



## ハブサイトの管理

この章の内容は、次のとおりです。

- [ハブサイトの設定およびセットアップの基本的ワークフロー \(4-1 ページ\)](#)
- [ウィザードの手順 1: システム設定項目の設定 \(4-2 ページ\)](#)
- [ウィザードの手順 2: ブランチ デバイスの認定 Cisco IOS ソフトウェア イメージのアップロード \(4-6 ページ\)](#)
- [ウィザードの手順 3: IP アドレス プールの設定 \(4-7 ページ\)](#)
- [ウィザードの手順 4: サービス プロバイダーの設定 \(4-10 ページ\)](#)
- [ウィザードの手順 5: IWAN 集約サイトの設定 \(4-12 ページ\)](#)
- [ハブサイトの設定の変更 \(4-19 ページ\)](#)
- [IWAN サイトと非 IWAN サイトの共存について \(4-19 ページ\)](#)
- [IP アドレス プールについて \(4-21 ページ\)](#)
- [プロビジョニング済みハブサイトの WAN 帯域幅の更新 \(4-22 ページ\)](#)
- [ハブサイトの QoS 帯域幅の割合の変更 \(4-23 ページ\)](#)

## ハブサイトの設定およびセットアップの基本的ワークフロー

ハブサイトを設定およびセットアップするには、Cisco IWAN アプリケーション (IWAN アプリ) に付属するウィザードを使用します。

表 4-1 ハブサイトの設定およびセットアップの基本的ワークフロー

いいえ。	タスク	参照先
1	システム設定項目を設定する。	<a href="#">ウィザードの手順 1: システム設定項目の設定 (4-2 ページ)</a>
2	認定された Cisco IOS ソフトウェア イメージをアップロードする。  (注) このウィザードの手順は、グリーンフィールドブランチ デバイスに対してのみ表示されます。	<a href="#">ウィザードの手順 2: ブランチ デバイスの認定 Cisco IOS ソフトウェア イメージのアップロード (4-6 ページ)</a>

表 4-1 ハブサイトの設定およびセットアップの基本的ワークフロー(続き)

いいえ。	タスク	参照先
3	IP アドレス プールを設定する。	<a href="#">ウィザードの手順 3: IP アドレス プールの設定(4-7 ページ)</a>
4	サービス プロバイダーを設定する。	<a href="#">ウィザードの手順 4: サービス プロバイダーの設定(4-10 ページ)</a>
5	IWAN 集約サイトを設定する。	<a href="#">ウィザードの手順 5: IWAN 集約サイトの設定(4-12 ページ)</a>

## ウィザードの手順 1: システム設定項目の設定

Netflow Collector、DNS、AAA、Syslog、SNMP、DHCP などのシステム設定項目を設定するには、次の手順を実行します。

一部のシステム設定項目が表示されないことがあります。必要に応じて [Show More] または [Show Less] ボタンをクリックし、設定を表示または非表示にしてください。

### 手順

- ステップ 1** 初めてログインする場合は、[CLI Credentials] ダイアログボックスでグローバル設定を指定するように指示されます。ユーザ名とパスワードを入力し、[Add] をクリックします。
- ステップ 2** 左側のナビゲーションパネルで、[IWAN] をクリックします。Cisco IWAN のホームページが開きます。
- ステップ 3** シスコインテリジェント WAN のホームページで、[Configure Hub Site & Settings] をクリックします。デフォルトで [Settings] タブが開き、[System Settings] ページが表示されます(次の図を参照)。

図 4-1 [Systems Settings] タブ

366191

ステップ 4 [Netflow Collector]領域で、次のプロパティを入力します。

フィールド	説明
Netflow Destination IP	NetFlow コレクタ (サーバ) の IP アドレス。 トラフィック統計情報がネットワーク デバイスから NetFlow コレクタに送信されます。
Port Number	NetFlow コレクタ (サーバ) のポート番号。

ステップ 5 [DNS]領域で、次のプロパティを入力します。

フィールド	説明
ドメイン名	DNS ドメイン名。
プライマリ サーバ	(任意)プライマリ DNS サーバの IP アドレス。
Secondary Server	(任意)セカンダリ DNS サーバの IP アドレス。

ステップ 6 [Authorization, Authentication, Accounting]領域で、次のプロパティを入力します。

フィールド	説明
I[P Address]	(任意)認証、許可、アカウントिंग(AAA)サーバの IP アドレス。 Cisco IWAN でサポートされる集中管理型 AAA サービスは、TACACS だけです。TACACS サーバを指定すると、デバイスはスポーク デバイスへの管理アクセス (SSH および HTTPS) に TACACS を使用します。TACACS を指定するかどうかに関わらず、スポーク デバイス上にローカル AAA ユーザ データベースが作成されるので、TACACS サーバを使用できない場合に対応できます。 次のデフォルト値のいずれかがローカル AAA ユーザ クレデンシャルに使用されます。 <ul style="list-style-type: none"> <li>• Cisco APIC-EM グローバル クレデンシャル</li> <li>• ブランチ ルータのグローバル デバイス クレデンシャルで指定されたユーザ名とパスワード</li> <li>• ハブのプロビジョニング時に入力されたユーザ名とパスワード</li> </ul>
Key	(任意)AAA サーバにアクセスするためのキー。

ステップ 7 [Syslog]領域で、次の情報を入力します。

フィールド	説明
Server IP	(任意)Syslog サーバの宛先 IP アドレス。 すべてのルータからの syslog メッセージがこのサーバに送信されます。

ステップ 8 [NAT/Proxy IP Address]領域で、以下を設定します。

フィールド	説明
APIC-EM Behind NAT/Proxy	APIC-EM コントローラが NAT ルータの背後にある場合は、[Yes]を選択します。
APIC-EM NAT/Proxy IP	APIC-EM コントローラのパブリック NAT パブリック IP アドレス。

ステップ 9 [SNMP]領域の [Version] フィールドでバージョン番号を選択します。選択した SNMP バージョン番号 (V2C または V3) に応じて、異なるプロパティが表示されます。

- SNMP バージョン V2C の場合は、次のプロパティを入力します。

フィールド	説明
Version	SNMP ソフトウェアのバージョン。値: V2C。
Read Community	SNMP V2C read コミュニティストリング。
Write Community	(任意) SNMP V2C write コミュニティストリング。
Retries	再試行数デフォルト: 3
Timeout (secs)	SNMP V2C に対してのみ表示されます。 タイムアウトの期間を指定します。デフォルト: 10
Trap Destination IP	(任意) SNMP サーバの IP アドレス。 (注) IP アドレスを入力しない場合は、SNMP サーバとして Cisco IWAN アプリが使用されます。  APIC-EM コントローラを管理対象ネットワーク デバイスの SNMP マネージャとして動作させるか、別の SNMP サーバを指定して SNMP トラップを処理させることができます。SNMP の設定によってハブとリモートサイトのデバイスからのインベントリが決まります。これらの値は設定に反映されます。

