Cisco Extensible Network Controller Configuration Guide, Release 1.0

First Published: October 07, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-30522-01

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.

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.

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.

CONTENTS

Preface

CHAPTER 1

CHAPTER 2

CHAPTER 3

CHAPTER 4

Preface

This preface contains the following sections:

Audience

This publication is for experienced network administrators who configure and maintain Cisco Extensible Network Controller.

Document Conventions

Command descriptions use the following conventions:

Convention	Description
bold	Bold text indicates the commands and keywords that you enter literally as shown.
Italic	Italic text indicates arguments for which the user supplies the values.
[x]	Square brackets enclose an optional element (keyword or argument).
[x | y]	Square brackets enclosing keywords or arguments separated by a vertical bar indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a vertical bar indicate a required choice.

Convention	Description
[x {y | z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
`variable`	Indicates a variable for which you supply values, in context where italics cannot be used.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Examples use the following conventions:

Convention	Description
`screen font`	Terminal sessions and information the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
italic screen font	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Overview

This preface contains the following sections:

About Cisco Extensible Network Controller

Cisco Extensible Network Controller (Cisco XNC) is a software platform that serves as an interface between the network elements in one direction (southbound) and third-party applications (northbound). Cisco XNC is a JVM-based application that runs on a Java Virtual Machine (JVM). Cisco XNC is based on a highly available, scalable, and extensible architecture that supports a network. Cisco XNC is built for extensibility using the Open Services Gateway initiative (OSGi) framework, which allows new functionality to be added.

Cisco XNC can support multiple protocol plugins in the southbound direction. In the current release, OpenFlow version 1.0 is available.

Cisco XNC provides the following:

- Multiprotocol capability with OpenFlow version 1.0 available in this release.
- Functionality to support network visibility and programmability, such as network topology discovery, network device management, forwarding rules programming, and access to detailed network statistics.
- A Service Abstraction Layer (SAL) that enables modular southbound interface support, such as OpenFlow.
- Consistent management access through the GUI or through Java or Representational State Transfer (REST) northbound APIs.
- Security features, such as role-based access control (RBAC), and integration with an external Active Directory using RADIUS or TACACS for authentication, authorization, and accounting (AAA) functions.
- Troubleshooting tools, such as analytics gathering and diagnostic packet injection.
- Cisco advanced features such as Topology Independent Forwarding (TIF), which enables the administrator to customize the path a data flow takes through the network.

- Cisco network applications such as Network Slicing that allows logical partitioning of the network using flow specification.
- High-availability clustering to provide scalability and high availability.

Cisco XNC GUI Overview

The Cisco XNC GUI contains the following areas and panes:

- A menu bar across the top of the window that provides access to the main categories of information in Cisco XNC.
- A topology map on the right that displays a visual representation of your network.
- Several panes with additional views and information on the selected category.

The menu bar contains the following items:

- The **Devices** tab—Provides access to the Cisco XNC network elements.
- The **Flows** tab—Provides access to flow entries and flow details.
- The **Troubleshoot** tab—Provides information about flows, ports, and policies for troubleshooting purposes.
- The **TIF Manager** tab—Provides access to paths and policies for Topology Independent Forwarding (TIF).
- The **Network Properties** tab—Provides access to property templates.
- The Slicing list—Provides access to different slices, and lists the current slice you are in. If no slices are created, or you have not selected a slice, the **default** drop-down list is displayed.

  Note You must have an administrative role and the Network Slicing application to view this list.

- The Online help button—Provides access to the online help for the current page.
- The administrative management list—Provides access to different administrative tasks, such as saving or managing users.

  Note The drop-down list displays the username that you used when you logged into Cisco XNC. In this documentation, this will be referred to as the **Admin** drop-down list.

Note Depending on the Cisco XNC applications that you have installed, the items on the menu bar may vary.

Using the Topology Diagram

The topology diagram displays a graphical view of your network. Once a device or link has been recognized by Cisco XNC, it is visible in the topology diagram. On all tabs in Cisco XNC, you can perform the following tasks:

- Hover over a switch to view the node name, the source ports, and the destination ports.
- Hover over a link to view the source and destination port of that link.
- Use the + and - keys to change the zoom level.
- Click and drag a switch to move it to a different location.
- Click and drag the background to move the entire topology to a different location.

