Release Notes for Cisco IWAN

First Published: 1/22/15
Last Updated: 1/23/15

This release notes document provides information about the Cisco Intelligent WAN (IWAN) Solution, release 2.0.

Contents

Introduction

These release notes provide a summary of the components in the latest release of the Cisco Intelligent Wide Area Network (Cisco IWAN) Solution. For further information on Cisco IWAN, see Related Documentation, page 21.

What's New in Cisco IWAN

Cisco IWAN is a prescriptive solution for leveraging multiple transport providers, including low cost business grade broadband services as part of your WAN transport strategy. IWAN is a suite of components that brings all the WAN optimization, performance routing, and security levels of leased lines and expensive MPLS VPN services to the public Internet. IWAN makes it possible to get the performance, reliability and security benefits of private and virtual private network services while allowing the option of using more attractively priced service offerings and require simpler peering relationships with the transport provider. The same prescriptive design may be used with any transport provider; an important flexibility to have when multiple regional providers are needed.

Cisco IWAN can be implemented using Command Line Interface (CLI) commands on the routers of the hub and branch sites. Details about implementing Cisco IWAN are in the Cisco IWAN Technology Design Guide—see Related Documentation, page 21.

Help with configurations can be provided using Cisco Prime Infrastructure management tool, which includes wizards/templates for IWAN. For further information on Cisco Prime Infrastructure for IWAN, see Cisco IWAN Automation and Management, page 14. Also refer to the Release Notes for Prime 2.2, and the Cisco Prime Infrastructure 2.X Deployment Guide– listed in Related Documentation, page 21.

Use Cases for Cisco IWAN

Cisco IWAN is a prescriptive solution for any site connected to two IP transport networks, whether dual MPLS, dual Internet, or hybrid MPLS and Internet.

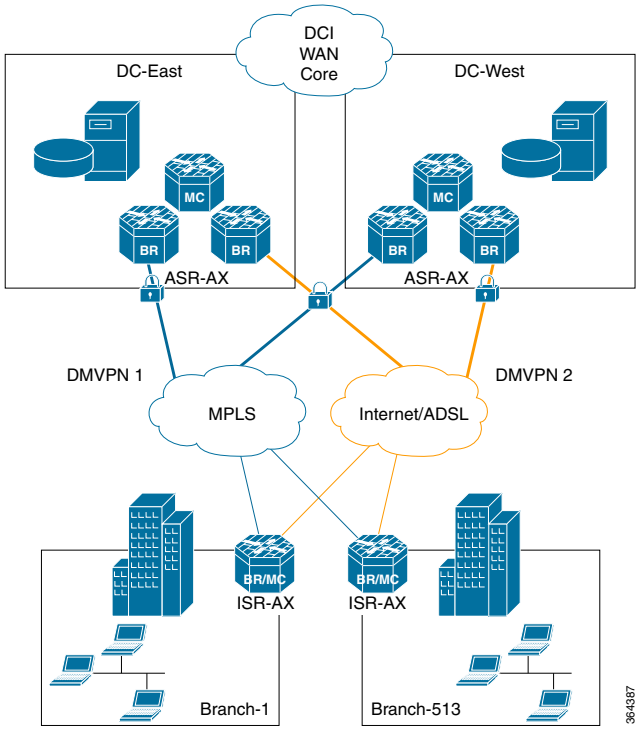
The following use cases are recommended for Cisco IWAN:

- IWAN Hybrid Design Model, page 3
- IWAN Dual Internet Design Model, page 4
- IWAN Dual MPLS Use Case, page 5

For further details about the two design models above, see the “IWAN Technology Design Guide” in Related Documentation, page 21.

