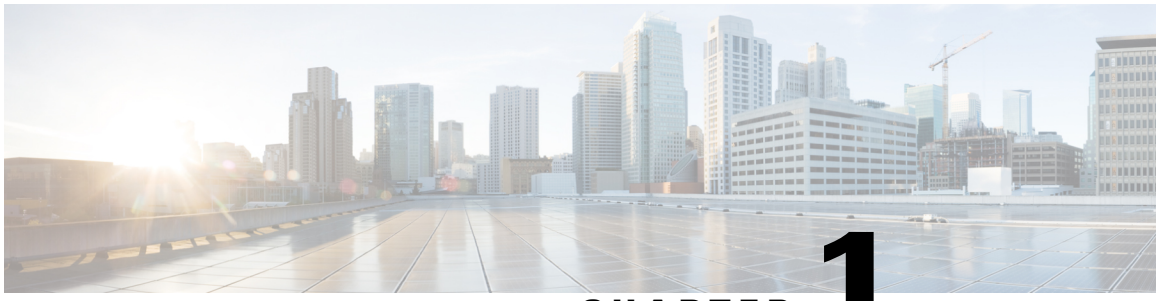
Cisco Extensible Network Controller Configuration Guide, Release 1.7

First Published: September 30, 2014

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

CONTENTS



CHAPTER 1

Overview

This preface contains the following sections:

About Cisco Extensible Network Controller

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

Cisco XNC can support multiple protocol plugins in the southbound direction. In Release 1.7, Cisco Plug-in for OpenFlow 1.0 and the Cisco One Platform Kit (onePK) 1.3.0 are supported.

Cisco XNC provides the following:

- Multiprotocol capability with the Cisco Plug-in for OpenFlow.
- 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, and Cisco Monitor Manager, which provides visibility into the network traffic.
- High-availability clustering to provide scalability and high availability.
- The Cisco Open Network Environment Platform Kit (Cisco onePK) version 1.3.0 is supported in Release 1.7 of Cisco XNC. The Cisco onePK plug-in communicates with the onePK agent.
- Support for onePK devices in the network and the ability to install TIF rules on onePK devices.
- A command line interface (CLI) framework for Cisco XNC.
- The Virtual Patch Panel Application (Port-to-Port Forwarding application) provides port-to-port traffic management within a switch or across the network without any need for physical connection changes or rewiring.
- Access to the Cisco XNC northbound API content from the application menu bar that enables you to view the API definitions and related calls.

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 about the selected category.

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

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 that you are in. If no slices have been configured, or you have not selected a configured slice, the **default** drop-down list is displayed.

Note You must have an administrative role to add, modify, or review the slices list.

- The **Online help** button—Provides access to the online help for the current page.

- A **Save** button—Enables you to save any additions or changes you make in the Cisco XNC application.
- A **Northbound API** button—Enables you to view northbound API content in a new browser tab, and displays the content and calls.
- The administrative management (**Admin**) drop-down list—Provides access to different administrative tasks, such as managing users, slices, network clusters, or viewing the OSGi components list.

Note The **Admin** drop-down list—Displays the username that you used when you logged into Cisco XNC.

Topology Tools

The left side of the **Topology** pane contains a group of tools that allow you to manipulate the content of the topology pane. Hovering over a tool displays its function. From the top of the pane to the bottom, the tools are as follows:

- Select node mode—Enables you to select one or more elements in the topology diagram. To select one or more elements, click on the first element and then drag your mouse across the diagram. The elements selected are highlighted with a circle around each one.
- Move mode—Moves the entire topology diagram, a single topology element, or a node group. To move an element or a node group, click it and drag it.
- Zoom in—Increases the size of the topology diagram.

Note You can also increase the size of the topology diagram by scrolling up with your mouse wheel.

- Zoom out—Decreases the size of the topology diagram.

Note You can also decrease the size of the topology diagram by scrolling down with your mouse wheel.

- Zoom by selection—Zooms in on a specific topology element. To zoom by selection, click the tool, and then click and drag your mouse across the element that you want to zoom in on. The zoom element display resets after a few seconds.
- Fit stage—Resets the topology diagram in that pane.
- Topology Settings—Choose the preferred **Display Icons as dots** setting. Click the radio button for the preference that you desire.
- Tool tips–Displays information about each tool or about nodes in the topology. To display tool tip information, hover over a tool or over a node in the diagram to display node information.

Pane Resizing

You can resize the panes in the GUI display by clicking the pane resize grippers as follows:

- To increase or decrease the height of either of the left or right bottom pane, click the pane resize grippers at the top of the pane, and then drag up or down with your mouse.
- To collapse either the lower right or lower left pane, hover over the pane resize grippers at the top of the pane until a double-ended arrow is displayed, and then click your mouse once.
- To restore a collapsed pane, hover over the pane resize grippers at the bottom of the pane until a double-ended arrow is displayed, and then click your mouse once.
- To increase or decrease the width of the two left panes at the same time, click the pane resize grippers at the top of the pane, and then drag left or right with your mouse.

Using the Topology Diagram

The topology diagram displays a graphical view of your network. After a device or link has been recognized by Cisco Extensible Network Controller (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 ports of that link.
- Hover over a tool to view the tool tip.
- Use the + (zoom in) or - (zoom out) tools, or move your mouse wheel up or down to change the zoom level.
- Click and drag a switch to move it to a different location.
- Click and drag a node group to move it to a different location.
- Click and drag the background to move the entire topology to a different location.

