CONFIGURATION GUIDE

RUCKUS SmartZone 6.1.1 (LT-GA) Switch Management Guide (SZ300/vSZ-H)

Supporting SmartZone 6.1.1

Part Number: 800-73287-001 Rev A
Publication Date: April 2023

Copyright, Trademark and Proprietary Rights Information

© 2023 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, COMMSCOPE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. CommScope does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. CommScope does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to CommScope that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL COMMSCOPE, COMMSCOPE AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF COMMSCOPE HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Contact Information, Resources, and Conventions **5**
Contacting RUCKUS Customer Services and Support 5
What Support Do I Need? 5
Open a Case 5
Self-Service Resources 6
Document Feedback 6
RUCKUS Product Documentation Resources 6
Online Training Resources 6
Document Conventions 7
Notes, Cautions, and Safety Warnings 7
Command Syntax Conventions 7

About This Guide **9**
New in This Document 9

Working with Switches **11**
Managing ICX Switches from SmartZone 11
Supported ICX Models 11
Overview of ICX Switch Management 13
ICX Switch Behavior with SmartZone 15
Enabling an ICX Device to Be Managed by SmartZone 16
Configuring the ICX Source Address to Be Used by SmartZone 16
Setting Up Switch Registrar Discovery 17
Preparing Stacking Devices to Connect to SmartZone 19
Configuring DHCP to Provide SmartZone IP Addresses to an ICX Switch 19
Manually Configuring the SmartZone IP Address on an ICX Switch 20
Displaying the SmartZone Connection Status 20
Disconnecting the ICX Switch from SmartZone 21
Disabling SmartZone Management on the ICX Switch 21
SmartZone Switch Management 21
Using Controller Settings to Manage Switch Groups 21
Creating Switch Groups 21
Creating Switch Registration Rules 25
Moving the Switches between Groups 29
Deleting Switches 31
Backing up and Restoring Switch Configuration 32
Rehoming Switches 36
Switching Over Clusters 36
Scheduling a Firmware Upgrade for Switch Group 38
Scheduling a Firmware Upgrade for Selected Switches 40
Viewing Switch Information 42
Configuring the Switch 45
Data Synching on the Switch Table 62
Switch Level Configuration 64
Generic CLI Configuration 73
Creating Config Backup for Switch Group 94
Viewing Configuration Alerts 95

Port Settings 96
Creating Routing Configurations 123
Managing Link Aggregation Groups (LAGs) 126
Creating a Switch Stack 127
Viewing Port Details 129
Viewing Switch Health 132
Viewing Alarms 136
Viewing Events 139
Viewing LLDP Neighbor Information 141
Viewing Traffic Trends in the Switch 143
Viewing Firmware History of the Switch 145
Deleting the Firmware Upgrade Schedules 146
Configuring the Group Firmware Settings 148
Accessing the switch CLI through SmartZone (Remote CLI) 151
Viewing PoE Utilization and Health Status of the Switch 154
Ability to Convert Standalone Switch to Stack 157
Troubleshooting Switch Issues 161
Troubleshooting Using Custom Events 163
Troubleshooting Using Remote Operations 166
Cable Testing on ICX Ports 169
Viewing Switches on the Dashboard 172

Contact Information, Resources, and Conventions

- Contacting RUCKUS Customer Services and Support 5
- Document Feedback 6
- RUCKUS Product Documentation Resources 6
- Online Training Resources 6
- Document Conventions 7
- Command Syntax Conventions 7

Contacting RUCKUS Customer Services and Support

The Customer Services and Support (CSS) organization is available to provide assistance to customers with active warranties on their RUCKUS products, and customers and partners with active support contracts.

For product support information and details on contacting the Support Team, go directly to the RUCKUS Support Portal using https://support.ruckuswireless.com, or go to https://www.commscope.com/ruckus and select **Support**.

What Support Do I Need?

Technical issues are usually described in terms of priority (or severity). To determine if you need to call and open a case or access the self-service resources, use the following criteria:

- Priority 1 (P1)—Critical. Network or service is down and business is impacted. No known workaround. Go to the **Open a Case** section.
- Priority 2 (P2)—High. Network or service is impacted, but not down. Business impact may be high. Workaround may be available. Go to the **Open a Case** section.
- Priority 3 (P3)—Medium. Network or service is moderately impacted, but most business remains functional. Go to the **Self-Service Resources** section.
- Priority 4 (P4)—Low. Requests for information, product documentation, or product enhancements. Go to the **Self-Service Resources** section.

Open a Case

When your entire network is down (P1), or severely impacted (P2), call the appropriate telephone number listed below to get help:

- Continental United States: 1-855-782-5871
- Canada: 1-855-782-5871
- Europe, Middle East, Africa, Central and South America, and Asia Pacific, toll-free numbers are available at https://support.ruckuswireless.com/contact-us and Live Chat is also available.
- Worldwide toll number for our support organization. Phone charges will apply: +1-650-265-0903

We suggest that you keep a physical note of the appropriate support number in case you have an entire network outage.

Self-Service Resources

The RUCKUS Support Portal at https://support.ruckuswireless.com offers a number of tools to help you to research and resolve problems with your RUCKUS products, including:

- Technical Documentation—https://support.ruckuswireless.com/documents
- Community Forums—https://community.ruckuswireless.com
- Knowledge Base Articles—https://support.ruckuswireless.com/answers
- Software Downloads and Release Notes—https://support.ruckuswireless.com/#products_grid
- Security Bulletins—https://support.ruckuswireless.com/security

Using these resources will help you to resolve some issues, and will provide TAC with additional data from your troubleshooting analysis if you still require assistance through a support case or RMA. If you still require help, open and manage your case at https://support.ruckuswireless.com/case_management.

Document Feedback

RUCKUS is interested in improving its documentation and welcomes your comments and suggestions.

You can email your comments to RUCKUS at #Ruckus-Docs@commscope.com.

When contacting us, include the following information:

- Document title and release number
- Document part number (on the cover page)
- Page number (if appropriate)

For example:

- RUCKUS SmartZone Upgrade Guide, Release 5.0
- Part number: 800-71850-001 Rev A
- Page 7

RUCKUS Product Documentation Resources

Visit the RUCKUS website to locate related documentation for your product and additional RUCKUS resources.

Release Notes and other user documentation are available at https://support.ruckuswireless.com/documents. You can locate the documentation by product or perform a text search. Access to Release Notes requires an active support contract and a RUCKUS Support Portal user account. Other technical documentation content is available without logging in to the RUCKUS Support Portal.

White papers, data sheets, and other product documentation are available at https://www.commscope.com/ruckus .

Online Training Resources

To access a variety of online RUCKUS training modules, including free introductory courses to wireless networking essentials, site surveys, and products, visit the RUCKUS Training Portal at https://commscopeuniversity.myabsorb.com/. The registration is a two-step process described in this video. You create a CommScope account and then register for, and request access for, CommScope University.

Document Conventions

The following table lists the text conventions that are used throughout this guide.

TABLE 1 Text Conventions

Convention	Description	Example
`monospace`	Identifies command syntax examples	`device(config)# interface ethernet 1/1/6`
bold	User interface (UI) components such as screen or page names, keyboard keys, software buttons, and field names	On the **Start** menu, click **All Programs**.
italics	Publication titles	Refer to the *RUCKUS Small Cell Release Notes* for more information.

Notes, Cautions, and Safety Warnings

Notes, cautions, and warning statements may be used in this document. They are listed in the order of increasing severity of potential hazards.

NOTE
A NOTE provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An ATTENTION statement indicates some information that you must read before continuing with the current action or task.



CAUTION
A CAUTION statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.



DANGER
A DANGER statement indicates conditions or situations that can be potentially lethal or extremely hazardous to you. Safety labels are also attached directly to products to warn of these conditions or situations.

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{**x**| **y**| **z**}	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x|**y**	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *member*[*member*...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

About This Guide

- New in This Document..... 9

New in This Document

TABLE 2 Key Features and Enhancements in SmartZone 6.1.1 (20 April 2023)

Feature	Description	Reference
• Managing ICX Switches from SmartZone • SmartZone Switch Management • Troubleshooting Switch Issues • Viewing Wired Devices on the Dashboard	**Updated**: Migrated topics from the RUCKUS SmartZone 300 and Virtual SmartZone-High Scale Administrator Guide, 6.1.1.	Throughout the guide.

Working with Switches

- Managing ICX Switches from SmartZone..... 11
- SmartZone Switch Management..... 21
- Troubleshooting Switch Issues..... 161
- Viewing Switches on the Dashboard..... 172

Managing ICX Switches from SmartZone

Supported ICX Models

The following ICX switch models can be managed from SmartZone:

TABLE 3 ICX Firmware Versions Compatible with SmartZone

ICX Model	First Supported FastIron Release	Last Supported FastIron Release
ICX 7150	08.0.80a	09.0.10a and subsequent patches
ICX 7150-C08P, -C08PT, -24F, -10ZP	08.0.92	09.0.10a and subsequent patches
ICX 7250	08.0.80a	09.0.10a and subsequent patches
ICX 7450	08.0.80a	09.0.10a and subsequent patches
ICX 7550	08.0.95a	-
ICX 7650	08.0.80a	-
ICX 7750	08.0.80a	08.0.95 and subsequent patches
ICX 7850	08.0.90	-
ICX 7850-48C	09.0.10a	-
ICX 8200	10.0.00	-
ICX 8200-24ZP, -48ZP2, -24FX, -24F, -48F, -C08ZP	10.0.10	-

The following table defines ICX and SmartZone release compatibility.

NOTE

FastIron 09.0.10a and later releases support management by SmartZone 6.1 and later.

NOTE

ICX switches with FIPS mode enabled do not support management by SmartZone.

TABLE 4 ICX and SmartZone Release Compatibility Matrix

	SmartZone 5.0[1]	SmartZone 5.1[1]	SmartZone 5.1.1	SmartZone 5.1.2	SmartZone 5.2	SmartZone 5.2.1 / 5.2.2	SmartZone 6.0	SmartZone 6.1	SmartZone 6.1.1
FastIron 08.0.80	Yes	Yes	Yes[1]	No	No	No	No	No	No

[1] Does not support ICX configuration.

TABLE 4 ICX and SmartZone Release Compatibility Matrix (continued)

	SmartZone 5.0[1]	SmartZone 5.1[1]	SmartZone 5.1.1	SmartZone 5.1.2	SmartZone 5.2	SmartZone 5.2.1 / 5.2.2	SmartZone 6.0	SmartZone 6.1	SmartZone 6.1.1
FastIron 08.0.90a	No	No	Yes	Yes	Yes	Yes	Yes	No	No
FastIron 08.0.91	No	No	Yes	Yes	Yes	No	No	No	No
FastIron 08.0.92	No	No	No	Yes	Yes	Yes	Yes	Yes	No
FastIron 08.0.95 and subsequent patches	No	No	No	No	No	No	Yes	Yes	Yes
FastIron 09.0.10a and subsequent patches	No	No	No	No	No	No	No	Yes	Yes
FastIron 10.0.00 and subsequent patches	No	No	No	No	No	No	No	No	Yes
FastIron 10.0.10 and subsequent patches	No	No	No	No	No	No	No	Yes	Yes

The following table provides details on switch management feature compatibility between ICX and SmartZone releases.

TABLE 5 Switch Management Feature Compatibility Matrix

Feature	SmartZone Release	ICX FastIron Release
Switch Registration	5.0 and later	08.0.80 and later
Switch Inventory	5.0 and later	08.0.80 and later
Switch Health and Performance Monitoring	5.0 and later	08.0.80 and later
Switch Firmware Upgrade	5.0 and later	08.0.80 and later
Switch Configuration File Backup and Restore	5.0 and later	08.0.80 and later
Client Troubleshooting: Search by Client MAC Address	5.1 and later	08.0.80 and later
Remote Ping and Traceroute	5.1 and later	08.0.80 and later
Switch Custom Events	5.1 and later	08.0.80 and later
Remote CLI Change	5.2.1 and later	08.0.90 and later
Switch Configuration: Zero-Touch Provisioning	5.1.1 and later	08.0.90a and later
Switch-specific Settings: Hostname, Jumbo Mode, IGMP Snooping, and DHCP Server	5.1.1 and later	08.0.90a and later
Switch Port Configuration	5.1.1 and later	08.0.90a and later
Switch AAA Configuration	5.1.1 and later	08.0.90a and later

[1] Does not support ICX configuration.

TABLE 5 Switch Management Feature Compatibility Matrix (continued)

Feature	SmartZone Release	ICX FastIron Release
Switch Client Visibility	5.1.2 and later	08.0.90a and later
Manage Switches from Default Group in SZ-100 / vSZ-E	5.1.2 and later	08.0.90a and later
DNS-based SmartZone Discovery	5.1.2 and later	08.0.95c and later
Download Syslogs for a Selected Switch[2]	5.2.1 and later	08.0.92 and later
Switch Topology	5.2 and later	08.0.92 and later
Designate a VLAN as Management VLAN	5.2.1 and later	08.0.92 and later[3]
Change Default VLAN	5.2.1 and later	08.0.95 and later
Configure the PoE Budget per Port on ICX through the Controller GUI with 1W Granularity	5.2.1 and later	08.0.95 and later
Configuring Protected Ports	5.2.1 and later	08.0.95 and later
Configuring QoS	5.2.1 and later	08.0.95 and later
Configuring Syslog	5.2.1 and later	08.0.95 and later
Geo Redundancy Active-Standby Mode	6.0 and later	08.0.95b and later
Generic CLI Configuration	6.0 and later	08.0.95b and later
Port-Level Override	6.0 and later	08.0.95b and later
Port-Level Storm Control Configuration	6.1 and later	08.0.95 and later
IPv6 Support (connection through static configuration only)	6.1 and later	09.0.10a and later
Save Boot Preference	6.1 and later	09.0.10a and later
Virtual Cable Testing	6.1 and later	09.0.10a and later
Blink LEDs	6.1 and later	09.0.10a and later
Send Event Email Notifications at Tenant Level	6.1 and later	09.0.10a and later
Update the status of a Switch	6.1 and later	09.0.10a and later
Convert Standalone Switch	6.1 and later	09.0.10a and later
Flexible Authentication Configuration	6.1 and later	09.0.10a and later
Network Segmentation	6.1.1 and later	09.0.10d and later[4]

Overview of ICX Switch Management

Beginning with SmartZone 5.0, the SmartZone administrator can monitor and manage switches and routers in the ICX 7000 series. SmartZone 5.1.1 introduced the capability to configure switches.

SmartZone ICX-Management supports the following ICX switch activities:

- Registration and authentication
- Switch inventory (for example, model, firmware version, and last backup)
- Health and performance monitoring (for example, status, traffic statistics, errors, and clients) with alarms
- Zero-touch provisioning

[2] To download system logs from SmartZone for a particular ICX switch, TFTP must be enabled.
[3] FastIron 10.0.00 and later releases do not support management VLANs.
[4] As an exception, FastIron release 10.0.00 does not support this feature.

- Configuration changes
- Port settings
- Configuration copy
- Configuration file backup and restore
- Firmware upgrade
- Client troubleshooting
- Remote Ping and Traceroute

NOTE
Refer to the Supported ICX Models on page 11 for more details.

Preparing ICX Devices to be Managed by SmartZone

NOTE
ICX-Management can be managed by SmartZone as well as by Ruckus Cloud. Refer to the *Managing ICX Switches from the Cloud* chapter in the *Ruckus FastIron Management Configuration Guide* for details about Ruckus Cloud switch management.

ICX devices can be managed by SmartZone. The following items are required to manage ICX devices:

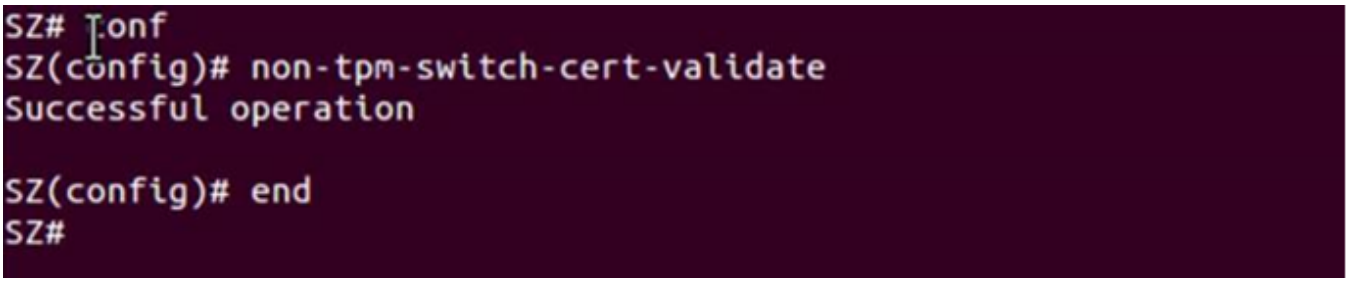
NOTE
Refer to the Supported ICX Models on page 11 for detailed information on software compatibility requirements and feature availability.

- The SmartZone IP address must be reachable by the ICX device through the Management interface or through switch or router interfaces.
- The ICX device must be made aware of the configured SmartZone IP address in one of the following ways:
  - Configure the DHCP server to use DHCP option 43.
  - Issue the following command at the global configuration level:

    ```
    ICX(conf)# manager active-list SmartZone_Control_IP_Address
    ```

  - Add an entry in the DNS server with the hostname ruckuscontroller or ruckuscontroller.*local domain* that points to the SmartZone IP address.
- On some ICX devices, self-signed certificates are used. SmartZone honors these certificates when the **non-tpm-switch-cert-validate** command is entered on the SmartZone console, as shown in the following example.

FIGURE 1 Command Required to Disable Certificate Check



NOTE
ICX 7650 and ICX 7850 devices are shipped with embedded certificates that are used for authentication with SmartZone.

- When SmartZone or ICX devices are behind network address translation (NAT), be sure to forward TCP ports 443 and 22 through NAT.
- Virtual platform requirements for supporting ICX devices are listed in the following table.

NOTE
Each unit in a stack is considered a separate switch unit for capacity management purposes.

TABLE 6 Virtual Platform Requirements for Supporting ICX Devices

Platform	Maximum Number of Switches Per Node	RAM	vCPU	Disk Storage
vSZ-E	200	18 GB	4	100 GB
vSZ-H	2000	30 GB	12	300 GB

The scaling limits in the table apply to switch-only deployments. For a mix of APs and switches, the scaling limits vary accordingly. SmartZone supports a 5-to-1 AP-to-switch ratio.

vSZ-E Example: vSZ-E supports up to 1,000 APs on a single node. If 200 APs are currently managed by SmartZone, there is room for 800 more APs or 160 ICX switches (800 divided by 5).

vSZ-H Example: vSZ-H supports up to 2,000 ICX switches on a single node. If 500 switches are currently managed, there is room for 1,500 more switches, or 7,500 APs (1500 multiplied by 5).

VIDEO
Onboarding ICX Switches to SmartZone. Using CLI commands to establish and verify switch connectivity to SmartZone.
Click to play video in full screen mode.

ICX Switch Behavior with SmartZone

NOTE
The full range of ICX-Management capabilities (including configuration support in SmartZone 5.1.1 or later) is available only when ICX devices have been upgraded to FastIron 08.0.90a or later using a Unified Forwarding Image (UFI). Beginning with FastIron 08.0.90, RUCKUS ICX devices support unified images that require custom upgrades from prior releases. Any ICX switch that is running a FastIron 08.0.80 non-UFI image on the ICX switch must follow a two-step image upgrade process to FastIron 08.0.90a through SmartZone controller image updates. If an ICX switch from the factory has a FastIron 08.0.80 non-UFI image, it must first be upgraded with a FastIron 08.0.90 UFI, followed by a FastIron 08.0.90a UFI, to avoid any boot configuration issues. Refer to the *RUCKUS FastIron Software Upgrade Guide* for more information.

NOTE
Campus Fabric (SPX) is not compatible with SmartZone. When SPX is enabled using the **spx cb-enable** command, SmartZone is disabled automatically. The following messages and syslog entry are displayed.

```
Console message
===============
Disabling SZ since SPX is enabled...
SZ Disable Initiated...
SZ Connection would be disconnected now if connected...

Syslog
=======
Aug  4 00:57:14:W:SZ:Disabling SZ, because SZ is not supported in SPX
```

If SPX is enabled on an ICX device and you try to enable SmartZone using the **no manager disable** command, the following warning message is displayed.

```
ICX(config)# no manager disable
SZ configuration is not allowed in SPX enabled setup. Please disable SPX to enable SZ
When ICX is managed through SZ, if 'spx cb-enable' is configured, SZ will be disconnected from ICX.
```

When an ICX switch is managed by SmartZone, the following considerations apply:

- All local configuration methods continue to be available to the local administrator, which means the switch can be configured through the console, Telnet, SSH, SNMP, or the web.
- It is recommended that the ICX switch be configured with the same NTP server as SmartZone.
- In an ICX stack, if a stack switchover or failover occurs, the original connection to SmartZone is closed, and the new active switch initiates a connection with SmartZone.

Enabling an ICX Device to Be Managed by SmartZone

There are several ways to make an ICX device aware of the SmartZone IP address:

- Use switch registrar discovery.
- Use DHCP option 43.
- Configure the ICX device manually using FastIron commands.

All of these methods are supported for new ICX switches with no configuration as well as for ICX switches with existing configuration.

Configuring the ICX Source Address to Be Used by SmartZone

By default, the IP address of the management port is included in the manager query as the ICX source address for an ICX-Management connection. Use the **management source-interface protocol manager** command to specify a different ICX source address.

NOTE
Only ICX devices with a router image support the **management source-interface protocol manager** command.

The **management source-interface protocol manager** command can specify an Ethernet, LAG, loopback, or virtual Ethernet (VE) interface. The IP address with the lowest number for the specified interface is used for the connection.

The following example configures an Ethernet port as the ICX source address for an ICX-Management connection.

```
ICX# configure terminal
ICX(config)# management source-interface ethernet 1/1/3 protocol manager
```

Refer to the *Ruckus FastIron Command Reference* for more information.

Setting Up Switch Registrar Discovery

The switch registrar is a RUCKUS-hosted cloud service that enables SmartZone discovery from ICX devices.

You can configure the ICX device to retrieve the correct SmartZone management IP address, IP address set, or fully qualified domain name (FQDN) from the switch registrar. The switch registrar must be set up in advance through Managed Service Provider (MSP) with SmartZone IP addresses or an FQDN and the ICX serial numbers they can manage.

> **NOTE**
> If SmartZone management is not enabled on the ICX device, switch registrar discovery does not occur.

How Switch Registrar Discovery Works

The ICX device sends an HTTP GET message to a default server host, sw-registrar.ruckuswireless.com, for the list of SmartZone management IP addresses or an FQDN, unless the system administrator configures an alternate host. The SmartZone IP address or FQDN obtained in response to the GET message is used to query the SmartZone device to set up a connection. If the ICX device receives a set of IP addresses from the switch registrar, it stores the information and tries the addresses in turn until a successful connection is established with the SmartZone device. The IP address, set of IP addresses, or FQDN obtained through the switch registrar is given priority above all other addresses in the list of SmartZone IP addresses, including addresses received from other sources such as the DHCP list, the active list, and the backup list. Once the ICX device has obtained a SmartZone IP address from the switch registrar, it no longer attempts switch registrar discovery.

This query is performed only for greenfield deployments and when the ICX device boots up with no startup configuration. ICX switches being upgraded from older releases that already have a configuration in place will not have the registrar-based SmartZone discovery turned on. The HTTPS session used for the database query uses the device certificate installed on the switch for SSL session establishment. For the initial release of the switch registrar, no server certificate validation will be performed.

Disabling or Enabling Switch Registrar Discovery

The system administrator can disable or enable switch registrar discovery from the command line.

> **NOTE**
> The registrar IP list is removed when you disable the switch registrar.

To disable switch registrar discovery, enter the **no manager registrar** command in global configuration mode, and use the **write memory** command to save the change, as shown in the following example.

```
ICX# configure terminal
ICX(config)# no manager registrar
ICX(config)# write memory
```

To restart the switch registrar discovery process, use one of the following commands at the privileged EXEC level:

- **manager registrar-query-restart**
- **manager reset**

To enable switch registrar discovery on an alternate registrar host server and save the entry to the startup configuration, enter the following commands.

```
ICX# configure terminal
ICX(config)# manager registrar sw-alternate.ruckuswireless.com
ICX(config)# write memory
```

> **NOTE**
> The **manager registrar** *hostname* command is for test purposes only. The **manager registrar-query-restart** command by itself is sufficient to initiate registrar-based SmartZone discovery.

Confirming Successful Switch Registrar Discovery

To display log entries specific to registrar queries, use the **show manager log** command.

When the switch registrar database has been successfully queried, a syslog message similar to the following is displayed.

```
Aug 8 21:47:17:I:MGMT Agent: SZ Switch Registrar Query to 54.186.143.194 Success
```

When the ICX device requires a restart to connect to the SmartZone address because a new registrar list has been received, a syslog message similar to the following is displayed.

```
Aug 8 21:47:17:I:MGMT Agent: Disconnect to SZ: 54.16.143.194, Got SZ ip via registrar
```

You can use the **show running-config** command to check for the name of the registrar host and the registrar list of SmartZone IP addresses.

The following example indicates that the ICX device uses the default switch registrar host and has obtained one SmartZone IP address (of a possible set of two addresses).

```
ICX# show running-config
!
!
manager registrar
manager registrar-list 23.251.150.119
!
!
```

You can also enter the **show manager status** command to obtain information on the switch registrar, as shown in the following example.

```
ICX# show manager status

============    MGMT Agent State Info     ===================

Config Status:Enabled Operation Status:Enabled
State:SSH CONNECTED  Prev State:SSH CONNECTING             Event:SZ_SSH_CONNECT_EVENT

SWR List                          : None
DNS List                :
Active List             : 10.176.160.116
Active List IPV6        : 2620:107:90d0:ab40::116
DHCP Option 43          : No
DHCP Opt 43 List        : None
Backup List             : None
Backup List IPV6        : None
Merged List             : 2620:107:90d0:ab40::116 10.176.160.116

SZ IP Used              : 2620:107:90d0:ab40::116
Port List               : 987
Server Port Used        : 443
Query Status            : APPROVED

SSH Tunnel Status -:
Tunnel Status           : Established
CLI IP/Port             : 127.255.255.253/59449
SNMP IP/Port            : 127.255.255.254/8253
Syslog IP/Port          : 127.0.0.1/20514
HTTP CLIENT IP/Port     : 127.0.0.1/5080
HTTP SERVER IP/Port     : 127.255.255.252/63098
Timer Status            : Not Running
```

Troubleshooting Switch Registrar Discovery

In the event that switch registrar discovery fails, check for the following conditions:

- The running configuration contains "manager disable".
- The switch registrar is not configured on the ICX device.
- The DNS configuration needed to resolve the switch registrar address is not present on the ICX device.

- The ICX device could not reach the switch registrar due to routing issues.

  NOTE
  If the switch registrar is enabled and you enter the **no manager disable** command, switch registrar discovery is still started when the registrar IP list is empty.

  NOTE
  The switch registrar discovery process continues to run until the configuration issues are fixed, a successful query result is obtained, or you enter a command to disable the switch registrar.

Preparing Stacking Devices to Connect to SmartZone

Consider the following guidelines when preparing ICX stacking devices to be discovered and managed by SmartZone:

- Define the stack configuration on the SmartZone device before connecting cables between the SmartZone and ICX devices.
- The devices to be managed in the stack must be part of a "firmware version" switch group configured on the SmartZone device.

If only the ICX device intended to be the stack active controller is an active switch under SmartZone control and is part of a configured "firmware version" switch group, perform the following steps to establish a stack:

- Connect all cables between ICX devices to form the desired stack configuration.
- On the active controller, enter the following commands in privileged EXEC mode:
  - **stack enable** (enables stacking on the active controller)
  - **stack zero-touch-enable** (triggers automatic discovery of the stack units and connections)
  - **write memory** (saves the running configuration to startup flash)

  No commands need to be entered on the other stack units in this case.

If all switches intended to be members of a stack have already joined and have been approved by SmartZone and are already part of a "firmware version" switch group, enter the following commands on the ICX devices to form a stack:

- On the active controller, enter the following commands in privileged EXEC mode:
  - **stack enable** (enables stacking on the active controller)
  - **stack zero-touch-enable** (triggers automatic discovery of the stack units and connections)
  - **write memory** (saves the running configuration to startup flash)
- On all other prospective stack members, configure the following commands in global configuration mode:
  - **stack suggested-id**
  - **stack ztp-force**
  - **write memory**

Configuring DHCP to Provide SmartZone IP Addresses to an ICX Switch

A DHCP server can be configured to send SmartZone IP addresses to ICX devices using DHCP Option 43.

Configure DHCP Option 43 on the DHCP server, using **RKUS.scg-address** to identify the SmartZone IP addresses.

A single SmartZone IP address or a comma-separated list can be configured. SmartZone IP addresses are sent with a sub-option value of 6. The ICX device ignores all other data in DHCP Option 43 if SmartZone IP addresses are present.

The following example shows a DHCP Option 43 configuration on a DHCP server. The IP addresses listed are examples only.

```
subnet 192.168.12.0 netmask 255.255.255.0 {
   range  192.168.12.100 192.168.12.199;
   option routers 192.168.12.1;
   option subnet-mask 255.255.255.0;
```

```
    option broadcast-address 192.168.12.255;
    option ntp-servers 192.168.11.22;
    class "Ruckus AP" {
       match if option vendor-class-identifier = "Ruckus CPE";
       option vendor-class-identifier "Ruckus CPE";
       default-lease-time 86400;
       vendor-option-space RKUS;
       option RKUS.scg-address "192.168.11.200, 192.168.11.201, 192.168.11.202";
    }
}
```

Manually Configuring the SmartZone IP Address on an ICX Switch

Complete the following steps to configure a list of SmartZone IP addresses on the ICX device.

1. Enter the **manager active-list** command followed by one or more priority IP addresses for the SmartZone device, as shown in the following example.

   The IP addresses listed are examples only.

   ```
   ICX# configure terminal
   ICX(config)# manager active-list 192.168.11.200 192.168.11.201 192.168.11.202
   ```

2. Use the **sz passive-list** *ip-address* command to configure the SmartZone IP addresses to be used for redundancy.

   ```
   ICX(config)# sz passive-list 10.176.160.118
   ```

Displaying the SmartZone Connection Status

Use the **show manager status** command to display the SmartZone IP address lists and information about the status of the connection.

```
device# show manager status

============    MGMT Agent State Info     ===================

Config Status:Enabled Operation Status:Enabled
State:SSH CONNECTED  Prev State:SSH CONNECTING             Event:SZ_SSH_CONNECT_EVENT

SWR List                          : None
DNS List                :
Active List             : 10.176.160.116
Active List IPV6        : 2620:107:90d0:ab40::116
DHCP Option 43          : No
DHCP Opt 43 List        : None
Backup List             : None
Backup List IPV6        : None
Merged List             : 2620:107:90d0:ab40::116 10.176.160.116

SZ IP Used              : 2620:107:90d0:ab40::116
Port List               : 987
Server Port Used        : 443
Query Status            : APPROVED

SSH Tunnel Status -:
Tunnel Status           : Established
CLI IP/Port             : 127.255.255.253/59449
SNMP IP/Port            : 127.255.255.254/8253
Syslog IP/Port          : 127.0.0.1/20514
HTTP CLIENT IP/Port     : 127.0.0.1/5080
HTTP SERVER IP/Port     : 127.255.255.252/63098
Timer Status            : Not Running
```

Disconnecting the ICX Switch from SmartZone

Use the **manager disconnect** command to disconnect the ICX switch from SmartZone and initiate a new connection based on the currently available list of SmartZone IP addresses.

Enter the **manager disconnect** command as shown.

This command can be executed on the local terminal.

```
ICX# manager disconnect
SZ Disconnect initiated...
```

Disabling SmartZone Management on the ICX Switch

When SmartZone management is disabled on the switch, the switch will not initiate a connection with SmartZone even if a SmartZone IP address is available.

Enter the **manager disable** command to disable SmartZone management on the ICX switch.

```
ICX(config)# manager disable
```

SmartZone Switch Management

Using Controller Settings to Manage Switch Groups

Controller allows you to create switch groups, similar to AP zones. Switches connecting to controller can be placed in one of these logical groups for better manageability. A Staging or Default Group is created by the controller automatically. All switches are placed in this group when they initially joining the controller. You have the option to create additional groups.

> **NOTE**
> In SZ300 and vSZ-H platforms, a warning message is displayed to move the switches from the Staging Group to another group for controller to monitor.

Using registration rules, you can specify which group the switch should be placed into. Refer to Creating Switch Groups on page 21 and Creating Switch Registration Rules on page 25 for additional information.

Creating Switch Groups

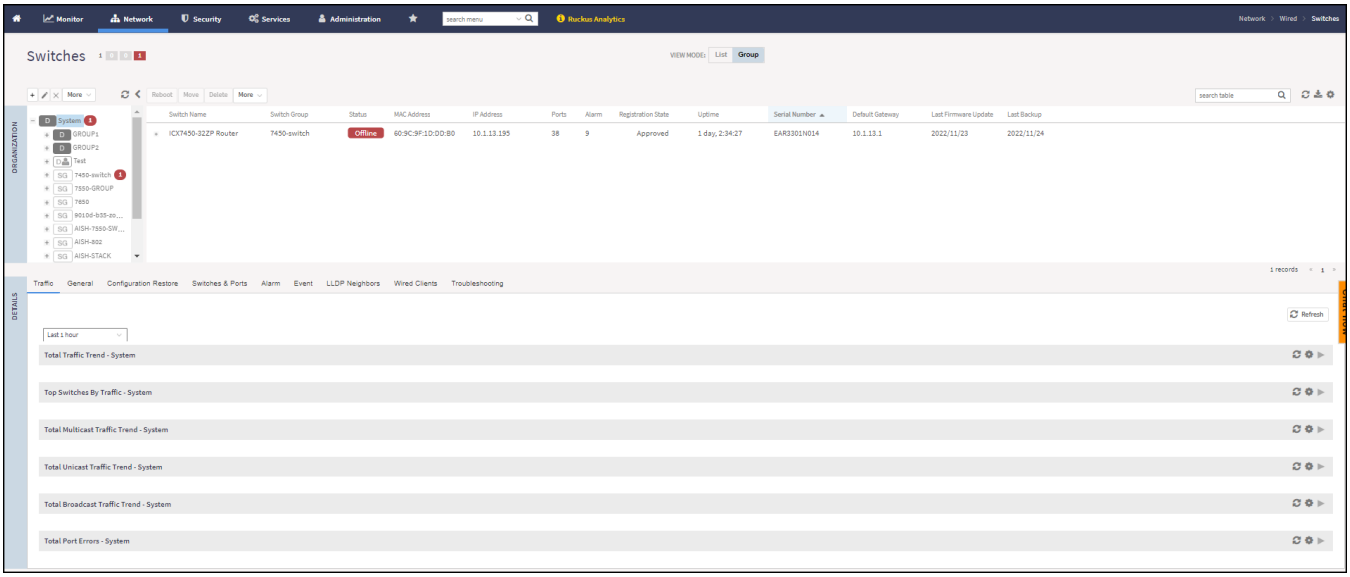
You can group switches based on your need, for example, you can group switches based on their size or their location.

You can only create a maximum of two levels within the group hierarchy. By default, all the switches are placed under the default switch group. You can create a group or sub-group and then move the switch under it. You can also modify or delete a group at any time.

After the switch is registered with the controller interface, you can monitor, view status or usage, and perform some basic management, including configuration backups and firmware management.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 2 Switches

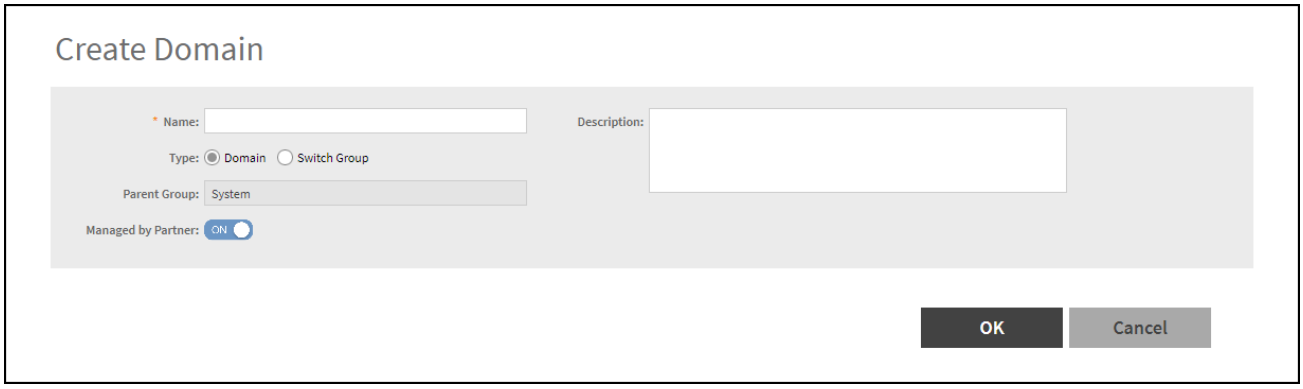


You can create a switch group or you can create a domain and add the switch group to that domain.

2. Complete the following steps to create a domain.

   a) In the **Organization** tab, click  to display the **Create Domain** dialog box.

   FIGURE 3 Create Domain

   b) Complete the following fields:

   - **Name**: Enter the domain name.
   - **Description**: Enter a brief description for the domain.
   - **Type**: Domain
   - **Parent Group**: Displays the parent group under which the switch group resides. By default **System** is selected.
   - **Managed by Partner**: This option is available if you select the group type as **Domain**. You can slide the radio button to ON or OFF to enable or disable partners from managing the switches.

   c) Click **OK**.

   The domain is created under the selected parent group in the **Organization** tab. The domain is identified with "D" symbol.

3. To create a individual switch group, in the **Organization** tab select the **System** and follow from the Step 5.
4. To create a switch group within a domain, in the **Organization** tab select the **Domain** from the list and follow from the Step 5.

5. In the **Organization** tab, click icon to display the **Create Switch Group** dialog box. You can also edit or configure the switch group by clicking icon.

FIGURE 4 Creating Switch Group

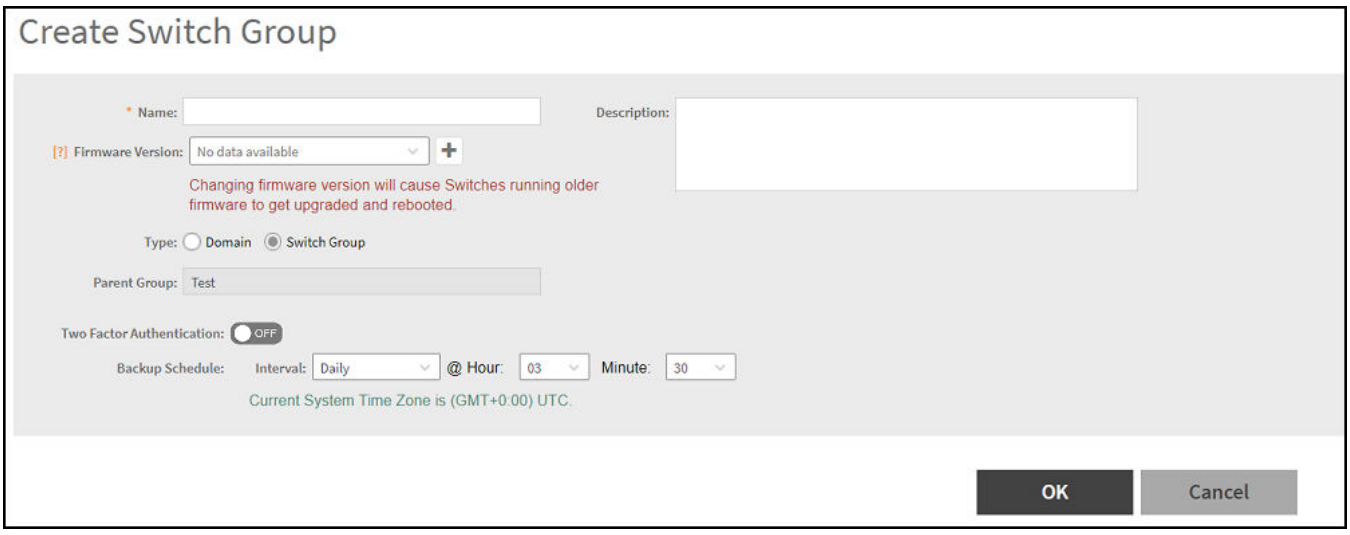
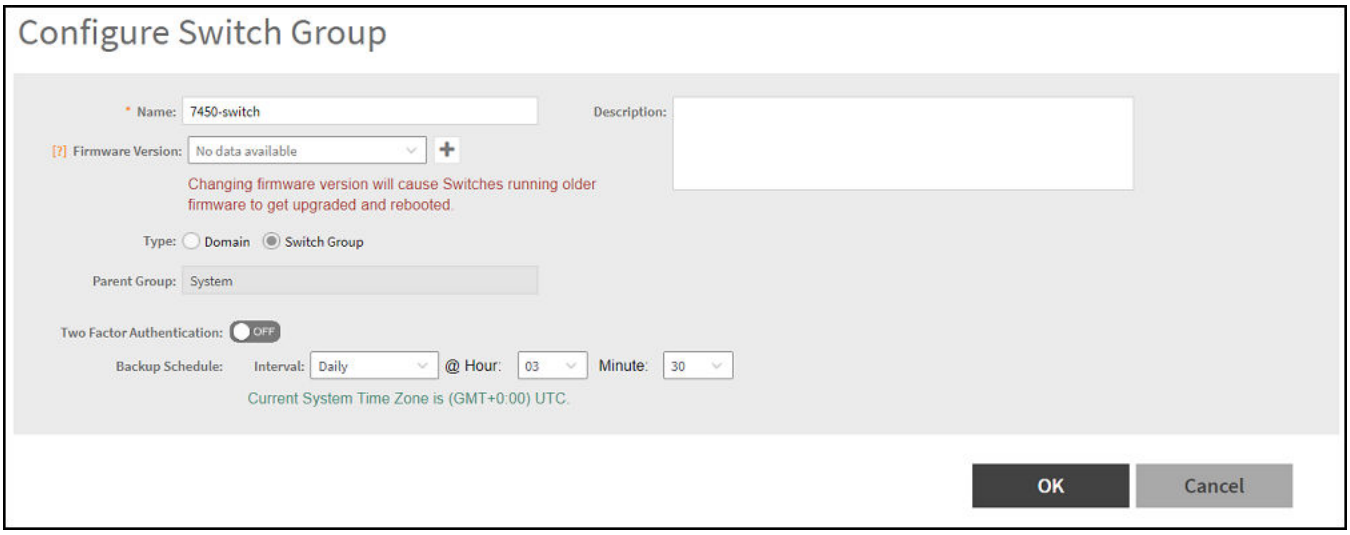


FIGURE 5 Configuring Switch Groups



Complete the following fields:

- **Name**: Type the name of the switch group that you want to create.
- **Description**: Enter a brief description for the switch group.
- **Firmware Version**: Select the Firmware version (optional) which will automatically upgrade the switches (running an older version) joining the group.
- **Type**: Select **Switch Group**. For enterprise devices such as SZ-300 and vSZ-H.
- **Parent Group**: Displays the parent group under which the switch group resides

- **Two Factor Authentication**: Switch **ON** to use the **Console CLI** or **Remote CLI** to access the **Switches**.

  NOTE
  Turning ON this feature will disable the SSH access to the switches.

  A **message** dialog box is displayed, click **OK**.

- **Backup Schedule**: Allows you to schedule the backup. From the **Interval** drop-down list, select the type of backup such as **Daily**, **Weekly**, or **Monthly**. If the backup selected is **Daily**, you can configure **@Hour** , and **Minute** fields. If the backup selected is **Weekly**, you can configure the **Every** (day of the week), **@Hour** , and **Minute** fields. If the backup selected is **Monthly**, you can configure **Every** (date), **@Hour** , and **Minute** fields.

  NOTE
  The default backup time for scheduling a **Daily** backup is 3:30 a.m. The backup schedule is configured on the level one switch group.

6. Click **OK**.

   The switch group is created under the selected parent group in the **Organization** tab. The switch group is identified with "SG" symbol.

Creating Switch Registration Rules

You can create registration rules for switch groups, which are identified and approved by the controller to establish connections. Typically, the switch is registered with the controller using an IP address, subnet, or model number.

Complete the following steps to create a registration rule.

1. On the menu, click **Network** > **Wired** > **Switch Registration** to display the **Switch Registration** window.

FIGURE 6 Switch Registration



2. Click + Create icon to display the **Switch Registration Rule** dialog box.

   Complete the following fields:

   - **Rule Description**: Provide a brief description of the registration rule you are creating to put the switches into specific groups.
   - **Group Name**: Select the switch group to which you want to apply this rule from the list.
   - **Rule Type**: Select **IP Address Range**, **Subnet**, or **Model Number** to apply the rule to the switch based on the rule type.
     - If you select **IP Address Range**, you must provide the range of the IP addresses for which this rule will apply.
     - If you select **Subnet**, you must provide the network address and subnet mask that will apply to the rule.
     - If you select **Model Number**, you must provide the model number of the device from the drop down list.

FIGURE 7 Creating Switch Registration Rules - IP Address Range

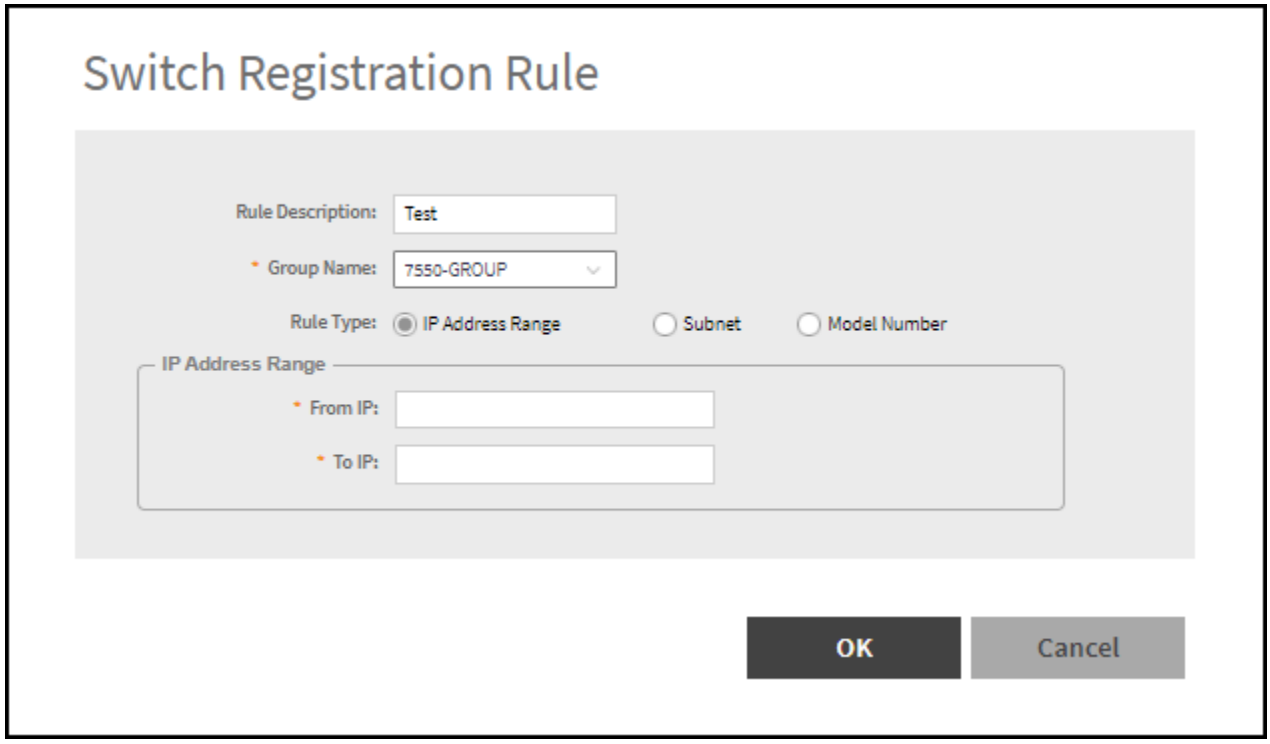


FIGURE 8 Creating Switch Registration Rules - Subnet

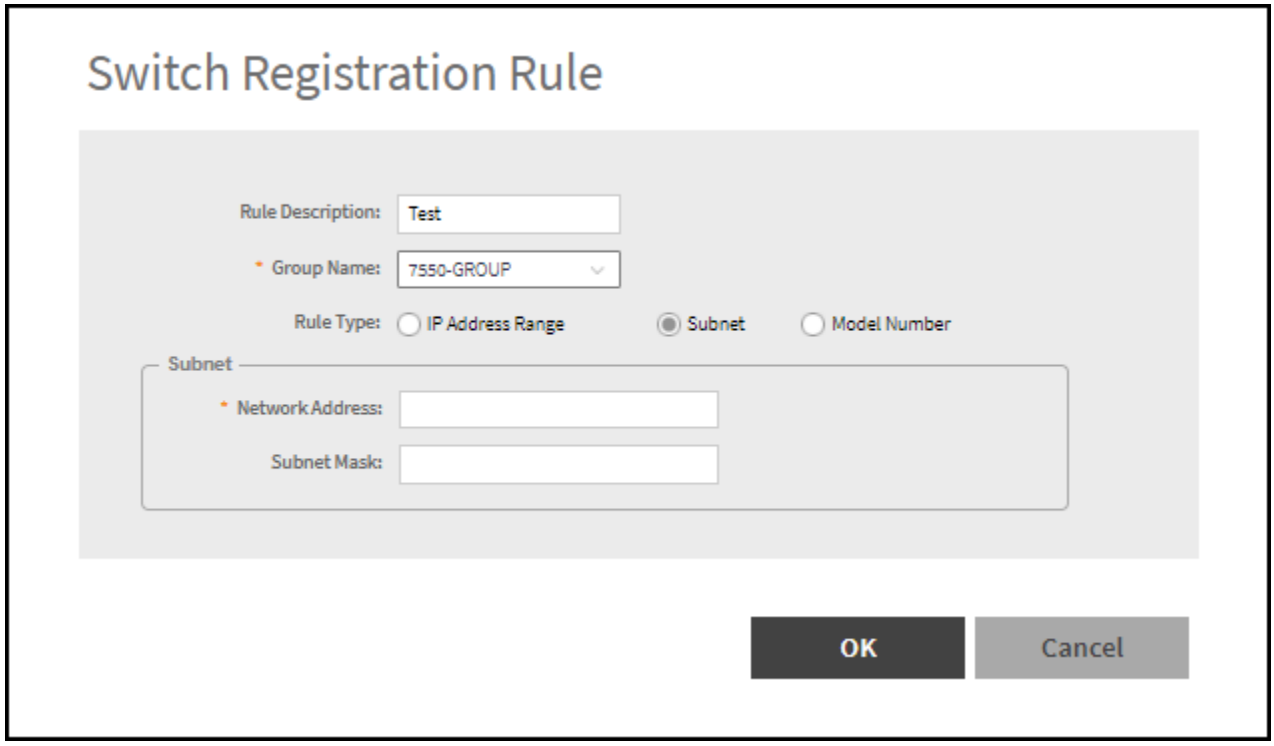
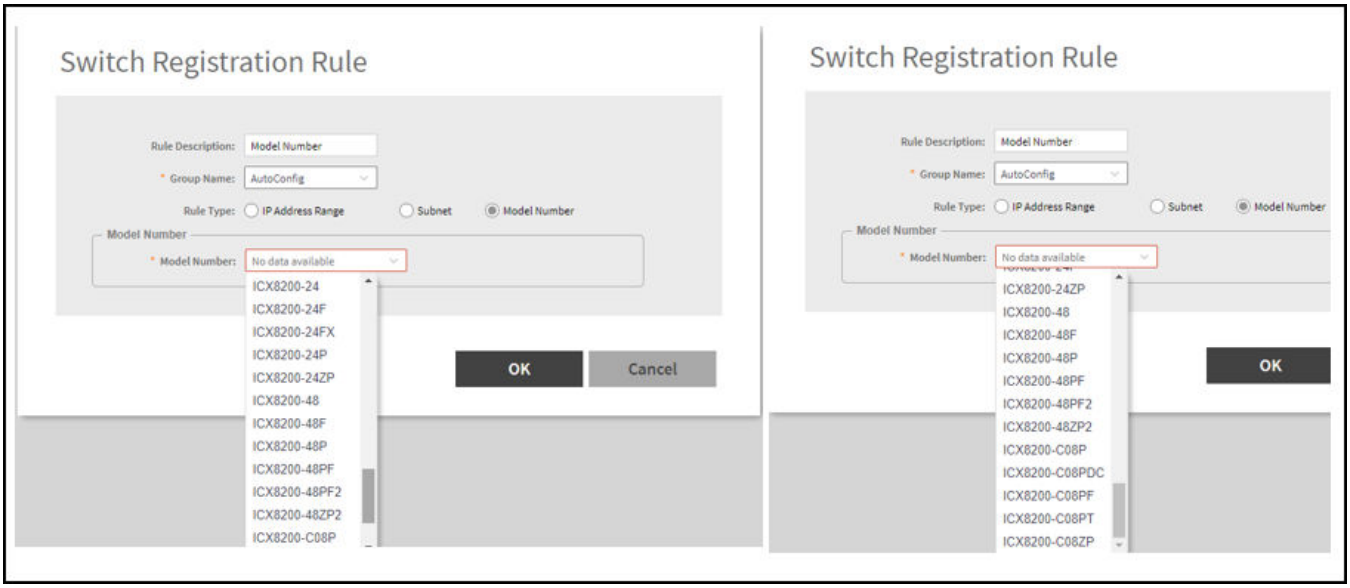


FIGURE 9 Creating Switch Registration Rules - Model Number



3. Click **OK**.

   You can edit, copy and delete the rule by selecting the rule and clicking **Configure**, **Clone**, and **Delete**, respectively.