Certain tabs also allow advanced tasks.

Saving Configuration Changes

You should periodically save the configuration changes that you make in Cisco XNC.

Note Any unsaved configuration changes will be lost if you stop the Cisco XNC application.

Step 1 On the Cisco XNC menu bar, click the **Admin** drop-down list.

Step 2 Choose **Save**.

CHAPTER 2

Managing Devices

This chapter contains the following sections:

Adding a Node Name

Adding user-friendly node names will help you to identify nodes in the topology diagram.

Step 1 On the Cisco XNC menu bar, click **Devices**.

Step 2 On the **Nodes Learned** tab, click the link for the node that you want to rename in the **Node Name** column.

Step 3 In the **Update Node Information** dialog box, complete the following fields:

Name	Description
Node ID field	The unique identifier for a network element, such as an OpenFlow switch.
Node Name field	The name that you want to assign to the node. This name can be between 1 and 100 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.

Name	Description
Tier drop-down list	Assign the tier property for the network element. This can be one of the following: • **Unknown** • **Access** • **Distribution** • **Core**
Operation Mode drop-down list	Choose how the traffic is handled based on the flows. This can be one of the following: • **Allow reactive forwarding—**No default flows are programmed. How traffic that does not match a flow is treated depends upon the switch implementation. • **Proactive forwarding only—**The following default flows are programmed on the switch: ◦ Punt ARP packets to Cisco XNC. ◦ Punt LLDP packets to Cisco XNC. ◦ Drop all other traffic.

Step 4 Click **Save**.

Viewing Expanded Nodes Information

Step 1 On the Cisco XNC menu bar, click **Devices**.

Step 2 On the **Nodes Learned** tab, click the icon in the top right corner.

Step 3 The **Nodes Learned** dialog box displays the following fields:

Name	Description
Node Name field	The name assigned to the node.
Node ID field	The ID of the node.
Tier Name field	The tier that you selected for the node.

Name	Description
MAC field	The MAC address of the node.
Ports field	The ports accessible on the node.

Step 4 Close the dialog box.

Viewing the Ports List

Step 1 On the Cisco XNC menu bar, click **Devices**.

Step 2 On the **Nodes Learned** tab, click the **Ports** link for a node.

Step 3 The **Ports List** dialog box displays all of the ports for the specified node.

Step 4 Close the dialog box.

Adding a Static Route

Step 1 On the Cisco XNC menu bar, click **Devices**.

Step 2 On the **Static Route Configuration** tab, click **Add Static Route**.

Step 3 In the **Add Static Route** dialog box, complete the following fields:

Name	Description
Name field	The name that you want to assign to the static route. This name can be between 1 and 100 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Static Route field	The IP address of the destination and subnet mask in the following format: *Destination_IP_Address/Subnet_Mask*
Next Hop field	The IP address of the next-hop device.

Step 4 Click **Save**.

Adding a Gateway IP Address

Step 1 On the Cisco XNC menu bar, click **Devices**.

Step 2 On the **Subnet Gateway Configuration** tab, click **Add Gateway IP Address**.

Step 3 In the **Add Gateway IP Address** dialog box, complete the following fields:

Name	Description
Name field	The name that you want to assign to the gateway IP address. This name can be between 1 and 100 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Gateway IP Address/Mask field	The IP address and subnet mask of the default gateway in the following format: *IP_Address/Subnet_Mask* **Note** • If your deployment includes only OpenFlow traffic, the Gateway IP Address can be set to the same IP address used as the default gateway for the host systems on that subnet. • If your deployment includes OpenFlow and non-OpenFlow traffic, the Gateway IP Address must be set to an unused IP address on that subnet.

Step 4 Click **Save**.

Adding Ports

Step 1 On the Cisco XNC menu bar, click **Devices**.

Step 2 On the **Subnet Gateway Configuration** tab, click **Add Ports**.