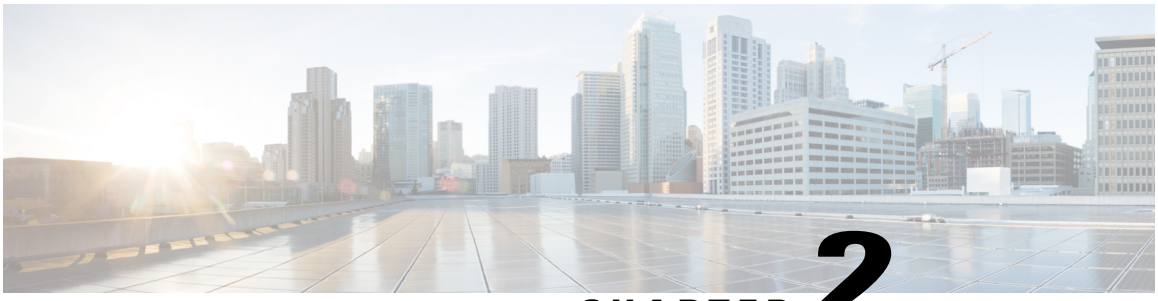
Certain tabs also allow advanced tasks.

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.

On the Cisco XNC menu bar, click the **Save** button.



CHAPTER 2

Managing Devices

This chapter contains the following sections:

Adding a Node Name

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

Step 1 On the menu bar, choose **Devices**, and then click the **Nodes Learned** tab.

Step 2 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. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").
Tier drop-down list	Choose 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 Address Resolution Protocol (ARP) packets. ◦ Punt Link Layer Discovery Protocol (LLDP) packets. ◦ Drop all other traffic.

Step 4 Click **Save**.

Viewing Expanded Nodes Information

Step 1 On the menu bar, choose **Devices**, and then click the **Nodes Learned** tab.

Step 2 Click the icon in the top right corner.

Step 3 The **Nodes Learned** dialog box displays these nonconfigurable 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.
MAC Address field	The MAC address of the node.
Ports field	The ports accessible on the node.

Step 4 Click the **X** in the upper right corner of the dialog box to close it.

Viewing the Ports List

Step 1 On the menu bar, choose **Devices**, and then click the **Nodes Learned** tab.

Step 2 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 Click the **X** in the upper right corner of the dialog box to close it.

Adding onePK Devices

Step 1 On the menu bar, choose **Devices**, and then click the **onePK** tab.

Step 2 Click **Add onePK Device**.

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

Name	Description
Address field	The IP address assigned to the Cisco onePK device.
Username field	The name of the user assigned to the device. **Note** The username that the admin enters in order to connect to the Cisco onePK agent.
Password field	The password of the user assigned to the device. **Note** This is the password that the admin enters in order to connect to the Cisco onePK agent.

Step 4 Click **Add onePK Device**.
The node configuration is added. When a physical device is associated with the address that you entered, a success message is displayed. The address is displayed in blue in the **Network Element Address** list of **onePK Devices** on the **onePK** tab.
When there is no physical device associated with the address that you entered, no connection is made, and a connection timed out error message is displayed. The address is grayed out in the **Network Element Address** list of **onePK Devices** on the **onePK** tab.

Removing onePK Devices

Step 1 On the menu bar, choose **Devices**, and then click the **onePK** tab.
Step 2 In the **onePK Devices** list, check the check box next to each device that you want to remove, or check the top check box to remove all onePK Devices.
Step 3 Click **Remove onePK Device**.
Step 4 In the **Remove onePK Device** confirmation dialog box, click **Remove onePK Device**.

Adding a Node Group

A node group allows you to visually group nodes in the Cisco Extensible Network Controller (XNC) topology diagram. Node groups do not create links between nodes.

Step 1 On the menu bar, choose **Devices**, and then click the **Device Groups** tab.

Step 2 Click **Add Group**.

Step 3 In the **Add Node Group** dialog box, complete the following field:

Name	Description
Name field	The name that you want to give the node group. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").

Step 4 Click **Add Group**.
The name of the group displays in the list of node groups.

What to Do Next

Add nodes to the node group.

Adding Nodes to a Node Group

Adding nodes to a node group visually associates the nodes with the node group in the topology diagram. Node groups are highlighted in different colors in the diagram.

Note If you add a node that already belongs to a node group to a new node group, it is automatically removed from the first node group and added to the new node group.

Before You Begin

Add a node group.

Step 1 On the menu bar, choose **Devices**, and then click the **Device Groups** tab.

Step 2 Click the name of the node group to which to want to add nodes in the **Node Groups** list.

Step 3 Add nodes to the group by doing one of the following:

- Click one or more nodes in the topology diagram, and then click **Add to group <group name>** in the topology diagram.

- Click the **Nodes in Group** tab, and then do the following:

a) In the **Add Nodes to Group - <group name>** dialog box, choose one or more nodes from the drop-down list.
b) Click **Add to group**.

The nodes display in the **Nodes in Group - <group name>** list on the **Nodes in Group** tab, and in the node group in the topology diagram.

Removing Nodes from a Node Group

Before You Begin

Add nodes to a node group.