   After the registration rules are created, they can be rearranged using the **Up** and **Down** options. They can be arranged in an order of priority. After the order of priority for the list of rules is finalized, click **Update Priority** to confirm.

Approving Switches

The switch must be approved so that it can be discovered and monitored by the controller.

- Switches that do not match any registration rule are automatically in the default group.
- At this point, a switch is not managed and the status is shown as offline.
- To actively manage a switch in this predicament, you must move it from the staging group to any other switch group or domain in SZ300 and vSZ-H platforms. In SZ100 and vSZ-E platforms, the default group behavior is similar to any other group. Refer to Moving the Switches between Groups on page 29 for more information.

  NOTE
  A switch capacity license (CAPACITY-SWITCH-DEFAULT) is available for controllers and switches managed by the controllers. The license is activated for devices running SmartZone 5.1 or later. Upgrading to SmartZone 5.1 from an earlier version activates the license by default. A 90-day license version is then available for trial or purchase. The controller manages switches only as defined in the Switch Capacity license and rejects individual switches or stacks when license capacity is reached. Any switch that exceeds license limits is moved to the service group, where it cannot be configured. When license capacity is again available, the controller accepts the switch for management. For the controllers (SZ100 or SZ300), a trial license will allow adding the maximum number of switches supported. In the case of vSZ-E or vSZ-H, a trial license will allow the addition of 5 switches.

  NOTE
  Based on the switch capacity license (CAPACITY-SWITCH-HA), you can approve a failover switch on a standby cluster to switch over to the original cluster.

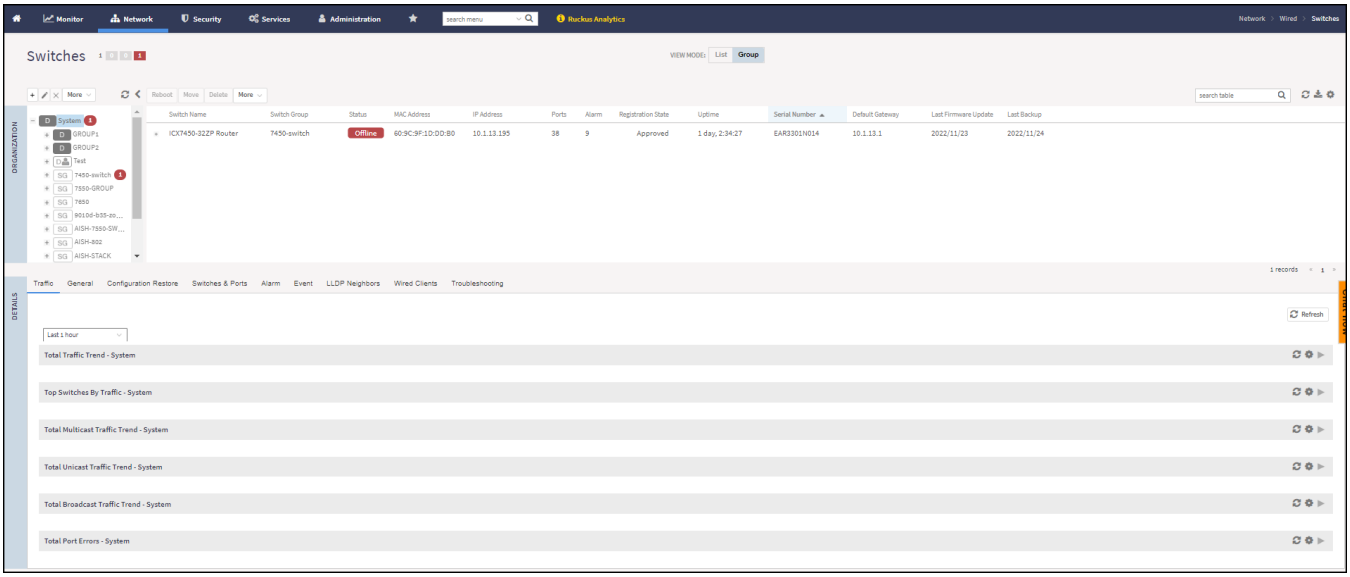
The recommendation is to always use switch registration rules so that the switches are placed in the correct switch group and avoid manual intervention.

Moving the Switches between Groups

You can move the switches within any group or sub-group within the system hierarchy to manage it.

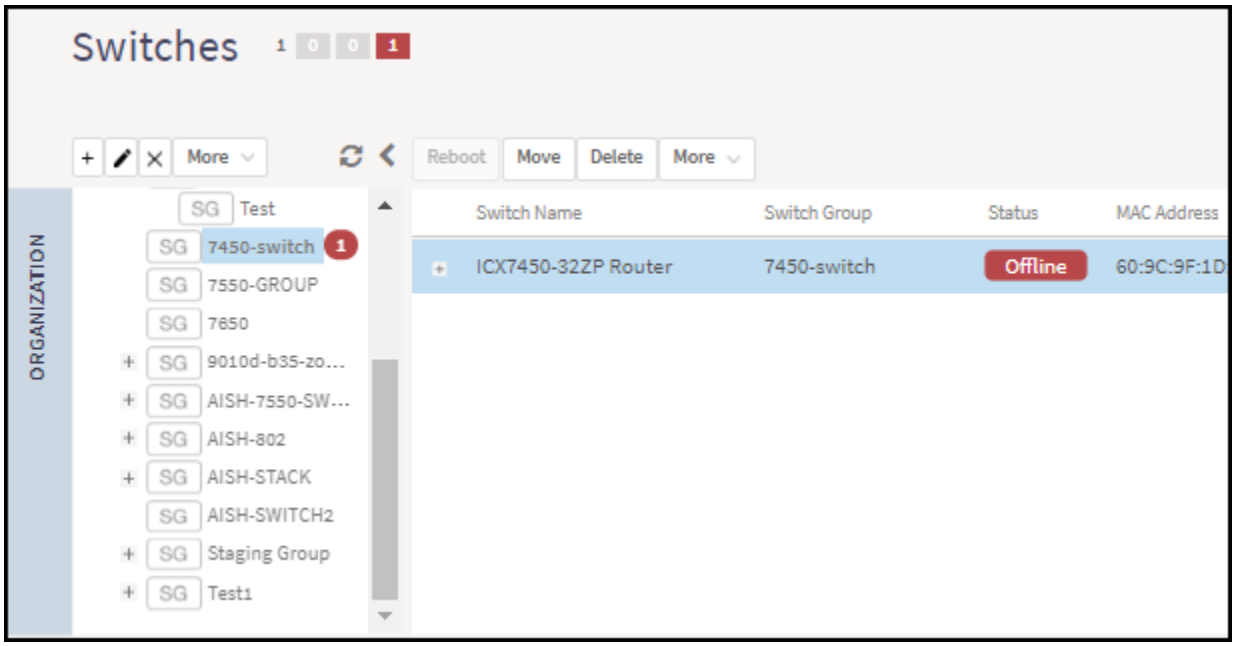
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 10 Switches



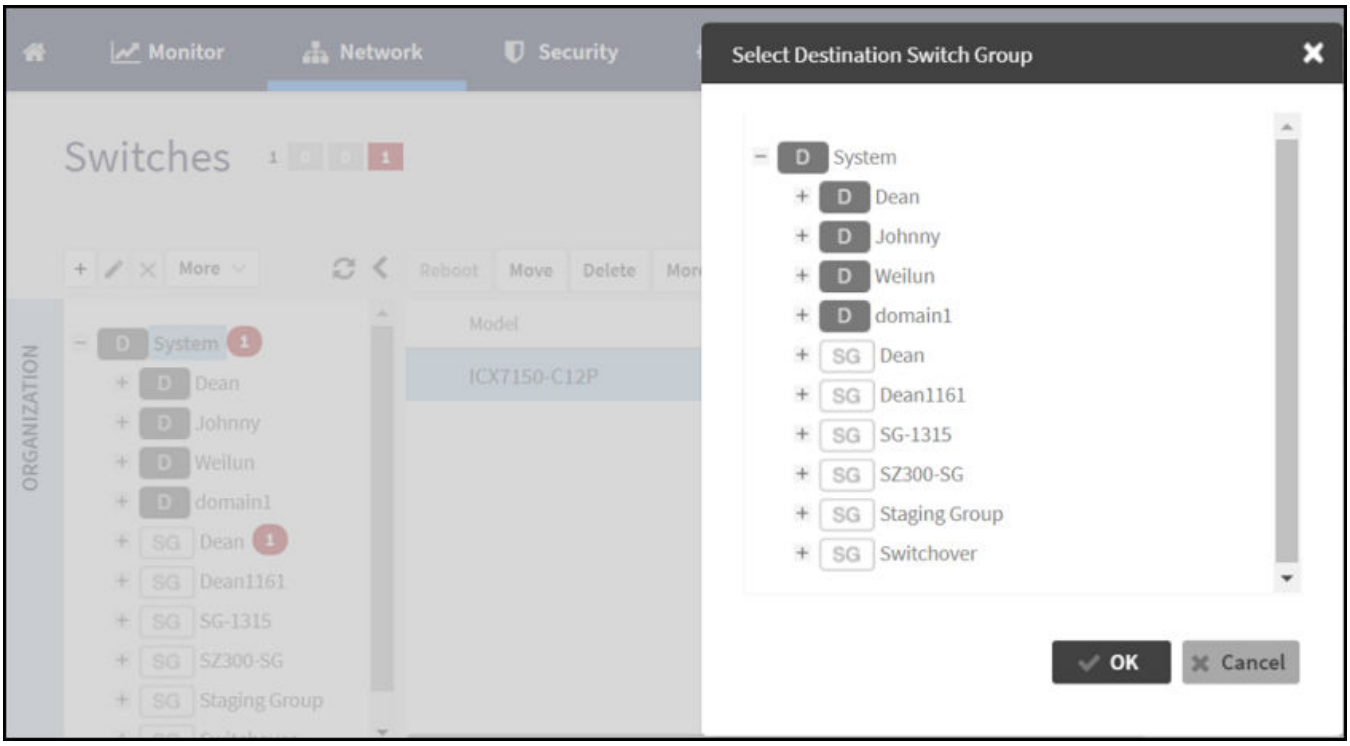
2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch** that you want to move.

FIGURE 11 Select Switches



3. Click **Move** icon to display the **Select Destination Switch Group** dialog box.

FIGURE 12 Moving the switch



The **Select Destination Switch Group** dialog box displays the system hierarchy.

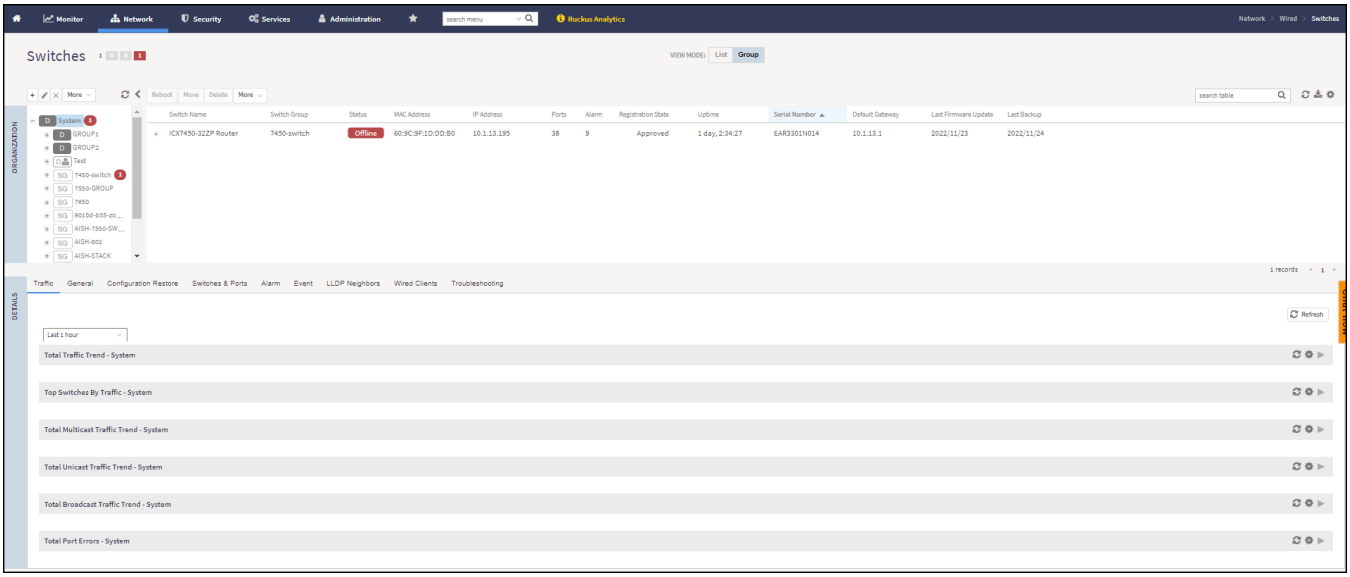
4. Select a **Domain** > **Switch Group** or **Switch Group** under which you want to move the selected switch.
5. Click **OK**.

Deleting Switches

You can delete switches that you do not want the controller to manage anymore.

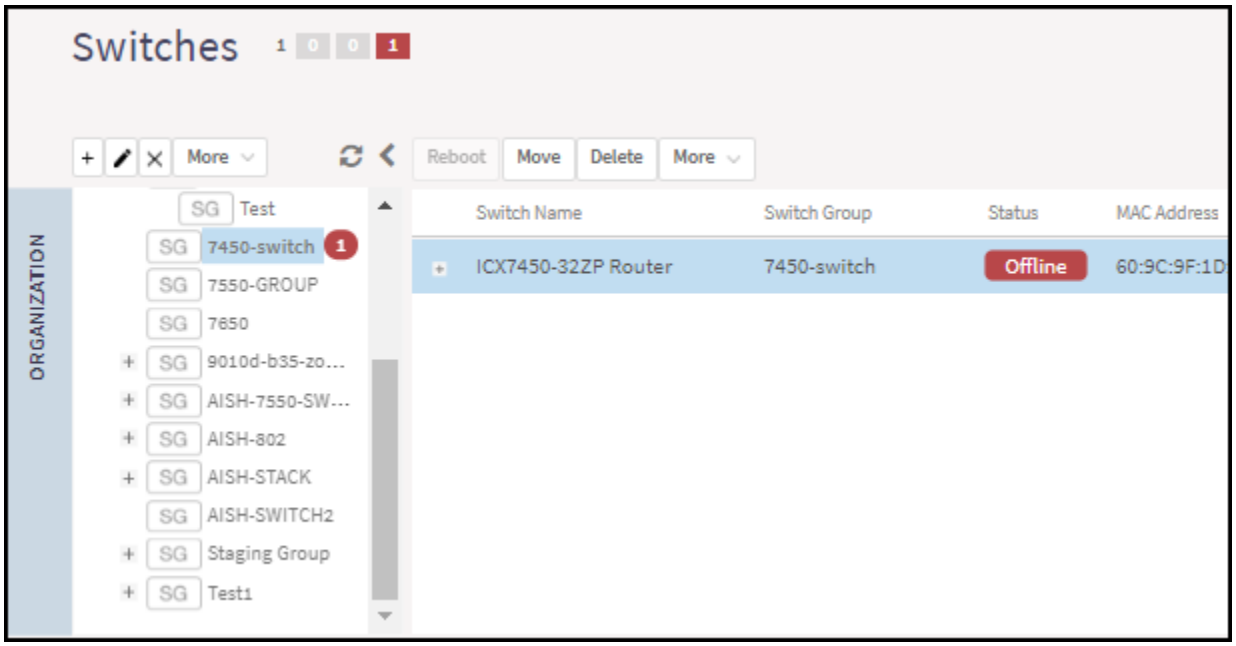
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 13 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch** that you want to delete.

FIGURE 14 Select Switches



3. Click **Delete** icon.

   The selected switch is deleted, and it will not be managed by the controller interface.

Backing up and Restoring Switch Configuration

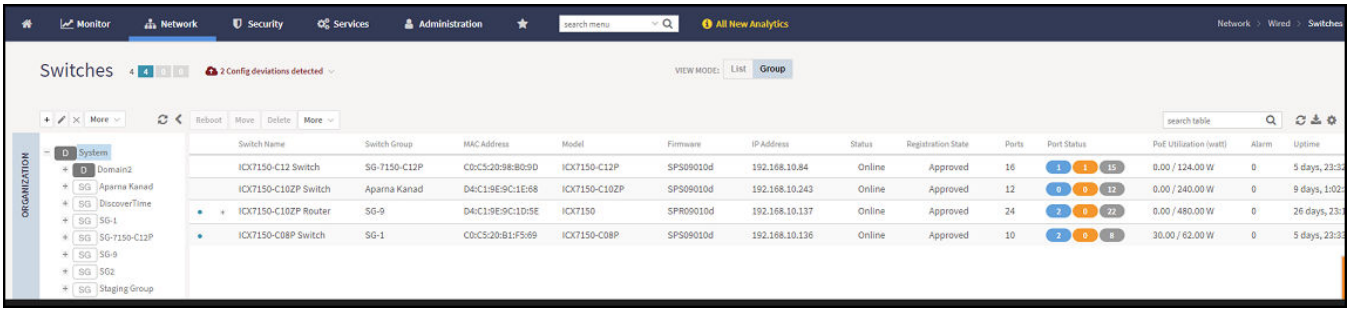
The controller can back up the switch's running configuration. By default, controller makes a backup of switch configuration on a daily basis. The configuration is only stored if there is a change between the last configuration backup and the current backup. Otherwise, it is discarded. Controller saves the last seven configuration backups. When needed, these backups can be restored to the switch. While performing network maintenance, you can initiate a backup without having to wait for the daily backup.

Perform the following steps to configure switch backups.

NOTE
Be sure to sync the controller to the NTP server during installation.

1. On the menu, click **Network** > **Wired** > **Switches** to disaply the **Switches** window.

FIGURE 15 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** to perform switch group configuration backup or select a **Switch** to perform a switch configuration backup.

FIGURE 16 Switch Group Configuration Backup

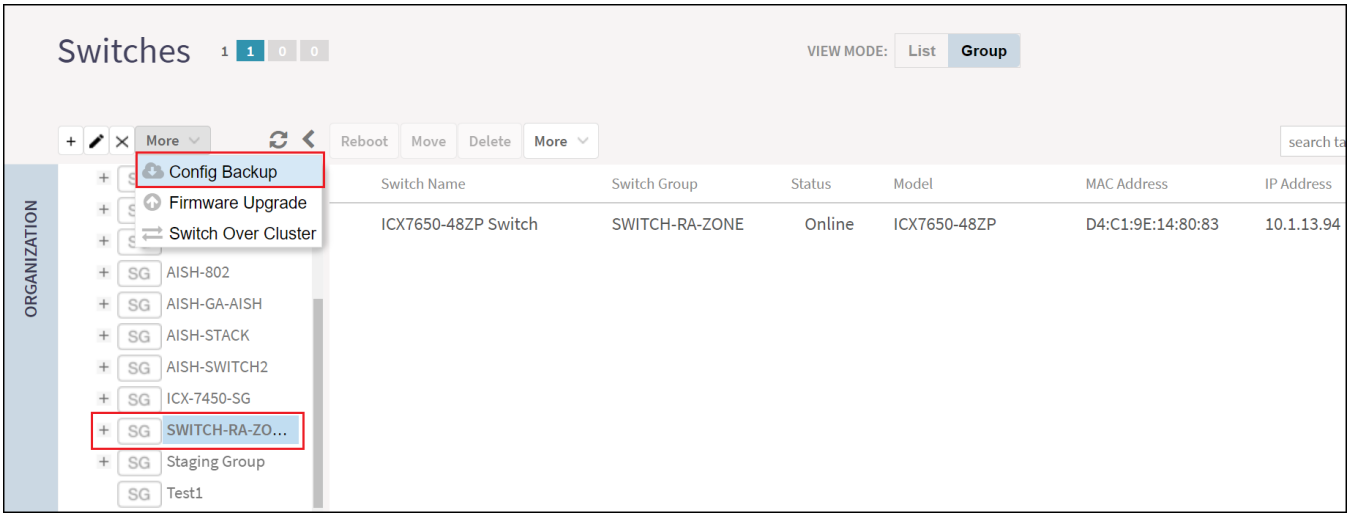
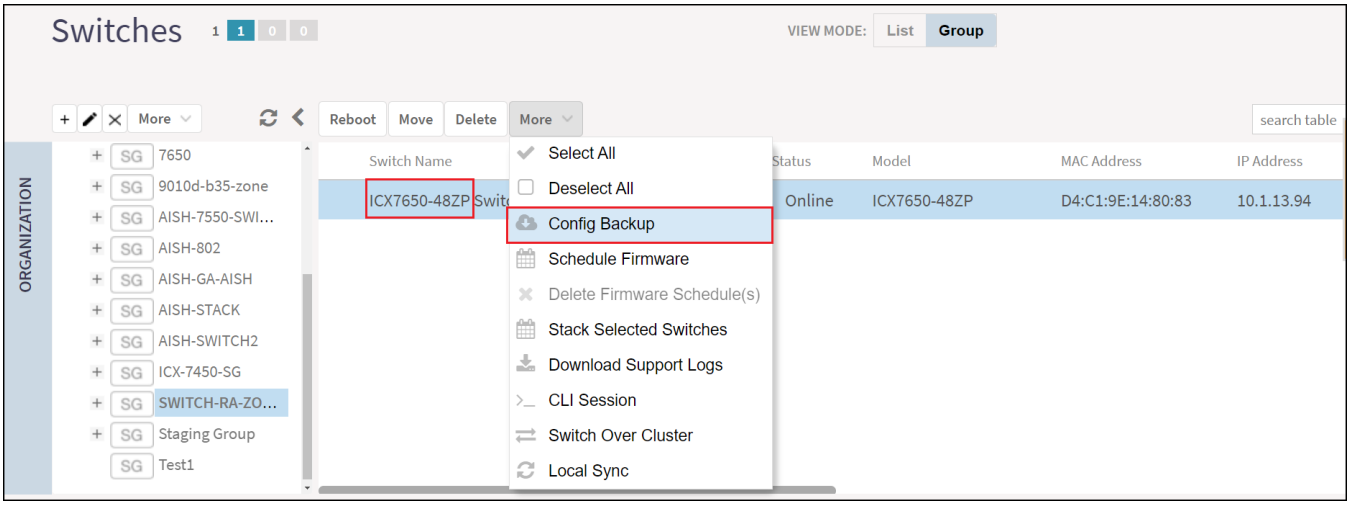
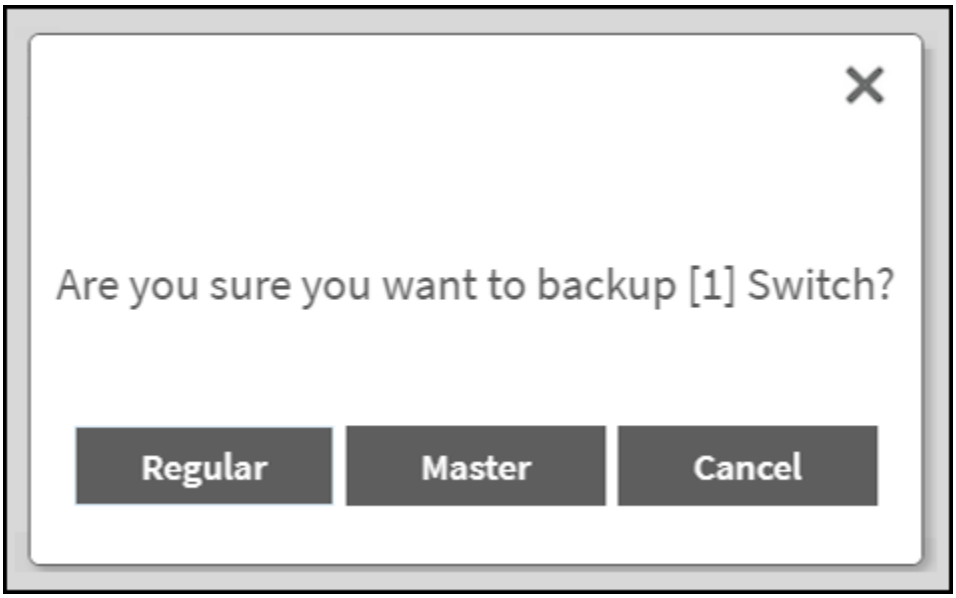


FIGURE 17 Switch Configuration Backup



3. Click **More** > **Config Backup** to display the **Configuration Backup** dialog box.

FIGURE 18 Configuring Backup



A confirmation message is displayed asking the type of backup that must be carried such as **Regular** or **Master**.

The master configuration backup is for the configuration change alert feature. It allows you to select a switch configuration backup to serve as the master configuration backup. If the latest regular configuration backup differs from the master configuration backup, the controller will automatically display an alert indicating a configuration change. The regular configuration backup are like the scheduled configuration backup that can be triggered by the user at any time.

NOTE
It is recommended to use master configuration backup, as the regular configuration backup will be removed if there are more than seven different configuration backups. The master configuration backup will not be removed in this case.

4. Click **Master**. A message is displayed confirming that the backup process has been initiated. Click **OK**.

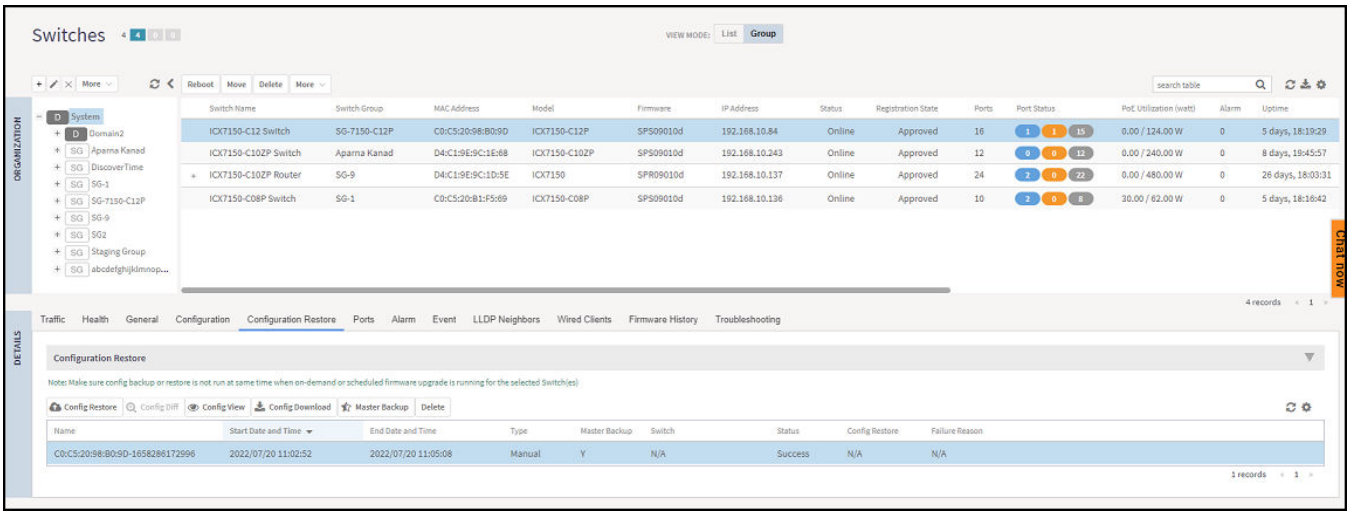
   After the backup is completed, the status is recorded in the **Configuration Restore** tab.

   NOTE

   - As soon as the switch connects to the controller, and when it is online, the controller retrieves all the information about the switch.
   - The controller maintains seven of the latest configuration backups for each switch.
   - The controller automatically backs up the configuration of each switch, once, every 24 hours.
   - If a previous switch configuration matches the current configuration, the latest configuration is saved and the old configuration is removed.

   Follow these steps to restore an individual switch configuration.

FIGURE 19 Configuration Restore



a. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch** for which you want to perform configuration restore.

b. In the **Details** tab, click **Configuration Restore** tab to display the listed configurations in the table.

c. Select a **Configuration** and click **Config Restore**. A message is displayed stating "Are you sure you want to restore this backup configuration to the Switch?", click **Yes** to display the message "Switch Configuration restore operation has started and it will take up to two minutes to complete. Refer to the configuraton table to know the status.", click **OK**.

Follow these steps to view the switch configuration differences.

a. In the **Configuration Restore** tab, select the **Configurations** for which you want to view differences in configuration details. You can use **Ctrl** and select the **Configurations**.

b. Click **Config Diff** icon to view the **Configurations Details** dialog box.

In the **Configuration Restore** tab, select the configuration to do the following actions.

- Click **Config View** icon to disaply the **Switch Config View** dialog box to see the configuration details.
- Click **Config Download** icon to download the copy of the configuration file.
- Click **Master Backup** icon to backup the switch configuration.
- Click **Delete** icon to delete the configuration file.

Rehoming Switches

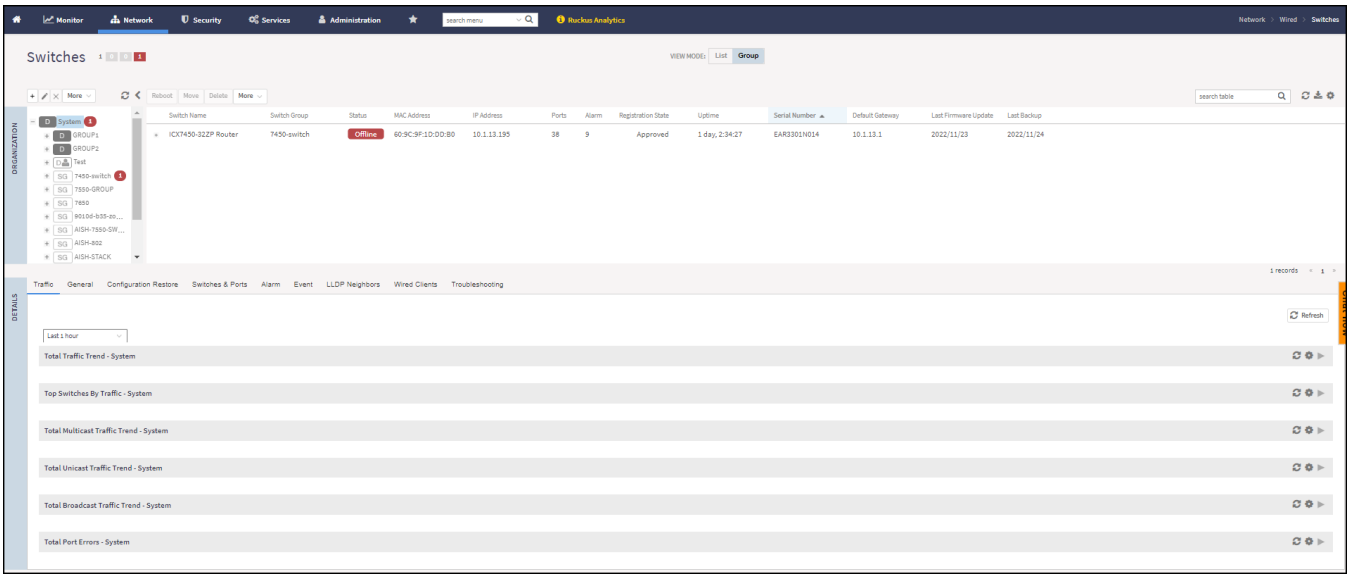
Rehoming is the process of returning the switches that have failed over to the standby cluster back to their original cluster (once it becomes available). Rehoming must be done manually. Switches that have failed over continue to be managed by the failover cluster until you rehome them.

NOTE
You can rehome switches only in a cluster redundancy environment. When switches of a certain active cluster fail over to a standby cluster, you must manually restore them to the original cluster after the active cluster is fixed and back to service.

Complete the following steps on the standby cluster to rehome switches to the original cluster:.

1. Select **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 20 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch** to rehome.
3. In the **System Domain**, click **More** > **Rehome Active Cluster** to display the **Confirmation** dialog box.
4. Click **Yes**.

Switching Over Clusters

Switchover helps move individual switches or switches in a switch groups across clusters.

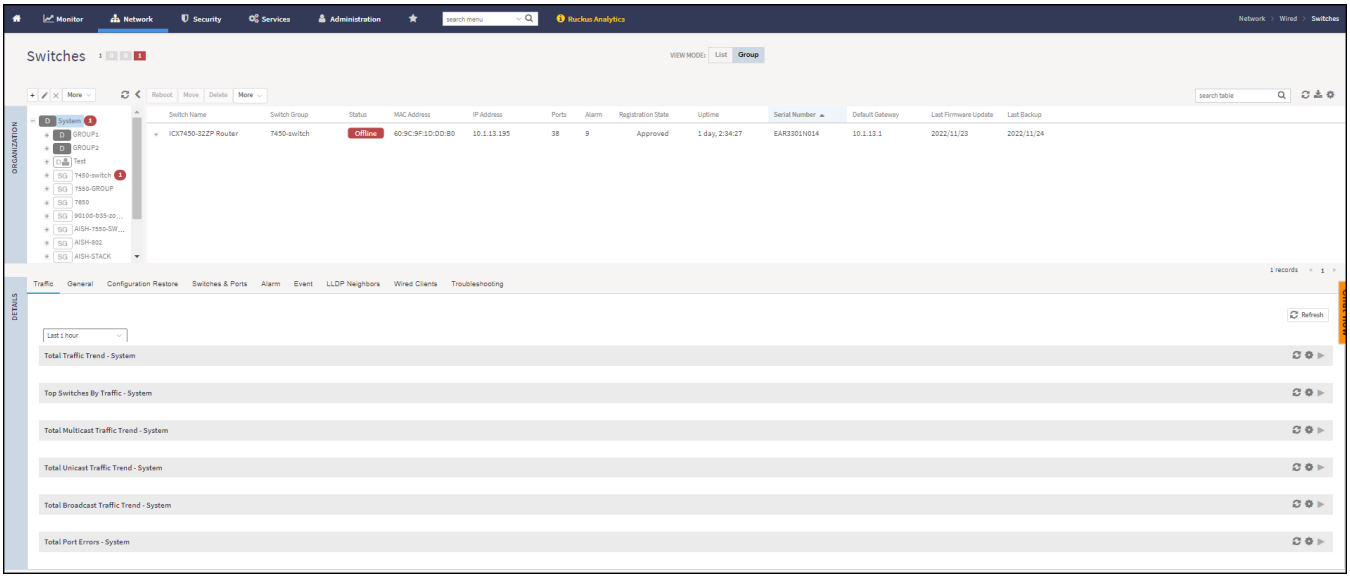
NOTE
Ensure that a switch registation rule is created on the target cluster before switching over to another cluster. For more information, refer to Creating Switch Registration Rules on page 25.

NOTE
Depending on the switch High Availability license on the standby cluster switches must be approved so that it can be discovered and monitored by the controller. For more information, refer to Approving Switches on page 28.

Complete the following steps to switch over from one cluster to another.

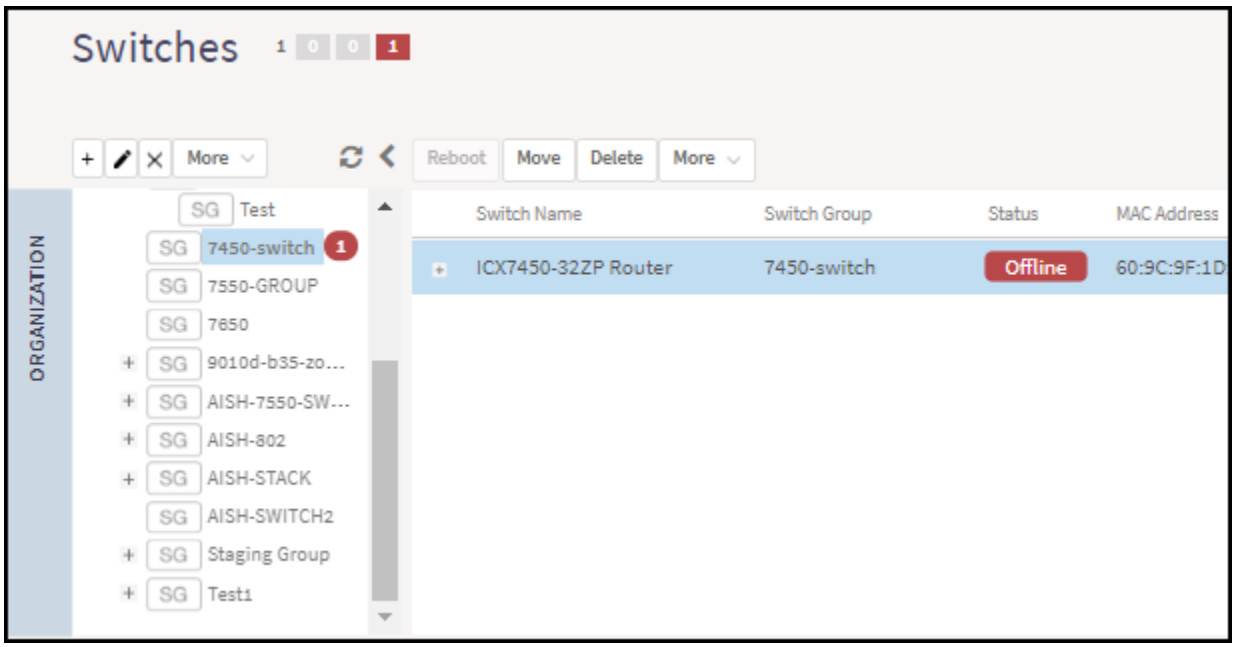
1. On the menu, click **Network** > **Switches** > **Switches** to display the **Switches** window.

FIGURE 21 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**.

FIGURE 22 Select Switch



3. In the **Organization** tab, click **More** > **Switch Over Cluster** to display the **Switch Over Cluster** dialog box.
4. In the **Control IP** field, enter the control IP address of the switchover target cluster.

5. Click **OK**. A **Confirmation** dialog box is displayed.
6. Click **YES** to confirm.

Scheduling a Firmware Upgrade for Switch Group

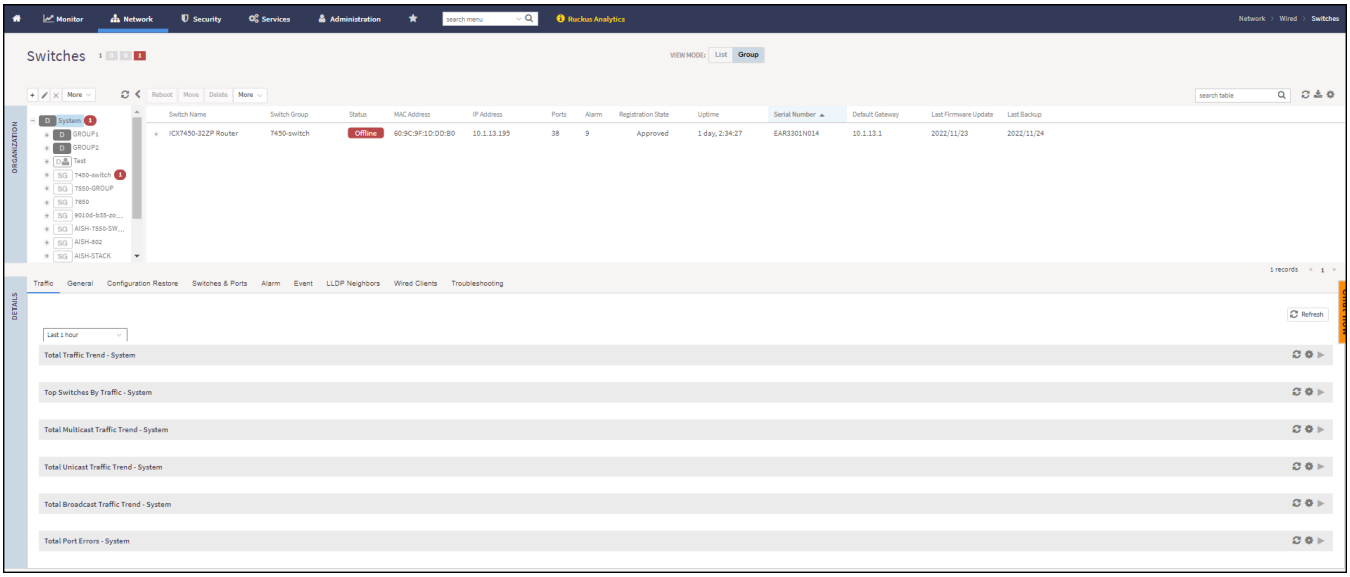
You can upgrade a switch group on a Level 1 group that has no default firmware setting. The forced upgrade allows the device to remain in the same firmware type (Layer 2 still Layer 2, Layer 3 still Layer 3) with only a change to the version type.

NOTE
If the switch group has a default firmware selected the **Firmware Upgrade** option is unavailable.

Complete the following steps to perform a firmware upgrade on the switch group.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 23 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group**.

3. Click **More** > **Firmware Upgrade** to display the **Upgrade Firmware (Group)** dialog box.

FIGURE 24 Selecting Firmware Upgrade for a Switch Group

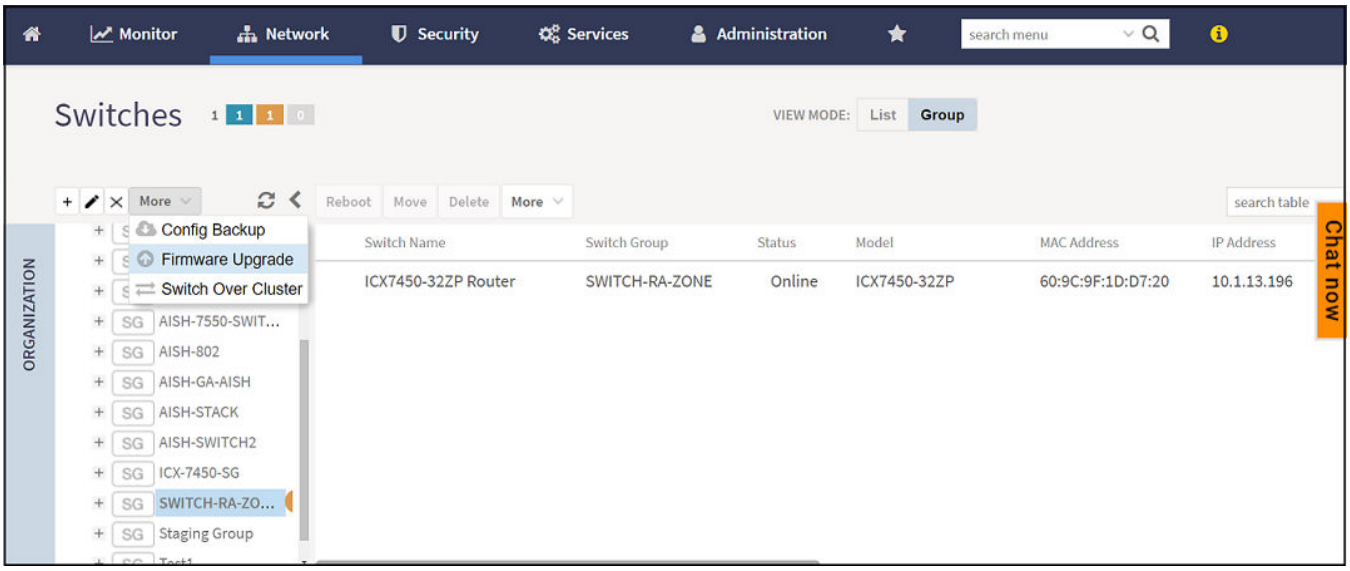
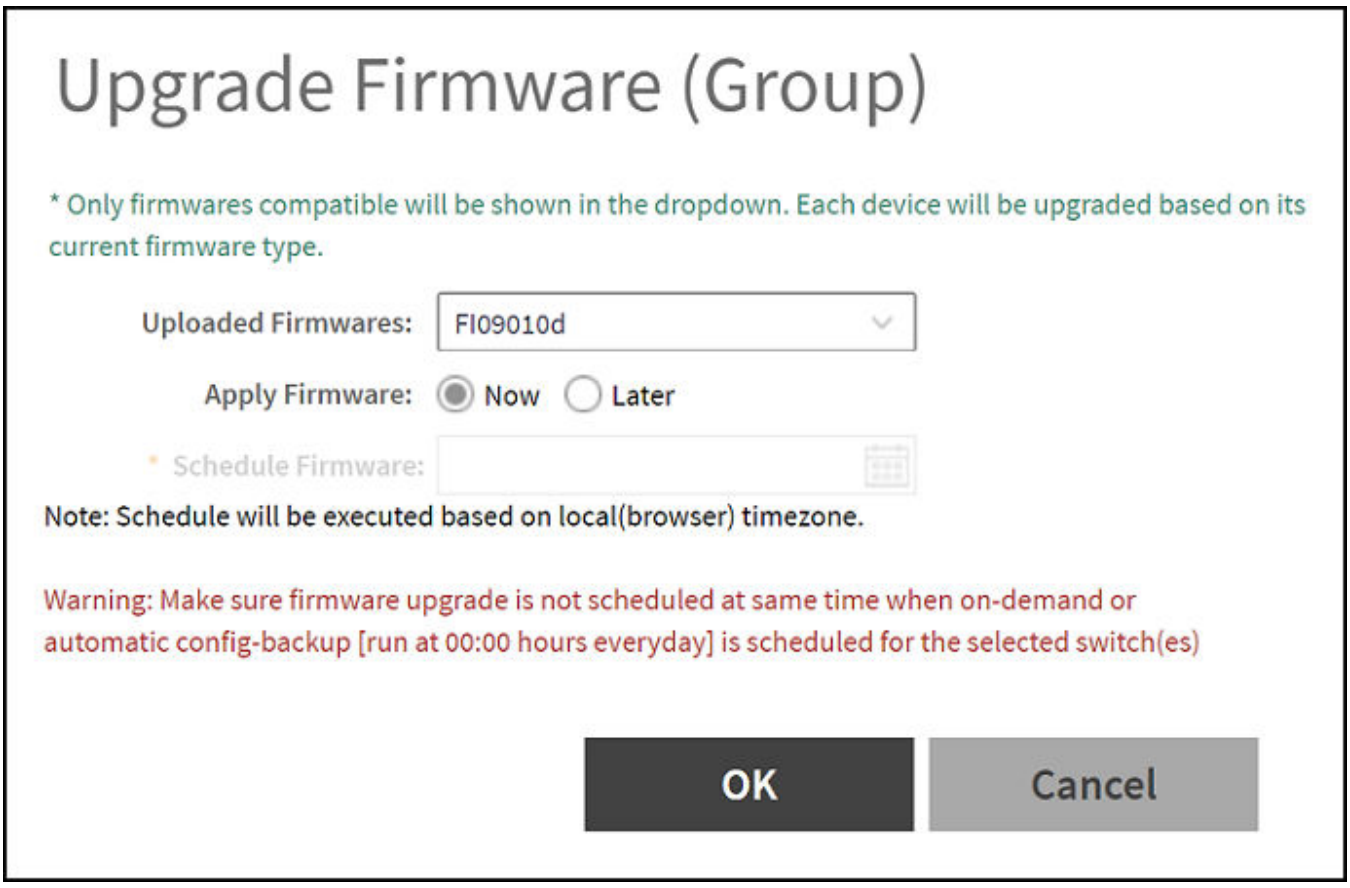


FIGURE 25 Scheduling the Upgrade for a Switch Group



4. Complete the following fields:
   - **Uploaded Firmwares**: Select firmware from the list.
   - **Apply Firmware**: Select Now or Later to set the new firmware version to the switch group.
   - **Schedule Firmware**: If you select Later for **Apply Firmware**, you must select the date to schedule the upload.
5. Click **OK**.

Scheduling a Firmware Upgrade for Selected Switches

You can upgrade or downgrade the firmware version of a switch or multiple switches that you are monitoring. You can upgrade the firmware on demand or schedule a firmware update for a list of selected switches.

