CHAPTER 4

Managing Hub Sites

This chapter contains the following sections:

Basic Workflow for Configuring and Setting Up the Hub Site

Use the wizard provided with the Cisco IWAN application (IWAN app) to configure and set up the hub site.

Table 4-1 Basic Workflow for Configuring and Setting Up the Hub Site

No.	Task	Reference
1	Configure system settings.	Wizard Step 1—Configuring System Settings, page 4-2
2	Upload certified Cisco IOS software images. **Note** This wizard step is displayed for greenfield branch devices only.	Wizard Step 2—Uploading Certified Cisco IOS Software Images, page 4-5
3	Configure IP address pools.	Wizard Step 3—Configuring IP Address Pools, page 4-6
4	Configure service providers.	Wizard Step 4—Configuring Service Providers, page 4-9
5	Configure the IWAN aggregation site.	Wizard Step 5—Configuring the IWAN Aggregation Site, page 4-12

Wizard Step 1—Configuring System Settings

Use this procedure to configure system settings such as Netflow Collector, DNS, AAA, Syslog, SNMP, and DHCP.

All of the system settings might not be displayed. Click the **Show More** or **Show Less** button as needed to display or hide the settings.

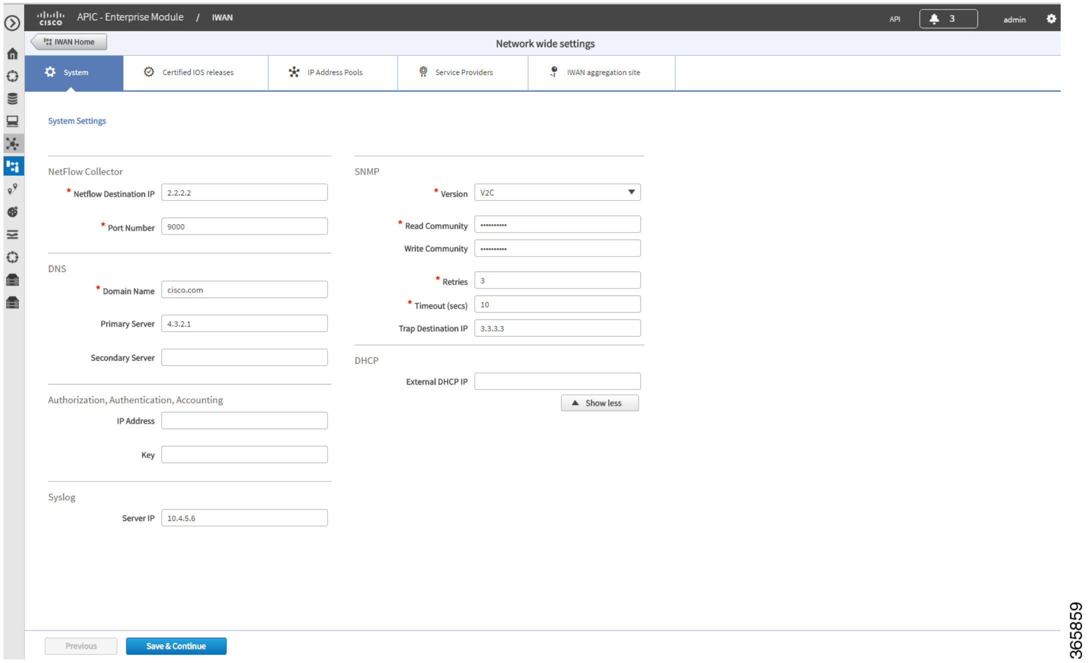
Procedure

Step 1 If you are logging in for first time, you are directed to specify the global settings in the CLI Credentials dialog box. Enter your user name and password, and then click **Add**.

Step 2 From the left navigation pane, click **IWAN**. The Cisco IWAN home page opens.

Step 3 From the Cisco IWAN home page, click **Configure Hub Site & Settings**. The Settings tab opens by default and the System Settings page displays as shown in the following figure:

Figure 4-1 Systems Settings Tab



NetFlow Collector

* Netflow Destination IP: 2.2.2.2

* Port Number: 9000

DNS

* Domain Name: cisco.com

Primary Server: 4.3.2.1

Secondary Server:

Authorization, Authentication, Accounting

IP Address:

Key:

Syslog

Server IP: 10.4.5.6

SNMP

* Version: V2C

* Read Community: ••••••••••

Write Community: ••••••••••

* Retries: 3

* Timeout (secs): 10

Trap Destination IP: 3.3.3.3

DHCP

External DHCP IP:

Step 4 In the **Netflow Collector** area, enter the following properties:

Field	Description
NetFlow Destination IP	IP address of the NetFlow collector (server). Traffic stats are sent from the network devices to the NetFlow collector.
Port Number	Port number of the NetFlow collector (server).

Step 5 In the **DNS** area, enter the following properties:

Field	Description
Domain name	DNS domain name.
Primary Server	(Optional) IP address of the primary DNS server.
Secondary Server	(Optional) IP address of the secondary DNS server.

Step 6 In the **Authorization, Authentication, Accounting** area, enter the following properties:

Field	Description
IP Address	(Optional) IP address of the Authentication, Authorization, and Accounting (AAA) server. TACACS is the only supported centralized AAA service for Cisco IWAN. When a TACACS server is provided, the devices use TACACS for management access to the spoke devices (SSH & HTTPS). Whether or not TACACS is provided, a local AAA user database is created on the spoke device, which is used when the TACACS server is not available. One of the following default values are used for the local AAA user credentials: • Cisco APIC-EM global credentials. • Username and password specified in the global device credentials for branch routers. • Username and password entered while provisioning the hub.
Key	(Optional) Key for accessing the AAA server.

Step 7 In the **Syslog** area, enter the following:

Field	Description
Server IP	(Optional) Destination IP address of the syslog server. Syslog messages from all routers are sent to this server.

Step 8 In the **SNMP** area, choose the version number in the Version field. Depending on the SNMP version number you choose, V2C or V3, different properties display.

