



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\(4-1 ページ\)](#)
- [\[System Settings\] の設定\(4-2 ページ\)](#)
- [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\(4-7 ページ\)](#)
- [アップロードされた Cisco IOS ソフトウェア イメージの削除\(4-8 ページ\)](#)
- [サービス プロバイダーの設定\(4-8 ページ\)](#)
- [IP アドレス プールの設定\(4-11 ページ\)](#)
- [IWAN 集約サイトの設定\(4-16 ページ\)](#)
- [ハブサイトの設定の変更\(4-24 ページ\)](#)
- [IWAN サイトと非 IWAN サイトの共存について\(4-24 ページ\)](#)
- [同種および異種トポロジ\(4-25 ページ\)](#)
- [IP アドレス プールについて\(4-27 ページ\)](#)
- [マルチトンネル終端\(MTT\)の設定\(4-28 ページ\)](#)
- [プロビジョニング済みハブサイトの WAN 帯域幅の更新\(4-33 ページ\)](#)
- [ハブサイトの QoS 帯域幅の割合の変更\(4-34 ページ\)](#)
- [サービス プロファイルの QoS 帯域幅の割合の変更\(4-35 ページ\)](#)
- [ユーザ定義の QoS 帯域幅サービス プロファイルの削除\(4-36 ページ\)](#)
- [ハブサイトの地理的な場所の設定\(4-36 ページ\)](#)
- [LiveAction を使用したネットワーク データの収集\(4-36 ページ\)](#)
- [APIC-EM と IWAN 非対応ネットワークとの間の相互運用性\(4-38 ページ\)](#)

ハブサイトの設定

IWAN アプリのホーム ページから、[Configure Hub Site & Settings] オプションを使用してハブサイトを設定します。以下に説明する設定タスク用のタブがある [Network Wide Settings] ページが開きます。

チュートリアルビデオ

[IWAN アプリ ハブのプロビジョニング](#)

表 4-1 [Network Wide Settings] ページ:タスク

タブ	タスク	次を参照してください
システム	次のものを含む、システム設定項目を設定します。 <ul style="list-style-type: none"> • NetFlow コレクタのサーバアドレス • DNS サーバ • Syslog サーバ • AAA サーバ • NAT/プロキシアドレス • SNMP • DHCP 	[System Settings] の設定 (4-2 ページ)
認定 IOS リリース	新しいグリーンフィールドブランチ デバイスにロードする Cisco IOS ソフトウェア イメージをアップロードします。	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 (4-7 ページ)
サービス プロバイダー	次のようにサービス プロバイダーを設定します。 <ul style="list-style-type: none"> • 各サービス プロバイダーの識別ラベル • 各サービス プロバイダーの接続のタイプ 	サービス プロバイダーの設定 (4-8 ページ)
IP Address Pools	IP アドレスを割り当てる IP アドレス プールを設定します。 <ul style="list-style-type: none"> • サービス プロバイダー(オーバーレイ) • ループバック • ブランチ サイト 	IP アドレス プールの設定 (4-11 ページ)
IWAN 集約サイト	IWAN 集約サイトは、次のように設定します。 <ul style="list-style-type: none"> • マスター コントローラ • ハブ サイト • ハブ デバイス:LAN、WAN、および MC の設定 	IWAN 集約サイトの設定 (4-16 ページ)

[System Settings] 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。

[Show More] または [Show Less] をクリックして、設定を表示または非表示にします。

手順

- 手順 1** 初めてログインした場合は、グローバル設定を [CLI Credentials] ダイアログボックスに指定します。ユーザ名とパスワードを入力し、[Add] をクリックします。
- 手順 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。
- 手順 3** Cisco IWAN 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 [System Settings] タブ

System Settings

NetFlow Collector

* Netflow Destination IP: 1.1.1.1

* Port Number: 9991

NAT/Proxy IP Address

* APIC-EM behind NAT/Proxy: No Yes

APIC-EM NAT/Proxy IP: _____

DNS

* Domain Name: cisco.com

SNMP

* Version: V2C

* Read Community: *****

To configure additional network settings like DHCP, AAA, Syslog and advance settings in SNMP, DNS, etc. click "Show more" link below:

[Show more](#)

Previous Save & Continue

I wish this page would...

手順 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。

手順 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。
Primary Server	(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。

手順 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
IP Address	<p>(任意) 認証、許可、アカウントिंग(AAA)サーバの IP アドレス。</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • Cisco APIC-EM グローバル クレデンシャル • 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 • 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
Key	(任意) AAA サーバにアクセスするためのキー。

手順 7 [Syslog] 領域で、次の情報を入力します。

フィールド	説明
Server IP	<p>(任意) Syslog サーバの宛先 IP アドレス。</p> <p>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。</p>

手順 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。

手順 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

フィールド	説明
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"> • Authentication and Encryption • [No Authentication and No Encryption] • [Authentication and No Encryption]
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"> • HMAC-SHA • HMAC-MDS
Username	認証ユーザ名。
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

フィールド	説明
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。

手順 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。

手順 11 [Save and Continue] をクリックします。

[Systems] タブで既存の値を更新した後に、変更を示す [Network Wide Settings Summary] ダイアログボックスが開きます。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。

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) この手順はグリーンフィールドブランチデバイスにのみ適用されます。

認定された Cisco IOS イメージをコンピュータから Cisco IWAN アプリ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。

