、[色の削除]ボタンをクリックします。VLAN の[色の修正]ボタンと[色の削除]ボタンが非表示になり、VLAN 番号が[色の割り当て]ボタンと共に[VLAN]フォルダに戻ります。

[ネットワークセキュリティの設定]ウィンドウ

このウィンドウは、次の場合に表示されます。

- [イベント通知]ウィンドウに、ネットワーク セキュリティの設定における競合が表示され、[解決]をクリックした場合。

ウィンドウのコンテンツは、ホストのアクセス セキュリティ レベルを[低]、[中]、または[高]のどれに設定したかに応じて変わります。

[イベント通知]ウィンドウでは、次のいずれかの理由によりこのウィンドウに移動します。

- Catalyst Express スイッチが同じセキュリティ レベルで設定されていない。競合を解決するには、セキュリティ レベルを[低]、[中]、または[高]に設定して[OK]をクリックします。
- MAC 認証テーブルに、承認に必要な MAC アドレスが記載されている。このタスクを実行するには、「ホスト レベル:[中]」を参照してください。
- Catalyst Express スイッチの RADIUS サーバの設定が同一ではない。この競合を解決するには、「ホスト レベル:[高]」を参照してください。

ホスト レベル:[低]

[低]レベルの場合、Configuration Assistant では次のセキュリティ機能が使用されます。

- **コミュニティ内におけるすべての Catalyst Express スイッチのブロードキャスト ストーム制御の有効化**

  ブロードキャスト ストーム制御は、ブロードキャスト パケットによるサブネットの転送とネットワーク パフォーマンスの低下を防ぎます。深刻なブロードキャスト ストームは、すべてのネットワーク トラフィックをブロックすることがあります。

- **コミュニティ内におけるすべての Catalyst Express スイッチのポート セキュリティ制御の有効化**

  ポート セキュリティ制御は、同時にポートにアクセスできる MAC アドレスの数を制限します。最大 MAC アドレス数は、ポートで設定される スマートポートロールに応じて変わります。この表には、スマートポートロールにより最大数がどのように変化するか示してあります。

スマートポートロール	MAC アドレスの最大数
[デスクトップ]	1
[IP Phone]	音声 VLAN が設定されている場合には 3、それ以外は 2
[アクセスポイント]	30
[スイッチ]	無制限
[ルータ]	無制限
[サーバ]	1

[ゲスト]	30
[診断]	無制限
[その他]	無制限

スマートポートの機能の詳細については、「ポートとデバイスのクイック設定」を参照してください。

ホスト レベル:[中]

[中]レベルでは、MAC 認証と呼ばれるセキュリティ機能が追加されます。つまり、デスクトップ、サーバ、プリンタ、IP Phone、アクセスポイント、スイッチ、またはルータが Catalyst Express スイッチ ポートを経由してコミュニティに接続されている場合、コミュニティへのアクセスが許可される前に、その MAC アドレスが MAC 認証テーブルに明示的に追加される必要があります。

次の場合に、MAC アドレスを MAC 認証テーブルに追加します。

- デバイスを Catalyst Express スイッチ上のポートに接続する。

  MAC アドレスを承認するには、[承認済]セルで[はい]を選択します。

- [MACアドレスの追加]をクリックし、[MACアドレスの追加]ウィンドウを使用します。

  追加された MAC アドレスは、必ず承認されます。

1 つまたは複数の MAC アドレスの承認を変更するには、該当する MAC アドレスを選択して[修正]をクリックし、[MACアドレスの修正]ウィンドウを使用します。MAC アドレスの[承認済]セルを編集することで、単一の MAC アドレスの承認を変更することもできます。

1 つまたは複数の MAC アドレスを削除するには、該当する MAC アドレスを選択して[削除]をクリックします。

ネットワーク内の Catalyst Express スイッチの MAC 認証テーブルは、同一である必要があります。同一でない場合、競合を解決するようプロンプトが表示されます。Network Assistant により、テーブルをマージするか、クリアすることができます。

ホスト レベル:[高]

[高]レベルは、Catalyst Express スイッチの 802.1x を設定します。802.1x とは、ネットワークにアクセスする際にユーザ名とパスワードの入力をホストに要求する、認証プロトコルです。入力されたユーザ名とパスワードは、承認されたユーザ名とパスワードが保存されている RADIUS サーバに転送されます。このウィンドウで RADIUS サーバを設定します。

注: 802.1x の認証は、デスクトップからのアクセス要求に対してのみ適用されます。

[高]レベルを使用すると、MAC 認証は必要なくなるので、オフにされます。

802.1x 認証を設定するには、次の手順に従います。

1. RADIUS サーバの IP アドレスを入力します。

2. Catalyst Express スイッチが RADIUS サーバと通信する際に使用する RADIUS キーを入力します。
3. RADIUS 認可に対する 0 から 65535 のUDP ポート番号を入力します。Cisco Secure ACS version 4.0 以降を稼動している場合には、デフォルトの UDP ポートは 1645 です。それ以前については、1812 です。

WLC526 を管理する場合

[ネットワークタイムサーバ]ウィンドウ

このウィンドウは、[システム時間]ウィンドウで [NTP]をクリックした場合に表示されます。

このウィンドウを使用して、Network Time Protocol（NTP; ネットワーク タイム プロトコル）クライアントから NTP サーバに定期的に Time-of-Day 要求が送信されるように設定できます。これによって、NTP サーバでは、デバイスから要求されたときに、クライアントのシステム クロックがサーバのクロックに同期されます。

セキュリティを強化するために、NTP 認証を設定できます。NTP 認証を設定すると、デバイスでは、サーバから正しい認証情報が提供されたときにだけ時刻が更新されるようになります。

NTP サーバからタイム更新を受け取るようにデバイスを設定し、NTP 認証を設定するには、[IPアドレス]フィールドにタイム サーバの IP アドレスを入力します。これは、このウィンドウ内で WLAN コントローラに適用される唯一のフィールドです。

[OK]をクリックし、[ネットワークタイムサーバ]ウィンドウを閉じて、[システム時間]ウィンドウに戻ります。

UC500、Cisco 800シリーズルータを管理する場合

[ネットワークタイムサーバ]ウィンドウ

このウィンドウは、[システム時間]ウィンドウで [NTP] をクリックした場合に表示されます。

このウィンドウを使用して、Network Time Protocol（NTP; ネットワーク タイム プロトコル）クライアントから NTP サーバに定期的に Time-of-Day 要求が送信されるように設定できます。これによって、NTP サーバでは、デバイスから要求されたときに、クライアントのシステム クロックがサーバのクロックに同期されます。

セキュリティを強化するために、NTP 認証を設定できます。NTP 認証を設定すると、デバイスでは、サーバから正しい認証情報が提供されたときにだけ時刻が更新されるようになります。

注：認証が正常に機能するように、まずサーバ管理者からキー情報を取得して、その情報を NTP 認証の各フィールドに入力する必要があります。

更新された時刻を NTP サーバから受信するようにデバイスを設定し、NTP 認証を設定するには、次の手順に従います。

1. [IPアドレス]フィールドで、タイム サーバの IP アドレスを入力します。
2. *オプション:* [キーID]フィールドに、サーバにパケットを送信するときに使用する認証キーを指定します。

   1 から 4294967295 の数値を入力します。

3. オプション: [キー値]フィールドに、秘密鍵を入力します。

   最大 32 文字の印刷可能文字を入力します。スペース、!、"、#、$、}、|、および ~ は使用できません。

4. オプション: [暗号タイプ]フィールドに、キー値の暗号化に使用する数値を入力します。

   1 から 4294967295 の数値を入力します。

5. [OK] をクリックし、[ネットワークタイムサーバ]ウィンドウを閉じて、[システム時間]ウィンドウに戻ります。

UC500、Cisco 800シリーズルータを管理する場合

[ネットワークの追加]ウィンドウ

このウィンドウは、[VPNサーバ]ウィンドウで[作成]([スプリットトンネリング])をクリックした場合に表示されます。

このウィンドウでは、VPN クライアントからのパケットがトンネリングされるサブネットワークを追加できます。

ネットワークを追加するには、次の手順に従います。

1. [ネットワーク]フィールドに、ネットワークの IP アドレスを入力します。
2. [サブネットマスク]フィールドに、サブネット マスクを入力します。
3. ウィンドウを閉じるには、[OK]をクリックします。

UC500、Cisco 800シリーズルータを管理する場合

[ファイアウォールとDMZ]ウィンドウ

[ホスト名]リストから、ファイアウォール(および、任意で非武装地帯)を有効にするデバイスを選択します。

[外部(信頼できない)インターフェイス]リストから外部インターフェイスを選択するか、[内部(信頼できる)インターフェイス]リストで内部インターフェイスのチェックボックスをオンにします。外部インターフェイスは WAN またはインターネットに接続します。内部インターフェイスは LAN に接続します。

注:

- 内部インターフェイスは複数選択できます。
- Cisco Configuration Assistant へのアクセスに使用するインターフェイスは、外部(信頼できない)インターフェイスとして選択しないでください。
- Cisco Configuration Assistant は、外部(信頼できない)インターフェイスからファイアウォールを介して起動することはできません。
- 内部インターフェイスまたは DMZ インターフェイスとしてすでに選択されている外部インターフェイスを選択すると、警告ダイアログが表示されます。
- DMZ インターフェイスとしてすでに選択されている内部インターフェイスを選択すると、警告ダイアログが表示されます。

[セキュリティレベル]スライダを適切なレベルに設定します。[セキュリティレベル]スライダは、インターフェイスを選択すると有効になります。[説明]領域に、各セキュリティ レベルのフィルタリング規則が表示されます。セキュリティ レベルは次のとおりです。

- [高]に設定すると、ネットワーク上でインスタント メッセージおよびポイントツーポイント アプリケーションを使用することはできません。ファイアウォールによって HTTP およびメール トラフィックが監視され、プロトコルに準拠していないトラフィックは破棄されます。ファイアウォールの内側で開始されたセッションの、他の Transmission Control Protocol(TCP)および User Datagram Protocol(UDP; ユーザ データグラム プロトコル)トラフィックは戻されます。
- [中]では、インスタント メッセージとポイントツーポイント アプリケーションの使用、および HTTP トラフィックとメール トラフィックが監視されます。ファイアウォールからは、ファイアウォールの内側で開始されたセッションの他の TCP および UPD トラフィックが戻されます。
- [低]では、アプリケーション トラフィックは監視されません。ファイアウォールからは、ファイアウォールの内側で開始されたセッションの他の TCP および UPD トラフィックが戻されます。

[DNSプライマリ]フィールドに、プライマリ Domain Name System(DNS; ドメイン ネーム システム)サーバの IP アドレスを入力します。注:デバイスに DNS が設定されている場合は、その DNS の IP アドレスが表示されるため、このフィールドには入力できません。[セキュリティレベル]スライダを[中]または[高]に設定した場合に、デバイスに DNS が設定されていないときは、DNS のプライマリ IP アドレスの入力が必要になります。

オプション:[DNSセカンダリ]フィールドに、セカンダリ DNS サーバの IP アドレスを入力します。

DMZ を作成するには、次の手順に従います。

1. [DMZインターフェイス]リストからインターフェイスを選択します。選択したインターフェイスが、ファイアウォールのインターフェイスとしても指定されている外部インターフェイスまたは内部インターフェイスである場合、警告ダイアログが表示されます。
2. [作成]をクリックし、[DMZサービスの作成]ウィンドウを使用します。

DMZ を削除するには、次の手順に従います。

1. IP アドレスを選択します。
2. [削除]をクリックします。確認のウィンドウが表示されます。
3. ウィンドウを閉じるには、[はい]をクリックします。

UC500、Cisco 800シリーズルータを管理する場合

[ファイアウォールとDMZ]ウィンドウ

このウィンドウは、**設定 > セキュリティ > ファイアウォールとDMZ** を選択した場合に表示されます。

[ホスト名]リストから、設定するデバイスを選択します。

このウィンドウには、次のタブがあります。

- [ファイアウォール]。ファイアウォールの作成または変更に使用します。
- [DMZ]。非武装地帯の作成または削除に使用します。

[ファイアウォール]

ファイアウォールの作成および変更には、同じ手順を使用します。

次の手順に従います。

1. [外部(信頼できない)インターフェイス]リストから外部インターフェイスを選択するか、[内部(信頼できる)インターフェイス]リストで内部インターフェイスのチェックボックスをオンにします。外部インターフェイスは WAN またはインターネットに接続します。内部インターフェイスは LAN に接続します。
    - 外部インターフェイスを選択した場合、[内部(信頼できる)インターフェイス]はグレー表示になります。
    - 内部インターフェイスは複数選択できます。
    - Cisco Configuration Assistant へのアクセスに使用するインターフェイスは、外部(信頼できない)インターフェイスとして選択しないでください。
    - Cisco Configuration Assistant は、外部(信頼できない)インターフェイスからファイアウォールを介して起動することはできません。
    - 内部インターフェイスまたは DMZ インターフェイスとしてすでに選択されている外部インターフェイスを選択すると、警告メッセージが表示されます。
    - DMZ インターフェイスとしてすでに選択されている内部インターフェイスを選択すると、警告メッセージが表示されます。
2. [セキュリティレベル]スライダを適切なレベルに設定します。[セキュリティレベル]スライダは、インターフェイスを選択すると有効になります。[説明]領域に、各セキュリティ レベルのフィルタリング規則が表示されます。
    - [高]に設定すると、ネットワーク上でインスタント メッセージおよびポイントツーポイント アプリケーションを使用することはできません。ファイアウォールによって HTTP およびメール トラフィックが監視され、セキュリティ プロトコルに準拠していないトラフィックは破棄されます。ファイアウォールの内側で開始されたセッションの、他の Transmission Control Protocol(TCP)および User Datagram Protocol(UDP; ユーザ データグラム プロトコル)トラフィックは戻されます。

- ［中］では、インスタント メッセージとポイントツーポイント アプリケーションの使用、および HTTP トラフィックとメール トラフィックが監視されます。ファイアウォールからは、ファイアウォールの内側で開始されたセッションの他の TCP および UPD トラフィックが戻されます。
- ［低］では、アプリケーション トラフィックは監視されません。ファイアウォールからは、ファイアウォールの内側で開始されたセッションの他の TCP および UPD トラフィックが戻されます。

3. ［DNSプライマリ］フィールドに、プライマリ Domain Name System（DNS; ドメイン ネーム システム）サーバの IP アドレスを入力します。注：デバイスに DNS が設定されている場合は、その DNS の IP アドレスが表示されるため、このフィールドには入力できません。［セキュリティレベル］スライダを［中］または［高］に設定した場合に、デバイスに DNS が設定されていないときは、DNS のプライマリ IP アドレスの入力が必要になります。
4. オプション：［DNSセカンダリ］フィールドに、セカンダリ DNS サーバの IP アドレスを入力します。

［DMZ］

DMZ を作成するには、次の手順に従います。

1. ［DMZインターフェイス］メニューからインターフェイスを選択します。選択したインターフェイスが、ファイアウォールのインターフェイスとしても指定されている外部インターフェイスまたは内部インターフェイスである場合、警告ダイアログが表示されます。
2. ［作成］をクリックし、［DMZサービスの作成］ウィンドウを使用します。
3. ウィンドウを閉じて変更を保存するには、［OK］をクリックします。

DMZ を削除するには、次の手順に従います。

1. IP アドレスを選択します。
2. ［削除］をクリックします。確認のウィンドウが表示されます。
3. ウィンドウを閉じるには、［はい］をクリックします。
4. ウィンドウを閉じて変更を保存するには、［ファイアウォールとDMZ］ウィンドウで［OK］をクリックします。

UC500 を管理する場合

［ファイル管理］ウィンドウ

このウィンドウは、機能バー上で **メンテナンス > ファイル管理** を選択した場合に表示されます。

次の表は、［概要］タブの各カラムについて説明しています。

カラム	説明
デバイス/ファイルシステム	すべてのデバイスと、それらのデバイス上にあるすべてのファイルシステムが一覧表示されます。

ステータス	ファイルシステムのステータスは、次のいずれかになります。 • なし:レポートするステータスがありません。 • [ファイルシステムは使用中です]:ファイルシステムの情報は使用できません。[更新]をクリックして、もう一度やり直してください。 • [ファイルシステムは一杯です]:ファイルシステムが満杯の状態です。空き容量の割合は 0 % です。 • [ファイルシステムは空です]:ファイルシステム内にファイルはありません。 • [ファイルシステムは読み取り専用です]:ファイルシステムはロックされており、変更できません。これは通常、コンパクト フラッシュ カードの物理スイッチ設定が原因です。
容量	ファイルシステムのサイズを最も近いメガバイト(MB)数に丸めた値です。
空き容量	ファイルシステムの空き容量を最も近い MB 数に丸めた値です。
空き容量の割合	ファイルシステムの合計容量に対する未使用率
ファイル数	ファイルシステム上のファイル数。ディレクトリおよび削除されたファイルは、ファイルとしてカウントされます。

次の表は、[ファイル数]タブの各カラムについて説明しています。

カラム	**説明**
デバイス/ファイルシステム	すべてのデバイスと、それらのデバイス上にあるすべてのファイルシステムが一覧表示されます。各ファイルシステム下には、ディレクトリおよびファイルのリストがあります。
圧縮	デバイスのクラス B ファイルシステムに削除ファイルがある場合にだけ表示されます。
サイズ	個々のファイルのサイズをキロバイト(KB)で示します。
タイプ	各ファイルのファイル タイプを一覧表示します(表示可能な場合)。一般的なファイル タイプには、システム ブート イメージ、Cisco IOS イメージ、設定などがあります。
修正日時	ファイルの変更日時を一覧表示します。
削除	ボックスをオンにして、削除するファイルを選択します。
復元	クラス B ファイルシステムに削除ファイルがあるデバイスの場合に表示されます。

ファイルを削除するには、次の手順に従います。

1. 削除するファイルと同じ行にあるボックスをオンにします。
2. [適用]をクリックします。
3. [更新]をクリックして、ファイルが削除されたことを確認します。
4. [OK]をクリックします。

注：vlan.dat、config.txt、env_vars、private_config.txt、および system_env_vars の各ファイルは削除しないでください。

UC500、Cisco 800シリーズルータを管理する場合

[ファイル管理]ウィンドウ

このウィンドウは、機能バーで **メンテナンス > ファイル管理** を選択した場合に表示されます。

次の表は、[概要]タブの各カラムについて説明しています。

カラム	説明
デバイス/ファイルシステム	選択されたデバイスおよびそのデバイス上のファイルシステムを一覧表示します。
ステータス	ファイルシステムのステータスは、次のいずれかになります。 • なし：レポートするステータスがありません。 • [圧縮が必要です]：クラス B ファイルシステム上に削除ファイルがあります。 • [圧縮中]：削除を指示されたファイルを消去中です。 • [ファイルシステムは使用中です]：ファイルシステムの情報は使用できません。[更新]をクリックして、もう一度やり直してください。 • [ファイルシステムは一杯です]：ファイルシステムに空き容量はありません。 • [ファイルシステムは空です]：ファイルシステム内にファイルはありません。 • [ファイルシステムは読み取り専用です]：ファイルシステムはロックされており、変更できません。これは通常、コンパクト フラッシュ カードの物理スイッチ設定が原因です。
容量	ファイルシステムのサイズを最も近いメガバイト（MB）数に丸めた値です。
空き容量	ファイルシステムの空き容量を最も近い MB 数に丸めた値です。
空き容量の割合	ファイルシステムの合計容量に対する未使用率
ファイル数	ファイルシステム上のファイル数。クラス C ファイルシステム上のディレクトリおよびクラス B ファイルシステム上の削除ファイルがファイル数に含まれます。

次の表は、[ファイル数]タブの各カラムについて説明しています。

カラム	説明
デバイス/ファイル	選択されたデバイスおよびそのデバイス上のファイルシステムを一覧表示します。各ファイルシステム下には、ディレクトリおよびファイルのリストがあります。

