



Deploying IWAN Routers

Cisco Prime Infrastructure 3.1

Job Aid



Copyright Page

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

THIS DOCUMENT IS CONSIDERED CISCO PROPERTY AND COPYRIGHTED AS SUCH. NO PORTION OF COURSE CONTENT OR MATERIALS MAY BE RECORDED, REPRODUCED, DUPLICATED, DISTRIBUTED OR BROADCAST IN ANY MANNER WITHOUT CISCO'S WRITTEN PERMISSION.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Deploying IWAN Routers Job Aid

© Copyright 2017 Cisco Systems, Inc. All rights reserved.

Contents

Basics.....	1
Overview.....	1
Introduction	1
Skills	2
Administrators	2
Terms.....	3
Configuration Templates	3
Spoke Router Branch Router Border Router	4
Parameters Variables	4
Deploying an IWAN Branch Router	5
Use Case Scenario.....	5
Process Overview.....	6
Process Steps	7
Task 1: Identify the Hub Router.....	8
Task 2: Select the Configurations for Deployment	9
Task 3: Select the Router Receiving the Configuration	14
Task 4: Select the Parameter Configuration Method.....	15
Task 5: Configure the Technology or Feature Parameters.....	16
Task 6: Review and Validate the Configuration CLI Code.....	23
Task 7: Schedule the Configuration Deployment Job and Configure Post-Deployment Options.....	24
Task 8: Start the Deployment Job and Validate Deployment	26
IWAN Feature Configuration Templates	31
Customization Overview.....	31
Automated IWAN Traffic Management.....	33
Performance Routing Overview	33
Video Demonstration	35
Deploying an IWAN Branch Router	35
Links.....	36
To Product Information	36
To Training	36
To Contact Us.....	36

Basics

Overview

Introduction

Cisco® Intelligent WAN (IWAN) is a comprehensive set of network traffic-control and security features for Cisco routers.

IWAN-enabled routers dynamically route paths for network traffic based on application, endpoint, and network conditions. This approach helps ensure consistent application performance and user experiences.

Cisco® Prime Infrastructure provides the IWAN enablement service, which is a technology solution that:

- ❖ Transitions among connectivity options, selecting the optimal and most cost effective routes for application traffic.
- ❖ Routes application traffic to optimize caching and performance so applications run faster, which improves the user experience.
- ❖ Provides a VPN overlay and robust encryption techniques that secure connectivity and traffic.

By using the IWAN enablement process, you deploy configurations to hub and branch routers based on their roles on the network. To support this process, Prime Infrastructure provides a series of templates that meet Cisco Validated Design standards. You can configure the templates to meet specific network requirements.

In greenfield deployments, the IWAN enablement process allows you to configure routers or sites collectively and consistently while reducing deployment timelines.

In brownfield deployments, the IWAN enablement process allows you to deploy tailored configuration settings or enable specific technologies on previously deployed devices. For example, [you can customize CVD templates to align to existing network requirements](#), and then apply them in IWAN enablement process for minor configurations adjustments to specific devices.

This job aid introduces you to the IWAN enablement process and the tasks that you perform to deploy hub and branch router configurations.

Skills

Administrators

To perform hub and branch router configuration, you need the following experience.

Proficient

- ❖ Prime Infrastructure navigation and application behaviors

Expert

- ❖ IWAN configuration and deployment concepts
- ❖ Practical IWAN configuration and deployment knowledge
- ❖ IWAN-related terminology, such as hub and spoke topology, router types
- ❖ IWAN technologies and how they affect network operations after deployment
- ❖ IWAN configuration-related CLI code concepts and practical coding knowledge

Terms

Configuration Templates

Configuration templates help automate configuration deployment and, when you are configuring large numbers of devices with the same configuration, help ensure configuration consistency.

Prime Infrastructure provides the following types of templates:

- ❖ **Features and Technologies and CLI templates**
System-provided or user-configured templates that contain the CLI code that configures specific features or on devices.
- ❖ **Composite templates**
System-provided or user-configured templates that support the deployment of a series of templates, each containing code that the device or devices require, in a single task.
- ❖ **Feature templates**
System-provided or user-configured templates that contain Cisco Validated Design specifications, which include the minimum parameters that you need to configure for optimal configuration deployment of a feature or technology.

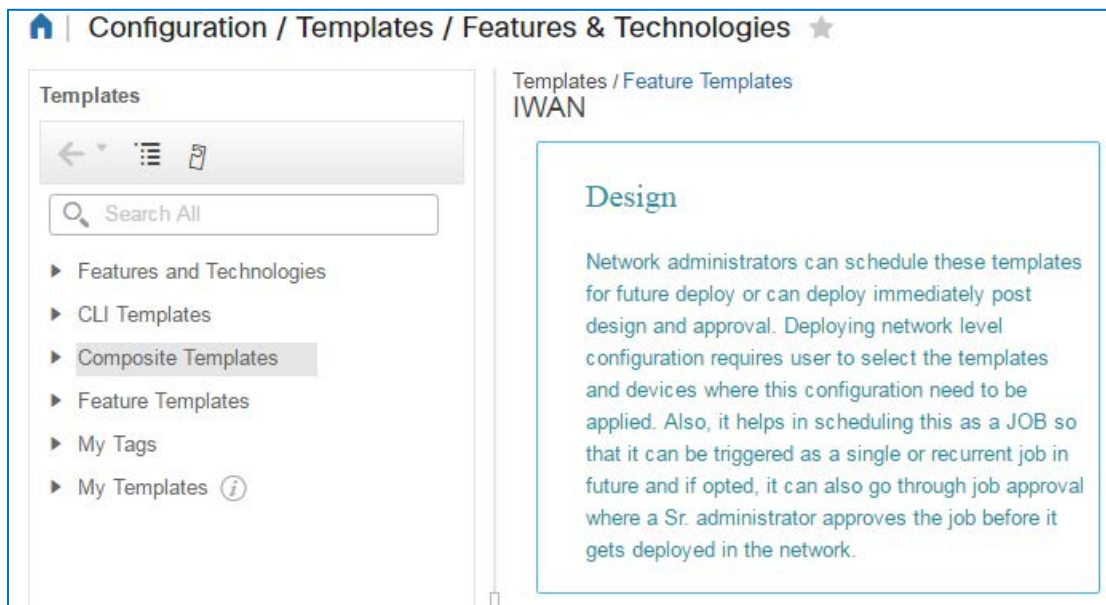


Note: For more information on the Cisco Validated Design program, [visit our Web site](#).

When system users configure new or change system-provided templates, those templates are stored under **My Templates**.



Note: Templates that you configure and save are available to other system users based on their access permissions.



Spoke Router | Branch Router | Border Router

These terms can be used interchangeably.

Parameters | Variables

The application uses the terms parameters and variables interchangeably to refer to the data values that system users apply in device configurations.

This documentation uses the term parameters.

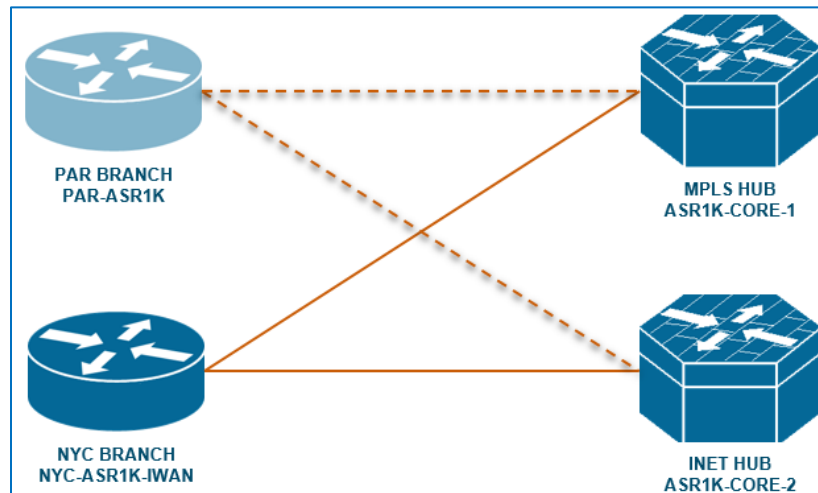
Deploying an IWAN Branch Router

Use Case Scenario

As an administrator, you are managing the deployment of a branch site on the network. The enterprise topology is using a hub and spoke model with a single data center.

You previously deployed and configured the data center hub router (master controller) and the topology includes the company's New York branch office.

You now need to connect the Paris branch to the data center hub router.



At this point, you have deployed the Paris branch's network devices by using the Prime Infrastructure Plug and Play process.



Note: For more information on the Plug and Play process and its associated tasks, [refer to the **Deploying Devices** job aid](#) and the [Bringing the Initial Router at a New Site Online](#) use case video.

Now, you are ready to configure the branch router that supports the connectivity of the remote site to the enterprise WAN and to the data center hub router.

Process Overview

To deploy IWAN configurations to routers:

1. Using the **DM VPNM Monitor Home** page, identify the hub router.
2. Using the IWAN Enablement wizard, select the technology configurations for deployment.
3. Select the branch router that you need to configure.
4. Select the parameter configuration method.
5. Configure the parameters for each technology that you are deploying.
6. Review and validate the CLI code that the system will deploy to the router.
7. Prepare and schedule the configuration deployment to the router.
8. On the **Job Dashboard** page, monitor the deployment process, and then validate the configuration.

Process Steps

The branch router is up and running. Now, it requires configuration of the technologies that will optimize the WAN by providing granular WAN access control, quality of service-based traffic management, application recognition and control, and application-aware automated traffic routing.

To configure technologies, Prime Infrastructure provides Cisco Validated Design (CVD) feature templates that you can select during the configuration process. By selecting these templates, the system populates the required parameters and, when system users configure the templates to support unique requirements, includes the additional custom parameters.



Tip: When you customize CVD feature templates, you can add, remove, or change parameters to align with the network configuration or meet specific operational requirements.

For more information, [refer to the CVD Feature Template Customization topic in this job aid.](#)

In this case, you can use [the CVD templates](#) without changes.



Important Note: Before you begin using the IWAN Enablement wizard, ensure you have access to all of the parameter values that you will need for each feature or technology that you are configuring.

After beginning to configure parameter values in the wizard, you cannot save your changes and return to complete the process later.

To begin, you want to identify the hub to which you want to connect the router. To do so, you navigate to the **DMVPN Monitor Home** page in **Application Visibility & Control** on the **Services** menu.

Services / Application Visibility & Control / DMVPN Monitor Home					
DMVPN Monitor Home					
Total 12					
Show Quick Filter					
Data Center Location	Device Name	Device Type	Device IP	Image Version	Active Spokes
TME-LAB	AMS-ASR1K-INET	Cisco ASR 1002-X Router	10.11.254.2	15.5(3)S2	0
TME-LAB	AMS-ASR1K-MPLS	Cisco ASR 1002-X Router	10.11.1.1	15.5(3)S2	0
SJ-HQ	ASR1K-CORE1	Cisco ASR 1004 Router	10.0.2.2	15.5(3)S2	3
SJ-HQ	ASR1K-CORE2	Cisco ASR 1004 Router	10.0.3.2	15.5(3)S2	4
HUB	INET_Hub.cisco.com	Cisco ASR 1001-X Router	192.168.139.185	15.5(3)S5	1
LOS ANGELES	LA-RTR4331-IWAN	Cisco 4331 Integrated Services Router	10.2.1.1	15.5(3)S2	0
HUB	MPLS_Hub.cisco.com	Cisco ASR 1001-X Router	192.168.139.184	15.5(3)S5	1
NEW YORK	NYC-RTR-INET	Cisco 4451 Series Integrated Services R...	10.16.255.2	15.5(3)S2	0
NEW YORK	NYC-RTR-MPLS	Cisco 4451 Series Integrated Services R...	10.16.1.1	15.5(3)S2	0
Santa Rosa	Router.cisco.com	Cisco 4351 Integrated Services Router	80.0.0.65	15.5(3)S5	0
Santa Rosa	Router.cisco.com	Cisco 4351 Integrated Services Router	80.0.0.66	15.5(3)S5	0

Task 1: Identify the Hub Router

The **DMVPN Monitor Home** page lists each hub router, also referred to as a master controller, in the enterprise topology and the number of branch routers, referred to as active spokes, connected to the hub routers.