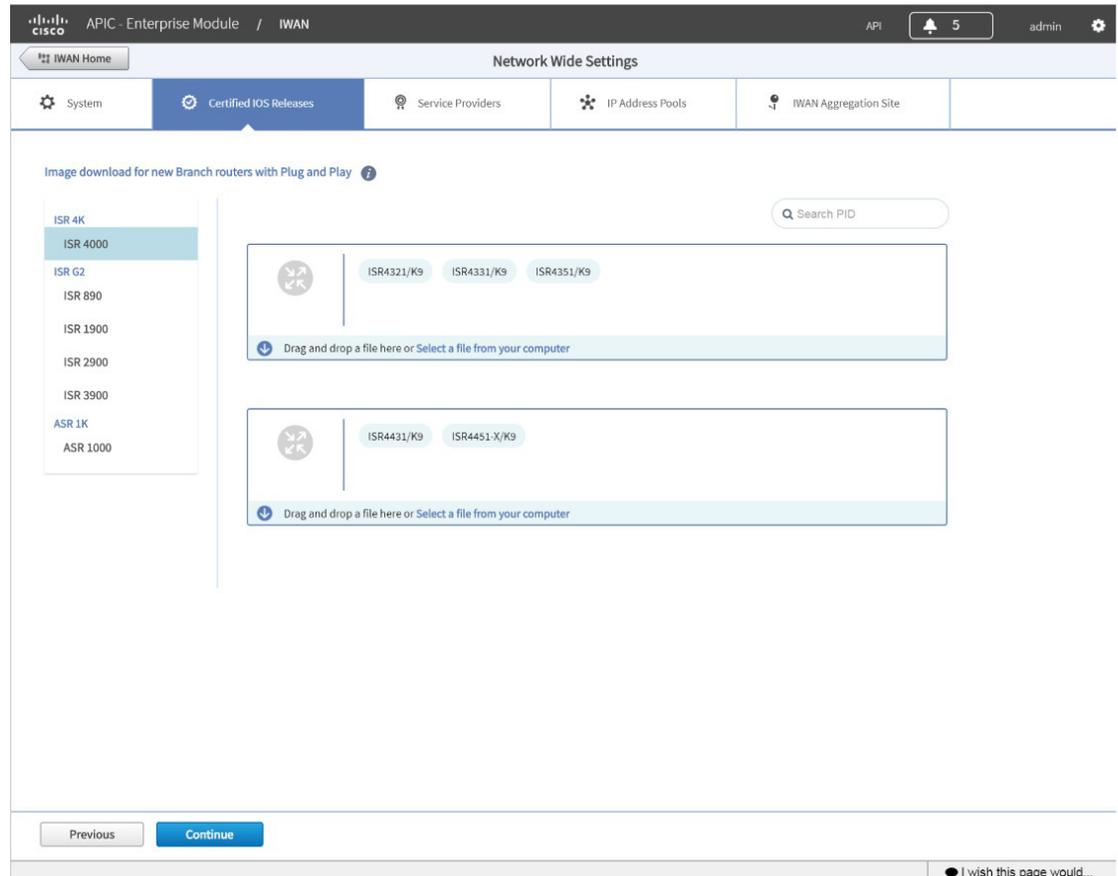


(注) 適切なソフトウェアイメージがすでにいずれかの新しいグリーンフィールドルータにインストールされている場合は、この手順をスキップできます。

手順

手順 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



手順 2 左ペインから、ルータタイプを選択します。

手順 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。

手順 4 [Continue] をクリックします。

アップロードされた Cisco IOS ソフトウェア イメージの削除

Cisco IOS ソフトウェア イメージを削除する前に、イメージを、デフォルトでそのイメージを使用するように設定されているプラットフォーム モデルから関連付けを解除する必要があります。イメージを削除するには、次の手順に従います。

手順 1 APIC-EM の左側のパネルでアイコンをクリックして、「ネットワークのプラグアンドプレイ」アプリを開きます。

手順 2 アップロードした画像を表示するページの上部の [Images] タブをクリックします。

手順 3 削除する画像のイメージ名をクリックして、[Image Info] ダイアログボックスを開きます。

手順 4 [Use this Image as Default] 列で、ボックスの選択をすべて解除し、さまざまなプラットフォームタイプからイメージの関連付けを解除します。(ヒント:[All] ボックスを2回クリックすると、列内のボックスがすべてクリアされます。)

手順 5 ダイアログボックスで [Save] ボタンをクリックします。

手順 6 削除する必要があるすべてのイメージに対して繰り返します。

手順 7 [Images] タブで、削除するイメージを選択して、左上にある [Delete] ボタンをクリックします。

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

手順 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 4-3 [Service Providers] タブ

The screenshot shows the Cisco I WAN configuration interface. The top navigation bar includes 'System', 'Certified IOS Releases', 'Service Providers' (selected), 'IP Address Pools', and 'I WAN Aggregation Site'. The main content area is titled 'Configure Service Providers' and contains two tables.

WAN Label	WAN Type	Metered
INTT	Public	<input type="checkbox"/>
MPLS	Private	<input type="checkbox"/>

Profile Name	Class Model
Default 4-Class Model	4 Class
Default 5-Class Model	5 Class
Default 6-Class Model	6 Class
Default 8-Class Model	8 Class

手順 2 [Configure Service Providers] 領域で、[+] アイコンをクリックして、以下のテーブルに表示されているプロパティを設定します。



(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"> プライベート パブリック

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] オプションを使用できます。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) 計量できるのは1つのリンクのみです。</p> <p>(注) パブリッククラウドに許可されるのは1つのリンクのみです。</p>
Available QoS Models for Service Providers	
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"> • 4 Class • 5 Class • 6 Class • 8 Class

手順 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 4-4 [Add Service Profile] ダイアログボックス

Class Name	DSCP	Priority Bandwidth (%)	Remaining Bandwidth (%)
Voice	EF	10	
CLASS1 DATA	AF31		
call-signaling			4
interactive-video			30
streaming-video			10
CLASS2 DATA	AF21		
critical-data			25
Default	0		
class-default			25
net-control-mgmt			5
scavenger			1

Total: 100

Buttons: Save, Cancel

手順 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"> • 4 Class • 5 Class • 6 Class • 8 Class
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 (%)	音声などの優先度クラスに割り当てる帯域幅の割合。
Remaining Bandwidth (%)	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 以上の値を入力します。[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。

手順 5 [Continue] をクリックします。[IWAN Aggregation Site] タブが開きます。IWAN 集約サイトの設定 (4-16 ページ) を参照してください。

IP アドレス プールの設定

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 プールの一般情報については、[IP アドレス プールについて \(4-27 ページ\)](#) を参照してください。



(注) IP アドレス プールを計画するときは、IWAN ネットワークの将来の拡張、および今後導入される可能性のあるリモート サイトなど、将来のすべての要件を考慮します。ハブ サイトのプロビジョニング後は、IP アドレス プールの設定を変更できません。



(注)

IWAN アプリの以前のバージョンは、汎用 IP アドレス プールと呼ばれます。1.5.0 リリース以降、IWAN アプリはサービス プロバイダー アドレス プール、グローバル アドレス プール、およびサイト固有アドレス プールを指します。

IWAN アプリでのアドレス プール設定の概要

汎用プール

汎用プールを使用して、DMVPN トンネルの IP アドレス、Cisco Performance Routing (PfR) の管理 ループバック アドレス、およびグリーンフィールド リモート サイトの LAN インターフェイスを割り当てます。

汎用プールに割り当てられるアドレス範囲が、ネットワークの他の場所で使用されていないことを確認します。

IWAN ネットワークで使用されるリモート サイトの数を入力します。これは、DMVPN オーバーレイの数に対応します。[IP Pool Calculator] をクリックして、汎用プールに必要なサブネット マスクを表示します。

ループバック プール

ループバック プールは、Cisco Performance Routing (PfR) の管理ループバック アドレスの IP アドレスを割り当てるために使用されます。

ループバック プールに割り当てられるアドレス範囲が、ネットワークの他の場所で使用されていないことを確認します。

IWAN ネットワークで使用されるリモート サイトの数を入力します。これは、DMVPN オーバーレイの数に対応します。[IP Pool Calculator] をクリックして、ループバック プールに必要なサブネット マスクを表示します。

LAN グリーンフィールドプール

汎用プールからグリーンフィールド リモート サイト LAN にアドレスを割り当てない場合には、次の 2 つのオプションがあります。

1. 独立した LAN グリーンフィールド プールを作成します。これは、すべてのリモート ブランチの単一の IP プールになります。VLAN の数と VLAN ごとのデバイスの数を [IP Pool Calculator] ボタンをクリックして入力することで、この単一 IP に必要なサブネット長を計算します。
2. すべてのサイトでリモート サイト VLAN に特定のアドレスを割り当てるには、サイト固有のプールを使用します。