Step 3 In the **Add Ports** dialog box, complete the following fields:

Name	Description
Gateway Name field	The name of the gateway address to which you want to bind the port.

Name	Description
Node ID field	The node that contains the port that you want to bind to the gateway address.
Select Port field	The port that you want to bind to the gateway address.

Step 4 Click **Save**.

Adding a SPAN Port

Step 1 On the Cisco XNC menu bar, click **Devices**.

Step 2 In the work area, click the **Span Port Configuration** tab and click **Add SPAN Port**.

Step 3 In the **Add SPAN Port** dialog box, complete the following fields:

Name	Description
Node drop-down list	Choose the node where you want to create a SPAN port.
Input Port field	The input port to use for the SPAN port.

Step 4 Click **Save**.

CHAPTER 3

Managing Flows

This chapter contains the following sections:

About Flow Programming

With Cisco XNC, you can configure individual flows in each network device. Flows are identified based on Layer 1 through Layer 4 criteria. After the flow is identified, you can specify the actions to be performed on the packets that match the flow specification. The criteria for matching and actions varies depending upon the switch. Possible actions are as follows:

- Dropping or forwarding the packet to one or more interfaces.
- Setting the VLAN ID and priority of the packets.
- Modifying the source and destination MAC address of the packets.
- Modifying the source and destination IP address of the packets.

All flows that you create are listed in the **Flow Entries** table on the **Flows** tab. Flows become active when you install them in the device.

Adding a Flow Entry

Step 1 On the Cisco XNC menu bar, click **Flows**.

Step 2 On the **Flow Entries** tab, click **Add Flow Entry**.

Step 3 In the **Flow Description** area of the **Add Flow Entry** dialog box, complete the following fields:

Name	Description
Name field	The name that you want to assign to the flow. This name can be between 1 and 100 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Node drop-down list	Choose the ID or node name for the device.
Input Port drop-down list	Choose the port on the node where traffic enters the flow.
Priority field	The priority that you want to apply to the flow. The default priority is 500. Flows with a higher priority are given precedence over flows with a lower priority. **Note** The priority is considered only when all of the Layer 2, Layer 3, and Layer 4 match fields are equal.
Hard Timeout field	The amount of time in milliseconds for the flow to be installed before it is removed from the flow table.
Idle Timeout field	The amount of time in milliseconds that the flow can be idle before it is removed from the flow table.
Cookie field	An identifier added to the flow. Cookies are specified by the controller when the flow is installed and are returned as part of each flow status and flow expired message.

Step 4 In the **Layer 2** area, complete the following fields:

Name	Description
Ethernet Type field	Required. The Ethernet type of the Layer 2 traffic. The default value is IPv4.
VLAN Identification Number field	The VLAN ID for the Layer 2 traffic.
VLAN Priority field	The VLAN priority for the Layer 2 traffic.
Source MAC Address field	The source MAC address of the Layer 2 traffic.
Destination MAC Address field	The destination MAC address of the Layer 2 traffic.

Step 5 In the **Layer 3** area, complete the following fields:

Name	Description
Source IP Address field	The source IP address of the Layer 3 traffic.

Name	Description
Destination IP Address field	The destination IP address of the Layer 3 traffic.
Protocol field	The Internet protocol of the Layer 3 traffic. Enter the IP protocol number in decimal, hex, or octal format.
ToS Bits field	The Type of Service (ToS) bits in the IP header of the Layer 3 traffic. **Note** Only the DSCP bits are supported on Cisco Nexus 3000 Series switches.

Step 6 In the **Layer 4** area, complete the following fields:

Name	Description
Source Port field	The source port of the Layer 4 traffic.
Destination Port field	The destination port of the Layer 4 traffic.

Step 7 In the **Actions** area, select one or more actions:

- Drop
- Loopback
- Flood
- Software Path
- Hardware Path
- Controller
- Add Output Ports
- Set VLAN ID
- Set VLAN Priority
- Strip VLAN Header
- Modify Datalayer Source Address
- Modify Datalayer Destination Address
- Modify Network Source Address
- Modify Network Destination Address
- Modify ToS Bits
- Modify Transport Source Port
- Modify Transport Destination Port

Step 8 Click **Install Flow** to install the flow into the device.