Services / Application Visibility & Control / DMVPN Monitor Home

DMVPN Monitor Home Total 12

Show Quick Filter

Data Center Location	Device Name	Device Type	Device IP	Image Version	Active Spokes
TME-LAB	AMS-ASR1K-INET	Cisco ASR 1002-X Router	10.11.254.2	15.5(3)S2	0
TME-LAB	AMS-ASR1K-MPLS	Cisco ASR 1002-X Router	10.11.1.1	15.5(3)S2	0
SJ-HQ	ASR1K-CORE1	Cisco ASR 1004 Router	10.0.2.2	15.5(3)S2	3
SJ-HQ	ASR1K-CORE2	Cisco ASR 1004 Router	10.0.3.2	15.5(3)S2	4
HUB	INET_Hub.cisco.com	Cisco ASR 1001-X Router	192.168.139.185	15.5(3)S5	1
LOS ANGELES	LA-RTR4331-IWAN	Cisco 4331 Integrated Services Router	10.2.1.1	15.5(3)S2	0
HUB	MPLS_Hub.cisco.com	Cisco ASR 1001-X Router	192.168.139.184	15.5(3)S5	1
NEW YORK	NYC-RTR-INET	Cisco 4451 Series Integrated Services R...	10.16.255.2	15.5(3)S2	0
NEW YORK	NYC-RTR-MPLS	Cisco 4451 Series Integrated Services R...	10.16.1.1	15.5(3)S2	0
Santa Rosa	Router.cisco.com	Cisco 4351 Integrated Services Router	80.0.0.65	15.5(3)S5	0
Santa Rosa	Router.cisco.com	Cisco 4351 Integrated Services Router	80.0.0.66	15.5(3)S5	0

To identify the hub router:

1. On the **DMVPN Monitor Home** page, in the list, locate the router.

In this case, each entry for the hub indicates one active branch router.

Services / Application Visibility & Control / DMVPN Monitor Home

DMVPN Monitor Home Total 12

Show Quick Filter

Data Center Location	Device Name	Device Type	Device IP	Image Version	Active Spokes
TME-LAB	AMS-ASR1K-INET	Cisco ASR 1002-X Router	10.11.254.2	15.5(3)S2	0
TME-LAB	AMS-ASR1K-MPLS	Cisco ASR 1002-X Router	10.11.1.1	15.5(3)S2	0
SJ-HQ	ASR1K-CORE1	Cisco ASR 1004 Router	10.0.2.2	15.5(3)S2	3
SJ-HQ	ASR1K-CORE2	Cisco ASR 1004 Router	10.0.3.2	15.5(3)S2	4
HUB	INET_Hub.cisco.com	Cisco ASR 1001-X Router	192.168.139.185	15.5(3)S5	1
LOS ANGELES	LA-RTR4331-IWAN	Cisco 4331 Integrated Services Router	10.2.1.1	15.5(3)S2	0
HUB	MPLS_Hub.cisco.com	Cisco ASR 1001-X Router	192.168.139.184	15.5(3)S5	1

2. To begin the IWAN enablement process, [go to task 2](#).

Task 2: Select the Configurations for Deployment

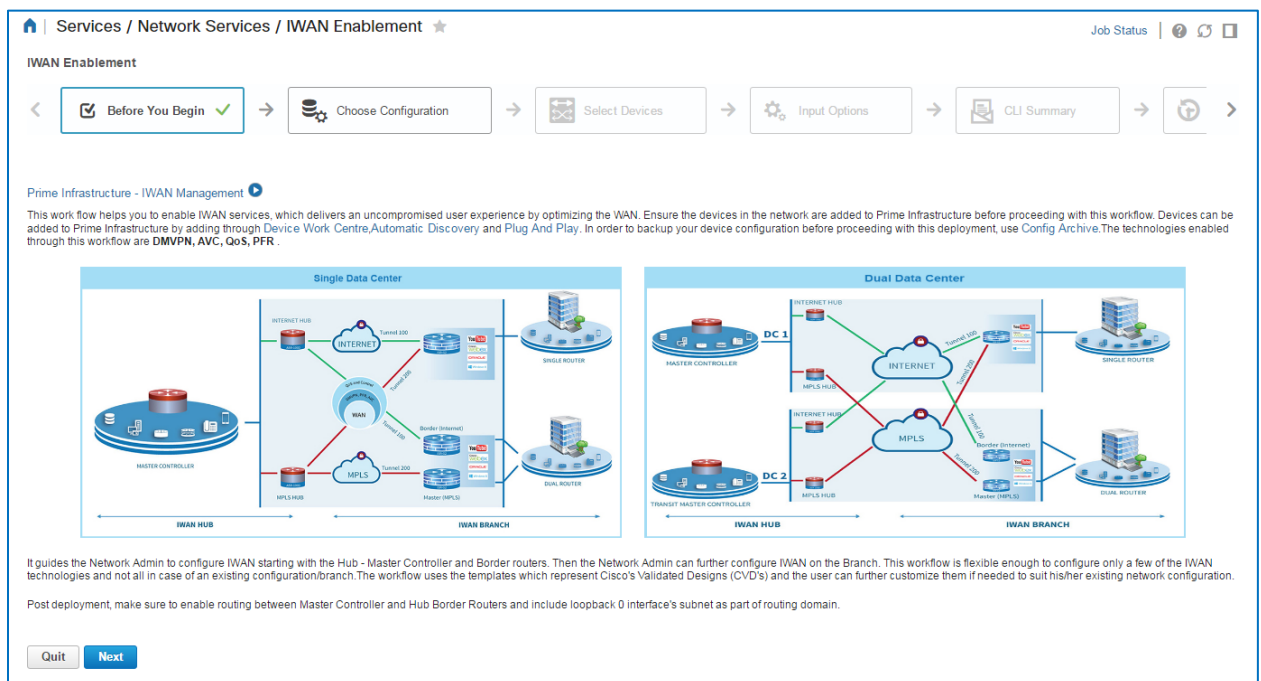
Now that you determined that the hub router can support the Paris branch router, you can configure the branch router by assigning the role that the router will perform in the WAN topology and then indicating the overlay protocol, and the VPN and technology configuration templates that contain the CLI code for router configuration.

Optionally, you also can deploy additional configuration after the device activation process is complete and Prime Infrastructure is managing the device.

In this case, you are deploying a single router on the branch side of the WAN. The single router will have one interface dedicated to managing Internet traffic and a second interface dedicated to managing MPLS traffic.

Based on requirements for the router, you will apply several technologies, and additional configuration after the IWAN configuration is deployed is not necessary.

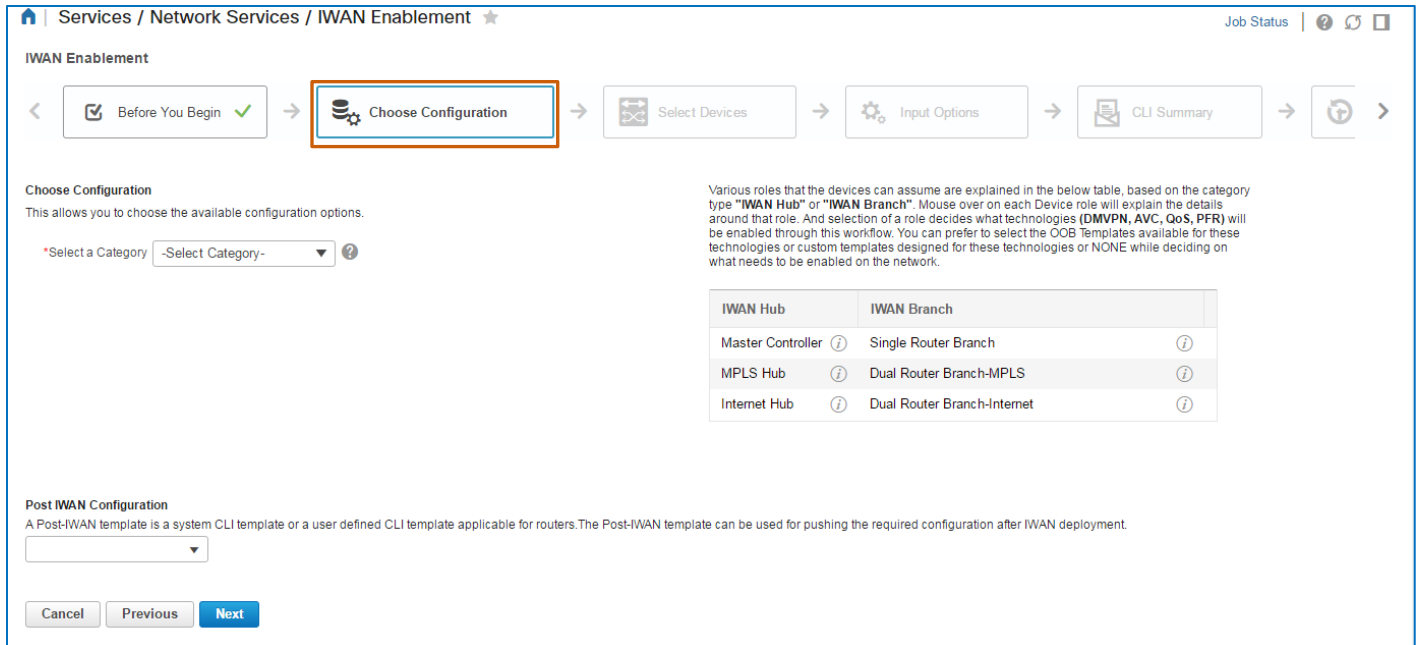
To begin, you navigate to the **IWAN Enablement** page, which provides a wizard to step you through the process.



Based on the use case, to select deployment configurations, follow these steps:

1. On the **IWAN Enablement | Before You Begin** page, click **Next**.

The **Choose Configuration** page opens.



IWAN Enablement

Services / Network Services / IWAN Enablement

Job Status

Before You Begin ✓ → **Choose Configuration** → Select Devices → Input Options → CLI Summary →

Choose Configuration

This allows you to choose the available configuration options.

*Select a Category -Select Category-

Various roles that the devices can assume are explained in the below table, based on the category type "IWAN Hub" or "IWAN Branch". Mouse over on each Device role will explain the details around that role. And selection of a role decides what technologies (DMVPN, AVC, QoS, PFR) will be enabled through this workflow. You can prefer to select the OOB Templates available for these technologies or custom templates designed for these technologies or NONE while deciding on what needs to be enabled on the network.

IWAN Hub	IWAN Branch
Master Controller	Single Router Branch
MPLS Hub	Dual Router Branch-MPLS
Internet Hub	Dual Router Branch-Internet

Post IWAN Configuration

A Post-IWAN template is a system CLI template or a user defined CLI template applicable for routers. The Post-IWAN template can be used for pushing the required configuration after IWAN deployment.

Cancel Previous Next

2. To select the type of router that you are deploying based on the network topology, in the **Select a Category** drop-down list, select whether you are deploying:
 - ❖ A single branch router or dual routers.
 - ❖ A single data center router or dual routers.

The system opens the **Select a Device Role** drop-down list.

Choose Configuration

This allows you to choose the available configuration options.

*Select a Category IWAN Branch

*Select a Device Role -Select Device Role-

- To select the router's function in the WAN topology, in the **Select a Device Role** drop-down list, select the type of router that you need to configure.