LAN グリーンフィールド プールに割り当てられるアドレス範囲が、ネットワークの他の場所で使用されていないことを確認します。

LAN ブラウンフィールドプール

すべてのブラウンフィールド サイトですべての既存 LAN サブネットの要約ルーティング エントリを作成するには、LAN ブラウンフィールド プール オプションを使用します。これは広告のすべてのブランチ LAN プレフィックスを表すハブからサマリー ルートのみをアドバタイズするために役立ちます。このエントリがない場合、IWAN アプリはブランチ LAN プレフィックスに特定のエントリを使用します。



(注)

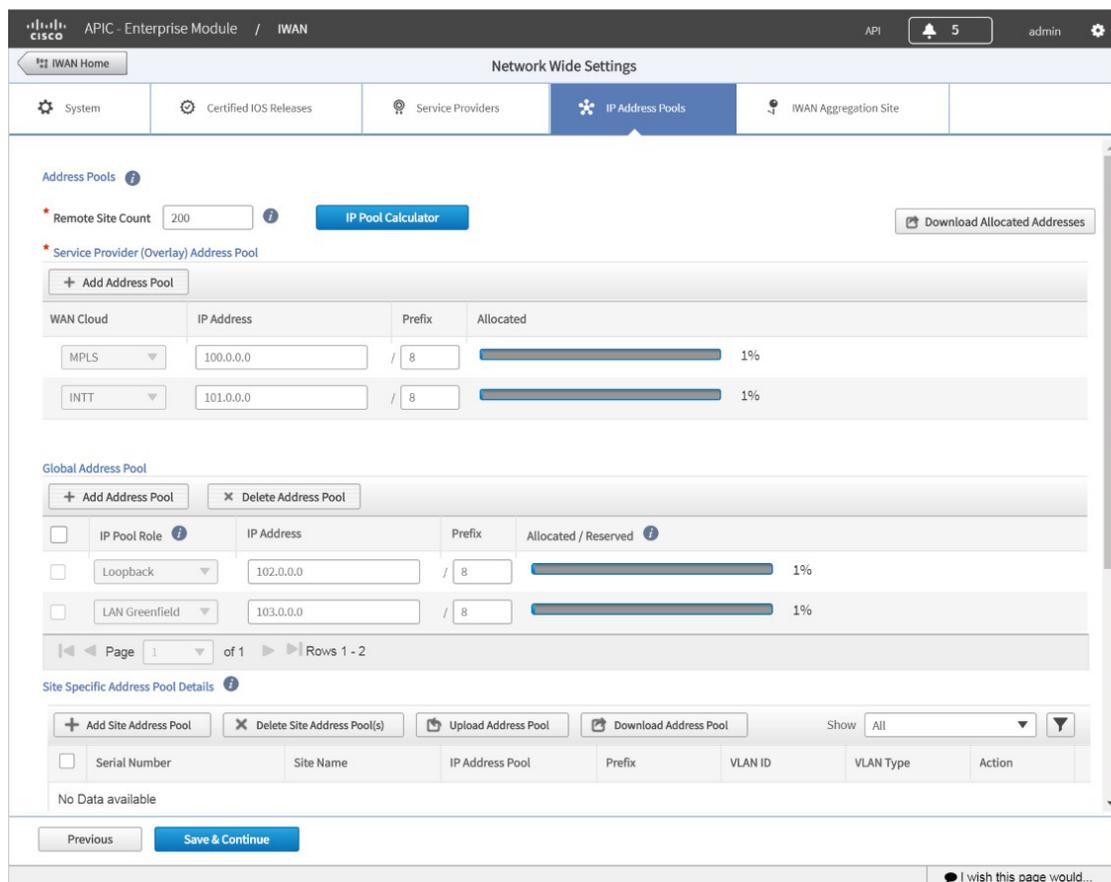
LAN グリーンフィールドと LAN ブラウンフィールドのプールは、Cisco Performance Routing (PfR) のエンタープライズ プレフィックス リストの定義で使用されます。

アドレス プールの設定

手順

手順 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 4-5 [IP Address Pool] タブ



手順 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。

手順 3 [IP Pool Calculator] ボタンをクリックします。

[Proposed IP Range] ダイアログボックスが開き、以下が表示されます。

- IP プールの推奨最小プレフィックス長の値
- VLAN ごとの IP アドレスの数、および VLAN の数の推奨値。

手順 4 [OK] または [Get IP Range] をクリックします。

手順 5 サービス プロバイダー アドレス プールを設定するには、[Service Provider (Overlay) Address Pool] セクションで、[+ Add Address Pool] をクリックします。

サービス プロバイダーごとに最大で 1 つのサービス プロバイダー アドレス プールを設定します。このプールからの IP アドレスは、オーバーレイ IP アドレスのニーズ用に使用されます。

フィールド	説明
WAN クラウド	サービス プロバイダー名を選択します。 (注) IWAN アプリ リリース 1.5.x で変更されたサービス プロバイダー IP アドレス プールの設定。既存の従来の設定をサポートするために IWAN アプリが 1.5.x 以外のリリースからのアップグレードとしてインストールされている場合、この手順では IWAN アプリは WAN クラウドラベルを既存のサービス プロバイダーに対して自動的に提供します。以前のリリースのサービス プロバイダー用に設定された WAN ラベルは、このページで WAN クラウドラベルに使用されます。例:「INET1」、「MPLS」
IP Address	IP アドレス プールの IP アドレス。このプールは、サービス プロバイダー オーバーレイ アドレスのニーズに対応します。
Prefix	CIDR プレフィックス。(クラスレス ドメイン間ルーティング(CIDR)のプレフィックス表記はサブネット マスクを定義します。)
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。

手順 6 グローバルアドレスプールを設定するには、[Global Address Pool] セクションで、[+ Add Address Pool] をクリックします。

フィールド	説明
IP プール ロール	次のロールを選択します。 <ul style="list-style-type: none"> ループバック: Cisco Performance Routing (PFR) の管理ループバック アドレスの IP アドレスを割り当てるために使用されます。 [LAN Greenfield]: 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。 [LAN Brownfield]: 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。 (注) 従来の構成をサポートするため、以前のバージョンの IWAN アプリからのアップグレードとしてインストールされている場合には、IWAN アプリは「汎用」をロールとして提供します。
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。(クラスレス ドメイン間ルーティング(CIDR)のプレフィックス表記はサブネット マスクを定義します。)
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。

手順 7 サイト固有の LAN の IP アドレス プールを設定するには、次のようにします。

- a. [+Add Site Address Pool] をクリックします。[Add Site Address Pool] ダイアログボックスが開きます。
- b. 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。新しい設定済み情報がテーブルに表示されます。

既定では、グリーンフィールド ブランチ サイトの IP アドレスの割り当ては次のとおりです。

- LAN グリーンフィールド IP アドレス プールがある場合、グリーンフィールド ブランチ サイトはこのアドレス プールを使用します。
- LAN グリーンフィールド IP アドレス プールがない場合、グリーンフィールド ブランチ サイトは汎用 IP アドレス プールを使用します (IWAN アプリ リリース 1.5.0 からリリース 1.5.x にアップグレードされた、アップグレード導入の場合のみ該当します)。

