CISCO™

Release Notes for Cisco IWAN Release 2.1.1

First Published: 04/20/2016
Last Updated: 06/13/2016

This release notes document provides information about Cisco Intelligent WAN (IWAN) Solution, Release 2.1.1.

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.

What's New in Cisco IWAN Release 2.1.1

The new features and enhancements in Cisco IWAN Release 2.1.1, introduced via Cisco IOS XE Release 3.16.2S, Cisco IOS Release 15.5(3)S2 and Cisco IOS Release15.5(3)M2a, are as follows:

Multiple VPN routing and forwarding (VRF) Support

Cisco IWAN 2.1.1 supports 20 VRFs on a hub and 7 VRFs on branches.

BGP Routing across the Overlay

Cisco IWAN Release 2.1.1 supports Internal BGP (iBGP) in addition to EIGRP across the overlay.

Multiple WAN Paths

Cisco IWAN Release 2.1.1 supports five paths in the IWAN domain. The paths can be a combination or mixture of MPLS, Internet, 4G or LTE interfaces. The paths terminate in a branch, but a branch might have two to five paths and branches might not share the same paths. When branches do not share the same paths, spoke-to-spoke tunnels cannot be established and the ability of Performance Routing (PfR) to manage performance is limited.

No additional feature configuration is required.

Advanced Load Balancing

In Cisco WAN 2.1, load balancing was performed when the **load balance** command was configured for traffic that did not have a performance or path preference policy. In Cisco IWAN 2.1.1, the **advanced** keyword is added to the **load balance** command, allowing paths to be excluded from load balancing for different traffic types, thereby making the load balancing policy flexible.

Path of Last Resort

A single path can be designated as the path of last resort. In most cases, this is a 4G or LTE path or service depending on usage.

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

Hierarchical Path Preference

The path preference policy has been enhanced to support more than two levels of path preference hierarchy.

SGT Based QoS

SGT Based QoS support is supported with Cisco IOS XE Release 3.16.2S and Cisco IOS Release15.5(3)S2. This feature matches a Security Group Tag (SGT) and sets Differentiated Services Code Point (DSCP) on a LAN ingress policy. The WAN egress policy is based on DSCP (as is in Cisco IWAN 2.1).

SGT Based QoS is not supported in 15.5(3)M2a.

Cisco Cloud Services Router (CSR) 1000V Series Support

Cisco Cloud Services Router (CSR) 1000V Series on the CSX platform or Cisco Unified Computing System (UCS) platform with multiple Ethernet interfaces, supports the following in Cisco IWAN Release 2.1.1:

- As a single branch router—Master Controller and border router (MC/BR)

- As a border router at the branch

- As a Master Controller (MC) in a hub site with scale enhancement from 500 sites to 2000 sites

Serviceability Enhancements

The following serviceability features are available in Cisco IWAN 2.1.1:

- TC State Change Reason, page 3

- Show command Enhancements, page 3

TC State Change Reason

The output of the **show traffic class** command has been enhanced to display uncontrolled to uncontrolled transitions due to lack of channel availability, for example, bandwidth not available, and bandwidth ceiling limit.

Show command Enhancements

1. The output of the **show channel** commands have been enhanced to display the label.

2. The output of the **show traffic class summary** command has been enhanced to display hexadecimal and text form of DSCP.

Cisco IWAN App Release 1.1

New features and functions are available in Cisco IWAN App Release 1.1.0 are as follows:

- Day-N addition and deletion of POP for datacenters

- Day 0 multilink support (more than two links) for hub sites

- Improved usability:

  - Autopopulating WAN interface information

  - Autopopulating OSPF LAN information

- Enable spoke provisioning with multiple interface

- Support for static IP address support in spokes for internet links

- Enhanced user experience through enhanced dashboard that displays provisioning and monitoring status, application experience and configuration differences

  Note: Cisco Prime Infrastructure Release 3.1 is required for this feature and will be available from April 2016.