システム	
圧縮	デバイスのクラス B ファイルシステムに削除ファイルがある場合にだけ表示されます。ファイルシステムから削除ファイルを永久に削除する場合、ボックスをオンにします。このチェックボックスは、ファイルシステムが読み取り専用の場合、またはファイルシステムに削除ファイルがない場合は、使用できません。
サイズ	各ファイルのサイズを KB で一覧表示します。
タイプ	各ファイルのファイル タイプを一覧表示します（表示可能な場合）。一般的なファイル タイプには、システム イメージ ファイル、IOS イメージ ファイル、設定ファイルが含まれます。
修正日時	ファイルの変更日時を一覧表示します。
削除	ボックスをオンにして、削除するファイルを選択します。ファイルがクラス B ファイルシステム内にあり、ファイルがすでに削除指定されている場合、ボックスにはすでにオンになっています。
復元	クラス B ファイルシステムに削除ファイルがあるデバイスの場合にだけ表示されます。ボックスをオンにして、削除しないファイルを選択します。

ファイルを削除するには、次の手順に従います。

1. 削除するファイルと同じ行にあるボックスをオンにします。
2. ［適用］をクリックします。
3. クラス B ファイルシステムからファイルを永久に削除する場合は、そのファイルが保存されているファイルシステムで圧縮操作を実行します。

注：システム ブート イメージまたは vlan.dat、config.txt、env_vars、private_config.txt、および system_env_vars のいずれかのファイルを削除しないでください。

圧縮操作がまだ最終的には削除していないファイルを復元するには、次の手順に従います。

1. 復元するファイルと同じ行にあるボックスをオンにします。
2. ［適用］をクリックします。

クラス B ファイルシステムを圧縮するには、次の手順に従います。

1. 圧縮するファイルシステムと同じ行にあるボックスをオンにします。
2. ［適用］をクリックします。

ファイルシステムを圧縮する際、ファイルが復元指定されたファイルシステム内にある場合、それらのファイルは圧縮操作前に復元されます。削除指定されたファイルがある場合、それらのファイルは圧縮操作前に削除されます。圧縮操作に数分かかる場合があります。

CE520 スイッチを管理する場合

[フィルタエディタ]ウィンドウ

このウィンドウは、テーブルを含む Configuration Assistant のウィンドウまたはウィザードで[フィルタ]をクリックした場合に表示されます。テーブルのカラム名が、このウィンドウのフィールド名になります。テーブルの行をフィルタリングする選択基準をフィールドに入力して必要な行だけを残します。

次の手順に従います。

1. 対応するテーブル カラムをフィルタリングしない場合、つまり、そのカラムに選択基準を指定しない場合は、フィールドは空白のままにします。
2. ドロップダウン リストのあるフィールドを使用する場合は、対応するカラムのエントリと照合する項目を選択します。
3. テキスト入力フィールドを使用する場合は、対応するカラムのエントリと照合する文字列を入力します。任意の長さの文字列の場合は、プレースホルダとしてアスタリスク(*)を使用します。任意の 1 文字の場合は、プレースホルダとして疑問符(?)を使用します。文字列に先行するか続くかにかかわらず特定の文字列と照合する場合は、「**文字列**」と入力します。

   例:

   - [LREソフトウェアアップグレード]ウィンドウでアップグレードに対して有効になっているインターフェイスだけを表示するには、[LREソフトウェアアップグレード]ウィンドウに作用する、[フィルタエディタ]ウィンドウ の[アップグレード]フィールドで、[有効にする]を選択します。
   - [ポート設定]ウィンドウで文字列「1234」を含む説明だけを表示するには、[ポート設定]ウィンドウに作用する、[フィルタエディタ]ウィンドウ の[説明]フィールドに「***1234***」と入力します。
4. [OK]をクリックします。使用していた Configuration Assistant のウィンドウまたはウィザードに戻ると、要求した情報のサブセットが表示されます。

AP521 を管理する場合

[変換ステータス]ウィンドウ

このウィンドウは、[LAPに変換]ウィンドウで 1 つまたは複数の自律型アクセスポイントを選択し、[ステータス]をクリックした場合に表示されます。このウィンドウには、変換中に自律型アクセスポイントから詳細メッセージが生成された場合にそれらのメッセージが表示されます。

次の表は、変換のステータスのメッセージについて説明しています。

メッセージ	説明
[続行するには、[変換の設定]ボタンをクリックします。]	デバイスを変換するには、[変換の設定]ウィンドウに情報を入力する必要があります。
[デバイスを変換するには、[変換]ボタンをクリックしま	デバイスの変換に必要なすべてのパラメータがデバイスに設定されました。

す。]	
[フラッシュの合計サイズを決定しています。]	デバイスの変換に使用できる十分な空き容量があるかどうかを、変換プロセスが確認しています。
[tarイメージファイルの情報ファイルを抽出しています。]	Cisco IOS イメージ tar ファイルから info ファイルが抽出されています。
[tarイメージファイルの情報ファイルを読み取っています。]	Cisco IOS イメージに関する詳細を確認するため、Cisco IOS イメージ tar ファイルの info ファイルが読み込まれています。
[デバイスのリロードを開始しました。]	正常に変換された後にデバイスがリロードされています。リロードが完了した後でも、ウィンドウをリフレッシュするまでこのメッセージは表示されます。
[デバイスの変換が正常に実行されました。]	変換は正常に完了しました。
[デバイスの変換に失敗しました。]	変換は失敗しました。詳細は[詳細]ウィンドウを参照してください。
[デバイス変換の処理中です。]	デバイスの変換を実行中です。
[デバイスの変換がキャンセルされました。]	変換がキャンセルされました。
[イメージをアップロードしています。]	イメージがデバイスにアップロードされています。
[IOSイメージの検証中]	デバイスでイメージを検証しています。

新しいイメージをインストールするための十分な容量がデバイスにない場合、[ファイル管理]ウィンドウへのリンクとともにメッセージが表示されます。[ファイル管理]ウィンドウを使用すると、ファイルシステムを管理できます。また、新しいイメージに使用する容量を確保するために必要に応じて古いイメージを削除できます。

ウィンドウでの作業が完了したら、[OK]をクリックします。

AP521 を管理する場合

[変換の設定]ウィンドウ

このウィンドウは、[LAPに変換]ウィンドウで 1 つまたは複数の自律型アクセスポイントを選択し、[変換の設定]をクリックした場合に表示されます。

変換後に WLAN コントローラで新しい IP アドレスをライトウェイト アクセスポイントに割り当てる場合は、[DHCP IPアドレス]を選択します。

変換後にライトウェイト アクセスポイントで同じホスト名をそのまま使用する場合は、[ホスト名の保持]を選択します。

[モード]リストで、ローカルに保存されている変換イメージを使用する場合は[標準]を選択し、それ以外の場合は[リモートTFTPサーバ]を選択します。

[標準]を選択した場合は、[変換イメージ]フィールドに変換イメージのファイル名を入力します。[参照]をクリックすると、ファイルを参照できます。

[リモートTFTPサーバ]を選択した場合:

1. [変換イメージ]フィールドに、変換イメージのフル パスとファイル名を入力します。
2. [TFTPサーバIPアドレス]フィールドに、TFTP サーバの IP アドレスを入力します。

   注: 複数デバイスを一度に変換するには、TFTP サーバが複数の要求およびセッションを同時に処理できる必要があります。

[ドメイン名]フィールドに、ドメインの名前を入力します。

[DNS IPアドレス]フィールドに、DNS アドレスを入力します。

[OK]をクリックして設定を保存します。設定値が[LAPに変換]ウィンドウに表示されます。

UC500 を管理する場合

[ポート設定]ウィンドウ

このウィンドウは、次のいずれかの処理を実行した場合に表示されます。

- 機能バー上で **設定 > ポート > ポート設定** を選択する。
- ツールバー上で  をクリックする。

まず、[ホスト名]リストからデバイスを選択します。デバイスのポートに関する情報が、次のタブに表示されます。

- [コンフィギュレーション設定]。管理者が設定および変更できる値が表示されます。
- [ランタイム ステータス]。ポートの実際のステータスが表示されます。

いずれかのタブの情報のサブセットを表示するには、[フィルタ]をクリックして[フィルタエディタ]ウィンドウを使用します。

[コンフィギュレーション設定]

次の表は、このタブに表示される情報について説明しています。

設定	説明
[説明]	ポートについての説明テキスト。複数のポートの説明を表示する場合は、[ポート設定] ウィンドウの[説明の記入]をクリックします。 「?」および「/」の文字を使用することはできません。 複数のポートを選択した場合は、このフィールドは使用できません。
[ステータス]	ポートを有効または無効にする設定。この設定は、実行時の設定とは異なる場合があります。たとえば、ポートに接続されているデバイスがない場合、このポートをランタイム ステータスが DOWN の状態で、管理上有効にできます。 無効になっているポートで他の設定を変更した場合、このポートを有効にするまでそれらの変更は適用されません。 ポートを無効にした場合、SNMP マネージャを設定していれば、linkdown トラップが管理ステーションに送信されます。
[デュプレックス]	デュプレックスの設定:[全二重]、[半二重]、または[自動]。ギガビット イーサネットおよびギガスタック GBIC ポートのデフォルト設定は[自動]です。これらのポートは、接続されているデバイスのデュプレックス機能に自動的に適合します。 デュプレックスの値を[自動]以外に設定するには、スピードの値が[auto]以外である必要があります。ポートのスピードが[auto]に設定されていて、ポートがスピード 1000Mbps で動作可能な場合、デュプレックスの値は、[自動]である必要があります。 ギガスタック GBIC スタック接続は、半二重モードで動作します。 ポイントツーポイント ギガスタック GBIC ポート接続は、全二重モードで動作します。
[スピード]	10/100-Mbps および 10/100/1000-Mbps ポートの設定: • [10](ポートは強制スピード 10Mbps で動作します) • [100](ポートは強制スピード 100Mbps で動作します) • [1000](ポートは強制スピード 1000Mbps で動作します) • [auto](ポートはすべての利用可能スピードを自動ネゴシエートし通告します) • [auto 10](ポートはリンクの他端に対して 10Mbps のスピードを自動ネゴシエートし通告します) • [auto 100](ポートはリンクの他端に対して 100Mbps のスピードを自動ネゴシエートし通告します) • [auto 100 1000](ポートはリンクの他端に対して 100 および 1000Mbps のスピードを自動ネゴシエートし通告します) • [auto 10 1000](ポートはリンクの他端に対して 10 および 1000Mbps のスピードを自動ネゴシエートし通告します) • [auto 1000](ポートはリンクの他端に対して 1000Mbps のスピードを自動ネゴシ

	エートし通告します） • ［auto 10 100］（ポートはリンクの他端に対して 10 および 100Mbps のスピードを自動ネゴシエートし通告します） • ［auto 10 100 1000］（ポートはリンクの他端に対して 10、100、および 1000Mbps のスピードを自動ネゴシエートし通告します） 10/100-Mbps および 10/100/1000-Mbps ポートのデフォルト設定は［auto］です。イーサネット ポートは、接続デバイスの伝送スピードに自動的に適合します。 **注**：次のポートのスピード設定を変更することはできません。 • 1000BASE-T、SX、LX/LH、ZX、DWDM、および CWDM GBIC • 1000BASE-SX、LX/LH、ZX、および CWDM SFP • XENPAK-10GB-LR、ER、CX4、SR、および LX4 • 100BASE-FX
［電力］	Catalyst Express 500 PoE スイッチ上の単一ポートの場合。ポートを使用して電源デバイスを検出し、それに給電する場合は、［自動］を選択します。それ以外の場合は、［never］を選択します。

このタブの変更、変更を加えるコマンドのプレビュー、およびコマンドを実行するには、次の手順に従います。

ポート設定の変更

ポートの設定を個別に変更するには、変更するポートに対応するセルをクリックします。

1 つ以上のポートの設定を変更するには、次の手順に従います。

1. ［インターフェイス］カラムでポートを選択します。

   Ctrl キーを押しながら各ポートを選択していくか、Shift キーを押しながら範囲の最初と最後のポートを選択します。

2. ［修正］をクリックして、［ポート設定の修正］ウィンドウを表示します。
3. 必要な変更を行います。
4. ［OK］をクリックしてウィンドウを閉じます。新しい設定が［ポート設定］ウィンドウに表示されます。

複数のポートを選択して、選択したいずれかのポートに有効ではない設定を指定すると、現在の設定が変更されないまま維持されます。たとえば、10BaseT イーサネット ポート、ファスト イーサネット ポート、およびギガビット ポートを選択した場合に、100Mbps のスピードを指定すると、10BaseT イーサネット ポートの設定は 10Mbps のまま、ギガビット ポートの設定は 1000Mbps のまま維持されます。

ポート説明の変更

ポートの説明を追加または変更するには、次の手順に従います。

1 つまたは複数のポートを選択します。ポートを 1 つだけ選択する場合は、そのポートの［説明］カラムのセルをクリックします。カーソルが点滅している場所にテキストを入力します。

複数のポートを選択する場合は、次の手順に従います。

1. ［説明の記入］をクリックして、［基本的なポートの説明］ウィンドウを表示します。
2. 必要な変更を行います。

   注 : ［基本的なポートの説明］ウィンドウからポートの説明の詳細ウィンドウに移動して、自動増分を最大 3 つの説明に対して指定できます。

3. ［OK］をクリックしてウィンドウを閉じます。

［ランタイム ステータス］

次の表は、このタブに表示される読み取り専用の情報について説明しています。

カラム	説明
インターフェイス	ポートを特定します。ファスト イーサネット、ギガビット イーサネット、または FDDI、モジュールまたはスロット番号（0、1、または 2）、およびポート番号。
説明	インターフェイスの説明。
イーサネットリンク	ポートの状態。ポートの状態が、［up］、［down］、または［administratively down］のいずれかで示されます。
デュプレックス	ポートのデュプレックス状態。
スピード	ポートのスピード。 ギガビット イーサネット ポートの場合、このフィールドは読み取り専用で、［1000］（1000Mbps）と表示されます。
状態	インライン パワーが接続デバイスに供給されているかどうかを示します。
割り当て	接続デバイスに割り当てられた電力量。
デバイス	インターフェイスからインライン パワーを受電しているデバイスのタイプを示します。
クラス	電力供給されるデバイスの IEEE 分類。電力供給されるデバイスの多くで、PoE で使用可能な 15.4W のフル電力を必要としません。 電力クラスの範囲は 0 から 4 で、デフォルトは 0 です。スイッチに割り当てられる電力量は、IEEE クラスによって異なります。

CE520 スイッチを管理する場合

［ポート設定］ウィンドウ

このウィンドウは、次のいずれかの処理を実行した場合に表示されます。

- 機能バー上で **設定 > ポート > ポート設定** を選択する。

- ツールバー上で  をクリックする。

まず、[ホスト名]リストからデバイスを選択します。デバイスのポートに関する情報が、次のタブに表示されます。

- [コンフィギュレーション設定]。管理者が設定および変更できる値が表示されます。
- [ランタイム ステータス]。ポートの実際のステータスが表示されます。

いずれかのタブの情報のサブセットを表示するには、[フィルタ]をクリックして[フィルタエディタ]ウィンドウを使用します。

[コンフィギュレーション設定]

次の表は、このタブに表示される情報について説明しています。

設定	説明
[説明]	ポートについての説明テキスト。複数のポートの説明を表示する場合は、[ポート設定]ウィンドウの[説明の記入]をクリックします。 「?」および「/」の文字を使用することはできません。 複数のポートを選択した場合は、このフィールドは使用できません。
[ステータス]	ポートを有効または無効にする設定。この設定は、実行時の設定とは異なる場合があります。たとえば、ポートに接続されているデバイスがない場合、このポートをランタイム ステータスが DOWN の状態で、管理上有効にできます。 無効になっているポートで他の設定を変更した場合、このポートを有効にするまでそれらの変更は適用されません。 ポートを無効にした場合、SNMP マネージャを設定していれば、linkdown トラップが管理ステーションに送信されます。
[デュプレックス]	デュプレックスの設定:[全二重]、[半二重]、または[自動]。ギガビット イーサネットおよびギガスタック GBIC ポートのデフォルト設定は[自動]です。これらのポートは、接続されているデバイスのデュプレックス機能に自動的に適合します。 デュプレックスの値を[自動]以外に設定するには、スピードの値が[auto]以外である必要があります。ポートのスピードが[auto]に設定されていて、ポートがスピード 1000Mbps で動作可能な場合、デュプレックスの値は、[自動]である必要があります。 ギガスタック GBIC スタック接続は、半二重モードで動作します。 ポイントツーポイント ギガスタック GBIC ポート接続は、全二重モードで動作します。
[スピード]	10/100-Mbps および 10/100/1000-Mbps ポートの設定: • [10](ポートは強制スピード 10Mbps で動作します)

	• [100]（ポートは強制スピード 100Mbps で動作します） • [1000]（ポートは強制スピード 1000Mbps で動作します） • [auto]（ポートはすべての利用可能スピードを自動ネゴシエートし通告します） • [auto 10]（ポートはリンクの他端に対して 10Mbps のスピードを自動ネゴシエートし通告します） • [auto 100]（ポートはリンクの他端に対して 100Mbps のスピードを自動ネゴシエートし通告します） • [auto 100 1000]（ポートはリンクの他端に対して 100 および 1000Mbps のスピードを自動ネゴシエートし通告します） • [auto 10 1000]（ポートはリンクの他端に対して 10 および 1000Mbps のスピードを自動ネゴシエートし通告します） • [auto 1000]（ポートはリンクの他端に対して 1000Mbps のスピードを自動ネゴシエートし通告します） • [auto 10 100]（ポートはリンクの他端に対して 10 および 100Mbps のスピードを自動ネゴシエートし通告します） • [auto 10 100 1000]（ポートはリンクの他端に対して 10、100、および 1000Mbps のスピードを自動ネゴシエートし通告します） 10/100-Mbps および 10/100/1000-Mbps ポートのデフォルト設定は[auto]です。イーサネット ポートは、接続デバイスの伝送スピードに自動的に適合します。 **注**：次のポートのスピード設定を変更することはできません。 • 1000BASE-T、SX、LX/LH、ZX、DWDM、および CWDM GBIC • 1000BASE-SX、LX/LH、ZX、および CWDM SFP • XENPAK-10GB-LR、ER、CX4、SR、および LX4 • 100BASE-FX
[電力]	Catalyst Express 500 PoE スイッチ上の単一ポートの場合。ポートを使用して電源デバイスを検出し、それに給電する場合は、[自動]を選択します。それ以外の場合は、[never]を選択します。
[自動 MDIX]	Automatic Medium-Dependent Interface Crossover（自動 MDIX）は、必要なケーブル接続の種類（ストレートスルーまたはクロスオーバー）を自動的に検出し、接続を適切に設定します。この設定が有効になっている場合、どちらかの種類のケーブルを使用でき、インターフェイスによって正しいケーブルの種類が自動的に選択されます。自動 MDIX が正しく機能するためには、インターフェイスのスピードを[auto]、[auto 10]、[auto 100]、[auto 1000]、[auto 10 100]、[auto 10 1000]、[auto 100 100]、または[auto 10 100 1000] に設定する必要があります。デュプレックス設定も[自動] にする必要があります。 ポートの自動 MDIX を有効にするには、[on] を選択します。ポートの自動 MDIX を無効にするには、[off]を選択します。 **注**：自動 MDIX は、1000 BASE-SX または 1000 BASE-LX SFP インターフェイスではサポートされません。

このタブの変更、変更を加えるコマンドのプレビュー、およびコマンドを実行するには、次の手順に従います。

ポート設定の変更

ポートの設定を個別に変更するには、変更するポートに対応するセルをクリックします。

1 つ以上のポートの設定を変更するには、次の手順に従います。

1. [インターフェイス]カラムでポートを選択します。

   Ctrl キーを押しながら各ポートを選択していくか、Shift キーを押しながら範囲の最初と最後のポートを選択します。

2. [修正]をクリックして、[ポート設定の修正]ウィンドウを表示します。
3. 必要な変更を行います。
4. [OK]をクリックしてウィンドウを閉じます。新しい設定が[ポート設定]ウィンドウに表示されます。