VLAN にカスタム IP アドレス プールを使用して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には、サイトをプロビジョニングする前に VLAN とカスタム IP アドレス プールを定義します。(これを実行すると、デフォルトで VLAN 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 プールを使用できなくなります。この場合、汎用 IP アドレス プール オプションは、1.5.0 より前のリリースから 1.5.x リリースの IWAN アプリにアップグレードされた導入にのみ適用されます。)



(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。サイトをプロビジョニングする前に慎重に計画します。



(注)

通常、グリーンフィールド ブランチ サイトの場合、LAN グリーンフィールド プールが必要です。これは次の場合のみはオプションです。

- グリーンフィールド ブランチ サイトには、定義されているサイト固有のプールがあります。
- これは単一ルータ ブランチ サイトです。

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。(クラスレス ドメイン間ルーティング (CIDR) のプレフィックス表記はサブネット マスクを定義します。) 値の範囲 (単一のシリアル番号): 16 ~ 30 値の範囲 (複数のシリアル番号): 16 ~ 29

フィールド	説明
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"> - VLAN タイプの値は 200 文字以下でなければなりません。 - VLAN タイプには「?」記号を使用できません。 - 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。

手順 8 多数のサイト固有アドレス プールをアップロードするには、次のようにします。

- a. [Site Specific Address Pool Details] セクションで、[Download Address Pool] をクリックして、次のテンプレート CSV ファイルをダウンロードします。
Controller_Profile_DD-MM-YYYY.csv
- b. すべての必要な情報を含む CSV ファイルを作成します。
- c. [Upload Address Pool] をクリックし、CSV ファイルをアップロードします。

手順 9 [Save & Continue] をクリックします。

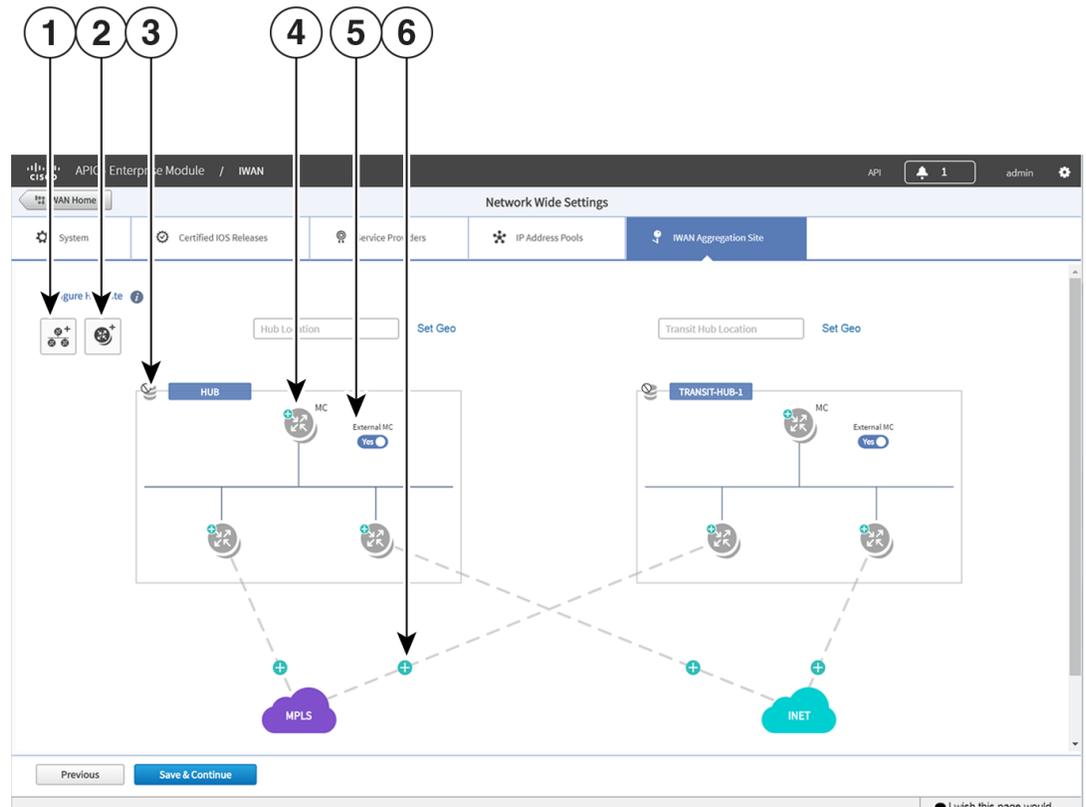
IWAN 集約サイトの設定

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	POP の追加	4	External MC ルータの設定
2	境界ルータの追加	5	[External MC] 切り替えボタン
3	LAN の設定	6	WAN リンクの設定

手順

手順 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、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。
SNMP	
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"> • Authentication and Encryption • [No Authentication and No Encryption] • [Authentication and No Encryption]
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"> • HMAC-SHA • HMAC-MDS
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。
SNMP Retries and Timeout	
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
SSH/Telnet	
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。

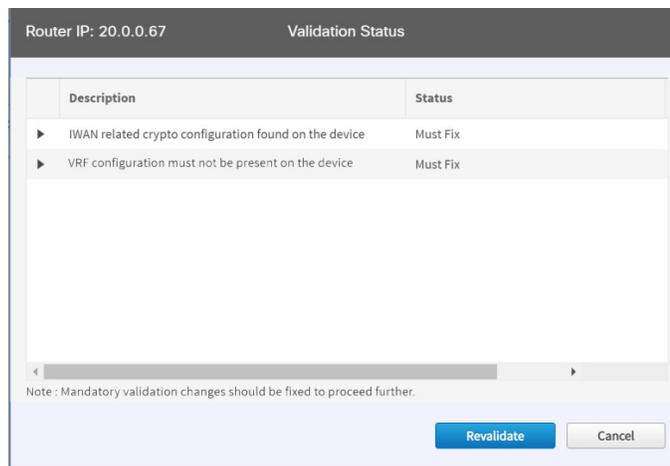
- [Add Device] をクリックします。

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。

手順 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。[LAN Routing] ダイアログボックスが開きます。

[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
Select LAN Protocol for Redistribution	
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	
Available (テーブル)	ハブ サイトの IP アドレスの自動入力されたリスト。
Selected (テーブル)	[Available] テーブルから選択された IP アドレス。

- b. 1 つ以上の IP アドレスを [Available] テーブルから選択し、矢印をクリックして、アドレスを [Selected] テーブルに移動させます。選択された IP アドレス (プレフィックス) のみ、ハブで設定されます。
- アドレスを [Selected] テーブルから削除するには、アドレスの上にカーソルを移動し、赤い X をクリックします。
- (オプション) [Add DCIP/Mask] リンクを使用して IP アドレスをフィルタリングします。
- c. [Save (保存)] をクリックします。

手順 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。
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

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
Bandwidth (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。
Use Loopback for DMVPN Tunnel	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 (4-24 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、Cisco IWAN 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、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。
Bandwidth (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。

手順 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] 領域で設定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。

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)。

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 Cisco IWAN 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。
- (Cisco IWAN 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。