Upload a valid firmware which is greater than version 8.0.80 to the controller.

NOTE
Ensure you sync the controller to the NTP server during installation. You can also do this from, go to **Administration** > **System** > **Time** > **Switches**.

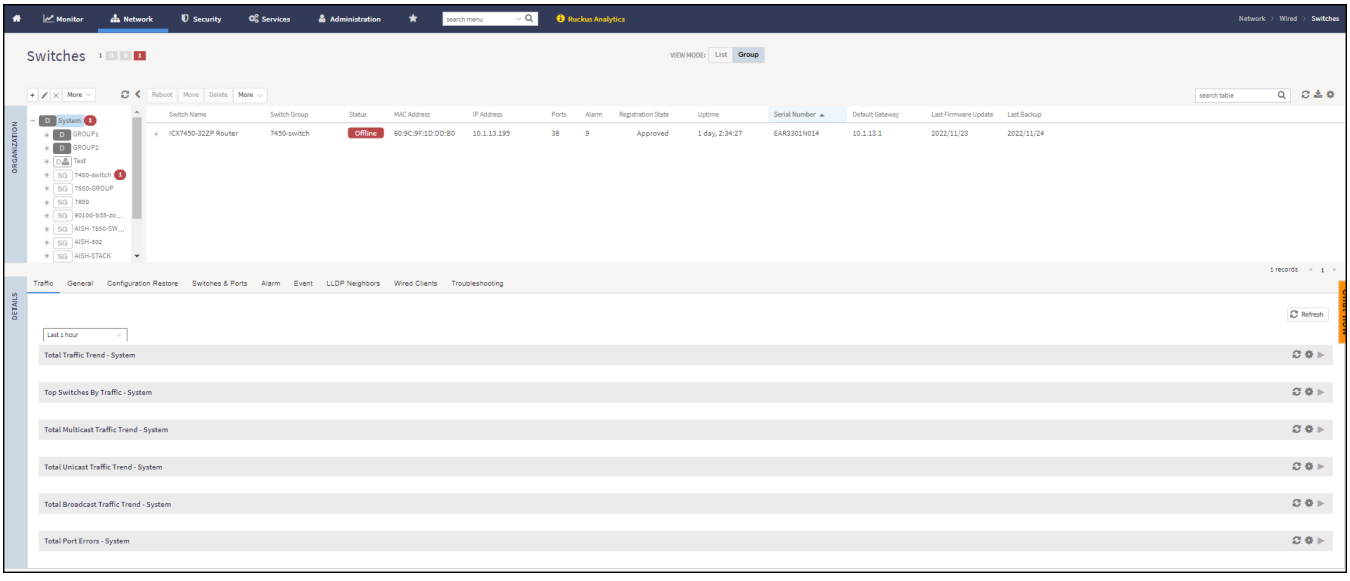
To upgrade the firmware for a group of switches, you must select multiple switches at the same time and perform steps 3 to 7. For more information on uploading the switch firmware, see *Uploading the Switch Firmware to the Controller*.

NOTE
Only firmware versions later than ICX 8.0.80 are supported.

Scheduling Firmware Upgrade

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

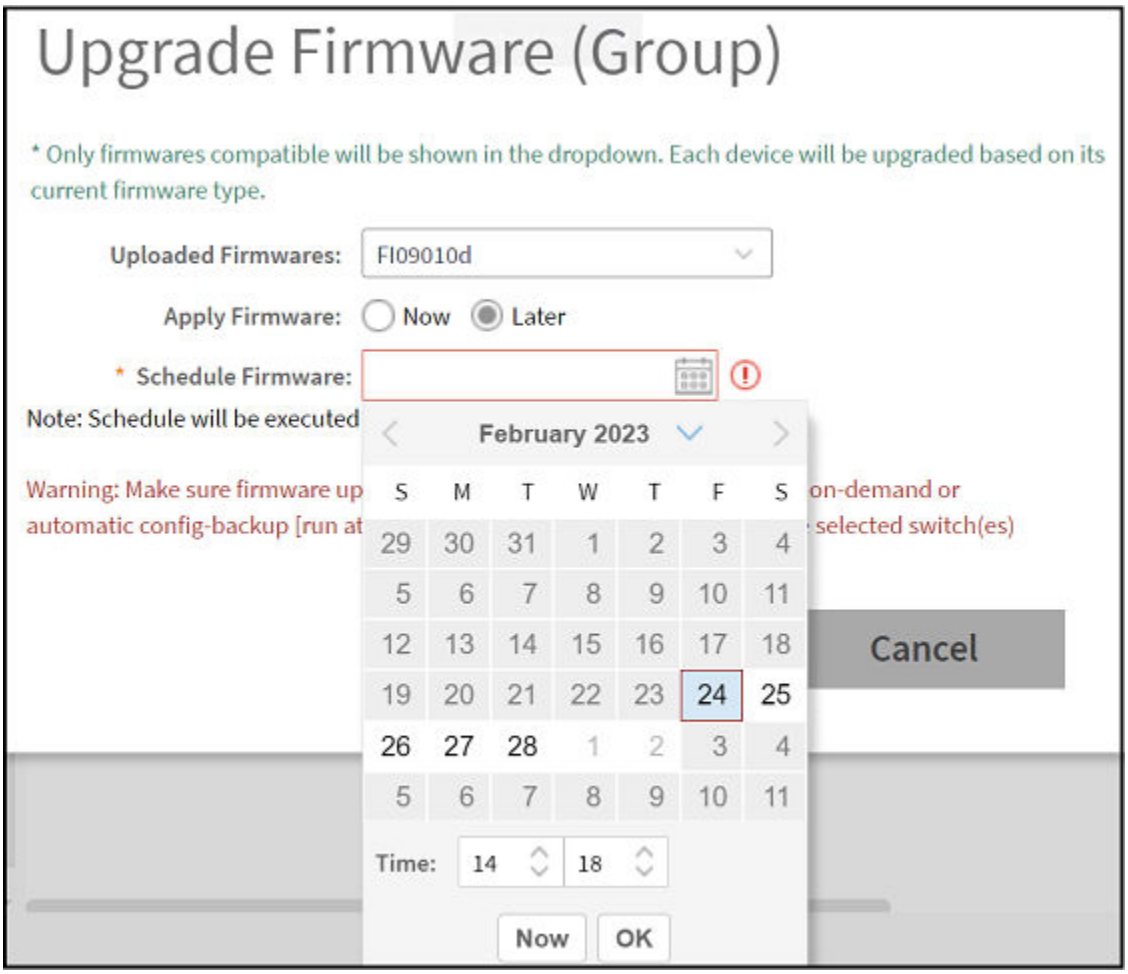
FIGURE 26 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch** that you want to upgrade.

3. Click **More** > **Schedule Firmware** to display the **Upgrade Firmware** dialog box.

FIGURE 27 Scheduling Firmware Upgrade



4. Complete the following fields:
   - **Uploaded Firmware**: Select the firmware version that you want the switch to be upgraded to.
   - **Firmware Type**: Select type of firmware you want to upload to the switch. Options include Switch and Router images.
   - **Apply Firmware**: Set when you want to apply the new firmware version to the switch. You can select Now or Later to schedule your upload. If you select Later, then you must select the date from the **Schedule Firmware** field.
5. Click **OK**.

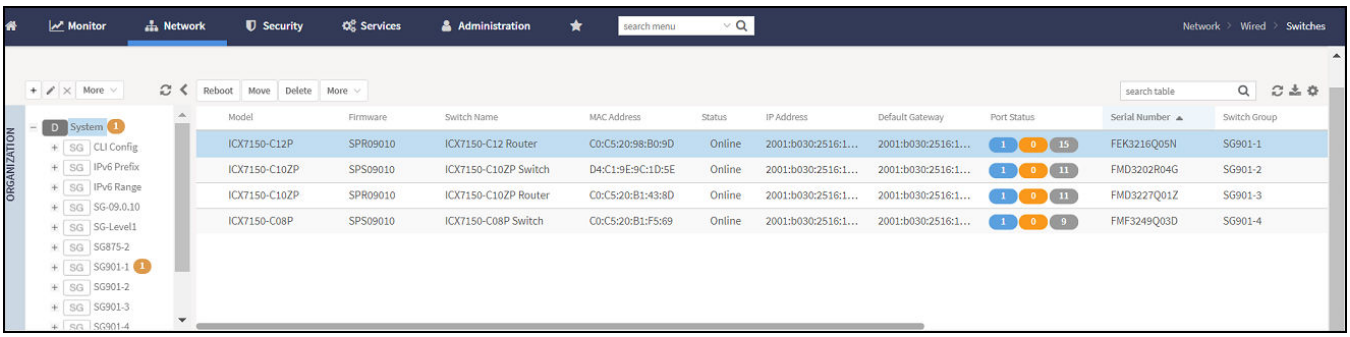
Viewing Switch Information

Details such as switch status, firmware version, and IP address are available for individual switches, stacks, and switch groups.

To view information on a switch, a stack, or a switch group, perform these steps.

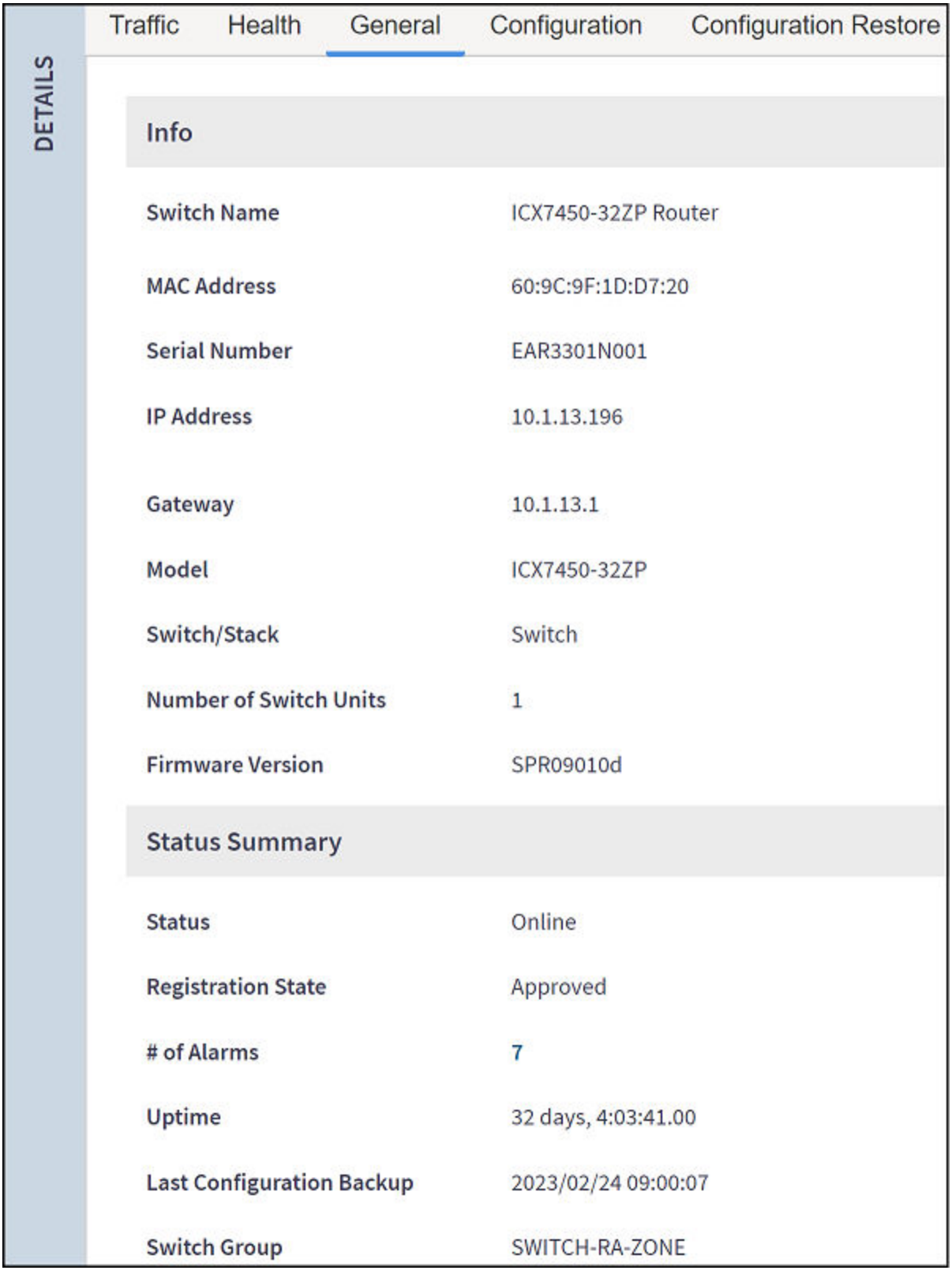
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 28 Switches



2. In the **Organization** tab, Select the **Domain** > **Switch Group** or **Switch Group** and select the **Switch** to display information specific to it. In the **Details** tab, click **General** tab to display the switch information.

FIGURE 29 Switch Stack and General Information



The following information about the selected switch is displayed in the **General** tab:

- Switch Name: The name of the switch or group.
- MAC Address: The MAC address of the switch.
- Serial Number: The serial number assigned to the switch.
- IP Address: The IP of the controller that monitors the switch.
- Gateway: The gateway IP address through which the switch, group, or stack forwards data.
- Model: The model number of the switch.
- Switch/Stack: Whether the selected system is a standalone switch or a stack of switches.
- Number of Switch Units: The number of switches in a group or stack.
- Firmware Version: The firmware version uploaded to the selected switch.
- Status: The status of the switch, such as Online, Offline, or Flagged.

  NOTE
  Flagged status indicates that one or more switches have an outstanding alarms and/or Port errors are seen on the switch ports. Click **Flagged** to view the flagged switches.

- Registration State: The status of the switch, such as Approved, Offline, Online, or Flagged (when an event or alarm is triggered).
- # of Alarms: The number of alarms generated for the selected switch or stack.
- Uptime: The time that has elapsed since reboot.
- Last Configuration Backup: The time the switch or stack configuration was last backed up.
- Switch Group: The name of the group to which the switch belongs.
- PoE Utilization (watts): The total switch PoE utilization. For example, if the total PoE allocation for the switch is 520 Watts, and 300 Watts are used, the column displays 300/520 W.

Configuring the Switch

SmartZone 5.1.1 introduces switch configuration capabilities. The following features are added:

- **Zero Touch Provisioning**: Greatly simplifies initial deployment of switches. Users can define switch configuration at a switch group level. Any new switch joining the group automatically gets provisioned.
- **Ongoing Configuration Changes**: Users can further modify the switch configuration as a part of network maintenance. This includes modifying switch group level settings, port settings, and routing interfaces.
- **Stack formation**: Users can configure individual switches to be formed into a stack directly from the controller.
- **Configuration copy**: Users can copy configuration from a working switch to one or multiple new switches seamlessly.

You can view and modify various configuration parameters of switches from the controller web interface. You can create switch configuration profiles at the group level, individual switch level and at the port level.

The **Configuration** page displays common configurations based on DNS, allows setting configuration values for a family of switches and also provides a summary of the switch configuration history.

You can update the configuration profile for new and existing switches, switches that join the controller after being offline, switches that may or may not have local feature changes via CLI/Telnet/SSH/other web interfaces.

After the switch configuration is updated successfully, you can continue to monitor the configuration deployed on the switch. If the switch configuration is not updated successfully, a message is displayed on the controller interface.

Zero Touch Provisioning using Group level Configuration

You can create and view configurations that are defined at the switch group level. Within the switch group, there is an option to define common configuration that is applicable to all the switch models in the group and another option to select configuration based on switch family, for example ICX 7150, ICX 7250, and so on. When a new switch without any existing configuration running FastIron version 8.0.90a or later version joins the controller, the group level configuration is automatically applied to the switch. This includes the global AAA settings, common configuration, and model-specific settings. If the switch joining the group already has an existing configuration, then the group level configuration is not applied during the initial join. Only the subsequent changes done at the group level are applied.

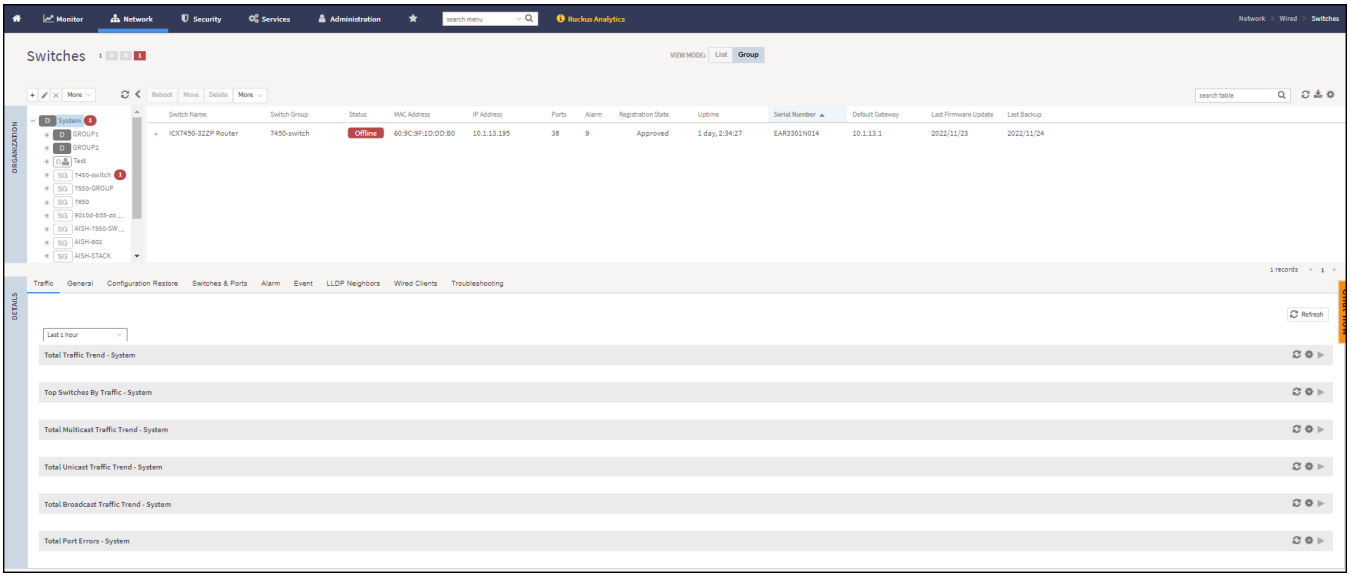
NOTE
ICX switches must run 08.0.90a or later version to take advantage of the switch configuration capabilities of the controller.

Creating Common Configuration

You can create, view, and edit the configuration settings for a group of switches.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 30 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and in the **Details** tab, click **Configuration** tab.

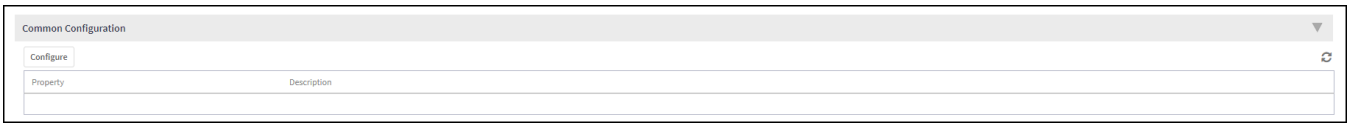
FIGURE 31 Configuration



3. In the **Common Configuration** tab, click **Configure** icon to display the **Common Configuration** dialog box.

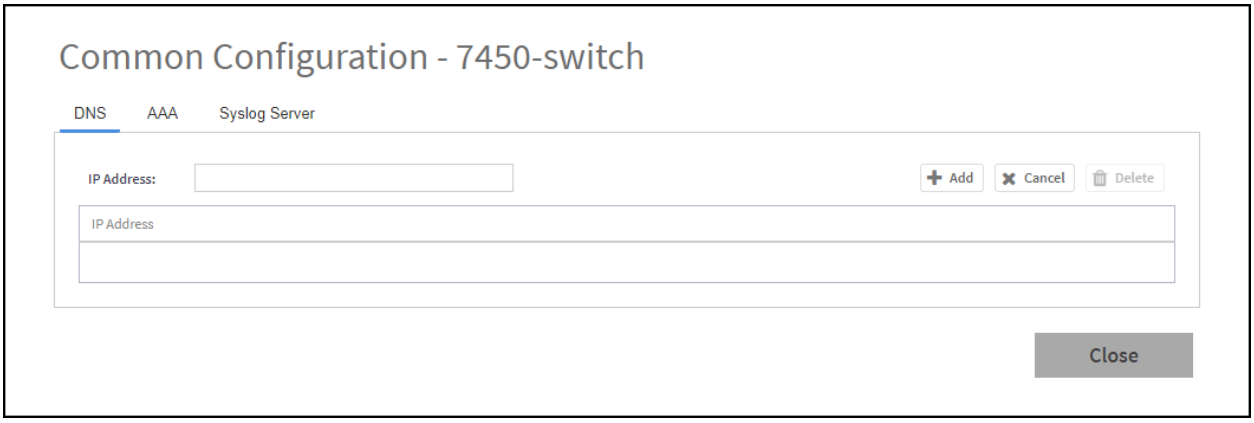
   NOTE
   In the following example, the Switch Group is the Default Group.

FIGURE 32 Common Configuration



a) Configure the **DNS** settings.
   1. Click **DNS** tab.

   FIGURE 33 DNS Settings

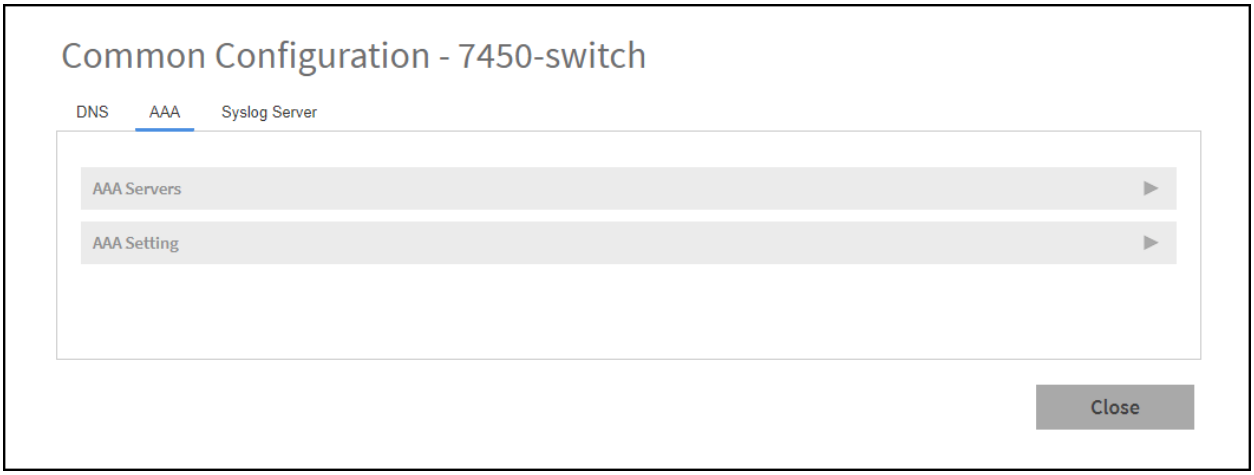


   2. Enter the **IP address** and click **Add**.

   The IP address is added to the **Common Configuration** page under **Property** and any new (factory default) switch joining this group will have the DNS configuration applied. If you want to edit the configuration, select it and click **Configure** to edit the settings.

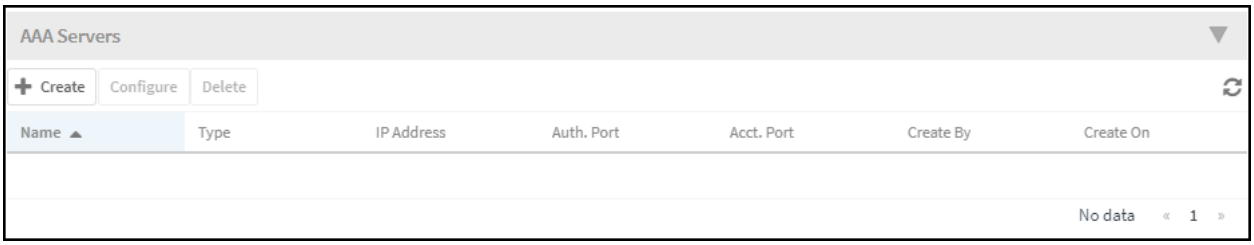
b) Configure the **AAA** settings.
   1. Click **AAA** tab.

FIGURE 34 AAA Settings



2. Configure the **AAA Servers** settings.

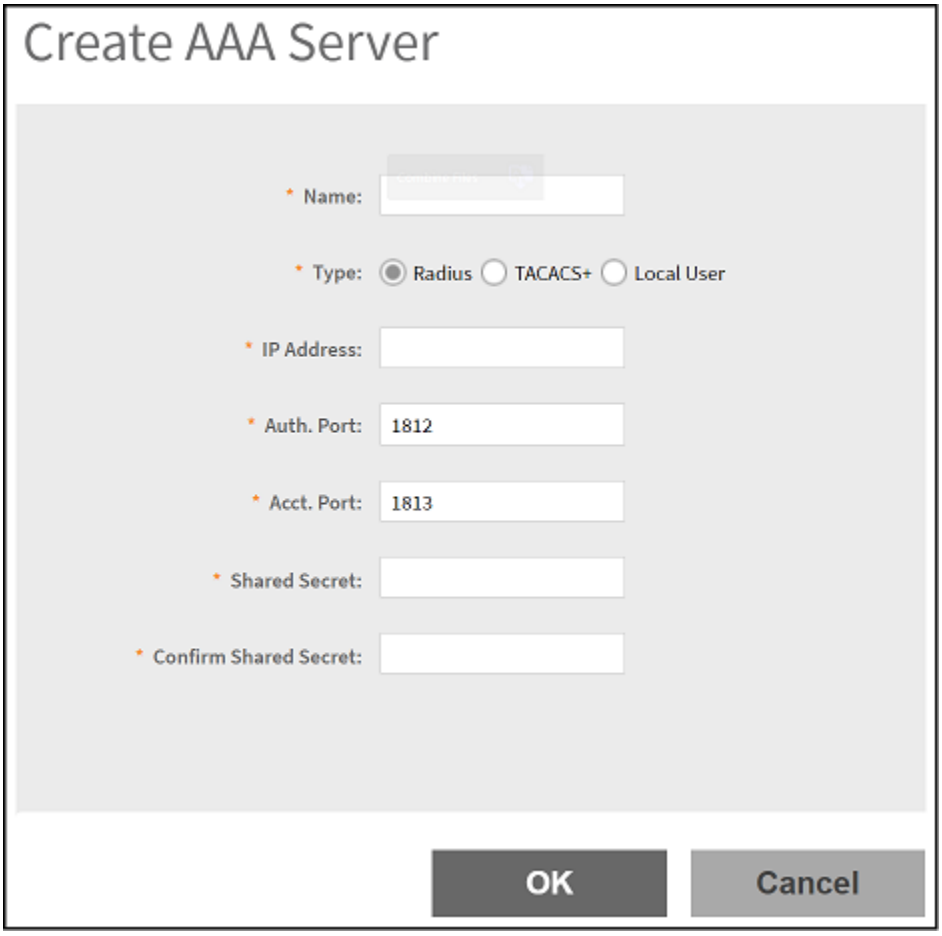
FIGURE 35 AAA Servers



a. Click 

icon to display the **Create AAA Server** dialog box and complete the AAA server configuration, refer to *Configuring Switch AAA Servers* in the *Management Guide*.

FIGURE 36 Create AAA Server

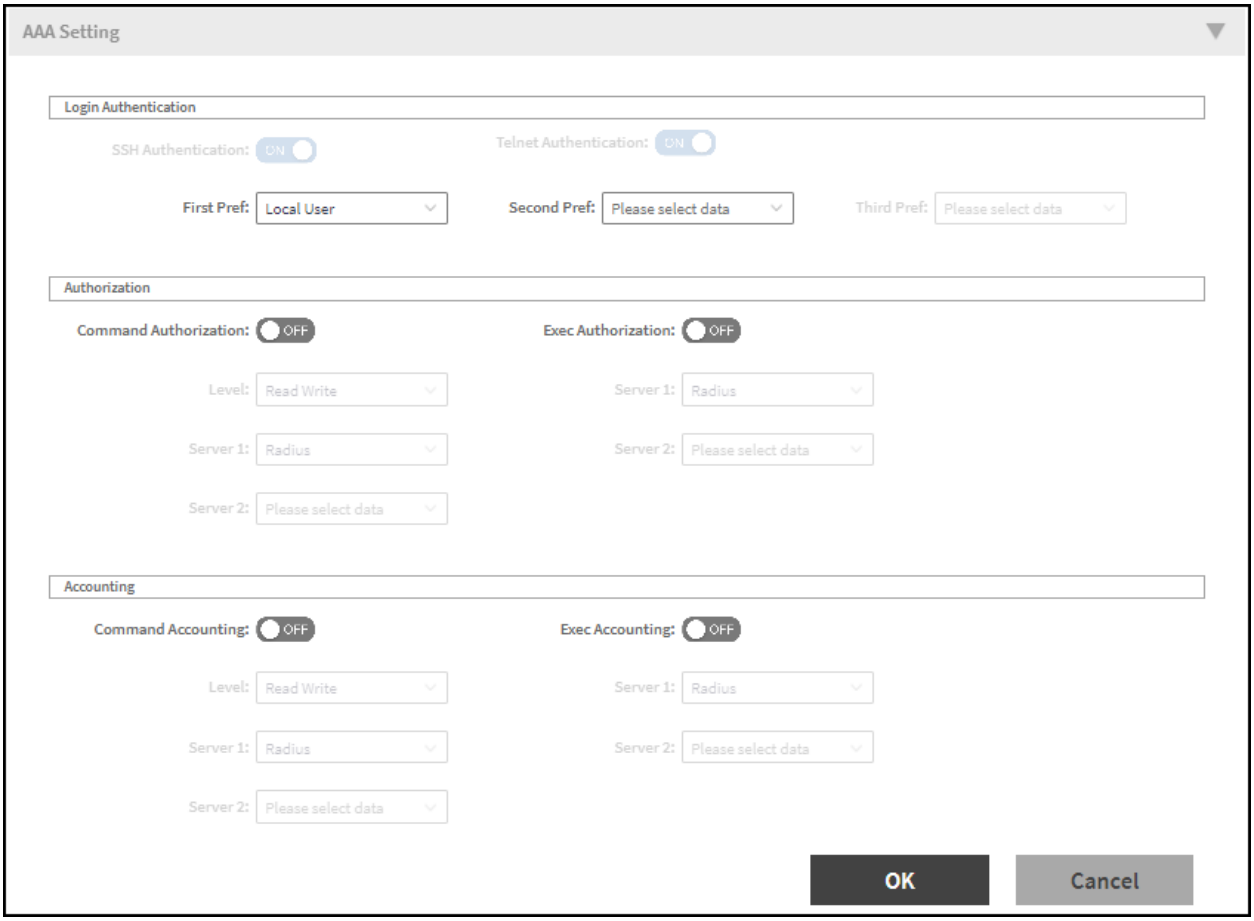


b. Click **OK**.

NOTE
You can also edit and delete the **AAA Servers** by selecting the options **Configure** and **Delete** respectively, from the **AAA Servers** tab.

3. Configure the **AAA Settings**.

FIGURE 37 AAA Settings



a. Complete the **AAA Settings**, refer to *Configuring Switch AAA Server Settings* in the *Management Guide*.

b. Click **OK**.

c) Configure the **Syslog Server** settings.

1. Click **Syslog Server** tab.

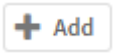
NOTE
This feature is supported on the switch firmware version 08.0.95.

FIGURE 38 Syslog Server Settings



2. Complete the following fields:
   - IP address: Enter the **IP address** of the external syslog server. Click **Cancel** to erase the entry in the field.
   - Ports: Enter the port number in the **Ports** field.

     NOTE
     The default port is 514, but the user can change it as per the requirements.

3. Click 

icon.

   NOTE
   Select the **IP Address** and click **Delete** icon to delete the syslog server **IP Address**.

d) Click **Close**.

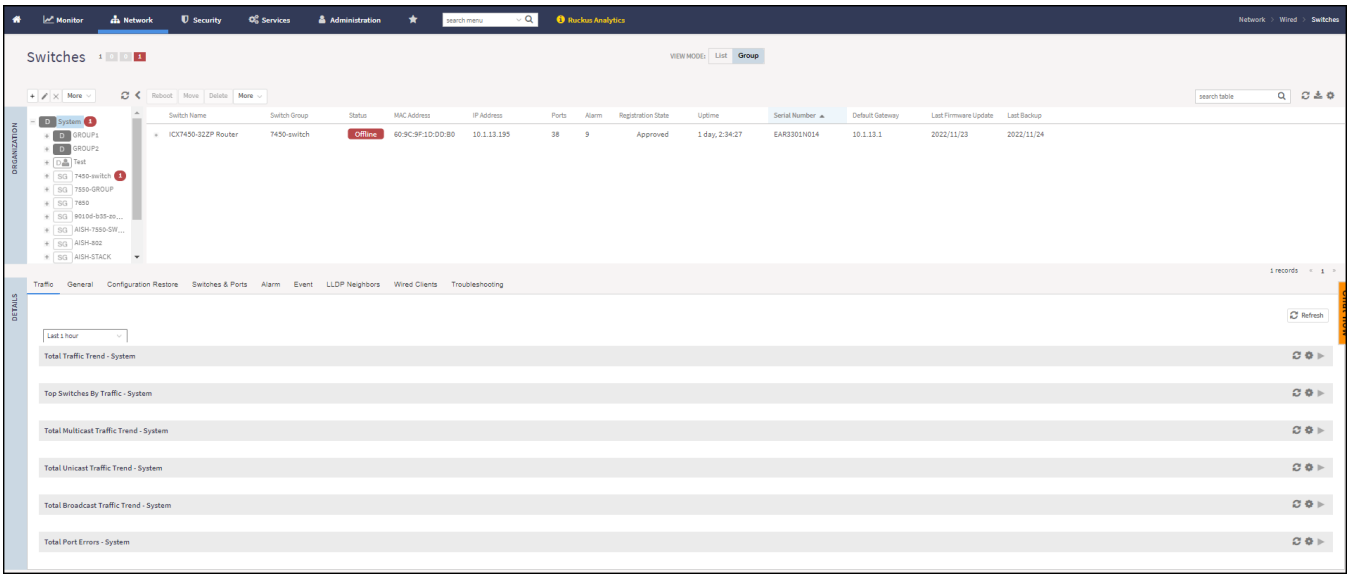
Creating Switch Model-Based Configurations

You can create and edit ACL, Layer 2, and Layer 3 configuration settings for a family of switches. You can also create or update the ACL to configure QoS profiles that prioritize VOIP and VIDEO VLAN traffic.

NOTE
Configuring the QoS Profiles requires ICX Firmware version 08.0.95.

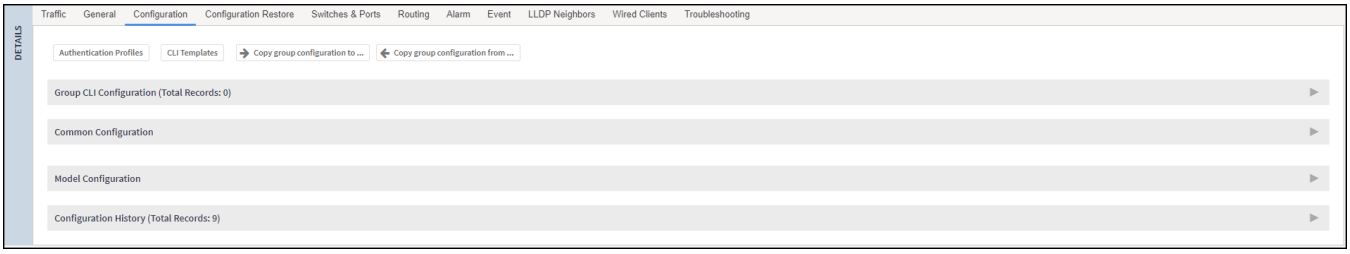
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 39 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and click **Configuration** tab.

FIGURE 40 Configuration

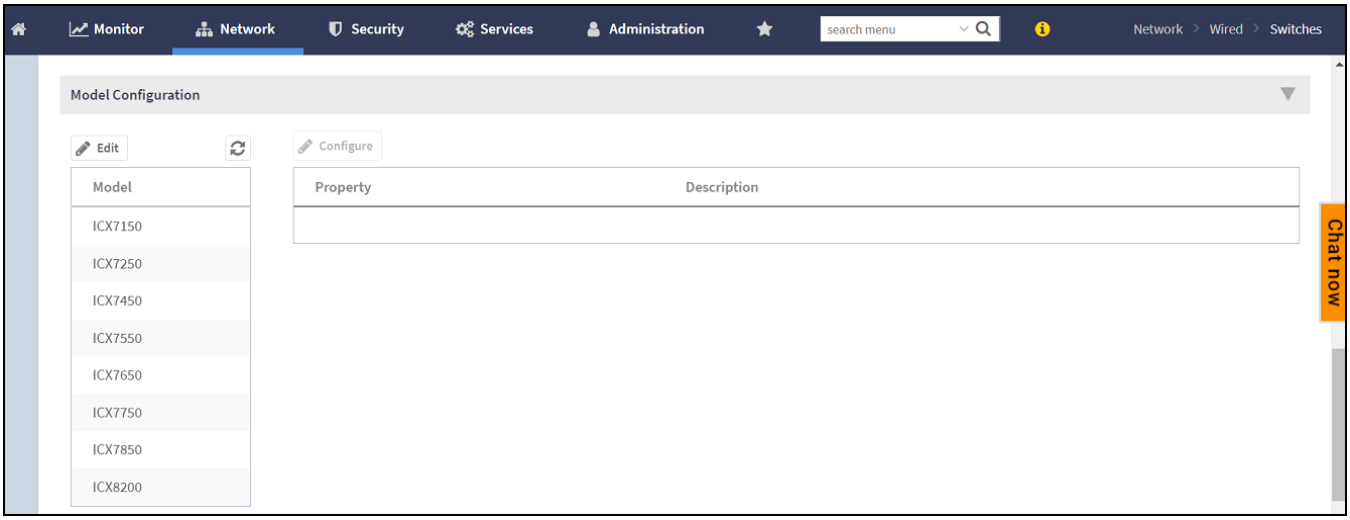


3. In the **Model Configuration**, select the **Switch Model** from the drop down list and click 

icon to display the **Feature Configuration** dialog box.

   NOTE
   The **Feature Configuration** page displays details about the ACL, VLAN, and static route. You can create, edit, and delete these configurations as necessary.

FIGURE 41 Model Configuration



a) Configure the **ACL** settings.
   1. Click **ACL** tab.
   2. Click 

icon to display the **ACL** fields.

FIGURE 42 ACL Configuration - Standard ACL Type

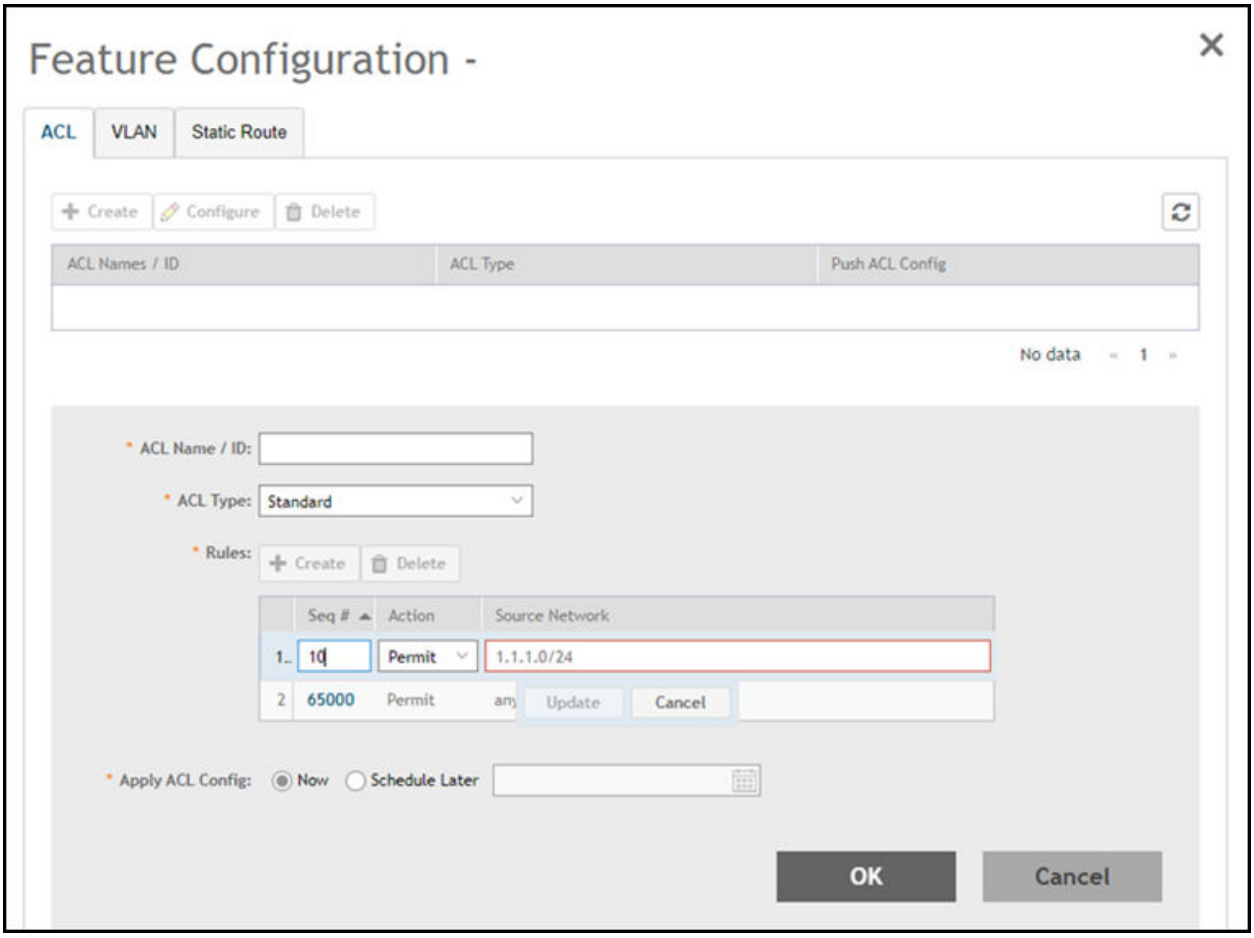
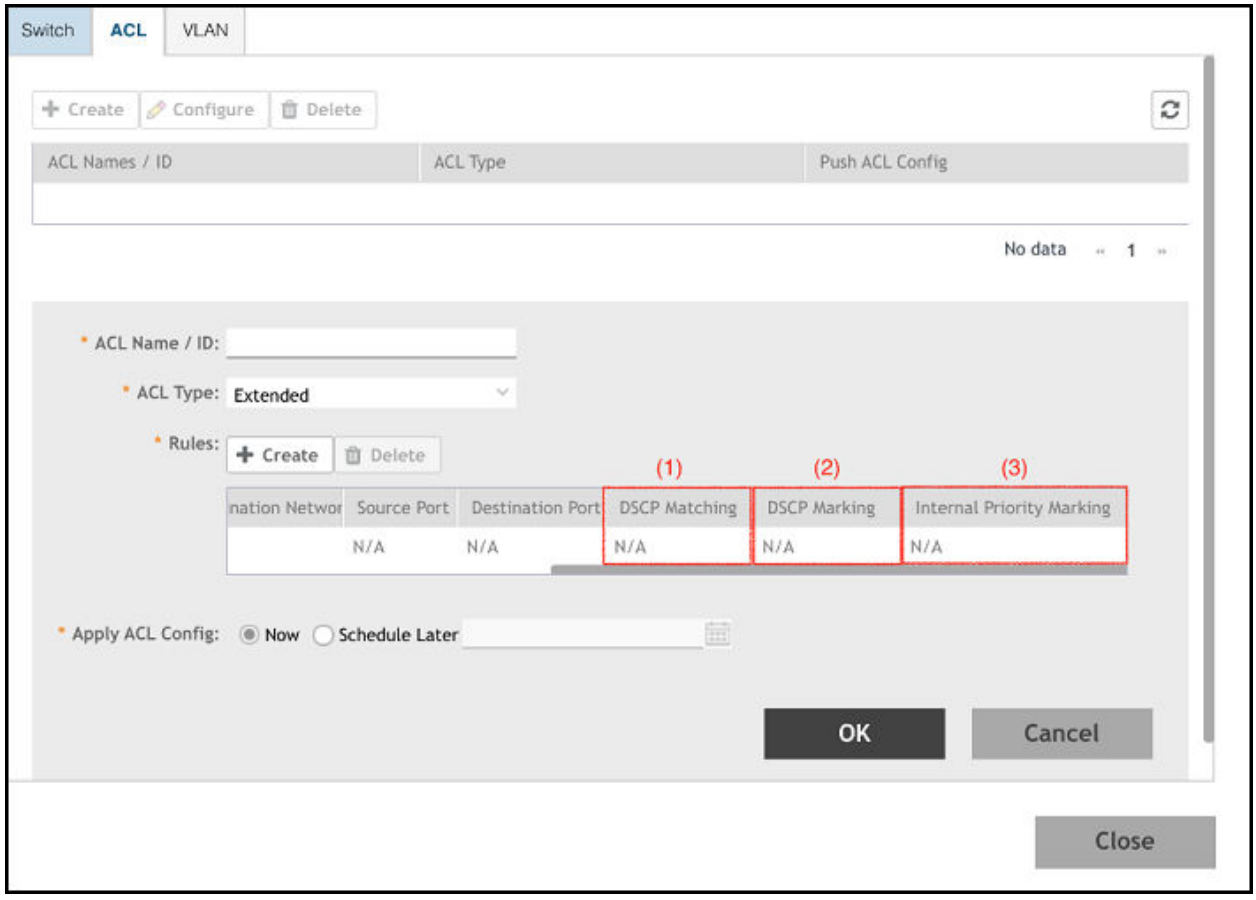


FIGURE 43 ACL Configuration with ICX Firmware version 08.0.95 - Extended ACL Type



3. Complete the following fields:
   - **ACL Name/ID**: Enter the name of the access control list or provide the list identifier.
   - **ACL Type**: Select Standard or Extended from the drop down list.
   - **Rules**: Click **Create** to create an ACL rule.
     - Complete the following fields to configure the following ACL rule for the Standard ACL type:

       You must provide the list sequence (**Seq#**), **Action** (Permit or Deny) and **Source Network** information to create the rule.

       NOTE
       Controller supports the "equal to" operator only.

       NOTE
       The Controller release 5.2.1 adds three new fields adds three fields (**DSCP Matching**, **DSCP Marking** and **Internal Priority Marking**) to configure QoS. After creating or updating the three fields, apply the ACL on a port or a VE to prioritize/de-prioritize traffic.

     - Complete the following fields to configure the following ACL rule for the Extended ACL type:
       - **Seq#**: Enter the sequence.
       - **Action**: Select Permit or Deny.

- **Source Network**: Enter the source network.
- **Destination Network**: Enter the destination network.
- **Source Port**: By default port 22 is selected.
- **Destination Port**: By default port 22 is selected.
- **DSCP Matching**: Enter the DSCP matching.
- **DSCP Marking**: Enter the DSCP marking.
- **Internal Priority Marking**: Enter the internal priority marking.

- **Apply ACL Config**: Select Now or Schedule Later. If you choose to schedule the configuration deployment for later, provide the time and date.
- Click **OK** to add the newly created ACL configuration to the **ACL** page. You can edit the configuration by selecting **Configure**.

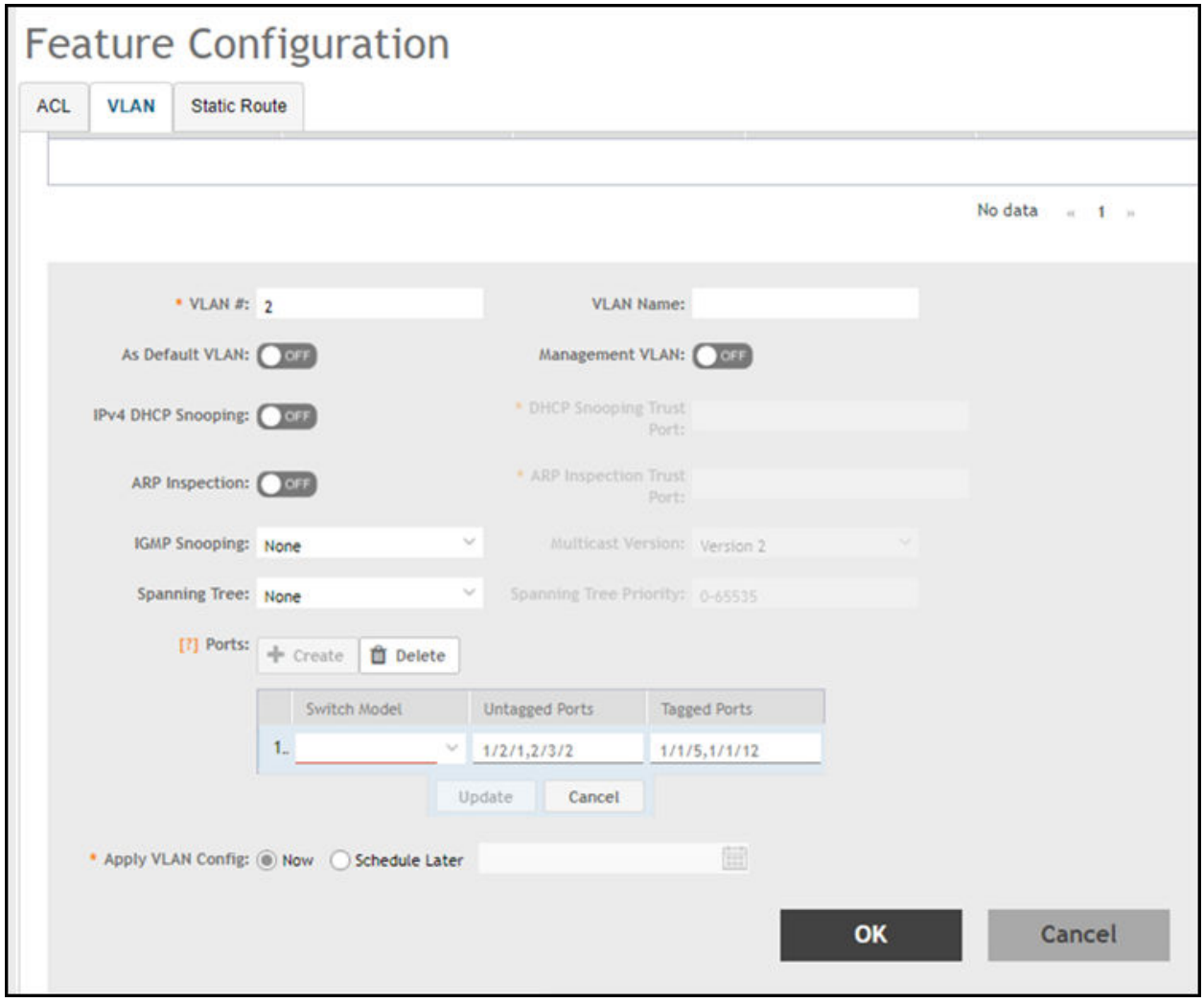
  NOTE
  You can also edit and delete the ACL configuration by selecting the options **Configure** and **Delete** respectively, from the **ACL** tab.

b) Configure the **VLAN** settings.