複数のポートを選択して、選択したいずれかのポートに有効ではない設定を指定すると、現在の設定が変更されないまま維持されます。たとえば、10BaseT イーサネット ポート、ファスト イーサネット ポート、およびギガビット ポートを選択した場合に、100Mbps のスピードを指定すると、10BaseT イーサネット ポートの設定は 10Mbps のまま、ギガビット ポートの設定は 1000Mbps のまま維持されます。

ポート説明の変更

ポートの説明を追加または変更するには、次の手順に従います。

1 つまたは複数のポートを選択します。ポートを 1 つだけ選択する場合は、そのポートの[説明]カラムのセルをクリックします。カーソルが点滅している場所にテキストを入力します。

複数のポートを選択する場合は、次の手順に従います。

1. [説明の記入]をクリックして、[基本的なポートの説明]ウィンドウを表示します。
2. 必要な変更を行います。

   注 : [基本的なポートの説明]ウィンドウからポートの説明の詳細ウィンドウに移動して、自動増分を最大 3 つの説明に対して指定できます。

3. [OK]をクリックしてウィンドウを閉じます。

[ランタイム ステータス]

次の表は、このタブに表示される読み取り専用の情報について説明しています。

カラム	説明
インターフェイス	ポートを特定します。ファスト イーサネット、ギガビット イーサネット、または FDDI、モジュールまたはスロット番号(0、1、または 2)、およびポート番号。
説明	インターフェイスの説明。

イーサネットリンク	ポートの状態。ポートの状態が、[up]、[down]、または[administratively down]のいずれかで示されます。
デュプレックス	ポートのデュプレックス状態。
スピード	ポートのスピード。 ギガビット イーサネット ポートの場合、このフィールドは読み取り専用で、[1000]（1000Mbps）と表示されます。
状態[1]	インライン パワーが接続デバイスに供給されているかどうかを示します。
割り当て[1]	接続デバイスに割り当てられた電力量。
デバイス[1]	インターフェイスからインライン パワーを受電しているデバイスのタイプを示します。
クラス[1]	電力供給されるデバイスの IEEE 分類。電力供給されるデバイスの多くで、PoE で使用可能な 15.4W のフル電力を必要としません。 電力クラスの範囲は 0 から 4 で、デフォルトは 0 です。スイッチに割り当てられる電力量は、IEEE クラスによって異なります。

[1]Catalyst Express PoE スイッチの場合に表示されます。

UC500 を管理する場合

[ポート設定の修正]ウィンドウ

このウィンドウは、次の場合に表示されます。

- [ポート設定]ウィンドウでポートを選択し、[修正]をクリックする。
- [前面パネル]ビューでポートを選択し、左クリックして、ポップアップ ウィンドウから[ポート設定]をクリックする。

  注：[前面パネル]ビューで複数のデバイスのポートを選択した場合は、[ポート設定の修正]ウィンドウに、変更の必要があるオプションが表示されない場合があります。このような設定を表示するには、機能バー上の **設定 > ポート > ポート設定** を選択してください。[ポート設定]ウィンドウで[修正]をクリックすると、これらの設定を変更できます。

ポート設定を変更するには、次の手順に従います。

1. [説明]フィールドに、選択したポートの説明を入力します。「?」および「/」の文字を使用することはできません。

   説明にはポートの識別に役立つ情報を入力します。たとえば、「end stations」などと入力すると、わかりやすく便利です。入力した説明の 18 文字までが表示されます。

2. 残りのパラメータ設定をドロップダウン リストから選択します。詳細については、「設定表」を参照してください。

3. ［OK］をクリックして、変更内容を確定し、ウィンドウを閉じます。

   新しい設定が［ポート設定］ウィンドウに表示されます。

複数のポートを選択して、選択したいずれかのポートに有効ではない設定を指定すると、現在の設定が変更されないまま維持されます。たとえば、10Base-T イーサネット ポート、ファスト イーサネット ポート、およびギガビット ポートを選択した場合に、100 Mbps のスピードを指定すると、10Base-T イーサネット ポートの設定は 10 Mbps のまま、ギガビット ポートの設定は 1000 Mbps のまま維持されます。

設定表

設定	説明
［説明］	ポートについての説明テキスト。（ポートを複数選択した場合は、このフィールドは無効になっています。複数のポートの説明を表示する場合は、［ポート設定］ウィンドウの［説明の記入］をクリックします。
［ステータス］	ポートを有効または無効にする設定。この設定は、実行時の設定とは異なる場合があります。たとえば、ポートに接続されているデバイスがない場合、このポートをランタイム ステータスがダウンの状態で、管理上有効にできます。 無効のポートで他の設定を変更した場合、このポートを有効にするまでそれらの変更は適用されません。 ポートを無効にした場合、SNMP マネージャを設定していれば、リンクダウン トラップが管理ステーションに送信されます。
［デュプレックス］	デュプレックスの設定：全二重、半二重、または auto。ギガビット イーサネット および ギガスタック GBIC ポートのデフォルト設定は auto です。これらのポートは、接続されているデバイスのデュプレックス機能に自動的に適合します。 ギガスタック GBIC スタック接続は、半二重モードで動作します。 ポイントツーポイント ギガスタック GBIC ポート接続は、全二重モードで動作します。 ギガビットおよび 10 GB イーサネット ポートは、接続デバイスのデュプレックス機能に自動的に適合します。これらのポートのデュプレックス設定（auto）を変更することができます。
［スピード］	10/100-Mbps および 10/100/1000-Mbps ポートの設定： • *10*（ポートは強制スピード 10Mbps で動作します） • *100*（ポートは強制スピード 100Mbps で動作します） • *1000*（ポートは強制スピード 1000Mbps で動作します） • *auto*（ポートはすべての利用可能スピードを自動的にネゴシエートし通告します） • *auto 10*（ポートはリンクの他端に対して 10Mbps のスピードを自動ネゴシエートし通告します）

	• *auto 100*(ポートはリンクの他端に対して 100Mbps のスピードを自動ネゴシエートし通告します) • *auto 100 1000*(ポートはリンクの他端に対して 100 および 1000Mbps のスピードを自動ネゴシエートし通告します) • *auto 10 1000*(ポートはリンクの他端に対して 10 および 1000Mbps のスピードを自動ネゴシエートし通告します) • *auto 1000*(ポートはリンクの他端に対して 1000Mbps のスピードを自動ネゴシエートし通告します) • *auto 10 100*(ポートはリンクの他端に対して 10 および 100Mbps のスピードを自動ネゴシエートし通告します) • *auto 10 100 1000*(ポートはリンクの他端に対して 10、100、および 1000Mbps のスピードを自動ネゴシエートし通告します) 10/100-Mbps および 10/100/1000-Mbps ポートのデフォルト設定は auto です。イーサネット ポートは、接続デバイスの伝送スピードに自動的に適合します。 **注**:次のポートのスピード設定を変更することはできません: • 1000BASE-T、SX、LX/LH、ZX、DWDM、および CWDM GBIC • 1000BASE-SX、LX/LH、ZX、および CWDM SFP • XENPAK-10GB-LR、ER、CX4、SR、および LX4 • 100BASE-FX
[電力]	Unified Communications 500 シリーズ プラットフォーム上の単一ポートの場合。ポートを使用して電源デバイスを検出し、それに給電する場合は、[auto]を選択します。それ以外の場合は、[never]を選択します。

CE520 スイッチを管理する場合

[ポート設定の修正]ウィンドウ

このウィンドウは、次の場合に表示されます。

- [ポート設定]ウィンドウでポートを選択し、[修正]をクリックする。
- [前面パネル]ビューでポートを選択し、左クリックして、ポップアップ ウィンドウから[ポート設定]をクリックする。

  注:[前面パネル]ビューで複数のデバイスのポートを選択した場合は、[ポート設定の修正]ウィンドウに、変更の必要があるオプションが表示されない場合があります。このような設定を表示するには、機能バー上の **設定 > ポート > ポート設定** を選択してください。[ポート設定]ウィンドウで[修正]をクリックすると、これらの設定を変更できます。

ポート設定を変更するには、次の手順に従います。

1. [説明]フィールドに、選択したポートの説明を入力します。「?」および「/」の文字を使用することはできません。

説明にはポートの識別に役立つ情報を入力します。たとえば、「end stations」などと入力すると、わかりやすく便利です。入力した説明の 18 文字までが表示されます。

2. 残りのパラメータ設定をドロップダウン リストから選択します。詳細については、「設定表」を参照してください。
3. [OK]をクリックして、変更内容を確定し、ウィンドウを閉じます。

   新しい設定が[ポート設定]ウィンドウに表示されます。

複数のポートを選択して、選択したいずれかのポートに有効ではない設定を指定すると、現在の設定が変更されないまま維持されます。たとえば、10Base-T イーサネット ポート、ファスト イーサネット ポート、およびギガビット ポートを選択した場合に、100Mbps のスピードを指定すると、10Base-T イーサネット ポートの設定は 10Mbps のまま、ギガビット ポートの設定は 1000Mbps のまま維持されます。

設定表

設定	説明
[説明]	ポートについての説明テキスト(ポートを複数選択した場合は、このフィールドは無効になっています複数のポートの説明を表示する場合は、[ポート設定]ウィンドウの[説明の記入]をクリックします)。
[ステータス]	ポートを有効または無効にする設定。この設定は、実行時の設定とは異なる場合があります。たとえば、ポートに接続されているデバイスがない場合、このポートをランタイム ステータスが DOWN の状態で、管理上有効にできます。 無効になっているポートで他の設定を変更した場合、このポートを有効にするまでそれらの変更は適用されません。 ポートを無効にした場合、SNMP マネージャを設定していれば、linkdown トラップが管理ステーションに送信されます。
[デュプレックス]	デュプレックスの設定:[全二重]、[半二重]、または[自動]。ギガビット イーサネットおよびギガスタック GBIC ポートのデフォルト設定は[自動]です。これらのポートは、接続されているデバイスのデュプレックス機能に自動的に適合します。 ギガスタック GBIC スタック接続は、半二重モードで動作します。 ポイントツーポイント ギガスタック GBIC ポート接続は、全二重モードで動作します。 ギガビットおよび 10 ギガビット イーサネット ポートは、接続デバイスのデュプレックス機能に自動的に適合します。これらのポートのデュプレックス設定([自動])を変更することができます。
[スピード]	10/100-Mbps および 10/100/1000-Mbps ポートの設定: • [10](ポートは強制スピード 10Mbps で動作します) • [100](ポートは強制スピード 100Mbps で動作します) • [1000](ポートは強制スピード 1000Mbps で動作します)

	• [auto]（ポートはすべての利用可能スピードを自動ネゴシエートし通告します） • [auto 10]（ポートはリンクの他端に対して 10Mbps のスピードを自動ネゴシエートし通告します） • [auto 100]（ポートはリンクの他端に対して 100Mbps のスピードを自動ネゴシエートし通告します） • [auto 100 1000]（ポートはリンクの他端に対して 100 および 1000Mbps のスピードを自動ネゴシエートし通告します） • [auto 10 1000]（ポートはリンクの他端に対して 10 および 1000Mbps のスピードを自動ネゴシエートし通告します） • [auto 1000]（ポートはリンクの他端に対して 1000Mbps のスピードを自動ネゴシエートし通告します） • [auto 10 100]（ポートはリンクの他端に対して 10 および 100Mbps のスピードを自動ネゴシエートし通告します） • [auto 10 100 1000]（ポートはリンクの他端に対して 10、100、および 1000Mbps のスピードを自動ネゴシエートし通告します） 10/100-Mbps および 10/100/1000-Mbps ポートのデフォルト設定は[auto]です。イーサネット ポートは、接続デバイスの伝送スピードに自動的に適合します。 **注**：次のポートのスピード設定を変更することはできません。 • 1000BASE-T、SX、LX/LH、ZX、DWDM、および CWDM GBIC • 1000BASE-SX、LX/LH、ZX、および CWDM SFP • XENPAK-10GB-LR、ER、CX4、SR、および LX4 • 100BASE-FX
[電力]	Catalyst Express 500 PoE スイッチ上の単一ポートの場合。ポートを使用して電源デバイスを検出し、それに給電する場合は、[自動]を選択します。それ以外の場合は、[never]を選択します。
[自動 MDIX]	Automatic Medium-Dependent Interface Crossover（自動 MDIX）は、必要なケーブル接続の種類（ストレートスルーまたはクロスオーバー）を自動的に検出し、接続を適切に設定します。この設定が有効になっている場合、いずれかの種類のケーブルを使用でき、インターフェイスによって不適切なケーブルが自動的に修正されます。自動 MDIX が正しく機能するためには、インターフェイスのスピードを[自動]、[auto 10]、[auto 100]、[auto 1000]、[auto 10 100]、[auto 10 1000]、[auto 100 100]、または[auto 10 100 1000]に設定する必要があります。デュプレックス設定も[自動] にする必要があります。 ポートの自動 MDIX を有効にするには、[on] を選択します。ポートの自動 MDIX を無効にするには、[off] を選択します。 **注**：自動 MDIX は、1000 BASE-SX または 1000 BASE-LX SFP インターフェイスではサポートされません。

CE520 スイッチを管理する場合

[ポート統計情報]ウィンドウ

このウィンドウは、機能バーで **モニタ > レポート > ポート統計情報** を選択した場合に表示されます。これにより、概要、送信の詳細、および受信の詳細の各タブに広範囲のポートの統計が表示されます。

次の表は、各タブに表示されるデータについて説明しています。

タブ	カラム	説明
概要	送信レート	現在の送信速度(Mbps)。これには、半二重操作によるコリジョンのため発生する不良パケットの送信および再送信が含まれます。
	受信レート	現在の受信速度(Mbps)。これには、不良パケット、廃棄パケット、および送信先のないパケットのデータ バイトが含まれます。
	送信帯域幅使用率	現在の送信速度と実際の速度に基づく、伝送による帯域幅利用率。
	受信帯域幅使用率	現在の受信速度と実際の速度に基づく、受信による帯域幅利用率。
	送信パケットレート	適格なパケットの現在の送信速度。これには、ユニキャスト、マルチキャスト、およびブロードキャストのパケットが含まれます。
	受信パケットレート	適格なパケットの現在の受信速度。これには、ユニキャスト、マルチキャスト、およびブロードキャストのパケットが含まれます。
	送信マルチキャスト/ブロードキャストパケット	適格なマルチキャストおよびブロードキャストのパケットの現在の送信速度。これには、ユニキャスト パケットが含まれません。
	受信マルチキャスト/ブロードキャストパケット	適格なマルチキャストおよびブロードキャストのパケットの現在の受信速度。これには、ユニキャスト パケットが含まれません。
	廃棄パケット合計	送信および受信の両方で廃棄されたパケットの合計数。
	エラーパケット合計	送信および受信の両方でエラーがあったパケットの合計数。
送信の詳細	ユニキャストパケット	ポートごとに送信された適切なユニキャスト パケットの合計数。これには、エラーのある送信済みパケット、またはマルチキャストやブロードキャストの送信先アドレスのある送信済みパケットは含まれません。

	マルチキャスト パケット	ポートごとに送信された適切なマルチキャスト パケットの合計数。これには、エラーのある送信済みパケット、またはユニキャストやブロードキャストの送信先アドレスのある送信済みパケットは含まれません。
	ブロードキャスト パケット	ポートごとに送信された適切なブロードキャスト パケットの合計数。これには、エラーのある送信済みパケット、またはユニキャストやマルチキャストの送信先アドレスのある送信済みパケットは含まれません。
	コリジョンパケット合計	1 から 15 回のコリジョン発生後にエラーなしで送信されたパケットの合計数。これには、すべての宛先のアドレス タイプのパケットが含まれ、リソース不足または遅延コリジョンのために廃棄されたパケットは含まれません。
	過剰コリジョンパケット	16 回のコリジョン後に送信に失敗したパケットの合計数。これには、すべての宛先のアドレス タイプのパケットが含まれます。
	送信中コリジョンパケット	送信中に検出された遅延コリジョンのために廃棄されたパケットの合計数。これには、パケットの 64 番目のバイトの送信後にコリジョンが発生したすべての送信パケットが含まれます。プリアンブルおよび SFD はフレームのバイト カウントには含まれません。
受信の詳細	ユニキャストパケット	ポートごとに受信された適切なユニキャスト パケットの合計数。これには、エラーのある受信済みパケット、マルチキャストまたはブロードキャスト送信先アドレスのある受信済みパケット、または過大および過小パケットを持つ受信済みパケットは含まれません。廃棄されたパケットや宛先のないパケットも含まれません。
	マルチキャスト パケット	ポートごとに受信された適切なマルチキャスト パケットの合計数。これには、エラーのある受信済みパケット、ユニキャストまたはブロードキャスト送信先アドレスのある受信済みパケット、または過大および過小パケットを持つ受信済みパケットは含まれません。廃棄されたパケットや宛先のないパケットも含まれません。
	ブロードキャスト パケット	ポートごとに受信された適切なブロードキャスト パケットの合計数。これには、エラーのある受信済みパケット、ユニキャストまたはマルチキャスト送信先アドレスのある受信済みパケット、または過大および過小パケットを持つ受信済みパケットは含まれません。廃棄されたパケットや宛先のないパケットも含まれません。
	廃棄パケット	受信帯域幅または受信バッファ容量の不足のため、または転送ルールにより転送されないよう要求されたために廃棄されたパケットの合計数。
	アラインメントエラー	アライメント エラーのある受信済みパケットの合計数。これには、FCS エラーと非整数のバイトの両方があるすべての受信済みパケットが含まれます。
	FCSエラー	FCS エラーのある受信済みパケットの合計数。これには、FCS エラーのある小型パケットは含まれません。
	コリジョンフラグメント	整数バイトおよび不良 FCS 値のある 64 バイト未満のフレームの合計数。

	過少パケット	適切な FCS 値がある 64 バイト未満の受信済みパケットの合計数。
	過大パケット	適切な FCS 値がある 1518 バイトを超える受信済みパケットの合計数。

指定されたデバイスのポートの統計を確認するには、[ホスト名]リストからデバイスを選択します。

統計を更新するには、[更新]をクリックします。

選択したデバイスのすべてのポートの統計をクリアするには、[カウンタのクリア]をクリックします。

ローカル ドライブへのレポートを保存するには、[レポートの保存]をクリックします。表示されたウィンドウで、レポートを保存するフォルダを選択します。

CE520 スイッチを管理する場合

[ポートの説明: 複数のポート]ウィンドウ

このウィンドウは、[ポート設定]ウィンドウで複数のポートを選択して、[説明の記入]をクリックした場合に表示されます。選択したポートの説明を示すための基本オプションと詳細オプションが表示されます。必要なオプションのセットを選択するには、ウィンドウの上部にあるリストから[基本]または[詳細]を選択します。選択したオプション セットの手順を使用します。

基本オプション

これらのオプションでは、2 つの部分で構成された説明が作成されます。すべての説明に表示される固定された語句と、それに続く、各説明で連続的に増加する数字または文字です。

次の手順に従います。

1. [定型テキスト]フィールドに、すべてのポートの説明で繰り返されるテキストを入力します。「?」および「/」の文字を使用することはできません。
2. [増分]フィールドに、数字または文字を入力します。入力した数字または文字は、最初に選択したポートの説明に表示されます。数字を入力した場合、後続のポートごとに説明の数字が 1 つずつ増加していきます。文字を入力した場合、後続のポートごとに説明の文字がアルファベット順で次の文字になっていきます。

   例: [定型テキスト]フィールドに「Room」と入力し、[増分]フィールドに「100」と入力した場合、選択した最初のポートには「Room 100」、2 番目のポートには「Room 101」という説明が表示され、以下、同様に続きます。