- For SNMP version V2C, enter the following properties:

Field	Description
Version	SNMP software version. Value: V2C.
Read Community	SNMP V2C read community string.
Write Community	(Optional) SNMP V2C write community string.
Retries	Number of retries. Default: 3

Field	Description
Timeout (secs)	Displayed for SNMP V2C only. Timeout period. Default: 10
Trap Destination IP	(Optional) IP address of the SNMP server. **Note** If you do not enter an IP address, the Cisco IWAN app is used as an SNMP server. The APIC-EM controller can serve as the SNMP manager for managed network devices or a separate SNMP server can be specified to handle SNMP traps. SNMP settings determine the inventory from hub and remote site devices and these values are reflected in the configuration.

- For SNMP version V3, enter the following properties:

Field	Description
Version	SNMP software version. Value: V3.
Mode	Choose the mode from the drop-down list. Options are: • Authentication and Encryption • No Authentication and No Encryption • Authentication and No Encryption
Auth. Type	Displayed if you chose Authentication and Encryption; or Authentication and No Encryption in the Mode field. Choose the authentication type from the drop-down list. Options are: • HMAC-SHA • HMAC-MDS
Username	The authentication username.
Auth. Password	Displayed if you chose Authentication and Encryption; or Authentication and No Encryption in the Mode field. The password for the authentication username.
Encryption Type	Displayed if you chose Authentication and Encryption in the Mode field. The encryption username.
Encryption Password	Displayed if you chose Authentication and Encryption in the Mode field. The password for the encryption username.
Retries	Number of retries. Default: 3

Field	Description
Timeout (secs)	Displayed for SNMP V2C only. Timeout period. Default: 10
Trap Destination IP	(Optional) IP address of the SNMP server. **Note** If you do not enter an IP address, the Cisco IWAN app is used as an SNMP server. The APIC-EM controller can serve as the SNMP manager for managed network devices or a separate SNMP server can be specified to handle SNMP traps. SNMP settings determine the inventory from hub and remote site devices and these values are reflected in the configuration.

Step 9 In the **DHCP** area, enter the following properties:

Field	Description
External DHCP IP	(Optional) Destination IP address of the DHCP server. The DHCP server that provides client computers and other TCP/IP-based network devices with valid IP addresses.

Step 10 Click **Save and Continue**. The Certified IOS Releases tab opens. See Wizard Step 2—Uploading Certified Cisco IOS Software Images, page 4-5.

Wizard Step 2—Uploading Certified Cisco IOS Software Images

Note This wizard step is displayed for greenfield branch devices only.

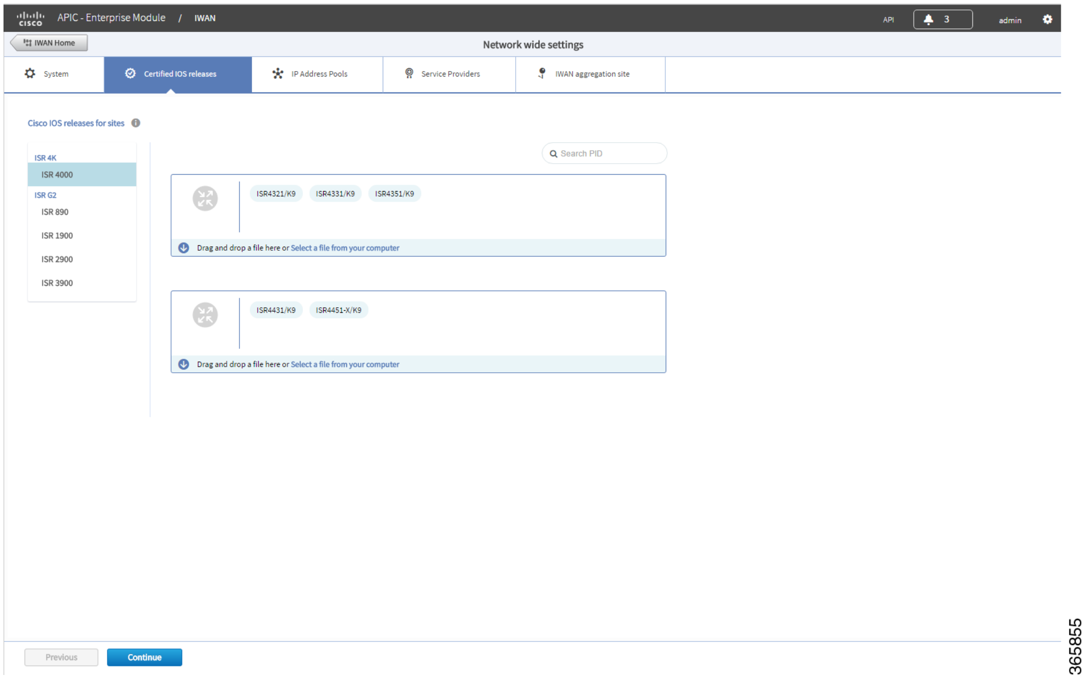
You can upload certified Cisco IOS images from your computer into the Cisco IWAN application. When a greenfield device comes up, the Plug-n-Play agent interacts with the Plug-n-Play server in Cisco APIC-EM, downloads the appropriate Cisco IOS software image to the device, and reloads the device with that image.

Note If the appropriate software image is already installed on your router, you can skip this step.

Procedure

Step 1 Click the **Certified IOS Releases** tab. The Cisco IOS Releases for Sites page opens as shown in the following figure:

Figure 4-2 Certified IOS Releases Tab



Step 2 From the left pane, choose the router type for which you want to upload the Cisco IOS image.

Step 3 Do one of the following:

- Drag and drop the Cisco IOS software image file from your computer into the GUI.
- Browse to the location where you have saved the Cisco IOS software image file and upload it into the system.

Step 4 Click **Continue**. The IP Address Pools page opens. See Wizard Step 3—Configuring IP Address Pools, page 4-6.