- SNMP バージョン V3 の場合は、次のプロパティを入力します。

フィールド	説明
Version	SNMP ソフトウェアのバージョン。値: V3。
モード	ドロップダウン リストからモードを選択します。次のオプションがあります。 <ul style="list-style-type: none"> <li>• 認証および暗号化</li> <li>• No Authentication and No Encryption</li> <li>• Authentication and No Encryption</li> </ul>
Auth.タイプ	[Mode] フィールドで [Authentication and Encryption] または [Authentication and No Encryption] を選択した場合に表示されます。 ドロップダウンリストから認証タイプを選択します。次のオプションがあります。 <ul style="list-style-type: none"> <li>• HMAC-SHA</li> <li>• HMAC-MDS</li> </ul>
Username	認証ユーザ名

フィールド	説明
Auth.Password]	[Mode] フィールドで [Authentication and Encryption] または [Authentication and No Encryption] を選択した場合には表示されます。 認証ユーザ名のパスワード。
Encryption Type	[Mode] フィールドで [Authentication and Encryption] を選択した場合には表示されます。 暗号化ユーザ名。
Encryption Password	[Mode] フィールドで [Authentication and Encryption] を選択した場合には表示されます。 暗号化ユーザ名のパスワード。
Retries	再試行数デフォルト:3
Timeout (secs)	SNMP V2C に対してのみ表示されます。 タイムアウトの期間を指定します。デフォルト:10
Trap Destination IP	(任意) SNMP サーバの IP アドレス。 (注) IP アドレスを入力しない場合は、SNMP サーバとして Cisco IWAN アプリが使用されます。  APIC-EM コントローラを管理対象ネットワーク デバイスの SNMP マネージャとして動作させるか、別の SNMP サーバを指定して SNMP トラップを処理させることができます。SNMP の設定によって ハブとリモートサイトのデバイスからのインベントリが決まります。これらの値は設定に反映されます。

ステップ 10 [DHCP]領域で、次のプロパティを入力します。

フィールド	説明
External DHCP IP	(任意) DHCP サーバの宛先 IP アドレス。 クライアント コンピュータや他の TCP/IP ベースのネットワーク デバイスに有効な IP アドレスを提供する、DHCP サーバを入力します。 DHCP サーバを追加するには、[IP Address] フィールドの横にある [+]アイコンをクリックして IP アドレスを入力します。 (注) 最大 5 つの DHCP サーバを追加できます。  DHCP サーバを削除するには、削除する [IP Address] フィールドの横にある [-]アイコンをクリックします。

ステップ 11 [保存して続行 (Save and Continue)] をクリックします。[Certified IOS Releases] タブが開きます。[ウィザードの手順 2: ブランチ デバイスの認定 Cisco IOS ソフトウェア イメージのアップロード \(4-6 ページ\)](#) を参照してください。

[Systems] タブの既存の値を更新すると、[Network Wide Settings Summary] ダイアログボックスが開き、変更内容が表示されます。次のいずれかを実行します。

- [Apply Now] オプション ボタンをクリックして、[Continue] をクリックします。
- [Schedule] オプション ボタンをクリックして、変更を適用する日時を指定し、[Submit] をクリックします。

## ウィザードの手順 2: ブランチデバイスの認定 Cisco IOS ソフトウェアイメージのアップロード



(注)

このウィザードの手順は、グリーンフィールド ブランチ デバイスに対してのみ表示されます。

認定された Cisco IOS イメージをコンピュータからシスコ インテリジェント WAN アプリケーションにアップロードできます。グリーンフィールド デバイス が出現すると、Plug-n-Play エージェントは Cisco APIC-EM 内の Plug-n-Play サーバとやり取りして、適切な Cisco IOS ソフトウェア イメージをデバイスにダウンロードし、そのイメージとともにデバイスをリロードします。



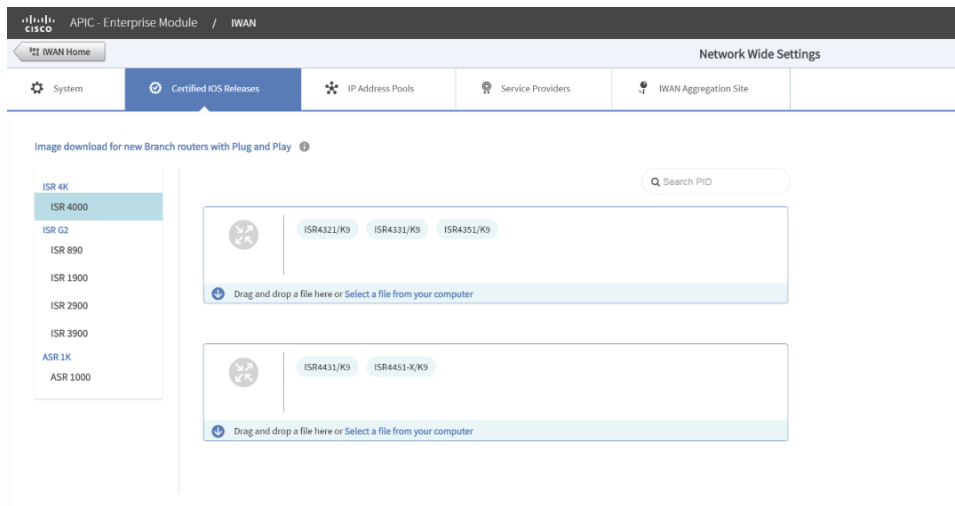
(注)

適切なソフトウェア イメージがすでにルータにインストールされている場合は、この手順をスキップできます。

### 手順

- ステップ 1 [Certified IOS Releases] タブをクリックします。[Cisco IOS Releases for Sites] ページが開きます (次の図を参照)。

図 4-2 [Certified IOS Releases] タブ



366200

- ステップ 2 左ペインで、Cisco IOS イメージをアップロードするルータのタイプを選択します。

- ステップ 3 次のいずれかを実行します。

- Cisco IOS ソフトウェア イメージ ファイルをコンピュータから GUI にドラッグアンドドロップします。
- Cisco IOS ソフトウェア イメージ ファイルが保存されている場所を参照して、ファイルをシステムにアップロードします。

- ステップ 4 [Continue] をクリックします。[IP Address Pools] ページが開きます。ウィザードの手順 3: IP アドレス プールの設定 (4-7 ページ) を参照してください。

## ウィザードの手順 3: IP アドレス プールの設定



(注)