Step 9 Click **Save Flow** to save the flow to the **Flow Entries** table but not to install the flow in the flow table of the device.

Viewing Flow Details

Step 1 On the Cisco XNC menu bar, click **Flows**.

Step 2 In the **Flow Entries** tab, locate the flow that you want to view.
Enter a value in the **Search** combo box and click the search icon to limit the number of entries that appear.

Step 3 In the **Flow Overview** area of the **Flow Detail** tab, perform one of the following tasks:

- Click **Remove Flow** to remove the flow from the **Flow Entries** table.
- Click **Install Flow** to install the flow into the flow table of the device.
- Click **Uninstall Flow** to remove the flow from the flow table of the device.

CHAPTER 4

Using TIF Manager

This chapter contains the following sections:

About TIF Manager

With the Topology Independent Forwarding (TIF) Manager, you can customize the path a data flow takes through the network. TIF Manager can also be invoked by any network-aware business application that communicates with Cisco XNC using REST APIs.

Creating a TIF Policy

The Topology Independent Forwarding (TIF) Manager allows you to create paths between hosts and devices.

Step 1 On the Cisco XNC menu bar, click **TIF Manager**.

Step 2 In the **TIF Policies** tab, click **Create TIF Policy**.

Step 3 In the **Create TIF Policy** dialog box, complete the following fields.

Name	Description
Name field	The name that you want to assign to the path. This name can be between 1 and 100 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Source IP field	The source IP address of the host.
Destination IP field	The destination IP address of the host.

Name	Description
Protocol drop-down list	Choose the protocol to be used for the path. This can be one of the following: • **any—**All protocols will be used. • **ICMP—**Only the ICMP protocol will be used. • **TCP—**Only the TCP protocol will be used. • **UDP—**Only the UDP protocol will be used. • **IPv6-ICMP—**Only the IPv6-ICMP protocol will be used.
Source Port field	The transport layer port number. If no source port is specified, any ports can be used.
Destination Port field	The destination port. If no destination port is specified, any ports can be used.
Path Type field	How the traffic will be routed between the source and destination IP. Click **Properties** to choose a property from one of the following categories: • Latency • Number • Bandwidth • String **Note** Any custom property templates created on the **Network Properties** will also be displayed in this list. Click the **Custom Path** radio button to choose an existing path from a drop-down list.

Step 4 Click **Create TIF Policy**.

Creating a Custom Path

Step 1 On the Cisco XNC menu bar, click **TIF Manager**.

Step 2 In the topology diagram, click the links that you want to include in the path.

Step 3 Click **Save Custom Path** to save the path to the **Existing Custom Paths** table.

CHAPTER 5

Troubleshooting

This chapter contains the following sections:

About Troubleshooting

Cisco XNC includes a variety of tools that you can use to troubleshoot your network connections. From the **Troubleshoot** tab, you can do the following:

- View all of the nodes in the network.
- View detailed information about the ports for each node in the network.
- View detailed information about the flows for each node in the network.
- View when the nodes were discovered by Cisco XNC in the **Uptime** tab.
- View detailed information about TIF policies in the **Policy Analyzer** tab.
- Run analytics on selected flows and TIF policies.

Viewing Flow and Port Detail Statistics

Step 1 On the Cisco XNC menu bar, click **Troubleshoot**.

Step 2 In the **Existing Nodes** tab, locate the node for which you want to view statistics.
Enter a value in the **Search** combo box and click the search icon to limit the number of entries that appear.

Step 3 Perform one of the following tasks:

- Click **Flows** to view detailed information on all flows programmed on the node.
- Click **Ports** to view detailed information on all ports of the node.

Note The statistics are updated every 160 seconds.

Policy Analyzer

The Policy Analyzer allows you to view detailed information about TIF policies. You can use the Policy Analyzer to perform the following tasks:

- Monitor selected flows.
- Run SDN trace against a flow.
- View the status of the last SDN trace.
- View aggregated statistics for the TIF policy.