Wizard Step 3—Configuring IP Address Pools

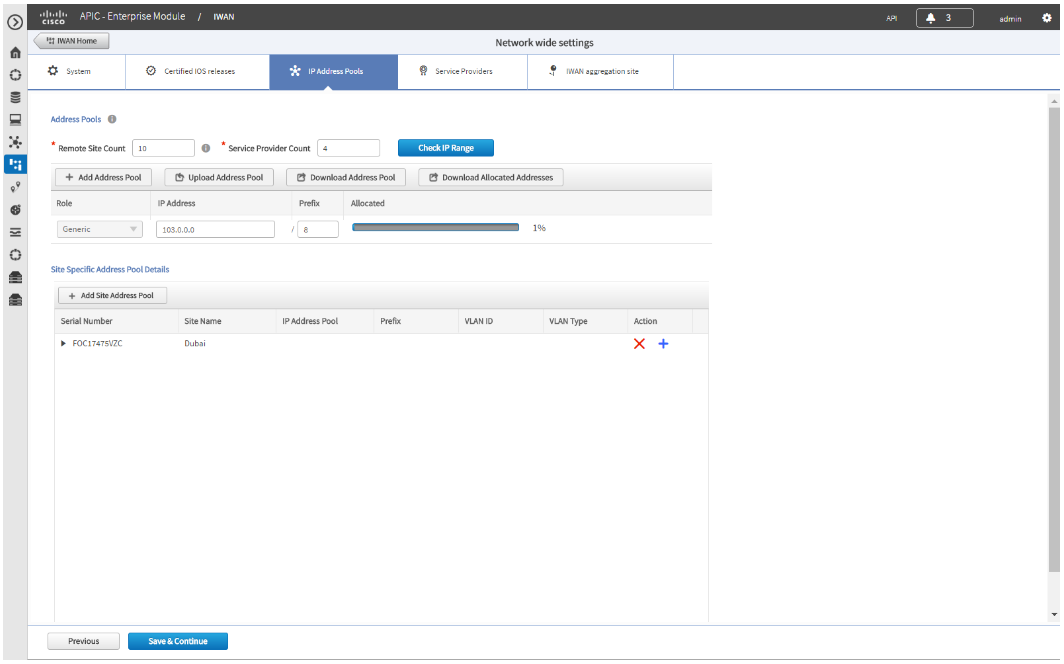
Note The generic IP address pool is used for overlay and loopback addresses. The generic IP address pool is divided according to the number of remote sites and service providers as you specify in the IP Address Pools tab. Plan by understanding your future requirements and specify the maximum number of service providers and remote sites that you might choose to deploy. Once the IP address pool settings are specified, they cannot be changed.

Use the IP Address Pools tab to define IP address pools. For information about IP Address Pools, see Understanding IP Address Pools, page 4-21.

Procedure

Step 1 Choose the **IP Address Pools** tab. The Address Pools page opens as shown in the following figure:

Figure 4-3 IP Address Pools Tab



* Remote Site Count: 10
* Service Provider Count: 4

Role	IP Address	Prefix	Allocated
Generic	103.0.0.0	/ 8	1%

Serial Number	Site Name	IP Address Pool	Prefix	VLAN ID	VLAN Type	Action
FOC17475VZC	Dubai					✕ +

Step 2 In the **Remote Site Count field**, enter the maximum number of remote sites to deploy.

If you are an existing customer with Cisco IWAN release 1.2.x, you can increase the remote site count by upgrading to Cisco IWAN release 1.3.x. Based on the availability of internal IP addresses in pre-reserved subnets (which are created during initial provisioning) you can specify a higher number of remote site count.

Step 3 In the **Service Provider Count** field, enter the maximum number of service providers that you might require.

If you are an existing customer with Cisco IWAN release 1.2.x, you can increase the service provider count by upgrading to Cisco IWAN release 1.3.x. You can specify a maximum of four service providers.

Step 4 Click the **Check IP Range** button. The Proposed IP Range page opens.

Based on the number of remote site and service provider count that you entered, the Proposed IP Range page provides information about the minimum suggested prefix length that you can use for the generic IP address pool, the prefix length for LAN interface pools, the number of IP addresses per VLAN, and the number of VLANs. Click **OK** or **Get IP Range**.

Step 5 Do one of the following:

- To manually enter an IP address, click **+ Add Address Pool**. Enter the following properties:

Field	Description
Role	Can be one of the following: • **Generic**—The first range always defaults to the generic IP address pool. • **LAN Greenfield**—Choose this option to define the LAN IP address pool for new greenfield branch devices. You can have any number of LAN greenfield IP address pools. • **LAN Brownfield**—Choose this option to define the LAN IP address pool for brownfield branch devices (devices with an existing configuration). You can have any number of LAN brownfield IP address pools.
IP Address	IP Address for the IP address pool.
Prefix	CIDR prefix.
Allocated	Displays the percentage of addresses in the pool that are used.

- To upload a large number of IP addresses, click **Upload Address Pool**, and then upload a .csv file from your computer.

  For details about the type of information that you must include in the .csv file, click the **Download Address Pool** tab. A Controller_Profile_DD-MM-YYYY.csv file is downloaded to your system, which provides the template details.

Step 6 Click **+ Add Site Address Pool** to enter information for the site-specific LAN IP address pool. The Add Site Address Pool dialog box opens. Enter the properties as shown in the table below, and then click **OK**.

By default, greenfield branch sites use IP addresses from the LAN greenfield IP address pool (if there is one) or from the generic IP address pool (if there is no LAN greenfield IP address pool). If you want to provision a new greenfield branch site using specific IP address pools for its VLANs (for example, if you do not want the VLANs to use IP addresses from LAN greenfield IP address pools and generic IP address pools), you can define the VLANs and respective IP address pools before you provision the site.

Note After a site is provisioned, you cannot move back-and-forth between site-specific IP address pool with VLANs and site-specific IP address pool without VLANs. Therefore, make sure that you have a clear vision before you start provisioning the site.

Field	Description
Serial Number	Serial number(s) of the site device(s). If a site has more than one device, include all serial numbers separated by a semi-colon.
Site Name	Name of the site.
IP Address Pool	IP address pool to be used for hosts in this VLAN.
Prefix	CIDR prefix.

VLAN ID	Range of values: 1–4094. **Note** The VLAN ID 99 is reserved for the transit VLAN, therefore you cannot use this ID for other VLANs.
VLAN Type	Enter a VLAN type or select it from the drop-down list. Values: Data, Guest, Voice and Video, Wireless. **Note** The following restrictions apply when you enter a VLAN type of your choice: – The VLAN type value should not be more than 200 characters in length. – The VLAN type should not include the ? character. – For site-specific address pools, you can enter a maximum of 20 entries per site.