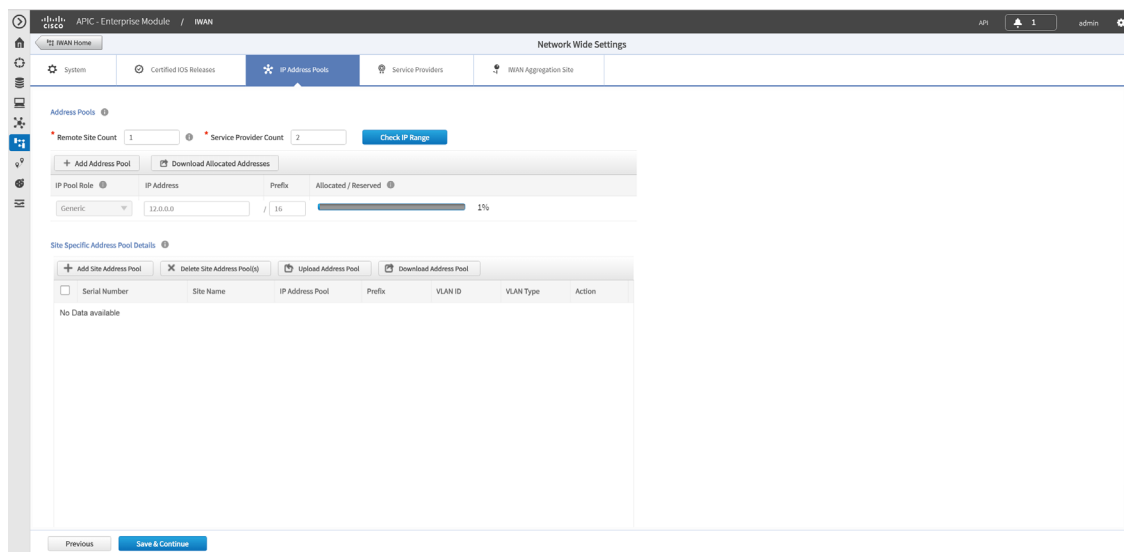
汎用 IP プールはオーバーレイ アドレスやループバック アドレスに使用されます。汎用 IP アドレス プールは、[IP Address Pools] タブで指定したリモート サイトとサービス プロバイダーの数に従って分割されます。将来の要件を把握して計画を立て、導入するサービス プロバイダーとリモート サイトの最大数を指定してください。IP アドレス プールの設定を指定した後は、それらを変更できません。

IP アドレス プールを定義するには、[IP Address Pools] タブを使用します。IP アドレス プールの詳細については、[IP アドレス プールについて \(4-21 ページ\)](#) を参照してください。

### 手順

ステップ 1 [IP Address Pool] タブを選択します。[Address Pools] ページが開きます(次の図を参照)。

図 4-3 [IP Address Pool] タブ



ステップ 2 [Remote Site Count] フィールドで、導入するリモート サイトの最大数を入力します。

Cisco IWAN リリース 1.2.x を使用している既存のお客様の場合は、Cisco IWAN リリース 1.3.x にアップグレードすることによりリモート サイトの数を増加できます。(初期プロビジョニング時に作成される) 事前予約済みサブネットの内部 IP アドレスの可用性に基づいて、より大きいリモート サイト数を指定できます。

ステップ 3 [Service Provider Count] フィールドで、必要なサービス プロバイダーの最大数を入力します。

Cisco IWAN リリース 1.2.x を使用している既存のお客様の場合は、Cisco IWAN リリース 1.3.x にアップグレードすることによりサービス プロバイダーの数を増加できます。最大 4 つのサービス プロバイダーを指定できます。

ステップ 4 [Check IP Range] ボタンをクリックします。[Proposed IP Range] が開きます。

入力したリモートサイトとサービスプロバイダーの数に基づいて、[Proposed IP Range] ページに、汎用 IP アドレスプールに使用可能な最小推奨プレフィックス長、LAN インターフェイスプールのプレフィックス長、VLAN ごとの IP アドレスの数、および VLAN の数に関する情報が表示されます。[OK] または [Get IP Range] をクリックします。

ステップ 5 次のいずれかを実行します。

- 手動で IP アドレスを入力するには、[+ Add Address Pool] をクリックします。次のプロパティを入力します。

フィールド	説明
ロール	次のいずれかです。 <ul style="list-style-type: none"> <li>• [Generic]: 最初の範囲は常に、デフォルトで汎用 IP プールになります。</li> <li>• [LANGreenfield]: 新しいグリーンフィールド ブランチ デバイスの LAN IP アドレス プールを定義するには、このオプションを選択します。任意の数の LAN グリーンフィールド IP アドレス プールを指定できます。</li> <li>• [LANBrownfield]: ブラウンフィールド ブランチ デバイス (既存の設定があるデバイス) の LAN IP アドレス プールを定義するには、このオプションを選択します。任意の数の LAN ブラウンフィールド IP アドレス プールを指定できます。</li> </ul>
IP Address	IP アドレスプールの IP アドレス。
Prefix	CIDR プレフィックス。
Allocated	プール内の使用されているアドレスの割合を表示します。

- 多数の IP アドレスをアップロードするには、[Upload Address Pool] をクリックして、コンピュータから .csv ファイルをアップロードします。  
.csv ファイルに含める必要がある情報の種類については、[Download Address Pool] タブをクリックしてください。テンプレートの詳細を含む Controller\_Profile\_DD-MM-YYYY.csv ファイルがシステムにダウンロードされます。

ステップ 6 [+ Add Site Address Pool] をクリックして、サイト固有の LAN IP アドレスプールの情報を入力します。[Add Site Address Pool] ダイアログボックスが開きます。下記の表に示すプロパティを入力し、[OK] をクリックします。

デフォルトでは、グリーンフィールド ブランチ サイトは LAN グリーンフィールド IP アドレスプールが存在する場合はその IP アドレスを使用し、存在しない場合は汎用 IP アドレスプールの IP アドレスを使用します。(たとえば、VLAN に LAN グリーンフィールド IP アドレスプールや汎用 IP アドレスプールの IP アドレスを使用したくない場合などに) VLAN に特定の IP アドレスプールを使用する新しいグリーンフィールド ブランチ サイトをプロビジョニングする場合は、サイトをプロビジョニングする前に VLAN とそれぞれの IP アドレスプールを定義できます。



(注) サイトをプロビジョニングした後は、VLAN があるサイト固有の IP アドレスプールと VLAN がないサイト固有の IP アドレスプールとの間を移動できません。したがって、サイトをプロビジョニングする前に、必ず明確なビジョンを確立しておく必要があります。



フィールド	説明
Serial Number	サイト デバイスのシリアル番号。 サイトに複数のデバイスがある場合は、すべてのシリアル番号をセミコロンで区切って指定します。
Site Name	サイト名。
IP Address Pool	この VLAN 上のホストに使用する IP アドレス プール。
Prefix	CIDR プレフィックス。
VLAN ID	値の範囲: 1 ~ 4094。 (注) VLAN ID 99 は中継 VLAN 用に予約されているため、この ID を別の VLAN に使用することはできません。
VLAN Type	VLAN のタイプを入力するか、ドロップダウン リストから選択します。 値: Data、Guest、Voice and Video、Wireless (注) VLAN タイプを入力する場合は、次の制限が適用されます。 <ul style="list-style-type: none"> <li>- VLAN タイプの値は 200 文字以下でなければなりません。</li> <li>- VLAN タイプには「?」記号を使用できません。</li> <li>- サイト固有のアドレス プールの場合は、サイトごとに最大 20 エントリを入力できます。</li> </ul>

**ステップ 7** 必要に応じてステップ 6 を繰り返し、さらにサイト アドレス プールを追加します。

**ステップ 8** [保存して続行 (Save and Continue)] をクリックします。[Service Providers] タブが開きます。[ウィザードの手順 4: サービス プロバイダーの設定 \(4-10 ページ\)](#) を参照してください。