Using the Policy Analyzer

Step 1 On the Cisco XNC menu bar, click **Troubleshoot**.

Step 2 In the **Policies** tab, choose the TIF policy that you want to analyze.
Enter a value in the **Search** combo box and click the search icon to limit the number of entries that appear.

Step 3 To monitor the TIF policy flows, perform the following tasks:

a) Check the check box for one or more flows.
b) Click **Start Monitor**.
c) When you have finished collecting flow data, click **Stop Monitor**.

Step 4 To run an SDN trace on a TIF policy flow, perform the following tasks:

a) Check the check box for the flow that you want to trace.
b) Click **SDN Trace**.

Step 5 Click **SDN Trace Status** to view the information from the last SDN trace that was run.

Step 6 Click **Policy Statistics** to view statistics for the selected TIF policy.

SDN Analyzer

The SDN Analyzer downloads packet capture (pcap) files for the interface that you select. The individual pcap files are consolidated into one zip file.

By default, the SDN Analyzer captures 5 pcap files with 100 MB of network data each. If more than the set amount of data is captured, the earlier data is overwritten. You can change the amount of data collected in the config.ini file.

Using the SDN Analyzer

The SDN Analyzer captures packets that come to Cisco XNC and outputs the results to a zip file. The location of the zip file depends upon your browser settings.

Before You Begin

You must have root privileges on the server that is running Cisco XNC to run the SDN Analyzer.

Step 1 On the Cisco XNC menu bar, click **Troubleshoot**.

Step 2 In the **SDN Analyzer** tab, click the interface that you want to view.

Step 3 Click **Start Analyzer**.

Step 4 When you have finished collecting data, click **Stop Analyzer**.

Changing the Default Values for the SDN Analyzer

Step 1 Navigate to the `xnc/configuration` directory that was created when you installed the software.

Step 2 Use any text editor to open the `config.ini` file.

Step 3 Locate the following parameters:

- troubleshoot.fileSize = 100
- troubleshoot.number = 5

Step 4 Change the files as appropriate. We recommend using a file size of no more than 100 MG, and increasing the number of pcap files.

Step 5 Save the file and exit the editor.

Step 6 Restart Cisco XNC.

CHAPTER 6

Managing Properties

This chapter contains the following sections:

About Network Properties

The **Network Properties** tab allows you to create your own properties that you can use to configure your TIF policies.

Default Properties

Cisco XNC provides the following properties by default:

- Latency
- Number
- Bandwidth
- String

Each property contains one or more policies. For example, the Number property contains policies that are related to numbers, such as weighted least cost path, or hop count based shortest path. The Bandwidth policy contains policies related to bandwidth, such as including or avoiding links with a specific bandwith.

Many of the policies also contain metrics that further define the property. The latency properties, for example, include time-based metrics. You could use a latency property with a policy to include only those links that have latency less than 1 nanosecond.

Custom Properties

You can create custom property templates based on an existing template. After you have created a custom property template, you can rename the policies that are associated with that template, create metrics for the template, and use that template as a parent to create additional templates. The custom properties can be used when you create TIF policies.

Manual Links

Create manual links if you have links that have not been discovered by Cisco XNC.

Adding a Link Property

Link properties use the values of both custom and default property templates.

Step 1 On the Cisco XNC menu bar, click **Topology**.

Step 2 In the topology diagram, click the link for which you want to set properties.

Step 3 In the **Properties** tab, click **Add Property**.

Step 4 In the **Add Property** dialog box, complete the following fields:

Name	Description
Property drop-down list	Choose the property that you want to add to the link.
Metric drop-down list	Choose the metric that you want to add to the link.
Value field	The value for the metric that you want to use for the link.

Step 5 Click **Add Property**.

Adding a Property Template

Step 1 On the Cisco XNC menu bar, click **Topology**.

Step 2 In the **Templates** tab, click **Add Template**.

Step 3 In the **Add Property Template** dialog box, complete the following fields:

Name	Description
Name field	The name that you want to assign to the property template This name can be between 1 and 100 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Parent drop-down list	Choose the parent template to use for the custom template.