IWAN Hybrid Design Model

Figure 1 IWAN Hybrid Design Model

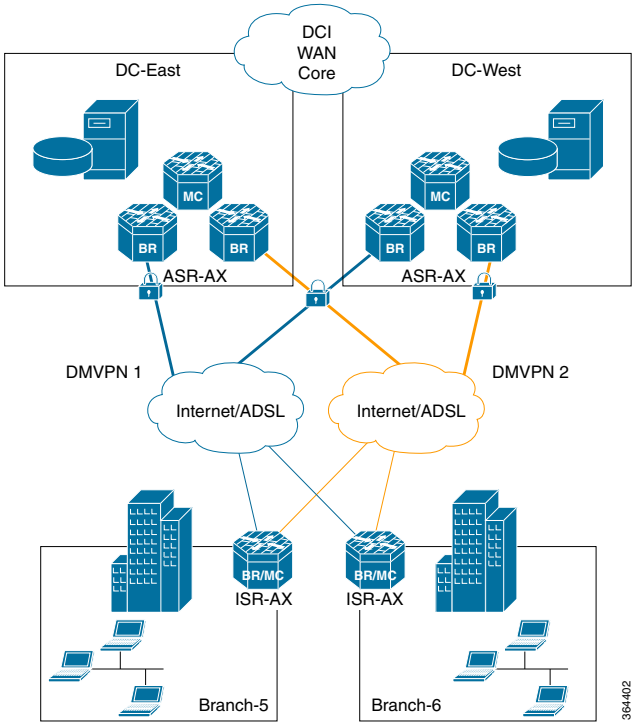


The hybrid design model has the following characteristics:

- Single MPLS VPN carrier for primary transport—using an MPLS WAN can provide more bandwidth for critical classes of services (key applications) and can provide SLA guarantees for these applications
- Single Internet link for secondary transport
- Front Door VRF (FVRF) on both MPLS and Internet links, with static default routing within the FVRF
- Single or dual WAN remote site routers

- Hub routers that connect to the Internet indirectly through a firewall demilitarized zone (DMZ) interface contained within the Internet edge

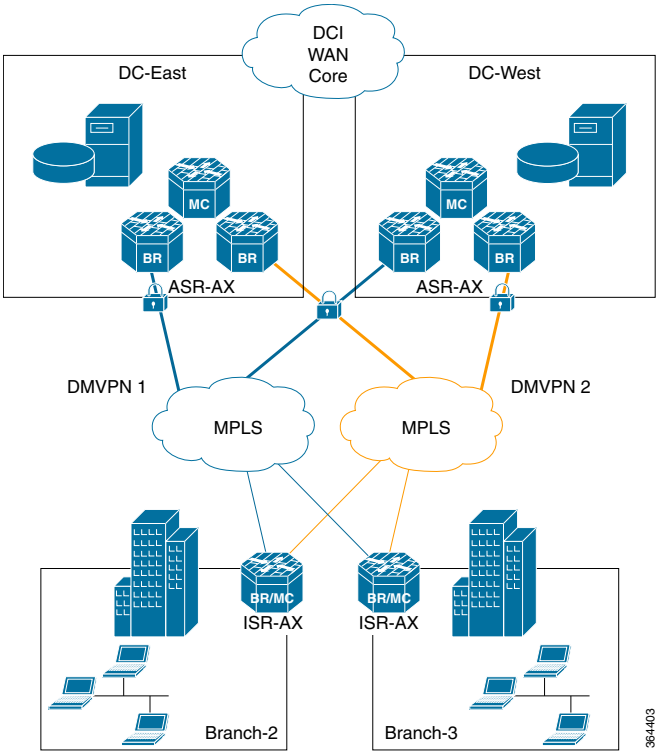
IWAN Dual Internet Design Model



The dual internet design model has the following characteristics:

- Two Internet links, which reduces cost while maintaining a high level of resiliency for the WAN
- Front Door VRF (FVRF) on both Internet links, with static default routing within the FVRF
- Single or dual WAN remote site routers
- Hub routers that connect to the Internet indirectly through a firewall demilitarized zone (DMZ) interface, which is contained within the Internet edge

IWAN Dual MPLS Use Case



The Dual MPLS use case is valid if you need stringent, application delivery, at a higher cost than other design models/use cases. Cisco IWAN adds the capability to fully utilize all bandwidth and to quickly respond to network issues.

For further information, see the Cisco IWAN Technology Design Guide, in Related Documentation, page 21.

Cisco IWAN Profiles

The following IWAN profiles can be used to categorize different groups of technologies configured on branch/remote sites.

Profile	Technologies	Notes
Base	■ DMVPN ■ QoS ■ PfRv3	DMVPN uses IPsec. These technologies are used in two IWAN Components—Application Optimization and Intelligent Path Control. See Components of Cisco IWAN, page 8.
Advanced	■ DMVPN ■ QoS ■ PfRv3 ■ Cisco Application Visibility and Control (AVC)	Direct Internet Access (DIA) may also be used. When using DIA, NAT is required—we recommend that you use Zone-Based Firewall (ZBFW) with NAT.
Advanced with WAAS	■ DMVPN ■ QoS ■ PfRv3 ■ Cisco Application Visibility and Control (AVC) ■ Cisco Wide Area Application Services (WAAS) Software	

System Requirements

The following sections describe the system requirements for Cisco IWAN Release 2.0.