Tip: The table on the page provides description of the router roles that you can configure.

To review a role description:

- Point to the information icon beside the role of interest.

Various roles that the devices can assume are explained in the below table, based on the category type "IWAN Hub" or "IWAN Branch". Mouse over on each Device role will explain the details around that role. And selection of a role decides what technologies (DMVPN, AVC, QoS, PFR) will be enabled through this workflow. You can prefer to select the OOB Templates available for these technologies or custom templates designed for these technologies or NONE while deciding on what needs to be enabled on the network.

IWAN Hub		IWAN Branch	
Master Controller		Single Router Branch	
MPLS Hub		Dual Router Branch-MPLS	
Internet Hub		Dual Router Branch-Internet	

The system opens the drop-down lists that you use to select the configuration files.



Note: The options that the system opens vary based on the router category that you select and the role that you assign the router.

The templates that are available in drop-down lists appear based on their configurations and tags.

For more information on tags, [refer to the Cisco® Prime Infrastructure 3.1 User Guide.](#)

Choose Configuration

This allows you to choose the available configuration options.

*Select a Category IWAN Branch

*Select a Device Role Single Router Branch

Overlay Protocol EIGRP

DMVPN CVD-DMVPN-DHCP... ☐ Deploy PKI ☒ DHCP

PFR PfR-TME-Branch-3945

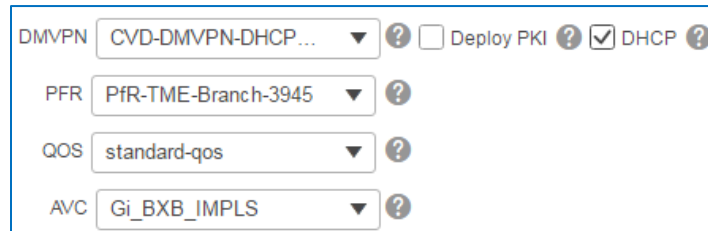
QOS standard-qos

AVC Gi_BXB_IMPLS

DIA-ZBFW CVD-DIA-ZBFW

CWS CVD-CWS-ISR4k

4. To indicate the protocol for the overlay network, in the **Overlay Protocol** drop-down list, select the protocol.
5. To configure applicable technologies, in each technology-related drop-down list, select the features template containing the configuration that the router requires.



DMVPN: CVD-DMVPN-DHCP... ? ☐ Deploy PKI ? ☒ DHCP ?

PFR: PfR-TME-Branch-3945 ?

QOS: standard-qos ?

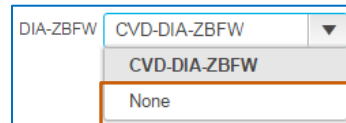
AVC: Gi_BXB_IMPLS ?



Tip: You can configure only those technologies or features that the router requires.

When the router does not require a configuration:

- ❖ In the applicable drop-down list, select **None**.



DIA-ZBFW: CVD-DIA-ZBFW ?

None

- ❖ In WANs that use dynamic multipoint VPN (DM VPN) for data exchanges among branches, to enable the DM VPN technology on the router, in the **DMVPN** drop-down list, select the applicable features template.
 - ◆ To enable the system to use a DHCP server to assign IP addresses to client devices on the network, accept the default selection of the **DHCP** check box.



Note: When you clear the **DHCP** check box, the system automatically refreshes the **DMVPN** drop-down list to select the CVD standard template that does not configure DHCP.

- ◆ To enable the system to use the Public Key Infrastructure to authenticate users logging on to VPN, select the **Deploy PKI** check box.



DMVPN: CVD-DMVPN-Single... ? ☒ Deploy PKI ? ☐ DHCP ?



Important Note: To configure the device for PKI authentication, an APIC-EM controller must be integrated with Prime Infrastructure.

Then, during the enablement process, the controller adds the device to its inventory, which activates the PKI service on the controller.

The PKI service then configures PKI certification on the device.

- ❖ To enable the [Performance Routing \(PfR\) technology, which selects optimal routes for application traffic](#), in the **PFR** drop-down list, select the applicable features template.

- ❖ To enable the Quality of Service (QoS) technology, which classifies network traffic for optimal routing, in the **QOS** drop-down list, select the applicable features template.
 - ❖ To enable the Application Visibility and Control (AVC) technology, which provides application level classification, monitoring, and traffic control on the router, in the **AVC** drop-down list, select the applicable features template.
6. Optionally, in configurations with Cisco IOS routers, to configure a firewall on the router that supports traffic management using security zone-based policies, in the **DIA-ZBFW** drop-down list, select the features template containing the firewall configuration that the router requires.

DIA-ZBFW

CVD-DIA-ZBFW
▼
?

7. Optionally, to configure routing of designated traffic to a Cisco Cloud Web Security (CWS) server for deeper security inspections, in the **CWS** drop-down list, select the features template containing the routing configuration that the router requires.

CWS

CVD-CWS-ISR4k
▼
?

8. Optionally, to deploy any additional configuration after the IWAN configuration process is complete and Prime Infrastructure is managing the device, in the **Post IWAN Configuration** drop-down list, select the feature, technology, or composite template that contains the additional configuration that the router needs to run.
9. To select the router or routers receiving the configuration files, click **Next**, and then, [go to task 3](#).

Choose Configuration

This allows you to choose the available configuration options. Please refer 'Prerequisites for Enabling IWAN Services' section in [Contextual help](#) on how to include user defined templates in the workflow.

*Select a Category IWAN Branch ?

*Select a Device Role Single Router Branch ?

Overlay Protocol EIGRP ?

DMVPN CVD-DMVPN-Single... ? ☒ Deploy PKI ? ☐ DHCP ?

PFR CVD-PfR ?

QOS CVD-QOS ?

AVC None ?

DIA-ZBFW None ?

CWS None ?

Post IWAN Configuration

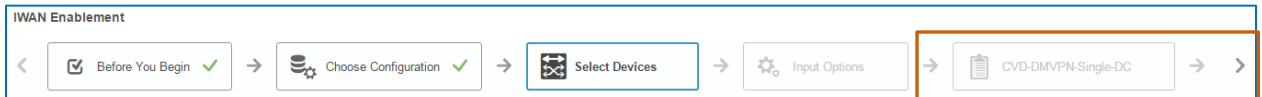
A Post-IWAN template is a system CLI template or a user defined CLI template applicable for routers.

Cancel
Previous
Next

Task 3: Select the Router Receiving the Configuration

When you navigate to the **Select Devices** page, the wizard updates to provide pages on which you configure each of the technologies or features that you selected.

Now, you are ready to select the router or routers to which you are deploying the configuration files.



In this case, you need to deploy the configuration to the Paris branch router.

To select the router or routers that you need to configure, follow these steps:

1. On the **Select Devices** page, in the **Devices** list, in the applicable category, select each router.
2. To indicate the method that you want to use to configure the technology parameters, click **Next**, and then, [go to task 4](#).

Services / Network Services / IWAN Enablement ★

IWAN Enablement

< ☒ Before You Begin ✓ → ☒ Choose Configuration ✓ → **Select Devices** → ☐ Input Options

NOTE: Devices listed in this table are filtered based on the type and IOS version(15.4 onwards) where the IWAN support is available.

Devices

<input type="checkbox"/>	Name	Description	Type	IP Address/DNS	Vendor
<input type="checkbox"/>	▶ All Devices	All Members			
<input checked="" type="checkbox"/>	▼ Device Type	Device Type			
<input checked="" type="checkbox"/>	▼ Routers	Routers			
<input checked="" type="checkbox"/>	▼ Cisco 4300 Series I...	Cisco 4300 Series Integrated S...			
<input type="checkbox"/>	LA-RTR4331-IWAN	LA-RTR4331-IWAN	Routers	10.2.1.1	Cisco
<input checked="" type="checkbox"/>	Router	Router	Routers	40.0.0.10	Cisco
<input type="checkbox"/>	Router.cisco.com	Router.cisco.com	Routers	50.0.0.10	Cisco
<input type="checkbox"/>	▶ Cisco 4400 Series In...	Cisco 4400 Series Integrated S...			
<input type="checkbox"/>	▶ Cisco ASR 1000 Ser...	Cisco ASR 1000 Series Aggre...			
<input type="checkbox"/>	▶ Location	Location based groups			
<input type="checkbox"/>	▶ User Defined	User Defined Device Groups			

Cancel Previous **Next**

Task 4: Select the Parameter Configuration Method

The IWAN Enablement wizard provides the following two methods for configuring technology parameters.

- ❖ The workflow method

When you select this method, you follow the steps in the IWAN wizard to configure technology parameters.

- ❖ The export and import CSV method

When you select this method, you export the technology parameters to a .CSV-formatted file. You manually configure all of the required values, and any optional values, that you need for each technology and router that you are configuring.

The file lists the device IP addresses for configuration in columns and the required and optional technology parameters.



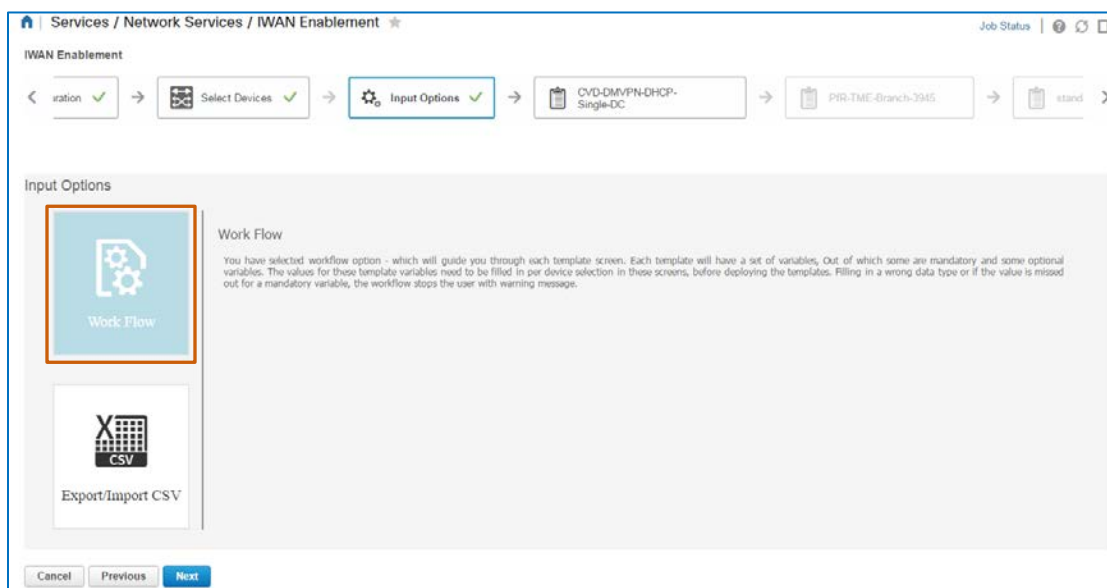
Tip: When managing a large system, the export and import method supports scalability more easily because you can maintain the spreadsheets with parameters locally and then import, as needed.

When completed, you import the configuration parameters by using the IWAN wizard.

To select the parameter configuration method, follow these steps:

1. On the **Input Options** page, click the applicable icon.
2. To configure the technology parameters, click **Next**, and then, [go to task 5](#).

In this case, you are using the workflow method so that you can use the wizard to configure the technology parameters.



Task 5: Configure the Technology or Feature Parameters

The wizard opens the first technology or feature that you need to configure. The workflow will continue to advance as you configure each technology or feature.

In the **Devices** list, the system selects the **All Selected Devices** option by default. This way, you can configure all of the parameters that apply to the devices [that you selected in task 2](#).

Services / Network Services / IWAN Enablement

Job Status

IWAN Enablement

CVD-DMVPN-Single-DC → CVD-PfR → CVD-QoS → CLI Summary → Prepare and Schedule

Values filled for the 'ALL Selected Devices' will be used for each device. Any device specific value will override the value provided in 'ALL Selected Devices'. When 'ALL Selected Devices' option.