同種および異種トポロジ

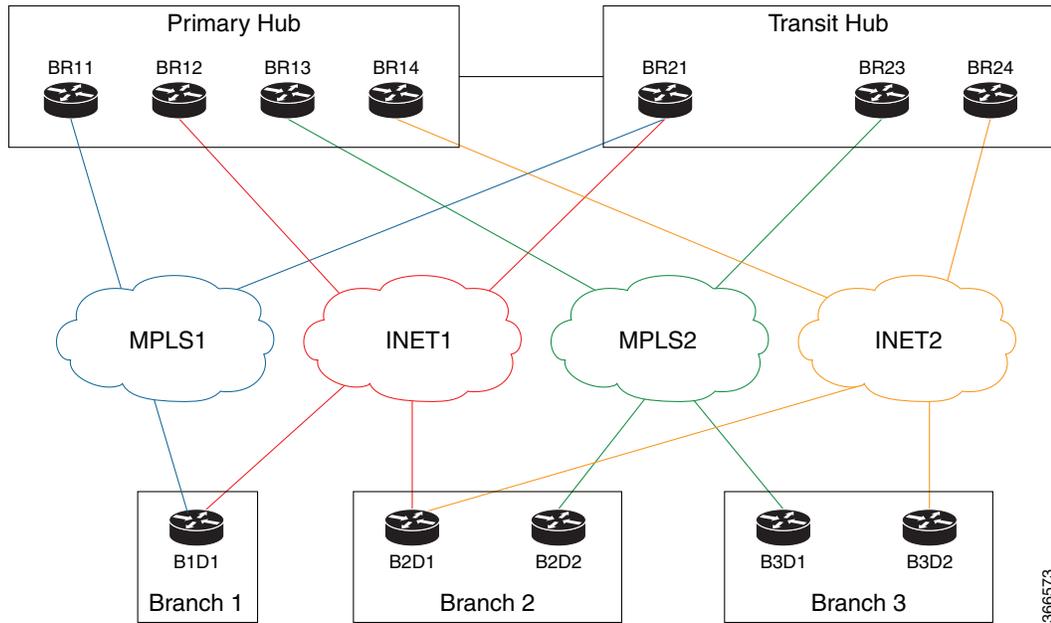
Cisco IWAN リリース 2.0 以降では、プロビジョニング済みのサイトで以下を実行できます。

- 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(Public または Private)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 プリファレンスに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)。

同種トポロジ

同種トポロジでは、プライマリ ハブ サイトおよび関連する中継ハブ サイトは、サービス プロバイダーへの接続はすべて同じです。単一のデバイスで複数の接続を持つことができるため、サイトでは接続を処理する異なる数のデバイスを持つことができます。例では、どちらのハブ サイトも4つすべてのサービス プロバイダーに接続しています。

図 4-7 同種トポロジ

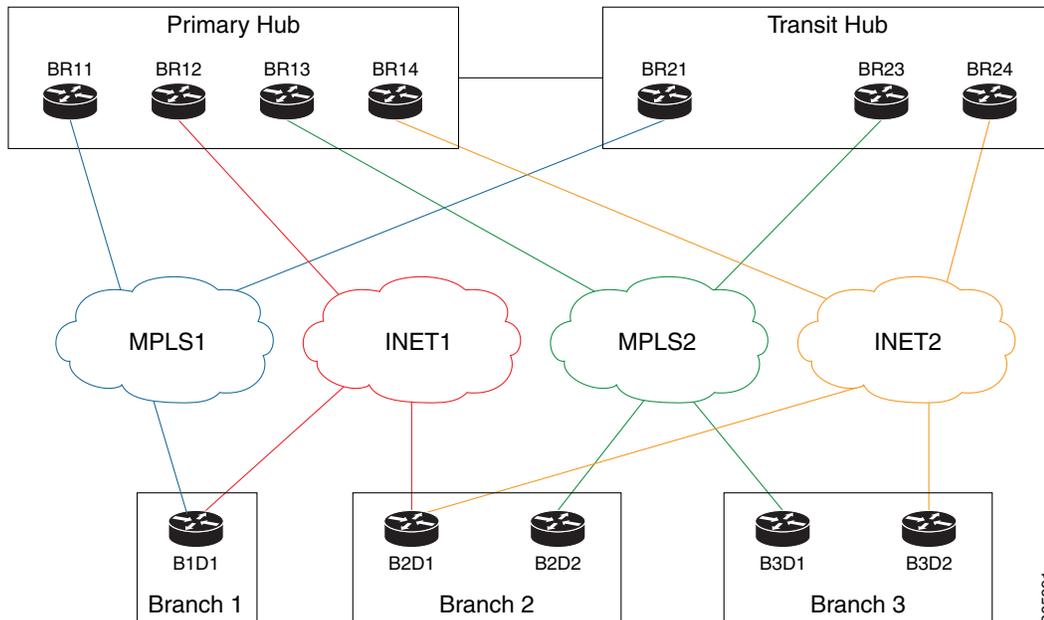


366573

異種トポロジ

異種トポロジでは、プライマリ ハブ サイトおよび関連する中継ハブ サイトは、同じすべてのサービス プロバイダーに接続するわけではありません。例では、プライマリ ハブは、4 つのサービス プロバイダーに接続されており、中継ハブは 3 つのみに接続されています。

図 4-8 異種トポロジ



365691

IP アドレス プールについて

IWAN アプリは、グローバル エンタープライズ IP アドレス プール スペースから自動的に IP アドレスを使用します。ハブとスポーク デバイスのプロビジョニング時に、IWAN アプリはユーザ構成 IP アドレス プールに割り当てられた IP アドレスを使用します。これには、インターフェイス、LAN、VPN オーバーレイ、ルーティング IP アドレスが含まれます。

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、グローバル 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するには、IP アドレス プールのサイズを適切に定義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。現行の Cisco IWAN リリースでは、初期プロビジョニングの後でもサイトやサービス プロバイダーの数は増やせませんが、指定済みの IP アドレス プールは変更できません。したがって、IP アドレス プールの定義時には、サービス プロバイダーの将来の規模やサイトのサイズを考慮することをお勧めします。サービス プロバイダー IP アドレス 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。

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、サービス プロバイダーと汎用グローバルの 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 プールまたはグローバル 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。

マルチトンネル終端(MTT)の設定

IWAN アプリは、ハブ デバイスの複数の WAN リンクをサポートします。サイトのプロビジョニング時(0 日目)またはプロビジョニング後(N 日目)に、複数のリンクをデバイスに追加できます。この機能は、プライマリ ハブ サイトおよび中継ハブ サイトの両方で利用可能です。(中継ハブ サイトがプライマリ ハブ サイトと並列に動作し、負荷分散またはフェールオーバー サポート(あるいはその両方)を提供します)。

プライマリ ハブ サイトと中継ハブ サイトがすべてのリンクへの接続を必要とする

プライマリ ハブ サイトと中継ハブ サイトを一緒に使用するトポロジの場合、プライマリ ハブ と中継ハブの両方は、プロビジョニング時(0 日目)に同じサービス プロバイダーに接続していることが必要です。これは「同種」トポロジと呼ばれます([同種および異種トポロジ\(4-25 ページ\)](#)を参照)。

プライマリ ハブ サイトと中継ハブ サイトでデバイスの数が異なる場合がある

プライマリ ハブ サイトと中継ハブ サイトを含むトポロジを使用している場合、デバイス構成は両方のサイトで同じである必要はありません。サイトのデバイスの数は異なる場合がありますが、それらのデバイスのほとんどは同じ接続を共有します。これには、単一のデバイスへの複数のリンクを構成することが必要になる場合があります。

