Cisco Extensible Network Controller Release Notes, Release 1.0 and 1.5

First Published: October 7, 2013
Last Updated: February 24, 2014
Part Number: OL-30571-01

This document describes the features, system requirements, resolved caveats, open caveats, and limitations for the Cisco Extensible Network Controller (XNC), Release 1.0 and 1.5.

Contents

This document includes the following sections:

Cisco Systems, Inc.
www.cisco.com

Revision History

Table 1 shows the revision history:

Table 1 Online Change History

Part Number	Revision	Release	Date	Description
OL-30571-01	A0	1.0	October 7, 2013	Created release notes for Cisco Extensible Network Controller, Release 1.0.
	B0	1.5	February 24, 2014	Updated release notes for Cisco Extensible Network Controller, Release 1.5.

Introduction

The Cisco XNC provides automation and orchestration of the network fabric, and allows dynamic, application-based configuration of networks and services. Cisco XNC enables programmability of the network using the Software Defined Networking (SDN) approach.

Cisco XNC is based on OpenDaylight and is built for extensibility using the Java Open Services Gateway initiative (OSGi) framework. This framework provides the flexibility needed for Cisco and Cisco partners and customers to extend the functions of the controller based on business needs. Cisco XNC also provides northbound Representational State Transfer (REST) APIs for business applications to access and program policies.

Cisco XNC has the capability to support multiple protocols to communicate with the devices. In Release 1.5, Cisco XNC supports OpenFlow version 1.0 and Cisco One Platform Kit (onePK) SDK version 1.1.

Note Not all service sets or onePK APIs are supported in the current onePK protocol plugin.

Scale Information

Table 2 lists the scale limits for Cisco XNC:

Table 2 Scale Limits

Description	Small	Medium	Large
Number of Devices	100	300	500
Number of TIF Policies	400	2000	4000
Number of Slices	25	100	200
Number of Proactive Flows	10,000	50,000	100,000

System Requirements

Table 3 lists the system requirements for Cisco XNC:

Table 3 System Requirements per Deployment Size

Description	Small	Medium	Large
CPUs (virtual or physical)	6-core	12-core	18-core
Memory	8 GB RAM	16 GB RAM	24 GB RAM
Hard disk	Minimum of 40 GB of free space available on the partition on which the Cisco XNC software is installed.		
Operating System	A recent 64-bit Linux distribution that supports Java, preferably Ubuntu, Fedora, or Red Hat.		
Other	Java Virtual Machine 1.7 or later. Python 2.7.3 to support the backup and restore script.		

Supported Web Browsers

The following web browsers are supported for Cisco XNC:

- Firefox 18.x and later versions
- Chrome 24.x and later versions

Note Javascript 1.5 or a later version must be enabled in your browser.

New Software Features

New Software Features in Release 1.5

Release 1.5 adds support for the following software features:

- Support for running the Cisco XNC Monitor Manager application within the Cisco Nexus 3000 or 3100 Series switches for single switch deployment (Monitor Manager Embedded).
- Availability of Cisco One Platform Kit (onePK) protocol plugin*

Note Not all service sets or onePK APIs are supported in the current onePK protocol plugin.

- Support for Tomcat tuning.
- CLI framework for XNC administration.
- REST API support for Monitor Manager application roles and groups.
- IPv6 support within Monitor Manager applications.
- GUI topology and usability enhancements, including editing capabilities for all policies, filters and rules within Cisco XNC and XNC applications.

- Dot1q support (QinQ) for Monitor Manager application edge port VLAN frame tagging.
- Felix console integration to manage osgi bundles.
- Manual consistency check and fix.
- VLAN support within flow specs.
- Support for TIF rule installation on pure onePK nodes.
- Support for deny rules, bidirectional filters, and other rule and filter enhancements in Monitor Manager application.

Release 1.5 adds support for the following application:

- Virtual Patch Panel Application (P2P Forwarding application)—provides port-to-port traffic management within a switch or across the network without any need for physical connection changes or rewiring.