Step 1 On the menu bar, choose **Devices**, and then click the **Device Groups** tab.

Step 2 Click the name of the node group from which to want to remove nodes in the **Nodes Groups** list.

Step 3 To remove nodes from the group, do one of the following:

- Click a node group in the topology diagram, and then:

a) Click the node you want to remove from the group.
b) Click **Remove from group – <group-name>** in the topology diagram.

- Click the **Nodes in Group** tab, and then:

a) Check the check box next to the node or nodes you want to remove in the list of **Nodes in Group <group name>**, or check the top check box in the list to select all nodes in the group for removal.
b) Click **Remove Nodes from <group-name>** .

Step 4 In the **Remove Nodes** confirmation dialog box, click **Remove**.

Removing a Node Group

Removing a node group disassociates the nodes added to it from the node group, and the node group is no longer displayed in the topology diagram.

Step 1 On the menu bar, choose **Devices**, and then click the **Device Groups** tab.

Step 2 In the **Node Groups** list, check the check box next to the name of the node group you want to remove, or check the top check box to select all node groups for removal.

Step 3 Click **Remove Group**.

Step 4 In the **Remove Group** confirmation dialog box, click **Remove Group**.
The node group is removed and no longer displays in the topology diagram.

Adding a Static Route

Step 1 On the menu bar, choose **Devices**, and then click the **Static Route Configuration** tab.

Step 2 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. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").
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**.

Removing a Static Route

Before You Begin

Add one or more static routes.

Step 1 On the menu bar, choose **Devices** and then click the **Static Route Configuration** tab.

Step 2 Check the check box next to the name of each static route that you want to remove, or check the top check box to select all static routes for removal.

Step 3 Click **Remove Static Route**.

Step 4 In the **Remove Static Route** confirmation dialog box, click **Remove Static Route**.

Adding a Gateway IP Address

Step 1 On the menu bar, choose **Devices**, and then click the **Subnet Gateway Configuration** tab.

Step 2 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. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").
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**.

Removing a Gateway IP Address

Before You Begin

Add one or more gateway IP addresses.

Step 1 On the menu bar, choose **Devices**, and then click the **Subnet Gateway Configuration** tab.

Step 2 Check the check box next to the name of each gateway IP address you want to remove, or check the top check box to remove all gateway IP address entries.

Step 3 Click **Remove Gateway IP Address**.

Step 4 In the **Remove Gateway IP Address** confirmation dialog box, click **Remove Gateway IP Address**.

Adding Ports

Step 1 On the menu bar, choose **Devices**, and then click the **Subnet Gateway Configuration** tab.

Step 2 Click **Add Ports**.

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

Name	Description
Gateway Name drop-down list	The name of the gateway address to which you want to bind the port.
Node ID drop-down list	The node that contains the port that you want to bind to the gateway address.
Select Port drop-down list	The port that you want to bind to the gateway address.

Step 4 Click **Save**.

Adding a SPAN Port

Step 1 On the menu bar, choose **Devices**, then click the **SPAN Port Configuration** tab.

Step 2 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 drop-down list	Choose the input port to use for the SPAN port.

Step 4 Click **Save**.

Removing a SPAN Port

Before You Begin

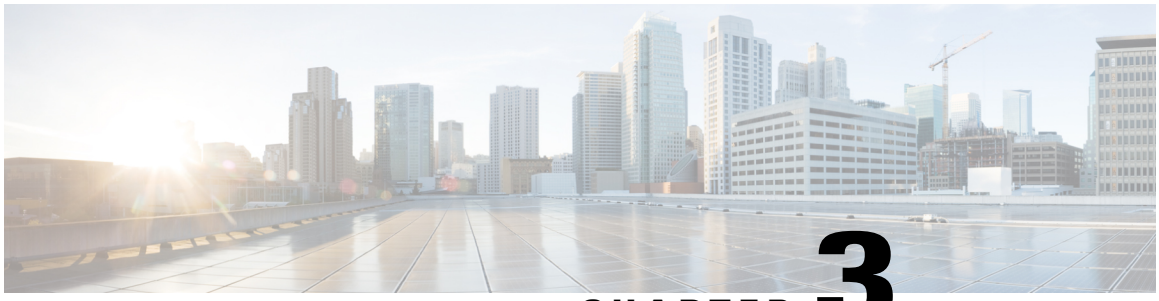
Add one or more SPAN ports.

Step 1 On the menu bar, choose **Devices**, and then click the **SPAN Port Configuration** tab.

Step 2 Check the check box next to each entry in the **Node** and **SPAN Port** list that you want to remove, or check the check box at the top of the list to choose all SPAN ports for removal.

Step 3 Click **Remove SPAN Port**.

Step 4 In the **Remove SPAN Port** confirmation dialog box, click **Remove SPAN Port**.



CHAPTER 3

Managing Flows

This chapter contains the following sections:

About Flow Programming

With Cisco Extensible Network Controller (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 addresses of the packets.
- Modifying the source and destination IP addresses 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 menu bar, choose **Flows**, and then click the **Flow Entries** tab.