たとえば、プライマリ サイトに2つのデバイスがあり、それぞれにサービス プロバイダーへの単一のリンクがあり、関連する中継サイトにはデバイスが1つしかない場合、その唯一のデバイスにはプライマリ サイトと同じ接続を提供する2つのリンクが必要です。

プロビジョニング時(0 日目)の複数の WAN リンク構成:機能、制限事項、手順

機能

表 4-4 プロビジョニング時(0 日目)の複数の WAN リンク機能

機能
サービス プロバイダー、デバイス、リンク
サポートされるサービス プロバイダー:2 から 4
ハブ サイトのデバイスの最小数:1
デバイスごとのリンクの最大数:3

表 4-4 プロビジョニング時(0日目)の複数のWANリンク機能(続き)

機能
オプション
パブリック/プライベートリンクの任意の組み合わせでマルチリンクハブサイトをプロビジョニングします。
ハブサイトで別のデバイスをプロビジョニングして、異なるセットのリンクを動作するように準備できます。
各サイトで異なる数のデバイスがある複数のハブサイトをプロビジョニングします。

要件および制約事項

表 4-5 プロビジョニング時(0日目)の複数のWANリンク要件および制限

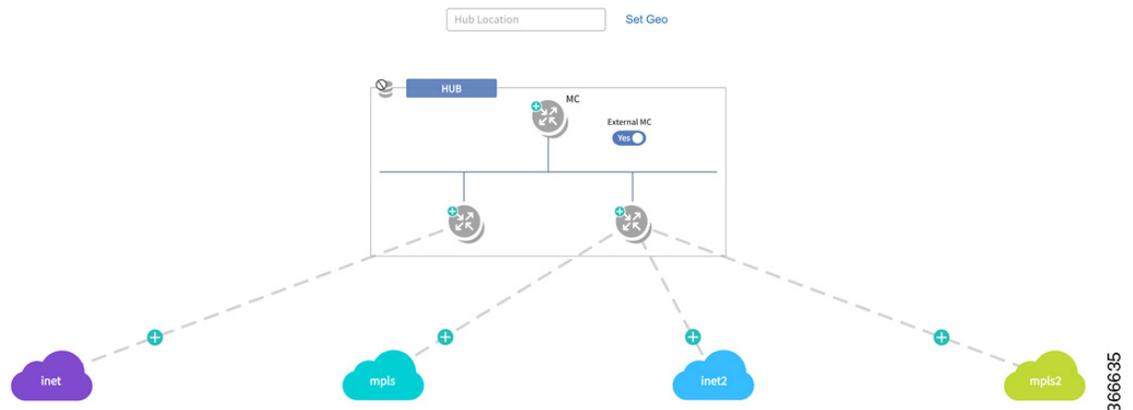
要件/制限事項
参加デバイスのOS
Cisco IOS XE 16.3.3
接続
ハブサイトのプロビジョニング時(0日目)には、各ハブサイトはすべてのサービスプロバイダーへの接続が必要です。

プロビジョニング時(0日目)にハブデバイスへ複数リンクを追加する

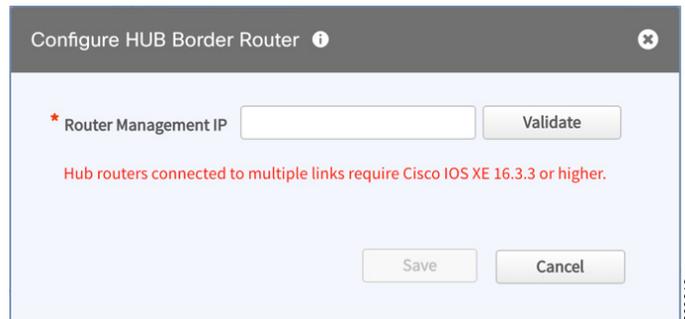
プロビジョニング前(0日目)にデバイスにリンクを追加するには、デバイスとクラウドの間リンクを描画する必要があります。次の手順を使用してください。

手順

- 手順 1 [Network Wide Settings] ページ > [IWAN Aggregation Site] タブを開きます。
- 手順 2 ハブデバイスのリンクを追加するには、デバイスをクリックして押し続け、目標のクラウドアイコンにまで線を「描画」します。必要な場合は、複数の新しいリンクを描画します。
新しく描画されたリンクは、まだ構成されていないことを示す点線として表示されます。



- 手順 3** 新しいリンクがあるデバイスをクリックします(または、1 つ以上のデバイスにリンクを追加する場合、新しいリンクがあるいずれかのデバイスをクリックします)。
- ダイアログボックスが表示され、ルータ管理 IP の入力が求められます。このダイアログボックスはまた、この操作を実行するには、デバイスが Cisco IOS XE 16.3.3 を稼働している必要があることも示します。



- 手順 4** 必要な情報を入力し、[Save] ボタンをクリックして続行します。
- 手順 5** 以降のダイアログボックスで、必要に応じて SNMP および SSH/Telnet の情報を入力し、[Add Device] ボタンをクリックします。
- 手順 6** LAN IP インターフェイス領域で、使用するインターフェイスを選択し、[Save] ボタンをクリックします。
- IWAN アプリでは、いくつかの検証を実行します。任意の検証が失敗した場合、[Validation Status] ダイアログボックスが表示され、エラーが示されます。たとえば、デバイス OS が、それに対して描画したリンクと互換性がない場合には、妥当性確認エラーが表示されます。
- 手順 7** 新しい各リンクで、新しいリンクのプラス記号をクリックして [Configure Link] ダイアログボックスを開きます。
- 手順 8** WAN IP インターフェイスと他の必須フィールドの情報を入力します。
- 手順 9** [Save] ボタンをクリックします。
- リンクを示す線は実線です(かつては点線でした)。
- 手順 10** 他のデバイスに新しく描画されたリンクがある場合、デバイスを 1 つずつクリックし、それぞれに対して上記の手順を繰り返します。
- 手順 11** ページの下部で、[Save & Continue] ボタンをクリックします。
- 設定の概要が表示されます。
- 手順 12** [Continue] ボタンを押して、プロビジョニングを開始します。

プロビジョニング後(N日目)の複数のWANリンク構成:機能、制限事項、手順

機能

表 4-6 プロビジョニング後(N日目)の複数のWANリンク機能

機能
サービス プロバイダー、デバイス、リンク
サポートされるサービス プロバイダー:2 から 4
ハブ サイトのデバイスの最小数:1
デバイスごとのリンクの最大数:3
オプション
新しいリンクを1つ以上のハブ デバイスに追加します(プロビジョニング後(N日目)で既存のハブ デバイスへのリンクを追加する(4-32 ページ)を参照)。
ハブ サイトで別のデバイスをプロビジョニングして、異なるセットのリンクを動作するように構成できます。
マルチリンク デバイスがある中継ハブ サイトを削除します。