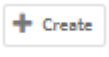
1. Click **VLAN** tab.
2. Click 

icon to display the **VLAN** fields.

FIGURE 44 VLAN Configuration

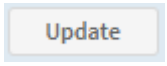


3. Complete the following VLAN fields:
   - **VLAN #**: Enter the number of the VLAN.
   - **VLAN Name**: Enter the name of the Layer 2 VLAN.
   - **As Default VLAN**: If you enable the **As Default VLAN** the **VLAN Name** is changed to **DEFAULT-VLAN** and the Management settings correspond to the previous VLAN settings.
   - **Management VLAN**: By enabling this, you can configure Management VLAN for the switches or switch groups. To configure Managemnt VLAN for switches or switch groups refer the topic Creating Switch Level Configuration on page 65.
   - **IPv4 DHCP Snooping**: Enable or disable IPv4 DHCP Snooping. Enabling this option allows the controller to send the ACL-per-port-per-VLAN message to the switch to reboot it. If you enable IPv4 DHCP Snooping, you must provide the trusted port for this option in the **DHCP Snooping Trust Port** field.
   - **APR Inspection**: enable or disable ARP Inspection. Enabling this option allows the controller to send the ACL-per-port-per-VLAN message to the switch to reboot it. If you enable IPv4 DHCP Snooping, you must provide the trusted port for this option in the **ARP Inspection Trust Port** field.

- **IGMP Snooping**: Select **None**, **Active**, or **Passive** from the list. The Internet Group Management Protocol (IGMP) allows the switch to track the communication between hosts and routers based on which the switch maintains a map of which links need which IP multicast streams. If you select **Active** or **Passive**, you are required to select the **Multicast Version** as well.
- **Spanning Tree**: Select **None**, **STP (802.1d)**, or **RSTP (802.1w)** from the list. Both Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) prevent creation of bridge loops when you have redundant paths in your network, and the broadcast radiation that results from them. If you select **STP 802.1d** or **RSTP 802.1w**, you are required to select the **Spanning Tree Priority** as well.
- **Ports**: Click 

icon and complete the following fields:

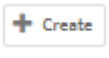
  NOTE
  Different set of ports can be entered for each switch model.

  - **Switch Model**: Select the switch model from the drop down list.
  - **Untagged Ports**: Enter the ports.
  - **Tagged Ports**: Enter the tag ports.
  - Click 

icon.
- **Apply VLAN Config**: Select Now or Schedule Later. If you choose to schedule the configuration deployment for later, provide the time and date.
- Click **OK** to add the newly created VLAN configuration to the **VLAN** page.

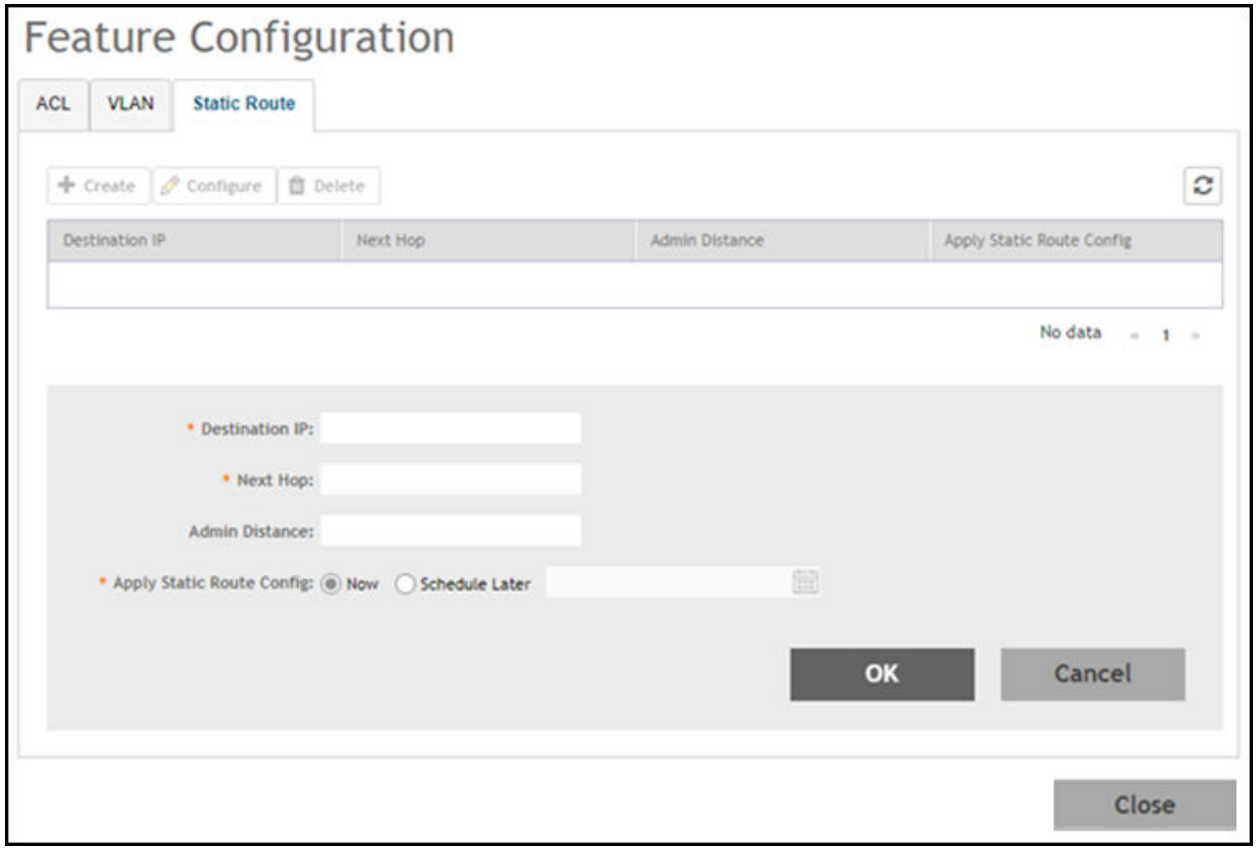
  NOTE
  You can also edit and delete the VLAN configuration by selecting the options **Configure** and **Delete** respectively, from the **VLAN** tab.

c) Configure the **Static Route** settings.

1. Click **Static Route** tab.
2. Click 

icon to display the **Static Route** fields.

FIGURE 45 Static Route Configuration



3. Complete the following Static Route fields:
   - **Destination IP**: Enter the destination IP address.
   - **Next Hop**: Enter the next-hop IP address. Multicast and broadcast IP addresses are not allowed.
   - **Admin Distance**: Enter a value from 1 through 255.
   - **Apply Static Route Config**: Select Now or Schedule Later. If you choose to schedule the configuration deployment for later, provide the time and date.
   - Click **OK** to add the newly created static route configuration to the **Static Route** page.

     NOTE
     You can also edit and delete the Static Route configuration by selecting the options **Configure** and **Delete** respectively, from the **Static Route** tab.

d) Click **Close**.

The IP address is added to the **Model Configuration** page under **Property**. If you want to edit the configuration, select it and click **Edit** to edit the settings.

NOTE
Any changes made to the group level configuration including common configuration and switch model-based configuration will be applied to all the switches belonging to the group.

Configuration defined at group level can be chosen to be applied instantaneously by selecting the **Now** option or schedule for a later time using **Schedule later** option. The scheduling option is only applicable if you are trying to make changes to existing switches in the group. For any new switches that are joining the group, this configuration gets applied instantaneously.

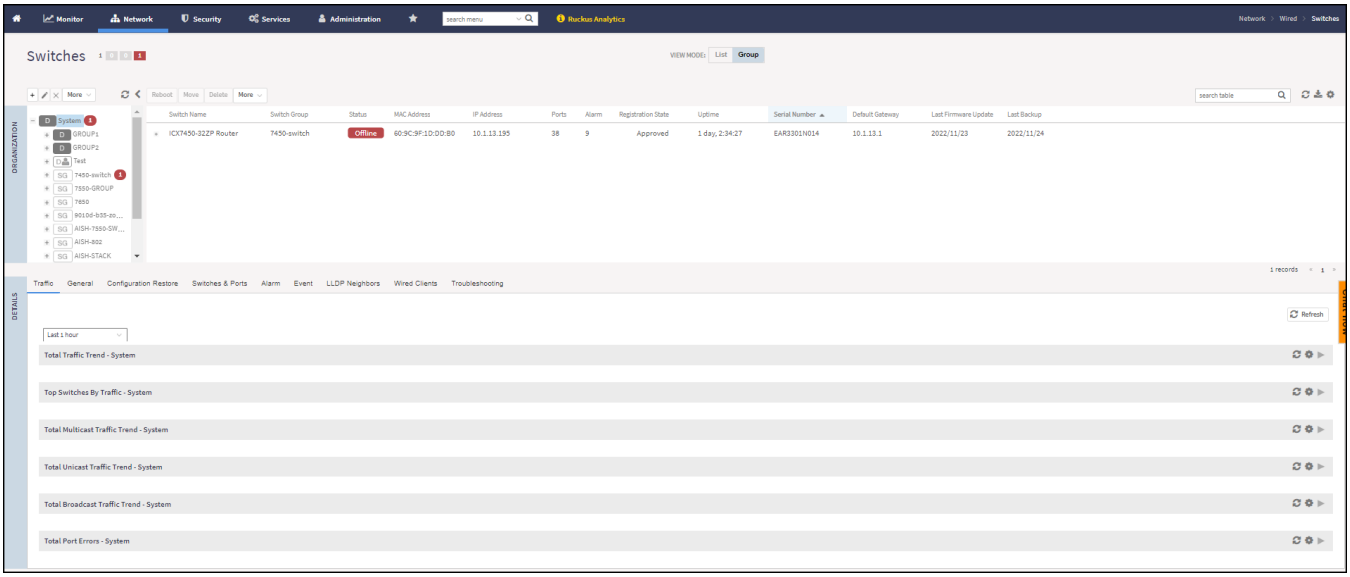
Copying Switch Group Configuration

You can copy the configuration settings from a working switch to one or multiple new switches.

NOTE
It is recommended to exercise caution when using the copy configuration option as it replaces the entire configuration of the destination switch.

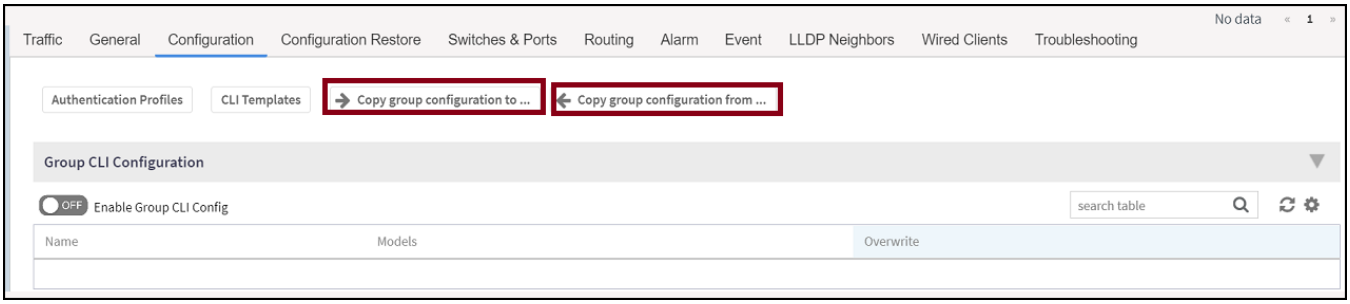
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 46 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and in the **Details** tab click **Configuration** tab.

FIGURE 47 Switch Group Configuration Tab



3. Click **Copy group configuration to** icon to display the **Copy config To Other Switches** dialog box.
4. Select a **Domain** > **Switch Group** or **Switch Group** to which you want to copy the configuration profile, and click **OK**.

5. Click **Copy group configuration from** icon to to display the **Copy config From Another Switch** dialog box.
6. Select a **Domain** > **Switch Group** or **Switch Group** from which you want to get the configuration profile, and click **OK**.

Accessing AAA Settings for Switch Configuration

You can create, view, and edit the configuration settings for a group of switches.

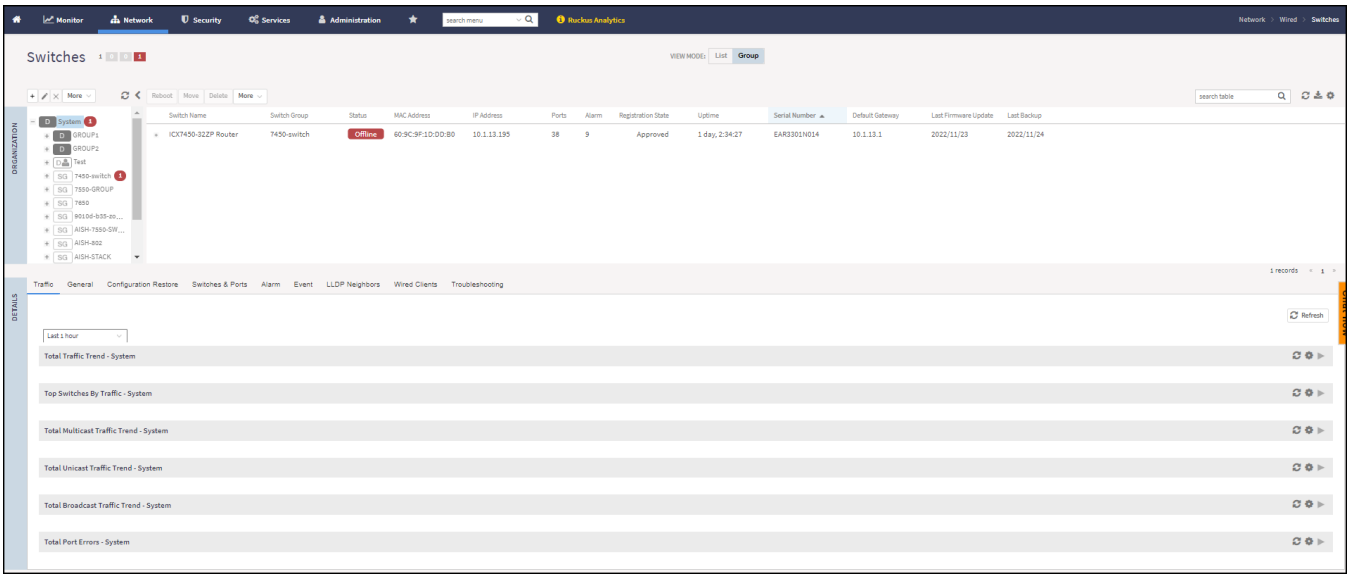
Configure the switch AAA settings, refer to *Configure the AAA settings* in the Creating Common Configuration on page 46.

Viewing the Configuration History of Switches

You can view the configuration details of switches from the **Configuration History** tab.

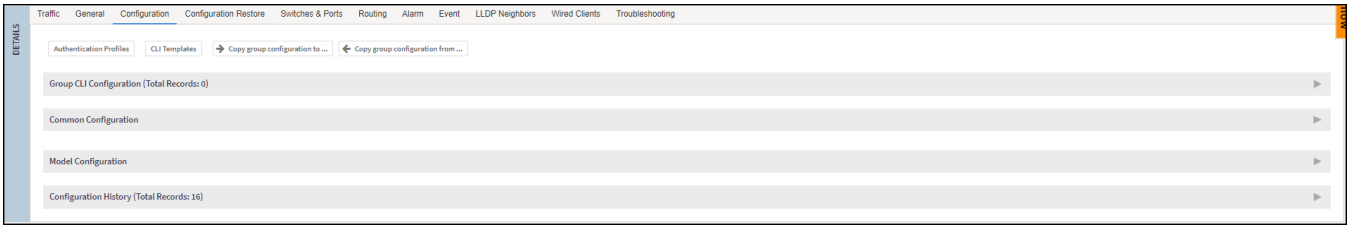
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 48 Switches



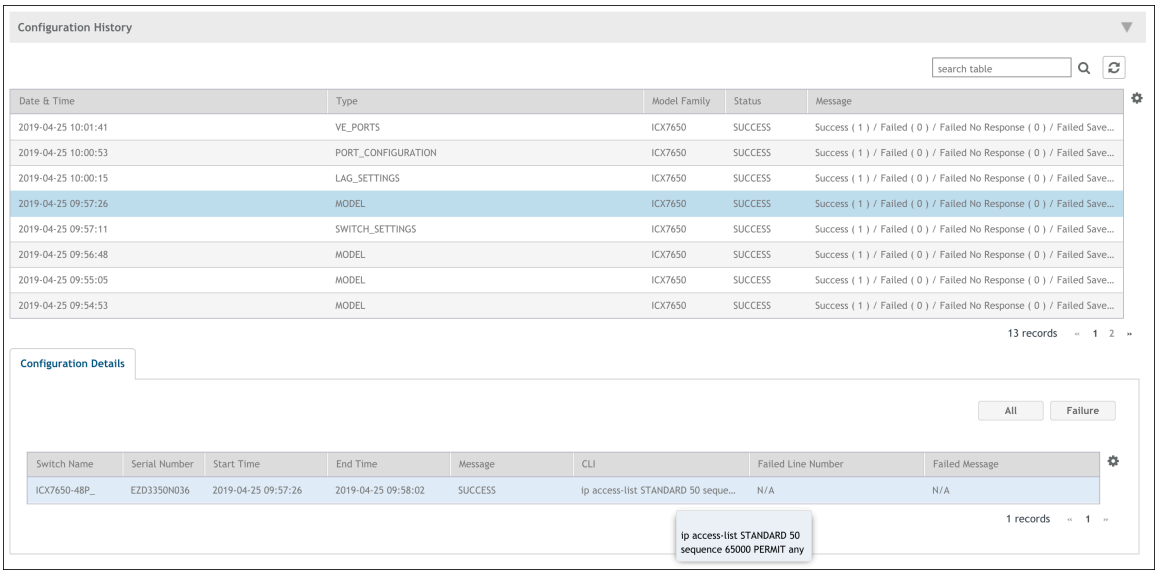
2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and in the **Details** tab, click **Configuration** tab.

FIGURE 49 Switch Configuration Tab



3. Click **Configuration History** tab to view the following configuration information:

FIGURE 50 Configuration history



Information about the date and time at which the configuration profile was created, type of configuration, switch model or switch family that its created for, configuration status and a message confirming the configuration implementation on the switch/switch group is displayed.

Select the **Switch** to display the **Configuration Details** tab. You can see more information about the switch.

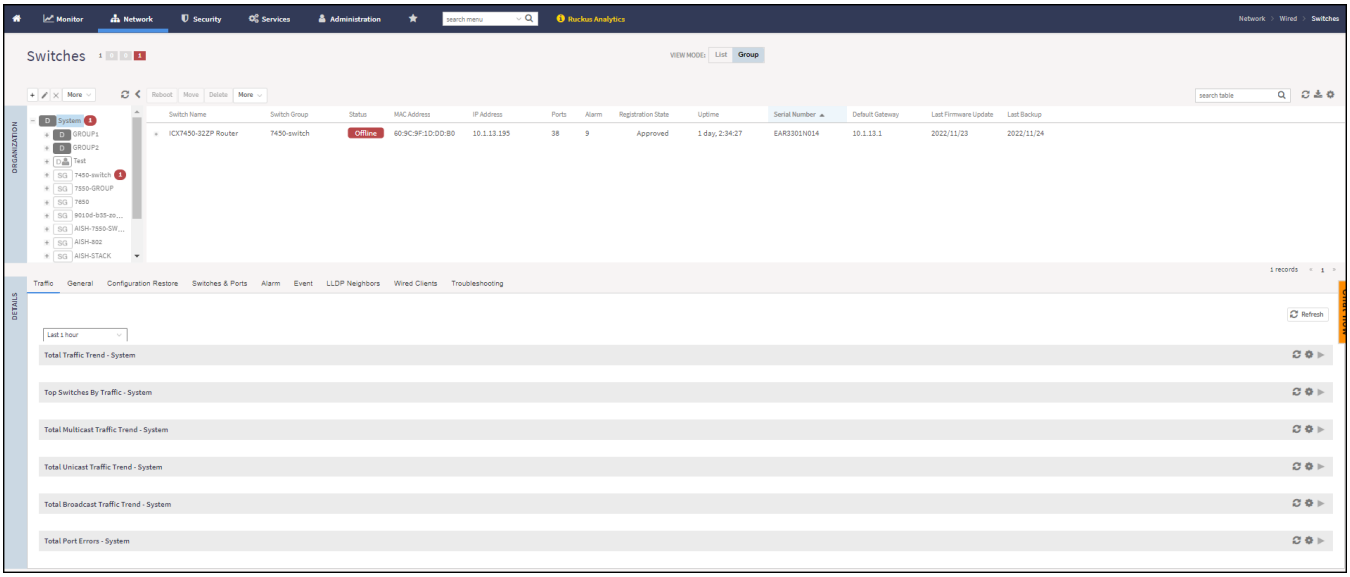
Data Synching on the Switch Table

When a switch running FastIron 08.0.90 or later joins the controller, the controller runs the Local Sync operation every 5 minutes. If the changes are made on the switch console or any configuration changes are deployed on the controller, the controller syncs those corresponding changes to the switch or port table five minutes later, which causes a delay. Therefore, beginning with SmartZone 6.1.1, the Local Sync time is reduced from 5 minutes to 3 minutes to speed up the process.

When a CLI session is closed, Local Sync is triggered automatically to update the changes on the controller. Similarly, the controller can trigger Local Sync manually for a selected switch.

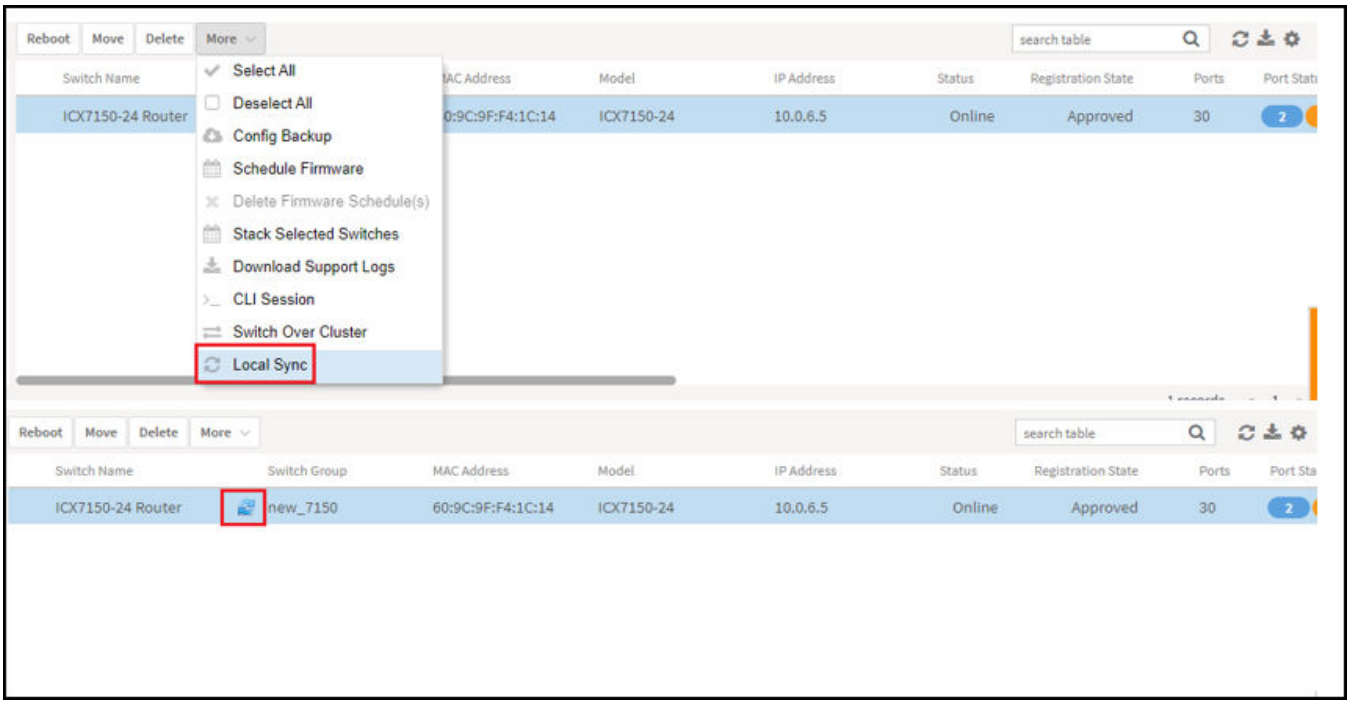
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 51 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**. Click **More** > **Local Sync** .

FIGURE 52 Selecting LocalSync on the Controller UI



Switch Level Configuration

In addition to the group level configuration, individual switch-level configuration can be edited by selecting the switch from the Switch table.

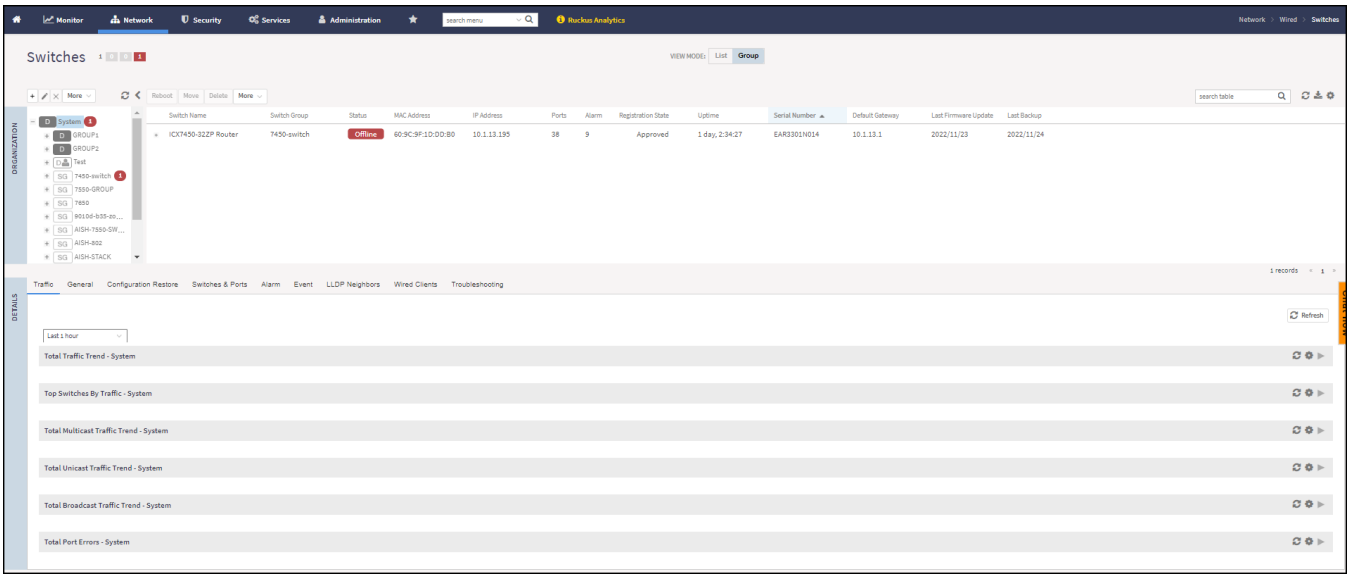
Switch-specific settings include **Hostname**, **Jumbo Mode**, **IGMP Snooping**, and **DHCP Server**. In addition, the switch configuration defined at the group level is available for editing at the switch level.

Creating Switch Level Configuration

You can configure switch, ACL, VLAN, and static route settings for each switch.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

   FIGURE 53 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and in the **Details** tab, click **Configuration** tab.

3. In the **Model Configuration** tab, select the **Switch Model** and click 

icon to display the **Feature Configuration** dialog box.

4. Configure the Switch settings.
   a) Click **Switch** tab.

   FIGURE 54 Switch Configuration



   b) Complete the following fields:
   - **Name**: Enter the name of the switch.
   - **IGMP Snooping**: Select the profile from the list.
   - **Boot Flash**: Select the **Default**, **Primary** or **Secondary** option to configure boot preference.
   - **Jumbo Mode**: Enable this option to reboot the switch.
   - **DHCP Server:** Enable this option and click **Create** to configure the following DHCP server settings:

     NOTE
     You must disable the DHCP client before enabling the DHCP server.

     - **Pool Name:** Enter a name.
     - **Network/Mask**: Enter the network address and network mask.
     - **Excluded Range**: Enter the network range to be excluded.
     - **Lease Time**: Enter the lease time duration.
     - **Default Router IP**: Enter the default router IP address.
     - **Options**: Click **Create** and enter the option number, , select a type, and enter a value for the option.

     Click **Update** to apply the option.

5. Configure the switch ACL settings, refer to *Configure the ACL settings* in the Creating Switch Model-Based Configurations on page 51.

6. Configure the switch **VLAN** settings.

   NOTE
   You can create a new VLAN and set it as the default VLAN.

   a) Click **VLAN** tab.

   b) Click  icon to display the **VLAN** fields.

FIGURE 55 VLAN Configuration

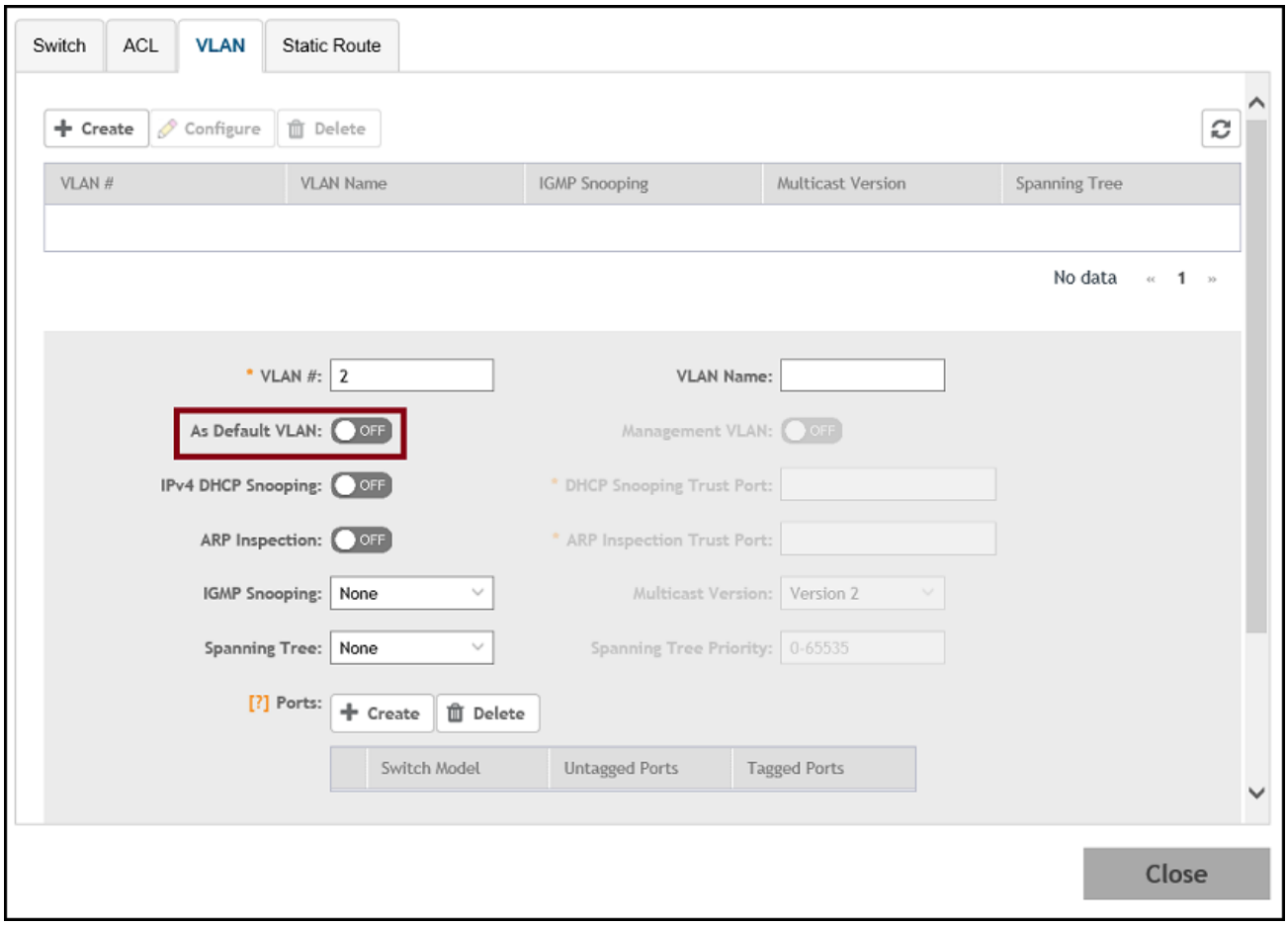
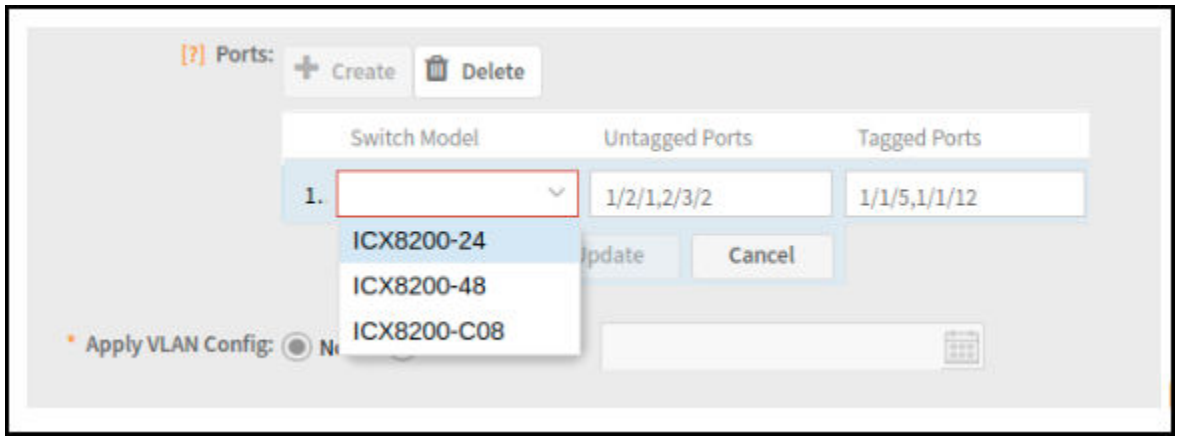


FIGURE 56 Creating Port and Adding Port Details



c) Complete the following fields:

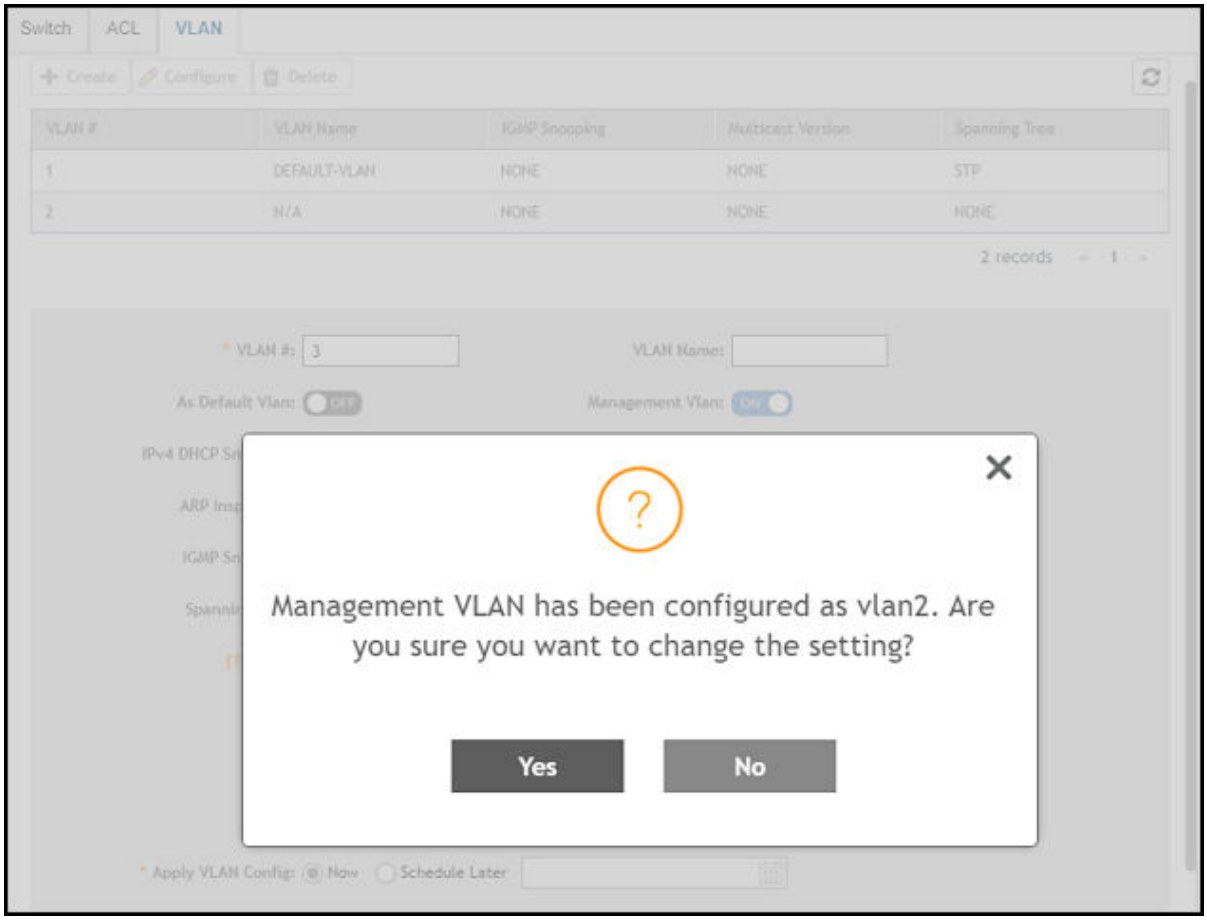
- **VLAN#**: Enter a unique number for VLAN.
- **VLAN Name** is changed to **DEFAULT-VLAN** and the Management settings correspond to the previous VLAN settings.

  NOTE
  If you enable the **As Default VLAN**, the **VLAN Name** is changed to **DEFAULT-VLAN** and the Management settings correspond to the previous VLAN settings.

- **Management VLAN**: You can configure the Management VLAN for the switches or switch groups in the following ways:
  - Enable **Management VLAN**, and click **OK**.

    If the VLAN is configured as the default VLAN, enable or disable **Management VLAN** on the default VLAN, and click **OK**. A dialogue box is displayed, as shown in the following.

FIGURE 57 Management VLAN Confirmation



If **Management VLAN** is enabled on a VLAN and you try to enable it on another VLAN, the controller displays a dialogue box showing the VLAN ID that has been configured as the Management VLAN. If you click **Yes**, the controller overwrites the settings.

- For a switch group, the controller displays a dialogue box, as shown in the following figure.

FIGURE 58 Management VLAN Confirmation Dialogue Box

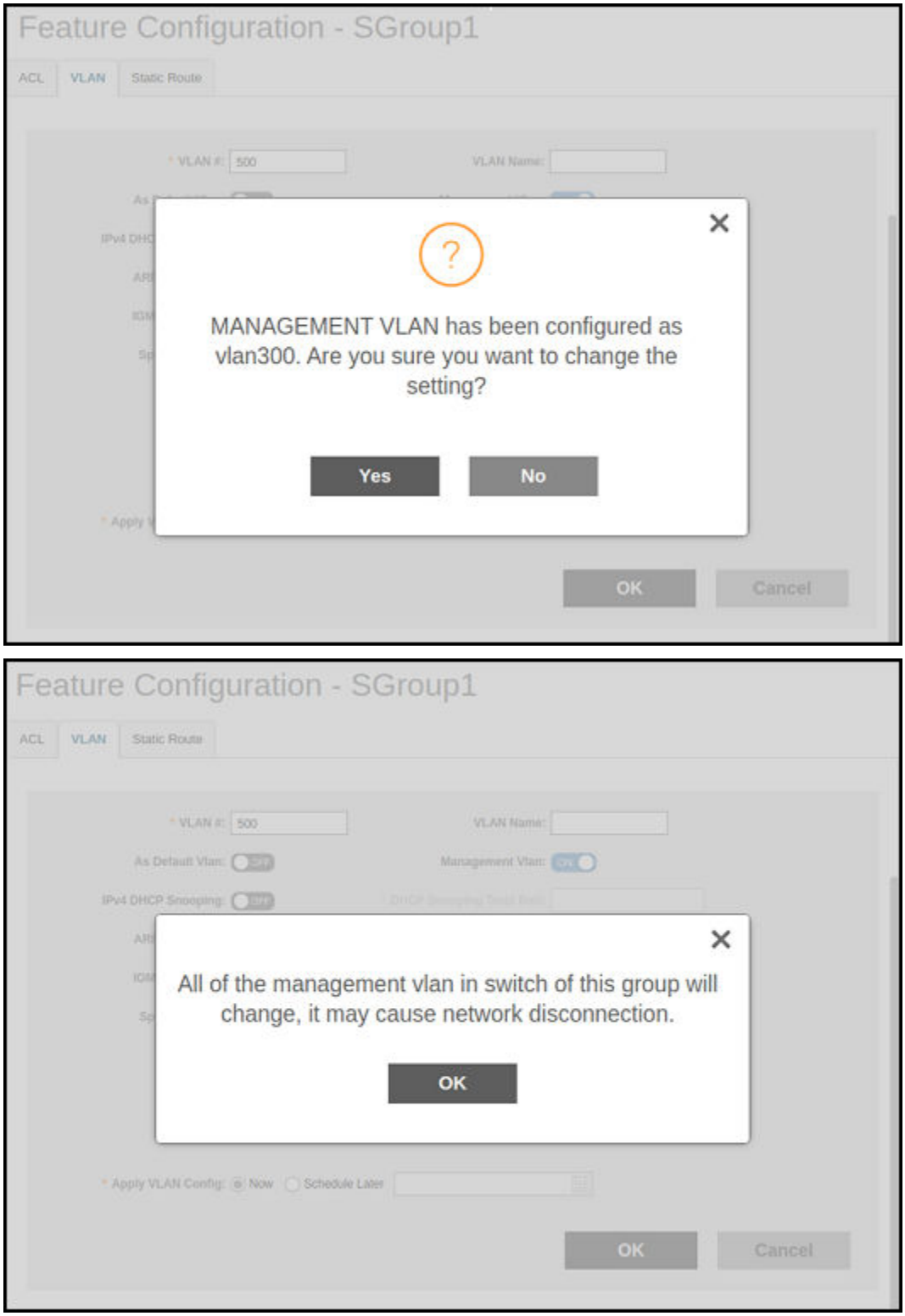


FIGURE 59 Management VLAN Confirmation Message

- **IPv4 DHCP Snooping**: Enable or disable IPv4 DHCP Snooping. Enabling this option allows the controller to send the ACL-per-port-per-VLAN message to the switch to reboot it. If you enable IPv4 DHCP Snooping, you must provide the trusted port for this option in the **DHCP Snooping Trust Port** field.
- **APR Inspection**: enable or disable ARP Inspection. Enabling this option allows the controller to send the ACL-per-port-per-vlan message to the switch to reboot it. If you enable IPv4 DHCP Snooping, you must provide the trusted port for this option in the **ARP Inspection Trust Port** field.
- **IGMP Snooping**: Select **None**, **Active**, or **Passive** from the list. The Internet Group Management Protocol (IGMP) allows the switch to track the communication between hosts and routers based on which the switch maintains a map of which links need which IP multicast streams. If you select **Active** or **Passive**, you are required to select the **Multicast Version** as well.
- **Spanning Tree**: Select **None**, **STP (802.1d)**, or **RSTP (802.1w)** from the list. Both Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) prevent creation of bridge loops when you have redundant paths in your network, and the broadcast radiation that results from them. If you select **STP** or **RSTP**, you are required to select the **Spanning Tree Priority** as well.
- **Ports**: Click **Create** to assign the ports to the switch model. Enter values for **Switch Model**, **Untagged Ports**, and **Tagged Ports**.
- **Apply VLAN Config**: Select **Now** or **Schedule Later**. If you choose to schedule the configuration deployment for later, provide the time and date.
- Click **OK** to add the newly created VLAN configuration to the **VLAN** tab.

NOTE
You can also edit and delete the VLAN configuration by selecting the options **Configure** and **Delete** respectively, from the **VLAN** tab.

7. Configure the switch Static Route settings, refer to *Configure the Static Route settings* in the Creating Switch Model-Based Configurations on page 51.
8. Click **Close**.

   The configurations are updated under **Property**. If you want to edit the configuration, select it and click **Edit** to edit the settings.

   NOTE
   Use the switch-level option to add additional ACLs, VLANs, or static routes other than those already defined at the switch group level. Use the group-level configuration to make changes to existing settings at the group level.

Copying Configuration

If you already have a switch with the desired set of features configured, controller provides an option to load the current configuration of the switch, remove unique settings like hostname, IP addresses, and so on, and copy it to one or more target switches. This procedure is applicable only if the target switches have no existing configuration.

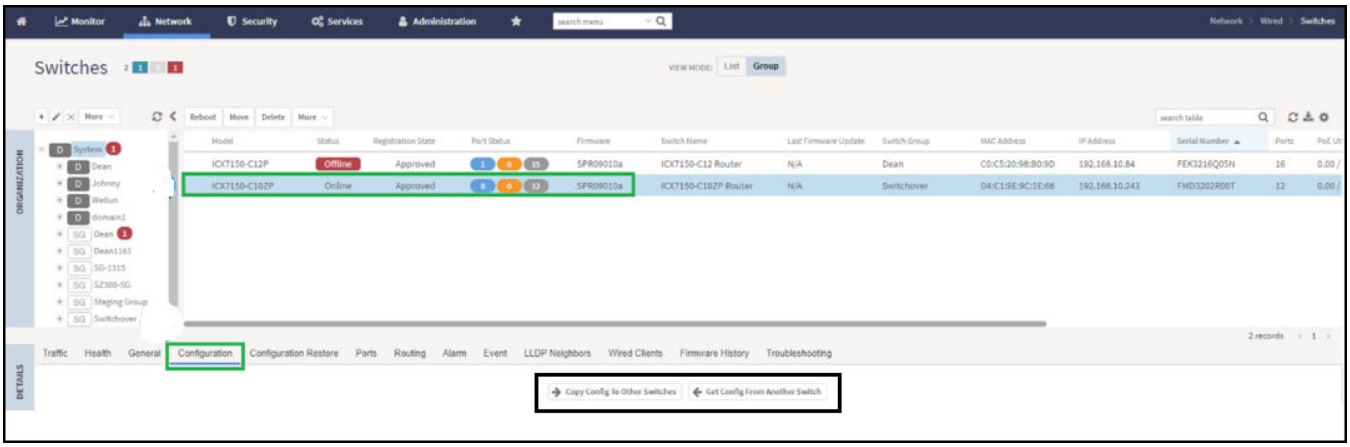
Complete the following steps to copy configuration to one or more target switches.

1. From the main menu, go to **Network** > **Wired** > **Switches.**

   The **Switches** page appears.

2. Select the switch and then the **Configuration** tab.

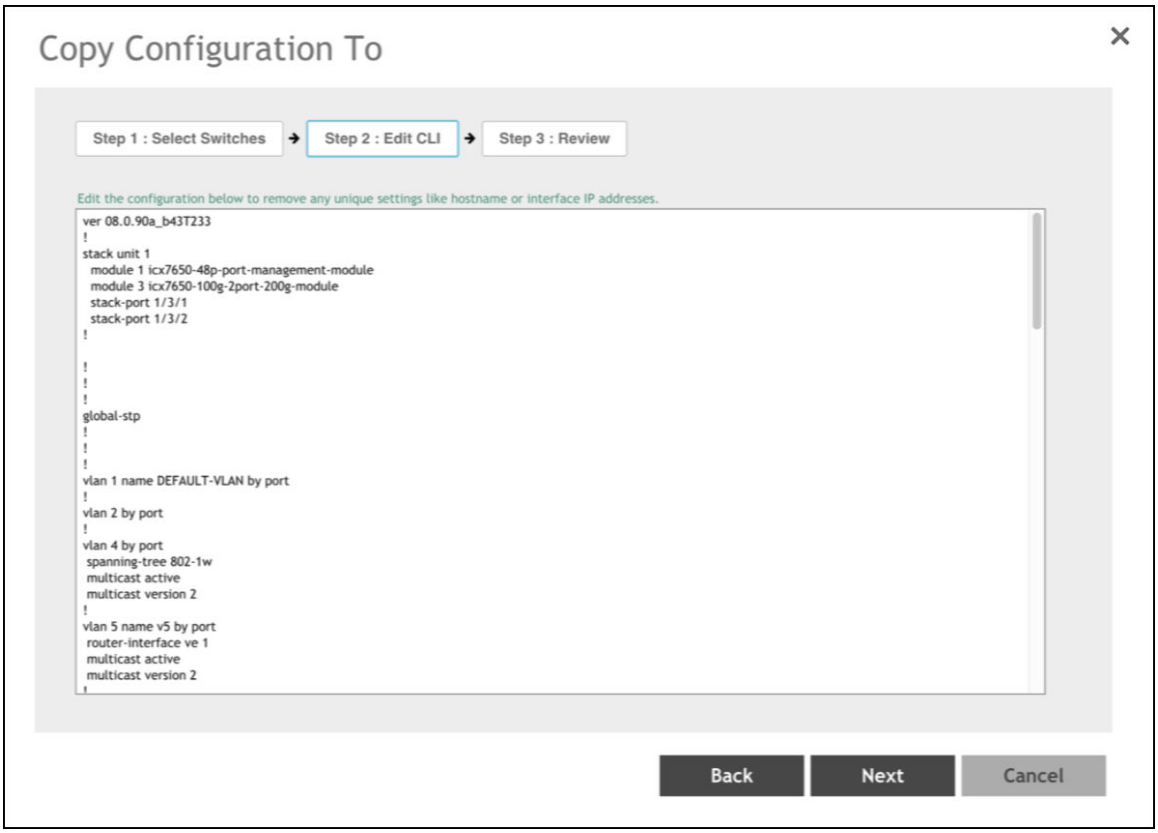
FIGURE 60 Switch Group Configuration Tab



3. Click **Copy Configuration To**. This option lets you replace the entire configuration (startup-config) of the selected switch with that of a source switch.
4. Click **Get Configuration From** and select the switch or group from which you want to get the configuration profile, and click **OK**. This option lets you replace the entire configuration of destination switches (one or more) with the configuration of the selected switch.