Step 2 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. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@"). **Note** You cannot change the name of the flow entry after it is saved.
Node drop-down list	Choose the ID or node name for the device. **Note** The node you choose cannot be changed one you save the flow entry.
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	The Ethernet type for the Layer 2 traffic. The Ethernet type for IPv4, in hexadecimal format, is displayed by default. Either accept the default value, or enter one of the following, in hexadecimal format: • **IPv6** • **ARP** • **LLDP**
VLAN Identification Number field	The VLAN ID for the Layer 2 traffic.
VLAN Priority field	The VLAN priority for the Layer 2 traffic.

Name	Description
Source MAC Address field	The source MAC address for the Layer 2 traffic.
Destination MAC Address field	The destination MAC address for 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. **Note** The format of the source IP address must match the Ethernet type that you entered in the **Ethernet Type** field for Layer 2.
Destination IP Address field	The destination IP address of the Layer 3 traffic. **Note** The format of the destination IP address must match the Ethernet type that you entered in the **Ethernet Type** field for Layer 2.
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.
Protocol field	The Internet protocol number of the Layer 4 traffic. Enter the IP protocol number in decimal, hexadecimal, or octal format.

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**
- **Flood All**
- **Enqueue**
- **Set VLAN CFI**
- **Push VLAN**
- **Set EtherType**

Step 8 Do one of the following:

- Click **Install Flow** to install the flow into the device.
- Click **Save Flow** to save the flow to the **Flow Entries** table but not install the flow in the flow table of the device.

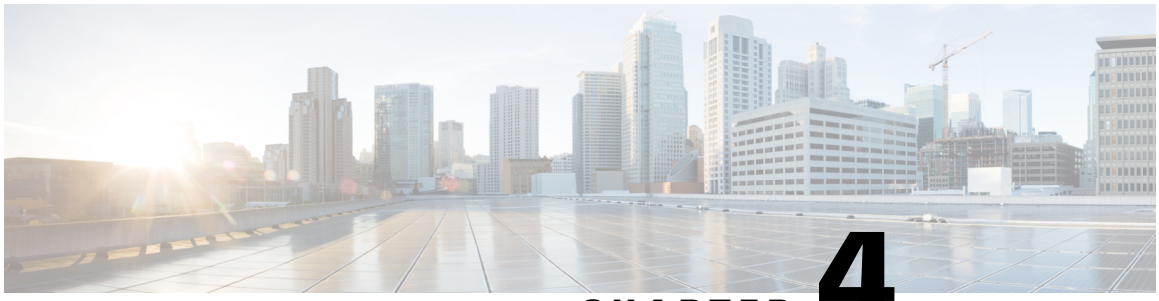
Viewing Flow Details

Step 1 On the menu bar, choose **Flows**, and then click the **Flow Entries** tab.

Step 2 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 **Edit Flow** to edit the flow in 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 that a data flow takes through the network. TIF Manager can also be invoked by any network-aware business application that communicates with Cisco Extensible Network Controller (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 menu bar, choose **TIF Manager**, and then click the **TIF Policies** tab.

Step 2 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 TIF policy. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@"). **Note** The name cannot be changed after the TIF policy is saved.
Source IP field	The source IP address of the host.
Destination IP field	The destination IP address of the host.
Protocol drop-down list	Choose the protocol to be used for the policy. This can be one of the following: • **any—**All protocols are used. • **ICMP—**Only the ICMP protocol is used. • **TCP—**Only the TCP protocol is used. • **UDP—**Only the UDP protocol is used. • **IPv6-ICMP—**Only the IPv6-ICMP protocol is 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 number. 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 in the **Network Properties** area is also displayed in this list. Click the **Custom Path** radio button to choose an existing path from the drop-down list.

Step 4 Click **Create TIF Policy**.

Editing a TIF Policy

Note The name of the TIF policy cannot be changed.

Before You Begin

Create one or more TIF policies.

Step 1 On the menu bar, choose **TIF Manager**, and then click the **TIF Policies** tab.

Step 2 Click **Edit** next to the name of the TIF policy that you want to change.

Step 3 In the **Edit TIF Policy** dialog box, complete the following fields:

Name	Description
Name field	The name that you want to assign to the TIF policy. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@"). **Note** The name cannot be changed after the TIF policy is saved.
Source IP field	The source IP address of the host.
Destination IP field	The destination IP address of the host.
Protocol drop-down list	Choose the protocol to be used for the policy. This can be one of the following: • **any—**All protocols are used. • **ICMP—**Only the ICMP protocol is used. • **TCP—**Only the TCP protocol is used. • **UDP—**Only the UDP protocol is used. • **IPv6-ICMP—**Only the IPv6-ICMP protocol is 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 number. If no destination port is specified, any ports can be used.

Name	Description
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 in the **Network Properties** area is also displayed in this list. Click the **Custom Path** radio button to choose an existing path from the drop-down list.

Step 4 Click **Save TIF Policy**.

Removing TIF Policies

Step 1 On the menu bar, choose **TIF Manager**, and then click the **TIF Policies** tab.

Step 2 Check the check box next to the **Name** of each TIF policy that you want to remove, or check the top check box to select all TIF policies for removal.

Step 3 Click **Remove TIF Policy**.

Step 4 In the **Remove TIF Policy** confirmation dialog box, click **Remove TIF Policy**.

Creating a Custom Path

Step 1 On the menu bar, choose **TIF Manager**.

Step 2 At the top of the topology diagram, enter the name that you want to give the custom path in the field next to the **Save Custom Path** button.