   注: 複数の部分からなる増分(たとえば、「103-4B」)を作成する必要がある場合は、詳細オプションを使用する必要があります。

3. [OK]をクリックして、[ポート設定]ウィンドウに説明を入力します。

詳細オプション

これらのオプションでは、基本オプションで提供される増分よりもレベルの多い増分が提供されます。「Room 100」、「Room 101」、「Room 102」、...「Room 120」などの説明を作成する代わりに、「Room 100-1A」、「Room 100-1B」、「Room 100-1C」、...「Room 300-5E」などの多重レベルの説明を作成できます。この例では、ルーム番号には 3 つの部分があり、各部分が独立して増加します。

次の手順に従います。

1. [定型テキスト]フィールドに、すべてのポートの説明で繰り返されるテキストを入力します。
2. 必要に応じて第 1 レベル ボックス内の入力フィールドを使用します。
    1. [コネクタ]フィールドに、増加させていく中央の値の前に置く 1 つの文字を入力します（通常、第 1 レベルのコネクタは使用されません）。
    2. [最小]フィールドに、増加させていく左端の値の開始値（例では「100」）を入力します。
    3. [最大]フィールドに、開始値を増加させていくことができる最高値を入力します。開始値の増加を制限しない場合は、このフィールドを空白のままにできます。
    4. [増分]フィールドに、開始値を増加させていくときに使用する増分を入力します。
3. 必要に応じて第 2 レベル ボックス内の入力フィールドを使用します。
    1. [コネクタ]フィールドに、増加させていく中央の値の前に置く 1 つの文字を入力します。
    2. [最小]フィールドに、増加させていく中央の値の開始値（例では「1」）を入力します。
    3. [最大]フィールドに、開始値を増加させていくことができる最高値を入力します。開始値の増加を制限しない場合は、このフィールドを空白のままにできます。
    4. [増分]フィールドに、開始値を増加させていくときに使用する増分を入力します。
4. 必要に応じて第 3 レベル ボックス内の入力フィールドを使用します。
    1. [コネクタ]フィールドに、増加させていく中央の値の前に置く 1 つの文字を入力します（例では使用されていません）。
    2. [最小]フィールドに、増加させていく右端の値の開始値（例では「A」）を入力します。
    3. [最大]フィールドに、開始値を増加させていくことができる最高値を入力します。
    4. [増分]フィールドに、開始値を増加させていくときに使用する増分を入力します。

       開始値が文字の場合、増分は昇順のアルファベット順でスキップする文字数になります。増分が 1 の場合、文字はスキップされません。2 の場合、A からは C、E、G と増加していきます。

5. [OK]をクリックして、[ポート設定]ウィンドウに説明を入力します。

注：[定型テキスト]フィールドおよび[コネクタ]フィールドには、「?」および「/」の文字を使用できません。

増分は右から左に進みます。たとえば、3 つのレベルの説明では、第 2 レベルが最初に増加する前に、第 3 レベルがすべての範囲を通して増加します。次に、第 3 レベルは開始値にリセットされ、第 2 レベルが 2 回目に増加する前に第 3 レベルがすべての範囲を通して再度増加し、以下、同様に続きます。第 2 レベルがすべての範囲を通して増加した後、第 2 レベルと第 3 レベルの両方がそれぞれの開始値にリセットされ、第 1 レベルが初めて増加します。

この例では第 3 レベルだけに文字が使用されていますが、文字または数字をいずれのレベルでも使用できます。

3 つより少ないレベルを使用できます。1 つまたは 2 つのレベルだけを使用する場合、文字と数字のいずれを使用するかは問題ではありません。

CE520 スイッチを管理する場合

[ポートロールの修正]ウィンドウ

このウィンドウは、[スマートポート]ウィンドウで 1 つまたは複数のポートを選択して[修正]をクリックした場合に表示されます。1 つのポートを選択した場合、[インターフェイス]フィールドにそのポート名が表示されます。複数のポートを選択した場合、[インターフェイス]フィールドに[複数]と表示されます。

選択したポートにロールを適用するには、次の手順に従います。

1. [ロール]リストで、接続するデバイスに対応したロールを選択します。

選択するロール	**ポートの接続先**
[デスクトップ]	デスクトップ
[IP Phone+デスクトップ]	IP Phone およびデスクトップ
[プリンタ]	プリンタ
[スイッチ]	スイッチ
[ルータ]	ルータ
[アクセスポイント]	アクセスポイント
[サーバ]	サーバ
[ゲスト]	組織の内部サブネットへのアクセス権のないエンド ホスト
[診断]	スニファ
[その他]	その他のデバイス

2. 選択したロールに応じて、[属性]セクションに入力します。

選択したロール	**実行する手順**
[デスクトップ]、[プリンタ]、[ゲスト]、または[その他]	[アクセスVLAN]フィールドから VLAN を選択します。これは、ポートとデスクトップ間でデータを送信する VLAN です。
[IP Phone+デスク	1. [アクセスVLAN]リストから VLAN を選択します。これは、ポート間で

トップ]	データ パケットを送信する VLAN です。 2. [音声VLAN]リストから別の VLAN を選択します。これは、ポート間でボイス パケットを送信する VLAN です。
[スイッチ]、[ルータ]、または[アクセスポイント]	[ネイティブVLAN]リストからネイティブ VLAN を選択します。ポートはトランクポートとして設定され、ネイティブ VLAN によりタグなしのトラフィックが送信されます。
[サーバ]	1. [アクセスVLAN]リストから VLAN を選択します。 2. [サーバタイプ]リストで、次のサーバの種類からいずれかを選択することにより、サーバ転送の優先順位を指定します。 [信頼]:Voice over IP(VoIP)用に使用するサーバ。音声品質の優先順位および[重要]タイプのサーバと同等の優先順位がすべてのトラフィックに与えられます。例として、Cisco Call Manager などがあります。 [重要]:主としてビジネス サーバより重要なトラフィックを組織に提供するサーバ。そのため、ビジネス サーバより優先順位が高くなります。例として、ビジネス トランザクション用のサーバなどがあります。 [ビジネス]:[標準]のサーバより高い優先順位が与えられるが、[重要]または[信頼]サーバより優先順位が低いサーバ。例として、業務記録を保存するサーバなどがあります。 [標準]:その他のサーバ タイプよりも低い優先順位で処理されるサーバ。例として、Web サーバなどがあります。
[診断]	1. [発信元ポート]リストから、監視する送信元を選択します。 2. Intrusion Detection System(IDS; 侵入検知システム)を宛先ポートへ接続する場合は、[入力VLAN]リストから入力 VLAN を選択します。それ以外の場合は、[なし]を選択します。IDS によってパケットが送信される際には、入力 VLAN が使用されます。

ウィンドウでの操作が終了したら、[OK]をクリックします。[スマートポート]ウィンドウに戻ります。

UC500 を管理する場合

[ポートロールの修正]ウィンドウ

このウィンドウは、[スマートポート]ウィンドウの[ポート設定]タブで 1 つまたは複数のポートを選択して[修正]をクリックした場合に表示されます。1 つのポートを選択した場合、[インターフェイス]フィールドにそのポート名が表示されます。複数のポートを選択した場合、[インターフェイス]フィールドに[複数]と表示されます。

選択したポートにロールを適用するには、次の手順に従います。

1. [ロール]リストで、接続するデバイスに対応したロールを選択します。

選択するロール	ポートの接続先
[デスクトップ]	デスクトップ
[IP Phone+デスクトップ]	IP Phone およびデスクトップ
[スイッチ]	スイッチ
[ルータ]	アクセス ルータまたは UC500 プラットフォーム
[アクセスポイント]	アクセスポイント

注： 10 GB イーサネット ポートを選択した場合、選択できるのは[スイッチ]および[ルータ]のみです。

2. 選択したロールに応じて、[属性]セクションに入力します。

選択したロール	実行する手順
[デスクトップ]	[アクセスVLAN]フィールドに VLAN の番号を入力します。これは、ポートとデスクトップ間でデータを送信する VLAN です。
[IP Phone+デスクトップ]	1. [アクセスVLAN]フィールドに VLAN の番号を入力します。これは、ポート間でデータ パケットを送信する VLAN です。 2. [音声VLAN]フィールドに、別の VLAN の番号を入力します。これは、ポート間でボイス パケットを送信する VLAN です。
[スイッチ]、[ルータ]、または[アクセスポイント]	[ネイティブ VLAN]フィールドに、ネイティブ VLAN の番号を入力します。ポートはトランク ポートとして設定され、ネイティブ VLAN によりタグなしのトラフィックが送信されます。

選択したポートからロールを削除するには、[ロール]リストから[なし]を選択します。ポートは工場出荷時のデフォルト設定にリセットされます。

ウィンドウでの作業が完了したら、[OK]をクリックします。[スマートポート]ウィンドウに戻ります。

CE520 スイッチを管理する場合

[ポートロールの詳細]ウィンドウ

このウィンドウは、[スマートポート]ウィンドウの[ポート設定]タブで[詳細]をクリックした場合に表示されます。

ポートを選択してから[詳細]をクリックする場合、選択されたポートのあるデバイスの拡張ヘッダが表示されます。ポートを選択しなかった場合、[スマートポート]ウィンドウで、すべてのデバイスの拡張ヘッダが表示されます。

デバイスのヘッダの下には拡張ポート ヘッダがあり、その下にはロールの詳細があります。ロールがポートに適用される場合、ロールのタイプおよび関連する設定情報が表示されます。ロールが何も適用されていない場合は[なし]と表示されます。

ウィンドウでの操作が終了したら、[OK]をクリックします。

UC500 を管理する場合

[ポートロールの詳細]ウィンドウ

このウィンドウは、[スマートポート]ウィンドウの[ポート設定]タブで[詳細]をクリックした場合に表示されます。

ポートを選択してから[詳細]をクリックする場合、選択されたポートのあるデバイスの拡張ヘッダが表示されます。ポートを選択しなかった場合、[スマートポート]ウィンドウで、すべてのデバイスの拡張ヘッダが表示されます。

デバイスのヘッダの下には拡張ポート ヘッダがあり、その下にはロールの詳細があります。ロールがポートに適用される場合、ロールのタイプおよび関連する設定情報が表示されます。ロールが何も適用されていない場合は[なし]と表示されます。

ウィンドウでの作業が完了したら、[OK]をクリックします。

CE520 スイッチを管理する場合

[ホスト名]ウィンドウ

このウィンドウは、機能バーで **設定 > デバイスプロパティ > ホスト名** を選択した場合に表示されます。

次の手順に従います。

1. [ホスト名]リストで、名前を変更するデバイスを選択します。

   設定 > デバイスプロパティ > ホスト名 を選択する前に[トポロジ]ビューでデバイスを選択していた場合は、選択したデバイスにホスト名が事前設定されています。

2. [新しいホスト名]フィールドに、デバイスの一意の名前を入力します。

   ホスト名の最大文字数は 31 文字です。

3. [OK]をクリックします。対象のデバイスの新しい名前を示した[トポロジ]ビューが再表示されます。

[設定]メニューで[設定の保存]を選択して、NVRAM に変更を保存します。

WLC526 を管理する場合

[無線]ウィンドウ

このウィンドウを使用すると、WLAN コントローラ上の無線のステータスを表示できます。

次の表は、このウィンドウのカラムに表示される情報について説明しています。

カラム	説明
MACアドレス	無線の MAC アドレス
アクセスポイント名	ライトウェイト アクセスポイントの名前
管理ステータス	インターフェイスのステータス（有効または無効）
動作ステータス	無線の運用ステータス（アップまたはダウン）
チャネル番号	アクセスポイントのチャネル番号
送信パワー（mW）	アクセスポイントの伝送パワー レベル
アンテナ	アンテナのタイプ（内部または外部）

ウィンドウを閉じるには、[OK]をクリックします。

WLC526 を管理する場合

[無線インターフェイス]ウィンドウ

このウィンドウを使用すると、WLAN コントローラ上のすべての無線インターフェイス設定を表示したり、WLAN コントローラに動的（ユーザ定義）無線インターフェイスを設定したりできます。

次の表は、このウィンドウのカラムについて説明しています。

カラム	説明
名前	動的インターフェイスおよび静的インターフェイスなどの無線インターフェイス名（management、ap-manager、および virtual）
VLAN	無線インターフェイスに関連付けられている VLAN
ポート	無線インターフェイスの物理ポート番号
IPアドレス	無線インターフェイスの IP アドレス

WLAN コントローラに動的無線インターフェイスを設定する手順は、次のとおりです。

1. ［ホスト名］リストから対象の WLAN コントローラを選択します。
2. インターフェイスを作成するには、［作成］をクリックして、［インターフェイスの作成］ウィンドウに入力します。

   注: 1 つのコントローラで最大 8 つの動的インターフェイスをサポートできます。

設定を変更するには、無線インターフェイス名を選択して、［更新］をクリックし、［インターフェイスの修正］ウィンドウを使用します。

設定を削除するには、無線インターフェイス名を選択して、［削除］をクリックします。

注: 変更したり削除したりできるのは、動的インターフェイスだけです。静的インターフェイスを変更したり削除したりできません。

変更を保存してウィンドウを閉じるには、［無線インターフェイス］ウィンドウで［OK］をクリックします。

WLC526 を管理する場合

［無線インターフェイスの更新］ウィンドウ

このウィンドウは、［無線インターフェイス］ウィンドウで［修正］をクリックした場合に表示されます。このウィンドウを使用すると、無線インターフェイスの設定を変更できます。

次の手順に従います。

1. ［VLAN ID］フィールドに、無線インターフェイスに関連付ける VLAN ID を入力します。
2. ［ポート］リストから、無線インターフェイスのポートを選択します。
3. ［IP アドレス］フィールドに、無線インターフェイスの IP アドレスを入力します。
4. ［サブネットマスク］リストから、無線インターフェイスのサブネット マスクを選択します。
5. ［ゲートウェイIPアドレス］フィールドに、デフォルト ゲートウェイの IP アドレスを入力します。
6. ［DHCPサーバIPアドレス］フィールドに、DHCP サーバの IP アドレスを入力します。
7. このウィンドウに必要な情報を入力したら、［OK］をクリックして、変更を保存し、ウィンドウを閉じます。

WLC526 を管理する場合

［無線インターフェイスの作成］ウィンドウ

このウィンドウは、［無線インターフェイス］ウィンドウで［作成］をクリックした場合に表示されます。このウィンドウを使用すると、無線インターフェイスを作成できます。

次の手順に従います。

1. ［インターフェイス名］フィールドに、無線インターフェイスの名前を入力します。

2. ［VLAN ID］フィールドに、無線インターフェイスに関連付ける VLAN ID を入力します。
3. ［ポート］リストから、無線インターフェイスのポートを選択します。
4. ［IP アドレス］フィールドに、無線インターフェイスの IP アドレスを入力します。
5. ［サブネットマスク］リストから、無線インターフェイスのサブネット マスクを選択します。
6. ［ゲートウェイIPアドレス］フィールドに、デフォルト ゲートウェイの IP アドレスを入力します。
7. ［DHCPサーバIPアドレス］フィールドに、DHCP サーバの IP アドレスを入力します。
8. このウィンドウに必要な情報を入力したら、［OK］をクリックして、変更を保存し、ウィンドウを閉じます。

WLC526 を管理する場合

［無線クライアント］ウィンドウ

このウィンドウを使用すると、WLAN コントローラ上の無線クライアントのステータスを表示できます。

次の表は、このウィンドウのカラムに表示される情報について説明しています。

カラム	説明
MACアドレス	クライアントの MAC アドレス
ステータス	クライアント接続のステータス • ［Idle］ • ［Pending］ • ［Authenticated］ • ［Associated］ • ［Active］ • ［Power Save］ • ［Disassociated］ • ［Excluded］ • ［Probing］
アクセスポイント名	クライアントの ライトウェイト アクセスポイントの名前
SSID	クライアントの SSID
Radio	クライアントのタイプ • ［802.11a］ • ［802.11b］ • ［802.11g］
認証済	クライアントの認証ステータス（yes または no）

ウィンドウを閉じるには、[OK]をクリックします。

WLC526 を管理する場合

[無線コントローラダッシュボード]ウィンドウ

このウィンドウでは、[システム]、[AP概要]、[WLAN]、[WLC統計情報]、および[AP統計情報]の各タブ上に、WLAN コントローラのさまざまな統計が表示されます。

次の表は、[システム]セクションに表示されるデータについて説明しています。

カラム	説明
コントローラ名	コントローラの名前
接続時間	WLAN コントローラを最後に起動してからの経過時間
温度	内部シャーシの温度
CPU	WLAN コントローラの CPU の合計使用量
メモリ	WLAN コントローラのメモリの合計使用量

次の表は、[AP概要]セクションに表示されるデータについて説明しています。

カラム	説明
コントローラ名	コントローラの名前
802.11b/g無線	無線のステータス([接続中]または[ダウン])
APステータス	アクセスポイントのステータス([接続中]または[ダウン])

次の表は、[WLAN]セクションに表示されるデータについて説明しています。

カラム	説明
WLAN名(コントローラ名)	コントローラの SSID 名
クライアント	この SSID に関連付けられているクライアントの数

次の表は、[WLC統計情報]セクションに表示されるデータについて説明しています。

注:データを合計数または比率で表示するように選択できます。

カラム	説明

コントローラ名	コントローラの名前
正常受信パケット	受信済みパケットの合計数または比率
破棄された受信パケット	破棄された受信済みパケットの合計数または比率
正常送信パケット	送信済みパケットの合計数または比率
破棄された送信パケット	破棄された送信済みパケットの合計数または比率

次の表は、[AP統計情報]セクションに表示されるデータについて説明しています。

カラム	**説明**
AP名(コントローラ名)	WLAN コントローラに関連付けられているアクセスポイント
送信フレーム数	送信したフレームの合計数
送信失敗数	送信に失敗したフレームの合計数

統計を更新するには、[更新]をクリックします。

UC500、Cisco 800シリーズルータを管理する場合

[ユーザオプション]ウィンドウ

このウィンドウは、[音声]ウィンドウの[ユーザ]タブで[詳細]をクリックした場合に表示されます。

電話のボタンを設定するには、次の手順に従います。

1. [タイプ]リストで、次のボタンのタイプから選択します。
   - [標準]:単一回線がボタンに割り当てられます。
   - [共有回線]:複数の電話が単一回線を共有します。(SIP 電話ではサポートされていません。)
   - [モニタ回線]:この回線のステータスは、共有回線がアイドル状態か使用中のどちらかであるということを意味します。(SIP 電話ではサポートされていません。)
   - [オーバーレイ]:複数のボタンを持つ電話上の 1 つのボタンを、複数の回線が共有します。(SIP 電話ではサポートされていません。)
2. [内線番号]フィールドに、ボタンの内線番号を入力します。

ユーザ オプションを設定するには、次の手順に従います。

1. [権限]メニューから Class of Restrictions(COR; 制限クラス)を選択します。COR では、この内線番号または電話番号の電話ユーザがアクセスできるダイヤル ピアが決定されます。有効なオプションは次のとおりです。

- [内線]。発信コールが、内線通話と緊急番号の呼び出しのみに制限されます。その他の通話は不可能です。
- [地域]。発信コールが、市内通話、内線通話、および緊急番号の呼び出しのみに制限されます。国内長距離電話や国際電話をかけることはできません。
- [国内]。発信コールが、国内長距離通話、市内通話、内線通話、および緊急番号の呼び出しのみに制限されます。国際電話をかけることはできません。
- [国際]。発信コールが、内線通話、市内通話、国内長距離通話、緊急番号の呼び出し、および国際通話で使用可能です。

2. ユーザが[音声]タブのリストにある制限された番号を呼び出さないようにするには、[ブロック制限番号]チェックボックスをオンにします。
3. [一斉同報グループ]メニューから、この IP Phone を割り当てる一斉同報 グループの番号を選択します。(SIP 電話では無効になっています。)
4. [インターコム]メニューから、この IP 電話で、プッシュ ツー トーク インターコム回線を通じてワンボタンで対話できるユーザ名を選択します。(SIP 電話では無効になっています。)
5. インターコム コールのスピーカー消音機能を有効または無効にするには、[インターコム ミュート]チェックボックスをオンまたはオフにします。(SIP 電話では無効になっています。)

