Release Notes for Cisco IWAN Release 2.2.1

First Published: 08/25/2017
Last Updated: 11/30/2017

This release notes document provide information about Cisco Intelligent WAN (IWAN) Solution, Release 2.2.1.

Contents

Introduction

This release notes provide a summary of the components in the latest release of the Cisco Intelligent Wide Area Network (Cisco IWAN) Solution.

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.

Recommended Release for Cisco IWAN Release 2.2.1

The recommended release for Cisco IWAN Release 2.2.1 is Cisco IOS XE Everest 16.6.x. However, if you wish to use Cisco IOS XE Denali16.3.x releases, use the latest release.

What's New in Cisco IWAN Release 2.2.1

The new features and enhancements in Cisco IWAN Release 2.2.1, introduced via Cisco IOS XE Everest 16.6.1 are as follows:

PfRv3 Remote Prefix Tracking

Starting with Cisco IOS XE Denali 16.3.5c and Cisco IOS XE Everest 16.6.1, the PFRv3 Site prefix feature enhances networks running Performance Routing Version3 (PfRv3) to learn local site prefixes from the Routing Information Base (RIB) table as well as track the remote site prefix using RIB.

For more information, see the following Cisco document:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/xe-16-6/pfrv3-xe-16-6-book/pfrv3-remote-prefix.html

PfRv3 Per Interface Probe Tuning

Starting with Cisco IOS XE Everest 16.6.1, the PfRv3 Per Interface Probe Tuning feature provides the flexibility to specify different profiles for a channel associated with an interface thereby allowing you to measure the metrics of a channel.

For more information, see the following Cisco document:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/xe-16-6/pfrv3-xe-16-6-book/pfrv3-int-probe.html

PfRv3-Inter-DC-Optimization

Starting with Cisco IOS XE Everest 16.6.1, the PfRv3-Inter-DC-Optimization feature provides support by routing traffic from a hub site to another for specific traffic types such as data, voice, video, etc.

For more information, see the following Cisco document:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/pfrv3/configuration/xe-16-6/pfrv3-xe-16-6-book/pfrv3-inter-dc.html

Cisco Software-Defined Application Visibility and Control (SD-AVC)

Cisco SD-AVC is a component of Cisco AVC, operating as a centralized network service, and providing the following benefits:

- Network-level application recognition consistent across the network
- Improved application recognition in symmetric and asymmetric routing environments
- Improved first packet classification

- Protocol Pack update at the network level
- Secure browser-based dashboard over HTTPS

The SD-AVC network service can be hosted on one of the IWAN hub routers and does not require any change to the IWAN network topology. This feature is available in Cisco IOS XE Everest 16.6.1.

For more information, see the following Cisco document:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/avc/sd-avc/1-1-0/ug/sd-avc-1-1-0-ug.html

System Requirements

The following sections describe the system requirements for Cisco IWAN Release 2.2.1, which are as follows:

- Supported Cisco Platforms and Software Releases, page 3
- Software Requirements, page 4
- Platforms and their Roles, page 5

Supported Cisco Platforms and Software Releases

Cisco IWAN Release 2.2.1 supports the following Cisco devices and software releases.

Platform	Model	Cisco IOS Software Release
Cisco ISR 4000 Series Routers	ISR 4221 ISR 4451 ISR 4431 ISR 4351 ISR 4331 ISR 4321	Cisco IOS XE Denali 16.3.5c or Cisco IOS Everest XE 16.6.x or higher maintenance releases of Cisco IOS XE Denali 16.3.x or Cisco IOS XE Everest 16.6.x **Note:** Cisco ISR 4221 Integrated Services Router is supported from Cisco IOS XE Everest 16.6.1 onwards.
Cisco ASR 1000 Series Routers	ASR 1001-X ASR 1001-HX ASR 1002-X ASR 1002-HX ASR 1004 ASR 1006 ASR 1006-X ASR 1009-X ASR 1013	Cisco IOS XE Denali 16.3.5c or Cisco IOS Everest XE 16.6.x or higher maintenance releases of Cisco IOS XE Denali 16.3.x or Cisco IOS XE Everest 16.6.x
Virtual Routers	Cloud Services Router 1000v ENCS 5400	Cisco IOS XE Denali 16.3.5c or Cisco IOS Everest XE 16.6.x or higher maintenance releases of Cisco IOS XE Denali 16.3.x or Cisco IOS XE Everest 16.6.x **Note:** Cisco ENCS 5400, ISRv is supported from Cisco IOS XE Denali 16.3.3 onwards.