Step 7 Repeat step 6 as required to add additional site address pools.

Step 8 Click **Save and Continue**. The Service Providers tab opens. See Wizard Step 4—Configuring Service Providers, page 4-9.

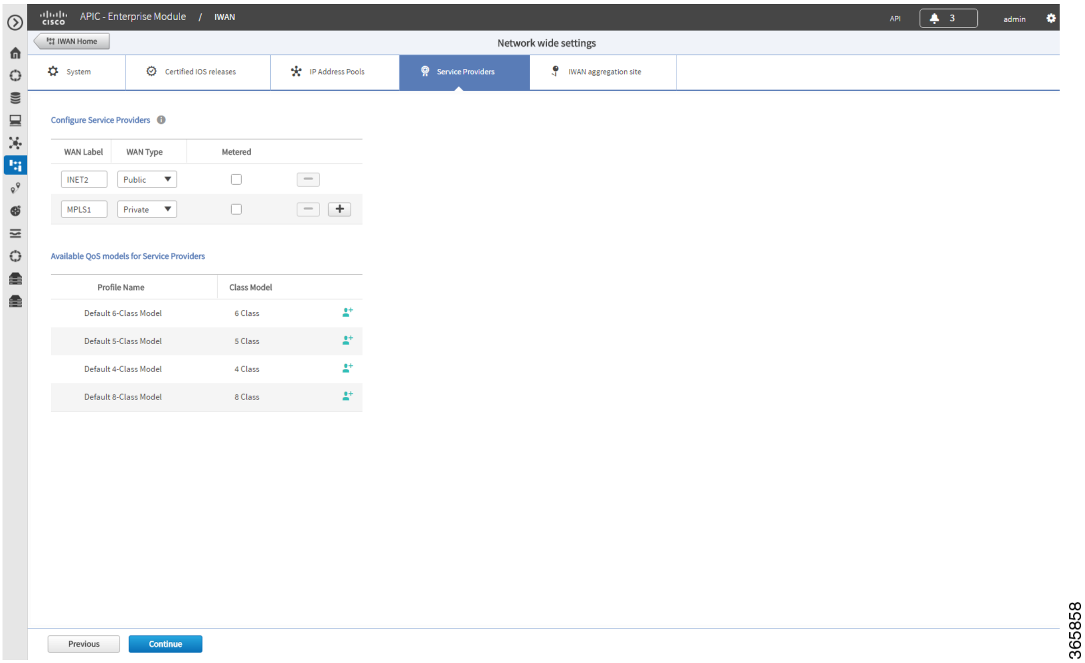
Wizard Step 4—Configuring Service Providers

Use the Service Providers tab to define the type of links and the number of service providers.

Procedure

Step 1 Choose the **Service Providers** tab. The Configure Service Providers Page opens as shown in the following figure:

Figure 4-4 Service Providers Tab



WAN Label	WAN Type	Metered
INET2	Public	□
MPLS1	Private	□

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

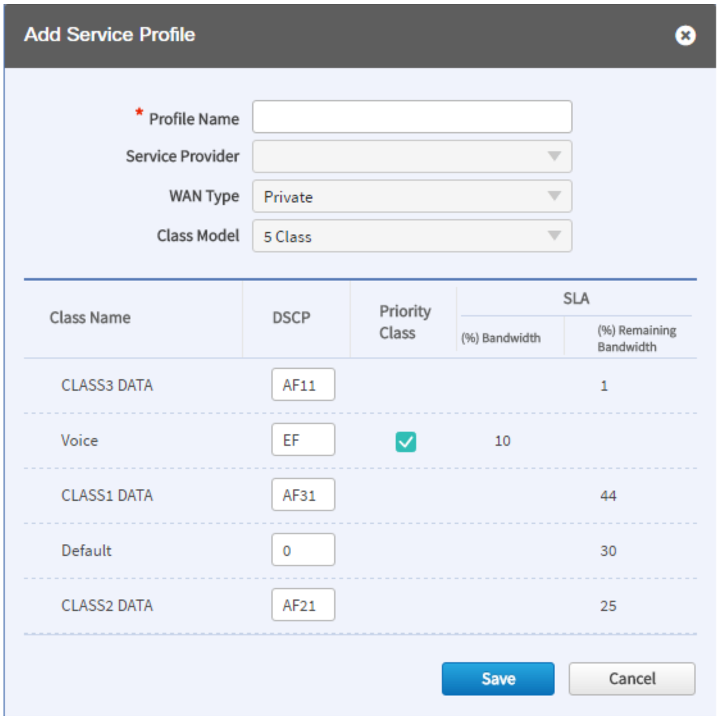
Step 2 From the **Configure Service Providers** area, click the **+** icon to define the following properties:

Note You can specify a maximum of four service providers.

Field	Description
WAN Label	WAN transport type. Can be a maximum of seven characters.
WAN Type	Can be one of the following: • Private • Public
Metered	Choose this option if the WAN is metered. **Note** You can choose the Metered option only when the number of service providers is greater than two. You cannot choose one of the link as a metered link if there are only two service providers. **Note** Only one link can be metered and is permitted on a public cloud.

Step 3 (Optional) If you require a custom class model than the default ones that are provided, click the **Available QoS Models for Service Providers** area, and then click the **+** icon next to the profile that most closely matches the service provider Service Level Agreement (SLA). The Add Service Profile dialog box opens as shown in the following figure:

Figure 4-5 Add Service Profile Dialog Box



Add Service Profile

* Profile Name	
Service Provider	
WAN Type	Private
Class Model	5 Class

Class Name	DSCP	Priority Class	SLA	
			(%) Bandwidth	(%) Remaining Bandwidth
CLASS3 DATA	AF11			1
Voice	EF	☑	10	
CLASS1 DATA	AF31			44
Default	0			30
CLASS2 DATA	AF21			25

Step 4 Enter the following profile information, and then click **Save**.