プライマリ内線番号を設定するには、次の手順に従います。

1. [ビジー時転送]フィールドに、この IP Phone の内線番号が話し中の場合に着信コールを転送する内線番号を入力します。[ビジー時転送]と[無応答時転送]には、ボイス メール番号が自動入力されます。自動入力されたボイス メール番号は、別の番号に変更することもできます。ボイス メール番号を変更した場合、自動入力されたボイス メール番号を新しい番号に変更するのか、それとも元の番号を引き続き使用するのかを確認するメッセージが表示されます。
2. [PSTN番号]フィールドに、PSTN 番号を入力します。
3. [無応答時転送]フィールドに、この IP Phone の内線番号が応答しない場合に着信コールを転送する内線番号を入力します。
4. [ピックアップグループ]メニューから、この IP Phone を割り当てるピックアップ グループの番号を選択します。(SIP 電話では無効になっています。)
5. [無応答時転送タイムアウト]フィールドに、まだ応答を受けていないコールをターゲットの内線番号に転送するまでの秒数を入力します。
6. [ハントグループ]メニューから、この IP Phone をメンバとして加えるボイス ハント グループの番号を選択します。(SIP 電話では無効になっています。)

CE520 スイッチを管理する場合

[ユーザとパスワード]ウィンドウ

このウィンドウは、機能バーで **設定 > デバイスプロパティ > ユーザとパスワード** を選択した場合に表示されます。このウィンドウを使用すると、すべてのコミュニティ デバイスへのアクセス権を管理者に付与したり、特定のデバイスに対するユーザ アクセスを管理したりできます。

まず、[全デバイス]を選択するか、[ホスト名]リストから特定のデバイスを選択します。

ウィンドウでの作業が完了したら、[OK]をクリックします。

すべてのコミュニティ デバイスへのアクセス権の付与

次の手順に従います。

1. [管理ユーザ名]フィールドに、管理者がコミュニティ内のすべてのデバイスへのアクセスに使用するユーザ名を入力します。
2. [パスワード]フィールドに、管理者が使用するパスワードを入力します。入力した情報は暗号化され、アスタリスクとして表示されます。
3. [パスワード確認]フィールドにパスワードをもう一度入力します。

特定のデバイスへのアクセスの管理

次のタブを使用します。

- [ローカルユーザ名/パスワード]。ユーザ名とパスワードを特権レベルに関連付けます。
- [HTTP認証]。Configuration Assistant にアクセスするためにユーザがユーザ名とパスワードの両方を入力するか、またはパスワードだけを入力するかを指定します。
- [イネーブル パスワード]。パスワードを特権レベルに関連付けます。
- [コンソール/Telnetパスワード]。パスワードをコンソールラインセッションおよび Telnet セッションに関連付けます。

[ローカルユーザ名/パスワード]

このタブには、ユーザ名、パスワード、およびそれらに関連付けられている特権レベルが表示されます。このタブでユーザ名とパスワードのペアが設定されているユーザは、関連付けられている特権レベルで Configuration Assistant にアクセスできます。

新しいユーザ アクセス レコード(新しいユーザ名、パスワード、および特権レベル)を入力するには、[作成]をクリックして、ローカルユーザ名/パスワードの作成ウィンドウを使用します。

ユーザ アクセス レコード内のパスワードまたは特権レベルを変更するには、変更対象を選択してから[修正]をクリックし、[ローカルユーザ名/パスワードの修正]ウィンドウを使用します。

ユーザ アクセス レコードを削除するには、削除するレコードを選択して、[削除]をクリックします。

[HTTP認証]

ユーザがパスワードだけを入力して選択したデバイスにアクセスできるようにするには、このタブの[イネーブル パスワード]をクリックします。ユーザがユーザ名とパスワードの両方を入力するようにするには、[ローカルユーザ名/パスワード]をクリックします。

パスワードを設定するには[イネーブル パスワード]タブを使用し、ユーザ名とパスワードを設定するには[ローカルユーザ名/パスワード]タブを使用してください。

[イネーブル パスワード]

このタブには、特権レベルとパスワードが表示されます。このタブに表示されるパスワードを入力すると、ユーザは関連付けられている特権レベルで Configuration Assistant にアクセスできます。

新しいパスワードおよび関連付けられる特権レベルを作成するには、[作成]をクリックして、イネーブル パスワードの作成ウィンドウを使用します。

注:1 から 15 までの各特権レベルにパスワードが関連付けられている場合は、[作成]ボタンは無効になっています。

パスワードを変更するには、変更するパスワードを選択して、[修正]をクリックし、イネーブル パスワードの更新ウィンドウを使用します。

パスワードを削除するには、削除するパスワードを選択して、[削除]をクリックします。パスワードとそれに関連付けられている特権レベルの両方がタブから削除されます。

[コンソール/Telnetパスワード]

このタブには、コンソールラインセッションおよび Telnet セッションに関連付けられているパスワードが表示されます。

Telnet セッションでは、ユーザは Telnet パスワードを使用してデバイスに読み取り専用でアクセスできます。ユーザはデバイスを設定できません。ユーザがデバイスに Telnet でアクセスすると、ユーザが共有しているパスワードの入力が求められます。ユーザ名の入力は求められません。管理者が Telnet パスワードを入力しないでおくか、削除した場合、ユーザは[ローカルユーザ名/パスワード]タブでユーザ名とパスワードを入力するよう求められます。

コンソール パスワードを入力すると、ユーザには読み取り/書き込みアクセス権が与えられます。イネーブル パスワードが作成されている場合、ユーザは、コンソール パスワードの代わりにイネーブル パスワードを入力して、読み取り/書き込みアクセス権を得る必要があります。

パスワードを作成または変更するには、[パスワード]フィールドに新しいパスワードを入力して、[パスワード確認]フィールドにもう一度入力します。

WLC526 を管理する場合

[ユーザとパスワード]ウィンドウ

このウィンドウは、機能バー上で **設定 > デバイスプロパティ > ユーザとパスワード** を選択した場合に表示されます。このウィンドウを使用すると、すべてのコミュニティ デバイスへのアクセス権を管理者に付与したり、特定のデバイスに対するユーザ アクセスを管理したりできます。

まず、[全デバイス]を選択するか、[ホスト名]リストから特定のデバイスを選択します。

ウィンドウでの作業が完了したら、[OK]をクリックします。

すべてのコミュニティ デバイスへのアクセス権の付与

次の手順に従います。

1. [管理ユーザ名]フィールドに、管理者がコミュニティ内のすべてのデバイスへのアクセスに使用するユーザ名を入力します。

2. [パスワード]フィールドに、管理者が使用するパスワードを入力します。入力した情報は暗号化され、アスタリスクとして表示されます。
3. [パスワード確認]フィールドにパスワードをもう一度入力します。

特定のデバイスへのアクセスの管理

選択したデバイスへのユーザ アクセスを付与するには、[作成]をクリックして、ローカルユーザ名/パスワードの作成ウィンドウを使用します。新しいユーザ アクセス レコードが[ユーザとパスワード]ウィンドウに表示されます。各レコードでは、ユーザが Configuration Assistant にアクセスできる特権レベルがユーザ名とパスワードに関連付けられます。

ユーザ アクセス レコードを削除するには、削除するレコードを選択して、[削除]をクリックします。

ウィンドウでの作業が完了したら、[OK]をクリックします。

[ライセンス管理]ウィンドウ

このウィンドウは、**メンテナンス > ライセンス管理** を選択した場合に表示されます。

評価ライセンスをインストールするには、次の手順に従います。

1. デバイスの[処理]リストで[評価]を選択します。
2. [適用]または[OK]をクリックし、ライセンスをインストールします。関連フィールドが更新されます。

永久または拡張ライセンスをインストールするには、次の手順に従います。

1. デバイスの[処理]リストで、[ライセンスファイル]を選択します。ブラウザウィンドウが表示され、ライセンスファイルが列挙されます。
2. ライセンスファイルをダブルクリックします。
3. [適用]をクリックし、ライセンスをインストールします。関連フィールドが更新されます。

ライセンスのインストールをキャンセルするには、[適用]または[OK]をクリックする前に[更新]をクリックします。インストールはキャンセルされ、ライセンスの元のステータスが表示されます。ライセンスが正常にインストールされると、付与された各ライセンスの機能が[機能]カラムに表示されます。

ネットワーク接続または更新のたびに、Cisco Configuration Assistant の[通知]ウィンドウには仮ライセンスの状態が表示されます。また、いずれかの機能のライセンスの期限満了の 10 日前以内になると、システムにより永久ライセンスのインストールが推奨されます。

CE520 スイッチを管理する場合

[リンクグラフ]ウィンドウ

このウィンドウは、次のいずれかの処理を実行した場合に表示されます。

- 機能バー上で **モニタ > レポート > リンクグラフ** を選択する。
- [トポロジ]ビューのリンクをクリックして、ポップアップ メニューで[リンクグラフ]を選択する。

このウィンドウを使用する目的は、次のとおりです。

- 表示されるデータのタイプの選択
- 表示されるグラフのタイプの選択
- 軸上の差分の変更
- データの長期スパンの表示

[インターフェイス]フィールドに記載されていないポートを選択するには、ポート番号を上書きしてスクロール ボタンを使用するか、  アイコンをクリックします。最後のオプションを選択した場合、[インターフェイスの選択]ウィンドウが開いてデバイスの前面パネルが表示されます。ポートをクリックして選択し、[OK]をクリックします。

表示されるデータのタイプの選択

データのタイプを選択するには、[データ]リストで[使用率(%)]、[送信/受信パケット]、[パケット転送方法]、または[パケット破棄およびエラー]をクリックします。各選択の結果は、次のとおりです。

データ タイプ	**結果**
使用率(%)	リンクに対応したポートで使用される帯域幅利用率を表示します。たとえば、リンクの帯域幅が100 Mbps で、一度に 20 MB が使用された場合、グラフはその瞬間 20% を示します。
送信/受信パケット	送信(赤)と 受信(青)の 2 つのグラフを表示します。 [送信バイト数]グラフでは、リンクに対応したポートで送信されたバイト数が表示されます。 [受信バイト数]グラフでは、リンクに対応したポートで受信されたバイト数の合計が表示されます。
パケット転送方法	ブロードキャスト/マルチキャスト パケット(赤)と ユニキャスト(青)の 2 つのグラフを表示します。 [ブロードキャスト/マルチキャスト パケット]グラフでは、リンクに対応したポートで送受信されたブロードキャストとマルチキャストのパケット数が表示されます。 [ユニキャスト]グラフでは、リンクに対応したポートで送受信されたユニキャストのパケット数が表示されます。
パケットの廃棄とエラー	エラー合計(青)とドロップされた合計パケット数(赤)の 2 つのグラフが表示されます。 [エラー合計]グラフでは、カウンタが最後にリセットされてからポートに累積された、エラーのあるパケットの合計数が表示されます。

	[ドロップされた合計パケット数]グラフでは、リンクに対応するポートでドロップされたパケットの合計数が表示されます。パケットのドロップは、バッファまたは帯域幅の不足のため、またはデバイス上のユーザ設定によるパケットのフィルタのため発生します。

表示されるグラフのタイプの選択

[タイプ]リストで、[折れ線]、[棒]、[積み重ね]、[範囲]、または[スタック範囲]をクリックしてグラフのタイプを選択します。各タイプのアピアランスは、次のとおりです。

グラフ タイプ	アピアランス
折れ線	データ ポイントが線で結ばれます。
棒	データ ポイントが棒の高さで示されます。
積み重ね	別々の色の複数の棒グラフが、相互に積み重なって表示されます。
範囲	データ ポイントが線で結ばれ、線の下の部分が塗りつぶされます。
スタック範囲	別々の色の複数の面積グラフが、相互に積み重なって表示されます。

軸上の差分の変更

デフォルトでは、x 軸上の時間の差分が 2 分間隔で表示されます。その差分の間隔を短くしたり、長くしたりするには、[拡大/縮小]ボタンをクリックします。

y 軸上の差分を算術的にではなく対数的に拡大する場合には、[対数表示]をオンにします。

データの長期スパンの表示

グラフの下にあるスクロール バーを使用し、左にスクロールしてグラフの外へ移動した過去のデータ ポイントを確認できます。その後で右にスクロールして最新のデータに戻ることができます。

注: グラフは、デバイスがポーリングされるたびに更新されます。ポーリング間隔(データ収集の頻度)を変更するには、**アプリケーション > 環境設定** を選択して [環境設定]ウィンドウを使用します。

CE520 スイッチを管理する場合

[リンクと接続性]ウィンドウ

このウィンドウを使用する目的は、次のとおりです。

- リンクをテストし、配線の問題を診断し、ケーブルの破損および障害の箇所を特定し、ポート速度の設定の不一致を診断して解決する。リンクが選択したポートに接続されている場合、このテストの開始時に少しの間停止することがあります。

  注: このテストに対応しているのは、銅線のイーサネット 10/100/1000 ポートのみです。

- ネットワークにおける 2 つのデバイス間のネットワーク接続性をテストする。たとえば、ホストとサーバの間のネットワーク接続性をテストできます。

リンクをテストするには、次の手順に従います。

1. [テストのタイプ]リストから[リンク(サービス停止)]を選択します。
2. [ホスト名]リストからホスト名を選択します。
3. [インターフェイス]リストからインターフェイスを選択するか、[インターフェイス]フィールドの横のアイコンをクリックして、表示するデバイスのインターフェイスを選択します。
4. [スタート]をクリックしてテストを開始します。

リンク上に何らかのエラーがある場合、エラー メッセージの説明と推奨事項が[結果]領域に表示されます。エラーがない場合には、エラーがないことを示すメッセージが表示されます。

リンクの問題を解決するには、[修正]ボタンをクリックします。速度の不一致の問題は、Configuration Assistant を使用した場合のみ解決できます。

2 つのデバイス間のネットワーク接続をテストするには、次の手順に従います。

1. [テストのタイプ]リストから[接続性]を選択します。
2. [発信元IPアドレス]フィールドに、いずれかのデバイスの送信元 IP アドレスを入力します。
3. [宛先IPアドレス]フィールドに、他のデバイスの送信先 IP アドレスを入力します。
4. [スタート]をクリックしてテストを開始します。

メッセージの説明と推奨事項が、[結果]領域に表示されます。

CE520 スイッチを管理する場合

[ローカルユーザ名/パスワードの修正]ウィンドウ

このウィンドウは、[ユーザとパスワード]ウィンドウの[ローカルユーザ名/パスワード]タブでエントリを選択し、[修正]をクリックした場合に表示されます。このウィンドウを使用すると、ユーザ名に関連付けられているパスワードおよび特権レベルを変更できます。

次の手順に従います。

1. パスワードを変更する場合は、[パスワード]フィールドに別のパスワードを入力します。入力した情報は暗号化され、アスタリスクとして表示されます。
2. [パスワード確認]フィールドにパスワードをもう一度入力します。
3. 特権レベルを変更する場合は、[特権レベル]リストから別の特権レベルを選択します。
4. [OK]をクリックします。

CE520 スイッチを管理する場合

イネーブル パスワードの更新ウィンドウ

このウィンドウは、パスワードを選択して、[ユーザとパスワード]ウィンドウの[イネーブル パスワード]タブで[修正]をクリックした場合に表示されます。このウィンドウを使用すると、関連付けられている特権レベルのパスワードを変更できます。

次の手順に従います。

1. [パスワード]フィールドに、表示された特権レベルに関連付ける別のパスワードを入力します。入力した情報は暗号化され、アスタリスクとして表示されます。
2. [パスワード確認]フィールドにパスワードをもう一度入力します。
3. [OK]をクリックします。

CE520 スイッチを管理する場合

イネーブル パスワードの作成ウィンドウ

このウィンドウは、[ユーザとパスワード]ウィンドウの[イネーブル パスワード]タブで[作成]をクリックした場合に表示されます。このウィンドウを使用すると、特権レベルおよび関連付けるパスワードを指定できます。

次の手順に従います。

1. [特権レベル]リストから特権レベルを選択します。

   レベル 15 では読み取り/書き込みアクセス、レベル 1 から 14 では読み取り専用アクセスが与えられます。

   特権レベルにすでにパスワードが関連付けられているかどうかは、このリストには表示されません。その情報は[ユーザとパスワード]ウィンドウにあります。

2. [パスワード]フィールドに、選択した特権レベルのユーザが Configuration Assistant へのアクセスに使用できるパスワードを入力します。入力した情報は暗号化され、アスタリスクとして表示されます。
3. [パスワード確認]フィールドにパスワードをもう一度入力します。
4. [OK]をクリックします。[ユーザとパスワード]ウィンドウに戻ると、[イネーブル パスワード]タブに新規エントリが表示されます。

UC500、Cisco 800シリーズルータを管理する場合

拡張DIDダイヤルプランの作成ウィンドウ

このウィンドウは、[音声]ウィンドウの[ダイヤルプラン]タブで DID の[設定]をクリックした場合に表示されます。

1対1 DID 変換では、1 つの PSTN 番号を 1 つのローカル内線番号に割り当てます。外部の発信者が個々のユーザの内線番号に直接ダイヤルできる場合には、この設定が一般的です。連続した一連の番号の範囲ごとに、1 つのダイヤル プランを設定する必要があります。

1対1 DID 変換を設定するには、次の手順に従います。

1. 変換を追加するには、[作成]をクリックします。
2. [ダイヤルプラン名]フィールドに、ダイヤル プランの名前を入力します。ダイヤル プランの説明は一意で、15 文字以内にする必要があります。
3. [DID範囲開始]フィールドに、PSTN 番号範囲の開始番号を入力します。番号の範囲は一意でなければなりません。PSTN 番号の範囲を重複して定義すると、エラーを発生します。
4. [DID範囲終了]フィールドに、PSTN 番号範囲の終了番号を入力します。
5. [内部番号開始]フィールドに、内線番号範囲の開始番号を入力します。この内線番号範囲の桁数は、[ダイヤルプラン]タブの[システムの内線番号]ウィンドウにある[内線番号の桁数]フィールドと一致している必要があります。内線番号範囲と PSTN 番号範囲は、等しくなければなりません。
6. [内部番号終了]フィールドに、内線番号範囲の終了番号を入力します。
7. [トランク]メニューで、音声のエンドポイントを選択します。このトランクを経由して、外線からの呼び出しが着信することになります。
8. [発信者ID]チェックボックスをオンにして、発信者の ID を有効にします。ローカル内線番号から発信した呼び出しの発信者の ID は、該当する PSTN 番号に変換されます。この設定が有効になるのは、PSTN 番号範囲と内線番号範囲が、照合用の末尾の数桁を共有する場合のみです。たとえば、次のパラメータの例を参照してください。
   - [DID範囲開始]: 1543331000
   - [DID範囲終了]: 1543331030
   - [内部番号開始]: 1000
   - [内部番号終了]: 1030

   1555331000 への呼び出しは、内線番号 1000 にリダイレクトされます。1555331001 への呼び出しは、内線番号 1001 に、それ以降も同様にリダイレクトされます。発信者の ID が有効になっている場合、内線番号 1000 からの呼び出しは、受信する電話に 1555331000 と表示されます。

多対1 DID 変換では、PSTN 番号の範囲を 1 つの内線番号に割り当てます。その内線番号は、自動音声応答、オペレータの内線番号、またはハント グループに対応しています。連続した一連の番号の範囲ごとに、1 つのダイヤル プランを設定する必要があります。

FXS/DID ポートおよび T1/CAS ポート（番号収集が一括ではない場合はその他のポート）のダイヤル プランの場合、1 つの多対1 ダイヤル プランだけを各ポートに定義できます。最大 15 の PSTN 番号を、各ダイヤル プランに定義できます。