Devices

☒ All Selected Devices

☐ Router

Loopback

* Loopback-IP

* Loopback-Subnet-Mask

Internet Tunnel

* Internet-WAN-Bandwidth-KBPS

* Internet-Tunnel-IP

* Internet-Tunnel-Subnet-Mask

* Internet-Tunnel-Subnet

* DC1-Internet-Hub-WAN-IP

* Internet-Hub-Tunnel-IP

* Internet-WAN-Interface

Apply

Cancel Previous Next

Scroll, as needed, to complete all of the required fields and any optional fields that you need.



Important Note: You must configure all of the required fields to continue the process.

You might need to scroll the page to see all of the fields that require an entry.

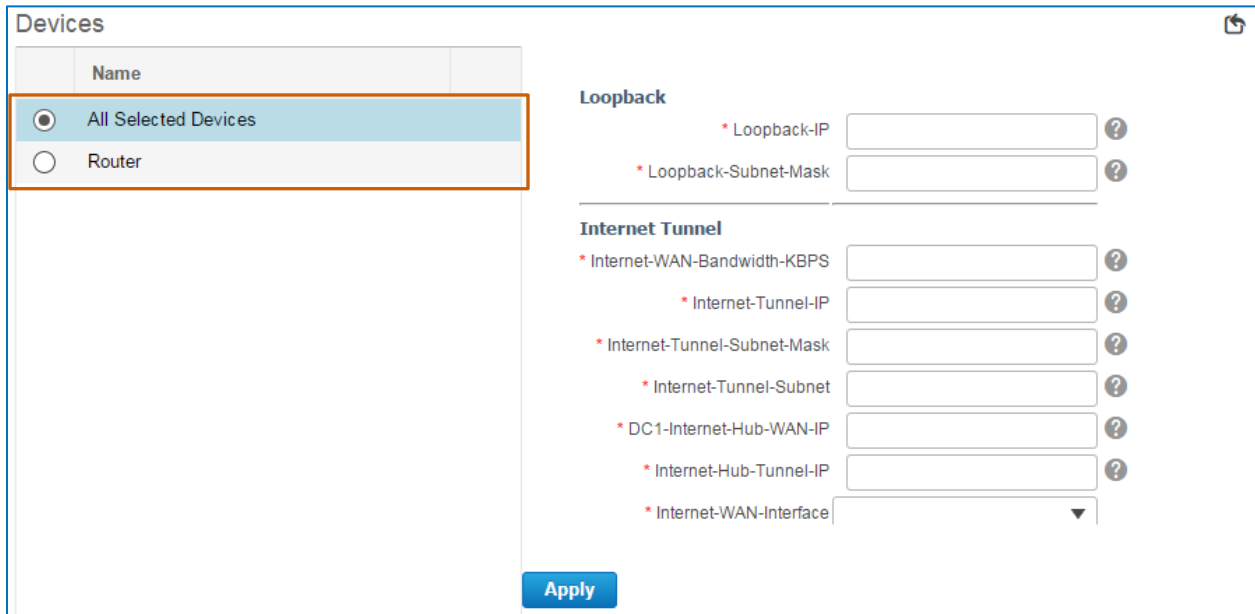
When you are configuring more than one router, you also can configure discrete parameters based on each router's requirements.

For example, by using the default selection of **All Selected Devices**, you can configure all of the common device parameter values for all of the routers that you are configuring.

After applying common parameter values, in the **Devices** list, you can select each individual router, and configure and apply discrete parameter values, as needed.



Important Note: When you apply values to individual routers in the same fields for which you applied global values, those values override the global values that you applied previously.



The screenshot shows the 'Devices' configuration page. On the left, there is a list of devices with two options: 'All Selected Devices' (selected with a radio button and highlighted by an orange box) and 'Router'. To the right, there are configuration fields for 'Loopback' and 'Internet Tunnel'. The 'Loopback' section includes fields for 'Loopback-IP' and 'Loopback-Subnet-Mask'. The 'Internet Tunnel' section includes fields for 'Internet-WAN-Bandwidth-KBPS', 'Internet-Tunnel-IP', 'Internet-Tunnel-Subnet-Mask', 'Internet-Tunnel-Subnet', 'DC1-Internet-Hub-WAN-IP', 'Internet-Hub-Tunnel-IP', and 'Internet-WAN-Interface'. Each field has a question mark icon for help. An 'Apply' button is located at the bottom right of the configuration area.



Tip: When you select an individual router entry, you also can preview the CLI code that the system will generate.

Reviewing and validating the CLI code helps ensure that the router will behave as expected with the configuration that you are deploying.

You can review all of the CLI code that the process will deploy in a later step.

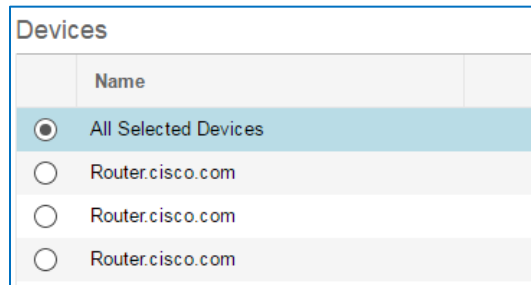


Important Note: Use caution when entering configuration data.

While the system does validate whether the data that you are entering meets formatting requirements, it does not validate whether the data that you are entering will function as expected in the network environment.

To configure the technology parameters, follow these steps:

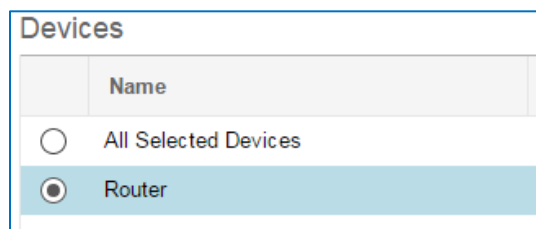
1. On the applicable technology page, in the **Devices** list:
 - ❖ To apply common values to all of the devices that you are configuring, accept the default selection of **All Selected Devices**.



The screenshot shows a 'Devices' section with a table. The table has a header row with 'Name' and a selection column. The first row is 'All Selected Devices' with a selected radio button. Below it are three rows with 'Router.cisco.com' and unselected radio buttons.

Name	
All Selected Devices	<input checked="" type="radio"/>
Router.cisco.com	<input type="radio"/>
Router.cisco.com	<input type="radio"/>
Router.cisco.com	<input type="radio"/>

- ❖ To configure discrete values on a single router, select the applicable entry.

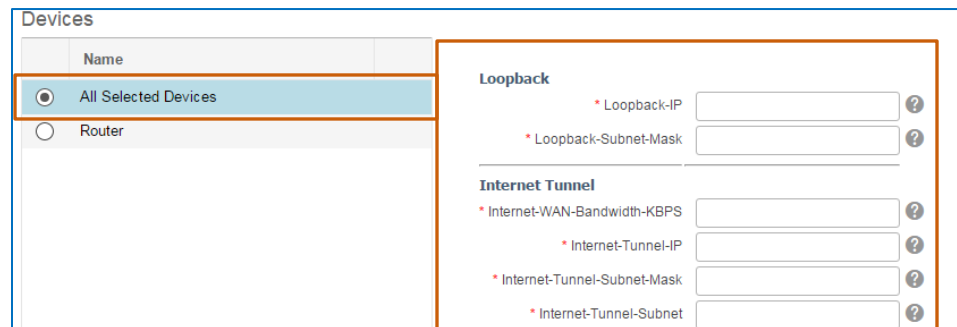


The screenshot shows a 'Devices' section with a table. The table has a header row with 'Name' and a selection column. The first row is 'All Selected Devices' with an unselected radio button. The second row is 'Router' with a selected radio button.

Name	
All Selected Devices	<input type="radio"/>
Router	<input checked="" type="radio"/>



Note: When **All Selected Devices** is active, the system lists the parameters for configuration.



The screenshot shows the configuration page with 'All Selected Devices' selected in the 'Devices' list. The configuration fields for 'Loopback' and 'Internet Tunnel' are visible and highlighted with an orange box.

Name	
All Selected Devices	<input checked="" type="radio"/>
Router	<input type="radio"/>

Loopback

* Loopback-IP ?

* Loopback-Subnet-Mask ?

Internet Tunnel

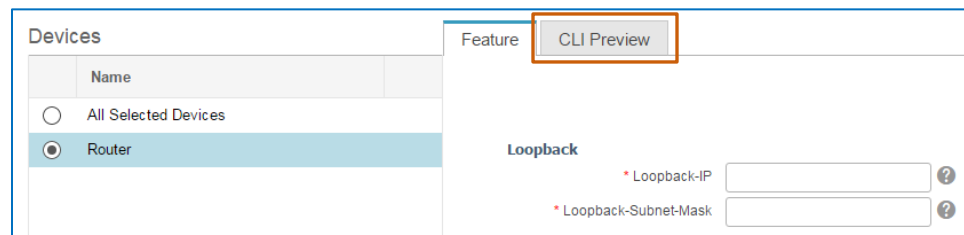
* Internet-WAN-Bandwidth-KBPS ?

* Internet-Tunnel-IP ?

* Internet-Tunnel-Subnet-Mask ?

* Internet-Tunnel-Subnet ?

When you select an individual router, the system opens the **Feature** tab with the parameter list and the **CLI Preview** tab, which displays the CLI code that the system will deploy based on the parameters that you configure in the list.



The screenshot shows the configuration page with 'Router' selected in the 'Devices' list. The 'Feature' tab is active, and the 'CLI Preview' sub-tab is highlighted with an orange box. The configuration fields for 'Loopback' are visible.

Name	
All Selected Devices	<input type="radio"/>
Router	<input checked="" type="radio"/>

Feature **CLI Preview**

Loopback

* Loopback-IP ?

* Loopback-Subnet-Mask ?

2. In the list, configure all of the required parameters, and any optional ones, that the router needs so that it runs as expected.



Note: When you need to configure a specific router component, such as an interface, you need to select the entry for that router in the **Devices** list.

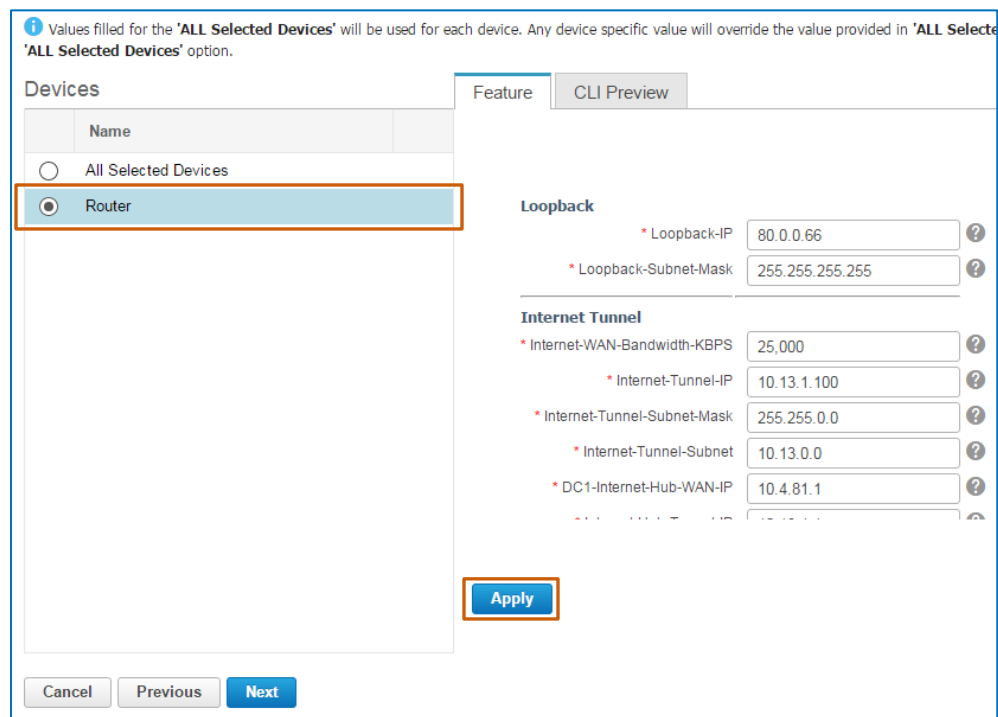
This action populates drop-down lists with the related components.