New Software Features in Release 1.0

Release 1.0 supports the following software features:

- Extensible, modular architecture—modules can be added, updated, or deleted without restarting the Cisco XNC application. The architecture allows Cisco XNC functions to be extended using Java. The Service Abstraction Layer (SAL) enables extensible southbound interface support beyond OpenFlow.
- Multiple access methods and controls—management access is available through the built-in GUI or through Java APIs or REST APIs. Security features include role-based access control (RBAC), integration with enterprise authentication, authorization, and accounting (AAA), and secure control protocols.
- Network visibility and troubleshooting—there are functions to support network topology discovery, network device management and forwarding rules programming, and access to detailed network statistics. Troubleshooting tools provide flow-level visibility for each device.
- High availability through clustering—multiple instances can be deployed in an active-active model. The active-active deployment model makes the controller both highly available and scalable. Synchronization of information and state across all controllers is provided in real time, which helps prevent loss of information in the event of a failure.
- Multiprotocol support—multiprotocol interface support allows OpenFlow 1.0 to communicate with devices. This support enables business applications to extend their use cases transparently across a multivendor network.

Release 1.0 provides the following applications:

- Monitor Manager application—applies the SDN approach to provide visibility into the network traffic.
- Network Slicing application—provides the capability to partition the network based on physical or logical (flow) criteria.
- Topology Independent Forwarding (TIF) application—provides the capability to define the forwarding path in the network based on application requirements.

Resolved Caveats

The following caveats were resolved in Release 1.5:

Table 4 Resolved Caveats in Release 1.5

Defect ID	Symptom	Found in Release:	Resolved in Release:
CSCum10670	In the XNC Monitor Manager application, all switches are now visible in the **Select Source Node** list when you apply a filter using the **Add Rule** dialog box.	1.0	1.5
CSCuj66859	The Cisco XNC backup script no longer outputs the incorrect filename to the console when it is run.	1.0	1.5
CSCug87845	The **Apply Filter** tab on the Cisco XNC GUI now displays color-coded table rows to show the status of the installation.	1.0	1.5

Open Caveats

The following caveats are open in Release 1.5:

Table 5 Open Caveats in Release 1.5

Defect ID	Symptom	Workaround
CSCun31902	When flows are added to a switch because of the TIF policies in a particular slice, the flows are not deleted when you delete the slice.	In the **Troubleshoot** tab, choose the **Flow Check** tab. For each switch on the slice, select the switch in the **Select a node** drop-down list, click **Inconsistent Node Flows**, then click **Fix Inconsistent Flows**.
CSCun06580	Traffic loss might be seen if you bring down one controller that is part of an HA cluster.	There is no workaround for this issue.
CSCul92372	If you remove the QinQ VLAN setting from an edge port in Monitor Manager, and then toggle the connection with a onePK client, the setting remains present and active on the switch interface.	In the Monitor Manager GUI, remove the QinQ VLAN setting, then add the QinQ VLAN setting, then remove it a second time.
CSCum86387	When six or more inter-switch links are present on the same switches, the individual links are hidden on the topology. This prevents you from adding a custom property to a particular link, or creating a custom path in TIF Manager.	Use the northbound REST APIs to add custom properties. There currently is no workaround to create custom paths for more than 5 inter-switch links.
CSCum81294	Running the Cisco XNC, Cisco Monitor Manager, and Cisco P2P Forwarding applications in different tabs in the same Firefox browser might cause Firefox to crash.	Use the Chromium or Google Chrome browser.
CSCum24979	Using the REST API to configure Point-to-Multipoint (P2MP) forwarding path options in Cisco Monitor Manager fails with the following error: `Can not deserialize instance of java.util.HashSet out of VALUE_STRING token`	Use the GUI to configure P2MP forwarding path options in Cisco Monitor Manager.
CSCum61509	Existing edge ports in rules cannot be modified.	Create a new rule with the modified edge port and delete the previous one.