Hardware and Software Requirements

Cisco IWAN, Release 2.0, supports the following Cisco platforms and software releases.

Device	Cisco IOS Software Release	Hub/Remote Site
Cisco ISR 4000 Series Routers	Cisco IOS XE 3.14 or higher.	Hub or remote site.
Cisco ASR 1000 Series Routers	Cisco IOS XE 3.14 or higher.	Hub site.
Cisco CSR 1000v Series Routers	Cisco IOS XE 3.14 or higher.	Hub site (Master Controller only).
Cisco ISR-G2 Series Routers	Cisco IOS 15.5(1)T1 or higher Cisco IOS 15.4(3)M1 or higher.	Remote site.

Cisco Wide Area Application Services

Cisco Wide Area Application Services (WAAS) release 5.5.1 or higher is supported by Cisco IWAN.

Cisco Prime Infrastructure

Cisco Prime Infrastructure release 2.2 or higher supports Cisco IWAN.

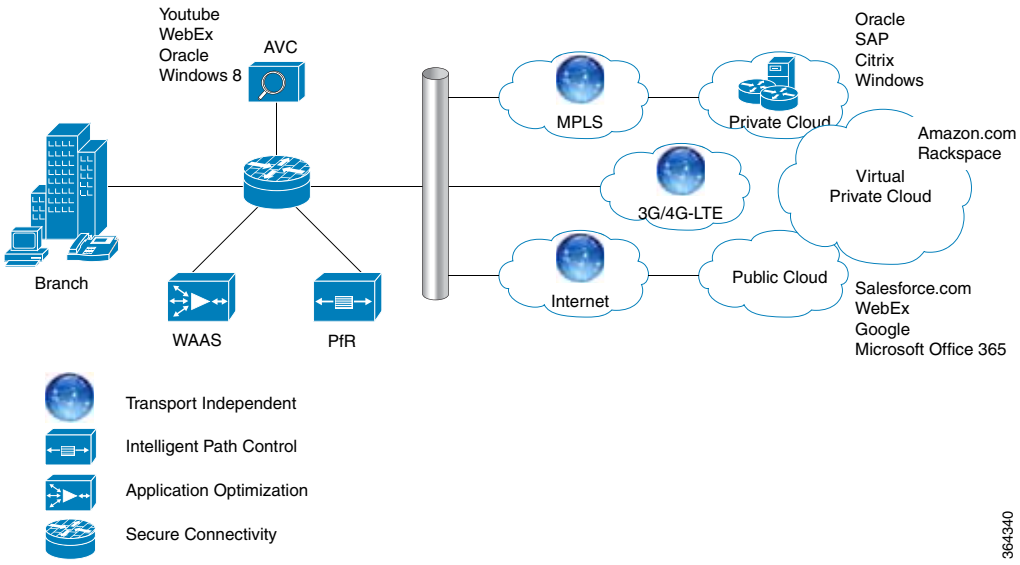
LiveAction

LiveAction version 4.1.2 or higher is supported by Cisco IWAN.

Components of Cisco IWAN

The four main components of the Cisco IWAN Solution are shown below:

Figure 2 IWAN Components



- Transport Independent Design, page 10
  - Consistent operational model
  - Simple provider migrations
  - Scalable and modular design
  - DMVPN IPsec overlay design
- Intelligent Path Control, page 11
  - Dynamically controlled data packet forwarding based on application type, performance, policies, and path status
  - Intelligent load-balancing of traffic over the best performing path based on the application policy
  - Improved network availability
  - Performance Routing (PfR) monitors the network performance—jitter, packet loss, delay—and forwards critical application traffic over the best path
  - Border routers collect traffic and path information and send it to the master controller, which detects and enforces the service policies to match the application requirement.
- Application Optimization, page 12
  - Application monitoring with Application Visibility and Control (AVC)
  - Application acceleration and bandwidth savings with WAAS

- Secure Connectivity, page 13
  - Certified strong encryption
  - Comprehensive Threat Defense with ASA and Cisco IOS Firewall/IPS
  - Cloud Web Security (CWS) for scalable secure Direct Internet Access (DIA)

Transport Independent Design

Transport Independent Design provides using Dynamic Multipoint VPN (DMVPN) as the GRE/IPsec VPN overlay. DMVPN is a Cisco software solution for building VPNs in an easy, dynamic and scalable manner with full authentication and encryption using IKEv2 and IPsec. Another part of the Transport Independent Design is the routing protocol that runs over the DMVPN tunnels and provides the base routing and forwarding for the data traffic that is flowing over IWAN. We recommend using either EIGRP or BGP (iBGP preferred). Transport Independent Design protects traffic between branch sites and between branch and hub sites (e.g traffic to the private data center).