Note For the Private WAN interface, a set of predefined service provider profiles are available. Egress QoS queuing is applied on the WAN Egress to fulfill the service provider SLA.

Field	Description
Profile Name	Name of the new service profile.
Service Provider	Choose the service provider from the drop-down list.
WAN Type	Choose the WAN Type from the drop-down list. Can be one of the following: • Private • Public

Field	Description
Class Model	Choose the service provider class model from the drop-down list. Options are: • 4 Class • 5 Class • 6 Class • 8 Class
Class Name	Displays the data class name.
DSCP	Displays the Differentiated Services Code Point (DSCP) values for each class. Once saved, it appears as a new profile. You cannot edit this value after it is saved.
Priority Class	Indicates the class that uses the most bandwidth.
SLA	Displays the percentages of used and available bandwidth (based on service level agreement offered by the service provider).

Note After you add the profile information, the profile details appear in the Available QoS Models for Service Providers area.

Step 5 Click **Continue**. The IWAN Aggregation Site tab opens. See Wizard Step 5—Configuring the IWAN Aggregation Site, page 4-12.

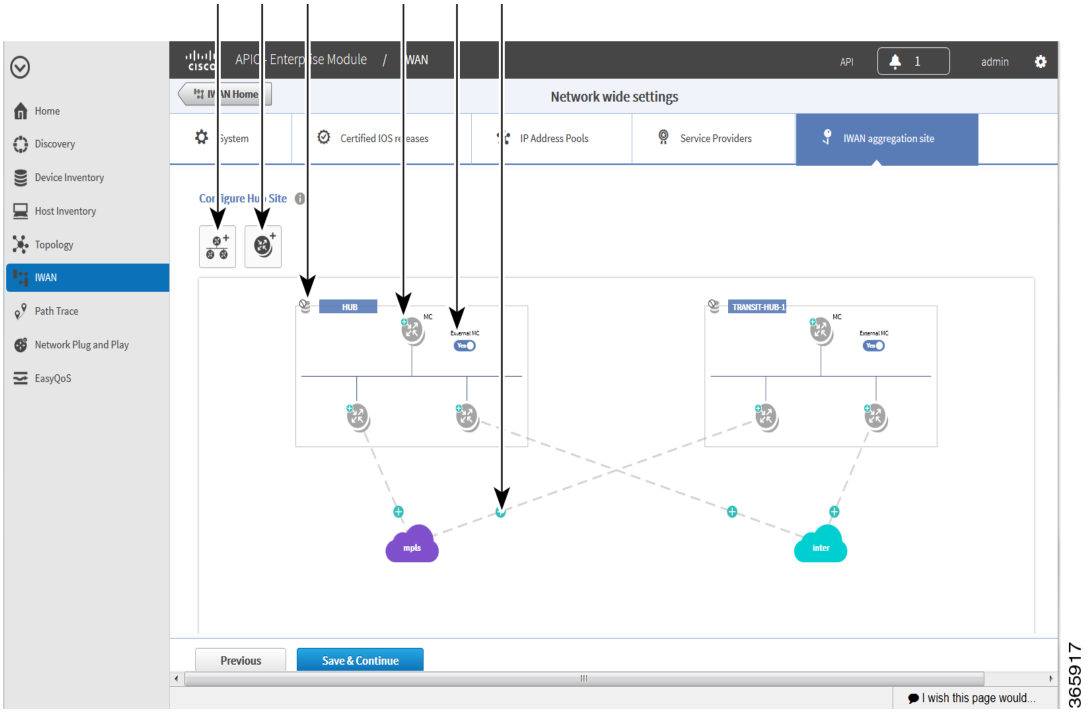
Wizard Step 5—Configuring the IWAN Aggregation Site

Use this procedure to do the following:

1. Discover hub devices.
2. Configure LANs.
3. Configure WANs.
4. Configure the external master controller.

Refer to the following figure to understand the procedure that follows:

Figure 4-6 IWAN Aggregation Site Tab



1	Add POP Icon	**4**	Configure External MC Router + Icon
2	Add Border Router Icon	**5**	External MC Toggle Button
3	Configure LAN Icon	**6**	Configure WAN Link + Icon

Procedure

Step 1 Discover hub devices. Do the following:

a. Select the **IWAN Aggregation Site** tab. The Configure Hub Site page opens and displays all of the service providers that you defined in wizard step 4 and the respective hub border routers.

b. Do one of the following:

– (Recommended) Click the **External MC** button (see # 5 in Figure 4-6) to toggle to **Yes**. A new router is added as a standalone master controller (MC).

– Click the **External MC** button to toggle to **No**. One of the border routers is designated as an MC.

c. To add an additional hub, click the **Add POP** icon ((see # 1 in Figure 4-6). A transit hub is added next to the primary hub (see TRANSIT-HUB-1 in the above figure).

Note You can specify a maximum of two hub sites during provisioning. You can add or delete routers after hub provisioning.

d. (Optional) To rename the new TRANSIT-HUB-1 to another name, click the name of the hub, and then add a different name.

Note You can only change the name of the hub during initial configuration, before routers are added to it.