多対1 DID 変換を設定するには、次の手順に従います。

1. 変換を追加するには、[追加]をクリックします。

2. [ダイヤルプラン名]フィールドに、ダイヤル プランの名前を入力します。ダイヤル プランの説明は一意で、15 文字以内にする必要があります。
3. [DID範囲開始]フィールドに、PSTN 番号範囲の開始番号を入力します。番号の範囲は一意でなければなりません。PSTN 番号の範囲を重複して定義すると、エラーを発生します。
4. [DID範囲終了]フィールドに、PSTN 番号範囲の終了番号を入力します。
5. [宛先タイプ]メニューで、内線の呼び出し先のタイプを選択します。
6. [宛先]フィールドに、内線の呼び出し先を次のようにして入力します。
    - [オペレータ]。リダイレクト先のローカル内線番号を入力します。
    - [ハント グループ]。呼び出しがリダイレクトされるハント グループを選択します。(ハント グループは、[音声機能]タブで作成されたエントリに対応しています。)
    - 選択した[宛先タイプ]が自動音声応答の場合、内線の自動音声応答番号が自動的に入力されます。
7. [トランク]メニューから、音声のエンドポイントを選択します(この PSTN 番号範囲については、このトランクの呼び出しを経由して着信することになります)。

CE520 スイッチを管理する場合

チャネル グループの変更ウィンドウ

このウィンドウは、[イーサチャネル]ウィンドウでポート グループを選択して[修正]をクリックした場合に表示されます。

ローカルおよびリモート ポート グループの変更可能なオプションは、次のとおりです。

- ポート グループに属するポート
- ポートのモード
- ポートの優先度

[ステータス]カラムには、変更するかしないか判断する上で役立つ、ポートに関する情報が表示されます。表示できるステータスは、次のとおりです。

ステータス	意味
[in port-group]	ポートはポート グループ内で稼動しています。
[hot-standby]	最大 8 つの LACP ポートがすでにアクティブになっています。
[suspended]	ポートは、他のポートとの不整合などのため、一時的に稼動していません。
[standalone]	ポートは、ポート グループに属していないリモート ポートに接続されています。
[down]	ポートは稼動していません。接続されていないか、管理上停止している可能性があります。

完了したら、[OK]をクリックします。

デバイスの設定ウィザード

このウィザードは、新しいデバイスや、工場出荷時のデフォルトの設定にリセットされたデバイスを使用できるよう準備するために使用します。

まず、デバイスが属するデバイス ファミリを選択します。

提供されたカテゴリ 5 のイーサネット ケーブルを使用して、デバイスのデュアルパーパス ポートを UC 520 に接続します。

数分間待ってから、ADMIN LED がオフになったことを確認します。これは、デバイスが UC 520 から IP アドレスを受信したことを意味します。デバイスは設定され、Configuration Assistant で管理することができます。

デバイスに何も接続されていないことを確認します。

提供されている電源コードを使用して、AC 電源にデバイスを接続します。

次の手順に進む前に、SYSTEM LED の緑の点滅が停止して、緑の点灯になるまで待ちます。SYSTEM LED が緑に点灯しているときは、デバイスが正常に動作していることを意味します。

注： SYSTEM LED が緑に点滅しなかったり、緑の点灯に変わらなかったり、オレンジ色に変わらない場合、デバイスの Power-On Self Test（POST; 電源投入時自己診断テスト）は失敗しています。

ADMIN ボタンが緑に点滅していることを確認します。これは、デバイスにまだ IP アドレスが設定されていないことを意味します。

この手順では次を実行します。

1. 提供されているカテゴリ 5 のイーサネット ケーブルを使用して、PC をデバイスのダウンリンク ポートに接続します。接続が無線の場合も含め、PC をネットワークに接続しないでください。ラップトップを使用しており、ドックされているときは、ドックを解除します。

   静的な IP アドレスを使用して PC が設定されていないことを確認します。

2. PC がデバイスから IP アドレスを受け取るまで数秒待ちます。
3. ユーザ名およびパスワードの入力を求められたら、[キャンセル]をクリックし、[認証]ウィンドウを閉じます。既存のネットワークから切断されていないか、またはデバイスは設定済みです。

ウィザードによって、デバイスが正しく PC に接続され、コマンドを受信する準備が整っているかどうかが確認されます。

確認が完了すると、ウィザードにより結果が通知されます。

この手順では次を実行します。

1. [ホスト名]フィールドの *Switch* をデバイスのホスト名として受け入れるか、別のホスト名を入力します。次の文字は使用できません。

   スペース @ $ & * ( ) + = , : ' # % / ¥ ? ; < > { } | ^ ~ [ ] ` " !

2. [ユーザ名]フィールドに、デバイスへのアクセスに必要なユーザ名を入力します。次の文字は使用できません。

   スペース + # % / ¥ ? ; ' < > { } | ^ ~ ` [ ] " !

   最大 64 文字が許可されます。

3. [パスワード]フィールドに、デバイスへのアクセスに必要なパスワードを入力します。パスワードでは大文字と小文字を区別します。次の文字は使用できません。

   スペース + # % / ¥ ? < > { } | ^ ~ ` [ ] "

   最大 25 文字が許可されます。

4. [パスワード確認]フィールドにパスワードをもう一度入力します。

ウィザードでは、接続されている PC から日付、時間、時間帯の値が取得され、ドロップダウン リストに表示されます。これらの値のいずれかを変更する場合は、[PCとの同期]をオフにして、リストから他の値を選択します。

次の時間帯では、サマータイムがサポートされています。

- 北米

  (GMT - 09:00)アラスカ
  (GMT - 08:00)太平洋標準時(米国およびカナダ); ティファナ
  (GMT - 07:00)山地標準時(米国およびカナダ)
  (GMT - 06:00)中部標準時(米国およびカナダ)
  (GMT - 05:00)東部標準時(米国およびカナダ)
  (GMT - 03:30)ニューファンドランド(カナダ)

- ヨーロッパ

  (GMT - 01:00)アゾレス諸島、カーボベルデ島
  (GMT)グリニッジ標準時: ダブリン、エジンバラ、リスボン、ロンドン
  (GMT + 01:00)アムステルダム、コペンハーゲン、マドリッド、パリ、ビリニュス
  (GMT + 02:00)ヘルシンキ、エルサレム

- オーストラリア

  (GMT + 09:30)アデレード
  (GMT + 10:00)グアム、ポートモレスビー、シドニー

これらのいずれかの時間帯を選択すると、[サマータイム]チェックボックスが有効になり、オンになります。

IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを DHCP を使用して動的に割り当てるには、[動的(DHCP)]を選択します。[IPアドレス]、[サブネットマスク]、および[デフォルトゲートウェイ]フィールドが無効になり、デバイスが DHCP サーバに接続されると自動的に割り当てられます。

任意の IP アドレスを割り当てるには、[静的]を選択します。値は、[IPアドレス]、[サブネットマスク]、および[デフォルトゲートウェイ]フィールドに入力します。

[終了]をクリックすると、ウィザードへの入力がすべてデバイスに送信されます。設定の進捗状況が進捗状況バーに表示され、設定が終了するとステータス メッセージが通知されます。

デバイスから切断されます。デバイスの管理および追加設定を Configuration Assistant で行うには、PC およびデバイスをネットワークに接続します。

提供されている電源コードを使用して、AC 電源にデバイスを接続します。

提供されているカテゴリ 5 のイーサネット ケーブルを使用して、PC をデバイスのポート 1 に接続します。

注: IP アドレスを動的に受信するように PC が 設定されていることを確認します。

この手順では次を実行します。

1. [ホスト名]フィールドにホスト名を入力します。最大 31 文字が許可されます。
2. [ユーザ名]フィールドに、デバイスへのアクセスに必要なユーザ名を入力します。次の文字は使用できません。

   スペース + # % / ¥ ? ; ' < > { } | ^ ~ ` [ ] " !

   最大 24 文字が許可されます。
3. [パスワード]フィールドに、デバイスへのアクセスに必要なパスワードを入力します。パスワードでは大文字と小文字を区別します。次の文字は使用できません。

   スペース + # % / ¥ ? < > { } | ^ ~ ` [ ] "

   最大 24 文字が許可されます。
4. [パスワード確認]フィールドにパスワードをもう一度入力します。

ウィザードでは、接続されている PC から日付および時間の値が取得され、ドロップダウン リストに表示されます。これらの値のいずれかを変更する場合は、[PCとの同期]をオフにして、リストから他の値を選択します。

[国番号]ドロップダウン リストから国を選択します。デフォルトの国コードは[(US) United States]です。

管理インターフェイスの情報を入力します。

- [IPアドレス]フィールドに、管理インターフェイスのIPアドレスを入力します。
- [サブネットマスク]リストで、サブネット マスクを選択します。
- [デフォルトゲートウェイ]フィールドに、デフォルト ゲートウェイの IP アドレスを入力します。
- [VLAN ID]フィールドは読み取り専用です。デフォルトでは *1* が割り当てられています。

- [ポート]リストから、このインターフェイスのコントローラ物理ポートを選択します。
- [DHCPサーバIPアドレス]フィールドに、プライマリ DHCP サーバの IP アドレスを入力します。

AP マネージャ インターフェイスの情報を入力します。

- [転送モード]フィールドは読み取り専用です。デフォルトでは *LAYER3* が割り当てられています。
- [IPアドレス]フィールドに、AP マネージャ インターフェイスの IP アドレスを入力します。

  注: 管理インターフェイス、AP マネージャ インターフェイス、およびデフォルト ゲートウェイの IP アドレスは、同じサブネット内にある必要があります。

CE520 スイッチを次のように準備します。

1. AP521 に接続する CE520 スイッチを選択します。
2. CE520 スイッチ上の使用可能な PoE ポートを選択し、機能バーから[設定] > [スマートポート]を選択して、ポートのロールを[アクセスポイント]に変更します。
3. PoE ポートで、ネイティブ VLAN を **1** に変更します。
4. VLAN 1 から、稼動している DHCP サーバにアクセスできることを確認します。DHCP サーバの VLAN 1 クライアント用の IP プールには、少なくとも 1 つの使用可能な IP アドレスがある必要があります。

AP521 を次のように CE520 スイッチに接続します。

1. ケーブルおよび電源への接続は上面カバーから行います。AP521 を平らな場所に置き、ユーザの反対方向にカバーを、停止するまで静かにスライドさせます。
2. AP521 に何も接続されていないことを確認します。
3. カテゴリ 5 のイーサネット ケーブルを使用して、AP521 のイーサネット ポートを CE520 スイッチの PoE ポートに接続します。
4. AP521 のすべての LED が緑であることを確認します。

提供されている電源コードを使用して、AC 電源にデバイスを接続します。

このデバイスに他のネットワーク デバイスが接続されていないことを確認します。他のデバイスが接続されている場合、切断するか電源を落とします。

提供されているカテゴリ 5 のイーサネット ケーブルを使用して、PC をデバイスのダウンリンク ポートに接続します。PC を他のものに接続しないでください。

PC がデバイスから IP アドレスを受け取るまで数分待ちます。

ユーザ名とパスワードの入力を求められたら、ルータのデフォルトのクレデンシャルを入力します。

[次へ]をクリックし、接続の確認を開始します。

接続の確認が完了したら、ウィンドウに表示されている指示に従います。

ホスト名とユーザのクレデンシャルを設定するには、次の手順に従います。

1. [ホスト名]フィールドに、認証クレデンシャルとして使用するホスト名を入力します。この名前は 一語にする必要があります。また、疑問符やスペースを含むことはできません。
2. [ユーザ名]フィールドに、認証クレデンシャルとして使用する名前を入力します。この名前は一語にする必要があります。また、疑問符やスペースを含むことはできません。
3. [パスワード]フィールドに、このホスト名のパスワードを入力します。パスワードの長さは 1 から 25 文字にする必要があります。スペースを含めることもできます。
4. [パスワード確認]フィールドにパスワードをもう一度入力します。

インターネット接続を有効にするには、次の手順に従います。

1. [WANインターフェイス]リストからインターフェイスを選択します。
2. [修正]をクリックし、[インターネット接続の修正]ウィンドウを使用します。
3. 変更を保存してウィンドウを閉じるには、[OK]をクリックします。

ローカル設定を行うには、次の手順に従います。

1. [地域]リストから、Cisco Unified Communications Manager Express の地域を選択します。それによって、電話のトーンと鳴り方が設定されます。
2. [電話の言語]リストから、ユーザの電話に表示される言語を選択します。
3. [ボイスメールの言語]リストから、ユーザに聞かせるボイス メール プロンプトの言語を選択します。言語パックをインストールするには、次の手順に従います。
    1. Cisco Unified Communications Manager Express の、必要な言語の tar ファイルをダウンロードします。
    2. Cisco Unity Express の、必要な言語のパッケージ ファイルをダウンロードします。
    3. [言語ファイルの場所]フィールドに表示されているフォルダにファイルをコピーします。
    4. [適用]をクリックします。

注: ロケール、時間帯、または日付形式のパラメータを変更すると、IP Phone はリブートします。

このページに挙げられたパラメータが、デバイスに適用されます。

CE520 スイッチを管理する場合

ローカルユーザ名/パスワードの作成ウィンドウ

このウィンドウは、[ユーザとパスワード]ウィンドウの[ローカルユーザ名/パスワード]タブで[作成]をクリックした場合に表示されます。このウィンドウを使用すると、ユーザ名、パスワード、および関連付ける特権レベルを指定できます。

次の手順に従います。

1. [ユーザ名]フィールドに、ユーザが Configuration Assistant へのアクセスに使用する名前を入力します。
2. [パスワード]フィールドに、ユーザが使用するパスワードを入力します。入力した情報は暗号化され、アスタリスクとして表示されます。

3. ［パスワード確認］フィールドにパスワードをもう一度入力します。
4. ［特権レベル］リストで、特権レベルを選択します。

   レベル 15 では読み取り/書き込みアクセス、レベル 1 から 14 では読み取り専用アクセスが与えられます。

5. ［OK］をクリックします。［ユーザとパスワード］ウィンドウに戻ると、［ローカルユーザ名/パスワード］タブに新規エントリが表示されます。

用語集

AAA

認証、認可、課金。「トリプル エー」と読みます。

ABR

エリア境界ルータ。1 つ以上の OSPF エリアの境界に配置され、これらのエリアをバックボーン ネットワークに接続するルータ。ABR は、OSPF バックボーンとこれに接続されたエリアの両方のメンバと見なされます。このため、ABR では、バックボーンとエリアの両方のトポロジを表すルーティング テーブルが管理されます。

AES

高度暗号化規格。128、192、または 256 ビットのキーを使用してデータを暗号化および復号化できるブロック サイファ。「AES CCMP」も参照してください。

AES CCMP

Advanced Encryption Standard-Counter Mode with Cipher Block Chaining Message Authentication Code Protocol。AES を使用する暗号化プロトコル。CCMP アルゴリズムは、無線パケットのデータ発信元認証とデータ整合性を提供するメッセージ整合性コードを生成します。

AP マネージャ インターフェイス

ライトウェイト アクセスポイントが WLAN コントローラに追加された後、その二者間のすべてのレイヤ 3 通信に使用されるインターフェイス。

ARP

アドレス解決プロトコル。IP アドレスを MAC アドレスにマッピングするために使用されるインターネット プロトコル。

ATM

複数のサービス タイプ（音声、ビデオ、データなど）が固定長（53 バイト）のセルで伝送されるセル リレーの国際規格。固定長のセルを使用すると、ハードウェアでセルの処理を実行できるため、伝送の遅延を低減できます。ATM は、E3、SONET、T3 などの高速伝送メディアの利点を活用できるように設計されています。

AWP

選択型ポート。単一の論理ポートとして動作する 2 つの物理ポート。通常は、一方のポートがファイバ SFP コネクタを使用し、他方のポートが銅 RJ-45 コネクタを使用します。

BOOTP

ブートストラップ プロトコル。ネットワーク ノードで、ネットワークのブーティングに影響を与えるイーサネット インターフェイスの IP アドレスの特定に使用されるプロトコル。

CAC

コール アドミッション制御。特定のリンクで同時にアクティブにできるコール数を制限することによって、音質を規制するプロセス。CAC では、リンクの特定レベルの音質は保証されませんが、リンク上のアクティブなコールに消費される帯域幅をユーザが規制できるようにします。

CAS

Channel-associated signaling（CAS; チャネル連携信号）。音声チャネル内の信号情報の伝送。ネットワークで他の目的にユーザ帯域幅が失われるため、CAS 信号は、しばしば Robbed-bit signaling（RBS; 損失ビット シグナリング）とも呼ばれます。

CCKM

Cisco Centralized Key Management。無線 Voice over IP（VoIP）など、時間依存のアプリケーションをサポートするプロトコル。CCKM では、迅速なキー再生成技術を使用し、クライアントがコントローラを介することなく、1 つのアクセスポイントから別のアクセスポイントにローミングすることを可能にします。

CDP

Cisco Discovery Protocol。デバイスが他のデバイスに自身の存在をアドバタイズし、同一 LAN 上、または WAN のリモート側に配置されている他のデバイスの情報を受信する際に使用するプロトコル。

CEF

シスコ エクスプレス フォワーディング。IP 用の拡張レイヤ 3 スイッチング技術。CEF は、大規模で動的なトラフィック パターン（インターネット、ウェブ ベースのアプリケーション、および対話型セッションに関連付けられたものなど）を持つネットワークの、ネットワーク パフォーマンスとスケーラビリティを最適化します。

CGMP

Cisco Group Management Protocol。要求元クライアントに対する IP マルチキャスト パケットの伝送を制限することによって、これらのパケットのフラッディングを減少させるプロトコル。端末がクライアントになるには、CGMP グループに加入するための加入メッセージを送信します。グループから脱退する場合は、脱退メッセージを送信します。

Cisco Configuration Assistant

「Configuration Assistant」を参照。

Cisco Discovery Protocol

「CDP」を参照。

Cisco Group Management Protocol

「CGMP」を参照。

Configuration Assistant

デバイスのコミュニティの作成、デバイスの設定、リアルタイムのデバイス イメージの監視、およびネットワーク障害のトラブルシューティングを実行するアプリケーション。

DHCP

Dynamic Host Configuration Protocol。ホストで不要になった IP アドレスを再利用できるように、IP アドレスを動的に割り当てるメカニズム。

DID

ダイヤルイン。オペレータや電話の自動音声応答を使用せずに、発信者が Private Branch Exchange（PBX; 構内交換機）内の内線やパケット音声システムに直接ダイヤルすることができる、電話会社が提供するサービス。このサービスでは、PBX、ルータおよびゲートウェイに、電話番号の最後の 3 ～ 5 の桁のみを転送する、DID トランクが使用されます。IOS 音声デジタル（T1/E1）インターフェイスでの Direct-Inward-Dial（DID; ダイヤルイン）の概要も参照してください。

digest_authentication

ユーザ エージェント（UA）が Cisco CallManager に要求を送信する際、Cisco CallManager による SIP UA のアイデンティティの認証を可能にする、SIP トランクおよび電話用のプロセス。（SIP ユーザ エージェントとは、SIP メッセージを発信するデバイスまたはアプリケーションです。）SIP 電話でのダイジェスト認証の設定も参照してください。

DMZ

非武装地帯。インターネットとプライベート ネットワーク間のバッファ ゾーン。インターネット上の外部クライアントがアクセスするウェブ、FTP、およびメール サーバに通常使用されるパブリック ネットワークです。これらのパブリック アクセス サーバを個別の分離されたネットワークに配置することによって、内部ネットワークのセキュリティ強度を高めることができます。

DNS

ドメイン ネーム サービス。文字で構成されるドメイン名を、数字で構成される IP アドレスに変換するインターネット サービス。

Dynamic Host Configuration Protocol

「DHCP」を参照。

E&M

Equal Access North American。CAS シグナリングの 4 つの一般的な形態のうちの 1 つ。他には、グラウンドスタート、ループスタート、および EANA があります。

EANA

Equal Access North American。CAS シグナリングの 4 つの一般的な形態のうちの 1 つ。他には、グラウンドスタート、ループスタート、および E&M があります。