5. Edit the CLI commands to remove unique settings like IP settings and hostname and click **Next**.

FIGURE 61 Copy Configuration To - Edit CLI Page



6. Review CLI config and click **OK**.

Generic CLI Configuration

SmartZone 6.0 introduces capability to provision switches using predefined CLI configuration making it easy for users to deploy any feature that ICX supports.

Group Level CLI Configuration

Users can pre-define CLI configuration for one or more switch models. When switches join this switch group, the CLI configuration gets applied to the startup-config and the switches are rebooted for the configuration to take effect.

Users can pre-define CLI configuration for one or more switch models. When switches join this switch group, the CLI configuration gets applied to the startup-config and the switches are rebooted for the configuration to take effect.

- After selecting the Group CLI configuration option, the existing GUI options at the switch group level are disabled, including common settings, model family based configurations, the **Copy configuration** to, and **Get configuration** from functions.
- If the Group CLI configuration is selected, only those switches joining the switch group after that point will inherit the configuration.
- Switch-level UI configuration options and routing must be read-only. However, ports and LAG settings can still be configured from the ports table.

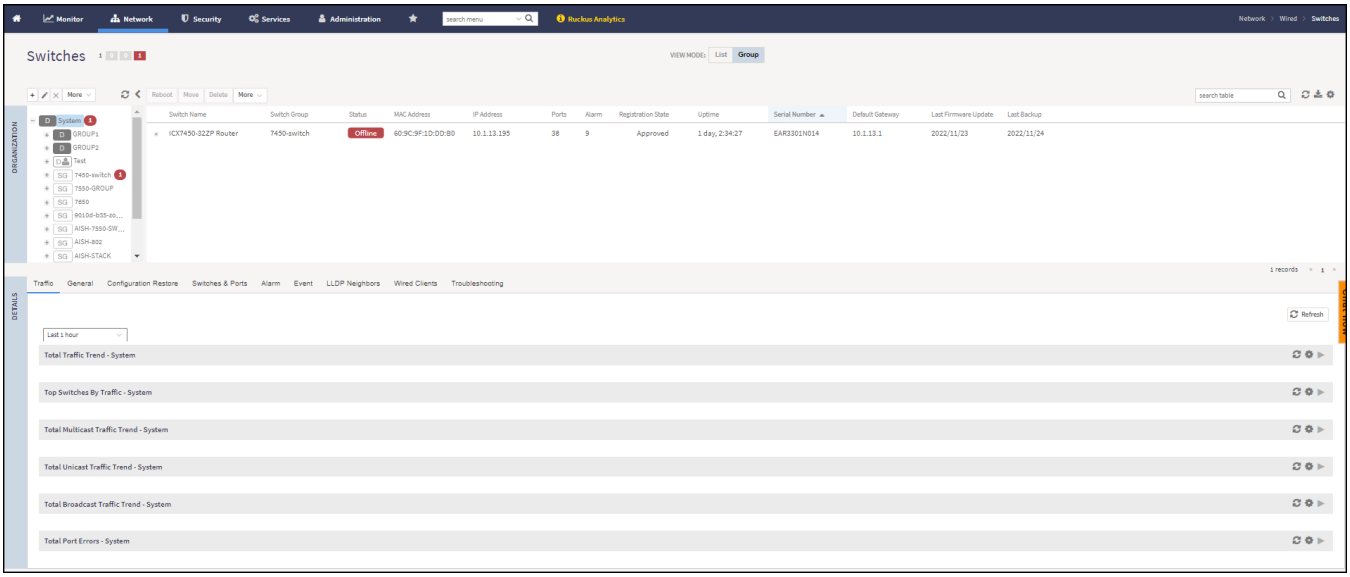
- You cannot return to GUI mode to define the Switch group configuration unless the switch group is deleted and re-created.

Enabling the Group CLI Configuration

An administrator can create a new template or modify an existing Group CLI configuration for the switch group before enabling the template.

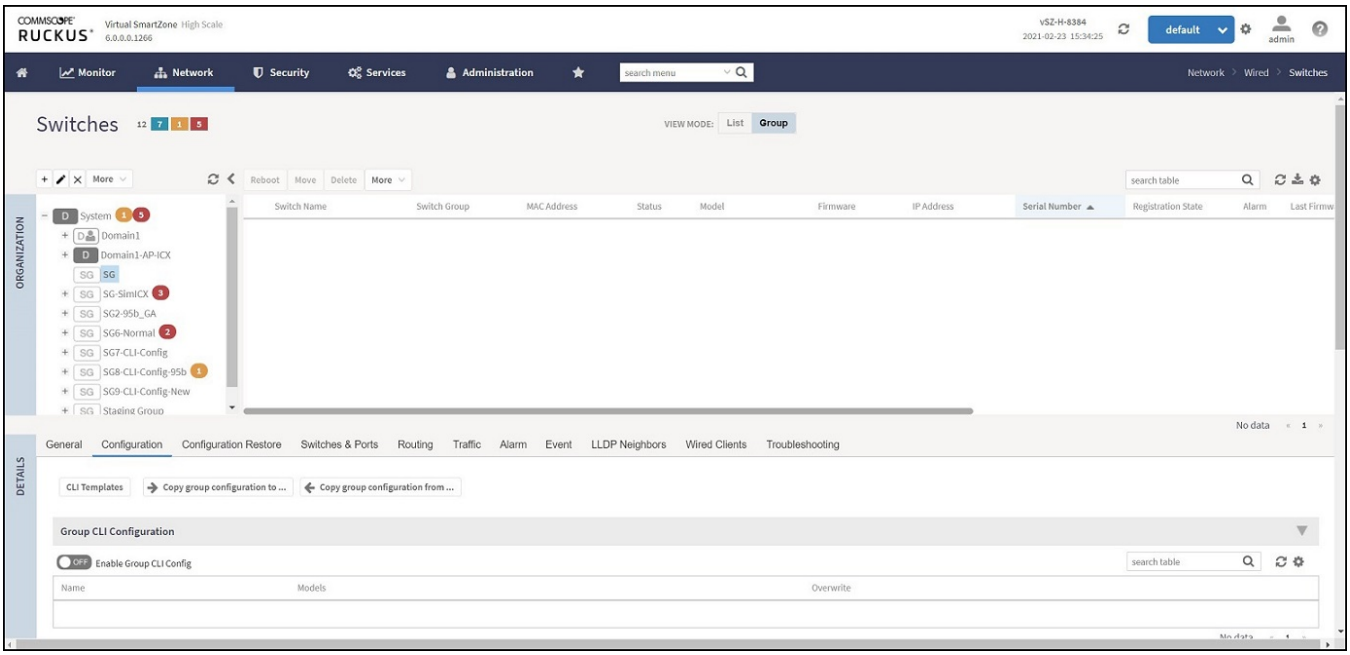
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 62 Switches



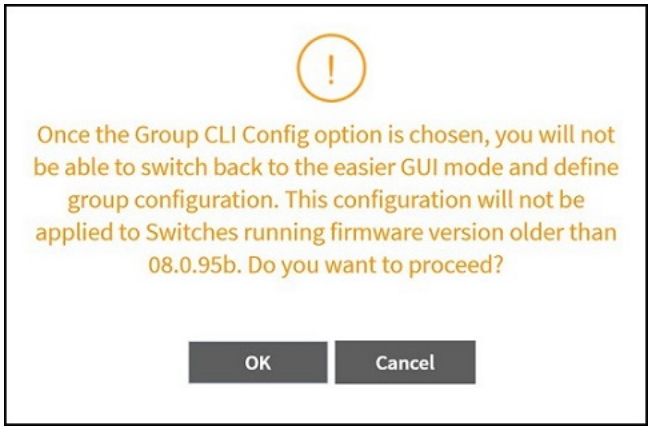
2. In the **Organization** tab, select a **Domain** or **Switch Group** and in the **Details** tab, click **Configuration** tab.

FIGURE 63 Enabling Group CLI Config setup



3. In the **Group CLI Configuration** tab, switch ON **Enable Group CLI Config** to display the **Confirming Group CLI Configuration Setup** dialog box.

FIGURE 64 Confirming Group CLI Configuration Setup



4. Click **OK** to display the **Group CLI Configuration** dialog box.

5. In the **Choose Model**, select one or more ICX models to create a new Group CLI Configuration template and click **Next** to display the **CLI Configuration** tab. You can also select an existing ICX model and click **Next** to modify the Group CLI configuration.

   NOTE
   Any ICX models that have already been selected in the Group CLI configuration will be unavailable and you cannot selecst them.

FIGURE 65 Choosing ICX Models



6. Enter the name of the Group CLI Configuration in the **Name** field. Insert the command lines in the space provided. Users can choose the CLI commands under the 'Examples' pane to build configuration. Alternatively, CLI commands can be typed directly or copied from a notepad and pasted into the 'CLI Configuration' box.

   NOTE
   It is recommended that users get familiarized with FastIorn commands and their ordering to avoid any issues with applying the configuration.

FIGURE 66 Entering the Name in the new Group CLI Configuration

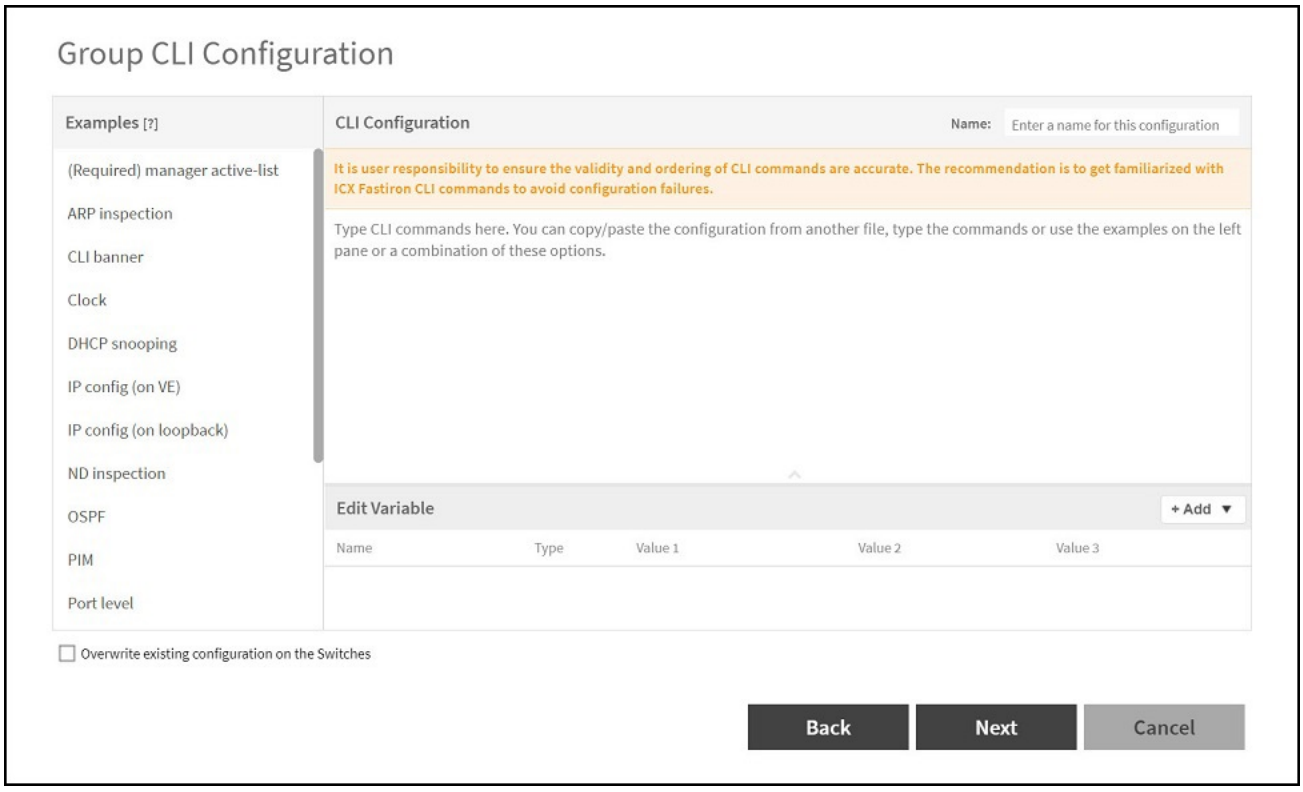


FIGURE 67 Inserting Command Lines in the new Group CLI Configuration

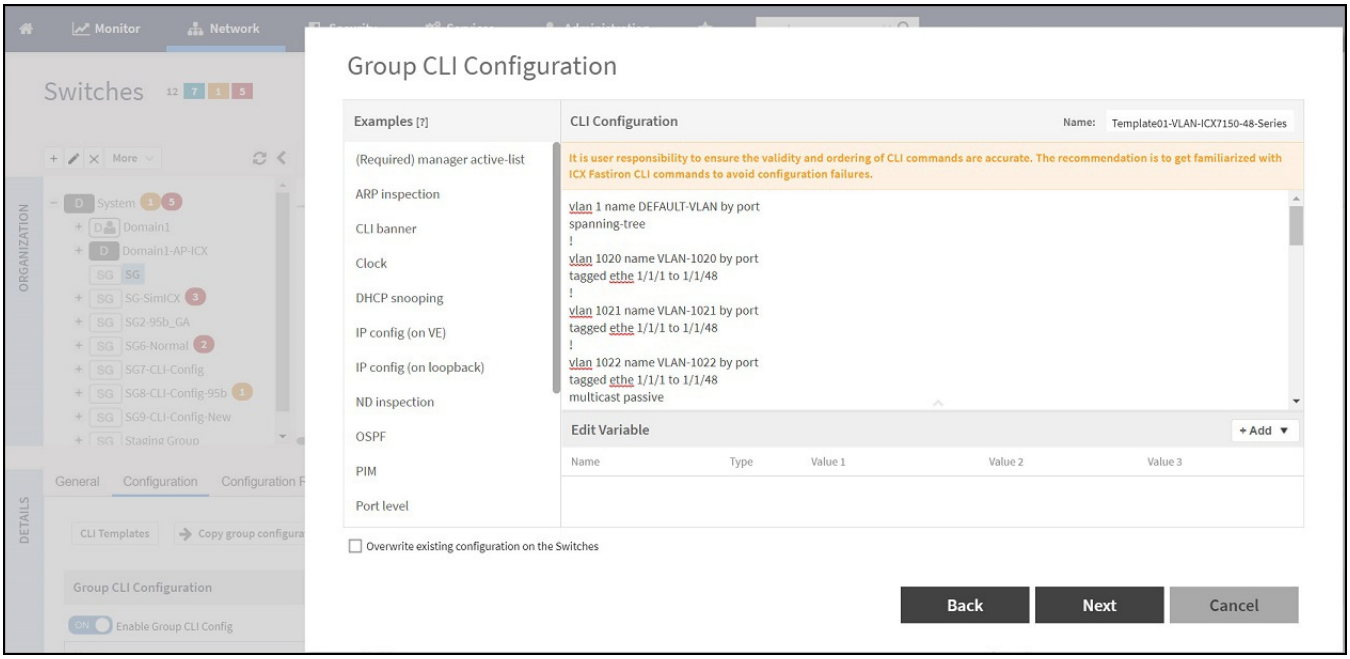


FIGURE 68 Support for space in variable string

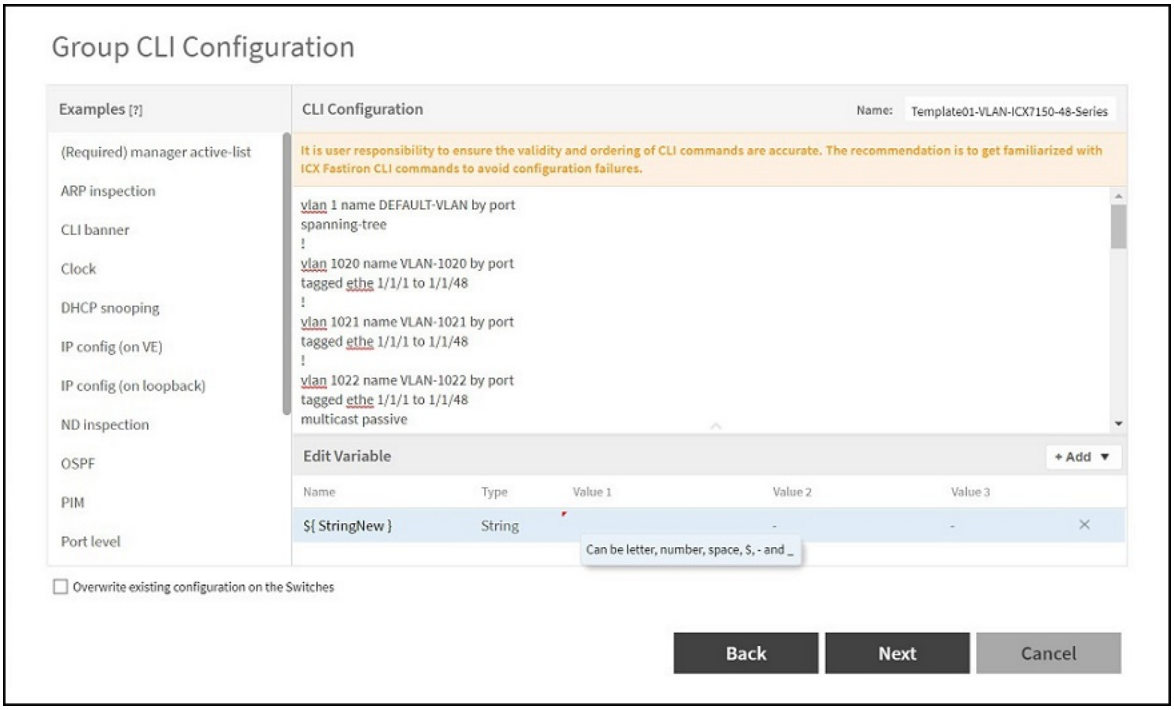


FIGURE 69 Support for dollar sign in varibale string

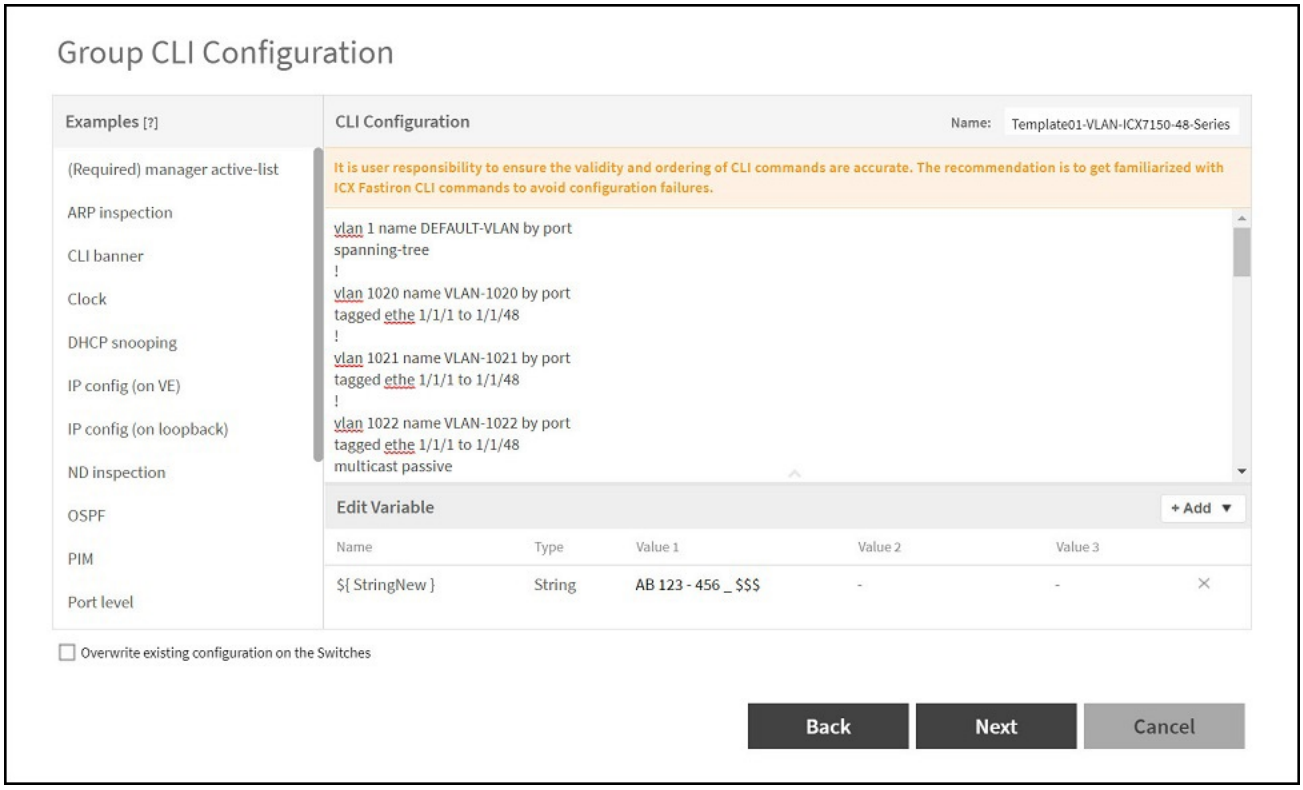


FIGURE 70 Example Template

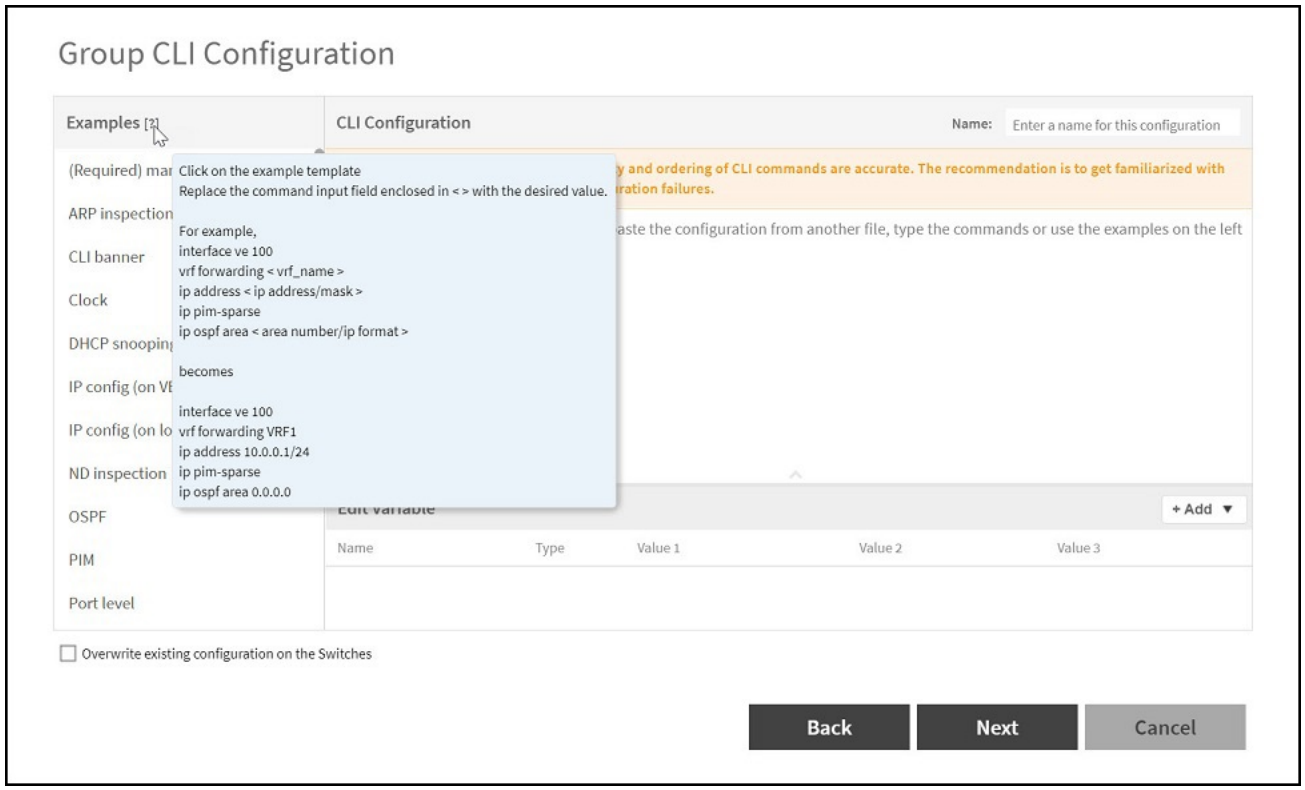


FIGURE 71 Support for IP address in variable

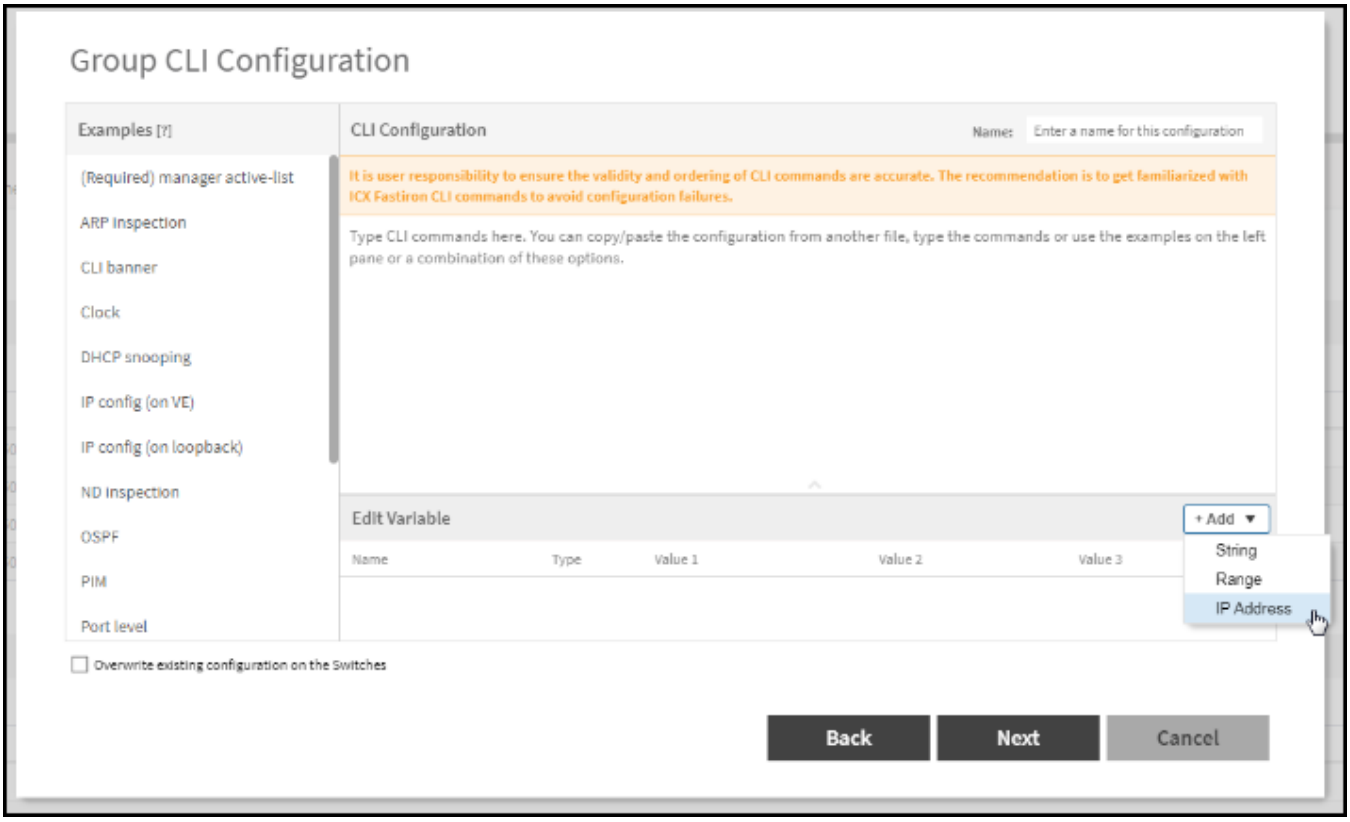


FIGURE 72 Details of fields in IP address in varibale

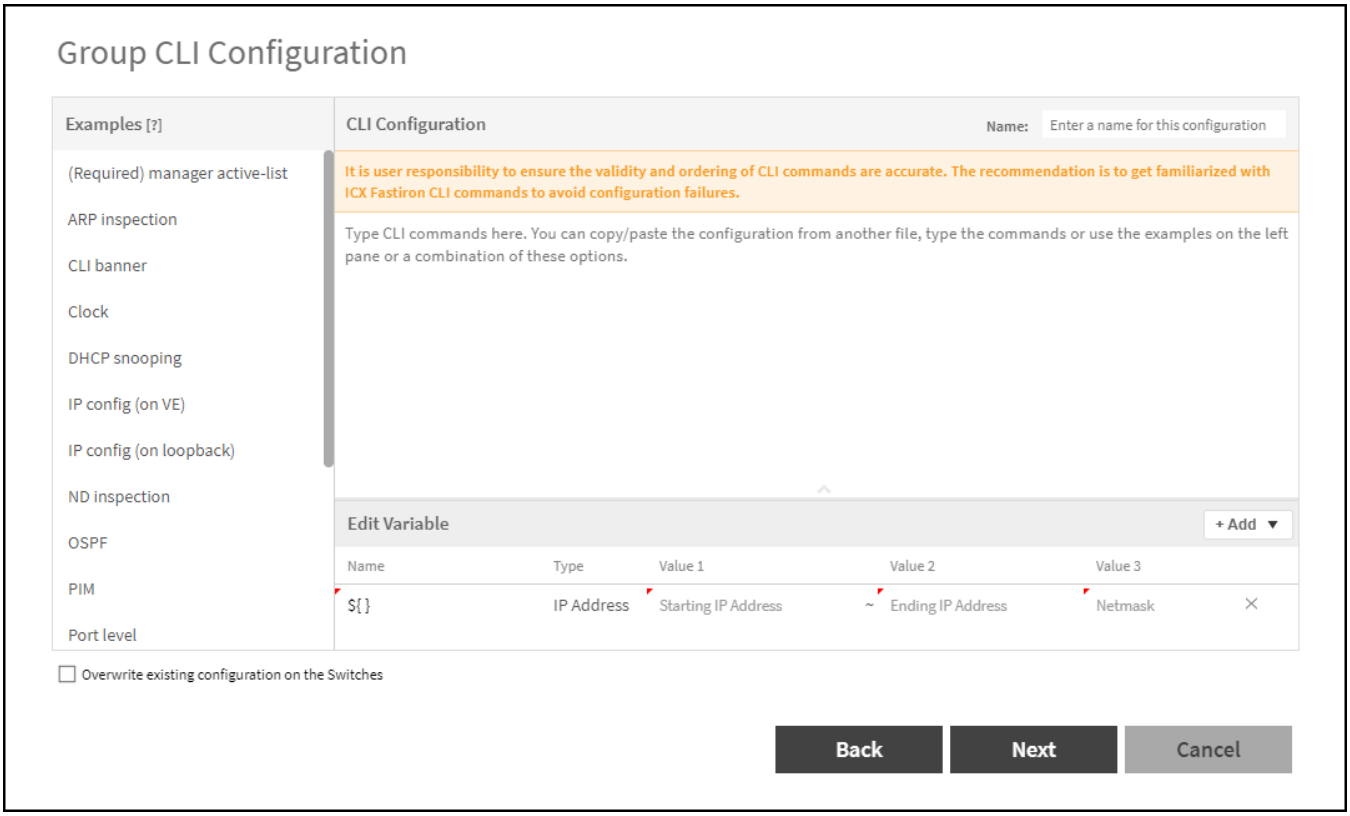
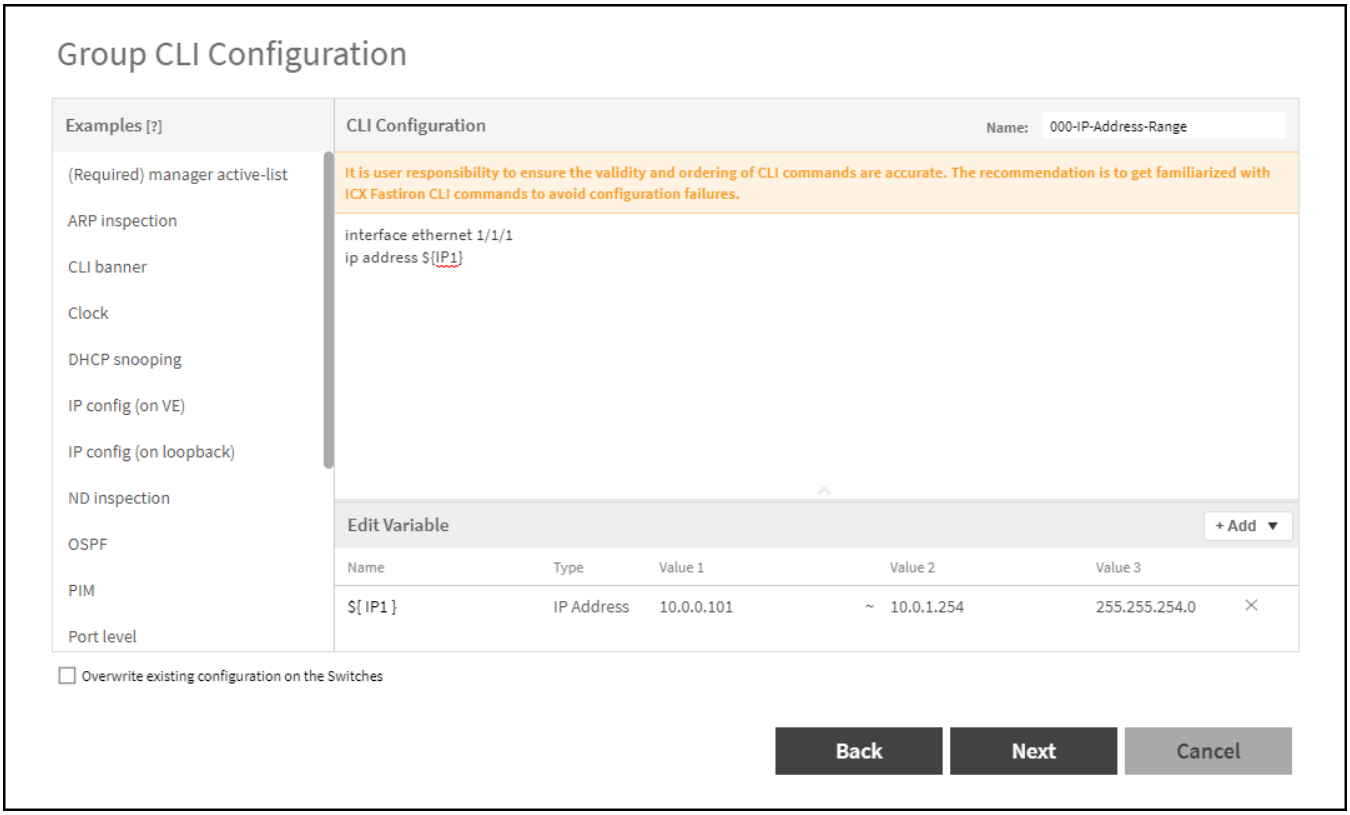


FIGURE 73 Example for IP address in variable



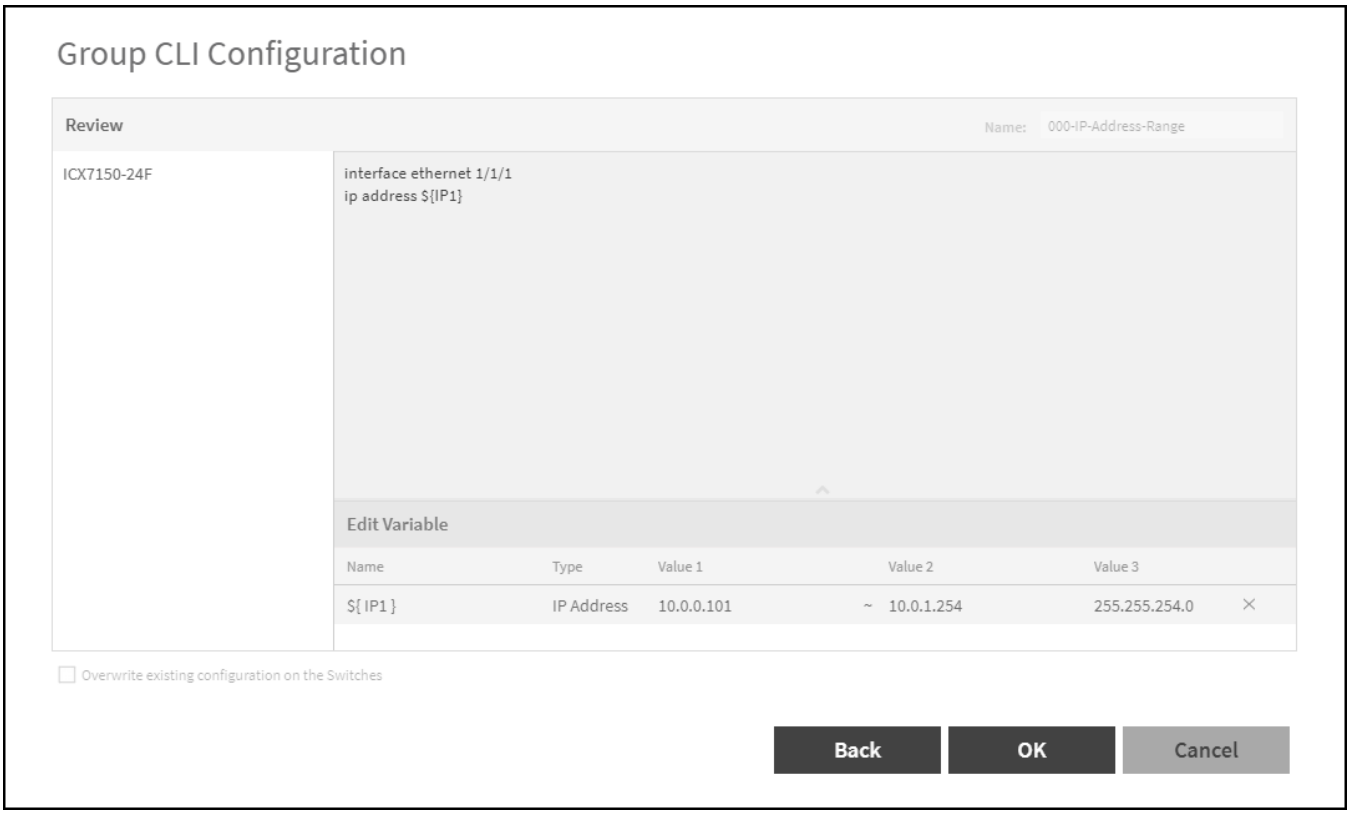
7. Variables asists in applying unique configuration to the switches. For example, IP address can be defined as a variable so that each switch gets assigned a unique IP address . In the **Edit Varible** field, enter the **Name**, **Type**, **Value 1**, **Value 2** and **Value 3** of the variables, where **Value1** denotes the “Starting IP Address”, **Value 2** denotes the “Ending IP Address”, and **Value 3** is the “Netmask".

   NOTE
   The **Edit Variable** field is optional.

   By default, the **Overwrite existing configuration on the Switches** option is not selected and only the factory-default switches (no start-up config) will inherit the group level configuration. If this option is selected, smart zone will replace the existing configuration of the switch with the configuration defined for the group

8. After reviewing the Group CLI Configuration, click **OK**.

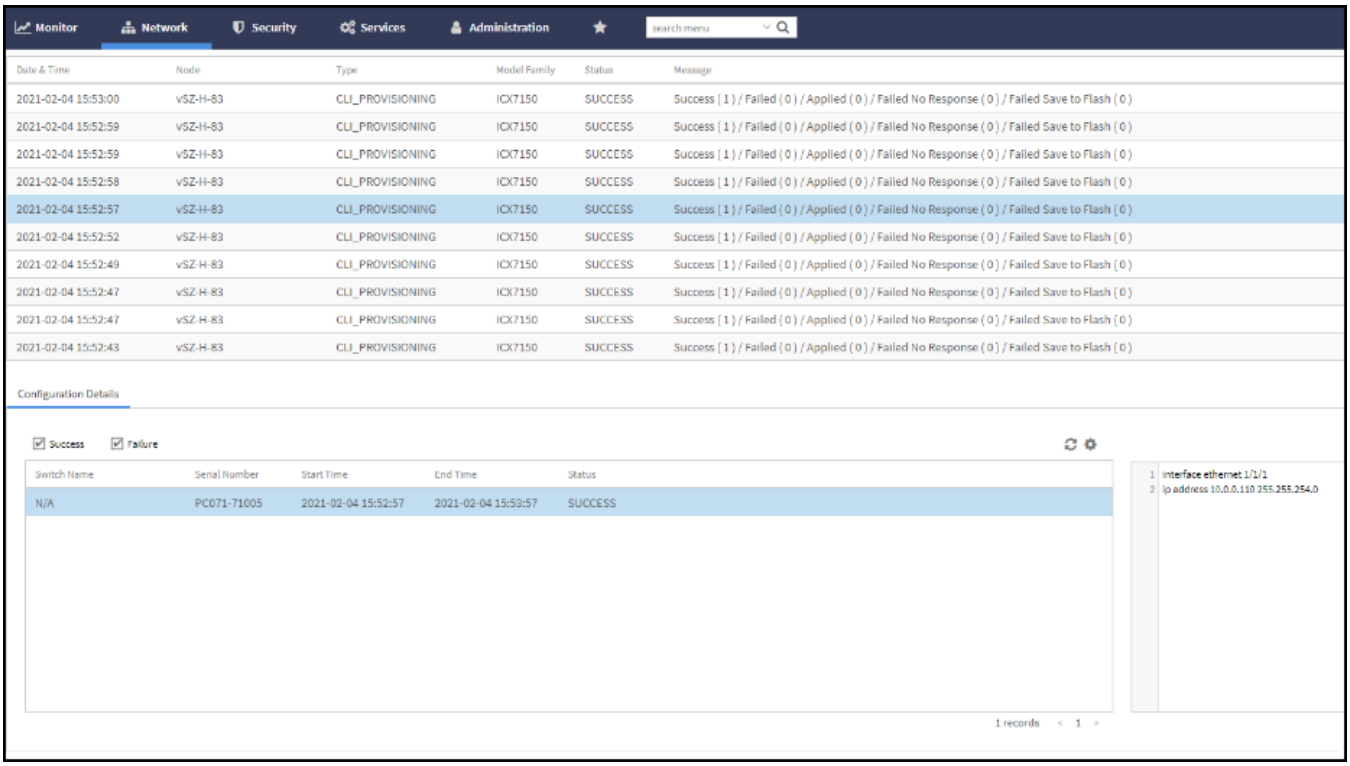
FIGURE 74 Reviewing the Group CLI Configuration



9. A confirmation dialog box is displayed, click **OK**.

10. The switch group is now Group CLI Configuration enabled and is available for provisioning.

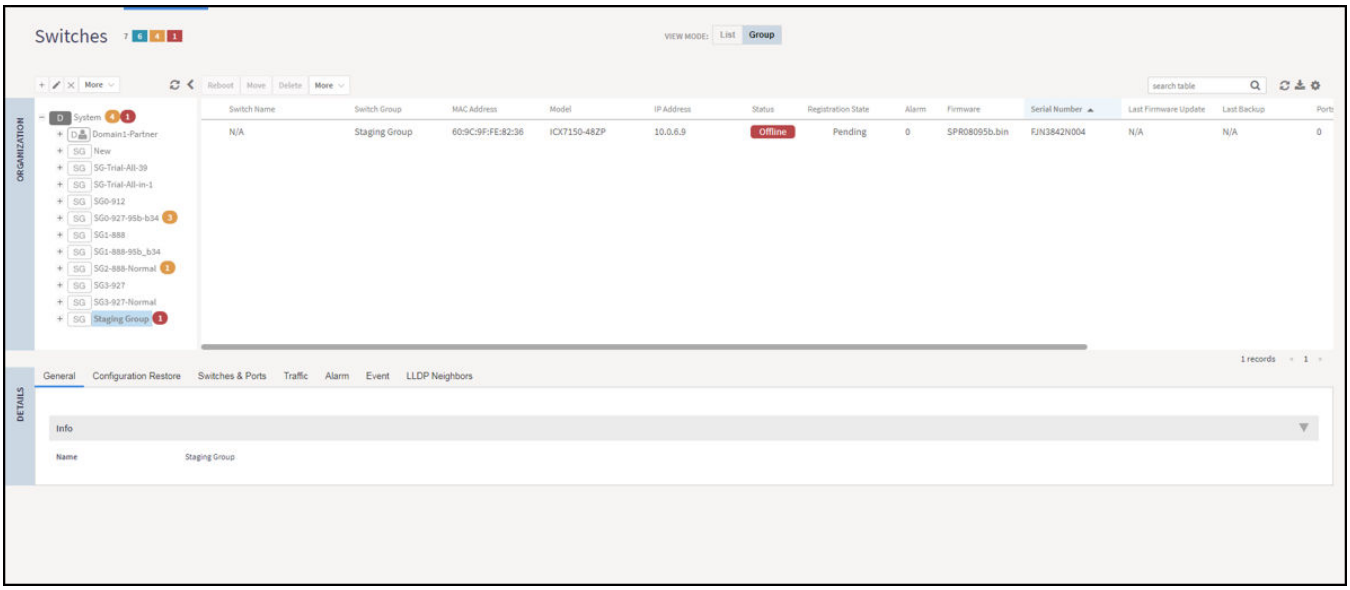
FIGURE 75 Provisioning the Group CLI Configuration Setup



11. After the configuration is setup, any factory default switch joining the group will get the configuration applied and rebooted for the configuration to take effect.

12. In the **Organization** tab, select a **Domain** or **Switch Group** and select the **Switches** .

FIGURE 76 Discovering a New switch



CLI Templates

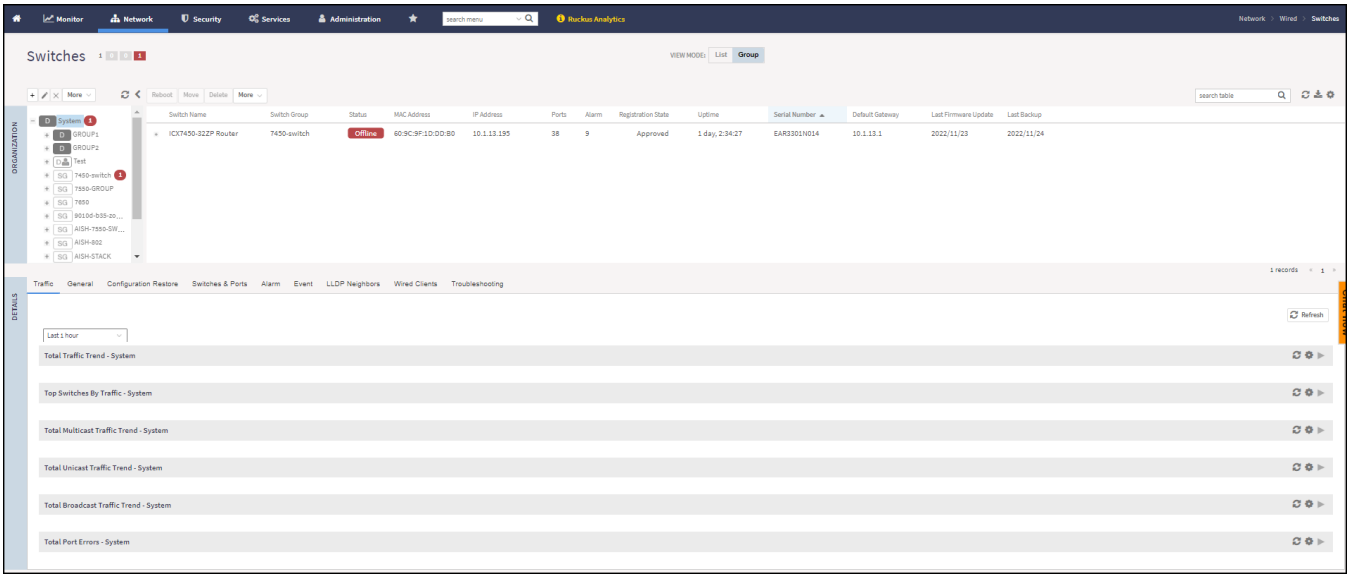
CLI templates enable users to make incremental configuration changes on the fly to the selected switches. CLI templates are not tied to any switch or switch group. Once defined, they can be applied to any selected switch(es) or Switch Groups.

NOTE
Only an administrator with Full Access permission can update CLI configurations. The validity of CLI commands and their ordering rests solely with the administrator.

Using CLI templates

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

   FIGURE 77 Switches

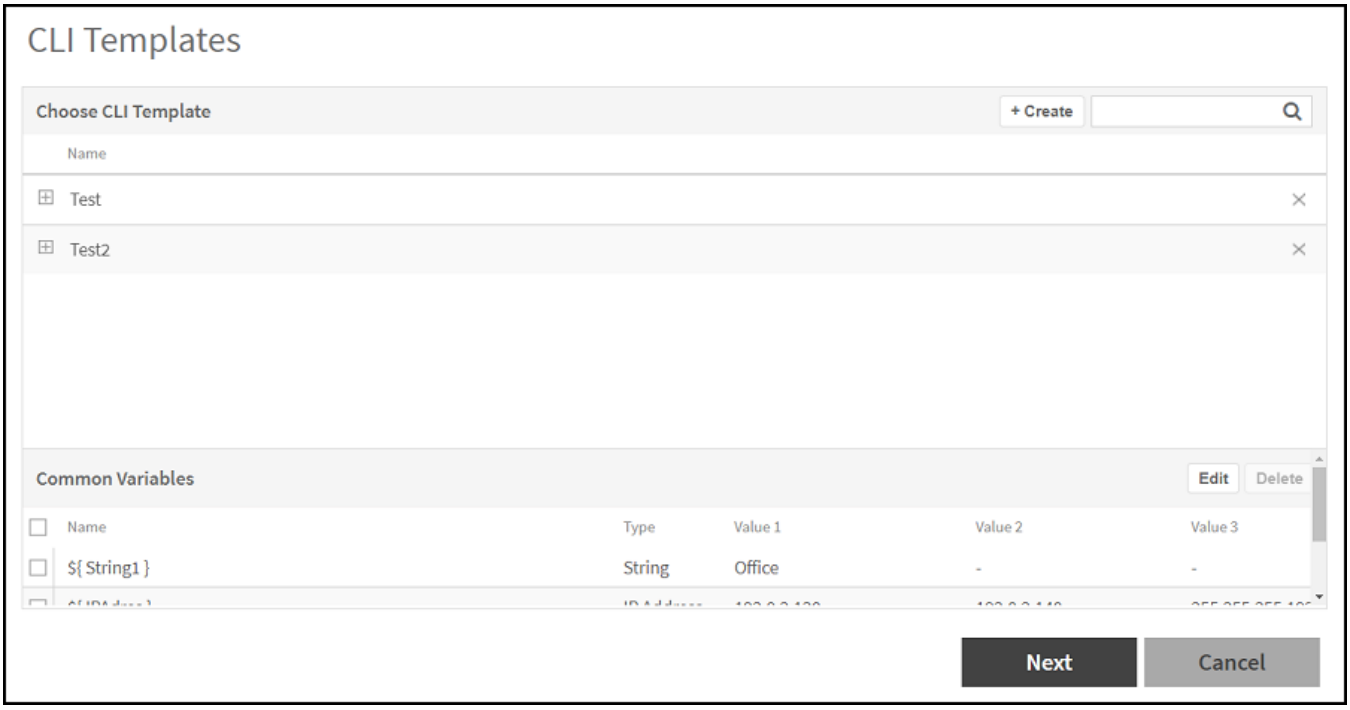


2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and in the **Details** tab, click **Configuration** tab.