要件および制約事項

表 4-7 プロビジョニング後(N日目)の複数のWANリンク要件および制限

要件/制限事項
参加デバイスの OS
Cisco IOS XE 16.3.3
接続
ハブのサイトのプロビジョニング後(N日目)、ハブ サイトはサービス プロバイダーへ別の接続を持つ場合があります。これは「異種配置」と呼ばれます(同種および異種トポロジ(4-25 ページ)を参照)。
制限事項
プロビジョニング後(N日目)のハブ ルータからは既存のリンクを削除できません。デバイス上に、クラウドに接続されている最後のリンクがある場合、接続されているブランチをプロビジョニング解除し、ハブ デバイスを削除します。これを行った後に、目的のリンクを使用すればブランチ サイトを再プロビジョニングできます。
新しいリンクをハブ「マスター コントローラ」(MC)デバイスに追加することはできません。デバイスにリンクを追加すると、デバイス上のルーティング操作は中断します。
ブランチ サイトへの接続を提供する唯一のデバイスにリンクを追加する場合、そのサイトへの接続がこの処理中に失われます。

プロビジョニング後(N日目)で既存のハブデバイスへのリンクを追加する

プロビジョニング後(N日目)にデバイスにリンクを追加する手順は、プロビジョニング前(0日目)に使用する手順とは異なります。プロビジョニング前は、デバイスとクラウドとの間のリンクを描画することによってリンクを追加します。プロビジョニング後は、次の手順を使用します。



(注)

- デバイスにリンクを追加すると、デバイス上のルーティング操作は中断します。
- これはブランチ サイトへの接続を提供する唯一のデバイスであり、そのサイトへの接続がこの処理中に失われます。

手順

手順 1 IWAN_RECOVERY.cfg というファイル名を持つルータのブートフラッシュ上にクリーン コンフィグレーション ファイルを作成します。

これは、IWAN アプリがあるデバイスを使用する前の構成を含むコンフィグレーション ファイルです。ファイルには、現在の LAN、WAN、および SNMP の詳細と、追加される新しい WAN リンクの情報を含める必要があります。

手順 2 [Network Wide Settings] ページ > [IWAN Aggregation Site] タブを開きます。

手順 3 デバイスをクリックし、[Device Operations] ダイアログボックスを表示します。



手順 4 [Device Operations] ダイアログボックスで、[Add link to device] を選択し、[Start] ボタンをクリックします。

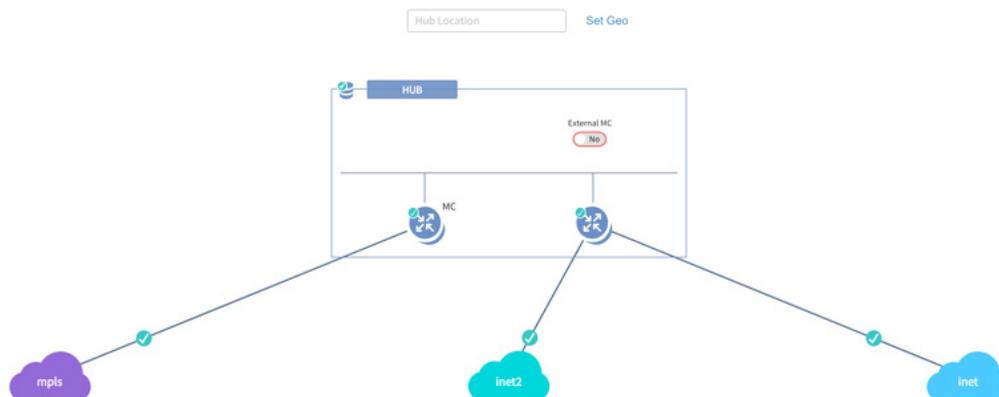
[Add link to device] ダイアログボックスが表示され、リンクの追加に関する重要な情報が示されます。

手順 5 [Add link to device] ダイアログボックスで各項目を選択し、確認して続行します。

手順 6 一連の [Configure Hub Border Router] ダイアログボックスが表示され、リンクを追加するためのオプションが提供されます。

- **自動メソッド:** デバイス上のクリーン コンフィグレーション ファイルに最新の LAN IP 情報と SNMP クレデンシャルが含まれている場合、IWAN アプリはユーザ入力を必要とせず、後続のダイアログボックスでフィールドに値を自動的に入力し、それらを自動的に閉じます。
結果: IWAN アプリはデバイスをクリーン コンフィグレーション ファイルで定義されている構成に戻し、既存の WAN リンクを自動的に追加し、新しいリンク情報の入力を求めます。
- **手動メソッド:** デバイス上のクリーン コンフィグレーション ファイルにさまざまな LAN IP 情報や別の SNMP クレデンシャルが含まれている場合、[Configure Hub Border Router] ダイアログボックスでその情報の入力が求められ、既存の WAN リンクでのデバイスの再プロビジョニングや新しいリンクの構成がサポートされます。情報を入力して、デバイスへの新しいリンクの追加を続行します。

プロセスを完了すると、新しいリンクはトポロジ内では実線として表示されます。



366644

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\(5-26ページ\)](#)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。

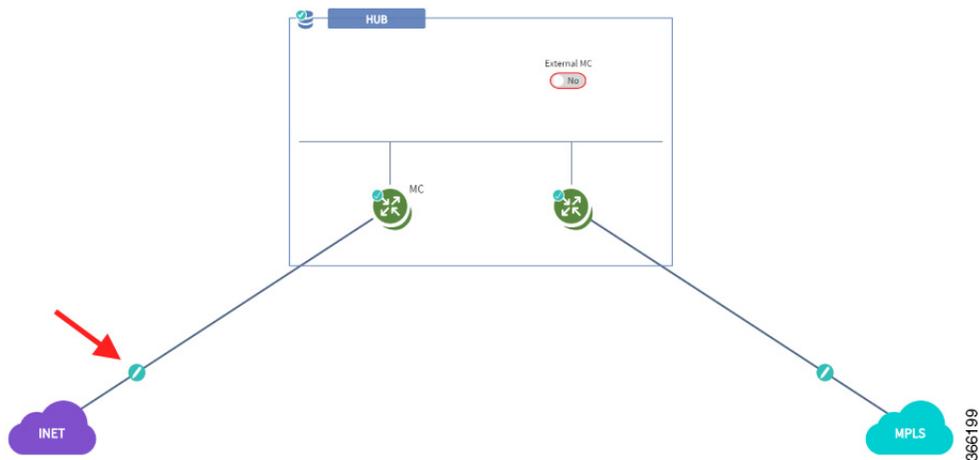
手順

- 手順 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。
- 手順 2 [Sites] タブをクリックします。
- 手順 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。

- 手順 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。



- 手順 5 [Bandwidth] フィールドに新しい値を入力します。
- 手順 6 ダイアログ ボックスで [Save] をクリックします。
- 手順 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。
- 手順 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

- 手順 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。
- 手順 2 [Sites] タブをクリックします。
- 手順 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。

- 手順 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。
- 手順 5 [Configure Link] ダイアログボックスで、[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ます。ダイアログボックスが開き、特定のサービス プロファイルの情報が表示されます。
- 手順 6 必要に応じて QoS 帯域幅の割合を変更します。
- 手順 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。