DMVPN has the following characteristics that are useful for IWAN:

- Spokes automatically build a dynamic permanent hub-and-spoke GRE/IPsec tunnel to the hub, but not to other spokes. The spokes register as NHRP clients of the NHRP server (hub).
- When a spoke needs to send a packet to a destination subnet behind another spoke, it queries via NHRP for the real (outside) address of the destination spoke.
- The responding spoke initiates a dynamic GRE/IPsec tunnel to the initiating spoke (because it now knows the initiating peer's real (outside) address).
- The dynamic spoke-to-spoke tunnel is built over the mGRE tunnel interfaces on the spokes.
- When traffic between these spokes ceases, the spoke-to-spoke tunnel is removed.

In addition, DMVPN provides the following additional capabilities for Cisco IWAN:

- Easy and consistent forwarding and multi-homing over different carrier service offerings, including Multiprotocol Label Switching (MPLS) and broadband (Internet). Cellular 3G/4G/LTE WAN transports are also supported, although they require a slightly more complex configuration to limit traffic over these networks if desired.
- Zero-touch provisioning on the hub when adding spokes to the network.
- Dynamic full mesh connectivity.
- Spokes can have dynamically allocated WAN addresses (For example: PPP, DHCP) and/or their WAN addresses can be dynamically NAT'ed.

Cisco IWAN 2.0 uses DMVPN Phase 3, whereas Cisco IWAN 1.0 used DMVPN Phase 2.The similarities and differences between
DMVPN Phase 2 and DMVPN Phase 3 are shown in the following table:

Table 1 DMVPN Phase 2 and DMVPN Phase 3 Comparison

DMVPN Phase 2 (IWAN 1.0)	DMVPN Phase 3 (IWAN 2.0)
Spoke to spoke tunnel functionality	Spoke to spoke tunnel functionality
Hubs must interconnect in daisy-chain	No hub daisy-chain
Spoke must have full routing table —cannot summarize routes	Spokes don't need full routing table —can summarize routes
Spoke-spoke tunnel triggered by spoke	Spoke-spoke tunnel triggered by hub
Routing protocol limitations	Remove routing protocol limitations
	NHRP routes and override-next-hop pushed into RIB for CEF forwarding

The main configuration differences between DMVPN Phase 3 and DMVPN Phase 2, are:

- Necessity to change the routing protocol configuration to use the hub's IP address as the route's next-hop when advertising routes learned from a spoke back out the mGRE tunnel to the other spokes.

  For example, when using EIGRP you configure **ip next-hop-self eigrp *as*** (default) instead of **no ip next-hop-self eigrp *as*** on the DMVPN hub router mGRE tunnel interface.

- Ability to summarize routes advertised to the spokes (recommended).

  Example: When using EIGRP you could configure **ip summary-address eigrp *as network mask*** on the mGRE tunnel interface on the hub, to summarize routes advertised by the hub to the spokes, which could include summarizing the networks that are behind the spokes.

- Necessity of adding NHRP configuration to mGRE tunnel interfaces to turn on DMVPN Phase 3 functionality**,** using the following commands:

  - **ip nhrp redirect** on hubs
  - **ip nhrp shortcut** on spokes

Cisco IWAN 2.0 increases the routing protocol hello and hold timers, which decrease the CPU utilization and increase the routing protocol scaling. However, this also increases the amount of time for the routing protocol to detect a down neighbor which slows convergence. With Cisco IWAN 2.0, PfRv3 is used to quickly redirect traffic from congested or down paths to other paths and recovers data packet forwarding much faster than waiting for routing protocol re-convergence. This PfRv3 redirection only applies to flows that are controlled by PfRv3. Any flows that are not controlled by PfRv3 will wait for the routing protocol to re-converge before these flows continue (their packets are not black-holed).

Intelligent Path Control

Intelligent Path Control improves application delivery and WAN efficiency. PfRv3 controls data packet forwarding by considering the application type, performance, policies, and path status. PfRv3 offers: PfR domains, plug and play configuration, auto discovery of sites, NBAR2 support (the current release of IWAN does not support asymmetric routing), passive monitoring (using performance monitors), smart probing, and VRF awareness, with fewer than ten lines of configuration. For PfRv3, all the policies are defined in one place—the Hub Master Controller, allowing centralized configuration.