3. To save the parameter values to the group of selected routers or a single router, with the applicable option selected, click **Apply**.



Important Note: Use caution when toggling between the **All Selected Devices** option and individual router options in the **Devices** list.

To retain your entries, you must click **Apply** before changing device selections or you will lose the data that you entered.



Values filled for the 'ALL Selected Devices' will be used for each device. Any device specific value will override the value provided in 'ALL Selected Devices' option.

Devices

Name
<input type="radio"/> All Selected Devices
<input checked="" type="radio"/> Router

Feature **CLI Preview**

Loopback

- * Loopback-IP: 80.0.0.66
- * Loopback-Subnet-Mask: 255.255.255.255

Internet Tunnel

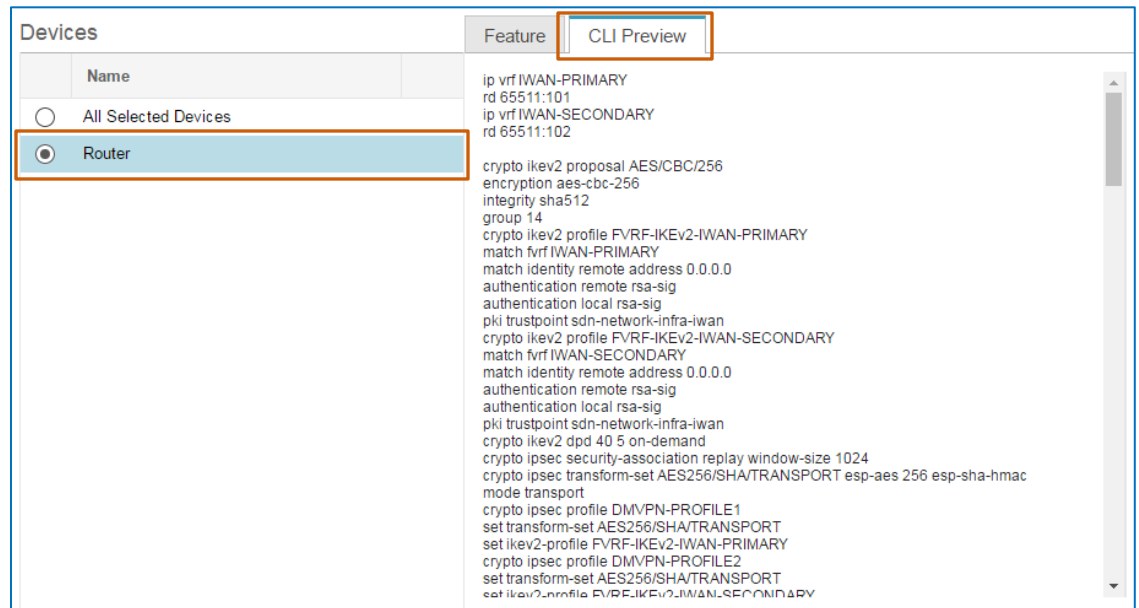
- * Internet-WAN-Bandwidth-KBPS: 25,000
- * Internet-Tunnel-IP: 10.13.1.100
- * Internet-Tunnel-Subnet-Mask: 255.255.0.0
- * Internet-Tunnel-Subnet: 10.13.0.0
- * DC1-Internet-Hub-WAN-IP: 10.4.81.1

Apply

Cancel Previous Next

4. To review the CLI code that the system will deploy to an individual router following the parameters that you configured, select that router in the list, and then click the **CLI Preview** tab.

The **CLI Preview** tab displays the code associated with the parameters that you configured.



Devices	Feature	CLI Preview		
<table border="1"> <thead> <tr> <th>Name</th> </tr> </thead> <tbody> <tr> <td><input type="radio"/> All Selected Devices</td> </tr> <tr> <td><input checked="" type="radio"/> Router</td> </tr> </tbody> </table>	Name	<input type="radio"/> All Selected Devices	<input checked="" type="radio"/> Router	<div>ip vrf IWAN-PRIMARY rd 65511:101 ip vrf IWAN-SECONDARY rd 65511:102</div> <div>crypto ikev2 proposal AES/CBC/256 encryption aes-cbc-256 integrity sha512 group 14 crypto ikev2 profile FVRF-IKEv2-IWAN-PRIMARY match frrf IWAN-PRIMARY match identity remote address 0.0.0.0 authentication remote rsa-sig authentication local rsa-sig pki trustpoint sdn-network-infra-iwan crypto ikev2 profile FVRF-IKEv2-IWAN-SECONDARY match frrf IWAN-SECONDARY match identity remote address 0.0.0.0 authentication remote rsa-sig authentication local rsa-sig pki trustpoint sdn-network-infra-iwan crypto ikev2 dpd 40 5 on-demand crypto ipsec security-association replay window-size 1024 crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac mode transport crypto ipsec profile DMVPN-PROFILE1 set transform-set AES256/SHA/TRANSPORT set ikev2-profile FVRF-IKEv2-IWAN-PRIMARY crypto ipsec profile DMVPN-PROFILE2 set transform-set AES256/SHA/TRANSPORT set ikev2-profile FVRF-IKEv2-IWAN-SECONDARY</div>
Name				
<input type="radio"/> All Selected Devices				
<input checked="" type="radio"/> Router				

- To configure another technology, click **Next**, and then return to step 1.

When you finish configuring all of the technologies that you need to deploy, to review and validate the CLI code, click **Next**, and then [go to task 6](#).

In this case, we are configuring three technologies, including DM VPN, PfR, and QoS.

The following screenshots illustrate the completed configuration parameters for each technology based on the use case and its network configuration.

DM VPN Technology Configuration

Feature	CLI Preview
Loopback <ul style="list-style-type: none"> * Loopback-IP <input type="text" value="80.0.0.66"/> ? * Loopback-Subnet-Mask <input type="text" value="255.255.255.255"/> ? 	
Internet Tunnel <ul style="list-style-type: none"> * Internet-WAN-Bandwidth-KBPS <input type="text" value="25,000"/> ? * Internet-Tunnel-IP <input type="text" value="10.13.1.100"/> ? * Internet-Tunnel-Subnet-Mask <input type="text" value="255.255.0.0"/> ? * Internet-Tunnel-Subnet <input type="text" value="10.13.0.0"/> ? * DC1-Internet-Hub-WAN-IP <input type="text" value="10.4.81.1"/> ? 	
<ul style="list-style-type: none"> * Internet-WAN-Interface <input type="text" value="GigabitEthernet0/0/1"/> ▼ MPLS Tunnel <ul style="list-style-type: none"> * MPLS-WAN-Bandwidth-KBPS <input type="text" value="25,000"/> ? * MPLS-Tunnel-IP <input type="text" value="10.33.1.100"/> ? * MPLS-Tunnel-Subnet-Mask <input type="text" value="255.255.0.0"/> ? * MPLS-Tunnel-Subnet <input type="text" value="10.33.0.0"/> ? * DC1-MPLS-Hub-WAN-IP <input type="text" value="172.16.1.1"/> ? * MPLS-Hub-Tunnel-IP <input type="text" value="10.33.1.1"/> ? * MPLS-WAN-Interface <input type="text" value="GigabitEthernet0/0/0"/> ▼ 	
Internet WAN <ul style="list-style-type: none"> * Internet-WAN-IP <input type="text" value="10.4.81.101"/> ? * Internet-WAN-Subnet-Mask <input type="text" value="255.255.255.252"/> ? * Internet-WAN-GW-IP <input type="text" value="10.4.81.102"/> ? MPLS WAN <ul style="list-style-type: none"> * MPLS-WAN-IP <input type="text" value="172.16.1.101"/> ? * MPLS-WAN-Subnet-Mask <input type="text" value="255.255.255.252"/> ? * MPLS-WAN-GW-IP <input type="text" value="172.16.1.102"/> ? 	
EIGRP <ul style="list-style-type: none"> * LAN-Subnet <input type="text" value="10.100.100.0"/> ? * LAN-Subnet-Mask <input type="text" value="255.255.255.0"/> ? 	

PfR Technology Configuration

Feature

CLI Preview

* Master-Controller-IP

10.8.88.10

?

* Auth-Password

Public

?

QoS Technology Configuration

Feature

CLI Preview

* DMVPN-Internet-Physical-Interface

10.4.81.101

?

* QOS-Marking-LAN-Interface

LAN_Ingress

?

* DMVPN-MPLS-Physical-Interface

172.16.1.101

?

* Device Type

ProductSeries

?

* Internet-WAN-Bandwidth-MBPS

1.5

▼

?

* MPLS-WAN-Bandwidth-MBPS

1.5

▼

?

Task 6: Review and Validate the Configuration CLI Code

With the parameters for each technology configured, you next need to review and validate the CLI code that the system will deploy to the router based on your configuration.



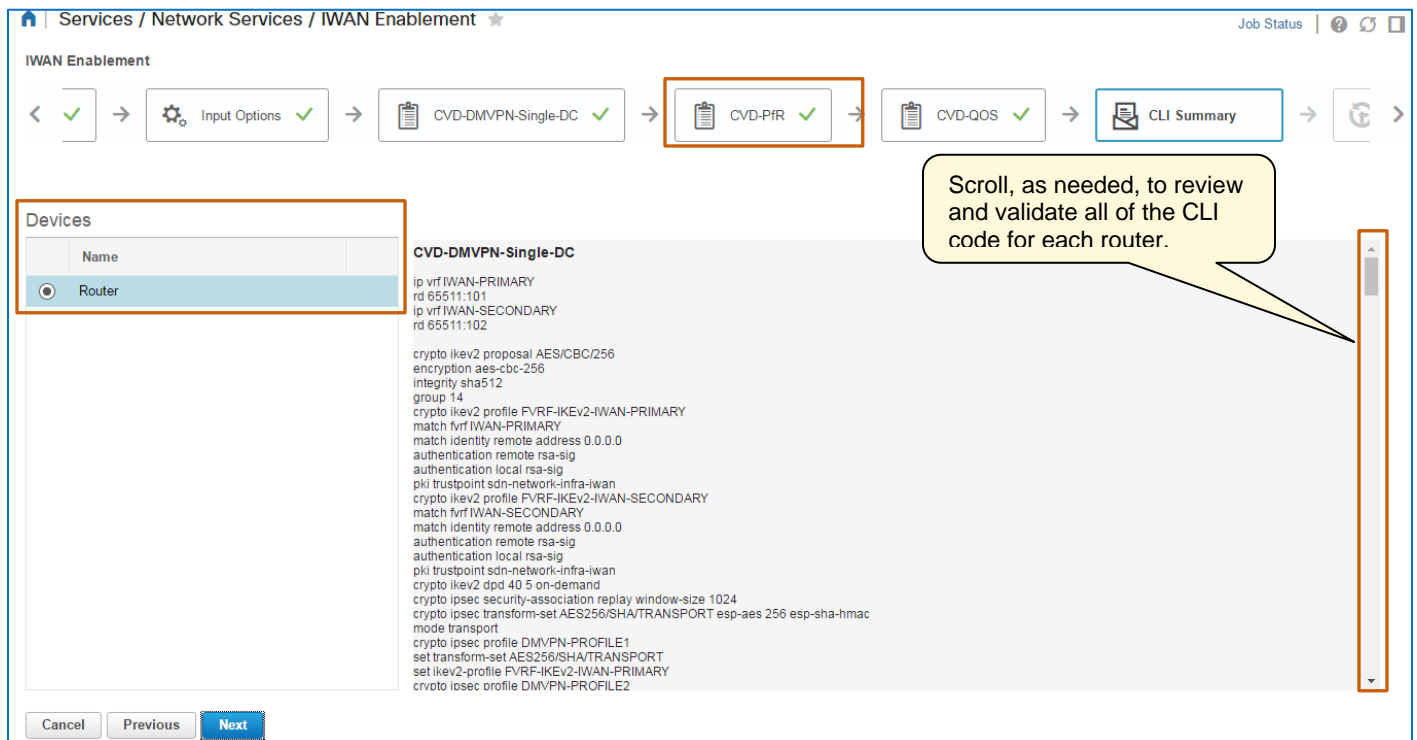
Important Note: Reviewing and validating the CLI code is a critical step that helps you ensure that the router will behave as expected when you deploy the configuration.