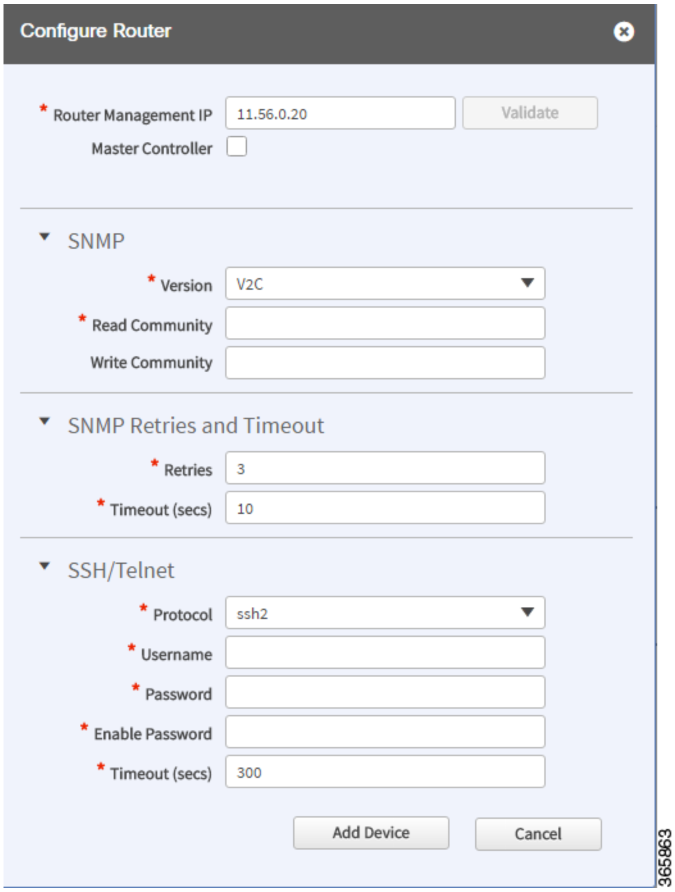
e. To add a border router to a hub, hover over the **Add Border Router** icon (see # 2 in Figure 4-6) the **Add to POP** options appear. Choose one of the two available hubs. A new border router is added in the appropriate hub.

Note You can have a maximum of four border routers in a hub site.

f. To configure the newly added border router, click on the **+** icon on top of the router, the Configure Router dialog box opens.

g. From the Configure Router dialog box, do the following:

- In the **Router Management IP** field, enter the management IP address of the hub router.
- Click **Validate**. The Configure Router dialog box opens again with additional fields as shown in the following figure:



Configure Router

* Router Management IP: 11.56.0.20 [Validate]

Master Controller □

SNMP

* Version: V2C

* Read Community:

Write Community:

SNMP Retries and Timeout

* Retries: 3

* Timeout (secs): 10

SSH/Telnet

* Protocol: ssh2

* Username:

* Password:

* Enable Password:

* Timeout (secs): 300

[Add Device] [Cancel]

Field	Description
Router Management IP	Hub router management IP address.
Master Controller	Check this option to choose this device as the Master Controller.
SNMP	
Version	SNMP version number. Depending on the version number you choose, different properties display.
Read Community (Displayed if you chose SNMP V2C.)	SNMP V2C read community string.
Write Community (Displayed if you chose SNMP V2C.)	(Optional) SNMP V2C write community string.
Mode (Displayed if you chose SNMP V3.)	Choose the mode from the drop-down list. Options are: • Authentication and Encryption • No Authentication and No Encryption • Authentication and No Encryption
Auth. Type (Displayed if you chose SNMP V3.)	Displayed if you chose Authentication and Encryption; or Authentication and No Encryption in the Mode field. Choose the authentication type from the drop-down list. Options are: • HMAC-SHA • HMAC-MDS
Username (Displayed if you chose SNMP V3.)	Displayed if you chose SNMP V3. The authentication username.
Auth. Password (Displayed if you chose SNMP V3.)	Displayed if you chose Authentication and Encryption; or Authentication and No Encryption in the Mode field. The password for the authentication username.
Encryption Type (Displayed if you chose SNMP V3.)	Displayed if you chose Authentication and Encryption in the Mode field. The encryption username.
Encryption Password (Displayed if you chose SNMP V3.)	Displayed if you chose Authentication and Encryption in the Mode field. The password for the encryption username.
SNMP Retries and Timeout	
Retries	Number of SNMP retries. Default: 3

Field	Description
Timeout (secs)	Number of seconds to wait before the system considers an SNMP request to have timed out. Default: 10
SSH/Telnet	
Protocol	Protocol used to communicate to the host (SSH or Telnet).
Username	SSH or Telnet username.
Password	SSH or Telnet password.
Enable Password	Enable password for the username.
Timeout (secs)	Number of seconds to wait before the system considers an SSH or Telnet request to have timed out.

- Enter the properties as shown in the table above.

Note These credentials can be entered only once. The values are automatically populated to the remaining hub devices in the system.

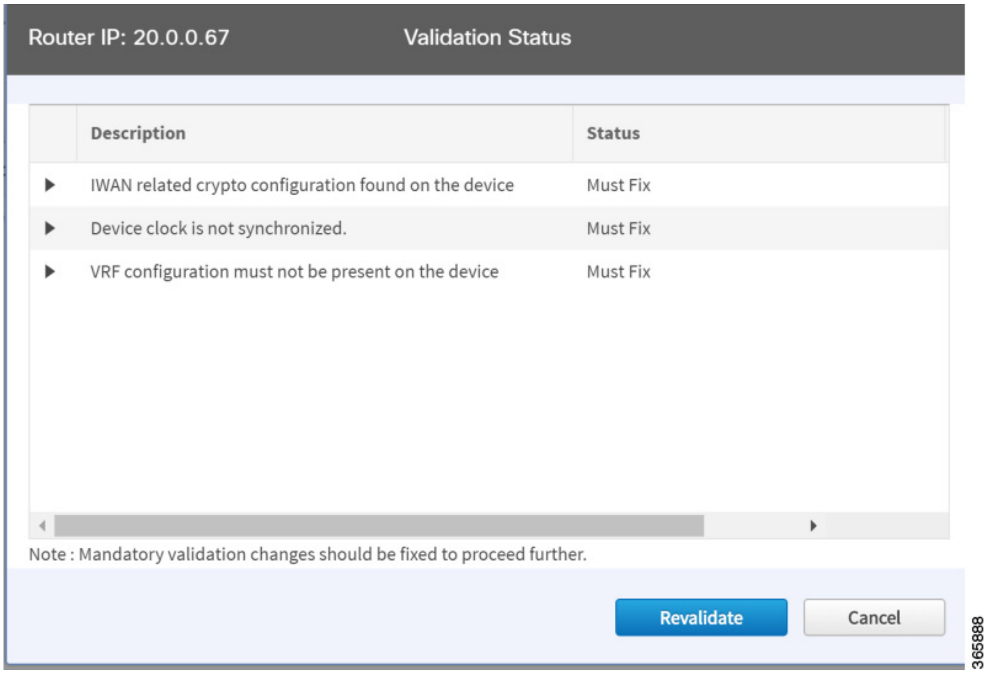
- Click **Add Device**.