3. Click **CLI template** icon to display the **CLI Templates** dialog box. You can select an existing CLI template with an existing common variables or create a new CLI template with a new common varibles.

   NOTE
   To edit existing common variables or add common variables. Click **Edit** icon, modify the common variables or add common variables and then click **Save**. For more information, see *Step 4 b Edit Variable*.

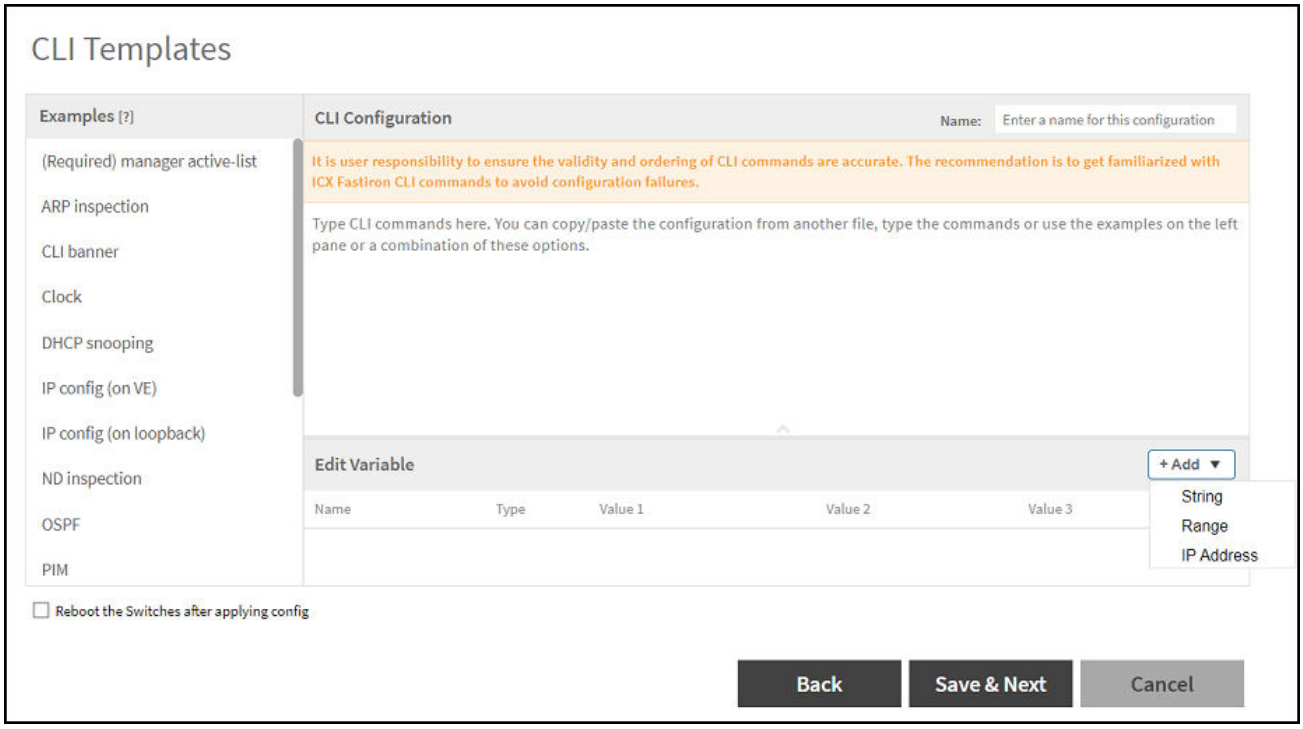
FIGURE 78 CLI Template



4. Complete the following steps to create a new CLI template.

   a) Click + Create icon to display the **CLI Templates** dialog box.

   FIGURE 79 CLI Templates Dialog Box



   b) Complete the following fields:

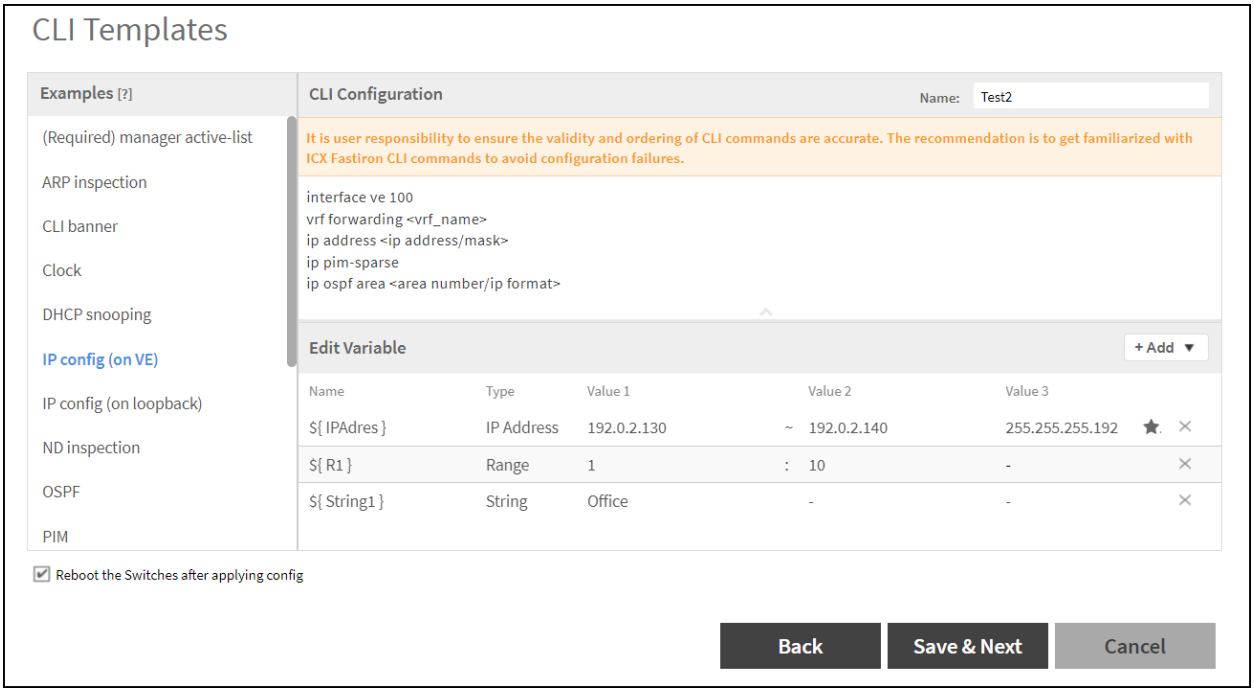
   - **Name**: Enter the name of the CLI template.
   - **Command Lines**: Insert or edit the command lines in the space provided. Users can choose the CLI commands under the 'Examples' pane to build configuration. Alternatively, CLI commands can be typed directly or copied from a notepad and pasted into the 'CLI Configuration' box.

     NOTE
     It is recommended that users get familiarized with FastIron commands and their ordering to avoid any issues with applying the configuration.

   - **Edit Variable**: Click + Add icon and select the **String** or **Range** or **IP Address** variable to add the **String** or **Range** or **IP Address** variable to the table. Variables helps to apply unique configuration to the switches. For example, IP address can be defined as a variable so that each switch gets assigned a unique IP address. In the **Edit Variable** field, enter the **Name**, **Type**, **Value 1**, **Value 2**, and **Value 3** for IP address variables, where Value1 denotes the “Starting IP Address”, Value 2 denotes the “Ending IP Address”, and Value 3 is the “Netmask". Click icon to add a new variables setting to the Common Variables.

     NOTE
     The **Edit Variable** field is optional.

FIGURE 80 Adding Common Variables

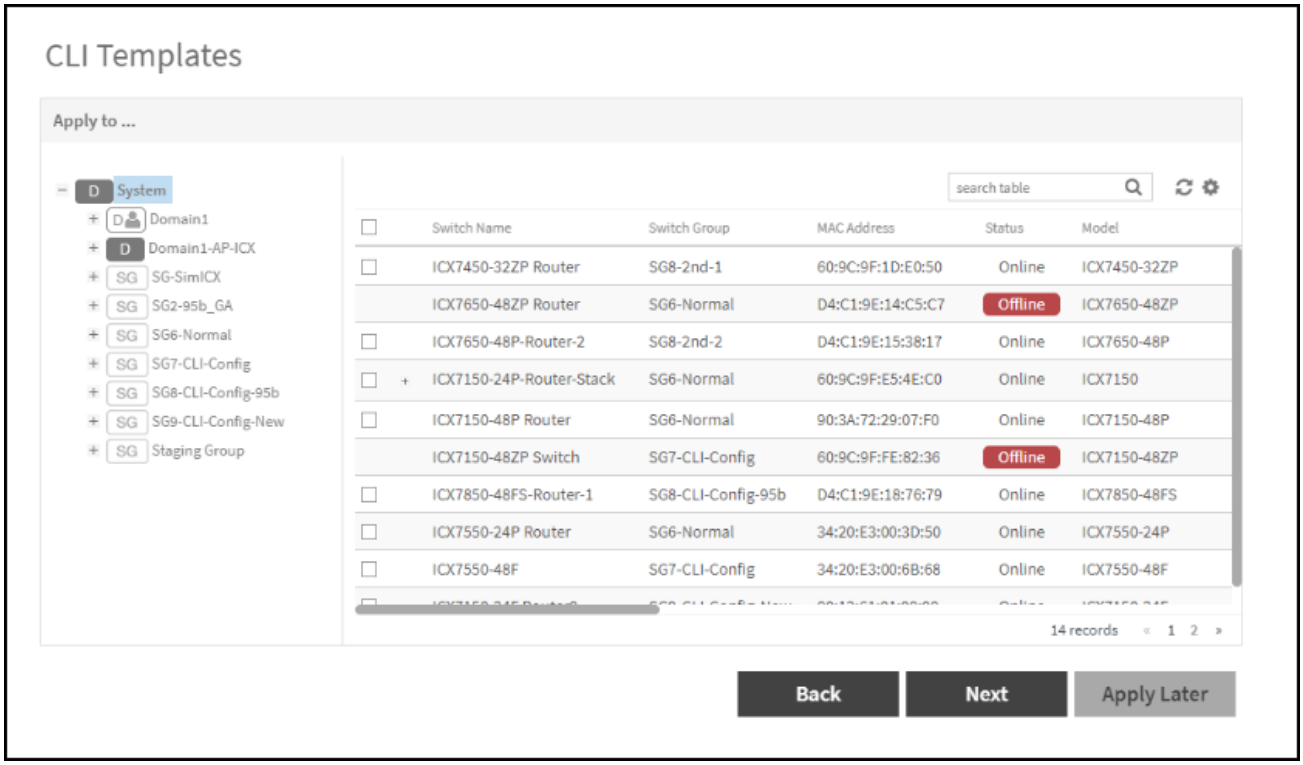


c) Select **Reboot Switches after applying config** check box if you want the switch to reload after the configuration update. If you do not select this option, the switch will not reload after the configuration update.

d) Click **Save & Next**.

e) Select the target switches check box and click **Next** to display the **Review** dialog box.

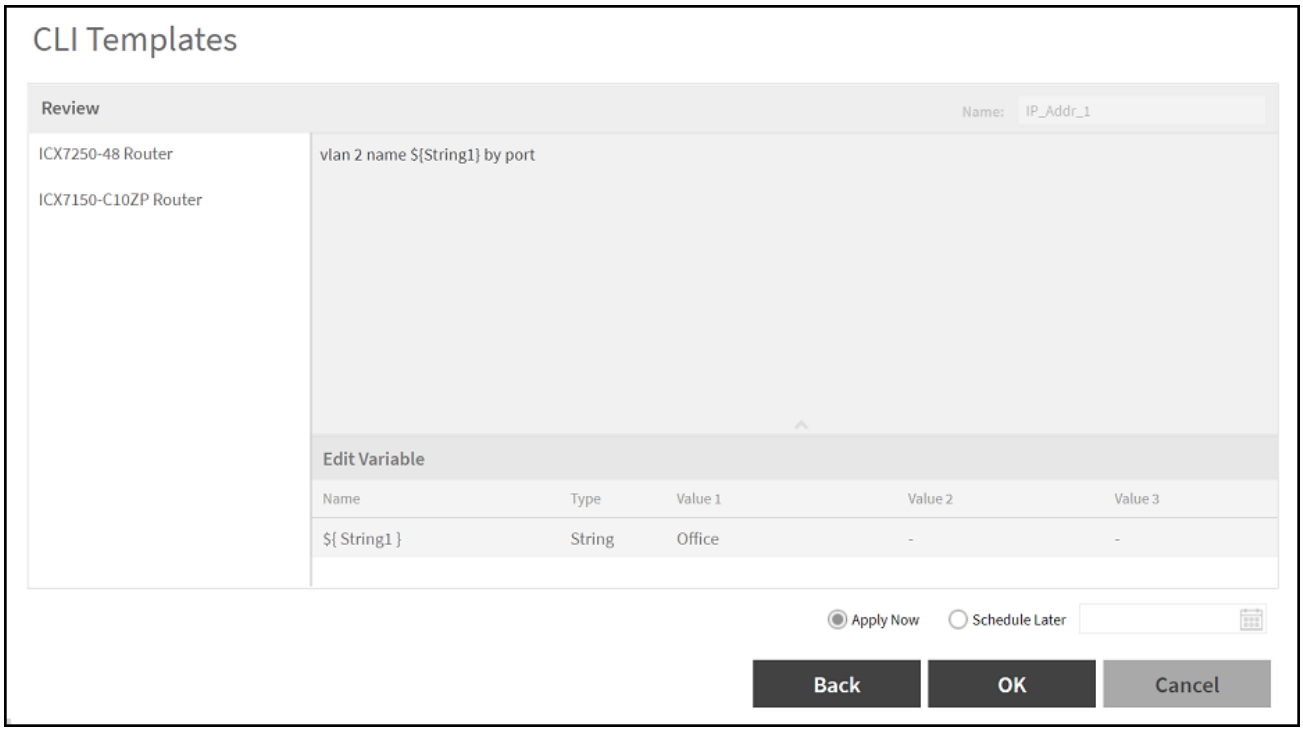
FIGURE 81 Selecting Switches



NOTE
Configuration will be applied only to the switches that are online. Users need to re-apply configuration for switches that are offline at a later time when they come back online.

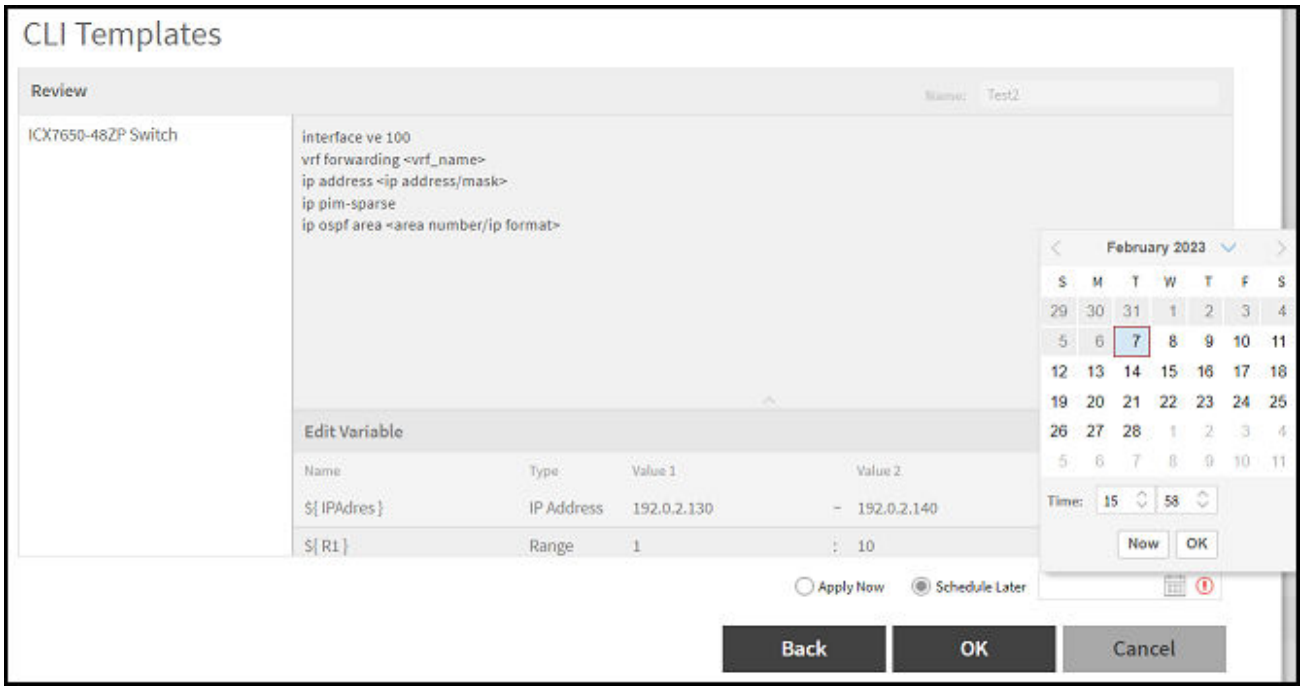
f) Review the CLI template.

FIGURE 82 Reviewing the CLI Template



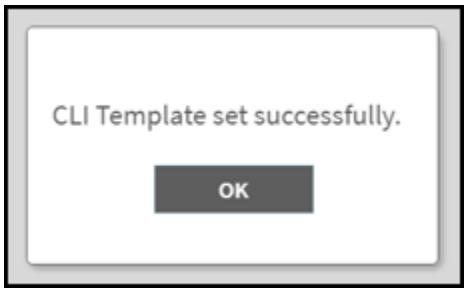
g) Select **Apply now** or **Schedule Later** to save the created template and apply to the selected switches. If you select the **Schedule Later** then select the **Date** and **Time** to apply the configuration.

FIGURE 83 Schedule Later Dialog Box



h) Click **OK** to display the **CLI Template Set Successfully** message.

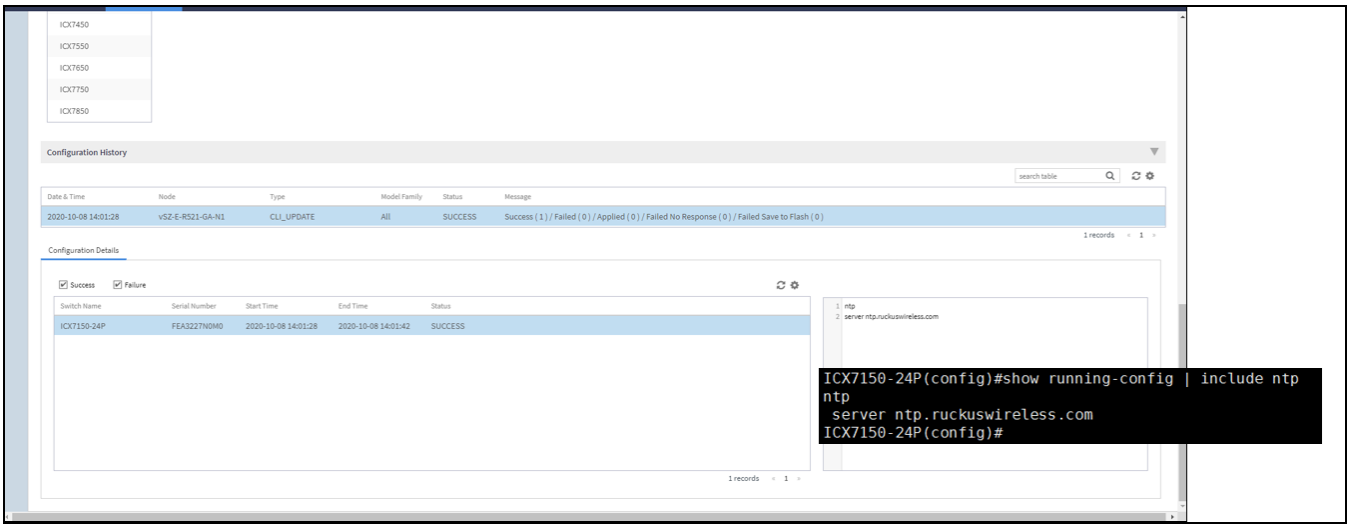
FIGURE 84 Applying the CLI Template



i) Click **OK**.

5. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and in the **Details** tab, click **Configuration** tab.
6. In the **Configuration History** tab, select the **Switch** to display the **Configuration Details** tab. Make sure that the CLI template is successfully added to the switch.

FIGURE 85 Updating the Command Lines to Switch



The following status messages are displayed on the **Status** tab.

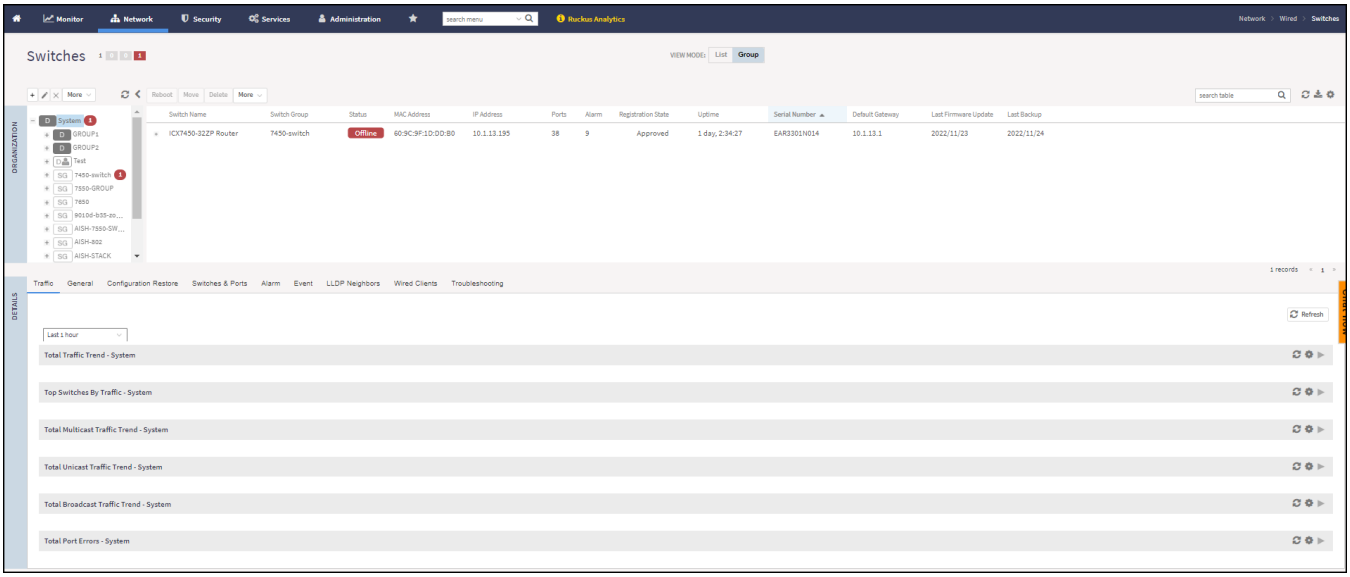
- **Success** if the configuration is applied successfully.
- **Failed** if there is a failure in configuring a switch.
- **Applied** if the configuration is partially successful with one ore more informational messages or warnings returned by the switch.

Creating Config Backup for Switch Group

The Master Config backup allows you to initate backup of switch group or domain.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

   FIGURE 86 Switches

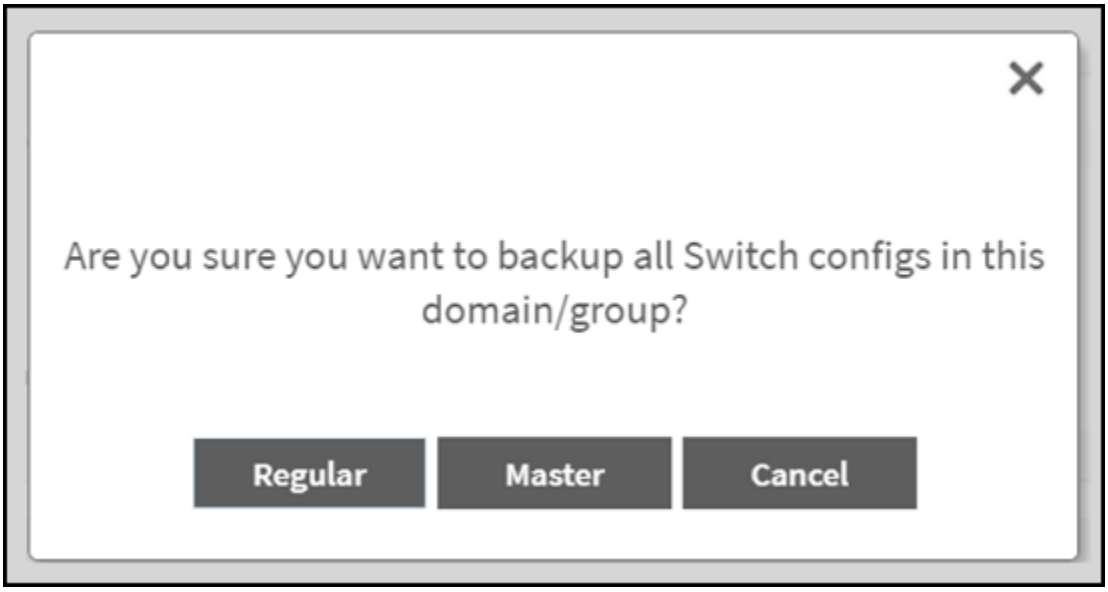


2. In the **Organization** tab, select the **Domain** > **Switch Group** or **Switch Group**.

3. Click **More** > **Config Backup**.

   A confirmation message is displayed asking the type of backup that must be carried such as **Regular** or **Master**.

   FIGURE 87 Backing up Switch group or Domain



4. Click **Master** to create master backup for switch groups.
5. **Switch config backup operation is triggered successfully** dialog box is displayed, click **OK**.

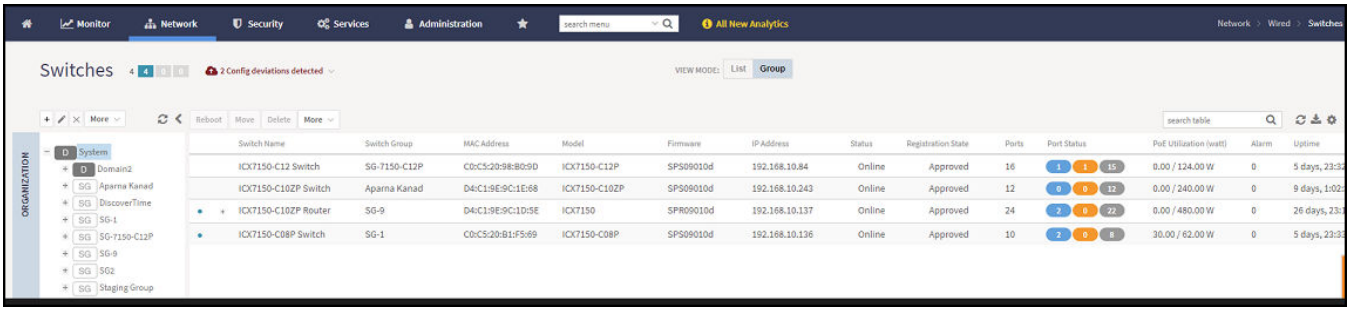
Viewing Configuration Alerts

If a config backup was selected as a master config backup, then you will receive an alert if there is any config backup generated later on with different content from the master one. For more information on config backup settings, refer the topics Backing up and Restoring Switch Configuration on page 32 and Creating Config Backup for Switch Group on page 94.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

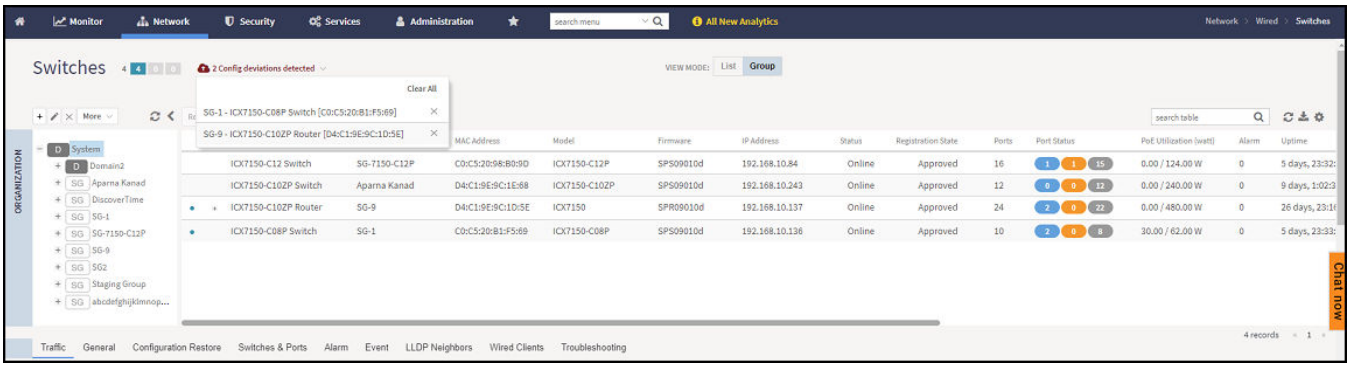
   The alert is displayed at the top of the switch page.

   FIGURE 88 Master Backup Alert



2. You can expand the drop down list to view the switches or switch groups for which the backup configuration was updated.

   FIGURE 89 Expanding the drop-down list of Alert



3. You can click Clear All to clear all of the alerts from the list, or you can individually remove each switch by clicking .

   NOTE

   The icon in the switch table announces that the backup in the switch configuration is changed. The icon and the alert are cleared automatically when the latest config is same as master backup config.

Port Settings

Port level configuration can be viewed and edited from the **Switch Port** page. You can select ports belonging to a single switch or from different switches within a switch group. The search box can be used to filter ports based on port numbers, names, or VLANs. Once the desired list of ports are filtered, you can select the ports and make changes to their existing settings by performing the procedure Creating Switch Level Configuration on page 65.

Creating a Port Template

The controller allows you to configure switch port settings. However, there are many advanced port settings that are not supported by the controller. You have to configure these advanced port settings on the switch console. So, the controller introduces with Port Template to improvise the deployment of the advanced port settings.

You can apply port template to joined or online switch ports for which the firmware version is 08.0.95b or higher. If the switch port is newly added, you have to apply the template again.

NOTE
You cannot apply port template to ports that belong to offline switches.

NOTE
Apply the new untag VLAN to selected ports. Make sure to untag the default VLAN from these ports before applying the Port Template.

You can create or edit a port template and attach it to the target port in the following two ways.

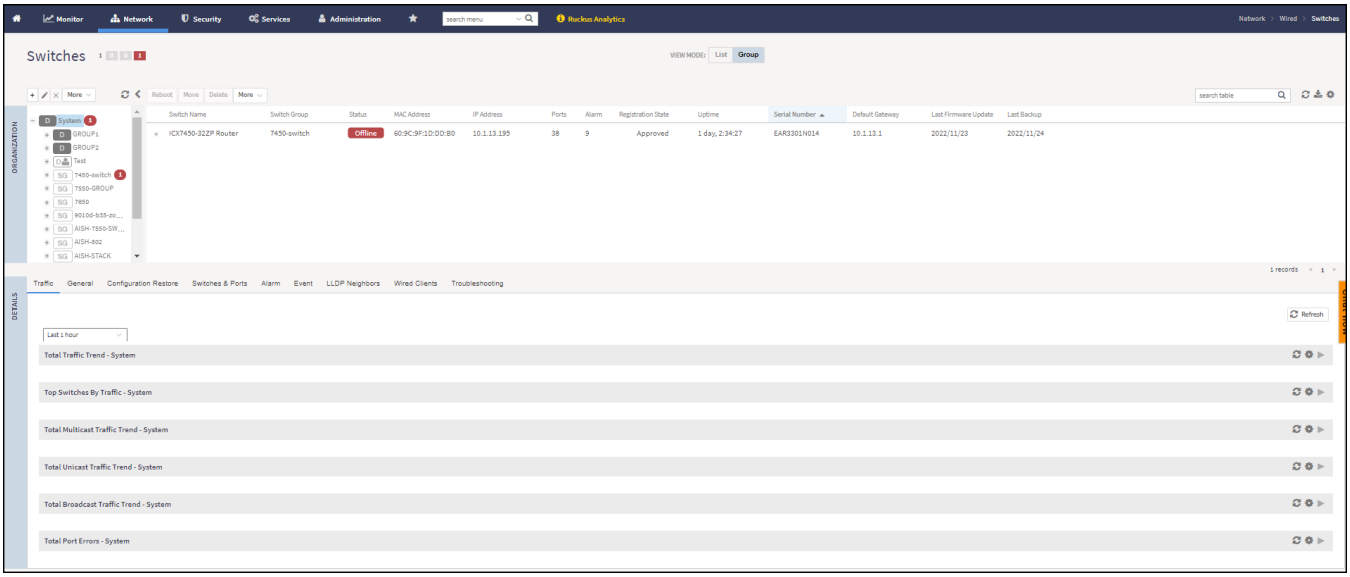
- Create or edit a port template and then assign it to target ports
- Select a target port and then assign the port template

Creating a Port Template and Assigning Target Ports

You can apply port template and assign port to the template by performing the below steps.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

   FIGURE 90 Switches



2. To create Port Template, select a **Domain** > **Switch Group** or **Switch Group** and in the **Details** tab, click **Switches and Ports** tab, or select a **Switch** and click **Ports** tab.

3. In the **Port Details** tab, click **Port Template** icon to display the **Port Template** dialog box.

FIGURE 91 Clicking Switches and Ports Tab

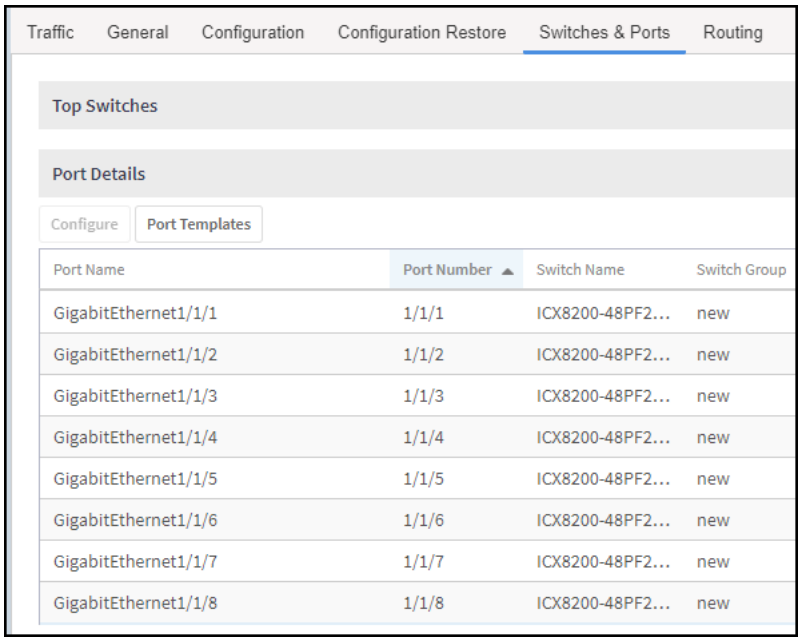
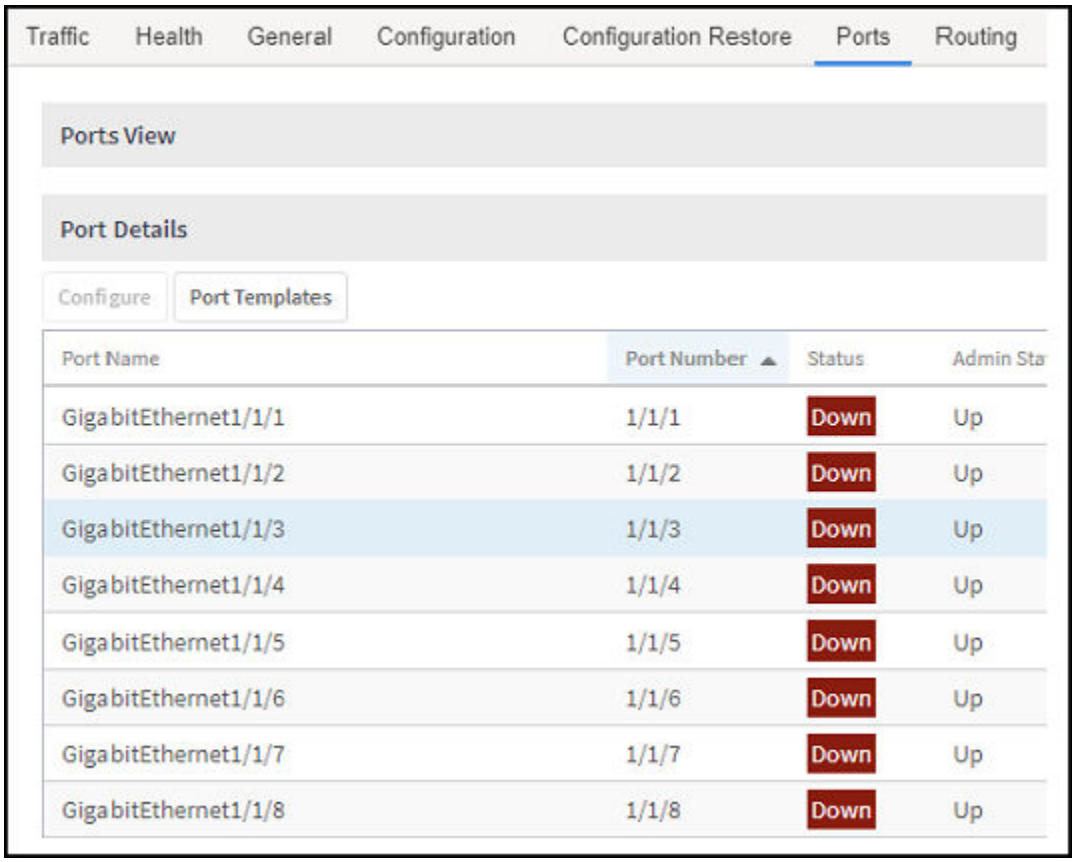


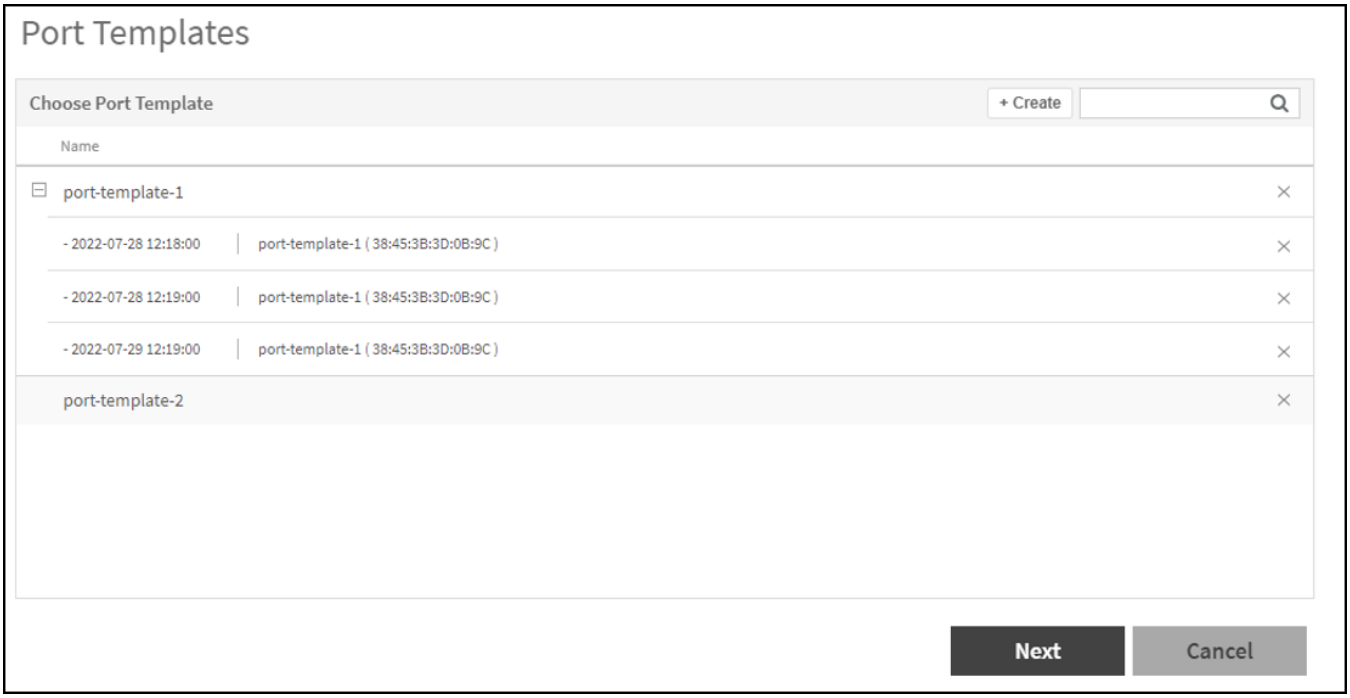
FIGURE 92 Clicking Ports Tab


Traffic
Health
General
Configuration
Configuration Restore
Ports
Routing
Ports View
Port Details
Configure
Port Templates
Port Name
Port Number
Status
Admin Sta
GigabitEthernet1/1/1 1/1/1 Down Up
GigabitEthernet1/1/2 1/1/2 Down Up
GigabitEthernet1/1/3 1/1/3 Down Up
GigabitEthernet1/1/4 1/1/4 Down Up
GigabitEthernet1/1/5 1/1/5 Down Up
GigabitEthernet1/1/6 1/1/6 Down Up
GigabitEthernet1/1/7 1/1/7 Down Up
GigabitEthernet1/1/8 1/1/8 Down Up

4. In the **Port Template** dialog box, expand "+" icon to view a list of scheduled port templates, click 

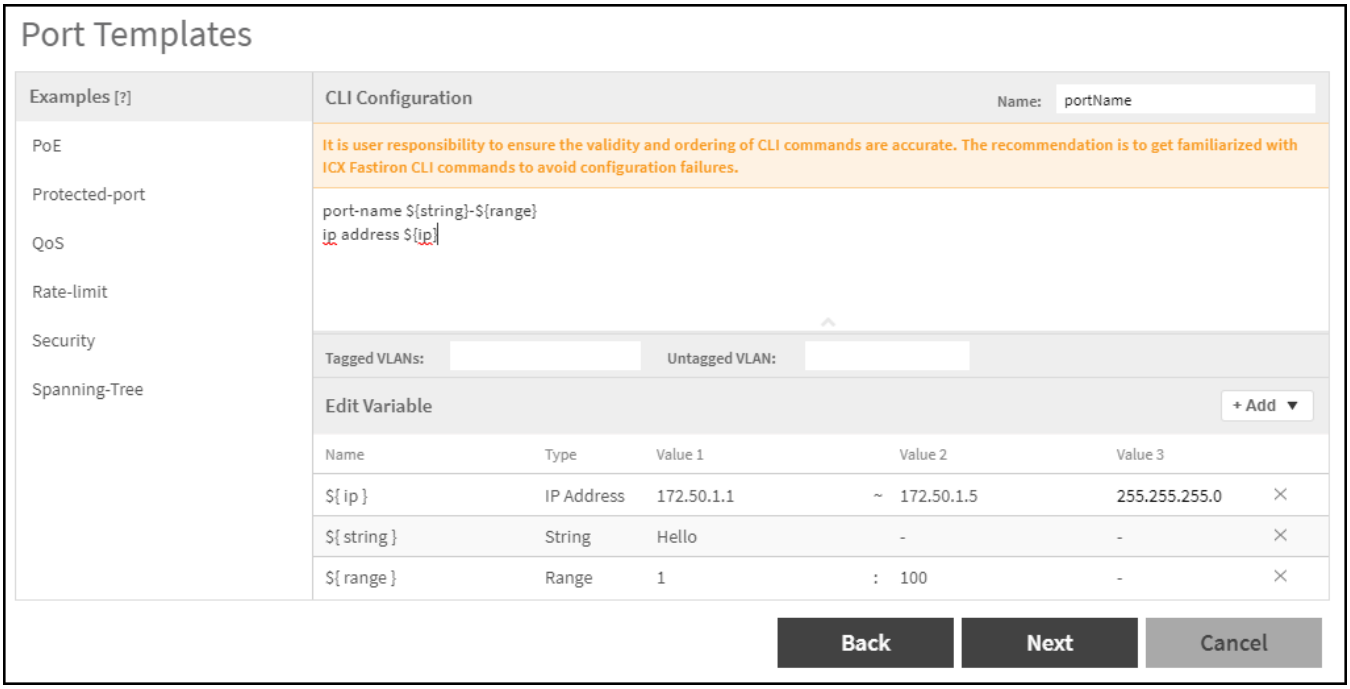
icon to create a new port template, or click "x" if you want to delete an existing template. Click **Next** to update the port template.

FIGURE 93 Choosing Port Template



5. To create a port template, complete the following steps:
   a) Enter the name of the port template in the **Name** field.
   b) Variables helps to apply unique configuration to the switches. If you want to use variable in the CLI Configuration editor, it must start with a symbol "$" and a pair of curly braces {VARIABLE_NAME}. For example, IP address can be defined as a variable so that each switch gets assigned a unique IP address. In the **Edit Variable** field, enter the **Name**, **Type**, **Value 1**, **Value 2**, and **Value 3** for IP address variables, where Value1 denotes the "Starting IP Address", Value 2 denotes the "Ending IP Address", and Value 3 is the "Netmask".
   c) In the **Tag** and **Untag VLAN** field, input the tag and untag VLAN for the port template.
   d) The **CLI Configuration** field provides a text editor to input command types for the template, including the variables.
   e) Click **Examples** to view the example command line references in the CLI Configuration editor.

FIGURE 94 Editing Port Template



6. After editing, click **OK** to save or update the port template. Click **Back** to view the previous step. Click **Cancel** to close the window.

7. Select a target port to apply the created template. To select a target port, select either switch group and click **Switches and Ports** tab, or select a switch and click **Ports** tab . After selecting the ports, click **Apply Port Template**.

   NOTE
   You can select at most 250 ports for applying port template.