You can return to and change configuration parameters, as needed, before you continue.



To review and validate the configuration CLI code, follow these steps:

1. On the **CLI Summary** page, in the **Devices** list, select each router, and, by using the scroll bar, review and validate the CLI code that the system will deploy.
2. To schedule the configuration deployment job and configure the post-deployment job options, click **Next**, and then, [go to task 7](#).



Services / Network Services / IWAN Enablement

Job Status

IWAN Enablement

< [Input Options] → [CVD-DMVPN-Single-DC] → **[CVD-PfR]** → [CVD-QoS] → [CLI Summary] → [Next]

Devices

Name
<input checked="" type="radio"/> Router

CVD-DMVPN-Single-DC

```
ip vrf IWAN-PRIMARY
rd 65511:101
ip vrf IWAN-SECONDARY
rd 65511:102

crypto ikev2 proposal AES/CBC/256
encryption aes-cbc-256
integrity sha512
group 14
crypto ikev2 profile FVRF-IKEV2-IWAN-PRIMARY
match fvrf IWAN-PRIMARY
match identity remote address 0.0.0.0
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint sdn-network-infra-iwan
crypto ikev2 profile FVRF-IKEV2-IWAN-SECONDARY
match fvrf IWAN-SECONDARY
match identity remote address 0.0.0.0
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint sdn-network-infra-iwan
crypto ikev2 dpd 40 5 on-demand
crypto ipsec security-association replay window-size 1024
crypto ipsec transform-set AES256/SHA/TRANSPORT esp-aes 256 esp-sha-hmac
mode transport
crypto ipsec profile DMVPN-PROFILE1
set transform-set AES256/SHA/TRANSPORT
set ikev2-profile FVRF-IKEV2-IWAN-PRIMARY
crypto ipsec profile DMVPN-PROFILE2
```

Cancel Previous **Next**

Scroll, as needed, to review and validate all of the CLI code for each router.

In this case, the CLI code that the system will deploy meets all configuration requirements and specifications.

Task 7: Schedule the Configuration Deployment Job and Configure Post-Deployment Options

With the CLI code validated, you are ready to schedule the deployment of the configuration code to the router or routers. You can schedule the deployment to occur immediately or at a later time.

When considering when to start deployment, keep in mind that factors like network traffic congestion or slower link speeds among hub or branch routers might affect when you want to schedule configuration deployment.

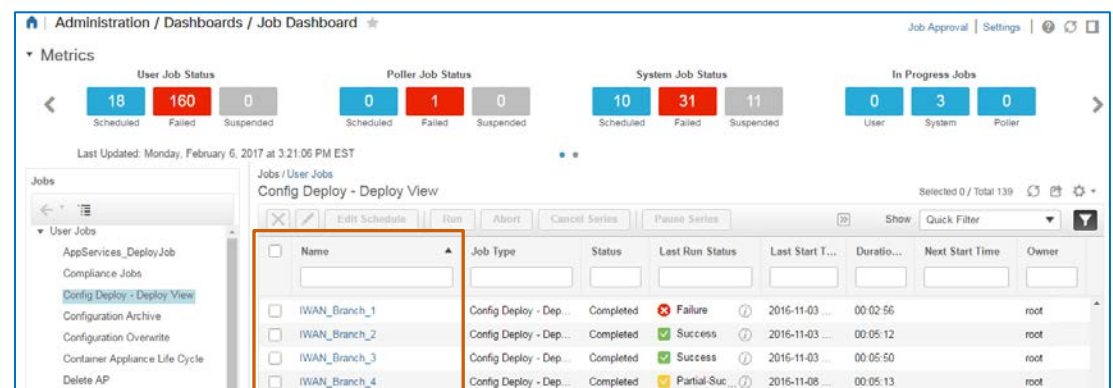
At this point, you also can indicate post-deployment options that you want the job to complete.

To schedule the deployment job and configure, follow these steps:

1. To make the configuration deployment job uniquely identifiable to system users, in the **Schedule** section, in the **Job Name** field, type the name.



Tip: Naming deployment jobs also helps users search for and find them more easily when reviewing the list on the **Job Dashboard** page in **Administration**.



Name	Job Type	Status	Last Run Status	Last Start Time	Duration	Next Start Time	Owner
IWAN_Branch_1	Config Deploy - Dep...	Completed	Failure	2016-11-03 ...	00:02:56		root
IWAN_Branch_2	Config Deploy - Dep...	Completed	Success	2016-11-03 ...	00:05:12		root
IWAN_Branch_3	Config Deploy - Dep...	Completed	Success	2016-11-03 ...	00:05:50		root
IWAN_Branch_4	Config Deploy - Dep...	Completed	Partial-Suc...	2016-11-08 ...	00:05:13		root

2. To schedule the configuration deployment job:
 - ❖ To start immediately, accept the default selection of **Now**.
 - ❖ To start at a scheduled time, click **Date**, and then, select the date and time for the job to begin running.

Schedule

Job Name

Paris_Branch_Deployment

Start Time

Now

Date

02/03/2017 01:55 PM

(MM/dd/yyyy hh:mm AM/PM)

3. In the **Job Option** section, to have the system copy the post-deployment running configuration to the startup configuration, select the **Copy Running Config to Startup** check box.



Note: When a device's startup configuration does not match its running configuration and the system reboots, it will apply the startup configuration to the device rather than the running configuration.

This mismatch situation can be problematic because the router might not run as expected after a reboot or a network issue.

4. To have the system store a copy of the post-deployment running configuration in the configuration archive, select the **Archive Config after Deploy** check box.



Note: Storing an archive copy of the configuration after deployment supports correcting mismatches or changing device configurations when you see unexpected behavior.

In those cases, you can retrieve a configuration from the archive and redeploy it to the device.

▼ **Job Option**

Copy Running Config to Startup ☒ ?


Archive Config after Deploy ☒ ?

5. To schedule the deployment job and validate deployment, click **Next**, and then, [go to task 8](#).


In this case, we are starting the deployment job immediately, and when the job completes, the system will copy the running configuration to the device's startup configuration and add a copy of the configuration to the configuration archive.

IWAN Enablement


<
→

 CVD-DMVPN-Single-DC ✓


→

 CVD-PfR ✓


→

 CVD-QoS ✓

→

 CLI Summary ✓


→

 Prepare and Schedule

>

▼ **Schedule**

Job Name

Start Time ☒ Now ☐ Date 

(MM/dd/yyyy hh:mm AM/PM)

NOTE: Each job scheduled here goes through Job Approval if the respective function is selected to go through job approval in Administration -> Settings -> System Settings->Job Approval. Post approval the scheduled jobs will run. If there is a delay in job approval, the runs scheduled in the above times slots will not run by PI Job Manager.

▼ **Job Option**

Copy Running Config to Startup ☒ ?

Archive Config after Deploy ☒ ?

Cancel
Previous
Next

Task 8: Start the Deployment Job and Validate Deployment

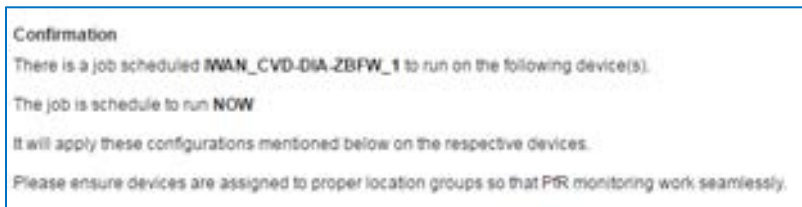
In this final step in the process, you have another opportunity to perform a high-level review of the routers to which the system is deploying and the technology configurations that each will receive.

You also can see the deployment job name and the running schedule.

After starting the configuration deployment, in **Administration**, you can monitor the job's status and validate the deployment.

To start the deployment job and validate deployment, follow these steps:

1. On the **Confirmation** page, in the **Confirmation** section, to ensure that the job name and schedule are what you expect, review the line items.



2. To review the routers that will receive configurations and the technologies configurations that they will receive, in the list, review the line items.
3. To return to a previous page to make any changes to devices, configurations, or technologies, click **Previous**.
4. To start the deployment job, click **Deploy**.

Services / Network Services / IWAN Enablement
Job Status

IWAN Enablement

/ PN-Single-DC ✓ → CVD-PIR ✓ → CVD-QOS ✓ → CLI Summary ✓ → Prepare and Schedule ✓ → Confirmation

Confirmation

There is a job scheduled **Paris_Branch_Deployment** to run on the following device(s).

The job is schedule to run **NOW**

It will apply these configurations mentioned below on the respective devices.

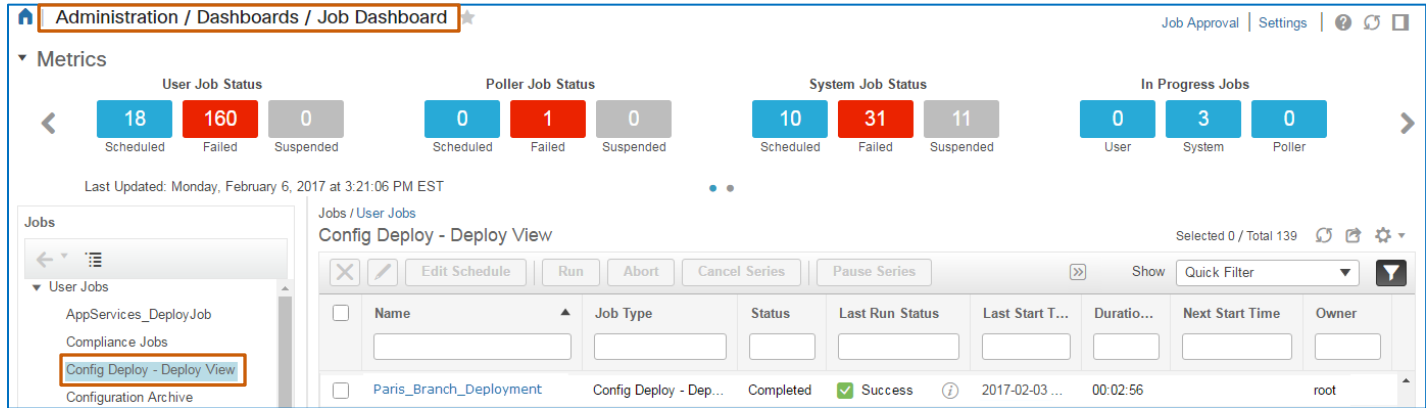
Please ensure devices are assigned to proper location groups so that PIR monitoring work seamlessly.

Device Name	Configuration
Router	CVD-DMVPN-Single-DC CVD-PIR CVD-QOS

Cancel Previous Deploy

The system generates a job.

5. To review the job status, navigate to the **Job Dashboard** page in **Administration**.
6. On the **Job Dashboard** page, in the **User Jobs** section, click **Config Deploy – Deploy View**.