- Support for coexistence of non-IWAN sites with IWAN sites

- Update download link for Cisco IWAN App to point to APIC-EM release 1.1

Supported Cisco Platforms and Releases

System Requirements

The following sections describe the system requirements for Cisco IWAN 2.1.1, which are as follows:

- Supported Cisco Platforms and Software Releases, page 4

- Software Requirements, page 6

- Platforms and their Roles, page 7

Supported Cisco Platforms and Software Releases

Cisco IWAN 2.1.1 supports the following Cisco devices and software releases.

Platform	Model	Cisco IOS Software Release
Cisco ISR 4000 Series Routers	ISR 4451x ISR 4431 ISR 4351 ISR 4331 ISR 4321	Cisco IOS XE 3.16.5aS or 15.5(3)S5a or higher maintenance releases of Cisco IOS XE 3.16.x.
Cisco ASR 1000 Series Routers	ASR 1001x ASR 1002x ASR 1004-RP2/ESP40 ASR 1006-RP2/ESP40 ASR 1006-RP2/ESP100 ASR 1009X-RP2/ESP200	Cisco IOS XE 3.16.5aS or 15.5(3)S5a or higher maintenance releases of Cisco IOS XE 3.16.x.

Platform	Model	Cisco IOS Software Release
Cisco CSR 1000v Series Routers	Cloud Services Router 1000v	Cisco IOS XE 3.16.5aS or 15.5(3)S5a or higher maintenance releases of Cisco IOS XE 3.16.x.
Cisco ISR-G2 Series Routers	ISR 1921	Cisco IOS 15.5(3)M5a or higher maintenance releases of Cisco IOS 15.5(3)M.
	ISR 1921-ISM	
	ISR 1941	
	ISR 1941-ISM	
	ISR 2901	
	ISR 2901-ISM	
	ISR 2911	
	ISR 2911-ISM	
	ISR 2921	
	ISR 2921-ISM	
	ISR 2951	
	ISR 2951-ISM	
	ISR 3925	
	ISR 3925E	
	ISR 3925E-ISM	
	ISR 3925-ISM	
	ISR 3945	
	ISR 3945-E	
	ISR 3945E-ISM	
	ISR 3945-ISM	
	ISR 890F	
	ISR 890FW	
	ISR 890W	
	ISR 892FSP	

Software Requirements

Cisco Wide Area Application Services

Cisco Wide Area Application Services (WAAS) release 5.5.5a or higher.

Cisco Prime Infrastructure

Cisco Prime Infrastructure release 3.1.

IWAN Controller

IWAN Controller Release 1.1 is supported.

LiveAction

LiveAction version 5.0.1 or higher is suggested.

Platforms and their Roles

Platform	Role
Cisco ISR 4000 Series Routers	Hub or remote site.
Cisco ASR 1000 Series Routers	Hub site or remote site.
Cisco CSR 1000v Series Routers	Hub site (Master Controller only). Branch site border router or single router Master Controller or Border Router combination (MC/BR)
Cisco ISR-G2 Series Routers	Remote site.

Limitations and Restrictions

This section lists limitations and restrictions in Cisco IWAN 2.1.1:

- Cisco Cloud Services Router (CSR) 1000V Series is not supported as hub border router.

- It is recommended that the unreachable timer be configured to four seconds.

- The following configuration is recommended for the hold-queue command on the loopback interface of the branch router (MC/BR):

```
interface loopback0
 hold-queue 1024 in
 hold-queue 1024 out
```

  Note: The hold-queue adjustment is not required on ISR-G2 but required on all Cisco IOS XE devices—ASR1k, ISR4k, Cisco Cloud Services Router (CSR) 1000V Series

- A single tunnel interface is supported for each border router at the IWAN POP.

Caveats

- Cisco Bug Search Tool, page 7
- Caveats in Cisco IWAN 2.1.1, page 8

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 2.1.1

This section provides information about the caveats in Cisco IWAN 2.1.1.