FIGURE 95 Selecting Target Port by Clicking Switches and Ports Tab

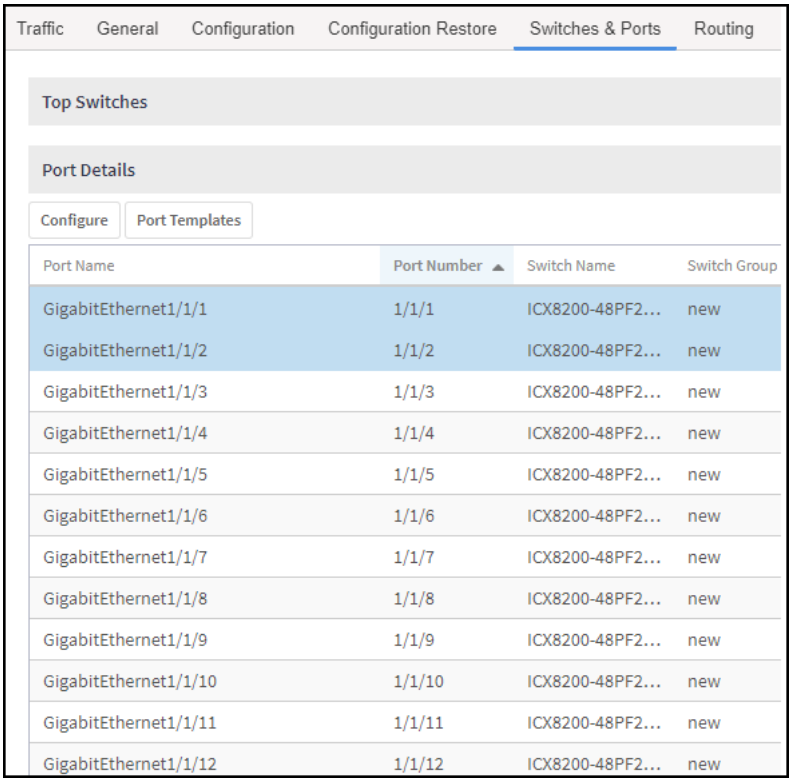
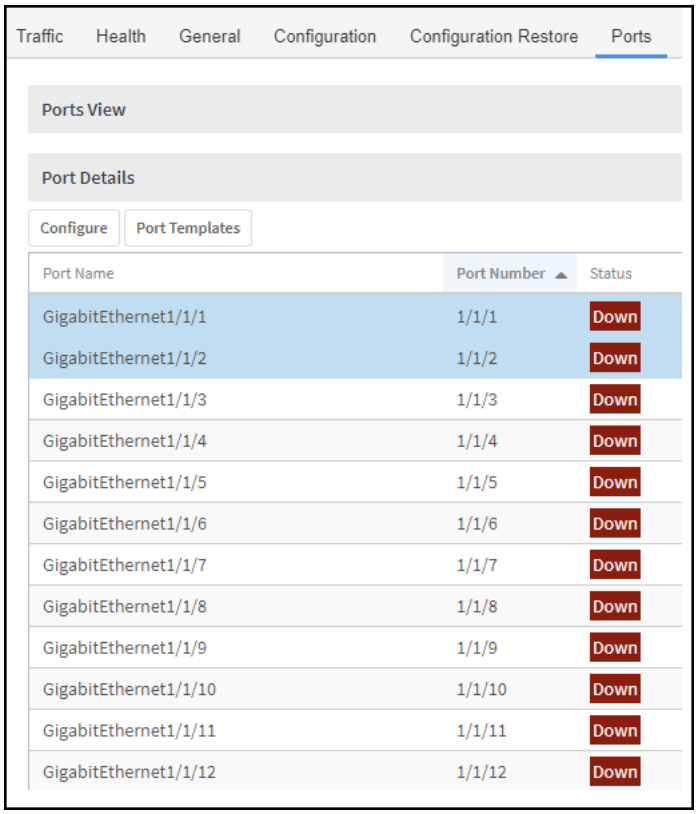
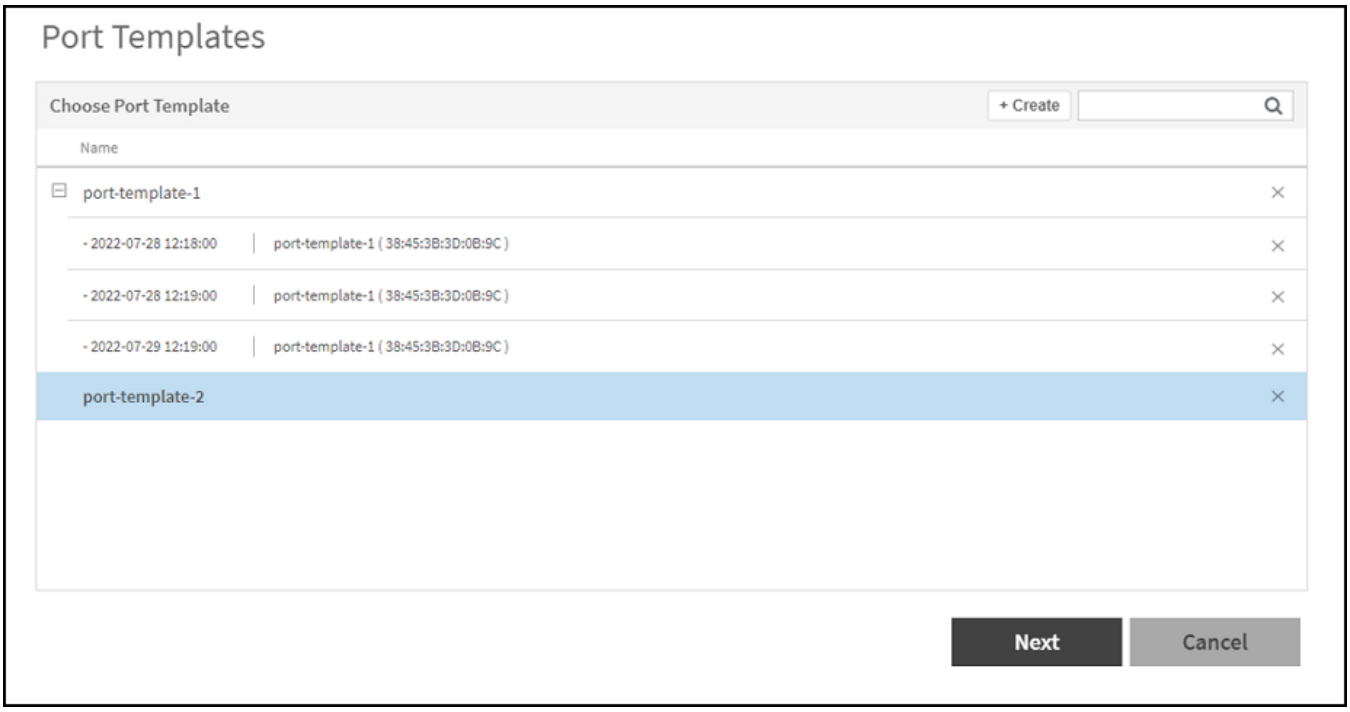


FIGURE 96 Selecting Target Port by Clicking Ports Tab


Traffic
Health
General
Configuration
Configuration Restore
Ports
Ports View
Port Details
Configure
Port Templates
Port Name
Port Number
Status
GigabitEthernet1/1/1 1/1/1 Down
GigabitEthernet1/1/2 1/1/2 Down
GigabitEthernet1/1/3 1/1/3 Down
GigabitEthernet1/1/4 1/1/4 Down
GigabitEthernet1/1/5 1/1/5 Down
GigabitEthernet1/1/6 1/1/6 Down
GigabitEthernet1/1/7 1/1/7 Down
GigabitEthernet1/1/8 1/1/8 Down
GigabitEthernet1/1/9 1/1/9 Down
GigabitEthernet1/1/10 1/1/10 Down
GigabitEthernet1/1/11 1/1/11 Down
GigabitEthernet1/1/12 1/1/12 Down

8. After clicking **Apply Port Template**, a **Port Template** page is displayed that lists all the available port templates. Expand "+" to view a list of scheduled port templates. Select the target port template, and click **Apply** to review the applied configurations. You can select scheduled port template, and click **Next** to update the scheduled port template configurations.

FIGURE 97 Applying Port Template



9. Verify the details for the target ports, Port Template CLIs, Tag and Untag VLANs and the variables in the **Review** page. Click "+" on the left of **Review** page to add more ports to the list. You can also organize the port list by selecting a port and dragging it above or below . Click "x" to delete switch port from the list. Select **Apply Now** to apply the port template immediately. Select **Schedule Later** to apply the port template at the specified schedule time. After selecting either **Apply Now** or **Schedule Later**, click **OK**.

   The various operations that can be performed on the ports in the port list are as shown below.

FIGURE 98 Adding Ports to the List

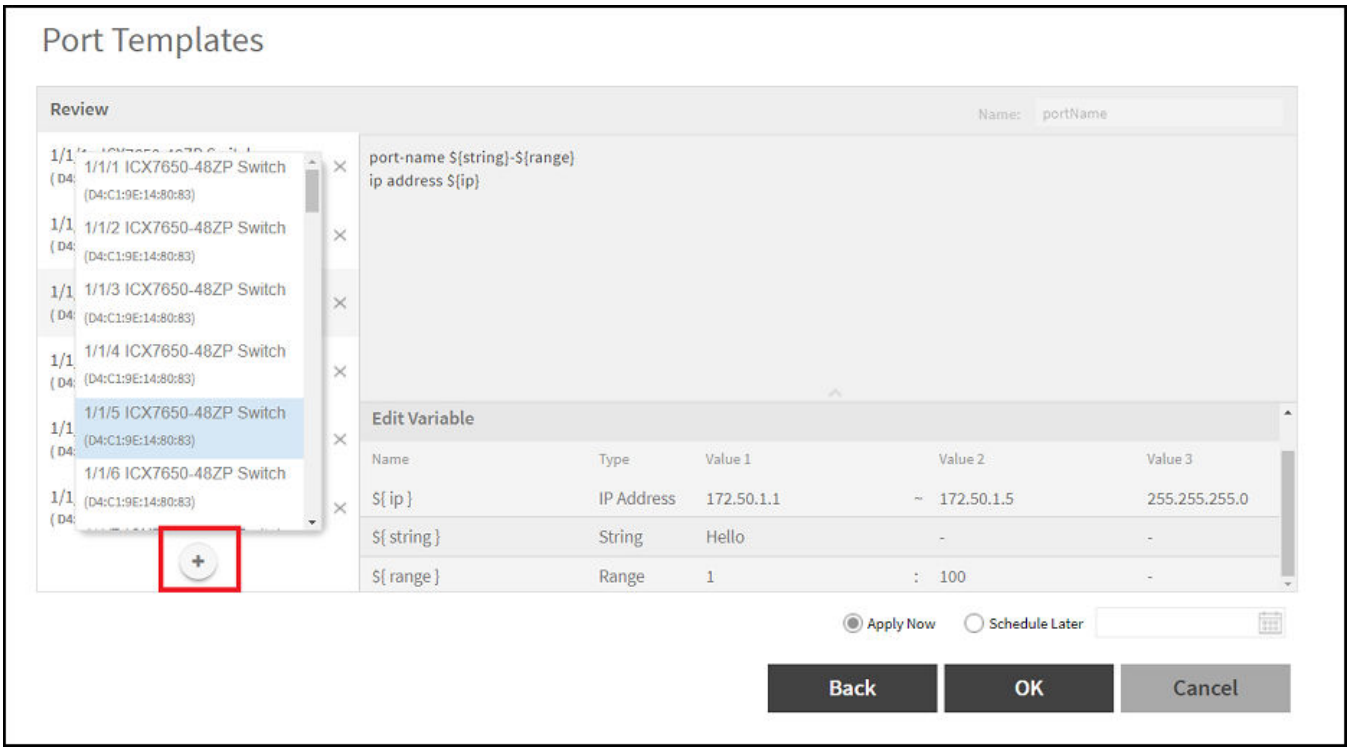


FIGURE 99 Organizing the Port List

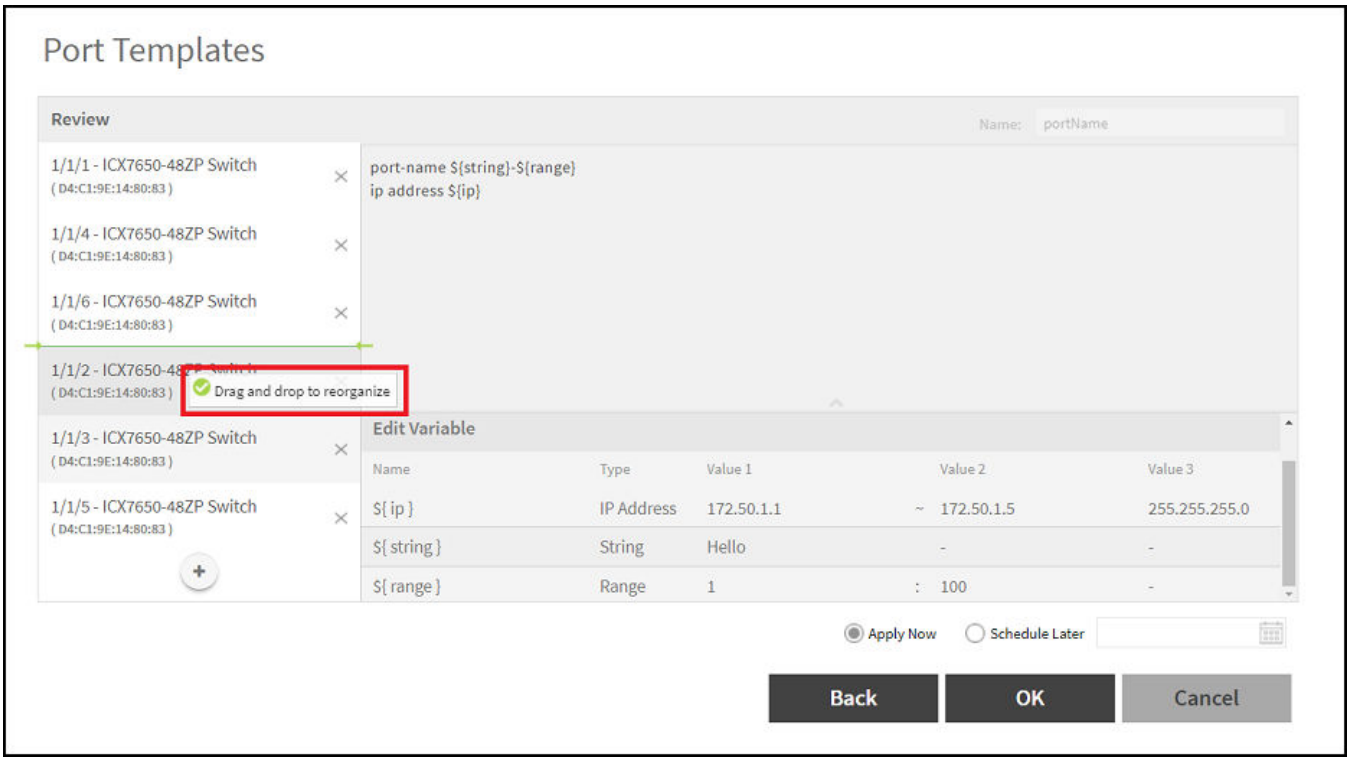
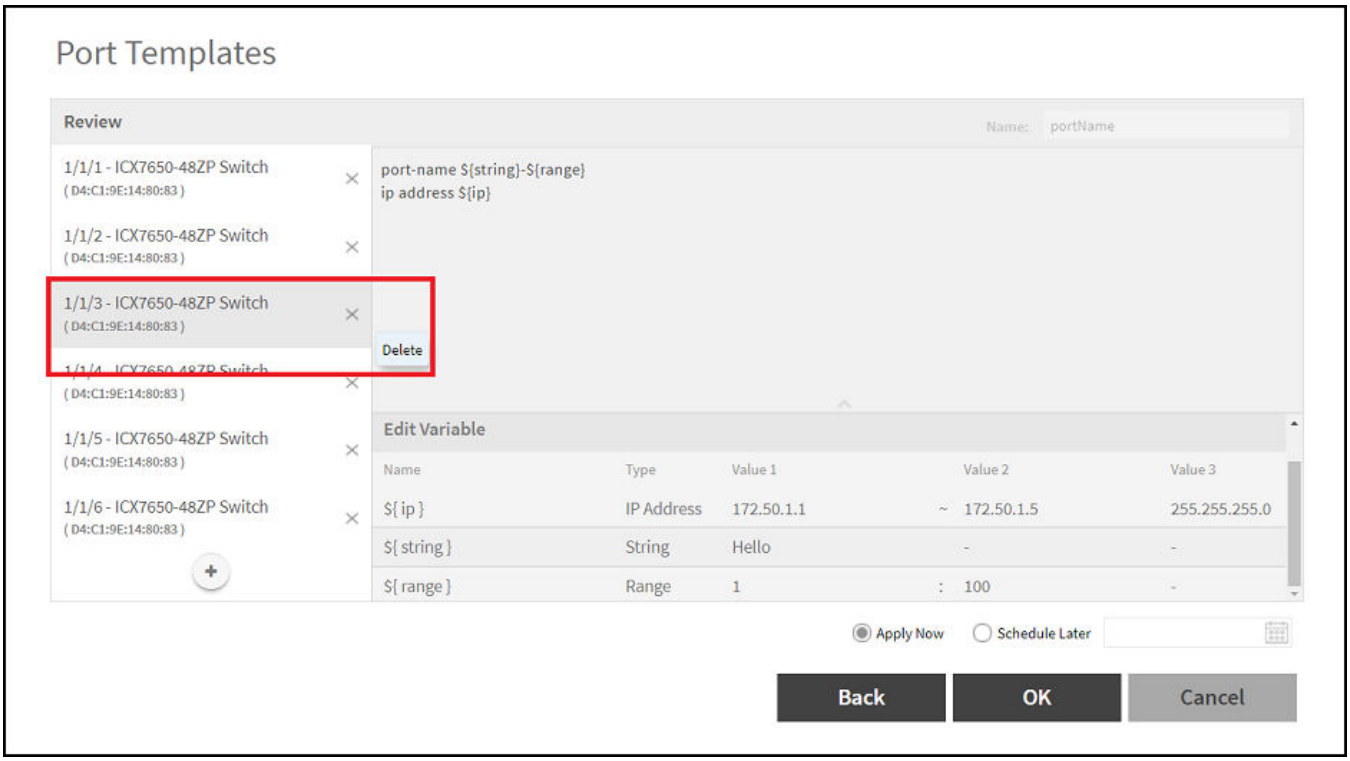


FIGURE 100 Deleting Port from the List



10. A **Port Template applied successfully** message dialog box is displayed, click **OK**.

Selecting Target Ports and Assigning Port Template

You can apply the port template to selected target port by performing the below steps.

1. From the main menu, go to **Network** > **Wired** > **Switches**.

2. Select target port by either selecting a **Domain** > **Switch Group** or **Switch Group**, and clicking **Switches and Ports** tab, or selecting a **Switch** and clicking **Ports** tab.

FIGURE 101 Clicking Switches and Port Tab to Select Target Ports

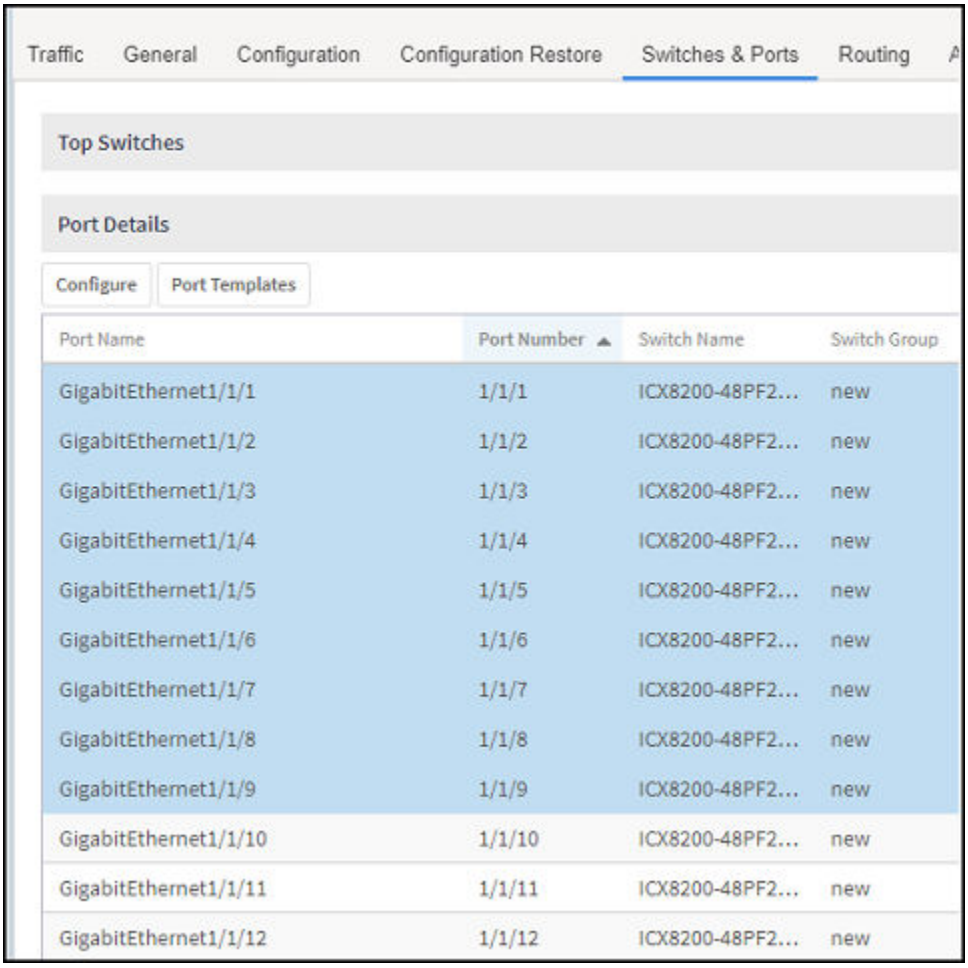
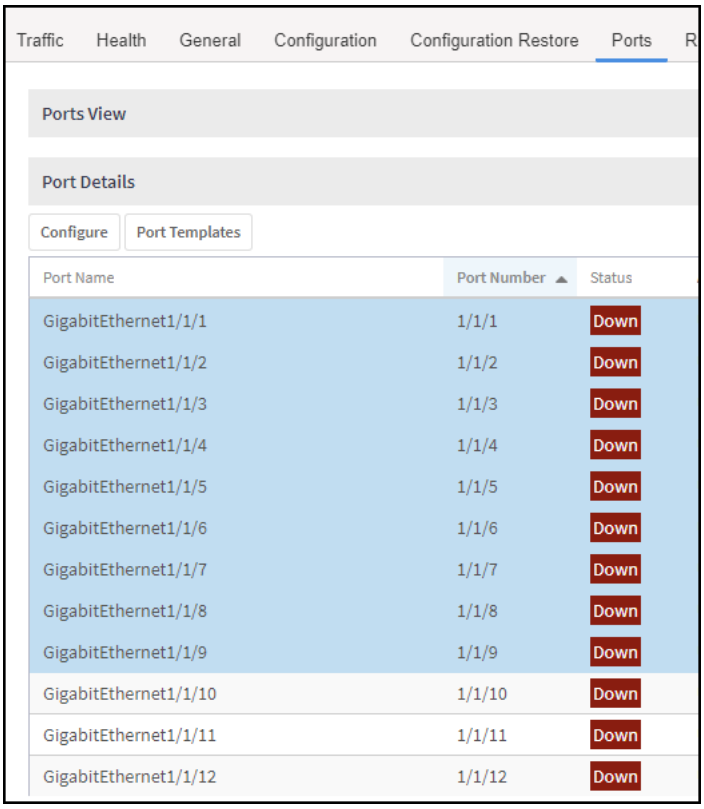
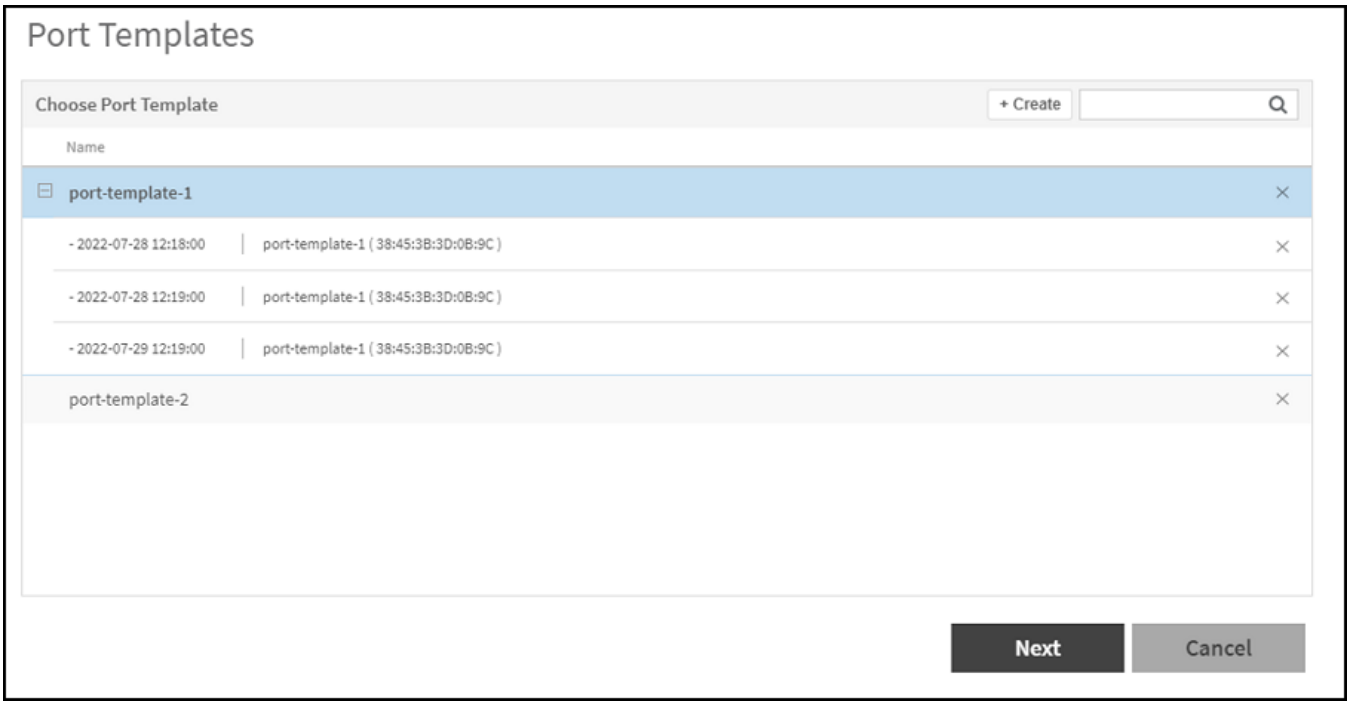


FIGURE 102 Clicking Ports Tab to Select target Ports


Traffic
Health
General
Configuration
Configuration Restore
Ports
R
Ports View
Port Details
Configure
Port Templates
Port Name
Port Number
Status
GigabitEthernet1/1/1 1/1/1 Down
GigabitEthernet1/1/2 1/1/2 Down
GigabitEthernet1/1/3 1/1/3 Down
GigabitEthernet1/1/4 1/1/4 Down
GigabitEthernet1/1/5 1/1/5 Down
GigabitEthernet1/1/6 1/1/6 Down
GigabitEthernet1/1/7 1/1/7 Down
GigabitEthernet1/1/8 1/1/8 Down
GigabitEthernet1/1/9 1/1/9 Down
GigabitEthernet1/1/10 1/1/10 Down
GigabitEthernet1/1/11 1/1/11 Down
GigabitEthernet1/1/12 1/1/12 Down

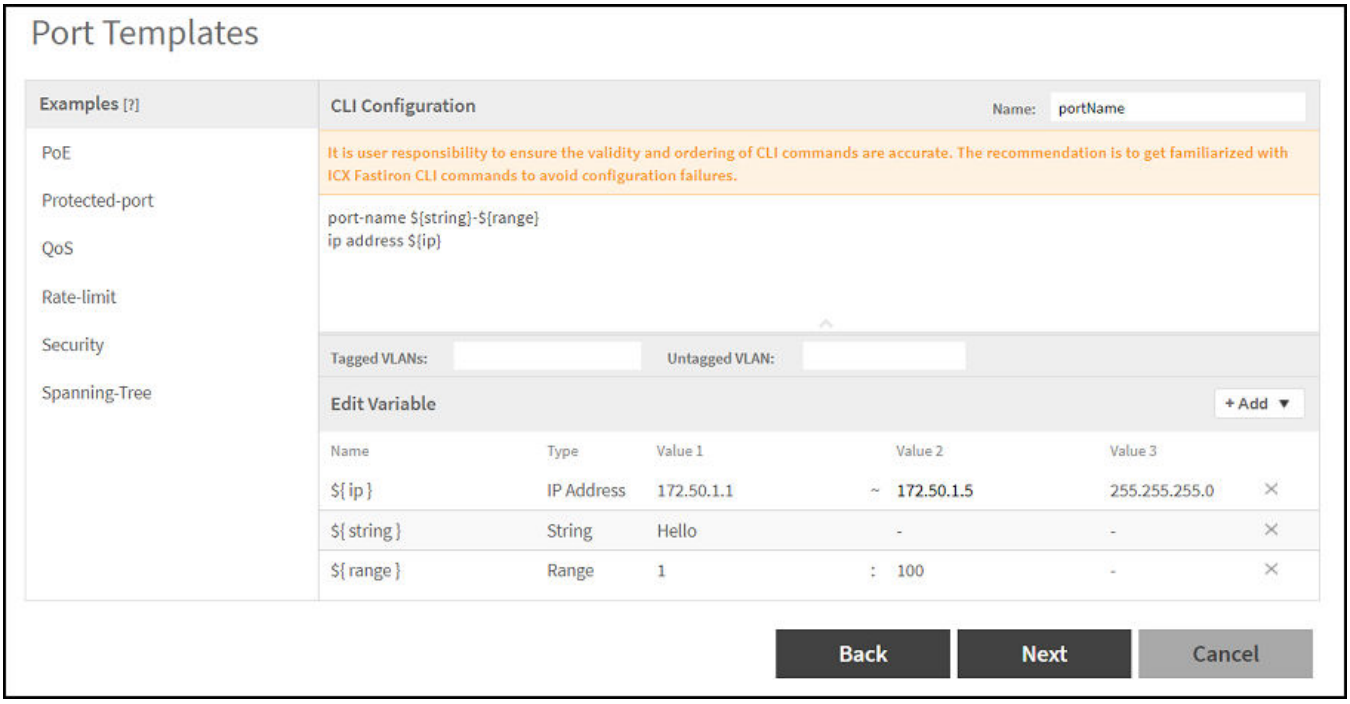
3. After selecting the target port, click **Port Template** tab. A **Port Template** page is displayed that lists the available port templates. Click **Create** to create a new port template, or expand "+" to view a list of scheduled port templates. Select an existing scheduled port template, and click **Next** to update the scheduled port template configurations. After selecting the target port template, click **Apply**.

FIGURE 103 Creating Port Template



4. After creating a port template or selecting an existing template, input the below parameters and click **Apply**. Click **Back** to view the previous page. Click **Cancel** to close the window.

FIGURE 104 Adding Parameters to Port Template



a) Enter the name of the port template in the **Name** field.

b) Variables helps to apply unique configuration to the switches. If you want to use variable in the CLI Configuration editor, it must start with a symbol “$” and a pair of curly braces {VARIABLE_NAME}. For example, IP address can be defined as a variable so that each switch gets assigned a unique IP address. In the **Edit Variable** field, enter the **Name**, **Type**, **Value 1**, **Value 2**, and **Value 3** for IP address variables, where Value1 denotes the “Starting IP Address”, Value 2 denotes the “Ending IP Address”, and Value 3 is the “Netmask".

c) In the **Tag** and **Untag VLAN** field, input the tag and untag VLAN for the port template.

d) The **CLI Configuration** field provides a text editor to input command types for the template, including the variables.

e) Click **Examples** to view the example command line references in the CLI Configuration editor.

5. Verify the details for the target ports, Port Template CLIs, Tag and Untag VLANs and the variables in the **Review** page . Click "+" on the left of **Review** page to add more ports to the list. You can also organize the port list by selecting a port and dragging it above or below . Click "x" to delete switch port from the list. Select **Apply Now** to apply the port template immediately. Select **Schedule Later** to apply the port template at the specified schedule time. After selecting either **Apply Now** or **Schedule Later**, click **OK**.

   The various operations that can be performed on the ports in the ports list are as shown below.

FIGURE 105 Adding Ports to the List

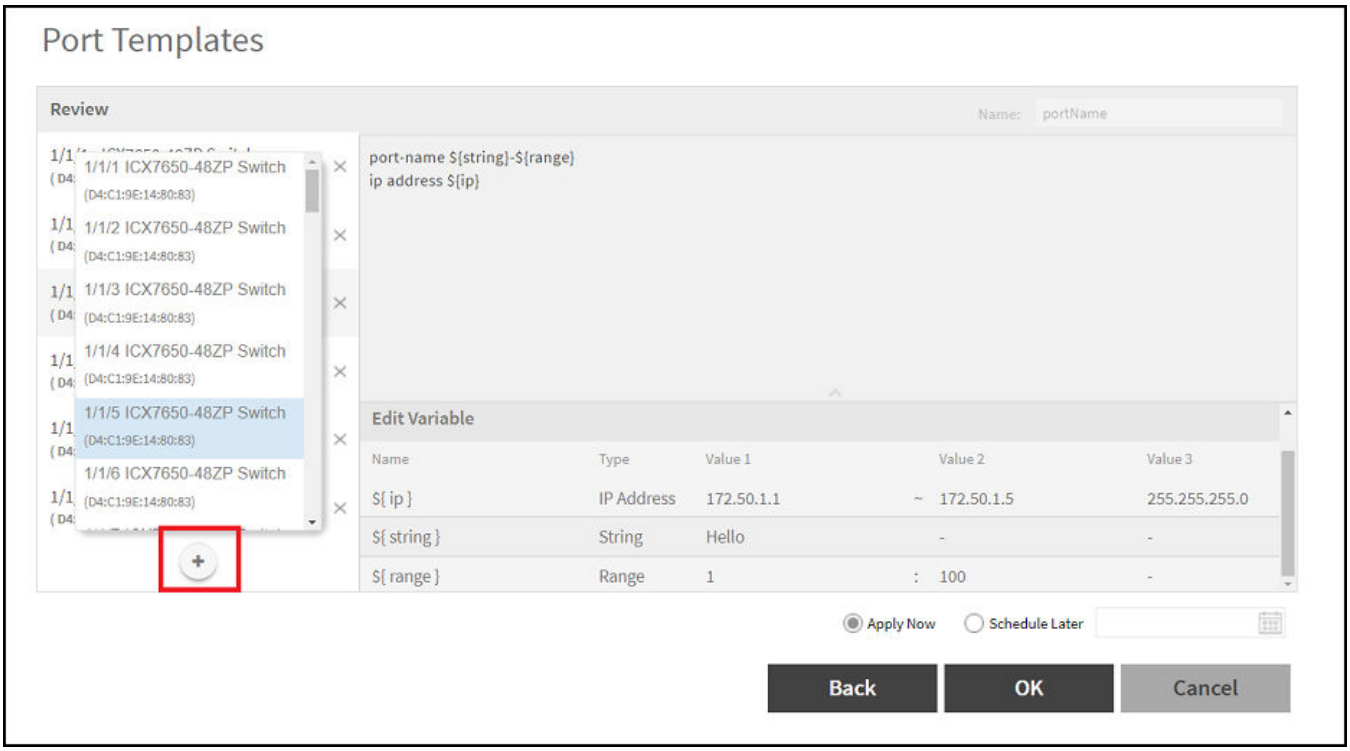


FIGURE 106 Organizing the Port List

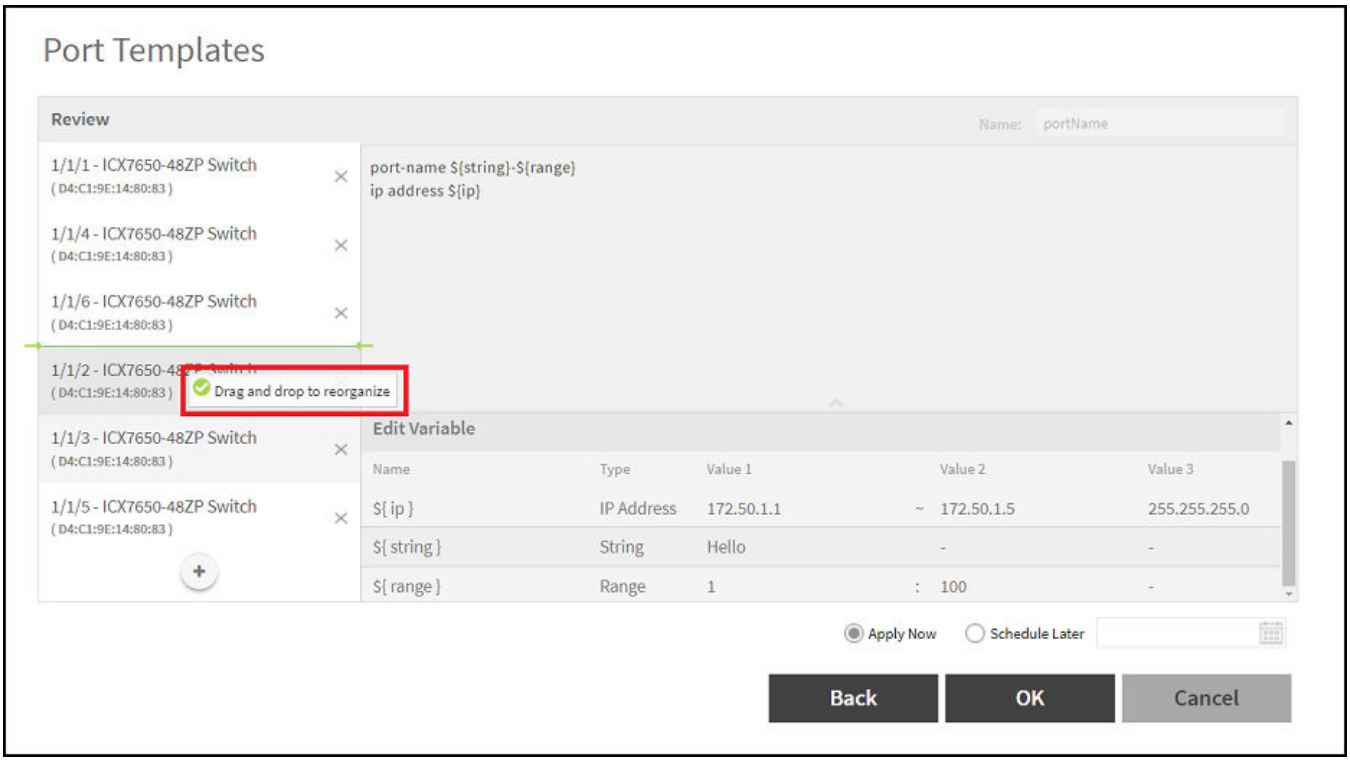
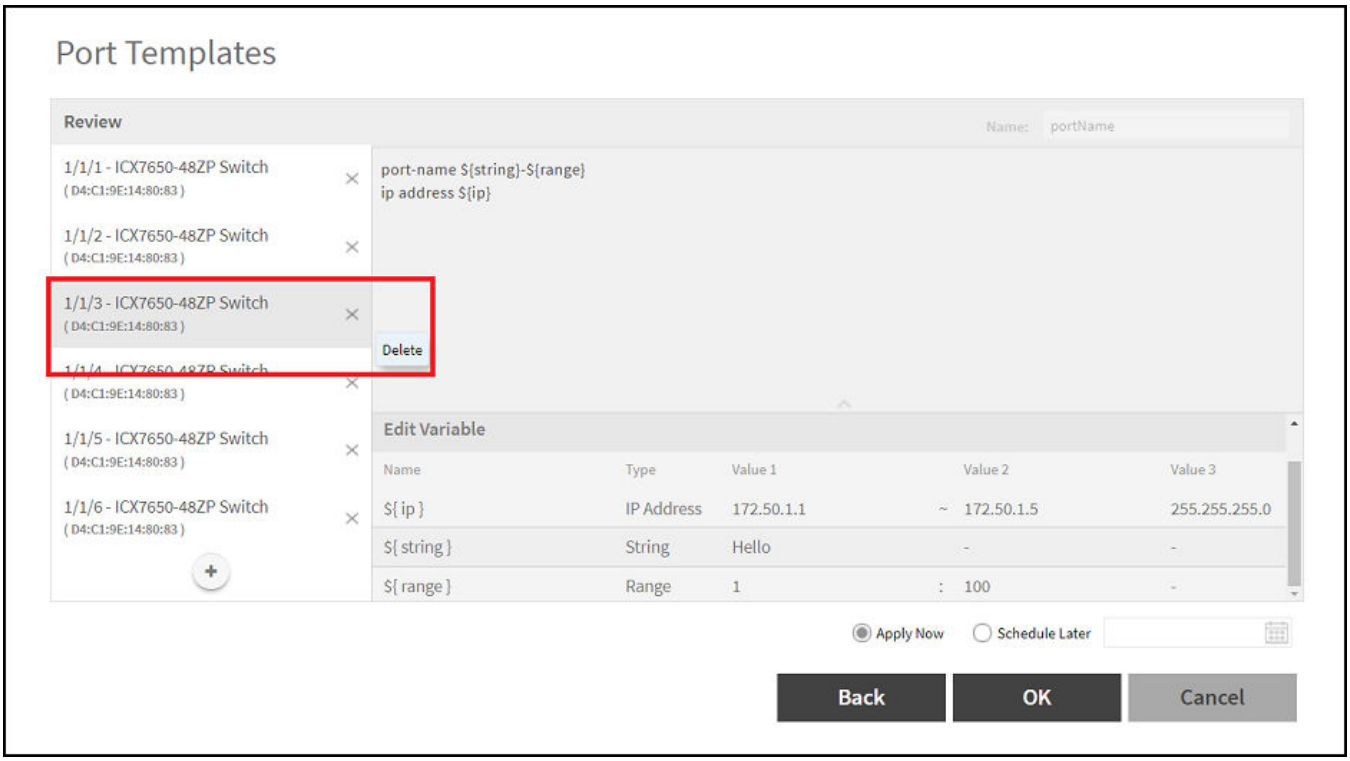


FIGURE 107 Deleting Port from the List



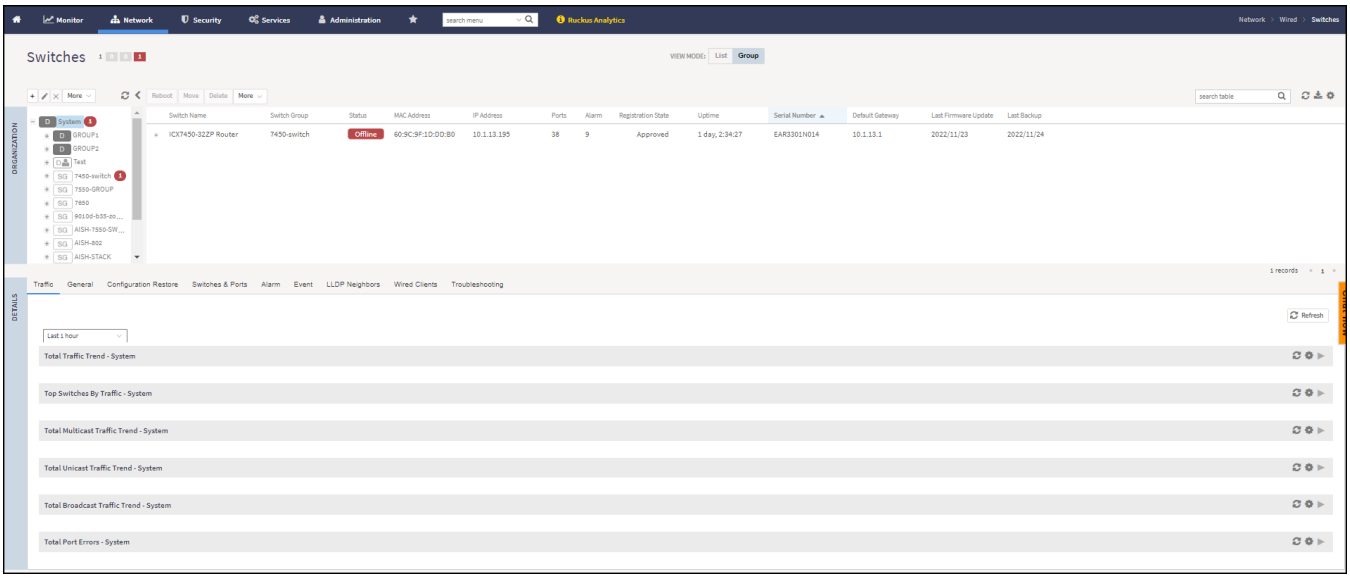
Configuring Port Settings for a Switch

Port settings enable you to configure ports for a switch, stack, or switch group. You can also invoke the ACL in port configuration for applying the Quality of Service (QoS) settings to proritize VOIP and VIDEO VLAN traffic.

NOTE
Port settings for QoS can only be configured for switches that are executing firmware version 08.0.95 and above.

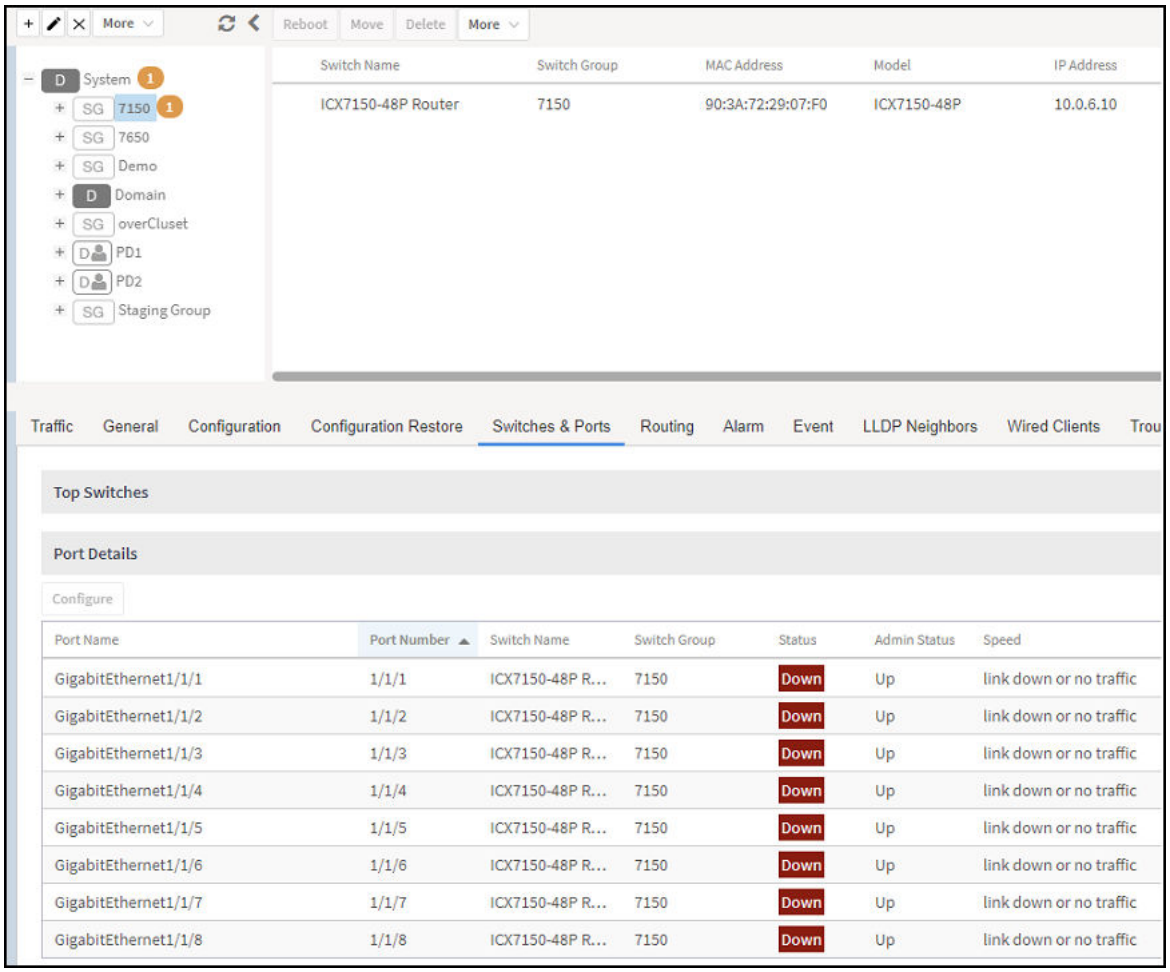
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 108 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and in the **Details** tab, click the **Switches and Ports** tab.

FIGURE 109 Switch Port Page



3. In the **Port Details** tab, select the port that must be updated and click **Configure** to display the **Port Settings** window.

FIGURE 110 Port Settings Showing Single Update

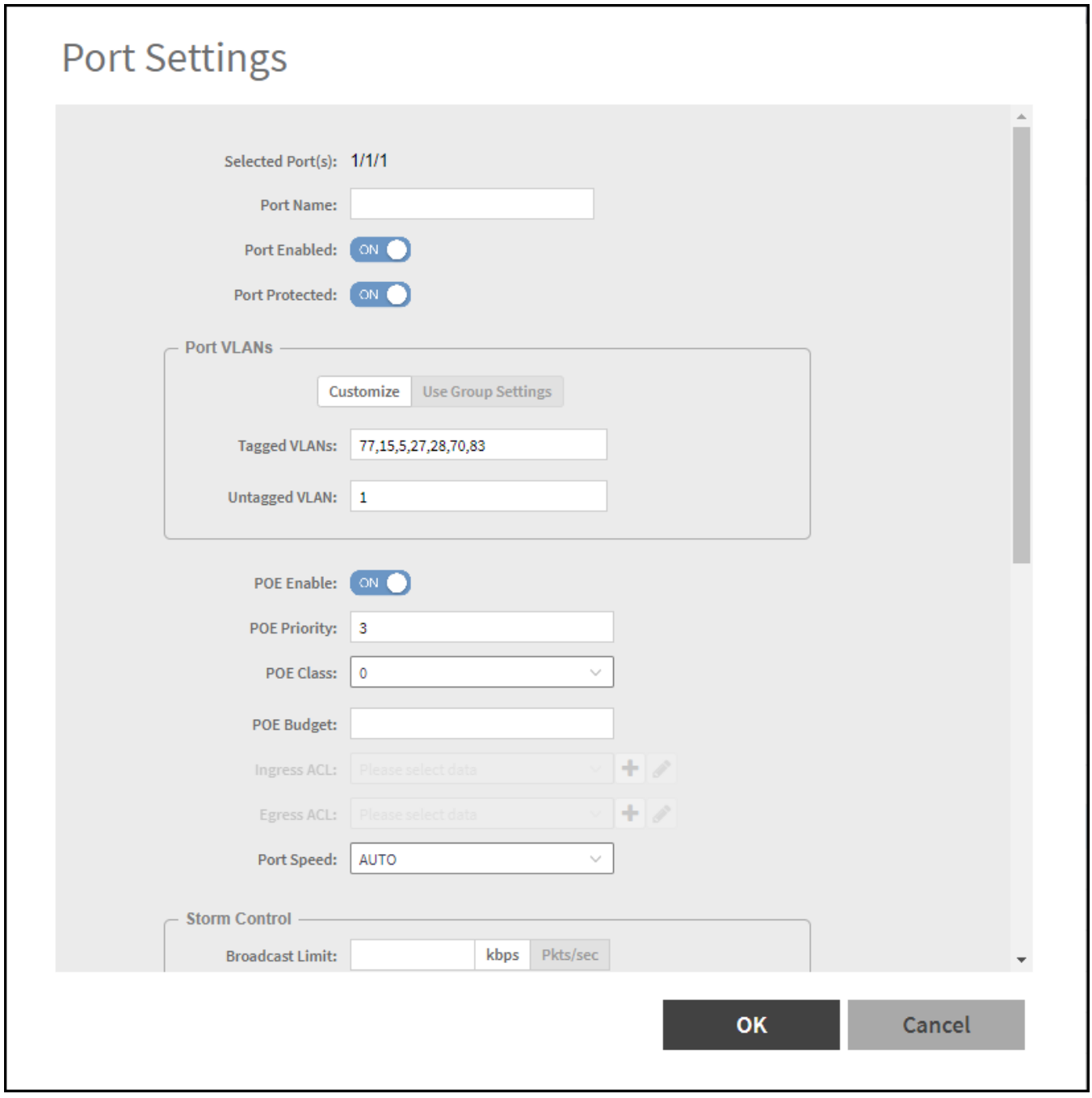


FIGURE 111 Poret Settings Showing Multiple Update

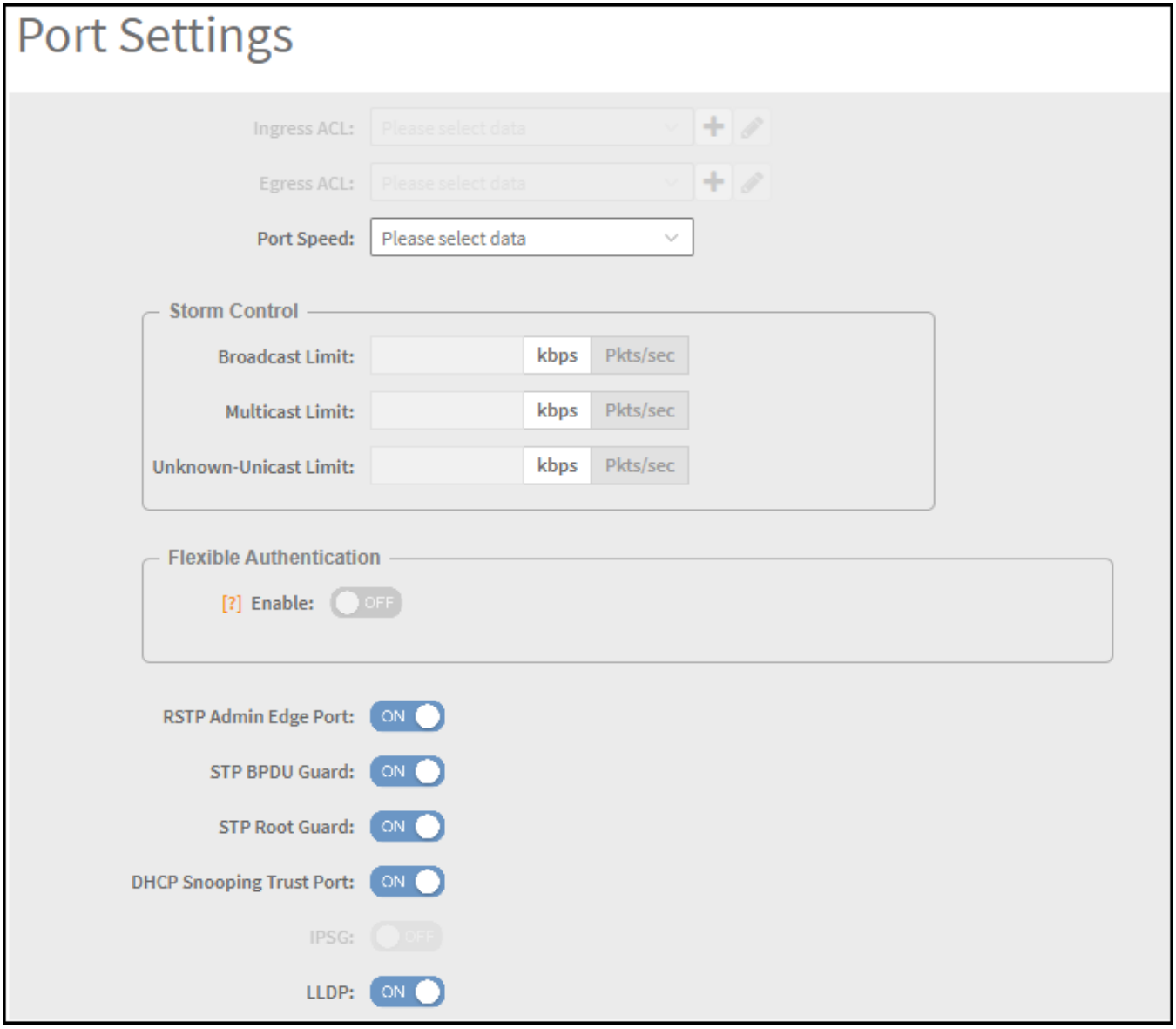
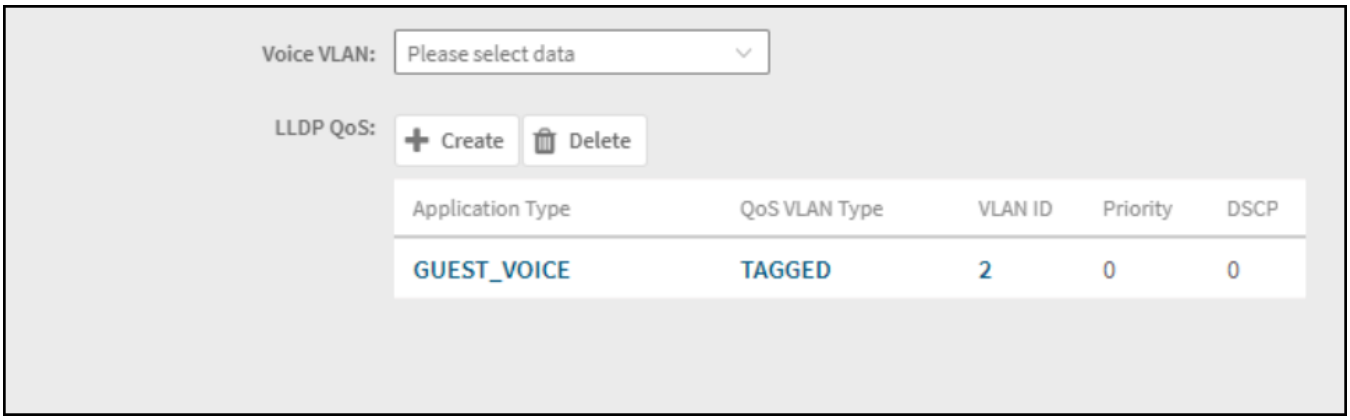


FIGURE 112 Port Settings for QoS


Voice VLAN:
Please select data
LLDP QoS:
Create
Delete
Application Type
QoS VLAN Type
VLAN ID
Priority
DSCP
GUEST_VOICE
TAGGED
2
0
0

4. Complete the following fields:
   - **Port Name**: Enter the port name.
   - **Port Enabled**: Click to enable the port.
   - **Port Protected**: Click to enable the protected port.