Administration / Dashboards / Job Dashboard

Job Approval | Settings | ? | ? | ?

Metrics

User Job Status: 18 Scheduled, 160 Failed, 0 Suspended

Poller Job Status: 0 Scheduled, 1 Failed, 0 Suspended

System Job Status: 10 Scheduled, 31 Failed, 11 Suspended

In Progress Jobs: 0 User, 3 System, 0 Poller

Last Updated: Monday, February 6, 2017 at 3:21:06 PM EST

Jobs / User Jobs

Config Deploy - Deploy View

Selected 0 / Total 139

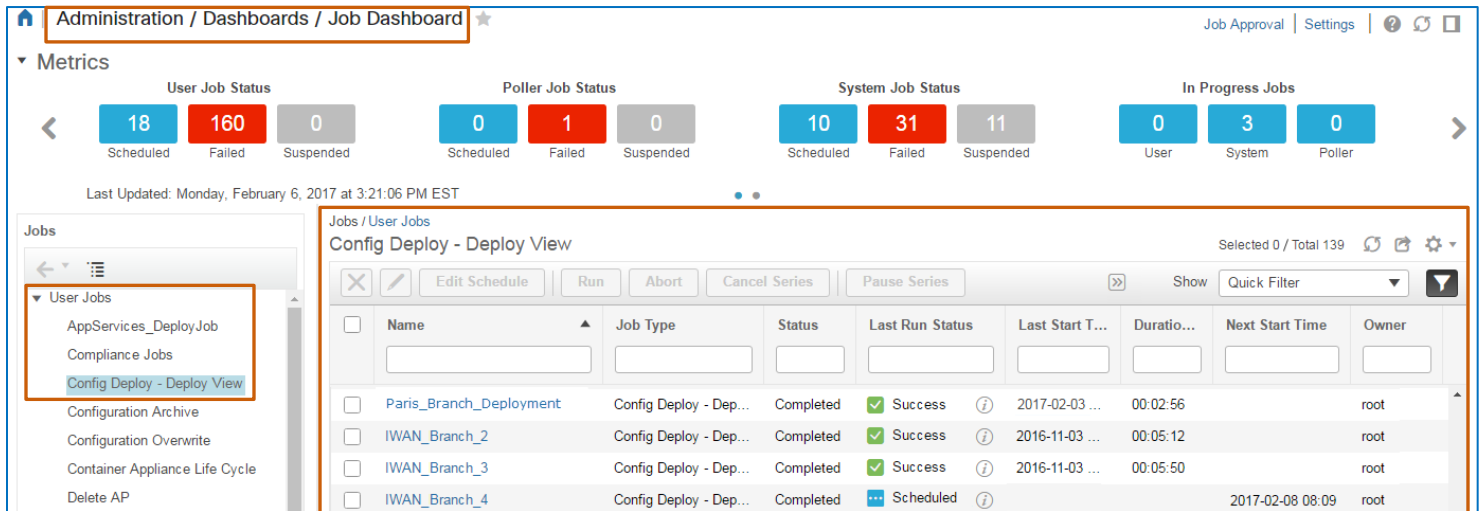
Name	Job Type	Status	Last Run Status	Last Start T...	Duratio...	Next Start Time	Owner
Paris_Branch_Deployment	Config Deploy - Dep...	Completed	Success	2017-02-03 ...	00:02:56		root

The page lists the configuration deployment jobs that system users have scheduled, are running, or have completed.



Tip: To find the job more easily, in the **Name** filter field, begin typing the job name.

As you type, the page filters automatically to display only those jobs with names that include the text.



Administration / Dashboards / Job Dashboard

Job Approval | Settings | ? | ? | ?

Metrics

User Job Status: 18 Scheduled, 160 Failed, 0 Suspended

Poller Job Status: 0 Scheduled, 1 Failed, 0 Suspended

System Job Status: 10 Scheduled, 31 Failed, 11 Suspended

In Progress Jobs: 0 User, 3 System, 0 Poller

Last Updated: Monday, February 6, 2017 at 3:21:06 PM EST

Jobs / User Jobs

Config Deploy - Deploy View

Selected 0 / Total 139

Name	Job Type	Status	Last Run Status	Last Start T...	Duratio...	Next Start Time	Owner
Paris_Branch_Deployment	Config Deploy - Dep...	Completed	Success	2017-02-03 ...	00:02:56		root
IWAN_Branch_2	Config Deploy - Dep...	Completed	Success	2016-11-03 ...	00:05:12		root
IWAN_Branch_3	Config Deploy - Dep...	Completed	Success	2016-11-03 ...	00:05:50		root
IWAN_Branch_4	Config Deploy - Dep...	Completed	Scheduled			2017-02-08 08:09	root

7. In the list, locate the job and, in the **Last Run Status** field, monitor the progress of the job.

The **Last Run Status** field indicates jobs that are scheduled to run, running, and, when completed, whether they are successful or have issues.

Jobs / User Jobs

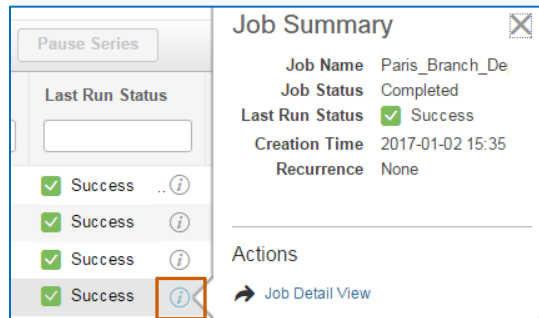
Config Deploy - Deploy View Selected 0 / Total 139

<input type="checkbox"/>	Name	Job Type	Status	Last Run Status	Last Start T...	Duratio...	Next Start Time	Owner
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/>	Paris_Branch_Deployment	Config Deploy - Dep...	Completed	✓ Success ⓘ	2017-02-03 ...	00:02:56		root
<input type="checkbox"/>	IWAN_Branch_2	Config Deploy - Dep...	Completed	✓ Success ⓘ	2016-11-03 ...	00:05:12		root
<input type="checkbox"/>	IWAN_Branch_3	Config Deploy - Dep...	Completed	✓ Success ⓘ	2016-11-03 ...	00:05:50		root
<input type="checkbox"/>	IWAN_Branch_4	Config Deploy - Dep...	Completed	✓ Partial-Suc... ⓘ	2016-11-08 ...	00:05:13		root
<input type="checkbox"/>	IWAN_Branch_1	Config Deploy - Dep...	Completed	✗ Failure ⓘ	2016-01-09 ...	00:00:03		prime

8. When the job completes, to evaluate the results at a high level:

- ❖ In the **Last Run Status** field, beside the status, click the information button, and then, in the **Job Summary** pop-up window, review the results.

In this case, the system successfully deployed the CLI code to the router.



- ❖ On the **DMVPN Monitor Home** page, for each hub router entry, determine whether the **Active Spokes** column number is incremented up by one.

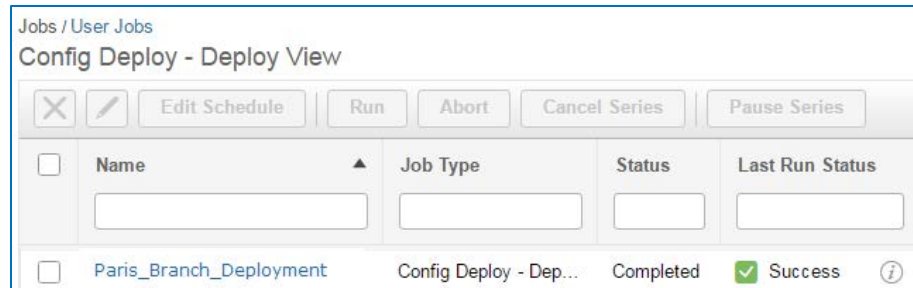
In this case, the **Active Spokes** column for the INET and MPLS hub router entries have incremented up by one, which indicates that the Paris branch router is connected to the hub router.

Services / Application Visibility & Control / DMVPN Monitor Home					
DMVPN Monitor Home					
Show Quick Filter					Total 12
Data Center Location	Device Name	Device Type	Device IP	Image Version	Active Spokes
TME-LAB	AMS-ASR1K-INET	Cisco ASR 1002-X Router	10.11.254.2	15.5(3)S2	0
TME-LAB	AMS-ASR1K-MPLS	Cisco ASR 1002-X Router	10.11.1.1	15.5(3)S2	0
SJ-HQ	ASR1K-CORE1	Cisco ASR 1004 Router	10.0.2.2	15.5(3)S2	3
SJ-HQ	ASR1K-CORE2	Cisco ASR 1004 Router	10.0.3.2	15.5(3)S2	4
HUB	INET_Hub.cisco.com	Cisco ASR 1001-X Router	192.168.139.185	15.5(3)S5	2
LOS ANGELES	LA-RTR4331-IWAN	Cisco 4331 Integrated Services Router	10.2.1.1	15.5(3)S2	0
HUB	MPLS_Hub.cisco.com	Cisco ASR 1001-X Router	192.168.139.184	15.5(3)S5	2
NEW YORK	NYC-RTR-INET	Cisco 4451 Series Integrated Services R...	10.16.255.2	15.5(3)S2	0
NEW YORK	NYC-RTR-MPLS	Cisco 4451 Series Integrated Services R...	10.16.1.1	15.5(3)S2	0
PARIS	Router	Cisco 4331 Integrated Services Router	40.0.0.10	15.5(3)S2	0
Santa Rosa	Router.cisco.com	Cisco 4351 Integrated Services Router	80.0.0.66	15.5(3)S5	0
Santa Rosa	Router.cisco.com	Cisco 4351 Integrated Services Router	80.0.0.65	15.5(3)S5	0


HUB	INET_Hub.cisco.com	Cisco ASR 1001-X Router	192.168.139.185	15.5(3)S5	2
LOS ANGELES	LA-RTR4331-IWAN	Cisco 4331 Integrated Services Router	10.2.1.1	15.5(3)S2	0
HUB	MPLS_Hub.cisco.com	Cisco ASR 1001-X Router	192.168.139.184	15.5(3)S5	2

Based on the settings that we selected for post deployment actions, the system also:

- ❖ Copied the new running configuration to the startup configuration on the device.
- ❖ Stored a copy of the configuration in the configuration archive.



The screenshot shows a web interface titled 'Jobs / User Jobs' and 'Config Deploy - Deploy View'. It features a toolbar with buttons: 'X', 'Edit Schedule', 'Run', 'Abort', 'Cancel Series', and 'Pause Series'. Below the toolbar is a table with the following columns: 'Name', 'Job Type', 'Status', and 'Last Run Status'. The table contains one entry: 'Paris_Branch_Deployment' with a job type of 'Config Deploy - Dep...', a status of 'Completed', and a last run status of 'Success' (indicated by a green checkmark). A link icon is present next to the 'Success' status.

	Name	Job Type	Status	Last Run Status
<input type="checkbox"/>	Paris_Branch_Deployment	Config Deploy - Dep...	Completed	Success 



Tip: You can evaluate the job results at a detailed level by clicking job name link in the **Name** field.