Step 3 In the topology diagram, click the links that you want to include in the path.

Step 4 Click **Save Custom Path** to save the path to the **Existing Custom Paths** table.

Viewing a Custom Path

Before You Begin

Create a custom path.

Step 1 On the menu bar, choose **TIF Manager**.

Step 2 Click **View/Edit Path** in the **Existing Custom Paths** table next to the path that you want to display.
The custom path links are displayed in the topology diagram.

Step 3 In the **Links Information** tab, enter a node number in the **Search** box, and click the search icon to narrow the list of nodes displayed for the path.

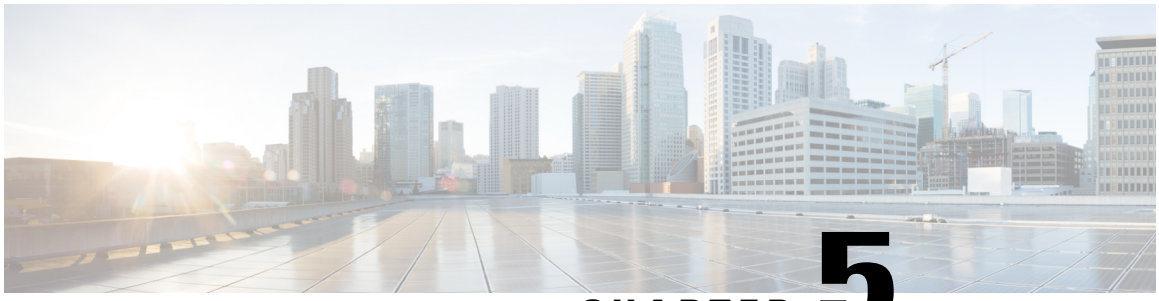
Removing Custom Paths

Step 1 On the menu bar, choose **TIF Manager**.

Step 2 Check the check box next to the path name of each custom path that you want to remove in the **Existing Custom Paths** tab, or check the top check box to choose all custom paths for removal.

Step 3 Click **Remove**.

Step 4 In the **Remove Path(s)** confirmation dialog box, click **Remove Path(s)**.



CHAPTER 5

Troubleshooting

This chapter contains the following sections:

About Troubleshooting

Cisco Extensible Network Controller (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 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 menu bar, choose **Troubleshoot**, and then click the **Flow Check** tab.

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

Note The statistics are updated every 120 seconds.

Viewing Inconsistent Controller Flows or Inconsistent Node Flows

Step 1 In the menu bar, choose **Troubleshoot**, and then click the **Flow Check** tab.

Step 2 From the **Select a node** drop-down list, choose a node.
The node is displayed, with the number of **Inconsistent Controller Flows** and **Inconsistent Node Flows**, if any, next to each type.

Step 3 Click either **Inconsistent Controller Flows** or **Inconsistent Node Flows** to view details for any inconsistent flows.
Details are displayed in the **Statistics** tab.

What to Do Next

Fix inconsistent controller flows or inconsistent node flows.

Exporting Inconsistent Flow Details

In order to view and save inconsistent controller or inconsistent node flow details for reference, you can export them to a comma-delimited file.

Step 1 In the menu bar, choose **Troubleshoot**, and then click the **Flow Check** tab.

Step 2 Choose a node from the **Select a node** drop-down list.

The node is displayed, with the number of **Inconsistent Controller Flows** and **Inconsistent Node Flows** next to each type.

Step 3 Choose either **Inconsistent Controller Flows** or **Inconsistent Node Flows**.
The list of **Inconsistent Controller Flows** or **Inconsistent Node Flows** is displayed in the **Statistics** tab.

Step 4 Check the check box next to one or more inconsistent flows, or check the check box at the top of the list to choose all flows in the list.

Step 5 Click **Export All**, and then click **Export Flow Details**.

Step 6 Save the inconsistent flow detail information as a `.csv` file that you can open later for analysis.

Fixing Inconsistent Flows

Note When you fix an inconsistent controller flow, the flow is installed on the switch. When you fix an inconsistent node flow, the flow is removed from the switch, because the controller is the authoritative source of flow information.

Step 1 In the menu bar, choose**Troubleshoot**, and then click the **Flow Check** tab.

Step 2 Choose a node from the **Select a node** drop-down list.
The node is displayed, with the number of **Inconsistent Controller Flows** and **Inconsistent Node Flows** next to each type.

Step 3 Click either **Inconsistent Controller Flows** or **Inconsistent Node Flows**.
The list of **Inconsistent Controller Flows** or **Inconsistent Node Flows** is displayed in the **Statistics** tab.

Step 4 Check the check box next to one or more inconsistent flows, or check the check box at the top of the list to choose all flows in the list.

Step 5 Click **Fix Inconsistent Flows**.

Step 6 In the **Fix Flows** confirmation dialog box, click **Fix Inconsistent Flows**.
The **Flow Check** tab redisplays **Inconsistent Controller Flows** and **Inconsistent Node Flows** with the updated number of each type.

Note If you chose all inconsistent flows in Step 4, the number displayed is 0.

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 a software-defined networking (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 menu bar, choose **Troubleshoot**, and then click the **Policies** tab.

Step 2 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 Monitor the TIF policy flows as follows:

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 Run an SDN trace on a TIF policy flow as follows:

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 Extensible Network Controller (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 Extensible Network Controller (XNC) to run the SDN Analyzer.