Platform	Model	Cisco IOS Software Release
Cisco ISR-G2 Series Routers—800 Series	C841 C891-24X-K9 C891F-K9 C891FW-A-K9 C891FW-E-K9 C892FSP-K9 C896VAG-LTE-GA-K9 C896VA-K9 C897VAB-K9 C897VA-K9 C897VAG-LTE-GA-K9 C897VAG-LTE-LA-K9 C897VAGW-LTE-GAEK9 C897VAMG-LTE-GA-K9 C897VA-M-K9 C897VAM-W-E-K9 C897VAW-A-K9 C897VAW-E-K9 C898-EA-K9 C898EAG-LTE-GA-K9 C898EAG-LTE-LA-K9 C899G-LTE-GA-K9 C899G-LTE-JP-K9 C899G-LTE-LA-K9 C899G-LTE-NA-K9 C899G-LTE-ST-K9 C899G-LTE-VZ-K9	Cisco IOS 15.7(3)M or higher maintenance releases of Cisco IOS 15.7(3)M
Cisco ISR-G2 Series Routers—1900 Series	ISR 1921 ISR 1941	Cisco IOS 15.7(3)M or higher maintenance releases of Cisco IOS 15.7(3)M
Cisco ISR-G2 Series Routers—2900 Series	ISR 2901 ISR 2911 ISR 2921 ISR 2951	Cisco IOS 15.7(3)M or higher maintenance releases of Cisco IOS 15.7(3)M
Cisco ISR-G2 Series Routers—3900 Series	ISR 3925 ISR 3925E ISR 3945 ISR 3945-E	Cisco IOS 15.7(3)M or higher maintenance releases of Cisco IOS 15.7(3)M

Software Requirements

Cisco Wide Area Application Services

Cisco Wide Area Application Services (WAAS) release 6.2.3c or higher.

Cisco Prime Infrastructure

Cisco Prime Infrastructure release 3.2 or higher is supported in Cisco IWAN Release 2.2.1.

IWAN Controller

IWAN Controller Release 1.5 is supported.

LiveAction

LiveAction version 6.0.2 or higher is suggested.

Platforms and their Roles

Platform	Role
Cisco ISR 4000 Series Routers	Hub site (ISR 4451, 4431 models) Branch site Master Controller, Standby MC or Transit MC (ISR 4451, ISR 4431 models)
Cisco ASR 1000 Series Routers	Hub site Branch site Master controller, standby master controller or transit master controller
Cisco CSR 1000v Series Routers	Hub site Branch site Master controller, standby master controller or transit master controller
Cisco ISR-G2 Series Routers	Branch site (ISR 890 series, ISR 1900 series, ISR 2900 series, ISR 3900 series)

Limitations and Restrictions

This section lists limitations and restrictions in Cisco IWAN 2.2.1:

- All devices on a site—master and border routers—must have the same software version.
- In IWAN POP, a PfR master controller and a PfR border router must be configured in different devices.
- The recommended upgrade procedure must be completed. Upgrades can be incremental. The upgrade procedure is available here:

  http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Intelligent_WAN/upgrade/iwan-upgrade.html
- The following are the default commands in Cisco IWAN Release 2.2.1:
  - **ip nhrp shortcut**
  - **if state nhrp**
  - **ip nhrp multicast dynamic**
  - **nhrp holdtime 600 seconds**