The device is verified in the background to determine if the device is suitable for provisioning. The following occurs:

The Cisco IWAN app accesses the router and checks its configuration to determine if it has any configuration that might conflict with the Cisco IWAN app. This is called Brownfield Validation.

If the router does not have conflicting configurations, an orange icon appears on top of the device and the Configure Router Dialog opens.

If the router has conflicting configurations, the Validation Status dialog opens listing all the validation failures, as shown in the following figure:



Router IP: 20.0.0.67 Validation Status

	Description	Status
▶	IWAN related crypto configuration found on the device	Must Fix
▶	Device clock is not synchronized.	Must Fix
▶	VRF configuration must not be present on the device	Must Fix

Note : Mandatory validation changes should be fixed to proceed further.

h. The validation status could be either Warning or Must Fix. Do the following:

- If the validation status is Warning, you can fix it or ignore it.
- If the validation status is Must Fix, remove the configurations suggested by the description, and then click **Revalidate**.

For information about the messages displayed in the Validation Status dialog box, see Appendix A, "Brownfield Validation Messages."

After the router is successfully validated (it does not have any Must Fix errors), the Configure Router dialog box opens.

i. From the Configure Router dialog box, select the appropriate **LAN IP-Interface** check box(es), and then click **Save**.

Note You can choose more than one LAN IP-Interface.

j. To connect the border router to the cloud, click on the router and drag it to the cloud.

k. Configure the other border routers using the above steps.

Step 2 Configure LANs. Do the following:

a. Click the icon on the top-left corner of the primary hub (see # 3 in Figure 4-6). The Configure LAN dialog box opens with the fields shown in the table below:

The Routing Protocol, AS Number, and Datacenter Prefix are collected from the devices and auto populated for ease of configuration. The common (matching) AS numbers between the devices are displayed for each routing protocol. You can change the AS numbers on the device, but we do not recommend it.

Field	Description
Routing Protocol	Default routing protocol running on the hub routers. Example: EIGRP, OSPF, BGP
AS Number	AS number or area number, depending on the routing protocol. **Note** If the LAN routing protocol is BGP, and there are no matching AS numbers from the other hub device, this field is grayed out. You must manually modify the LAN side routing in the device. **Note** BGP with different AS numbers is not supported.
Datacenter Prefix	IP addresses of the hub site, specified as a prefix.

b. Click **Save**.

Step 3 Configure WANs. Do the following:

a. Click the **+** icon on the link that connects the router and the cloud (see # 6 in Figure 4-6). The Configure Link dialog box opens.

The dialog boxes that appear depend on the WAN type that you specified while configuring the Service Provider—for example, Private or Public.

b. (For **Private** WAN) The Configure Link dialog box opens. Enter the following information for each link in the network:

Table 4-2 Configure Link Dialog Box—Private WAN

Field	Description
WAN IP-Address	IP address of the WAN interface.
Default Gateway	IP address of the default gateway.
Enable Non IWAN Sites	Check this option to enable communication between non-IWAN sites and the newly enabled IWAN POP (Hub) and spoke sites for staged migration of the network. See Understanding the Coexistence of IWAN Sites and Non-IWAN Sites, page 4-19.
Loopback IP-Interface	Choose a pre-provisioned loopback IP address from the drop-down list. This enables Cisco IWAN application to form a route between the existing sites and the new IWAN sites. **Note** The loopback interface must be configured on a private (MPLS) router. The loopback interface is required to support coexistence between the IWAN and non-IWAN sites and must be configured before adding the device to Cisco APIC-EM. It is recommended that you specify a loopback IP address in the same subnet as the WAN interface.
Bandwidth (Mbps)	Symmetrical bandwidth for upload and download.
Service Profile	Profile name configured in the Service Providers tab.

c. (For **Public** WAN) The Configure Link dialog box opens. Enter the following information for each link in the network:

Table 4-3 Configure Link Dialog Box—Public WAN

Field	Description
WAN IP-Address	IP address of the WAN interface.
Default Gateway	IP address of the default gateway.
NAT Enabled	Check this option if NAT IP address is used.
NAT IP Address	NAT'd IP address.
Bandwidth (Mbps)	Symmetrical bandwidth for upload and download.
Service Profile	Profile name configured in the Service Providers tab.

d. Click **Save**.

Step 4 Configure the external master controller.

During initial hub and router setup, if you clicked the **External MC** button to toggle to **Yes**, a new router was added as a standalone MC. Do the following:

a. Click the **+** icon on top of the External MC router (see # 4 in Figure 4-6). The Configure Router dialog box opens.

For a dedicated master controller, the device must be greenfield validated. No conflicting configuration with IWAN or dynamic routing protocols are supported for LAN and WAN.

b. In the **Router Management IP** field, enter the management IP address of the hub router.

c. Click **Validate**. The Configure Router dialog box opens.

d. Enter the Router Management IP address, SNMP, SSH or Telnet protocol information, and then click **Save**.

Modifying the Configuration for the Hub Sites

After you have completed all of the wizard steps in the Hub Site and Settings area, you can go back and modify the properties at a later time. Fields that are grayed out, cannot be modified.

Understanding the Coexistence of IWAN Sites and Non-IWAN Sites

The coexistence of IWAN and non-IWAN sites feature allows communication between the newly enabled IWAN POP (Hub) and spoke sites and the non-IWAN sites for staged migration of the network. The benefit of this feature is:

- You can deploy Cisco IWAN on a few sites prior to full scale deployment.
- Non-IWAN sites can continue to communicate with the hub and spoke routers that are IWAN enabled and vice-versa

Prerequisites for Enabling Support of Non-IWAN Sites Along With IWAN Solution

The following configurations must be completed before starting the Cisco IWAN app on APIC-EM workflows:

- Define the Cisco IWAN hub private (MPLS) border router.
- On the hub router:
  - A loopback interface must be enabled on the border router. It is recommended that you specify a loopback IP address in the same subnet as the WAN interface.
  - A static route must be added with the existing MPLS-CE as the default gateway (before provisioning the hub with Cisco IWAN application workflows).
- On the existing MPLS-CE router:
  - The loopback IP address on the IWAN MPLS border router must be advertised through BGP (or another routing protocol used for peering with MPLS provider) on the MPLS-CE router. The loopback IP must be reachable from all remote sites.