Step 1 On the menu bar, click **Troubleshoot**, and then click the **SDN Analyzer** tab.

Step 2 Click the interface that you want to view, and then click **Start Analyzer**.

Step 3 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.

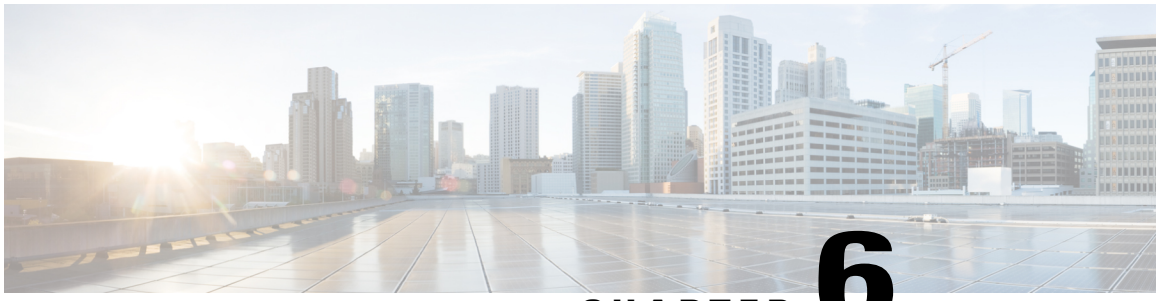
Step 3 Locate the following parameters:

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

Step 4 Change the files as appropriate. We recommend that you use a file size of no more than 100mb, and increase the number of pcap files.

Step 5 Save the file and exit the editor.

Step 6 Restart Cisco Extensible Network Controller (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 Extensible Network Controller (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 bandwidth.

Many of the policies also contain metrics that further define the property. The latency property, for example, includes 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 Extensible Network Controller (XNC).

Adding a Link Property

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

Step 1 On the menu bar, choose **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 menu bar, choose **Topology**, and then click the **Templates** tab.

Step 2 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 The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").
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 menu bar, choose **Topology**, and then click the **Templates** tab.
Step 2 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 menu bar, choose **Topology**, and then click the **Templates** tab.
Step 2 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. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").
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 menu bar, choose **Topology**, and then click the **Templates** tab.

Step 2 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 there are undiscovered links in the topology.

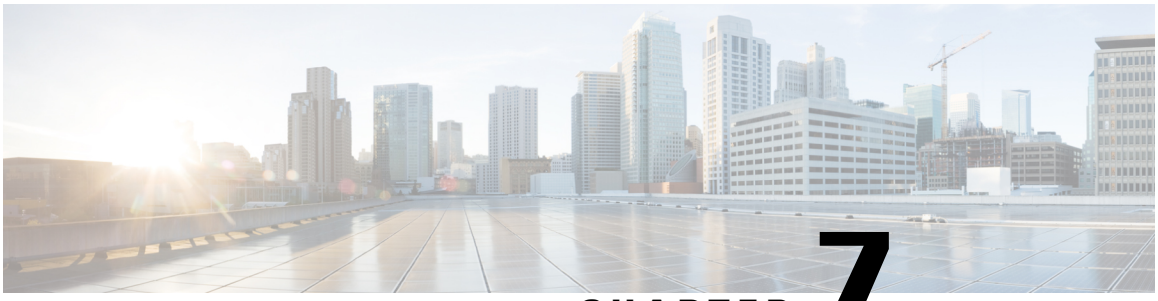
Step 1 On the menu bar, choose **Network Properties**, and then click the **Manual Links** tab.

Step 2 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. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").
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. This feature allows you to create multiple disjoint networks and assign different roles and access levels to each one. Each logical network can be assigned to departments, groups of individuals, or applications. Multiple disjoint networks can be managed using the Cisco Nexus Data Broker application.

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 ports used to identify the traffic that belongs to the slice.

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

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

Slices must be created by a Cisco Extensible Network Controller (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 if 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 From the **Admin** drop-down list, choose **Slices**.

Step 2 On 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. The name may contain between 1 and 256 alphanumeric characters including the following special characters: underscore (_), hyphen (-), plus (+), equals (=), vertical bar (|), or at sign (@). **Note** The slice name cannot be changed once it is saved.
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 From 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

Create a slice before you add a flow specification.

Note Be default, a flow specification is bidirectional.

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

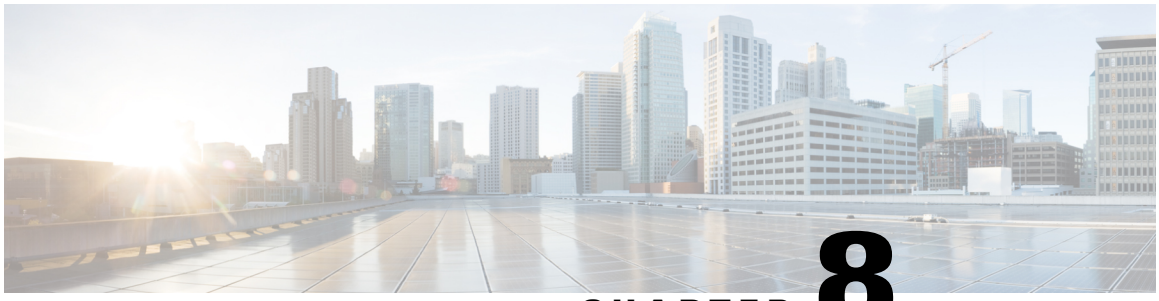
Step 2 On the **Flow Spec** tab, choose the slice for which you want to add a flow specification.
Enter a value in the **Search** combo box and click the search icon to limit the number of entries that appear.