  Note: The above are default commands on devices with Cisco IOS XE Release Denali 16.3.3, not for devices with Cisco IOS Release 15.6(3)M2 and Cisco IOS Release 15.7(3)M.
- The default unreachable timer in PfRv3 is 4 seconds.
- If the branch devices are upgraded before the hub devices, the PfRv3 unreachable timer must be set to four seconds on the hub routers.
- A message appears when a branch device, enabled with MD5 password, establishes a TCP connection with a master controller on port 17749. However, the branch device is not able to establish a connection because the server socket might not be open or the master controller may be down. This message might be misleading and has no functional impact on the system.
- When the primary service provider link goes down, communication between spokes will be down. To avoid this, configure the **max-secondary-path ibgp** command when configuring EIGRP or BGP on a branch device. The value of the command must be *n-1* where *n* is the number of service provider multiplied by number of data centers. If a network has two data centers and two service providers, the value of the command must be three.

Caveats

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.

Caveats in Cisco IWAN Release 2.2.1

This section provides information about the caveats in Cisco IWAN Release 2.2.1.

Caveats in Cisco IWAN Release 2.2.1

Identifier	Description
CSCve69466	CPU utilization is 100% for HUB BR with MTT scale with 16.6.1 image
CSCve15722	The second and later PfRv3 VRF configurations are missing after reload
CSCve39308	cft_fid_table_new_flow causing Memory Fragmentation on c3900
CSCve61738	PfRv3: Continuation of the Smart Probe Jitter Issue in CSCvd78176
CSCve95485	TSN: Not show function when the Box crashes
CSCvf43101	Internet channel going towards hub from branch are not updated once default route is removed
CSCvf48097	Application policy ID not seen on branch devices when configured in PFR policy on HUB-MC
CSCvf56374	IDC traffic classes are uncontrolled for certain DSCP's
CSCvf62777	CSR router restarts whenever no passthrough configuration is passed
CSCvc46230	PfRv3: Unexpected Reload While Evaluating/Moving TC's Between Channels
CSCvd45803	On 4400 spoke next-hop to hub is not getting updated with new changed ip
CSCvd90560	Incorrect channel next-hop for branch to branch traffic
CSCve21272	PLR channels are not clearing up when the site id is down
CSCve44159	MC and BR Channels are available but TC is UC with Channels Unavailable status
CSCve51878	B1MCBR has a parent-route next-hop for TMCBR (0:0|2:5) even though there are no channels to that BR
CSCve51885	After withdraw ISP1 prefixes on Hub/Thub, 'master channels' output on B1MCR 'site prefixes' empty
CSCvf09796	Channel with remote end point 0.0.0.0 is available instead of unavailable
CSCvf53007	CENT RC ERROR: Invalid value of r_agent on 16.6.1 image
CSCve87995	Traffic class splitting when the MML length set is more than the mask length learnt in sp database
CSCvg35332	Incorrect and multiple border reachable on auto tunnel in dual router branch
CSCvf98863	MMA crash observed on Hub Router in IWAN setup
CSCvf98783	PFR Crash on 4431 observed with Dual Router Branch with BR reload
CSCvg05896	IWAN EIGRP SAF - seq number mismatch after branch reload
CSCvf31193	CSR1k: Crash observed after "show ip route" command

CSCvf87437	High memory utilization in the QFP over QM RM process
CSCvf56274	BGP VRF route redistribution into global routing table fails after a VRF route flap
CSCvd14310	Overlapping Loopback Interface Causes Incorrect Forwarding Decision with AppNav and PfR

Caveats in Prime Infrastructure 3.2

Identifier	Description
CSCve74859	PI3.1.5 can not display the PFR monitoring topology properly
CSCve92694	IWAN: Live Option does not display all apps but 5 minute, 15 and 30 minute does
CSCvd25266	Prim UI for Multi VRF: Selecting VRF105 from TCA event takes me to VRF101 page.
CSCvd29626	IWAN2.2 Multi VRF Prime does not display all flows when site prefixes are split
CSCve92575	IWAN: Represent topology correctly when flows failover to different DC's and normalize
CSCve94691	IWAN: Not all RC events contain Previous and current SP path

Software Download Information

The following table provides the path on Download Software page for downloading the software for Cisco IWAN Release 2.2.1.