Step 4 Click **Add Template**.

Changing Policy Names for a Custom Property Template

You can change the policy names for custom property templates. Policies that belong to default property templates cannot be changed.

Step 1 On the Cisco XNC menu bar, click **Topology**.

Step 2 In the **Templates** tab, in the **Property Templates** table, click the Parent column for the custom property for which you want to change policy names.

Step 3 In the **Policies** tab, click the policy name that you want to change.

Step 4 In the **Change Policy Name** dialog box, enter the new policy name.

Step 5 Click **Submit**.

Adding Metrics to a Custom Property Template

You can add metrics to any custom property template.

Step 1 On the Cisco XNC menu bar, click **Topology**.

Step 2 In the **Templates** tab, in the **Property Templates** table, click the Parent column for the custom property for which you want to add metrics.

Step 3 In the **Properties** tab, click **Add Metric**.

Step 4 In the **Add Metrics** dialog box, complete the following fields:

Name	Description
Metric Name field	The name to be used for the metric.

Name	Description
Factor field	The factor to be used for the metric.
Default Value field	The optional default value to be used for the metric.

Step 5 Click **Add Metric**.

Editing Custom Metrics

You can edit metrics that belong to a custom property template. You cannot edit default metrics.

Step 1 On the Cisco XNC menu bar, click **Topology**.

Step 2 In the **Templates** tab, in the **Property Templates** table, click the Parent column for the custom property for which you want to edit the metrics.

Step 3 In the **Properties** tab, click the metric that you want to edit.

Step 4 In the **Add Metrics** dialog box, you can do the following:

- Enter a default value and click **Set Default Value**.
- Click **Remove Metric** to delete the metric.
- Click **Cancel** to close the dialog box without making any changes.

Creating a Manual Link

Note You should create manual links only if undiscovered links are in the topology.

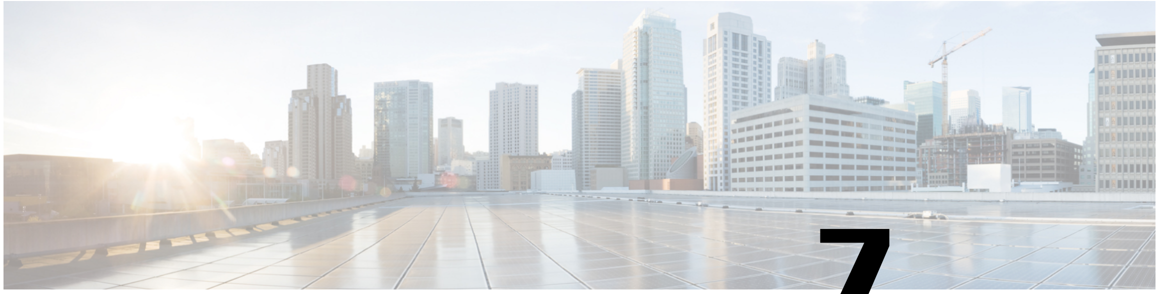
Step 1 On the Cisco XNC menu bar, click **Network Properties**.

Step 2 On the **Manual Links** tab, click **Create Link**.

Step 3 In the **Create Link** dialog box, complete the following fields:

Name	Description
Name field	The name that you want to assign to the link. This name can be between 1 and 100 alphanumeric characters. You cannot use spaces or any special characters, and you cannot change this name after the object has been saved.
Source Node drop-down list	Choose the source node for the link.
Source Port drop-down list	Choose the source port on the selected node.
Destination Node drop-down list	Choose the destination node for the link.
Destination Port drop-down list	Choose the destination port on the selected node.

Step 4 Click **Create Link**.



CHAPTER 7

Managing Slices

This chapter contains the following sections:

About Slice Manager

The Slice Manager provides a way for you, as a network administrator, to partition networks into many logical networks. Each logical network can be assigned to departments, groups of individuals, or applications. The Slice Manager creates slices based on the following criteria:

- Network devices—The devices that can be used in the slice.

  Network devices can be shared between slices.