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 specification. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@").
VLAN field	The VLAN ID or the range of VLAN IDs that you want to use for the flow specification.
Source IP field	The source IP address that you want to use for the flow specification.
Destination IP field	The destination IP address that you want to use for the flow specification.
Protocol field	The IP protocol number in decimal format that you want to use for the flow specification.
Source Port field	The source port that you want to use for the flow specification.
Destination Port field	The destination port that you want to use for the flow specification.

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 Extensible Network Controller (XNC) uses Remote Authentication Dial-In User Service (RADIUS) or Terminal Access Controller Access-Control System Plus (TACACS+) to communicate with an AAA server.

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

Adding an AAA Server

Step 1 From 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.

Name	Description
Server Secret field	The shared secret configured on the AAA server.
Protocol drop-down list	Choose the protocol for the AAA server. This can be one of the following: • **Radius+** • **TACACS+**

Step 4 Click **Save**.

What to Do Next

If you chose RADIUS as the protocol for the AAA server, you need to configure user authentication for RADIUS.

Configuring User Authentication for RADIUS Server

User authorization on a RADIUS server must conform to the Cisco Attribute-Value (av-pair) format.

In the RADIUS server, configure the Cisco av-pair attribute for a user as follows:

```
shell:roles="Network-Admin Slice-Admin"
```

Viewing an AAA Server

Step 1 From 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 an AAA Server

Step 1 From 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 Extensible Network Controller (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 applications.
- **Network Operator—**Provides read-only privileges to all 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 Extensible Network Controller (XNC).

Viewing User Information

Step 1 From 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 From 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. A username can be between 1 and 32 alphanumeric characters and contain any special character except a period ("."), forward slash ("/"), pound sign ("#"), percent sign ("%"), semicolon (";"), question mark ("?"), or backslash ("\").
Password field	The password for the user. Passwords must be between 8 and 256 characters long, contain uppercase and lowercase characters, have at least one numeric character, and have at least one nonalphanumeric character.
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 applications. • **Network Operator—**Provides read-only privileges to all 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 From the **Admin** drop-down list, choose **Users**.

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

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

Step 4 In the **Change Password** dialog box, enter the new password in the **New Password** and in the **Verify New Password** fields.

Step 5 Click **Submit**.

Step 6 Click **Close** in the **Manage User** dialog box.

Step 7 Click **Close** in the **User Management** dialog box.

Deleting a User

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

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

Step 2 In the **User Management** dialog box, click 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 From the **Admin** drop-down list, choose **Clusters**.
The **Cluster Management** dialog box lists the IP addresses of all of the Cisco Extensible Network Controller (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.**

Viewing the OSGi Console

You can view all of Cisco Extensible Network Controller (XNC) bundles that comprise the application by viewing the OSGi Web Console.

Note This procedure does not provide a step-by-step guide to everything you can do in the OSGi Web Console for **Cisco XNC Bundles** list. It guides you in opening the OSGi Web Console and viewing bundle information.

Step 1 From the **Admin** drop-down list, choose **OSGi**.
A new browser tab opens.

Step 2 Enter your username and password, and then press **Enter**.
The **Cisco – XNC Bundles** list is displayed. In this page you can view all of the active packages, filter on the package name to specify bundle names, and complete other tasks.

Step 3 When you are finished viewing the list, close the **Cisco – XNC Bundles** browser tab.

Viewing the Northbound API Content

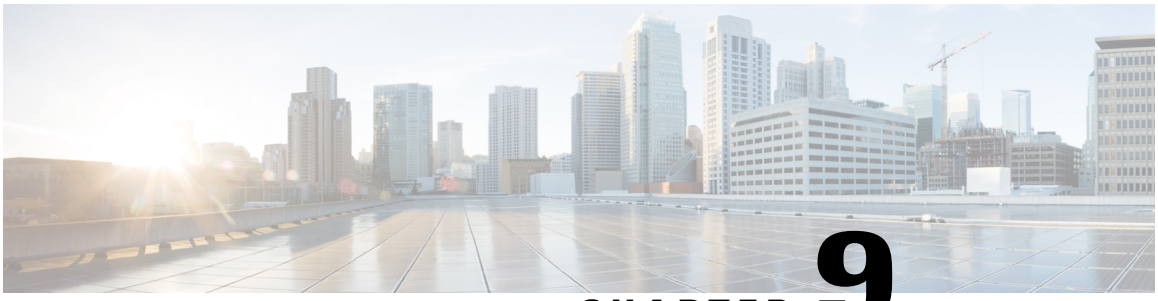
You can view all of Cisco Extensible Network Controller (XNC) northbound API content for the application by opening a browser tab using the **Northbound API** tool (book icon) in the menu bar.

Step 1 From the menu bar, click the **Northbound API** button.
A new browser tab (Swagger UI) is opened and the complete list of northbound API content used in Cisco XNC is displayed.