Software	Path
Cisco IOS XE Software	Downloads Home > Products > IOS and NX-OS Software > IOS XE > IOS XE S > IOS XE Release 2 > Routers > platform > IOS XE Software-Everest-16.6.1
Cisco IOS Software	Downloads Home > Products > IOS and NX-OS Software > IOS > IOS Software Release 15M&T > IOS Software Release 15.6M&T > Routers > *platform* > IOS Software-15.7(3)M
Prime Infrastructure 3.2 Software	Downloads Home > Products > Cloud and Systems Management > Routing and Switching Management > Network Management Solutions > Prime Infrastructure > Prime Infrastructure 3.2 > Prime Infrastructure Patches-3.2
Cisco Intelligent Wide Area Network Application (IWAN App) 1.5.1 Software'	Products > Cloud and Systems Management > Policy and Automation Controllers > Application Policy Infrastructure Controller Enterprise Module (APIC-EM) > APIC-1.5 (IWAN) https://software.cisco.com/download/release.html?mdfid=286208072&flowid=77162&softwareid=286291196&release=1.5%20(IWAN)&relind=AVAILABLE&rellifecycle=&reltype=latest
Cisco Wide Area Application Services Software	Downloads Home > Products > Application Networking Services > Wide Area Application Services > Wide Area Application Services (WAAS) Software > Wide Area Application Services (WAAS) Software-6.2.3c (https://software.cisco.com/download/release.html?mdfid=280484571&flowid=122&softwareid=280836712&release=5.5.7b&relind=AVAILABLE&rellifecycle=&reltype=latest)

Related Documentation

Documentation	Description
Cisco Application Policy Infrastructure Controller Enterprise Module Deployment Guide	Information about the underlying Cisco APIC-EM product including deployment steps, verification, and troubleshooting.
Cisco IWAN Application on APIC-EM Release Notes	Description of the features, system requirements, prerequisites, and caveats for the Cisco Intelligent Wide Area Network Application (Cisco IWAN App) on APIC-EM.
Cisco IWAN Application on APIC-EM User Guide	Information about the installation, deployment, configuration of Cisco IWAN on APIC-EM. Explains the Cisco IWAN GUI and how to manage connected devices and hosts within your network.
Cisco IWAN Technology Design Guides	Cisco IWAN designs are explained in the Cisco IWAN technology design guides. Look for the guides in the Cisco Validated Designs (CVDs).
Cisco Open Plug-n-Play Agent Configuration Guide	PnP Agent documentation for Cisco IOS XE software.
Cisco Prime Infrastructure Documentation	Information about configuration guides, deployment guides, release notes, and other Cisco Prime Infrastructure documentation.
Configuration Guide for Network Plug and Play on APIC-EM	Documents the PnP server application in the APIC-EM.
Live Action	Documentation on LiveAction software.
Release Notes for Cisco Network Plug and Play	Description of the features and caveats for Cisco Network Plug and Play.
Release Notes for the Cisco Application Policy Infrastructure Controller Enterprise Module	Description of the features and caveats for the Cisco Application Policy Infrastructure Controller Enterprise Module (Cisco APIC-EM).
Solution Guide for Cisco Network Plug and Play	Overview of the Plug and Play solution, component descriptions, summary of major use cases, and basic deployment requirements, guidelines, limitations, prerequisites, and troubleshooting tips.

Obtain Documentation and Submit 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*.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. The RSS feeds are a free service.