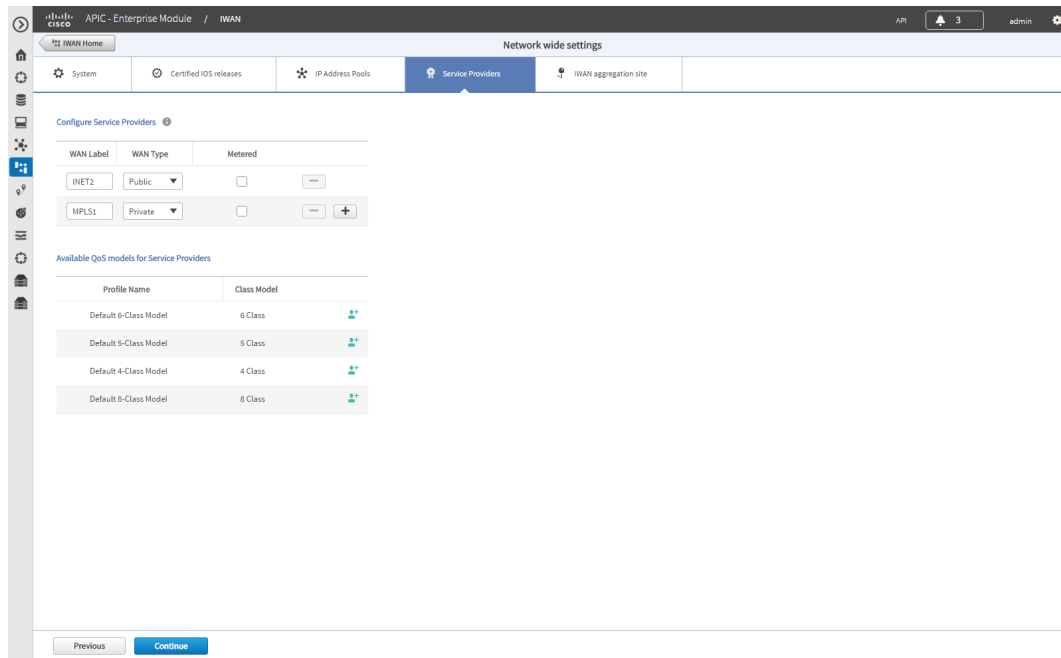
## ウィザードの手順4:サービスプロバイダーの設定

リンクのタイプとサービスプロバイダーの数を指定するには、[Service Providers] タブを使用します。

### 手順

- ステップ 1** [Service Providers]タブを選択します。[Configure Service Providers] ページが開きます(次の図を参照)。

図 4-4 [Service Providers] タブ



365958

- ステップ 2** [Configure Service Providers]領域で、[+] アイコンをクリックして次のプロパティを定義します。



(注) 最大4つのサービスプロバイダーを指定できます。

フィールド	説明
WAN Label	WAN トランスポート タイプ。最大7文字まで指定できます。
WAN Type	次のいずれかです。 <ul style="list-style-type: none"> <li>プライベート</li> <li>パブリック</li> </ul>

フィールド	説明
Metered	<p>WAN が従量制の場合はこのオプションを選択します。</p> <p>(注) サービスプロバイダーの数が3つ以上の場合にのみ、[Metered] オプションを選択できます。サービスプロバイダーが2つしかない場合に一方のリンクを従量制リンクとして選択することはできません。</p> <p>(注) パブリッククラウドでは、1つのリンクだけが従量制リンクとして許可されます。</p>
<b>Available QoS Models for Service Providers</b>	
Profile Name	すべての使用可能なサービスプロファイルの名前が一覧表示されます。
Class Model	<p>それぞれのサービスプロファイルに対応するクラスモデルが一覧表示されます。</p> <ul style="list-style-type: none"> <li>• 4 Class</li> <li>• 5 Class</li> <li>• 6 Class</li> <li>• 8 Class</li> </ul>

**ステップ 3** (任意) 提供されているデフォルトクラスではなくカスタムのクラスモデルが必要な場合は、[Available QoS Models for Service Providers] 領域をクリックし、サービスプロバイダーのサービスレベル契約 (SLA) に最も合致するプロファイルの横にある [+] アイコンをクリックします。[Add Service Profile] ダイアログボックスが開きます(次の図を参照)。

図 4-5 [Add Service Profile] ダイアログボックス

Class Name	DSCP	Priority Bandwidth (%)	Remaining Bandwidth (%)
Total: 100			
Voice	EF	10	
CLASS1 DATA			
call-signaling			4
interactive-video			30
streaming-video			10
CLASS2 DATA			
critical-data	AF21		25
Default			
class-default	0		25
net-control-mgmt			5
scavenger			1

**ステップ 4** 次のプロファイル情報を入力し、[Save] をクリックします。



(注) プライベート WAN インターフェイスの場合は、一連の定義済みサービス プロバイダーのプロファイルを使用できます。サービス プロバイダーの SLA を満たすために、出力 QoS キューイングが WAN 出力に適用されます。

フィールド	説明
Profile Name	新しいサービス プロファイルの名前
Class Model	クラス モデルのタイプが表示されます。次のいずれかです。 <ul style="list-style-type: none"> <li>• 4 Class</li> <li>• 5 Class</li> <li>• 6 Class</li> <li>• 8 Class</li> </ul>
Class Name	データ クラス名が表示されます。
DSCP	各クラスの DiffServ コード ポイント (DSCP) 値が表示されます。保存すると、新しいプロファイルとして表示されます。保存後は、この値を変更できません。
Priority Bandwidth (%)	プライオリティ クラスに割り当てる帯域幅の割合。例: Voice。
残りの帯域幅 (%)	ストリーミング ビデオや重要なクラスなど、他のクラスに割り当てる帯域幅の割合。 (注) 0 よりも大きい値を入力する必要があります。[Remaining Bandwidth] 列のすべてのデータ クラスの合計値が 100 % を超えることはできません。



(注) プロファイル情報を追加すると、[Available QoS Models for Service Providers] 領域にプロファイルの詳細情報が表示されます。

ステップ 5 [Continue] をクリックします。[IWAN Aggregation Site] タブが開きます。ウィザードの手順 5: [IWAN 集約サイトの設定 \(4-12 ページ\)](#) を参照してください。