サービスプロファイルの QoS 帯域幅の割合の変更

サービスプロファイルに対するグローバルな QoS 帯域幅の割合はいつでも変更できます。サービスプロファイルを使用するすべての WAN 接続は、接続がハブサイト用かブランチサイト用かに応じて更新されます。この操作は、サービスプロファイルを使用しているサイトがプロビジョニング後(N日目)であっても可能です。

サービスプロファイルに対して QoS 帯域幅の割合をグローバルに更新すると、接続ごとに個別に割合を更新することと比較して、時間を節約できます。これは、変更が特定のサービスプロファイルを使用する各 WAN 接続を対象としている場合に便利です。

手順

- 手順 1 IWAN アプリのホームページで、[Configure Hub Site & Settings] をクリックします。[Network Wide Settings] ページが開きます。
- 手順 2 [Service Providers] タブが開きます。
- 手順 3 [Available QoS models for Service Providers] セクションに、既存のサービスプロファイル(デフォルトプロファイルとユーザが作成したプロファイルを含む)がリストされます。サービスプロファイルを編集するには、プロファイルの鉛筆型アイコンをクリックします。[Edit Service Profile] ダイアログボックスが開きます。

Class Name	DSCP	Priority Bandwidth (%)	Remaining Bandwidth (%)
VOICE	EF	20	Total: 100
CALL-SIGNALING	CS3	4	
CRITICAL-DATA	AF21	25	
INTERACTIVE-VIDEO	AF41	30	
NET-CONTROL-MGMT	CS6	5	
SCAVENGER	CS1	1	
STREAMING-VIDEO	AF31	10	
DEFAULT	0	25	

- 手順 4 必要に応じて QoS 帯域幅の割合を変更します。
- 手順 5 [Update] ボタンをクリックします。変更された帯域幅の割合は、サービスプロファイルを使用しているすべての WAN リンクに適用されます。

ユーザ定義の QoS 帯域幅サービス プロファイルの削除

使用中でないユーザ定義の QoS 帯域幅サービス プロファイルを削除できます。

手順

-
- 手順 1** IWAN アプリのホームページで、[Configure Hub Site & Settings] をクリックします。[Network Wide Settings] ページが開きます。
- 手順 2** [Service Providers] タブが開きます。
- 手順 3** [Available QoS models for Service Providers] セクションに、既存のサービス プロファイル(デフォルト プロファイルとユーザが作成したプロファイルを含む)がリストされます。ユーザ定義のサービス プロファイルを削除するには、プロファイルの「X」アイコンをクリックします。
- 使用中のサービス プロファイルを削除すると、IWAN アプリにより警告が表示されます。
-

ハブサイトの地理的な場所の設定

必要に応じて、ハブサイトの地理的な場所を設定します。場所はいつでも設定できるため、サイトのプロビジョニング後(N日目)でも可能です。

地理的なサイトの場所を設定した後、その情報が [Siteslists] ページおよびサイトの [Site Details] ページに表示されます。

手順

-
- 手順 1** IWAN アプリのホームページで、[Configure Hub Site & Settings] をクリックします。[Network Wide Settings] ページが開きます。
- 手順 2** [IWAN Aggregation Site] タブが開きます。
- 手順 3** 各ハブ サイトの上部で、次のいずれかを実行します。
- a. フィールドに市区町村郡名を入力します。入力すると、市区町村郡オプションが表示されます。いずれか1つを選択します。
- または
- b. [Set Geo] をクリックして、マップ ビューにその場所を設定します。
-

LiveAction を使用したネットワーク データの収集

IWAN アプリはネットワーク統計情報「コレクタ」とともに動作して、IWAN ネットワークからネットワーク パフォーマンス データを収集します。具体的には、コレクタは Cisco AVC および Performance Routing (PfR) Netflow レコードをネットワーク内のルータから IWAN アプリにエクスポートします。

デフォルトでは、IWAN アプリは [Cisco Prime Infrastructure](#) とともに動作して、ネットワーク パフォーマンス データを収集します。必要に応じて、パフォーマンス データの収集に [LiveAction](#) を使用するように、IWAN アプリを設定できます。

IWAN アプリが LiveAction を使用していることを示すもの

IWAN アプリが LiveAction を使用するように設定されている場合、マップ ビューにサードパーティによるモニタリングのインジケータが示されます。



LiveAction を使用する際の制限事項

- ネットワーク データの収集に LiveAction を使用する場合、アプリケーションのステータスで IWAN サイトの表示をフィルタリングすることはできません。
- [Site Details] ダイアログボックスにアプリケーションのステータスは表示されません。

LiveAction ネットワーク監視の有効化

LiveAction ネットワーク監視の有効化については、[カスタム設定のデフォルト テンプレート \(6-2 ページ\)](#) の LiveAction テンプレートを参照してください。

LiveAction の設定

手順

- 手順 1 IWAN アプリのホームページで、[Configure Hub Site & Settings] をクリックします。[Network Wide Settings] ページが開きます。
- 手順 2 [System] タブを開きます。
- 手順 3 [Netflow Collector] セクションで、次の手順を実行します。
 - a. [Netflow Destination IP] フィールドで、コネクタのアドレスを設定します。
 - b. [Port Number] フィールドで、Live Action によって使用されるポートとして 2055 を入力します。



(注) Cisco Prime Infrastructure を使用している場合、ポート番号を 9991 に設定します。

APIC-EM と IWAN 非対応ネットワークとの間の相互運用性

APIC-EM によって管理される IWAN 対応ブランチ サイトが IWAN 非対応ネットワークとの間をフローするトラフィックを処理する場合、IWAN アプリを使用して、IWAN 非対応ネットワークをデバイスのエンタープライズプレフィックスリストとして手動で構成します。これがなければ、IWAN アプリはブランチ サイトでデバイスをプロビジョニングできない可能性があります。IWAN 非対応ネットワークをエンタープライズプレフィックスリストとして追加するには、LAN ブラウンフィールドプールとしてグローバルアドレスプールを作成する、または DC プレフィックスリストを追加するという2つの方法があります。

LAN ブラウンフィールドプールの追加

手順

-
- 手順 1 IWAN アプリのホームページで、[Configure Hub Site & Settings] をクリックします。
 - 手順 2 [IP Address Pools] タブを開きます。
 - 手順 3 [Global Address Pool] 領域で、[Add Address Pool] ボタンをクリックします。[Global Address Pool] テーブルに新しい行が追加されます。
 - 手順 4 [IP Pool Role] 列で、アドレス プールを定義するための新しい行で、[LAN Brownfield] を選択します。
 - 手順 5 新しい行で、IWAN 非対応ネットワークのネットワーク IP アドレスとマスクを入力します。
-

DC プレフィックスリストの追加

手順

-
- 手順 1 IWAN アプリのホームページで、[Configure Hub Site & Settings] をクリックします。
 - 手順 2 [IWAN Aggregation Site] タブが開きます。
 - 手順 3 ハブのアイコンをクリックします。[LAN Routing] ダイアログボックスが開きます。
 - 手順 4 [LAN Routing] ダイアログボックスで、[Add DCIP/Mask] をクリックし、IWAN 非対応ネットワークのサブネット IP とマスクを入力します。プラス記号(+)をクリックして、入力を完了します。
 - 手順 5 [LAN Routing] ダイアログボックスで、[Save] をクリックします。
-