EAP

拡張認証プロトコル。アクセスポイントが無線クライアント デバイスと RADIUS サーバによる認証の実行および動的 WEP キーの生成を補助する認証方式。

EAP でのオープン認証

アクセスポイントがすべてのクライアント デバイスに対して、ネットワークに接続する前に EAP 認証の実行を強制する認証方式。

Easy VPN

Cisco Unified Client Framework に基づく、集中 VPN 管理ソリューション。Cisco Easy VPN は、Cisco Easy VPN リモート クライアントと Cisco Easy VPN サーバの 2 つのコンポーネントで構成されます。

EIGRP

Enhanced IGRP。コンバージェンス プロパティと動作効率に優れ、リンクステート プロトコルとディスタンスベクタ プロトコルの利点を兼ね備えた、Cisco 版の IGRP。

FRU（現場交換可能ユニット）

ユーザまたは技術者による現場での取り外しおよび交換が可能なハードウェア コンポーネント。

FTP

ファイル転送プロトコル。TCP/IP プロトコル スタックの一部で、ホスト間のファイルの転送に使用されます。

GBIC

ギガビット インターフェイス コンバータ。電流（デジタルの高低）を光信号に、および光信号をデジタル電流に変換するトランシーバ。GBIC は通常、高速ネットワーキング用インターフェイスとして光ファイバ システムおよびイーサネット システムで使用されます。データ転送速度は、毎秒 1 ギガビット（Gbps）以上です。

HSRP

Hot Standby Routing Protocol。ネットワークの高可用性を実現し、ネットワーク トポロジの透過的な変更を可能にするプロトコル。このプロトコルではデバイス グループが作成され、そのうちの 1 つのリード デバイスが、ホット スタンバイ アドレスに送信されるすべてのパケットを処理します。このリード デバイスは、グループ内の他のデバイスによって監視され、リード デバイスに障害が発生した場合は、他のいずれかのデバイスがリード デバイスの役割とホット スタンバイ アドレスを継承します。

HWIC

高速 WAN インターフェイス カード。ルーティング機能を持つ Cisco デバイスで、統合されたアクセスポイント機能を提供する HWIC フォームファクタ内の無線 LAN インターフェイス。

ICMP

インターネット制御メッセージ プロトコル。エラーを報告し、IP パケット処理に関連するその他の情報を提供する、ネットワーク レイヤ インターネット プロトコル。

IGMP

インターネット グループ管理プロトコル。LAN 上のホストとルータ間で、ホストが属するマルチキャスト グループの特定に使用されるプロトコル。

IGMP スヌーピング

ホストからルータに送信される IGMP パケット内のレイヤ 3 情報をレイヤ 2 スイッチが検査すること。スイッチは、検出した情報から、メンバ ポートを追加するか削除するかを判断します。

IGRP

Interior Gateway Routing Protocol。大規模な異種ネットワーク間のルーティングに関する問題に対処する Interior Gateway Protocol。

IKE

インターネット キー エクスチェンジ。IPSec やその他の規格と組み合わせて使用されるキー管理プロトコル規格。IPSec は IKE なしでも設定できますが、IKE を使用すると他の機能や柔軟性が付加され、IPSec 規格の設定も簡略化されるため、IPSec の質を高めることができます。IKE は、IPSec ピアの認証、IPSec キーのネゴシエーション、および IPSec セキュリティ アソシエーションのネゴシエーションを提供します。

Interior Gateway Protocol

自律システム内のルーティング情報の交換に使用されるインターネット プロトコル。

IP Phone

IP ネットワークを介して音声通信を提供するフル機能の電話。

IPSec

参加ピア間のデータの機密性、データの整合性、およびデータ認証を提供する、オープン スタンダードの枠組み。IPSec は、これらのセキュリティ サービスを IP レイヤで提供します。IPSec では、IKE を使用して、ローカル ポリシーに基づいてプロトコルとアルゴリズムのネゴシエーションが処理され、IPSec で使用される暗号キーと認証キーが生成されます。IPSec を使用すると、2 つのホスト間、2 つのセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホスト間の 1つ以上のデータ フローを保護できます。

IP アドレス

TCP/IP を使用するホストに割り当てられる 32 ビットのアドレス。このアドレスは 5 つのクラス（A、B、C、D、E）のいずれかに属し、ピリオドで区切られた 4 つのオクテット（ドット付きの 10 進数表記）で書き込まれます。各アドレスは、ネットワーク番号、サブネットワーク番号（任意）、およびホスト番号で構成されます。ネットワーク番号とサブネットワーク番号の組み合わせはルーティングに使用され、ホスト番号はネットワークまたはサブネットワーク内の個々のホストのアドレス指定に使用されます。サブネット マスクは、IP アドレスからネットワーク情報およびサブネットワーク情報を抽出するために使用されます。

ISL

スイッチ間リンク。VLAN の情報をスイッチとルータ間のトラフィック フローとして管理する、Cisco 独自のプロトコル。

LACP

リンク集約制御プロトコル。複数の物理インターフェイスをバンドルして 1 つの論理インターフェイスを形成するための、IEEE 802.3AD 仕様をサポートするプロトコル。

LEAP

Lightweight Extensible Authentication Protocol（ライトウェイト拡張認証プロトコル）。ログオン パスワードを共有秘密として使用する、クライアントおよび RADIUS サーバ間の強力な相互認証をサポートする、無線 LAN 用の 802.1X 認証タイプ。ユーザごと、セッションごとの動的な暗号鍵が提供されます。

LED ポーリング間隔

Configuration Assistant がコミュニティ内のポートをポーリングして、ポートの LED の色の変化を表示する頻度。「グラフ ポーリング間隔」、「状態ポーリング間隔」、および「ネットワーク ポーリング間隔」も参照してください。

MAC

メディア アクセス制御。IEEE で定義されているデータ リンク レイヤの下位レイヤである 2 つのサブレイヤ。MAC サブレイヤは、トークン パッシングとコンテンションのどちらを使用するかなどの、共有メディアへのアクセスを指定します。

MAC アドレス

LAN に接続されている各ポートまたはデバイスに要求される、標準化されたデータ リンク レイヤ アドレス。ネットワーク内の他のデバイスは、これらのアドレスを使用してネットワーク内の特定のポートの場所を見つけて、ルーティング テーブルとデータ構造を作成および更新します。MAC アドレスは 6 バイトの長さで、IEEE により制御されます。

MEL CAS

Mercury Exchange Limited（MEL）Channel Associated Signaling。英国で主に使われている、音声シグナリング プロトコル。「CAS シグナリング」、「グラウンドスタート」、「EANA」、および「E&M」も参照してください。

MWI サーバ

SIP MWI（メッセージ受信のインジケータ）サーバとは、SIP MWI メッセージを Cisco Unity Connection サーバおよび他のすべての Cisco Unified CM Express ルータ（SIP MWI クライアント）間でリレーする、プロキシ サーバです。

NAT

ネットワーク アドレス変換。IP アドレスをグローバルに一意のものにする必要性を低減するためのメカニズム。NAT を使用すると、グローバルに一意でない IP アドレスを使用している組織が、それらのアドレスをグローバルにルーティングできる IP アドレスに変換することにより、インターネットに接続できるようになります。

NetFlow

着信パケットをフローに分類できる一部のルータの機能。フロー内のパケットは同一の方法で処理できる場合が多いため、この分類を使用すると、ルータの作業を一部省略して、スイッチング処理を高速化できます。

NTP

ネットワーク タイム プロトコル。インターネット上に配置されているラジオ クロックとアトミック クロックを参照してローカルの正確なタイムキーピングを確保するプロトコル。

OSPF

Open Shortest Path First。ホップ カウントに制限を設けず、ルーティングの変更を即時に伝播し、可変長のサブネット マスクをサポートし、実際のリンク コストに基づく負荷分散を可能にするリンクステート プロトコル。また、ネットワークをエリアと呼ばれる小領域に区分することによって、リンクステートの更新によって発生するトラフィックを制限します。

PAD

パケット アセンブラ/ディスアセンブラ。単純なデバイス（特定のプロトコルのフル機能をサポートしていないキャラクタモードの端末など）をネットワークに接続するデバイス。PAD は、データをバッファに入れ、このようなエンド デバイスに送信されるパケットの組み立てまたは分解を行います。

PAT

ポート アドレス変換。TCP 接続または UDP 対話の送信元ポートを変換することによって、グローバル アドレス プール内のアドレスを節約します。複数の異なるローカル アドレスが同一のグローバル アドレスにマッピングされ、ポート変換によって必要な一意性が確保されます。グローバル プールのアドレスは、常に PAT アドレスより優先的に使用されます。

PBX

構内交換機。加入者の構内に配置されるデジタルまたはアナログ電話交換機で、専用電話網および公衆電話網の接続に使用されます。

PIM

Protocol Independent Multicast。既存の IP ネットワークに IP マルチキャスト ルーティングを追加できるマルチキャスト ルーティング アーキテクチャ。PIM は、ユニキャスト ルーティング プロトコルには依存せず、稠密モードと希薄モードの 2 つのモードで使用できます。「PIM 稠密モード」および「PIM 希薄モード」も参照してください。

PIM 希薄/稠密モード

マルチキャスト グループが稠密モードの場合はインターフェイスが稠密モードとして処理され、マルチキャスト グループが希薄モードの場合はインターフェイスが希薄モードとして処理される動作モード。ルータがグループのランデブー ポイント（RP）を検出した場合、グループは希薄モードになります。

PIM 希薄モード

データがネットワーク内の最小限の数のルータに配信される動作モード。パケットは、RP（ランデブー ポイント）で明示的に要求された場合にだけ送信されます。受信者は広範囲に分散しており、送信されるデータグラムがダウンストリーム ネットワークで必ずしも使用されるわけではないことが想定されています。希薄モードを使用すると、明示的な加入メッセージの定期的更新に依存することになり、RP が必要になります。「PIM 稠密モード」および「PIM 希薄/稠密モード」も参照してください。

PIM 稠密モード

プルーニングや切り捨てが発生するまで、すべての発信インターフェイスにパケットが転送される動作モード。受信者の密度が高く、転送されるデータグラムをダウンストリーム ネットワークで受信したのち、それらのデータグラムが使用される可能性が高いことが想定されています。稠密モードを使用すると、デフォルトでフラッディング動作が生じます。「PIM 希薄モード」および「PIM 希薄/稠密モード」も参照してください。

PKI

公開キー インフラストラクチャ。証明書管理、保存管理、キー管理、トークン管理などの機能を通じてデータ通信における非対称キー暗号方式の使用をサポートする、認証局（CA）および登録局（RA）のシステム。または、非対称キーの交換に使用する規格。このタイプの交換では、

メッセージ受信者はメッセージ内の署名を信頼することができ、メッセージ送信者は目的の受信者に対してメッセージを適切に暗号化できます。「キー管理」を参照してください。

PoE

Power over Ethernet。接続されているデバイスに、電源コードからではなく、データ ケーブルから給電する技術。

Power over Ethernet

「PoE」を参照。

PPPoE

Point-to-Point Protocol over Ethernet。イーサネット フレーム内でカプセル化されたポイントツーポイント プロトコル（PPP）。PPPoE を使用すると、イーサネット ネットワーク上のホストは、ブロードバンド モデムを介してリモート ホストに接続できます。

PSTN

公衆電話交換網。世界的に使用されている、さまざまな電話網とサービスを指す一般用語。

QoS

Quality of Service。選択したネットワーク トラフィックに、より品質の高いサービスを提供するネットワークの機能。QoS の第一の目的は、専用の帯域幅、ジッタと遅延の制御（一部のリアルタイムの対話型トラフィックで必要）、および損失特徴の改善の優先度を設定することです。

RADIUS

リモート認証ダイヤルイン ユーザ サービス。モデムと ISDN 接続の認証、および接続時刻のトラッキングに使用されるデータベース。

RIP

Routing Information Protocol。インターネットで最もよく使用されている Interior Gateway Protocol。ホップ カウントがルーティング メトリックとして使用されます。

RP

ランデブー ポイント。PIM-SM（PIM 希薄モード）の共有マルチキャスト配信ツリーのルートであるマルチキャスト ルータ。

RP

ランデブー ポイント。PIM 希薄モードの実装において、マルチキャスト グループのメンバシップをトラッキングし、マルチキャスト グループのアドレスにメッセージを転送するよう指定されたルータ。

RPS（冗長電源システム）

最大 6 個のネットワーク デバイスの内部電源をシームレスにフェールオーバーするための冗長電源システム。RPS は、接続されているデバイスの内部電源障害を自動的に検知して、障害が生じたデバイスに給電し、ネットワーク トラフィックの損失を防ぎます。

SDP

1. セッション記述プロトコル。IP 上のマルチメディア トランスポートを確立するのに必要な情報を定義するためのプロトコル。SDP は、セッションの告知、セッションの招待、トランスポートのアドレス、メディアのタイプなどの情報を送信します。たとえば SIP コールの場合、SDP メッセージは、NTE を使用して送信するイベントや NTE ペイロード タイプの値を示します（NTE を使用する場合）。2.セキュア デバイス プロビジョニング。Cisco IOS クライアントや Cisco IOS 証明書サーバなどの 2 つのエンド デバイス間に PKI（公開キー インフラストラクチャ）を展開します。

SFP

着脱可能小型フォーム ファクタ。現場交換可能レーザー光トランシーバ モジュール。SFP モジュールを使用すると、他のスイッチへのギガビット アップリンク接続が可能になります。

SFP（着脱可能小型フォーム ファクタ）モジュール

100BASE および 1000BASE のポートにプラグインされ、光ファイバまたは銅ケーブルのネットワークを使用してモジュール ポートに接続される、ホットスワップ可能な入出力デバイス。

SFTP

SSH ファイル転送プロトコル。SFTP は SSH の一部であり、ルータ上で常に有効になっています。適切な権限レベルを持つユーザは、SFTP を使用して、ルータにファイルをコピーしたり、ルータからファイルをコピーしたりできます。

SIP

セッション開始プロトコル。特に 2 つのパーティ間の音声会議など、呼処理セッションを有効にします。SIP はセッション記述プロトコル（SDP）と連動して呼のシグナリング処理を行います。SIP を使用すると、ルータは SIP Voice over IP（VoIP）ゲートウェイおよび VoIP プロキシ サーバをサポートできます。

SMTP

シンプル メール転送プロトコル。メール サービスを提供するインターネット プロトコル。

SNMP

簡易ネットワーク管理プロトコル。ネットワーク デバイスを監視および制御する手段のほか、設定、統計情報収集、パフォーマンス、およびセキュリティを管理する手段を提供する、TCP/IP ネットワークのプロトコル。

SPAN

スイッチド ポート アナライザ。監視対象の一連のポート（または VLAN）の指定に使用される機能。これらの送信元ポート上のトラフィックのコピーは、1 つの指定された宛先ポートに送信されます。通常、送信元ポート上のトラフィックを確認するには、ネットワーク アナライザを宛先ポートに接続します。「ローカル SPAN」および「リモート SPAN」も参照してください。

SSH

セキュア シェル。TCP/IP などの信頼できるトランスポート レイヤの上位で実行されるアプリケーションで、強力な認証機能および暗号化機能を提供します。

SSID

サービス セット ID。無線ネットワーク上のパケットに添付されて、各パケットをそのネットワークの一部として識別するコード。相互に通信を試行する無線デバイスはすべて、同じ SSID に関連付ける必要があります。

STP

スパニング ツリー プロトコル。複数のブリッジまたはスイッチで構成されるネットワークを管理するための一般的な技術です。ネットワーク トポロジが変わると、STP はブリッジとスイッチを透過的に再設定し、ポートを転送状態またはブロッキング状態にして、ループが作成されるのを防ぎます。各 VLAN は個別のブリッジとして処理され、STP の個別インスタンスが各 VLAN に適用されます。

SVI

スイッチ仮想インターフェイス。レイヤ 3 のデバイスで VLAN へのアクセスに使用する IP アドレスが割り当てられている VLAN。SVI は、VLAN 間でパケットをルーティングするように設定できます。

TCAM

Ternary CAM。ACL および QoS ポリシーのハードウェア実装に使用されるメモリ ブロック。パケットを受信すると、スイッチはハードウェア テーブル ルックアップ（TCAM ルックアップ）を実行して、そのパケットを許可または拒否します。ACL または QoS ポリシーが多すぎたり、TCAM がいっぱいになったりすると、パフォーマンスに悪影響が生じます。

TCP

Transmission Control Protocol。信頼性のある全二重データ伝送を提供する、接続指向のトランスポート レイヤ プロトコル。TCP は、TCP/IP プロトコル スタックの一部です。

TCP/IP

世界規模のインターネットワークの構築を支援するプロトコル スイートの一般名。

Telnet

インターネットなどの TCP/IP ネットワークのターミナル エミュレーション プロトコル。Telnet は、ウェブ サーバをリモートに制御するための一般的な手段です。

Temporal Key Integrity Protocol

「TKIP」を参照。

TFTP

Trivial File Transfer Protocol。ネットワークを介したコンピュータ間のファイル転送を実現する FTP の簡易バージョン。通常は、クライアント認証（ユーザ名とパスワードなど）は使用されません。

TKIP

Temporal Key Integrity Protocol。WEP に対する攻撃を阻止するための暗号化方式。WEP には、侵入者が、暗号化されたパケットに含まれる初期化ベクタ（IV）と呼ばれる暗号化されていないセグメントを使用して WEP キーを算出できるという脆弱性があります。

Transmission Control Protocol

「TCP」を参照。

Transmission Control Protocol/Internet Protocol

「TCP/IP」を参照。

Trivial File Transfer Protocol

「TFTP」を参照。

UDP

ユーザ データグラム プロトコル。TCP/IP スタックのうちのコネクションレス型トランスポート レイヤ プロトコル。UDP は、確認応答や配信保証を行わずにデータグラムを交換する簡易プロトコルであるため、エラー処理と再送信は他のプロトコルで処理する必要があります。

VLAN

物理的に構成された LAN ではなく、ビジネスの目的または特定のプロジェクトに合わせて作成されたワークグループで構成される論理的な LAN。各メンバの実際の位置には依存しません。

VLAN トランキング プロトコル

「VTP」を参照。

VLAN メンバシップ ポリシー サーバ

「VMPS」を参照。

VPN

バーチャル プライベート ネットワーク。パブリック インフラストラクチャ上でプライベート ネットワークと同レベルのネットワーク セキュリティとプライバシーを実現します。VPN を使用すると、ネットワーク間のすべてのトラフィックが暗号化されるため、パブリック TCP/IP ネットワーク上で IP トラフィックを安全に伝送することができます。VPN では、IP レベルのすべての情報の暗号化にトンネリングが使用されます。

VTP

VLAN トランキング プロトコル。ネットワーク全体における VLAN の追加、削除、名前変更を管理することによって VLAN 構成の一貫性を保持する、レイヤ 2 のメッセージング プロトコル。

VTP プルーニング

プルーニング適格リストに指定されたトランク ポートの VLAN に対する、ブロードキャスト、マルチキャスト、および不明なユニキャストのフラッディング トラフィックを阻止すること。

WEP

Wired Equivalent Privacy。通信の機密性を保つために、アクセスポイントとクライアント デバイス間の通信をスクランブルする暗号化技術。アクセスポイントとクライアント デバイスはどちらも、無線信号の暗号化および復号化に同じ WEP キーを使用します。

Wi-Fi Protected Access

「WPA」を参照。

WINS

Windows Internet Naming Service。特定のネットワーク コンピュータに関連付けられている IP アドレスを特定する Windows システム。

Wired Equivalent Privacy

「WEP」を参照。

WMM

Wireless Multimedia。無線 LAN 用の QoS 拡張。WMM では、802.11E QoS Basic Service Set（QBSS; QoS 基本サービス セット）標準を満たすデバイスをサポートしています。WMM では、音声、ビデオ、およびベストエフォート型データに対するディファレンシエーテッド サービスを有効にして、ネットワーク上で他のトラフィックより先に音声トラフィックを処理できるようにします。