- Network device interfaces—The device interfaces that can be used in the slice.

  Network device interfaces can be shared between slices.

- Flow Specification—A combination of source and destination IP, protocol, and source and destination transport port used to identify the traffic that belongs to the slice.

  Flow specs can be assigned to different slices if the associated network devices and interfaces are disjoint.

Note You can also use VLAN IDs to segregate the slice traffic.

Slices must be created by a Cisco XNC user with the Network Administrator role. After creation, the slices can be managed by a user with the Slice Administrator role.

Slices can overlap provided each slice has at least one unique attribute. For example, a slice can share the same physical switches and ports, but be differentiated by the type of traffic it receives.

Adding a Slice

Step 1 On the **Admin** drop-down list, choose **Slices**.

Step 2 From the **Slices** tab, click **Add Slice**.

Step 3 In the **Add Slice** dialog box, complete the following fields:

Name	Description
Slice Name field	The name that you want to assign to the slice.
Static VLAN field	The static VLAN that you want to assign to the slice.

Step 4 Click **Add Slice**.

Adding Nodes and Ports to a Slice

Before You Begin

You must have created a slice before you can add nodes and ports.

Step 1 On the **Admin** drop-down list, choose **Slices**.

Step 2 On the **Slices** tab, choose the slice for which you want to add entries.
Enter a value in the **Search** combo box and click the search icon to limit the number of entries that appear.

Step 3 In the topology diagram, click a node that you want to add to the slice.

Step 4 In the **Add Slice Entry** dialog box, choose the port or ports that you want to add to the slice.

Step 5 Click **Add Entry**.

Step 6 Repeat Step 3 through Step 5 for each node and port that you want to add to the slice.

Adding a Flow Specification

Before You Begin

You must have created a slice before you can add a flow specification.

Step 1 On the **Admin** drop-down list, choose **Slices**.

Step 2 On the **Flow Spec** tab, choose the slice for which you want to add a flow specification.
Enter a value in the **Search** combo box and click the search icon to limit the number of entries that appear.

Step 3 On the **Detail** tab, click **Add Flow Spec**.

Step 4 In the **Add Flow Spec** dialog box, complete the following fields:

Name	Description
Name field	The name that you want to use for the flow spec.
Source IP field	The source IP address that you want to use for the flow spec.
Destination IP field	The destination IP address that you want to use for the flow spec.
Protocol field	The IP protocol number in decimal format that you want to use for the flow spec.
Source Port field	The source port that you want to use for the flow spec.
Destination Port field	The destination port that you want to use for the flow spec.

Step 5 Click **Add Flow Spec**.

CHAPTER 8

Administrative Tasks

This chapter contains the following sections:

About AAA Servers

AAA enables the security appliance to determine who the user is (authentication), what the user can do (authorization), and what the user did (accounting). Cisco XNC uses Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) to communicate with a AAA server.

Remote authentication and authorization is supported using the AAA server. For each user to be authenticated, Cisco XNC uses both the login credentials and an attribute-value (AV) pair that assigns the authorized role for the user is configured as part of the user administration. After successful authentication, the Cisco AV pair is returned to Cisco XNC for resource access authorization.

Adding a AAA Server

Step 1 On the **Admin** drop-down list, choose **AAA**.

Step 2 In the **AAA Configuration** dialog box, click **Add Server**.

Step 3 In the **Add AAA Server** dialog box, complete the following fields:

Name	Description
Server Address field	The IP address of the AAA server.
Server Secret field	The password for the AAA server.

Name	Description
Protocol drop-down list	Choose the protocol for the AAA server. This can be one of the following: • **Radius+** • **TACACS+**

Step 4 Click **Save**.

Viewing a AAA Server

Step 1 On the **Admin** drop-down list, choose **AAA**.

Step 2 In the **AAA Configuration** dialog box, click a **Server Address**.

Step 3 After viewing the server information in the **Remove AAA Configuration** dialog box, click **Close.**

Step 4 In the **AAA Configuration** dialog box, click **Close.**

Deleting a AAA Server

Step 1 On the **Admin** drop-down list, choose **AAA**.