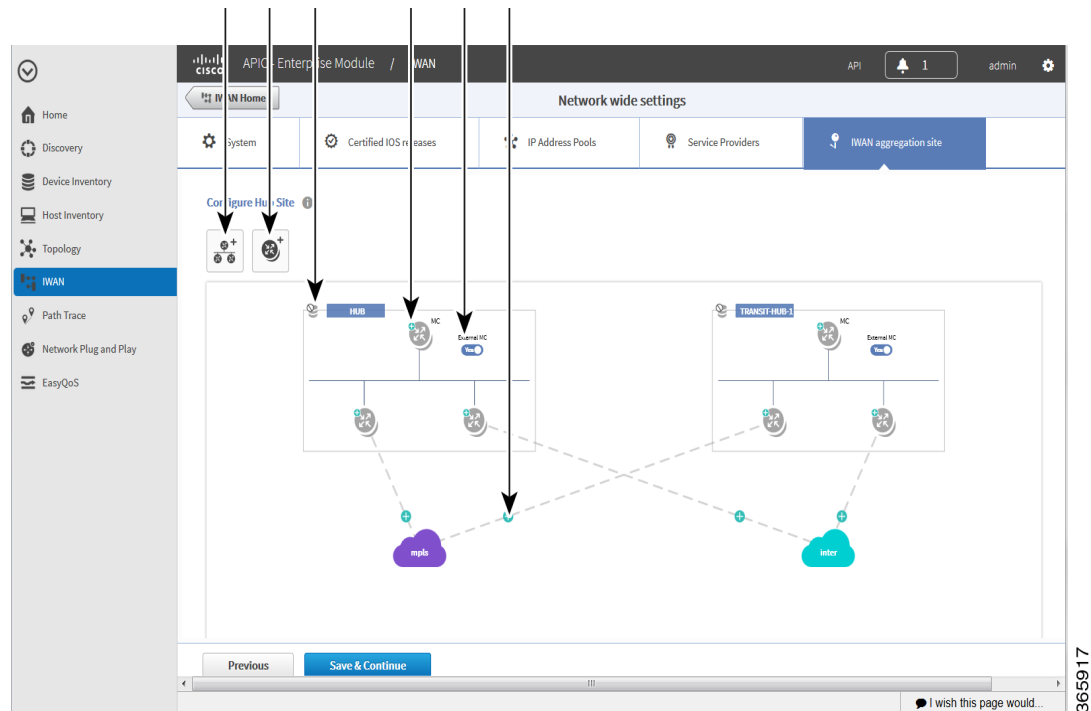
## ウィザードの手順 5: IWAN 集約サイトの設定

この手順を使用して、以下を実行します。

1. ハブ デバイスの検出。
2. LAN の設定。
3. WAN の設定。
4. 外部マスター コントローラの設定。

次の図を参照して、実行する手順を把握してください。

図 4-6 [IWAN Aggregation Site] タブ



1	[Add POP] アイコン	4	[Configure External MC Router +] アイコン
2	[Add Border Router] アイコン	5	[External MC] 切り替えボタン
3	[Configure LAN] アイコン	6	[Configure WAN Link +] アイコン

## 手順

**ステップ 1** ハブ デバイスの検出。次の手順を実行します。

- a. [IWAN Aggregation Site] タブを選択します。[Configure Hub Site] ページが開き、ウィザードの手順 4 で定義したすべてのサービス プロバイダーとそれぞれのハブ境界ルータが表示されます。
- b. 次のいずれかを実行します。
  - (推奨) [External MC] ボタン (図 4-6 の 5) をクリックして [Yes] に切り替えます。新しいルータがスタンドアロン マスター コントローラ (MC) として追加されます。
  - [External MC] ボタンをクリックして [No] に切り替えます。境界ルータの 1 つが MC として指定されます。
- c. さらにハブを追加するには、[Add POP] アイコン (図 4-6 の 1) をクリックします。プライマリハブの横に中継ハブが追加されます (上の図の TRANSIT-HUB-1 を参照)。



(注) プロビジョニング時には最大 2 つのハブ サイトを指定できます。ハブのプロビジョニング後に、ルータを追加または削除できます。

- d. (任意)新しい TRANSIT-HUB-1 を別の名前に変更するには、ハブの名前をクリックして別の名前を追加します。



(注) ハブの名前は初期設定時(ハブにルータを追加する前)にのみ変更できます。

- e. 境界ルータをハブに追加する場合は、[Add Border Router]アイコン(図 4-6 の2)の上にカーソルを移動すると、[Add to POP]オプションが表示されます。2つの使用可能なハブのいずれかを選択します。新しい境界ルータが当該ハブに追加されます。



(注) 1つのハブサイトに最大4つの境界ルータを指定できます。

- f. 新たに追加した境界ルータを設定するには、ルータ上部の [+]アイコンをクリックして、[Configure Router] ダイアログボックスを開きます。
- g. [Configure Router] ダイアログボックスで、次の手順を実行します。
- [Router Management IP]フィールドに、ハブルータの管理 IP アドレスを入力します。
  - [Validate]をクリックします。[Configure Router]ダイアログボックスが再び開き、追加のフィールドが表示されます(次の図を参照)。

フィールド	説明
Router Management IP	ハブ ルータの管理 IP アドレス。
マスター コントローラ	デバイスをマスター コントローラとして選択するには、このオプションをオンにします。
<b>SNMP</b>	
Version	SNMP のバージョン番号。 選択したバージョン番号に応じて異なるプロパティが表示されます。
Read Community (SNMP V2C を選択した場合に表示)	SNMP V2C read コミュニティ スtring。
Write Community (SNMP V2C を選択した場合に表示)	(任意)SNMP V2C write コミュニティ スtring。
モード (SNMP V3 を選択した場合に表示)	ドロップダウン リストからモードを選択します。次のオプションがあります。 <ul style="list-style-type: none"> <li>• 認証および暗号化</li> <li>• [No Authentication and No Encryption]</li> <li>• [Authentication and No Encryption]</li> </ul>
Auth.タイプ (SNMP V3 を選択した場合に表示)	[Mode] フィールドで [Authentication and Encryption] または [Authentication and No Encryption] を選択した場合に表示されます。 ドロップダウン リストから、認証タイプを選択します。次のオプションがあります。 <ul style="list-style-type: none"> <li>• HMAC-SHA</li> <li>• HMAC-MDS</li> </ul>
Username (SNMP V3 を選択した場合に表示)	SNMP V3 を選択した場合に表示されます。 認証ユーザ名
Auth.Password] (SNMP V3 を選択した場合に表示)	[Mode] フィールドで [Authentication and Encryption] または [Authentication and No Encryption] を選択した場合に表示されます。 認証ユーザ名のパスワード。
Encryption Type (SNMP V3 を選択した場合に表示)	[Mode] フィールドで [Authentication and Encryption] を選択した場合に表示されます。 暗号化ユーザ名。
Encryption Password (SNMP V3 を選択した場合に表示)	[Mode] フィールドで [Authentication and Encryption] を選択した場合に表示されます。 暗号化ユーザ名のパスワード。
<b>SNMP の再試行回数およびタイムアウト</b>	
Retries	SNMP の再試行回数。デフォルト:3
Timeout (secs)	SNMP 要求がタイムアウトしたと見なされるまでの待機秒数。デフォルト:10

フィールド	説明
<b>SSH/Telnet</b>	
Protocol	ホストとの通信に使用されるプロトコル (Telnet または SSH)。
Username	SSH または Telnet のユーザ名。
Password	SSH または Telnet のパスワード。
Enable Password	ユーザ名のイネーブルパスワード。
Timeout (secs)	SSH または Telnet 要求がタイムアウトしたと見なされるまでの待機秒数。