From this tab, you can do the following:

- Show or hide the operations for an API.
- List the operations for an API.
- Expand the operations for an API.

Step 2 When you are finished viewing northbound API content, close the browser tab.



CHAPTER 9

Port-to-Port Forwarding

This chapter contains the following sections:

About Port-to-Port Forwarding

The Cisco Extensible Network Controller (XNC) Virtual Patch Panel (port-to-port forwarding) application allows you to manage port-to-port (P2P) traffic within a switch or across the network without any need for physical connection changes or rewiring. Port-to-port forwarding reduces the time-consuming, manual process of interconnecting two ports, either within a switch or between switches, across the network to forward traffic. With the Cisco XNC port-to-port forwarding application, you can programmatically create a virtual patch panel.

The principal benefits of the Cisco XNC port-to-port forwarding application are as follows:

- The ability to automate a P2P path
- Automatic VLAN assignment and tagging for traffic that originates in the port
- No need to take the device offline
- Capability to scale the process across the data center network

Configuring EtherTypes for Ports

The `config.ini` file for Cisco Extensible Network Controller (XNC) is pre-provisioned with some parameters for the P2P feature to work properly on Cisco supported switches. There are two parameters:

- p2p.nonConventionalNodes—This parameter should not be modified without first contacting Cisco support.

- p2p.nonConventionalNodesEthertypes—This parameter specifies the comma-separated list of frames for which the P2P paths are applicable. The default frame type is IPv4, which means that each P2P path is only applicable for IPv4 packets.

Step 1 Open the `config.ini` file for editing and locate the `p2p.nonConventionalNodesEthertypes` parameter.

Step 2 Modify the `p2p.nonConventionalNodesEthertypes` parameter to suit your needs. An example of a valid configuration follows:
`p2p.nonConventionalNodesEthertypes=IPv4,IPv6,ARP`

Step 3 Save your work and close the file.

Step 4 Restart Cisco Extensible Network Controller (XNC).

Logging in to the Cisco XNC Port-to-Port Forwarding GUI

You must log into the Cisco XNC port-to-port forwarding GUI using HTTPS.

The default HTTPS web link for the Cisco XNC port-to-port forwarding GUI is *https://Controller_IP:8443/p2p*

Note Before you can use HTTPS, you must manually specify the https:// protocol in your web browser.

Step 1 In your web browser, enter the Cisco XNC port-to-port forwarding GUI web link.

Step 2 On the launch page, enter your username and password.
The default username and password is admin/admin.

Step 3 Click **Log In**.

Adding a Port-to-Port Forwarding Path

You can add P2P paths and view them in the topology diagram.

Step 1 On the **Paths** tab, click **Add Path**.

Step 2 In the **Add P2P Path** dialog box, complete the following fields:

Name	Description
Path Name field	The name that you want to give the forwarding path. The name can contain between 1 and 256 alphanumeric characters including the following special characters: underscore ("_"), hyphen ("-"), plus ("+"), equals ("="), open parenthesis ("("), closed parenthesis (")"), vertical bar ("|"), period ("."), or at sign ("@"). **Note** The path name cannot be changed once it has been saved.
Source Node drop-down list	Choose the source node that you want to use in the forwarding path.
Source Port drop-down list	Choose the source port of the node that you want to use in the forwarding path.
Destination Node drop-down list	Choose the destination node that you want to use in the forwarding path.
Destination Port drop-down list	Choose the destination port of the node that you want to use in the forwarding path.
Source VLAN field	The source VLAN ID that you want to use in the forwarding path. **Note** This field is optional.
Destination VLAN field	The destination VLAN ID that you want to use in the forwarding path. **Note** This field is optional.

Step 3 Click **Add Path**.
The path is installed. The source node, port, and VLAN, and the destination node, port, and VLAN are displayed beneath the **Path Name** in the **List of Paths** , and the path is highlighted in the topology diagram.

Note VLAN information is displayed only if you configured a source or a destination VLAN.

Editing a Port-to-Port Forwarding Path

You can edit an existing port-to-port forwarding path.

Step 1 On the **Paths** tab, click **Edit** next to the path you want to update.

Step 2 In the **Edit P2P Path** dialog box, complete the following fields:

Name	Definition
Path Name field	The name of the P2P path. **Note** You cannot change the path name in this dialog box.
Source Node drop-down list	Choose the new source node that you want to use in the forwarding path.
Source Port drop-down list	Choose the new source port of the node that you want to use in the forwarding path.
Destination Node drop-down list	Choose the new destination node that you want to use in the forwarding path.
Destination Port drop-down list	Choose the new destination port of the node that you want to use in the forwarding path.
Source VLAN field	The new source VLAN ID that you want to use in the forwarding path. **Note** This field is optional.
Destination VLAN field	The new destination VLAN ID that you want to use in the forwarding path. **Note** This field is optional.

Step 3 Click **Save Path**.

Deleting One or More Port-to-Port Forwarding Paths

You can delete one or more existing port-to-port forwarding paths.

Step 1 On the **Paths** tab, do one of the following:

- Check the check box next to the path or paths that you want to delete
- Check the check box next to the **Path Name** in the **List of Paths** to select all port-to-port forwarding paths

Step 2 Click **Delete Path**.

Step 3 In the **Remove P2P Path** confirmation dialog box, click **Remove Path**.