Table 5 Open Caveats in Release 1.5

Defect ID	Symptom	Workaround
CSCuj26104	Custom paths cannot be created using northbound APIs.	Use the GUI to create custom paths.
CSCum44054	Static flow entries cannot be modified when using onePK.	Create a new static flow entry with the changes that you want to make and delete the previous one.
CSCul56895	If you start the Cisco Monitor Manager application immediately after upgrade, the browser may be directed to http://<ip_address>:8080/monitor/j_security_check and you may see a 404 error.	Perform the following: • Wait until the controller has fully initialized before accessing the GUI. • Clear your browser cache and cookies. • Remove "j_security_check" from the URL.
CSCuj39532	When using HA clustering, if the current coordinator is brought down at the same time that a new node is brought up, the caches may stop syncing.	Do not stop the cluster coordinator and bring up a new node at the same time.
CSCum54358	Configuring a static flow with 5 parameter matches with the set Source MAC Address or set Destination MAC Address action fails when using onePK to communicate between the controller and the network device. You will see the following error: **`Caught exception while adding action fields for flow`**	There is no workaround for this issue. The set Source MAC Address and set Destination MAC Address actions are not supported with onePK.
CSCum54401	Configuring a static flow with 5 parameter matches with the set VLAN ID action fails when using onePK to communicate between the controller and the network device. You will see the following error: **`Caught exception while adding action fields for flow`**	There is no workaround for this issue. The set VLAN ID action is not supported with onePK.
CSCum54799	Configuring a static flow with 5 parameter matches with the set VLAN priority action fails when using onePK to communicate between the controller and the network device. You will see the following error: **`Caught exception while adding action fields for flow`**	There is no workaround for this issue. The set VLAN priority action is not supported with onePK.

The following caveats are open in Release 1.0:

Table 6 Open Caveats in Release 1.0

Defect ID	Symptom	Workaround
CSCuj66859	The Cisco XNC backup script outputs the incorrect filename to the console when it is run. The actual file output is **`xnc-`***`yy-mm-dd_time`***`.tar`**, but the script displays *`yy-mm-dd_time`***`.tar`**.	When you run the restore script, prepend the prefix **`xnc-`** before the filename. Resolved in Release 1.5.
CSCuj64658	Metrics configured using a northbound API for a custom property template of type 'string' are not visible in the Cisco XNC GUI.	In the **Network Properties** tab, click the custom property template, then click **Add Metric** to create a metric.
CSCuf56767	Existing flows and rules cannot be edited.	Delete the flow or rule that you want to change and create a new one.

Table 6 Open Caveats in Release 1.0

Defect ID	Symptom	Workaround
CSCuj42461	A user with the network administrator role cannot modify the password of another network administrator.	Run the `adminpasswordreset.sh` script to restore the network administrator password to the factory default.
CSCuj55054	If there is only one OpenFlow port on a supported Cisco Nexus 3000 switch, which is used as either an input or output port, and that port is changed to a non-OpenFlow port or is administratively shutdown, all rules are removed from the port, but the flows are reinstalled after the port is brought back up or changed back to an OpenFlow port. If there are additional ports on the flow used as output ports, however, the flow is uninstalled when the first port is shutdown or changed to a non-OpenFlow port.	This issue has no known workaround.
CSCug87845	You cannot configure rules if the switch does not have enough space to program and install the rule. The **Apply Filter** tab on the Cisco XNC GUI does not display that the rules are pending and not installed.	This issue has no known workaround. Do not program rules that exceed the switch capacity. Resolved in Release 1.5.

Known Limitations and Behaviors

The following known limitations and behaviors are not otherwise documented:

Table 7 Known Limitations in Release 1.0 and 1.5

Defect ID	Symptom	Workaround
CSCum94140	When a default metric is created using northbound REST APIs for a String-based child property template without any metrics, the default value is not displayed in the GUI.	This is a display issue only. To fix the issue: • Always add metric, then refer to that metric when adding default values using the Northbound REST API. • Always specify the name and factor when adding a String-based metric. If the factor is not used, set the value to zero.
CSCuj54980	After a Linux user with administrative or superuser privileges starts or stops Cisco XNC, any user with lesser privileges is not able to start or stop the controller.	Another Linux user with administrative or superuser privileges must perform one of the following: • Use the **chown -R** command to change the owner of all files owned by the admin or superuser to the current user. OR • Delete all files owned by the admin or superuser.

Related Documentation

For more information, see the related documents at the following link:

http://www.cisco.com/en/US/products/ps13400/tsd_products_support_series_home.html

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/en/US/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.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.