- 上記の表の説明に従って、プロパティを入力します。



(注) これらのクレデンシャルは 1 回だけ入力できます。これらの値は、システム内の残りのハブ デバイスに自動的に入力されます。

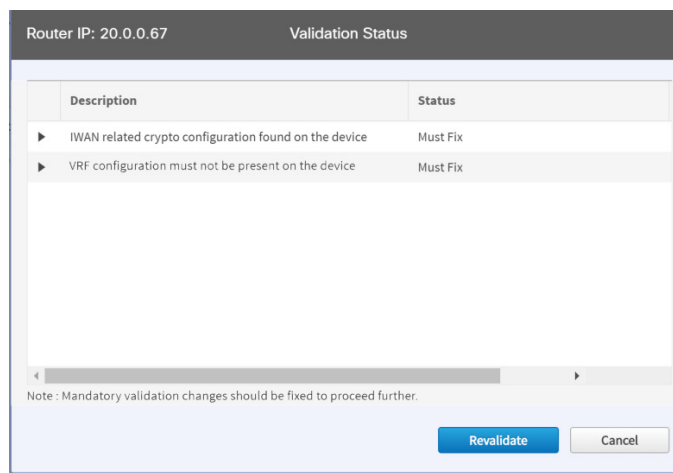
- [Add Device] をクリックします。

デバイスがバックグラウンドで検証され、プロビジョニングに適しているかどうか判断されます。以下が実行されます。

Cisco IWAN アプリはルータにアクセスしてその設定をチェックし、Cisco IWAN アプリと競合する可能性がある設定が含まれているかどうかを確認します。これはブラウフィールド検証と呼ばれます。

ルータに競合する設定がない場合は、デバイスの上部にオレンジ色のアイコンが表示され、[Configure Router] ダイアログが開きます。

ルータに競合する設定がある場合は、[Validation Status] ダイアログが開き、すべての検証エラーが一覧表示されます(次の図を参照)。



- h. 検証ステータスは [Warning] または [Must Fix] のいずれかになります。次の手順を実行します。
  - 検証ステータスが [Warning] の場合は、エラーを修正または無視することができます。
  - 検証ステータスが [Must Fix] の場合は、説明で示された設定を削除し、[Revalidate] をクリックします。



[Validation Status] ダイアログボックスに表示されるメッセージの詳細については、付録 A「ブラウフィールド検証メッセージ」を参照してください。

ルータの検証に成功した場合([Must Fix] エラーがない場合)は、[Configure Router]ダイアログボックスが開きます。

- i. [Configure Router] ダイアログボックスで、適切な [LAN IP-Interface] チェックボックスをオンにして、[Save] をクリックします。



(注) 複数の LAN IP インターフェイスを選択できます。

- j. 境界ルータをクラウドに接続するには、ルータをクリックしてクラウドにドラッグします。  
k. 上記の手順を使用して、他の境界ルータを設定します。

ステップ 2 LAN の設定。次の手順を実行します。

- a. プライマリ ハブの左上隅にあるアイコン(図 4-6の 3)をクリックします。[Configure LAN] ダイアログボックスが開き、次の表に示すフィールドが表示されます。

[Routing Protocol]、[AS Number]、[Datacenter Prefix]は、設定しやすいように、デバイスから収集されて自動的に入力されます。各ルーティング プロトコルに対してデバイス間の共通(一致) AS 番号が表示されます。デバイスの AS 番号は変更できますが、お勧めしません。

フィールド	説明
Routing Protocol	ハブ ルータで実行するデフォルトのルーティング プロトコル。 例: EIGRP、OSPF、BGP
AS Number	ルーティングプロトコルに応じて、AS 番号またはエリア番号。 (注) LAN ルーティング プロトコルが BGP で、もう一方のハブ デバイスからの照合 AS 番号がない場合、このフィールドはグレー表示されます。デバイスの LAN 側ルーティングを手動で変更する必要があります。 (注) 異なる AS 番号の BGP はサポートされません。
Datacenter Prefix	プレフィックスとして指定したハブ サイトの IP アドレス。

- b. [Save(保存)] をクリックします。

ステップ 3 WAN の設定。次の手順を実行します。

- a. ルータとクラウドを接続しているリンク上の [+]アイコン(図 4-6 の 6)をクリックします。[Configure Link]ダイアログボックスが開きます。

表示されるダイアログボックスは、[Service Provider]の設定時に指定した WAN のタイプ ([Private] または [Public] など)に応じて異なります。

- b. [Public]WAN を指定した場合は、[Configure Link] ダイアログボックスが開きます。ネットワークのリンクごとに次の情報を入力します。

表 4-2 [Configure Link] ダイアログボックス:Public WAN

フィールド	説明
WAN IP-Address	WAN インターフェイスの IP アドレス。
デフォルト ゲートウェイ	デフォルト ゲートウェイの IP アドレス。

表 4-2 [Configure Link] ダイアログボックス: Public WAN (続き)

フィールド	説明
NAT Enabled	NAT IP アドレスを使用する場合は、このオプションをオンにします。
NAT IP Address	パブリック IP アドレス
帯域幅 (Mbps)	アップロードとダウンロードの対称帯域幅。
サービス プロファイル	ドロップダウン リストからサービス プロファイルを選択します。  ドロップダウン リストには、デフォルトのサービス プロファイルと、[Service Providers] タブで設定したカスタムの 8 Class サービス プロファイルが含まれています。

- c. [Private]WAN を指定した場合は、[Configure Link] ダイアログボックスが開きます。ネットワークのリンクごとに次の情報を入力します。

表 4-3 [Configure Link] ダイアログボックス: Private WAN

フィールド	説明
WAN IP-Address	WAN インターフェイスの IP アドレス。
デフォルト ゲートウェイ	デフォルト ゲートウェイの IP アドレス。
Enable Non IWAN Sites	ネットワークの段階的移行に向けて、非 IWAN サイトと新たに有効になった IWAN POP (ハブ) およびスポーク サイトとの通信を有効にするには、このオプションをオンにします。IWAN サイトと非 IWAN サイトの共存について (4-19 ページ) を参照してください。
Loopback IP-Interface	ドロップダウン リストからプロビジョニング済みのループバック IP アドレスを選択します。これにより、シスコ インテリジェント WAN アプリケーションで既存サイトと新規 IWAN サイト間のルートを形成できるようになります。  (注) ループバック インターフェイスはプライベート (MPLS) ルータに設定する必要があります。ループバック インターフェイスは、IWAN サイトと非 IWAN サイトの共存をサポートする必要があります。デバイスを Cisco APIC-EM に追加する前に設定しておく必要があります。ループバック IP アドレスは WAN インターフェイスと同じサブネット内に指定することをお勧めします。
帯域幅 (Mbps)	アップロードとダウンロードの対称帯域幅。
サービス プロファイル	ドロップダウン リストからサービス プロファイルを選択します。  ドロップダウン リストには、デフォルトのサービス プロファイルと、[Service Providers] タブで設定されたカスタム サービス プロファイル (4 Class, 5 Class, 6 Class, 8 Class) がすべて含まれています。

- d. [Save] をクリックします。

#### ステップ 4 外部マスター コントローラの設定。

ハブおよびルータの初期設定時に、[External MC]ボタンをクリックして [Yes]に切り替えた場合は、新しいルータがスタンドアロン MC として追加されています。次の手順を実行します。

- a. External MC ルータの上部にある [+]アイコン(図 4-6 の 4)をクリックします。[Configure Router] ダイアログボックスが開きます。  
専用のマスター コントローラを使用する場合は、デバイスをグリーンフィールド検証する必要があります。IWAN やダイナミック ルーティング プロトコルと競合する設定は、LAN および WAN でサポートされません。
- b. [Router Management IP]フィールドに、ハブ ルータの管理 IP アドレスを入力します。
- c. [Validate]をクリックします。[Configure Router] ダイアログボックスが開きます。
- d. [Router Management IP] のアドレス、[SNMP]、[SSH/Telnet] のプロトコル情報を入力し、[Save] をクリックします。