Identifier	Description
CSCux19847	RTP application-table cannot be exported and shown up properly
CSCuw88062	Crypto CA traceback with PNP profile & APIC EM on ISR 43xx routers
CSCux90363	IOS-ZBF: Missing "default" keyword in "?" for zone security
CSCux65871	%PERF_MONITOR_RESOURCE-1-RM_SET: RESOURCE EVENT RAISE under scale

Identifier	Description
CSCuy39229	Border Parent Route not recovered after TAG CLASH
CSCuy01555	PfRv3/MNH – branch to hub channel has wrong nexthop
CSCux88058	XE316:PfRV3 Channel next-hop not withdrawn with BGP down
CSCux43553	XE316: ASR1001X BR ucode crashed at ipv4_input_cent_rc_process
CSCux36581	CSR1000v: part of MMA punt records lost and not accounted on LSMPI interface
CSCux82241	EIGRP SAF sequence not same for site-prefix and discovered site
CSCux92391	SAF service 5 is not seen on 3945e branch after HUB MC reload
CSCux85593	TCP RST message is not being transferred from FVRF to other VRF
CSCux75926	Out of sync of traffic-classes btw MC/BR after IPC chunk failure
CSCvd14310	Overlapping Loopback Interface Causes Incorrect Forwarding Decision with AppNav and PfR

Caveats in Cisco IWAN 2.1.1MR

This section provides information about the caveats in Cisco IWAN 2.1.1 MR.

Identifier	Description
CSCuz68649	Internal Services Module – Crypto Engine crash
CSCuz69416	PfR branch MCPLO-UCODE crash

Software Download Information

The following table provides the path on Download Software page for downloading the software for Cisco IWAN Release 2.1.1.

Software	Path
Cisco IOS XE Software	Products > IOS and NX-OS Software > IOS XE > IOS XE S > IOS XE 3S > Routers > *platform* > Software on Chassis > IOS XE Software-3.16.5aS (https://software.cisco.com/download/special/release.html?config=684110644675436ad1349ee490ed79ff)
Cisco IOS Software	Downloads Home > Products > IOS and NX-OS Software > IOS > IOS Software Release 15M&T > IOS 15.5M&T > *platform* > IOS Software-15.5(3)M5a (https://software.cisco.com/download/special/release.html?config=1ad84c394cb5e333c4a79d0b4a7448ef)
Prime Infrastructure 3.1 Software	Downloads Home > Products > Cloud and Systems Management > Routing and Switching Management > Network Management Solutions > Prime Infrastructure > Prime Infrastructure 3.1 > Prime Infrastructure Software-3.1.0
Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) 1.0 Software	Products > Cloud and Systems Management > Policy and Automation Controllers > Application Policy Infrastructure Controller Enterprise Module (APIC-EM) > APIC-EM Software-1.1
Cisco Wide Area Application Services Software	Products > Application Networking Services > Wide Area Application Services > Wide Area Application Services (WAAS) Software > Wide Area Application Services (WAAS) Software-5.5.5a

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 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) at http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-branch-wan/cvd_ent_wan.html
Cisco Open Plug-n-Play Agent Configuration Guide	PnP Agent documentation for Cisco IOS XE.
Cisco Prime Infrastructure 3.1	Refer to this guide for information about Cisco Prime Infrastructure, which can be used to configure Cisco IWAN.
Cisco Prime Infrastructure 3.1 Release Notes	Description of the features and caveats for Cisco Prime Infrastructure.
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 Intelligent Wide Area Network Application (Cisco IWAN App)	Description of the features, system requirments, prerequisites, and caveats for the Cisco Intelligent Wide Area Network Application (Cisco IWAN App) on APIC-EM.
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.
Software Configuration Guide for Cisco IWAN on APIC-EM	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.

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 delivers content directly to your desktop using a reader application. The RSS feeds are a free service.