For further information on PfRv3, see http://docwiki.cisco.com/wiki/PfRv3:Home

Application Optimization

Cisco Application Visibility and Control (AVC) and Cisco Wide Area Application Services (WAAS) provide application performance visibility and optimization over the WAN.

Cisco AVC provides application awareness with deep packet inspection of traffic to identify and monitor applications' performance. Visibility and control at the application level (layer 7) is provided through AVC technologies such as Network-Based Application Recognition 2 (NBAR2), NetFlow, quality of service (QoS) and Performance Monitoring. Cisco AVC allows IT to determine what traffic is running across the network, tune the network for business-critical services, and resolve network problems. With increased visibility into the applications on the network, better QoS and PfR policies can be enabled to help ensure that critical applications are properly prioritized across the network.

Cisco WAAS provides application-specific acceleration capabilities that improve response times while reducing WAN bandwidth consumption. Cisco WAAS can compress data in flight using long-lived compression techniques including standards-based compression (LZ) and context-aware data redundancy elimination (DRE). Coupled with TCP optimizations that enable more intelligent and high-performance use of the network, Cisco WAAS also provides application-specific acceleration features for both encrypted and unencrypted applications such as Common Internet File System/Server Message Block Protocol (CIFS/SMB), Messaging Application Program Interface/Encrypted Messaging Application Program Interface (MAPI/eMAPI), Citrix ICA, HTTP and Secure HTTP (HTTPS) acceleration and object caching with Akamai Connect, SharePoint optimizations, and others.

Cisco Wide Area Application Services (WAAS) can compress data in flight using long-lived compression techniques including standards-based compression (LZ) and context-aware data redundancy elimination (DRE). Coupled with TCP optimizations that enable more intelligent and high-performance use of the network. Cisco WAAS also provides application-specific acceleration features for both encrypted and unencrypted applications such as Common Internet File System/Server Message Block Protocol (CIFS/SMB), Messaging Application Program Interface/Encrypted Messaging Application Program Interface (MAPI/eMAPI), Citrix ICA, HTTP and Secure HTTP (HTTPS) acceleration and object caching with Akamai Connect, SharePoint optimizations, and others.

Cisco Application Visibility and Control

1. Application response time metrics do not work properly (produces invalid results) for remote sites with dual router spokes and for hub routers due to asymmetric routing. In asymmetric routing, a packet traverses from a source to a destination in one path and takes a different path when it returns to the source. For example, in the case of an IWAN with dual router spokes, a packet goes from the source to the destination using the first router's WAN interface and returns to the source using the second router's WAN interface.

2. Applications might not be classified properly by NBAR2 for remote sites with dual router spokes and for hub routers, due to asymmetric routing.

3. Enable Cisco AVC/Cisco Next Generation Network-Based Application Recognition (NBAR2) on the LAN interface with Cisco WAAS when you are using Web Cache Communication Protocol (WCCP) redirection.
   Note: This limitation is *not* applicable for Cisco IOS 15.5(1)T or higher—Cisco AVC/NBAR2 can be enabled on the WAN interface with Cisco WAAS Software when you are using WCCP redirection.

   Note: There is no limitation with Cisco WAAS Software if you are using AppNav-XE redirection.

Cisco WAAS Software

1. PfRv3 and WCCP are supported only with Cisco IOS release of 15.4(3) M1 or higher.

   Note: PfRv3 and WCCP are not supported with platforms running Cisco IOS-XE releases (e.g, ISR 4000 Series).

2. WCCP-L2 redirection is not supported with PfRv3.

Secure Connectivity

Secure connectivity protects the WAN and has the Direct Internet Access (DIA) feature to offload user traffic directly to the Internet. The use of strong IPsec encryption, Cisco Zone-Based Firewall (ZBFW), and access lists protect the WAN over the public Internet and the WAN edge from Internet intrusion. Securely forwarding remote-site user Internet destined traffic directly to the Internet rather than routing this traffic over the WAN to the hub site improves public cloud application performance while reducing traffic over the WAN. Cisco Cloud Web Security (CWS) service provides a cloud-based web proxy to centrally manage and secure user traffic accessing the Internet.

Cisco Zone-Based Firewall (ZBFW), also called Zone Policy Firewall, is a Cisco IOS-integrated stateful firewall implemented on the Cisco Integrated Services Routers (ISR) and Cisco Aggregation Services Routers (ASR) routing platforms. Firewall zone policies are configured by using the Cisco Common Classification Policy Language (CPL or C3PL), which employs a hierarchical structure to define inspection for network protocols and the groups to which the inspection will be applied. Users familiar with the Cisco IOS Modular QoS CLI (MQC) will recognize the use of class maps to specify which traffic will be affected by the action applied in a policy map.