## ハブ サイトの設定の変更

[Hub Site and Settings] 領域でウィザード手順をすべて完了すると、後から戻ってプロパティを変更できます。グレー表示のフィールドは変更できません。

## IWAN サイトと非 IWAN サイトの共存について

IWAN サイトと非 IWAN サイトの共存機能を使用すると、ネットワークの段階的移行に向けて、新たに有効になった IWAN POP(ハブ)およびスポークサイトと非 IWAN サイトとの間で通信できるようになります。この機能の利点は次のとおりです。

- 全面的な導入に先立ち、少数のサイトに シスコ インテリジェント WANを導入できる。
- 非 IWAN サイトは、IWAN 対応のハブおよびスポーク ルータとの通信を継続できる(逆も同様)。

## IWAN ソリューションと非 IWAN サイトの同時サポートを有効にするための前提条件

APIC-EM ワークフローで Cisco IWAN アプリを起動する前に、次の設定を完了しておく必要があります。

- Cisco IWAN ハブ プライベート(MPLS)境界ルータを定義する。
- ハブ ルータで以下を実行する。
  - 境界ルータでループバック インターフェイスを有効にする必要があります。ループバック IP アドレスは WAN インターフェイスと同じサブネット内に指定することをお勧めします。
  - (シスコ インテリジェント WANアプリケーション ワークフローに従ってハブをプロビジョニングする前に)既存の MPLS-CE をデフォルト ゲートウェイとしてスタティック ルートを追加する必要があります。

- 既存の MPLS-CE ルータで以下を実行する。
  - IWAN MPLS 境界ルータ上のループバック IP アドレスを、MPLS-CE ルータ上の BGP (または MPLS プロバイダーとのピアリングに使用される他のルーティングプロトコル) によってアドバタイズする必要があります。ループバック IP は、すべてのリモート サイトからアクセスできる必要があります。

Cisco IWAN リリース 1.1.0 以降、2つのハブと2つのクラウドを指定して、より多くのデバイスをクラウドに追加できるようになったので、マルチリンク ネットワークが可能になりました。つまり、マルチリンク ネットワークに2つのデータセンターを配置して、各データセンターに4つのリンクを持つ4つのデバイスを含めることができます。

## 異種 WAN サイトの例

Cisco IWAN リリース 2.0 以降では、プロビジョニング済みのサイトで以下を実行できます。

- WAN クラウドとサービス プロバイダーを追加する。
- 任意のタイプ (Private または Public) のリンクを最大2つ追加する。新しいリンクによって既存のデバイスの優先度が影響を受けたり、パス プリファレンスが変更されることはありません。
- 異なるハブ サイトを異なるサービス プロバイダーに接続する (サービス プロバイダーの最大数は4)。

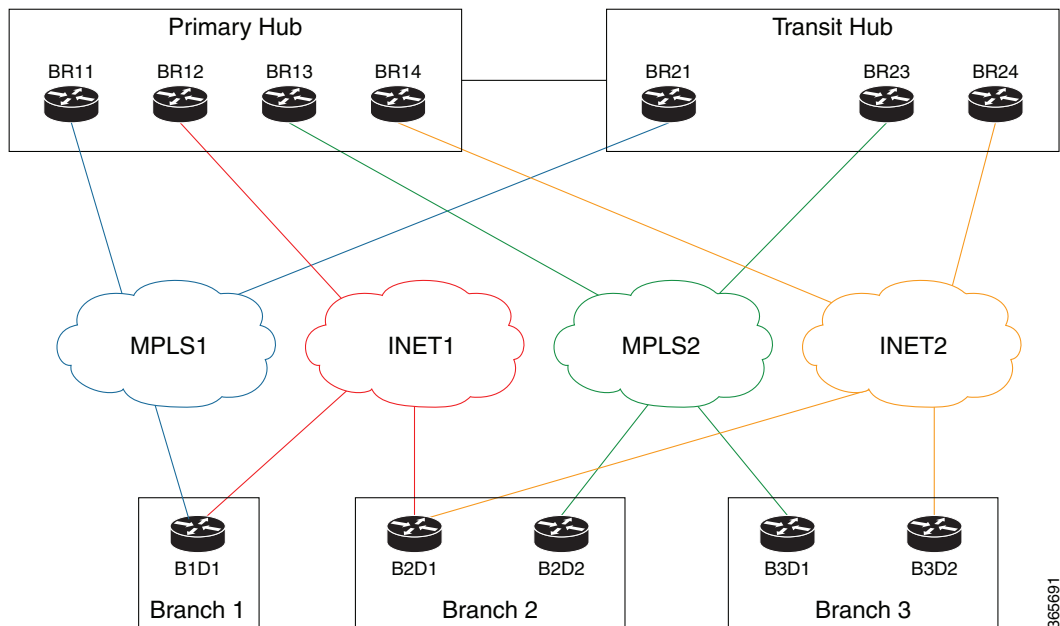


(注)

上記の変更点はサイトのプロビジョニング時には実行できません。

次の図は異種トポロジーの例を示しています。この例では、プライマリ ハブが4つのサービス プロバイダーに接続され、中継ハブが3つのサービス プロバイダーに接続されています。この例は、両方のハブ サイトが同数のサービス プロバイダーを持つ必要がないことを示しています。

図 4-7 MPLS リンクに接続されている中継ハブ



365691

## IP アドレス プールについて

シスコ インテリジェント WANアプリケーションは、グローバル エンタープライズ IP アドレス プール スペースから切り分けられた IP アドレスを自動的に使用します。この機能をサポートするには、シスコ インテリジェント WANアプリケーション用に 1 つの汎用グローバル IP アドレス プールを定義する必要があります。ハブとスポーク デバイスをプロビジョニングするために、この汎用 IP アドレス プールから IP アドレスが割り当てられます。これにはインターフェイス、LAN、VPN オーバーレイ、およびルーティングの IP アドレスが含まれます。

必要に応じて、1 つ以上の LAN グリーンフィールド IP アドレス プールを定義して、ブランチ LAN 側の IP アドレス空間をさらに調整できます。すべての LAN グリーンフィールド IP アドレス プールが使い尽くされると、汎用 IP アドレス プールが使用されます。

IWAN サイトの長期的なニーズに対応できるように、汎用 IP アドレス プールのサイズを適切に設定することが重要です。VPN 要件では、サイトをプロビジョニングする前に、内部でサブネットを定義して割り当てることが指示されています。Cisco IWAN リリース 1.3 では、初期プロビジョニングの後にサイトやサービス プロバイダーの数を増加できますが、指定済みの汎用 IP アドレス プールを変更することはできません。したがって、サービス プロバイダーやサイトの将来の規模を念頭に置いて、汎用 IP アドレス プールを定義することを推奨します。汎用 IP プールはオーバーレイ アドレスやループバック アドレスに使用されます。汎用 IP プールは、[IP Address Pools] タブで指定されたリモート サイトとサービス プロバイダーの数に従って分割されます。