Effective with Cisco IWAN Release 1.1.0, you can have two hubs, two clouds and add more devices to the cloud, thereby enabling a multilink network. In other words, a multilink network can have two datacenters and each datacenter can have four devices with four links.

Example of a Heterogeneous WAN Site

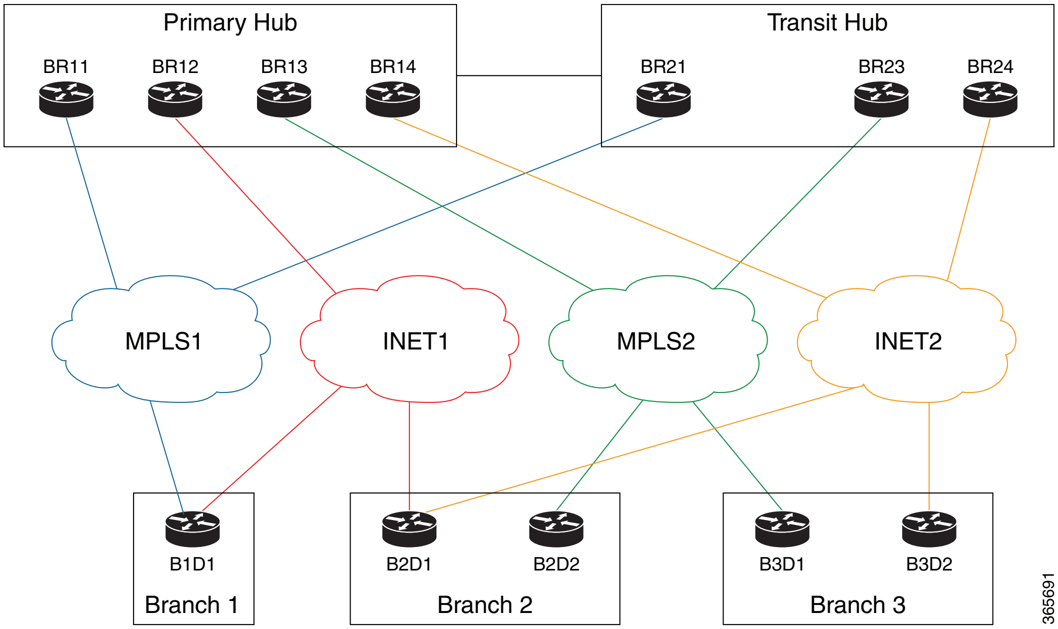
Effective with Cisco IWAN Release 2.0, you can perform the following for a provisioned site:

- Add WAN clouds and service providers.
- Add a maximum of two links of any type (Private or Public). The new links do not affect the existing device priority nor do they change the path preference.
- Connect different hub sites to different service providers (the maximum number of service providers is four).

Note You cannot perform the above changes during site provisioning.

See the following figure for an example of heterogeneous topology where the primary hub is connected to four service providers and the transit hub is connected to three service providers. This example shows that both hub sites do not need to have exactly the same number of service providers.

Figure 4-7 Transit Hub Connected to MPLS Link



Understanding IP Address Pools

The Cisco IWAN application automatically uses the IP addresses carved from the global enterprise IP address pool space. To support this functionality, one generic global IP address pool must be defined for the Cisco IWAN application. IP addresses are allocated from the generic IP address pool to provision the hub and spoke devices, which include interface, LAN, VPN overlay, and routing IP addresses.

Optionally, one or more LAN greenfield IP address pools can be defined to further refine the branch LAN side IP address space. If all LAN greenfield IP address pools are exhausted, the generic IP address pool is used.

It is important to define the size of the generic IP address pool to cater to the long term needs of the IWAN site. VPN requirements dictate that subnets must be defined and allocated internally before any sites are provisioned. At Cisco IWAN release 1.3, you can increase the site and service provider counts after initial provisioning, but you cannot change the generic IP address pool once specified. Therefore, we recommend that you define the generic IP address pool keeping in mind the future scale of service provider and site sizes. The generic IP address pool is used for overlay and loopback addresses. The generic IP address pool is divided according to the number of remote sites and service providers as specified in the IP Address Pools tab.

Optionally, wherever specific IP addresses are required, site-specific LAN and VLAN requirements can be defined and prioritized over the generic global IP address pools.

Site-Specific Profile

Site-specific profile is optional and is required only for pre-provisioning LAN IP addresses on each site. Pre-provisioning allows you to define a site using the site name and device combination before devices are added to the unclaimed device list. This is accomplished by matching the device serial number with the site name. VLAN definition for each site allows you to specify IP address pool ranges, otherwise, the LAN greenfield IP address pools or the generic IP address pool provides the required LAN IP addresses.

Branch Site-Specific Profile

You can pre-provision specifications for the branch sites. A single or dual router site can be defined using device serial numbers and site name along with VLANs for the site.

For a single router branch, you must specify the serial number of the device. For a dual router branch, you must specify the serial number of both the devices separated by a semi-colon. The Cisco IWAN app automatically matches the site name and device serial numbers and uses the previously defined VLANs and IP address pools. Thus, branch sites are available before the devices are displayed in the site provisioning workflow under unclaimed devices.

Defining the site and VLAN enables you to easily configure the devices when devices are provisioned in the site provisioning workflow. When the devices are claimed and provisioned, the site provisioning workflow does not conflict with the existing site configuration and site name.

You cannot modify the IP address pools after you have saved them.

LAN Brownfield IP Address Pool

In the Cisco IWAN release 1.3, the LAN brownfield role was introduced to define LAN IP addresses for brownfield branch devices.

When a brownfield branch is provisioned, its VLAN subnets are reserved.

If the VLAN subnets are subnets of a LAN brownfield IP address pool, they are reserved from a LAN brownfield IP address pool.

If there are no LAN brownfield subnets for the VLAN subnets, they are reserved as site-specific IP address pools.

The add, delete, and update operations are not allowed on brownfield site-specific IP address pools.