For secure connectivity in IWAN 2.0, DMVPN with IPsec pair-wise encryption is used for securing the tunnels between sites over which all of the data and control plane traffic traverses. This method is the same as the one used in Cisco IWAN 1.0, except that we have expanded the IPsec encryption protocols to include Suite-B protocols. One main change for IWAN 2.0 is that IKEv2 is used rather than ISAKMP for setting up pair-wise encryption with either Pre-shared Keys (PSK) or Public Key Infrastructure (PKI) authentication between the encryption peers. The available protocols for data level (ESP) encryption are: ESP-AES, ESP-GCM[1] and ESP-GMAC[1] These three protocols have key lengths of 128, 192, and 256 respectively.

The available protocols for ESP HMAC Integrity checking are: ESP-MD5-HMAC and ESP-SHA-HMAC (256, 384, 512) [1]. Even though any of these protocols may be used, the tested and recommended protocols for IWAN 2.0 are IKEv2 with PKI, ESP-AES 256 encryption and ESP-SHA-HMAC integrity.

[1]New with Suite-B support.

For information about which Cisco IOS releases are compatible with CWS, see Cisco Cloud Web Security (CWS) On ISR-G2 - FAQ.

Cisco IWAN Automation and Management

You can use Cisco Prime Infrastructure to provide templates that help to configure IWAN. The Cisco Prime IWAN Wizard (menu option **Service > IWAN**) is a convenient, workflow-based tool that easily provisions IWAN branches and hubs. The wizard forms part of the Cisco Prime 2.2 suite and can be accessed via the same web browser instance. It enables IWAN configuration on the routers starting from hub and branch selection, and proceeds to the DMVPN, PfRv3, QoS and AVC parts of the overall solution deployment. The wizard achieves this with a combination of form-based inputs and intelligent, back-end translation of these inputs into specific CLI sequences on the Cisco router. Many complex CLI sequences are abstracted away from the user, promoting effectiveness in the configuration tasks. At the end of the workflow, the configuration that was created in the wizard can be viewed in the tool and you are able to go back and correct previously entered data. Finally, the generated configuration is sent, ready to be activated, to the target router via the “Deploy” button.For further information on Cisco Prime Infrastructure, see the deployment guide and release notes that are referenced in Related Documentation, page 21.

Limitations and Restrictions

Limitations and Restrictions for Cisco IWAN 2.0

This section lists limitations and restrictions for Cisco IWAN 2.0, divided into each of the four IWAN components and for Automation and Management (e.g Cisco Prime Infrastructure).

Transport Independent Design–Limitations and Restrictions

For PfRv3 to be able to build and use spoke-spoke tunnels over the non-primary DMVPN network paths you must disable the NHRP route-watch functionality using the **no nhrp route-watch** command on the mGRE tunnels of the spoke routers.

This can have the following side-effects:

- For data flows that are *not* directly controlled by PfRv3 and are using a spoke-spoke tunnel over the non-primary DMVPN path.
  - These flows can be black-holed for an extended period of time if this spoke-spoke tunnel over the non-primary DMVPN path fails, but the remote spoke is still reachable via the hub.
- For data flows that are directly controlled by PfRv3 and are using a spoke-spoke tunnel over the non-primary DMVPN path.
  - These flows will be quickly redirected over alternate available paths by PfRv3 if this spoke-spoke tunnel over the non-primary DMVPN path fails.

Intelligent Path Control–Limitations and Restrictions

- IPv6 is not supported for PfRv3.
- PfR does not work properly when ZBFW is configured for secure connectivity. This limitation only applies for dual router remote sites using ISR G2 routers with a Cisco IOS T train image.

  Note There is a workaround for Cisco ISR 4000 Series routers that use Cisco IOS XE software.
- APP ID based policies are not allowed in IWAN 2.0 due to limitations of NBAR2 and routing asymmetry.

Application Optimization–Limitations and Restrictions

Cisco Application Visibility and Control

- Application response time metrics produce invalid results for remote sites with dual router spokes and dual hub routers, due to asymmetric routing. In asymmetric routing, a packet traverses from a source to a destination in one path and takes a different path when it returns to the source. For example, in the case of an IWAN with dual router spokes, a packet goes from the source to the destination using the first router's WAN interface and returns to the source using the second router's WAN interface.
- Applications might not be classified properly by NBAR2 for remote sites with dual router spokes and for hub routers, due to asymmetric routing.