WPA

Wi-Fi Protected Access。無線 LAN システムのデータの保護およびアクセス制御のレベルを向上させる、標準ベースの相互運用可能なセキュリティ機能拡張。WPA キー管理を使用して、クライアントおよび認証サーバは、EAP 認証方式によって相互認証を実行し、ペアワイズ マスター キー（PMK）を生成します。WPA では、データの保護に TKIP が使用され、認証済みキーの管理に IEEE 802.1X が使用されます。

WPA2

Wi-Fi Protected Access 2。データの保護に AES CCMP を使用する、標準ベースの相互運用可能なセキュリティ機能拡張。WPA2 では、AES によって TKIP より強力な暗号化が実現されるため、WPA より高いレベルのセキュリティが確保されます。

WPA2-PSK

WPA2 事前共有キー。IEEE 802.1X ベースの認証を使用できない無線 LAN に対して WPA2 をサポートする認証方式。事前共有キーは、クライアントとアクセスポイントの両方に設定されます。

WPA-PSK

WPA 事前共有キー。IEEE 802.1X ベースの認証を使用できない無線 LAN に対して WPA をサポートする認証方式。事前共有キーは、クライアントとアクセスポイントの両方に設定されます。

WPA 事前共有キー

「WPA-PSK」を参照。

アクセス VLAN

データ トラフィックのスイッチで使用される VLAN。「ネイティブ VLAN」および「音声 VLAN」も参照してください。

アクセスポイント

無線ネットワークの中心、または無線デバイスと有線ネットワーク間の接続点として機能するデバイス。「自律型アクセスポイント」および「ライトウェイト アクセスポイント」も参照してください。

アクセス ポート

1 つの仮想 LAN（VLAN）のトラフィックを伝送するポート。トランク ポートと対照を成します。

宛先ベースの転送

パケットの宛先アドレスに基づいたポート グループ単位でのパケット転送。送信元ベースの転送と対照を成します。

アドバタイジング

他のルータが利用可能なルートのテーブルを保守管理できるように、定期的にルーティングとサービスの更新を送信するルータの処理。

アドレス解決プロトコル

「ARP」を参照。

アドレス集約

主要なネットワーク アドレスを、スーパーネットと呼ばれる連番のアドレス グループを表す集合体に分割するルーティング プロトコル機能。この機能により、選択されたインターフェイスにおけるより限定的なネットワークのアドバタイズメントは自動的に抑止されます。

アドレス マスク

1 つのアドレスの中でネットワークまたはサブネットを表す部分と、ホストを表す部分を示すために使用されるビットの組み合わせ。「IP アドレス」および「サブネット マスク」も参照してください。

イーサチャネル

スイッチ間またはスイッチとサーバ間の高帯域幅接続用の単一論理ポートとして機能する、ファスト イーサネットポートまたはギガビット イーサネット ポートのグループ。イーサチャネル内のポートに障害が発生すると、そのポート上で伝送されていたトラフィックは、イーサチャネル内の他のポートに転送されます。

イーサネット管理ポート

コンピュータを接続できるレイヤ 3 対応のホスト ポート。イーサネット管理ポートは、ネットワーク管理用のスイッチ コンソール ポートの代わりに使用できます。このポートは、スイッチを管理する目的だけに使用する必要があります。イーサネット管理ポートは、Cisco Configuration Assistant のポート設定機能および IP アドレス機能をサポートしています。

インターネット グループ管理プロトコル

「IGMP」を参照。

インターネット制御メッセージ プロトコル

「ICMP」を参照。

ウィンク スタート

発信側がオフフックになることにより回線を占有します。番号をアウトパルスする前に、他端での受信応答を待機します。これは、障害が発生しているトランクを識別する整合性確認の役割を果たし、ネットワークに、発信側へのリオーダー トーンの送信を許可します。

英数字

英字（大文字と小文字の A から Z）、数字（0 から 9）、および句読点。

エキスパート モード

機能ウィンドウでオプションを選択したり入力フィールドを使用したりすることによってユーザ インターフェイスと対話すること。ガイド モードと対照を成します。

エリア

OSPF リンクステート 更新を共有する近隣ルータのグループ。エリア ID と呼ばれる番号で識別されます。

エンドポイント

SIP の終端またはゲートウェイ。エンドポイントは、コールすることもコールされることもできます。情報のストリームを生成または終了させます。

オープン認証

すべてのデバイスに認証の実行を許可してからアクセスポイントとの通信を試みる認証方式。

親ウィンドウ

メニュー バーのオプションを選択するか、ツールバーのアイコンをクリックすることにより表示される設定ウィンドウ。子ウィンドウと対照を成します。

音声 VLAN

IP Phone からの音声トラフィックのスイッチで使用される VLAN。「アクセス VLAN」および「ネイティブ VLAN」も参照してください。

ガイド モード

一連の手順に応答することによりユーザ インターフェイスと対話すること。エキスパート モードと対照を成します。

外部インターフェイス

セキュリティ アプライアンスの外側にある他の信頼できないネットワーク（WAN またはインターネット）に接続する最初のインターフェイス。通常は、ポート 0 が使用されます。

拡張認証プロトコル

「EAP」を参照。

仮想 LAN

「VLAN」を参照。

仮想インターフェイス

DHCP サーバから IP アドレスを取得する無線クライアントの DHCP サーバ プレースホルダの役割を果たし、ウェブ認証ログイン ウィンドウのリダイレクト アドレスとして機能するインターフェイス。

可変係数

最小コストのパスのコストを乗じた数値。コストが均等でないルーティングで、コストが乗算値を上回るパスを対象から除外するために使用されます。

簡易ネットワーク管理プロトコル

「SNMP」を参照。

管理インターフェイス

デバイスを管理するためのデフォルトのインターフェイス。

管理上のスピード

管理者が指定するリンクのスピード。管理者がスピードを [auto]に指定した場合、実際のスピードは自動ネゴシエーションによって決まります。

キーシステム

1 から 25 人のユーザがいる小規模のオフィス向けの電話通信を処理するように設計された、小規模の電話システム。キーシステムには、アナログまたはデジタルがあります。キーシステムでは、各電話がすべての回線のすべての着信 PSTN コールに応答できます。システム内で複数のコールを同時に着信した場合は、それぞれのコールを目視できるため、IP Phone 上の対応する回線ボタンを押して直接コールを選択することができます。

ギガビット インターフェイス コンバータ

「GBIC」を参照。

共有認証

アクセスポイントに通信を試行しているすべてのデバイスに対して、そのアクセスポイントが暗号化されていないチャレンジ テキスト文字列を送信する認証方式。チャレンジ テキストが正しく暗号化された場合、アクセスポイントはそのデバイスからの認証要求を許可します。

グラウンドスタート

4 つある T1 CAS シグナリングの最も一般的な形態の 1 つですが、主に FXS、FXO または任意のアナログ ポートで使用されるアナログ信号です。他には、ループスタート、EANA、および E&M があります。

グラフ ポーリング間隔

Configuration Assistant がコミュニティのメンバにクエリーを実行して、デバイス グループ全体のデバイス利用率およびリンク利用率のデータを取得する頻度。この情報は、リンクのグラ

フおよび帯域幅のグラフの更新に使用されます。「状態ポーリング間隔」、「LED ポーリング間隔」、および「ネットワーク ポーリング間隔」も参照してください。

経路集約

多数のリンク アドバタイズメントを 1 つのアドバタイズメントに集約することによって、アドバタイズメントの数を減らすルーティング プロトコル機能。

子ウィンドウ

設定ウィンドウ内のボタンをクリックすると表示される別の設定ウィンドウ。親ウィンドウと対照を成します。

高速脱退

ルータからのマルチキャスト グループの削除を高速化するマルチキャスト ルーティング機能。あるメンバがグループから脱退すると、高速脱退機能により、そのグループの他のメンバ（スイッチ上の特定のポートから IP マルチキャスト パケットを受信しているデバイス）が検索されます。ポート上に他のメンバが存在しない場合、スイッチはそのポートをグループから削除します。そのグループにそれ以上ポートが存在しなければ、スイッチは、VLAN に接続されているルータにグループ全体を削除するよう通知します。

コミュニティ

メンバの IP アドレスを使用して管理されるデバイスのグループ。メンバとしては、スイッチ、ルータ、無線アクセス コントローラ、および自律型アクセスポイントがあります。

サービス セット ID

「SSID」を参照。

サブネット マスク

IP で使用される 32 ビットのアドレス マスク。IP アドレスにおいて、ネットワーク番号、サブネットワーク番号、およびノード番号を表すビットを示します。

事前共有鍵

IPSec で提供される認証方式。事前共有鍵では、1 つ以上のクライアントが、個別の共有秘密を使用して、IKE（インターネット キー エクスチェンジ）によって、ゲートウェイへの暗号化されたトンネルを認証できます。事前共有鍵は通常、クライアント数が 10 以下の小規模ネットワークで使用されます。事前共有鍵を使用する場合、セキュリティを確保するために認証局を使用する必要はありません。

自動ネゴシエーション

リンクされているポート同士が相互の特徴を調べ、最適な通信手段を選択する機能。

状態ポーリング間隔

Configuration Assistant がコミュニティ内のデバイスにクエリーを実行して、デバイスのリソースの利用率とデバイスの温度の測定値を取得する頻度。「グラフ ポーリング間隔」、「LED ポーリング間隔」、および「ネットワーク ポーリング間隔」も参照してください。

自律型アクセスポイント

WLAN コントローラからの操作が不要な、フル機能のスタンドアロン アクセスポイント。ライトウェイト アクセスポイントと比較してください。

シンプル メール転送プロトコル

「SMTP」を参照。

スイッチ仮想インターフェイス

「SVI」を参照。

スイッチ仮想インターフェイス（SVI）

レイヤ 3 のデバイスで VLAN へのアクセスに使用する IP アドレスが割り当てられている VLAN。SVI は、VLAN 間でパケットをルーティングするように設定できます。

スイッチド ポート アナライザ

「SPAN」を参照。

スイッチ ポート

物理ポートに関連付けられるレイヤ 2 専用のインターフェイス。アクセス ポートまたはトランク ポートのいずれかになります。

スーパーネット

他のネットワークが集約されているネットワーク。集約されたネットワークはアドバタイズされず、アドレスもバックボーン ルーティング テーブルに存在しません。

スパニング ツリー プロトコル

「STP」を参照。

スプリット トンネリング

スプリット トンネリングを使用すると、VPN クライアントは暗号化なしにローカルに通信できます。ユーザは、トンネル経由でホーム ネットワーク宛てに伝送されるトラフィックだけを送信します。インスタント メッセージ、メール、通常のインターネット ブラウズなど他のトラフィックはすべて、VPN クライアントのローカル LAN を使用してインターネットに送信されます。

静的セキュア アドレス

アドレス テーブルに格納され、実行中の設定に追加される、手動で設定されたセキュア アドレス。「動的アドレス」および「スティッキ MAC アドレス」も参照してください。

静的ルート

明示的に設定されて、ルーティング テーブルに入力されたルート。静的ルートは、動的ルーティング プロトコルによって選択されるルートより優先されます。

セキュア アドレス

VLAN ごとに 1 つのポートだけに転送される MAC アドレス。セキュア アドレスは、スイッチがリロードされた場合でも維持されます。「動的アドレス」および「静的アドレス」も参照してください。

セキュア ポート

アドレス セキュリティ違反が発生した場合は常にユーザ指定の処理が実行されるポート。

選択型ポート

「AWP」を参照。

送信元ベースの転送

パケットの送信元アドレスに基づいたポート グループ単位でのパケット転送。宛先ベースの転送と対照を成します。

即時スタート

発信側がオフフックになることにより回線を占有し、応答を待つことなく、番号のアウトパルスを開始します。

即時脱退

ルータからのマルチキャスト グループの削除を高速化するマルチキャスト ルーティング機能。メンバがグループからの脱退希望を示すと、即時脱退機能により、そのメンバ ポートはグループから即座に削除されます。

遅延ダイヤル

発信側が回線を占有し、遠端側がオンフックかどうか確認するため 200ms 待機します。オンフックの場合、発信側が番号をアウトパルスします。遠端側がオフフックの場合、発信側では遠端側がオンフックになるまで番号のアウトパルスを待機します。

着脱可能小型フォーム ファクタ

「SFP」を参照。

通知名

システム イベントの種類と、それらのイベント通知の送信先メール アドレスを指定する情報コレクションの名前。

ディスタンスベクタ プロトコル

別のネットワークまでの距離のリストをホップ数（交差するルータの数）で管理するルーティング プロトコルの一種。このプロトコル タイプの例として、RIPv2 および EIGRP があります。リンクステート プロトコルと対照を成します。

デフォルト ゲートウェイ

別のネットワークへの出口と別のネットワークからの入り口の両方の役割を果たす、ネットワーク内のノード。

動的アドレス

ポートで学習される MAC アドレス。これは、アドレス テーブルに格納され、スイッチのリロード時に消去されます。ポート セキュリティを有効にしたときに学習された最初の MAC アドレスが、動的セキュア アドレスになります。「静的アドレス」も参照してください。

動的ルーティング

ネットワークトポロジやトラフィックの変更に自動的に適応するルーティング。「適応ルーティング」とも呼ばれます。

特権レベル

ユーザに付与される Configuration Assistant へのアクセスのレベルを指定する数字。レベル 15 では読み取り/書き込みアクセス、レベル 1 から 14 では読み取り専用アクセスが与えられます。

ドメイン名

インターネット上のホストに付けられる、親しみやすく覚えやすい名前。IP アドレスに対応しています。

トランク ポート

複数の VLAN のトラフィックを伝送するポート。アクセス ポートと対照を成します。

トンネル

インターネットなどの共有メディアを介した仮想チャネル。カプセル化されたデータ パケットの交換に使用されます。

内部インターフェイス

デバイスを、セキュリティ アプライアンスで保護された、内部の信頼できるネットワークに接続する最初のインターフェイス。

ネイティブ VLAN

IEEE 802.1Q トランク ポートからのタグのないパケットを伝送する VLAN。「アクセス VLAN」および「音声 VLAN」も参照してください。

ネットワーク EAP

アクセスポイントが無線クライアント デバイスと RADIUS サーバによる認証の実行および動的WEP キーの生成を補助する認証方式。

ネットワーク タイム プロトコル

「NTP」を参照。

ネットワーク ポート

スイッチが、宛先アドレスの不明なすべての VLAN トラフィックを転送するポート。この処理は、VLAN 内のすべてのポートに対するフラッディングの防止に役立ちます。

ネットワーク ポーリング間隔

Configuration Assistant がコミュニティのメンバをポーリングして、デバイス グループのステータスと新規メンバの存在を確認する頻度。「グラフ ポーリング間隔」、「状態ポーリング間隔」、および「LED ポーリング間隔」も参照してください。

ハント グループ

電話会社の交換局または PBX システムによってまとめて関連付けられている、複数の電話回線。ハント グループに着信があると、使用されていない回線を検出するまでグループ内で循環され、その後、その電話（PBX システムの場合は内線）に着信されます。

ピックアップ グループ

ピックアップ グループと個々の IP Phone を管理者が関連付けることにより、電話のユーザが、別の内線番号や電話番号を呼び出しているコールに容易に応答（電話に出ること）できるようになります。

非同期転送モード

「ATM」を参照。

ファイアウォール

接続されているパブリック ネットワークとプライベート ネットワーク間のバッファとして指定された、1 つ以上のルータまたはアクセス サーバ。ファイアウォール ルータでは、アクセス リストとその他の方法を使用して、プライベート ネットワークのセキュリティを確保します。

フィンガ

対象の人物に特定のインターネット サイトのアカウントがあるかどうかを判別するソフトウェア ツール。多くのサイトでは、フィンガ要求の受信は許可されていません。

フェールオーバー

スタンバイ スイッチへの処理の振り替え。

プロセス ID

一連の同じ管理規則の下で動作し、共通のルーティング戦略を共有するネットワーク グループを識別する番号。

ホーム ネットワーク

VPNトンネルのサーバ側のネットワーク。たとえば、ホテルの宿泊客が、ホテルのネットワークに PC を接続し、自分の会社のネットワークに物理的に配置されているサーバに保存されているファイルをダウンロードする場合があります。この接続は、VPN トンネルを使用して、ホテルのネットワークからインターネット経由で会社のネットワークまで確立されます。この例の場合、ホテルのネットワークがリモート ネットワーク、会社のネットワークがホーム ネットワークになります。

ポーリング間隔

「グラフ ポーリング間隔」、「LED ポーリング間隔」、および「ネットワーク ポーリング間隔」を参照。

マクロ

「ロール」を参照。

マルチキャスト ルーティング

1 つのパケットのコピーを、可能なすべての宛先の選択されたサブセットに渡すことができるルーティング技術。ユニキャスト ルーティングと対照を成します。

メディア アクセス制御

「MAC」を参照。

ユーザ データグラム プロトコル

「UDP」を参照。

ユニキャスト ルーティング

1 つのパケットを単一の宛先にルーティングし、ルーティング プロトコルを使用してその宛先へのパスを特定するルーティング技術。マルチキャスト ルーティングと対照を成します。

ライトウェイト アクセスポイント

WLAN コントローラに依存して機能するアクセスポイント。WLAN コントローラによって AP 設定とファームウェアが管理されます。アクセスポイントの個々の設定は不要です。アクセスポイントでは、リアルタイムの MAC 機能だけが処理され、リアルタイムではない MAC 機能は WLAN コントローラで処理されます。このアーキテクチャは「スプリット MAC アーキテクチャ」と呼ばれます。自律型アクセスポイントと比較してください。

リモート SPAN

宛先ポートを含むスイッチから離れた位置に送信元ポートが配置されている SPAN セッション。ローカル SPAN と対照を成します。

リモート ネットワーク

VPNトンネルのクライアント側のネットワーク。たとえば、ホテルの宿泊客が、ホテルのネットワークに PC を接続し、自分の会社のネットワークに物理的に配置されているサーバに保存されているファイルをダウンロードする場合があります。この接続は、VPN トンネルを使用して、ホテルのネットワークからインターネット経由で会社のネットワークまで確立されます。この例の場合、ホテルのネットワークがリモート ネットワーク、会社のネットワークがホーム ネットワークになります。

リンク集約制御プロトコル。

「LACP」を参照。

リンクステート プロトコル

インターネットワークのマップを管理することにより、インターネットワークが代替ルートやパラレル パスを確認して負荷分散できるようにするルーティング プロトコルの一種。このプロトコル タイプの例として、OSPF があります。ディスタンスベクタ プロトコルと対照を成します。

リンクステート プロトコル

インターネットワークのマップを管理することにより、インターネットワークが代替ルートやパラレル パスを確認して負荷分散できるようにするルーティング プロトコルの一種。このプロトコル タイプの例として、OSPF があります。ディスタンスベクタ プロトコルと対照を成します。

ルーティング可能インターフェイス

ルーテッド ポートまたは SVI。

ルーティング プロトコル

利用可能なネットワークの距離や到達コストなどの情報を収集し、パケットのルーティング パスを特定するための一連の規則と使い方。

ルーテッド ポート

ルータ インターフェイスとして機能する、VLAN 以外のポート。

ルート スイッチ

スパンニングツリー トポロジの中心になるよう選択されたスイッチ。ネットワーク上のデータ フローはすべて、このスイッチを中心として捉えます。「ルート ポート」も参照してください。

ルート ポート

ルート スイッチへの最適なパスを持つスイッチ ポート。

ループスタート

4 つある T1 CAS シグナリングの最も一般的な形態の 1 つですが、主に FXS、FXO または任意のアナログポートで使用されるアナログ信号です。他には、グラウンドスタート、EANA、および E&M があります。

ローカル SPAN

送信元ポートと宛先ポートがすべて同一スイッチ上にある SPAN セッション。リモート SPAN と対照を成します。

ロール

事前定義された一連のコマンドを生成するコマンド。