固有の IP アドレスが必要な場合は、サイト固有の LAN 要件や VLAN 要件を定義し、汎用グローバル IP アドレス プールよりも優先させることができます。

### サイト固有のプロファイル

サイト固有のプロファイルはオプションであり、各サイトの LAN IP アドレスを事前プロビジョニングする場合にのみ必要です。事前プロビジョニングにより、要求されていないデバイスのリストにデバイスが追加される前に、サイト名とデバイスの組み合わせを使用してサイトを定義することができます。これは、デバイスのシリアル番号とサイト名を照合することで遂行されます。各サイトの VLAN 定義によって、IP アドレス プールの範囲を指定できます。指定しない場合は、LAN グリーンフィールド IP アドレス プールまたは汎用 IP アドレス プールから必要な LAN IP アドレスが提供されます。

### ブランチ サイト固有のプロファイル

ブランチ サイトの仕様を事前プロビジョニングできます。デバイスのシリアル番号とサイト名をサイトの VLAN とともに使用して、シングルまたはデュアル ルータ サイトを定義できます。

シングル ルータ ブランチの場合は、デバイスのシリアル番号を指定する必要があります。デュアル ルータ ブランチの場合は、両方のデバイスのシリアル番号をセミコロンで区切って指定する必要があります。Cisco IWAN アプリによって、サイト名とデバイスのシリアル番号が自動的に照合され、事前に定義した VLAN と IP アドレス プールが使用されます。したがって、当該デバイスが要求されていないデバイスとしてサイト プロビジョニング ワークフローに表示される前に、ブランチ サイトを使用できるようになります。

サイトと VLAN を定義すると、サイト プロビジョニング ワークフローでデバイスがプロビジョニングされる際に、デバイスを簡単に設定できます。デバイスが要求されてプロビジョニングされる際に、サイト プロビジョニング ワークフローは既存のサイト設定やサイト名と競合しません。

IP アドレス プールは保存後に変更できません。

**LAN ブラウンフィールド IP アドレス プール**

Cisco IWAN リリース 1.3 では、ブラウンフィールド ブランチ デバイスの LAN IP アドレスを定義するために、LAN ブラウンフィールド ロールが導入されました。

ブラウンフィールド ブランチがプロビジョニングされる際に、その VLAN サブネットが予約されます。

VLAN サブネットが LAN ブラウンフィールド IP アドレス プールのサブネットである場合、VLAN サブネットは LAN ブラウンフィールド IP アドレス プールから予約されます。

VLAN サブネットの LAN ブラウンフィールド サブネットがない場合は、サイト固有の IP アドレス プールとして予約されます。

追加、削除、更新の操作は、ブラウンフィールド サイト固有の IP アドレス プールでは許可されません。

## プロビジョニング済みハブサイトの WAN 帯域幅の更新


ハブサイトがプロビジョニングされた後(「N 日目」)、アップロードまたはダウンロードの WAN 帯域幅を変更できます。[プロビジョニング済みブランチサイトの WAN 帯域幅の更新\(5-24 ページ\)](#)も参照してください。

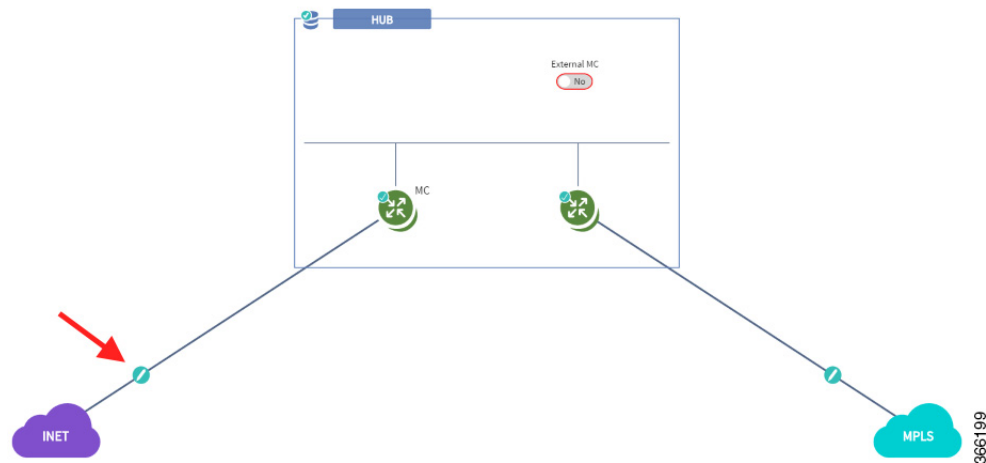
有効な帯域幅値はインターフェイスのタイプに応じて異なります。

- 10 ギガビット インターフェイス:0.1 ~ 10000 Mbps
- ギガビット インターフェイス:0.1 ~ 1000 Mbps
- セルラー インターフェイス:0.1 ~ 300 Mbps

帯域幅の設定を更新するには、次の手順を実行します。

**手順**

- 
- ステップ 1** IWAN アプリのホームページで、[Set up Branch Sites]をクリックします。
- ステップ 2** [Sites]タブをクリックします。
- ステップ 3** ハブサイトの鉛筆アイコン([Edit Site])をクリックします。[IWAN Aggregation Site] ページが開きます。
- 
- 
- (注) IWAN のフロントページで [Configure Hub Site & Settings]をクリックし、[IWAN Aggregation Site] タブをクリックすることによっても、このページに移動できます。
- 
- ステップ 4** WAN リンクの鉛筆アイコンをクリックします。[Configure Link] ダイアログボックスが開きます。



- ステップ 5 [Bandwidth] フィールドに新しい値を入力します。
- ステップ 6 ダイアログ ボックスで [Save] をクリックします。
- ステップ 7 ページの左下にある [Save & Continue] ボタンをクリックします。[Hub Site summary] ダイアログ ボックスが開きます。
- ステップ 8 [Continue] をクリックしてサマリーを終了します。

## ハブサイトの QoS 帯域幅の割合の変更

ハブ サイトがプロビジョニングされた後 (N 日目)、ハブ サイトの QoS 帯域幅の割合を変更できます。

### 手順

- ステップ 1 IWAN アプリのホームページで、[Set up Branch Sites] をクリックします。[Sites] ページが開きます。
- ステップ 2 [Sites] タブをクリックします。
- ステップ 3 ハブ サイトの鉛筆アイコン ([Edit Site]) をクリックします。



(注) IWAN のフロントページで [Configure Hub Site & Settings] をクリックし、[IWAN Aggregation Site] タブをクリックすることによっても、このページに移動できます。

- ステップ 4 WAN リンク (ルータとクラウド間のリンク) 上にある鉛筆アイコンをクリックします。[Configure Link] ダイアログボックスが開きます。
- ステップ 5 [Service Provider] フィールドの横にある [Edit] (鉛筆) アイコンをクリックして、モデルの説明があるダイアログボックスを開きます。
- ステップ 6 必要に応じて QoS 帯域幅の割合を変更します。
- ステップ 7 [Update] をクリックします。変更した帯域幅の割合が WAN リンクに適用されます。

■ ハブサイトの QoS 帯域幅の割合の変更