- You must enable Cisco AVC/Cisco Next Generation Network-Based Application Recognition (NBAR2) on the LAN interface with Cisco WAAS when you are using WCCP redirection. (WCCP—Web Cache Communication Protocol.)

  Note: This limitation is *not* applicable for platforms using Cisco IOS 15.5(1)T or higher—when using Cisco IOS 15.5(1)T or higher , Cisco AVC/NBAR2 can be enabled on the WAN interface with Cisco WAAS Software when you are using WCCP redirection.

  Note: No limitation applies with Cisco WAAS Software if you are using AppNav-XE redirection.

Cisco WAAS Software

- PfRv3 and WCCP are supported only with Cisco IOS release of 15.4(3) M1 or higher. **Note:** PfRv3 and WCCP are not supported with platforms running Cisco IOS-XE releases (e.g, ISR 4000 Series).
- WCCP-L2 redirection is not supported with PfRv3.

Secure Connectivity–Limitations and Restrictions

- WCCP-L2 redirection is not supported for Zone-based Fire Wall (ZBFW) or PfRv3.
- CWS is only available on ISR-G2 with IOS 15.4(3)M or higher. The IOS version used must support VRF-aware CWS—for IOS 15.4(1)T or higher. The Cisco IOS images that support VRF are: 15.4(1)T, 15.4(1)T1, 15.4(2)T, 15.5(1)T, 15.4(3)M or higher.
- PfR does not work properly when ZBFW is configured for secure connectivity. This limitation only applies for dual router remote sites using ISR G2 routers with a Cisco IOS T train image.

  Note There is a workaround for Cisco ISR 4000 Series routers that use Cisco IOS XE software.

Automation and Management–Limitations and Restrictions

Cisco Prime Infrastructure

- Pre-shared keys and DMVPN

Currently, only the option of DMVPN provisioning using pre-shared keys is supported. For example, DMVPN provisioning using certificates is not supported on the Prime IWAN Wizard.

In Cisco Prime 2.2, the Prime IWAN Wizard does not support provisioning of the 4G WAN Interface. Future updates to Cisco Prime and the Prime IWAN Wizard will address the support of 4G interfaces.

- DMVPN provisioning for a “brownfield” installation is not supported

A “brownfield” installation refers to an existing site with single or dual-wan that has previously been provisioned without consideration of IWAN solution. The Prime IWAN Wizard does not provide the ability to override the existing WAN interface settings on the existing branch or hub, and doing so can cause unintended effects on the existing router’s DMVPN/WAN configuration. For this reason, we strongly recommend that you use the Prime IWAN Wizard on “greenfield” deployments only; that is, where the branch and hub routers are being brought up with a WAN configuration for the first time.

Note: If you choose not use the Prime IWAN wizard, then to customize your deployment, you can use the Cisco Prime 2.2 Template feature instead.

Note: If you do not use the Prime IWAN wizard (menu option **Service > IWAN**), then the Cisco Prime 2.2 Template can be customized to address the greenfield deployment.

- Limited cross-checking for PfRv3 Auth Password between master controllers and border routers

When provisioning PfRv3 using the Prime IWAN wizard, each device is asked to be set up with a “PfR auth-password” that reflects ultimately into the Cisco IOS configuration on the Cisco router.

Note: In the Prime IWAN Wizard, there is no cross-checking done when provisioning PfRv3 Master Controllers with their Border Routers.

If the passwords do not match, the error is not flagged to the user in the Cisco Prime 2.2 GUI. The effect of this is that PfRv3 may not come up as a service on the Enterprise site as the passwords do not match between Master Controllers and Border Routers. To determine this condition, we recommend:

  - Making a note of the password and ensuring that it stays consistent between Master Controller and Border Routers.
  - Looking at the Cisco router console for TCP-AUTH error messages.

- While using the Prime IWAN wizard, there may occasionally be delays in fields being populated. This occurs during the provisioning of IWAN services such as DMVPN, AVC, QoS, or PfR. The fields that experience delay are the ones containing feature-level configuration data; that is, the data shown in the window pane on the right hand side.

The delay varies from a few seconds to longer than 5 minutes. Usually the system should be able to recover and populate this data after a short delay. If not, then we recommend that you start again from the first step of the workflow.

- Device selection is sometimes not visible.

The device selection shown in the window pane on the left hand side, may disappear when you click somewhere else on the window pane other than in the check box of the selected device. We therefore recommend that you click exactly in the middle of the check box. Usually the system should be able to recover and populate this data. If not, then we recommend that you start again from the first step of the workflow.