IWAN Feature Configuration Templates

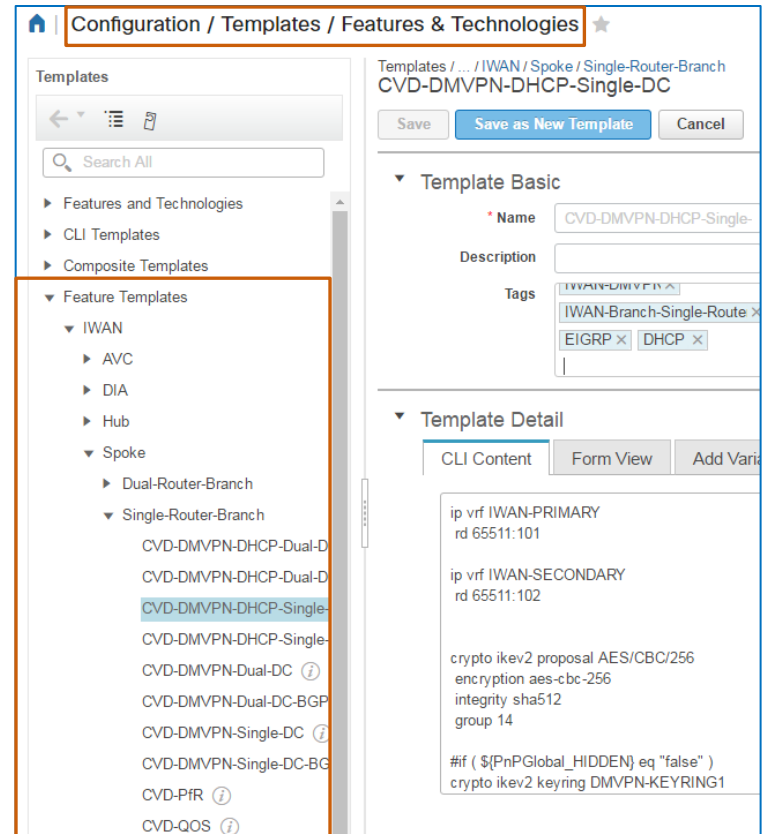
Customization Overview

IWAN feature configuration templates are system-provided or user-configured templates that contain Cisco Validated Design (CVD) specifications.



Note: For more information on the Cisco Validated Design program, [visit our Web site.](#)

CVD feature templates are available in the Feature Templates category on the **Features & Technologies** page.



Configuration / Templates / Features & Technologies

Templates / ... / IWAN / Spoke / Single-Router-Branch
CVD-DMVPN-DHCP-Single-DC

Save Save as New Template Cancel

Template Basic

Name CVD-DMVPN-DHCP-Single-DC

Description

Tags IWAN-DMVPN X IWAN-Branch-Single-Route X EIGRP X DHCP X

Template Detail

CLI Content Form View Add Vari

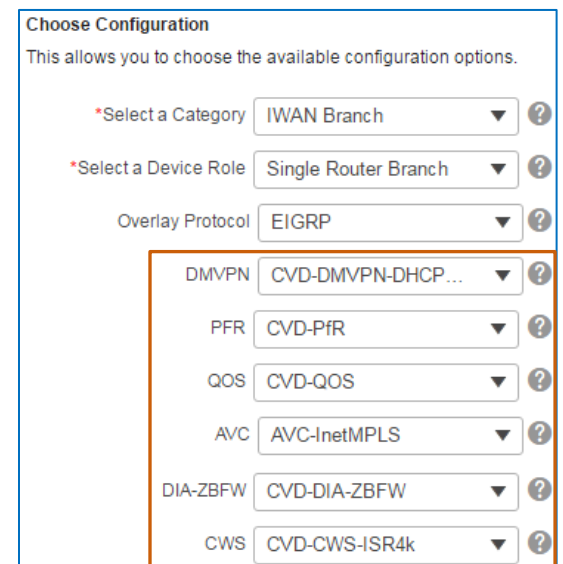
```
ip vrf IWAN-PRIMARY
rd 65511:101

ip vrf IWAN-SECONDARY
rd 65511:102

crypto ikev2 proposal AES/CBC/256
encryption aes-cbc-256
integrity sha512
group 14

#if ( $(PnPGlobal_HIDDEN) eq "false" )
crypto ikev2 keyring DMVPN-KEYRING1
```

These templates are the same ones that are available in the applicable technology or feature drop-down list in the **IWAN Enablement** wizard.



Choose Configuration

This allows you to choose the available configuration options.

*Select a Category IWAN Branch ?

*Select a Device Role Single Router Branch ?

Overlay Protocol EIGRP ?

DMVPN CVD-DMVPN-DHCP... ?

PFR CVD-PfR ?

QOS CVD-QOS ?

AVC AVC-InetMPLS ?

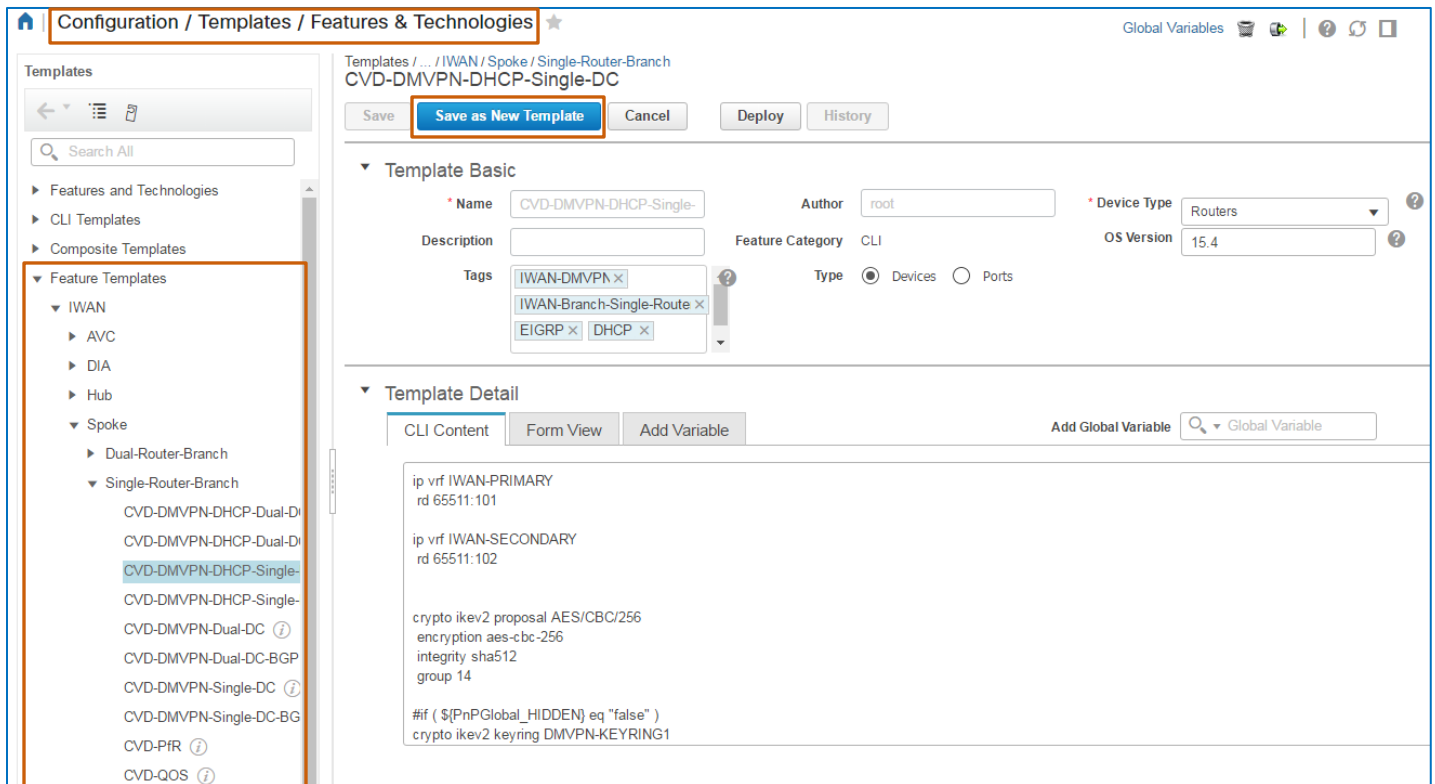
DIA-ZBFW CVD-DIA-ZBFW ?

CWS CVD-CWS-ISR4k ?

While you can use the IWAN feature templates as the system provides them, you also can add parameters, as needed, and indicate whether they are required or optional, to meet varying operational and business requirements on the network.

To customize IWAN feature templates in preparation for using the **IWAN Enablement** wizard for router configuration deployment, you can:

- ❖ Change baseline template parameter values and save the baseline template as a discrete template.
- ❖ Configure a series of similar, discrete templates by using the baseline template to address small differences among devices that require similar configurations.



The screenshot displays the Cisco Configuration Manager interface. The breadcrumb navigation at the top reads "Configuration / Templates / Features & Technologies". The left-hand "Templates" pane shows a tree structure under "Feature Templates" > "IWAN" > "Spoke" > "Single-Router-Branch", with "CVD-DMVPN-DHCP-Single-DC" selected. The main area shows the configuration for this template. The "Template Basic" section includes fields for Name ("CVD-DMVPN-DHCP-Single-"), Author ("root"), Device Type ("Routers"), Description, Feature Category ("CLI"), OS Version ("15.4"), and Tags ("IWAN-DMVPN", "IWAN-Branch-Single-Route", "EIGRP", "DHCP"). The "Template Detail" section shows the CLI content with tabs for "CLI Content", "Form View", and "Add Variable". The CLI content includes:

```
ip vrf IWAN-PRIMARY
rd 65511:101

ip vrf IWAN-SECONDARY
rd 65511:102

crypto ikev2 proposal AES/CBC/256
encryption aes-cbc-256
integrity sha512
group 14

#if ( ${PnPGlobal_HIDDEN} eq "false" )
crypto ikev2 keyring DMVPN-KEYRING1
```

Customizing IWAN feature templates before applying them in the IWAN configuration deployment process helps to automate the process, maintain configuration consistency, and shorten deployment timelines.

Automated IWAN Traffic Management

Performance Routing Overview

When you enable the Performance Routing (PfR) technology on devices, the system is able to monitor application traffic among routers.

Based on network performance, such as reachability, jitter, packet loss, or response time, the technology can reroute application traffic automatically to mitigate issues, where possible, while evenly distributing traffic to maintain equivalent link usage levels

It also reports whether the technology was able to return traffic to expected levels or whether issues remain unresolved.

When you enable PfR on devices, you can review the automated application traffic management activities that the IWAN performance routing function is performing on the **Performance Routing Monitoring** page.



Note: For detailed information on performance routing and intelligent path control, [refer to the Cisco Prime Infrastructure 3.1 User Guide](#).



You also can compare the performance of various WAN links by site, which can provide insight into link performance and whether to change traffic routing for better performance.

Services / Application Visibility & Control / PIR Monitoring

PIR Events
Compare WAN Links

Time Filter: Past 6 Hours

1

PIR Controlled Site
Select Site

Border Router
Select Border Router

WAN Interface / SP
Select WAN Interface

2

PIR Controlled Site
Select Site

Border Router
Select Border Router

WAN Interface / SP
Select WAN Interface

+

Select 2-3 WAN Links to compare
0 / 3 WAN Links Selected
Compare
Reset

Video Demonstration

Watching Demonstrations

To watch a demonstration:

- ❖ Click a demonstration link below, which opens an MP4 file.
Based on your system and configuration, you might need to start the video manually.



Notes: Video download and streaming times can vary.

Deploying an IWAN Branch Router

Watch the Demonstration



To review the process to IWAN routers online by using the **IWAN Enablement** wizard, [watch the Deploying an IWAN Branch Router video](#).
Approximate runtime: 11 mins

Links

To Product Information

[Visit the Cisco Web site to learn more about Cisco® Prime Infrastructure.](#)

[Visit the Cisco Web site to review or download technical documentation.](#)

To Training

[Visit the Cisco Web site to access other Cisco® Prime Infrastructure learning opportunities.](#)

[Visit the Cisco Web site to access learning opportunities for other Cisco products.](#)

To Contact Us

[Send us a message with questions or comments about this job aid.](#)



Note: Please send messages that address the content of this job aid or other training questions only.

Please follow your regular business process to request technical support or address technical or application-related questions.