Step 2 In the **AAA Configuration** dialog box, click a **Server Address**.

Step 3 In the **Remove AAA Configuration** dialog box, click **Remove.**

Step 4 In the **AAA Configuration** dialog box, click **Close.**

Users and Roles

Cisco XNC uses users and roles to manage user access. You can assign more than one role to a user. This can be one of the following:

- **Network Administrator—**Provides full administrative privileges to all Cisco XNC applications.
- **Network Operator—**Provides read-only privileges to the specified Cisco XNC applications.
- **Application User—**Provides privileges that are defined in the specified application.

- **Slice User**—Provides access to a specified slice.

Each user is assigned a role, which determines the permissions that they have. Slice users are assigned to both a role and a slice. The Admin user with the Network Administrator role is created by default when you install Cisco XNC.

Viewing User Information

Step 1 On the **Admin** drop-down list, choose **Users**.

Step 2 In the **User Management** dialog box you can do the following:

- View a list of usernames and the roles assigned to each user.
- Click an existing user to delete the user or change the password for the user.
- Click **Add User** to create a new user.

Step 3 When you are finished, click **Close**.

Adding a User

After creating a user, you can change the password, but you cannot change the roles assigned to the user.

Step 1 On the **Admin** drop-down list, choose **Users**.

Step 2 In the **User Management** dialog box, click **Add User**.

Step 3 In the **Add User** dialog box, complete the following fields:

Name	Description
Username field	The name that you want to assign to the user.
Password field	The password for the user.

Name	Description
Choose Role(s) drop-down list	Choose the role that you want to assign to the user. You can assign more than one role. This can be one of the following: • **Network Administrator—**Provides full administrative privileges to all Cisco XNC applications. • **Network Operator—**Provides read-only privileges to the specified Cisco XNC applications. • **Application User—**Provides privileges that are defined in the specified application. • **Slice User—**Provides access to a specified slice.
Role Name field	If you chose **Application User**, enter the name that you want to assign to the role.
Slices drop-down list	If you chose **Slice User**, choose the slice that you want to assign to the user.
Slice Role drop-down list	If you chose **Slice User**, choose the role that you want to assign to the user. This can be one of the following: • **Administrator—**Provides full administrative privileges to the specified slice. • **Operator—**Provides read-only privileges to the specified slice.
Assign button	Assigns a role to the user.

Step 4 Click **Add User**.

Step 5 In the **User Management** dialog box, click **Close.**

Changing the Password for an Existing User

Step 1 On the **Admin** drop-down list, choose **Users**.

Step 2 In the **User Management** dialog box, click on the user that you want to modify.

Step 3 In the **Edit User** dialog box, click **Change Password**.

Step 4 In the **Change Password** dialog box, enter the new password and then enter it a second time to verify.

Step 5 Click **Submit**.

Step 6 In the **User Management** dialog box, click **Close**.

Deleting a User

If you are signed in as a particular user, you cannot delete that user.

Step 1 On the **Admin** drop-down list, choose **Users**.

Step 2 In the **User Management** dialog box, click on the user that you want to modify.

Step 3 In the **Edit User** dialog box, click **Remove User**.

Step 4 In the **User Management** dialog box, click **Close**.

Viewing Cluster Management Information

Note The cluster management dialog boxes are read-only.

Before You Begin

You must have configured high availability clustering in order to view the cluster management information. See the *Cisco Extensible Network Controller Deployment Guide*.

Step 1 On the **Admin** drop-down list, choose **Clusters**.
The **Cluster Management** dialog box lists the IP addresses of all of the Cisco XNC instances in the cluster. Clusters can be denoted by one of the following icons:

- The ***** icon indicates the cluster node that is currently being viewed.
- The **C** icon indicates that the cluster node is the coordinator.

Step 2 In the **Cluster Management** dialog box, choose a cluster.
The **Connected Nodes** dialog box lists all of the nodes in the selected cluster.

Step 3 In the **Connected Nodes** dialog box, click **Close.**

Step 4 In the **Cluster Management** dialog box, click **Close.**