Caveats

Open Caveats for Cisco IWAN 2.0

This section provides information about the caveats in Cisco IWAN 2.0. Caveats describe unexpected behavior. Severity 1 caveats are the most serious caveats. Severity 2 caveats are less serious. Severity 3 caveats are moderate caveats. This section includes severity 1, severity 2, and selected severity 3 caveats. The category refers to one of the four Components of Cisco IWAN, page 8 associated with the caveat.

Identifier	Description	Category
CSCuq65126	Tunnel-head packet drops when per-Tunnel QOS with “set dscp tunnel xx”	Application Optimization
CSCur28290	ASR 1002x crashes after adding Adaptive QOS config.	Application Optimization
CSCur49002	ISR 4431 crash seen with 10/8 image at high load/CPU with WAAS config.	Application Optimization
CSCuq10904	ISR 4331:MMA perf-mon out-of-order in punted packets.	Application Optimization
CSCun34170	Media flows are dropped with " find and add failed : 0 / 20994" on 1002X.	Application Optimization
CSCus06314	IWAN Wizard - 4G WAN is not manageable.	Automation and Management
CSCur09111	ISR 4451 Device Moving to Partial Collection Failure for a device config.	Automation and Management

For further information on caveats, enter the caveat number (e.g CSCur28290) into the Bug Search Tool.

If you have an account on cisco.com, you can also use the Bug Search Tool to find select caveats of any severity. If the defect that you have requested is not displayed, it may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.) See Cisco Bug Search Tool, page 19 for further details.

Cisco Bug Search Tool

For more information about how to use the Cisco Bug Search Tool, including how to set email alerts for bugs and to save bugs and searches, you can also see the Help & FAQ within the Bug Search Tool .

About the Bug Search Tool

This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products. Within the Cisco Bug Search Tool, each bug is given a unique identifier (ID) with a pattern of CSCxxNNNNN, where x is any letter (a-z) and N is any number (0-9). The bug IDs are frequently referenced in Cisco documentation, such as Security Advisories, Field Notices and other Cisco support documents. Technical Assistance Center (TAC) engineers or other Cisco staff can also provide you with the ID for a specific bug. The Cisco Bug Search Tool enables you to filter the bugs so that you only see those in which you are interested.

In addition to being able to search for a specific bug ID, or for all bugs in a product and release, you can filter the open and/or resolved bugs by one or more of the following criteria:

- Last modified date
- Status, such as fixed (resolved) or open
- Severity
- Support cases

You can save searches that you perform frequently. You can also bookmark the URL for a search and email the URL for those search results

Before You Begin

You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can register for an account.

Using the Bug Search Tool

1. In your browser, navigate to the Cisco Bug Search Tool.
2. If you are redirected to a Log In page, enter your registered Cisco.com username and password and then, click Log In.
3. To search for a specific bug, enter the bug ID in the Search For field and press Enter.
4. To search for bugs related to a specific software release, do the following:

   In the Product field, choose Series/Model from the drop-down list and then enter the product name in the text field. If you begin to type the product name, the Cisco Bug Search Tool provides you with a drop-down list of the top ten matches. If you do not see this product listed, continue typing to narrow the search results.

   In the Releases field, enter the release for which you want to see bugs.

   The Cisco Bug Search Tool displays a preview of the results of your search below your search criteria.
5. To see more content about a specific bug, you can do the following:
   - Mouse over a bug in the preview to display a pop-up with more information about that bug.
   - Click on the hyperlinked bug headline to open a page with the detailed bug information.

Service and Support

For support issues, contact Cisco Support. When you contact Cisco Technical Support about an issue, it will be helpful to provide information such as the IWAN Use Case or IWAN Profile that you are using.

Related Documentation

See the following related documentation:

Documentation	Description
Cisco IWAN Technology Design Guide	Cisco IWAN designs are explained in the Cisco IWAN Technology Design Guide. Look for the guide in the Cisco Validated Designs (CVDs) at http://www.cisco.com/c/en/us/solutions/enterprise/design-zone/index.html.
Release Notes for Cisco Prime 2.2	Refer to this guide for information about Cisco Prime Infrastructure 2.x, which can be used to configure Cisco IWAN.
Cisco Prime Infrastructure 2.X Deployment Guide	Refer to this guide for information about deploying Cisco Prime Infrastructure, assuming that the basic wired and wireless network is already deployed.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application. The RSS feeds are a free service.