     NOTE
     Port Protected field is displayed only for the switches using SmartZone 5.2.1 and above.

   - **Port VLANs**: If you configure VLAN on both group model configuration and port settings, port level changes takes precedence.
   - **Customize**: Click customize to identify the ports that need to stay customized.
   - **Use Group Settings**: Click user group settings to rebind the identified ports back to the group level.
   - **Tagged VLANs**: Enter the tagged VLAN ID or VLAN ID range.
   - **Untagged VLAN**: Enter an untagged VLAN ID.
   - **POE Enable**: Click to enable PoE.
   - **POE Class**: Selecct the PoE class. You can configure the PoE budget on ports by setting the PoE class to 0 through 4.
   - **POE Priority**: Enter the PoE priority.
   - **POE Budget**: Allows users to manually set the PoE power limit.
   - **Ingress ACL**: Select the ingress ACL from the list.
   - **Egress ACL**: Select the egress ACL from the list.
   - **Port Speed**: Select the required Port Speed from the list.
   - **Storm Control**: If you set Storm Control configuration on a switch, and if this switch joins the controller, you must ensure that the Storm Control configuration on the controller is also set.The Storm Control includes the following fields - Broadcast, Multicast, and Unicast.

     NOTE
     The value 0 pkts/sec and 0 kbps indicates storm control is disabled.

   - **Broadcast Limit**: Enter the Broadcast Limit value in this field. The maximum value in **Pkts/sec** is 8388607 and the minimum value is 1; when the port speed is set to **Auto** or **Optic**, the maximum value in **kbps** is 1000000 and the minimum value is 1; when the port speed is other than auto or optic the minimum value in **kbps** is 1 and the maximum value is equivalent to the selected port speed .
   - **Multicast Limit**: Enter the Multicast Limit value in this field. The maximum value in **Pkts/sec** is 8388607 and the minimum value is 1; when the port speed is set to **Auto** or **Optic**, the maximum value in **kbps** is 1000000 and the minimum value is 1; when the port speed is other than auto or optic the minimum value in **kbps** is 1 and the maximum value is equivalent to the selected port speed .
   - **Unicast Limit**: Enter the Unicast Limit value in this field. The maximum value in **Pkts/sec** is 8388607 and the minimum value is 1; when the port speed is set to **Auto** or **Optic**, the maximum value in **kbps** is 1000000 and the minimum value is 1; when the port speed is other than auto or optic the minimum value in **kbps** is 1 and the maximum value is equivalent to the selected port speed .
   - **RSTP Admin Edge Port**: Click to enable the RSTP Admin Edge Port.
   - **STP BPDU Guard**: Click to enable the STP BPDU Guard.
   - **STP Root Guard**: Click to enable the STP Root Guard.
   - **DHCP Snooping Trust Port**: Click to enable the DHCP Snooping Trust Port.
   - **IPSG**: Click to enable IPSG.
   - **ILLDP**: Click to enable ILLDP.
   - **Voice VLAN**: Select the VLAN (tagged or untagged).
   - **LLDP QoS**: Click to enable LLDP-MED settings.

- **Application type**: Enter one of the application types : **Guest_Voice**, **Guest_Voice_Signaling**, **Softphone_Voice**, **Streaming_Video**, **Video_Conferencing**, **Video_Signaling**, **Voice**, and **Voice_Signaling**.
- **VLAN type**: The VLAN type can be priority-tagged, tagged, or untagged.
- **VLAN ID**: Enter the **VLAN ID** of the VLAN type.
- **Priority**: Enter the priority for the QoS setting.
- **DSCP**: Enter the DSCP value for the LLDP setting.

5. Click **OK**.

VIDEO
PoE per port settings. The below video displays the tasks to be performed to configure PoE on a port.
Click to play video in full screen mode.

Editing Ports Across Multiple Switches

Before 5.2.1 release, the user could edit multiple ports for an individual switch. But after 5.2.1 release, the controller allows the user to edit the ports across multiple switches within the same Switch Group.

For example, if you want to disable port 1/1/11 and 1/1/12 across multiple switches, the controller provides an option to filter the ports list by typing the search criteria.

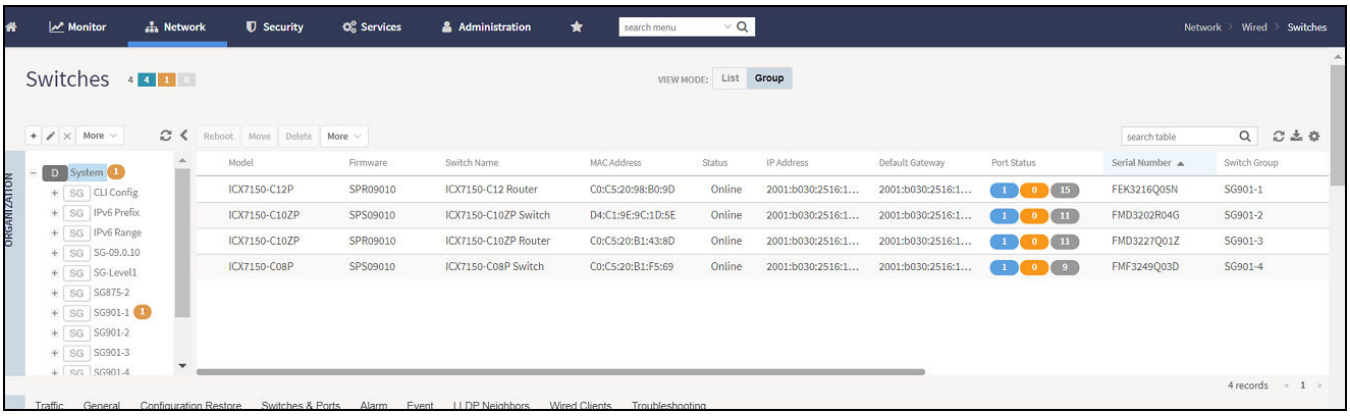
The search criteria is based on the following.

- Switch Name
- Port numbers - comma separated values (1/1/1,1/1/11,1/1/24), (or) Range of ports (1/1/1 to 1/1/20)
- VLAN membership
- PoE detected ports
- Port Status
- Admin Status

You must complete the following steps to edit ports across multiple switches.

1. On the menu, click **Network** > **Wired** > **Switches** to disaply the **Switches** window.

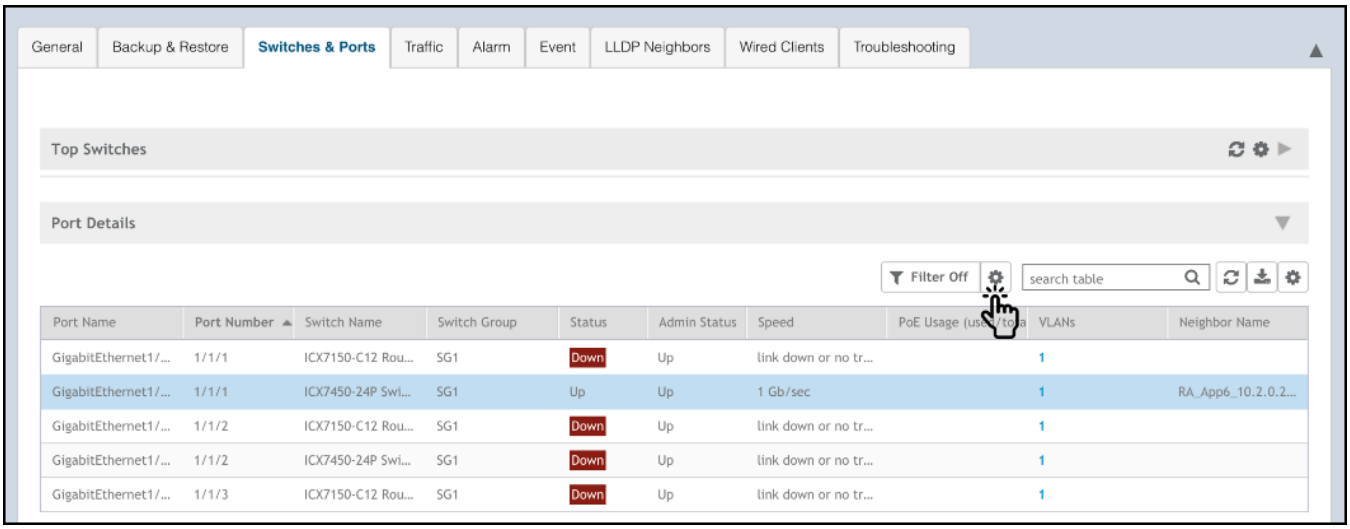
FIGURE 113 Switches Page



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group**.

3. In the **Details** tab, click **Switches and Ports** tab.

FIGURE 114 Viewing the Switches and Ports Page

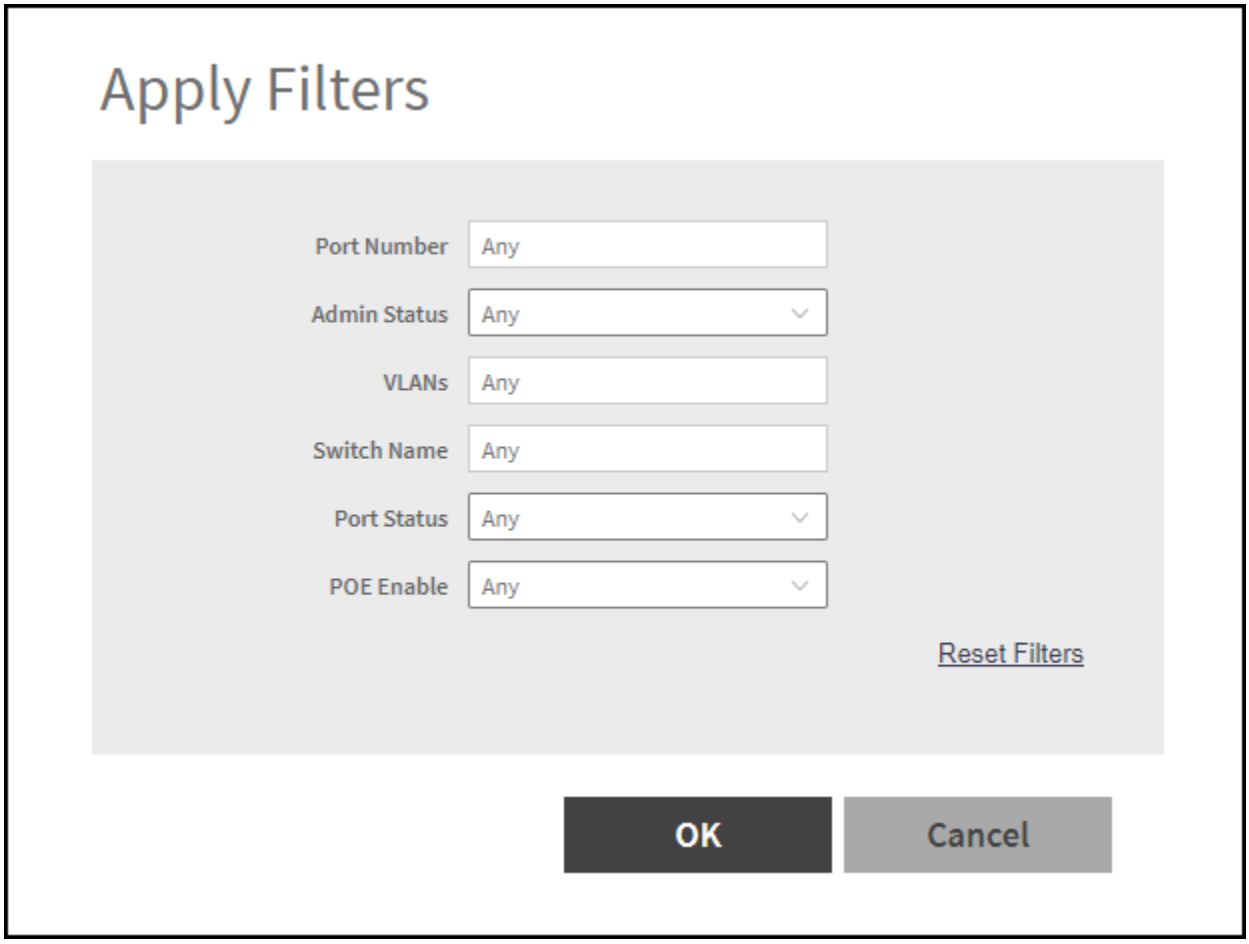


4. In the **Port Details** tab, click the icon.

   A dialogue box is displayed. The controller provides the following filters to combine several query conditions to filter-out the ports which you want to edit.

   NOTE
   Click **Reset Filters** to clear the search conditions.

   FIGURE 115 Applying Filter to Edit the Ports



5. Click **OK**.

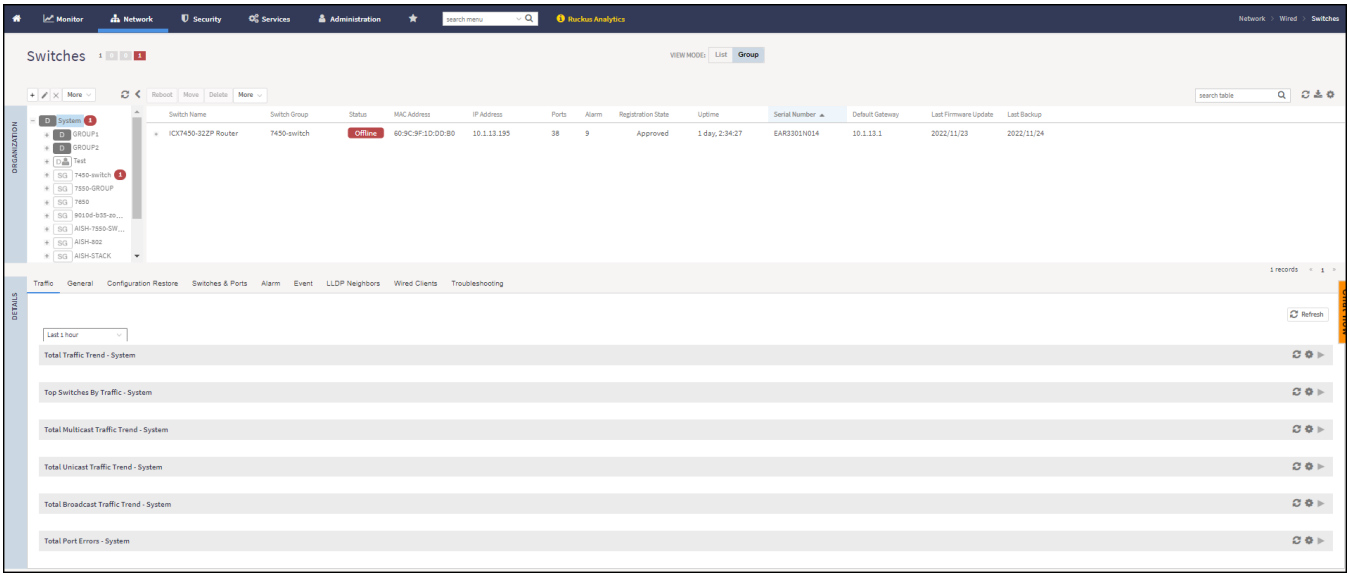
   The controller applies the above filters to return ports that meet the search criteria.

Creating Routing Configurations

You can create, edit, and delete routing configurations for an switch.

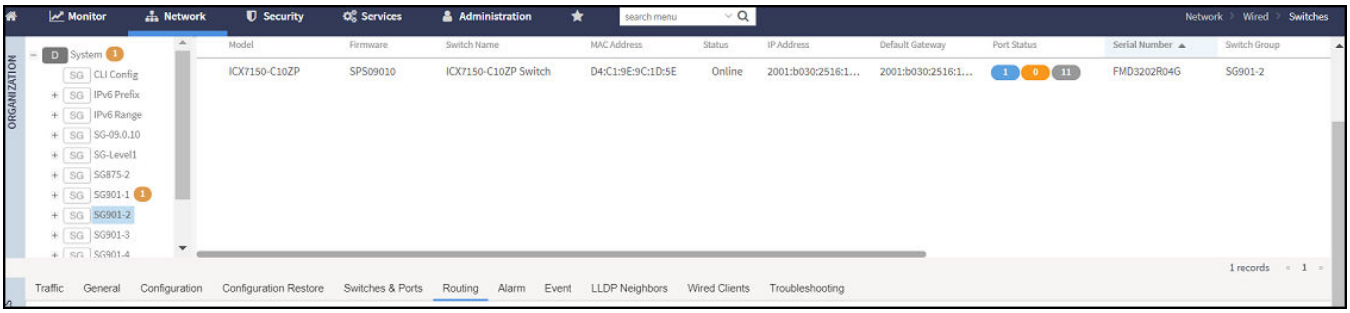
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 116 Switches



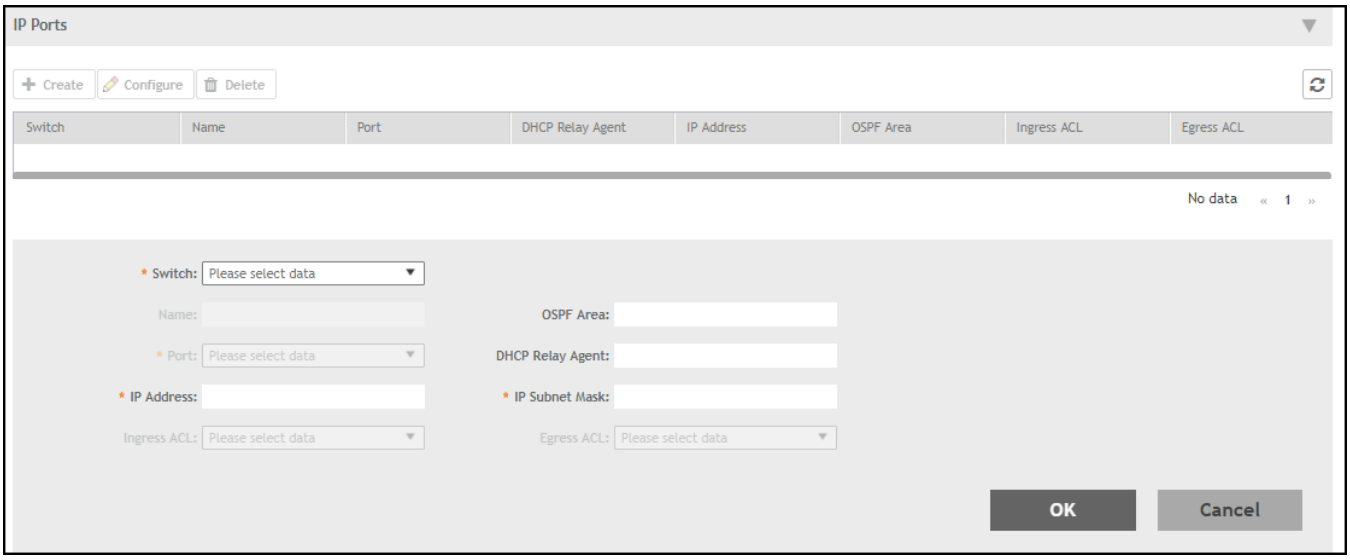
2. In the **Organization** tab, select the **Domain** > **Switch Group** or **Switch Group** and in the **Details** tab, click **Routing** tab.

FIGURE 117 Switch Routing Tab



3. In the **IP Ports** tab, click Create icon to display the **IP Ports** tab.

FIGURE 118 IP Ports Page



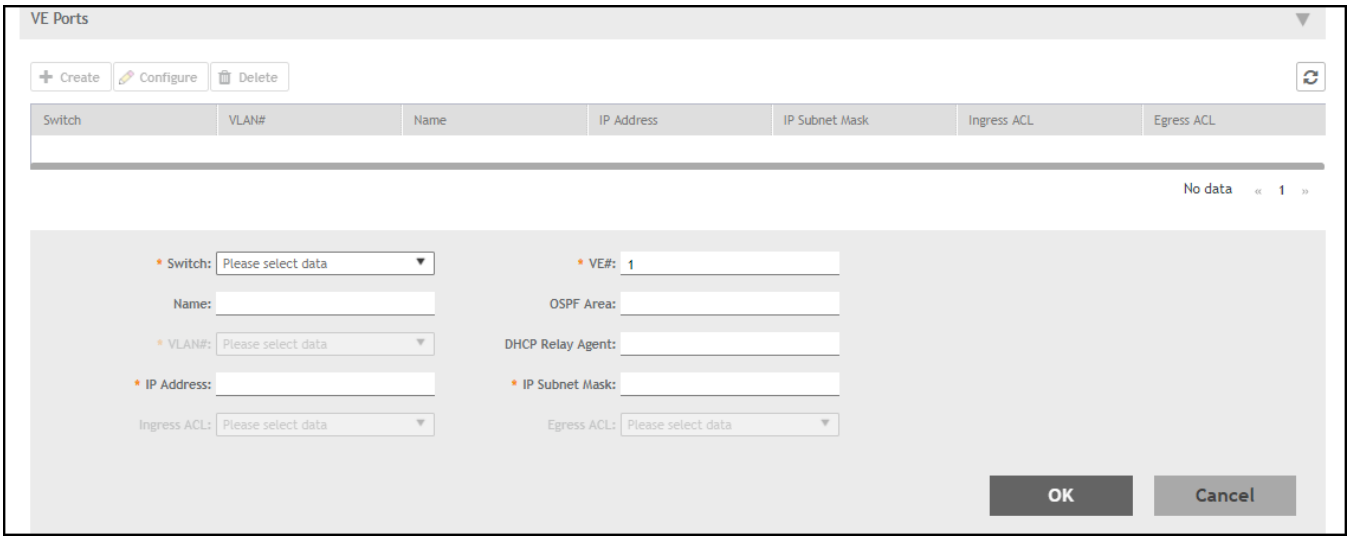
Complete the following fields:

- **Switch**: Select the switch from the drop down list.
- **Name**: Enter a name.
- **OSPF Area**: Enter the OSPF area IPv4 address.
- **Port**: Select the port number from the list.
- **DHCP Relay Agent**: Enter the DHCP relay agent IP address.
- **IP Address**: Enter a unicast IP address.
- **IP Subnet Mask**: Enter an IP subnet mask.
- **Ingress ACL**: Select the ACL for the ingress network interface.
- **Egress ACL**: Select the ACL for the egress network interface.

4. Click **OK**.

5. In the **VE Ports** tab, click Create icon to display the **VE Ports** tab.

FIGURE 119 VE Ports Page



Complete the following fields:

- **Switch**: Select the switch from the list.
- **VE#**: Enter the VE number. Range: 1 through 4095.
- **Name**: Enter a name.
- **OSPF Area**: Enter the OSPF area IPv4 address.
- **VLAN#**: Select the VLAN from the list.
- **DHCP Relay Agent**: Enter the DHCP relay agent IP address.
- **IP Address**: Enter a unicast IP address.
- **IP Subnet Mask**: Enter an IP subnet mask.
- **Ingress ACL**: Select the ACL for the ingress network interface.
- **Egress ACL**: Select the ACL for the egress network interface.

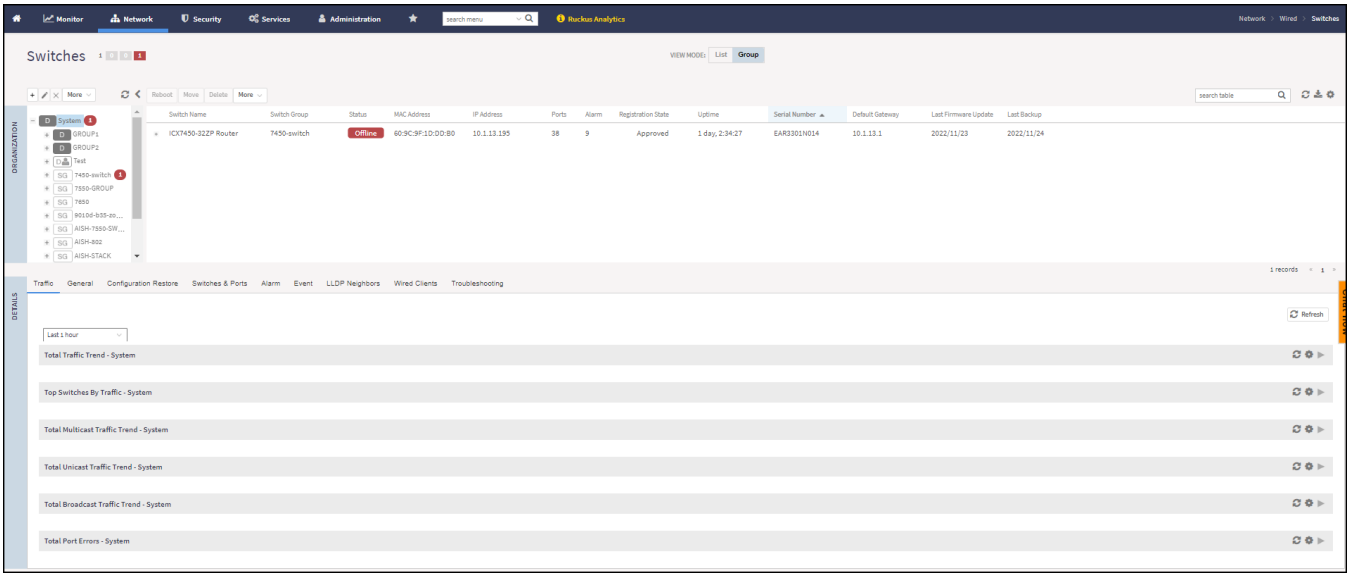
6. Click **OK**.

Managing Link Aggregation Groups (LAGs)

Controller provides an option to define LAGs at an individual switch level.

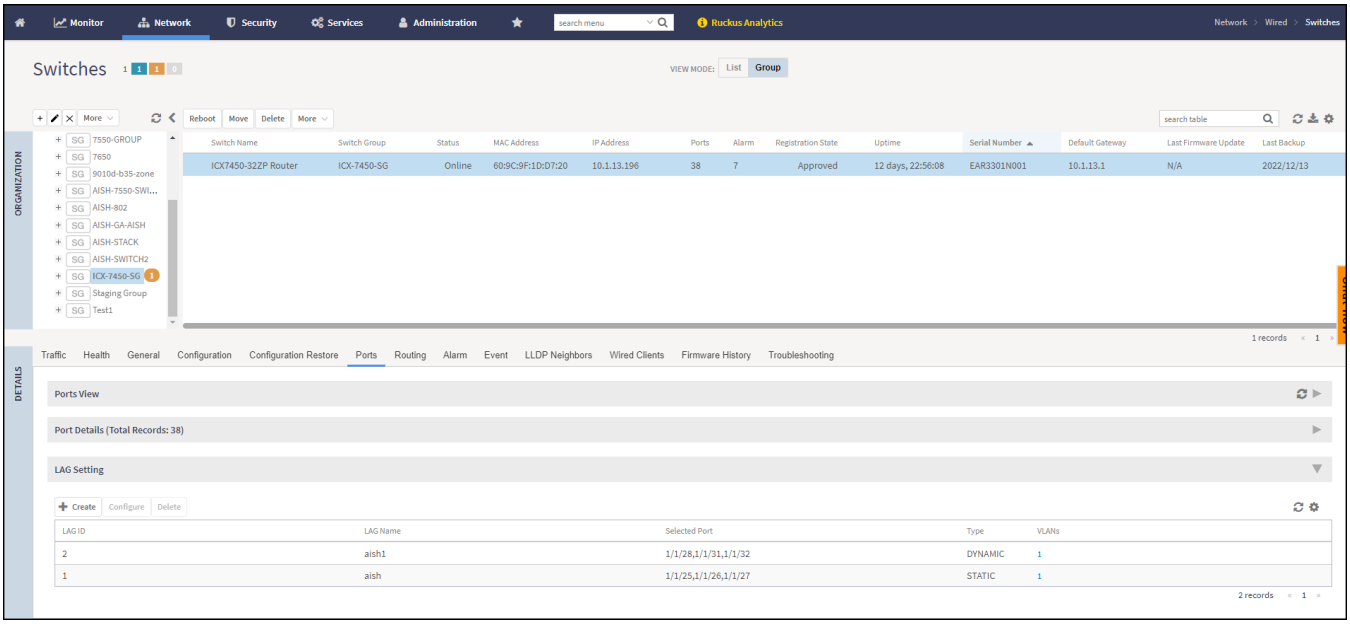
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 120 Switches



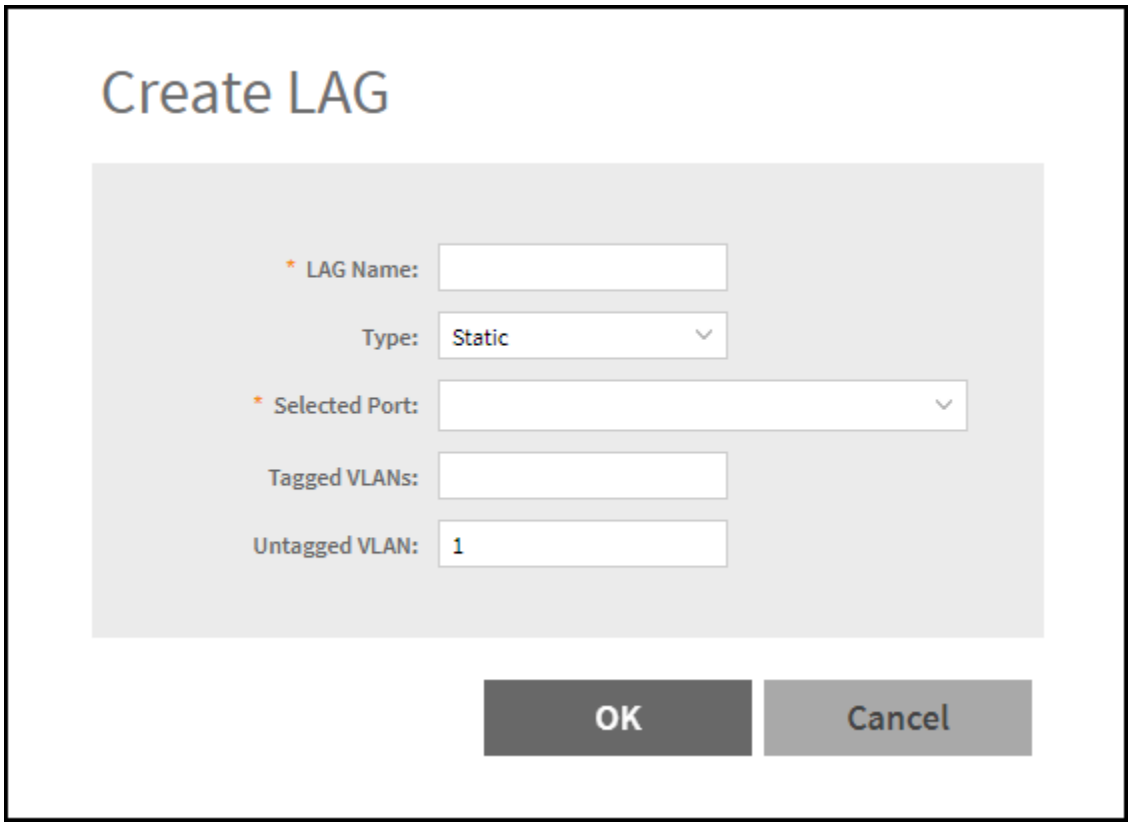
2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**.
3. In the **Details** tab, click **Ports** tab.

FIGURE 121 Ports



4. In the **LAG Setting** tab, click + Create icon to display the **Create LAG** dialog box.

FIGURE 122 Create LAG



5. Complete the following fields:
   - **LAG Name**: Enter a name.
   - **Type**: Select either **Static** or **Dynamic** from the list.
   - **Selected Port**: You can select multiple port numbers from the list.
   - **Tagged VLANs**: Enter the tagged VLAN ID or VLAN ID range.
   - **Untagged VLANs**: Enter an untagged VLAN ID.
6. Click **OK**.

Creating a Switch Stack

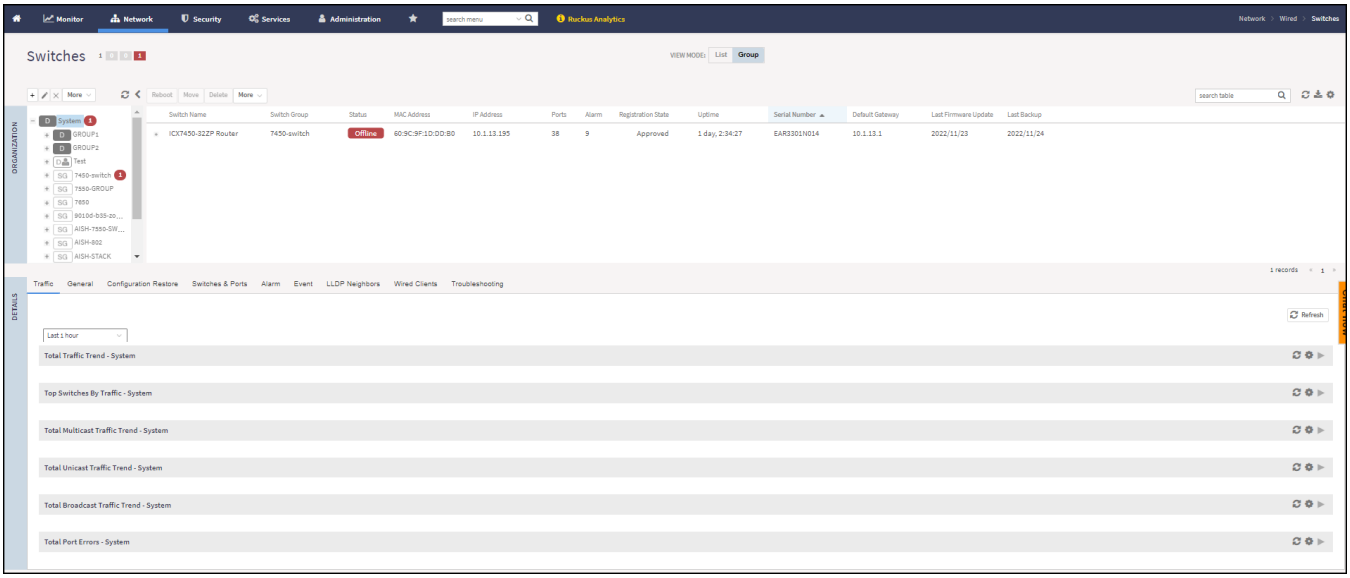
You can create a stack by selecting individual switches that are connected to the controller.

As a pre-requisite, you must configure switch stacking from controller before connecting the switch cables.

Complete the following steps to create a stack of switches.

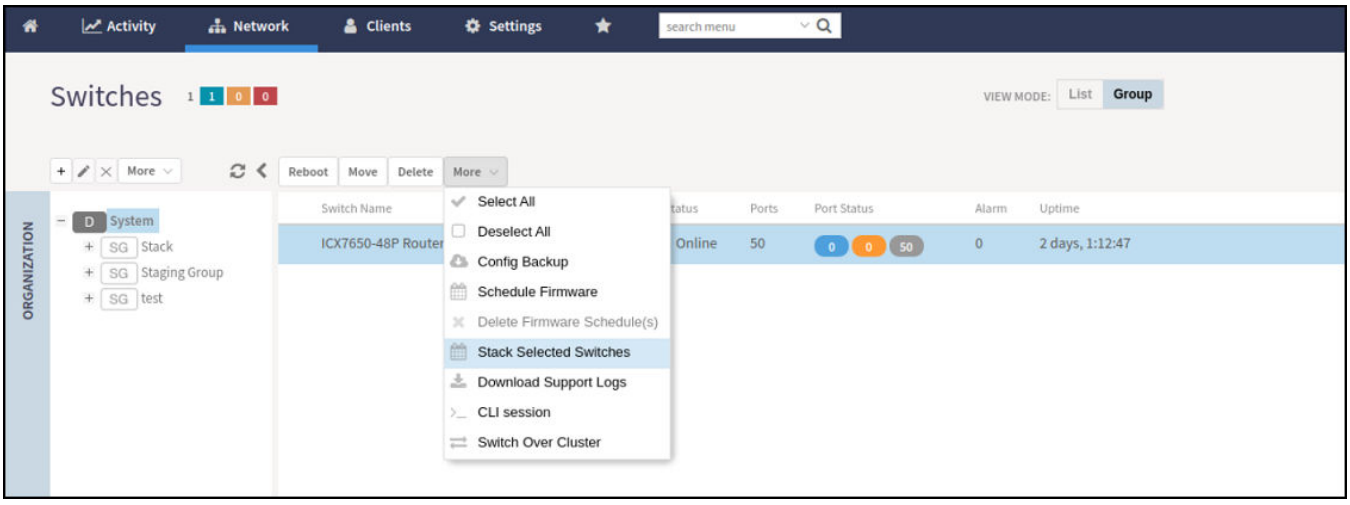
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

   FIGURE 123 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch** that are to be stacked. Click **More** > **Stack Selected Switches** to display **Create Stack** dialog box.

   FIGURE 124 Creating a Stack



3. Switch **ON** the **Active Role** and click **OK** to create the stack. After 15 minutes switches form stack as seen in the next step.
4. In the **Organization** tab, click **Domain** > **Switch Group** or **Switch Group** and select the stacked **Switch**.

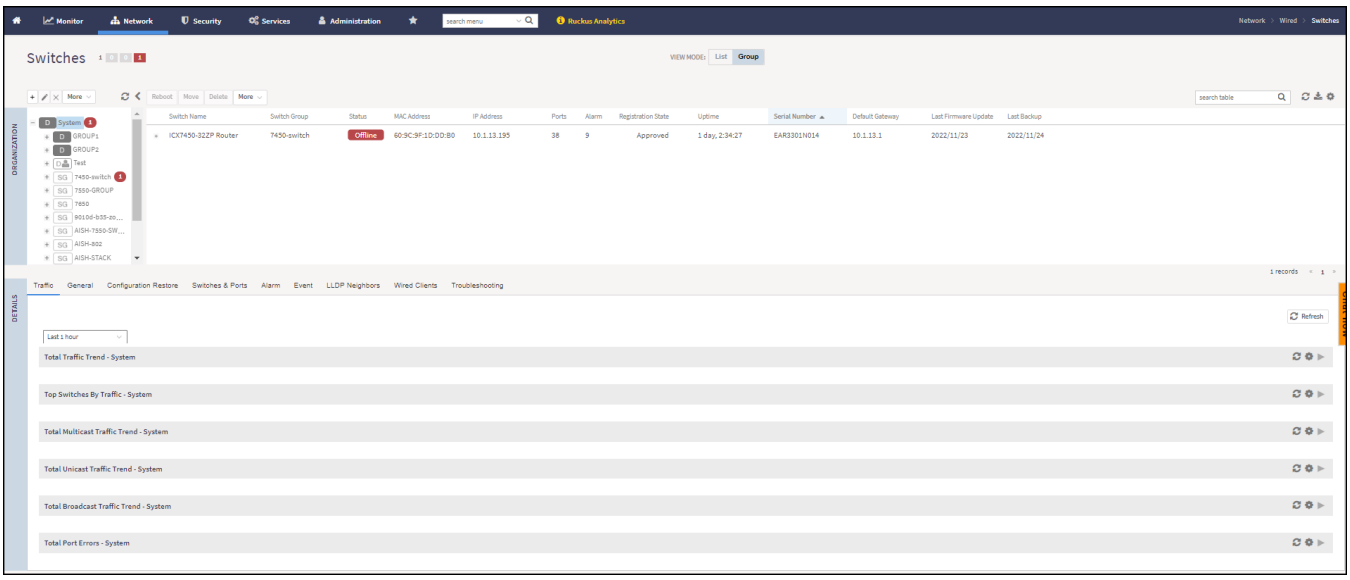
Viewing Port Details

Details on port use are available for individual switches, stacks, and switch groups.

Perform these steps to display information on ports for a switch, stack, or switch group.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

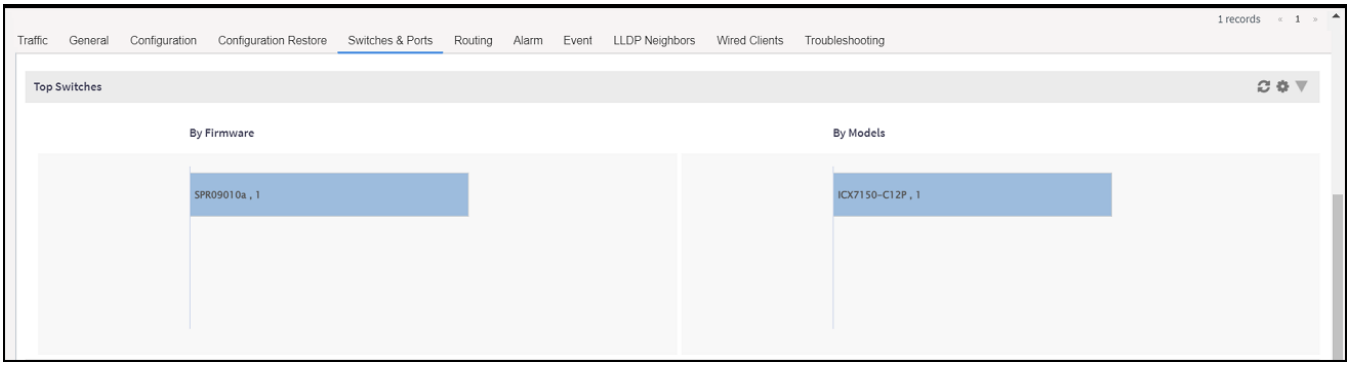
   FIGURE 125 Switches



2. In the **Organization** tab, select the **Domain** > **Switch Group** or **Switch Group** and in the **Details** tab, click **Switches and Ports** tab.

   For a switch group, a **Top Switches** tab similar to the following figure is displayed. The graphs provide information on top switches based on firmware and model.

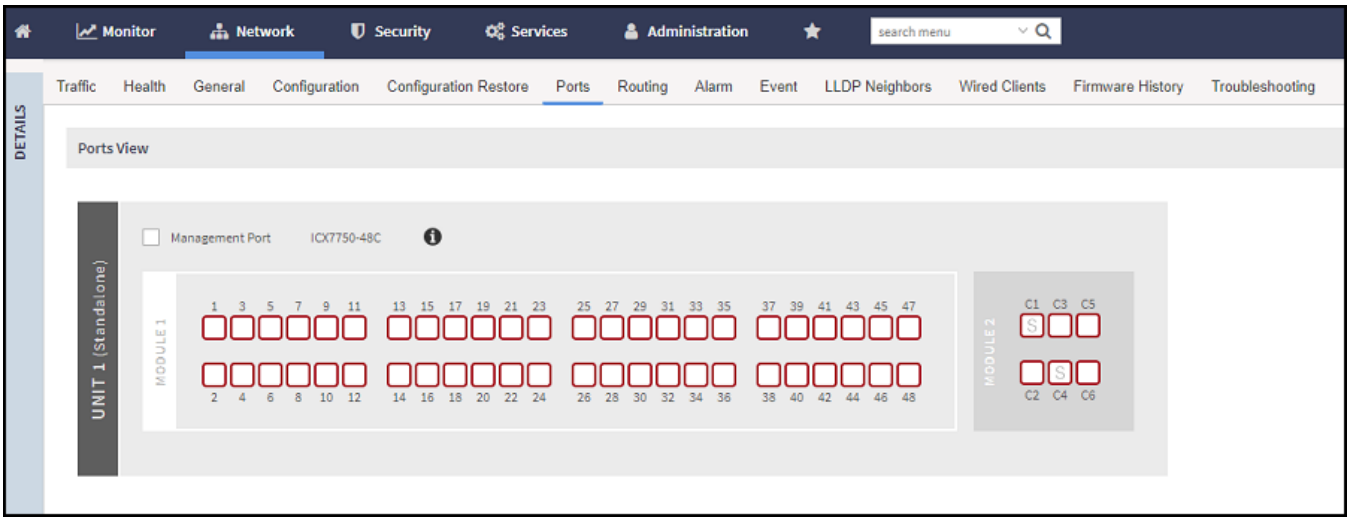
   FIGURE 126 Top Switches Page



3. In the **Switch Group**, select the **Switch** and click **Ports** tab to view the **Front Panel View** in the **Ports View** tab for additional port information as shown in the following figure.

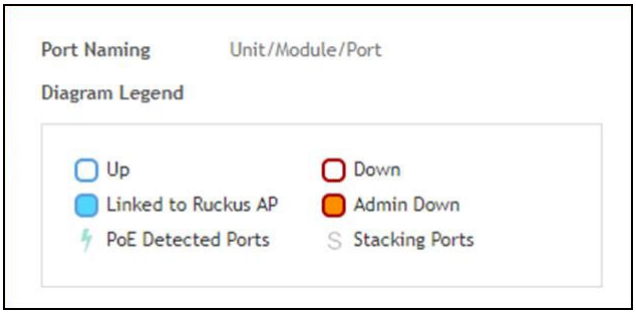
   The **Front Panel View** provides information on the state of all ports in each switch module, for example port Up, Down, or Administratively Down. Additional port details can be seen by hovering the mouse over the port.

FIGURE 127 Front Panel View



The following figure shows the diagram legend used in the Front Panel View page.

FIGURE 128 Diagram Legend



The following list further describes items in the Front Panel View legend.

- Up: Ports that are up or active.
- Warning: Ports that have packet errors.
- Down: Ports that are down or inactive.
- Linked to Ruckus AP: Ports that are linked to RUCKUS AP.
- Admin Down: Ports that have been manually disabled by the network administrator.
- PoE Detected Ports: Ports that are PoE detected.
- Stacking Ports: Ports that are stacked.

4. Click the switch name to view the **Port Details** page as shown in the following figure.

FIGURE 129 Port Details



The **Port Details** page provides the following information on each port:

> **NOTE**
> Ports for switch stacks are not configurable from the **Port Details** page.

- **Port Name**: The port name
- **Port Number**: The port number
- **Status**: Whether the port is operationally up or down
- **Admin Status**: Whether the port has been set to Up or Down by the network administrator
- **Speed**: The speed of the port
- **PoE Device Type**: Inline power device type, such as 802.3af, 802.3at, or Legacy device
- **PoE Usage (used/total watts)**: The PoE power usage compared to the allocated power
- **VLANs**: The VLANs to which the port is connected
- **Bandwidth IN (%)**: The bandwidth utilization for incoming traffic
- **Bandwidth OUT (%)**: The bandwidth utilization of the port for outgoing traffic
- **LAG Name (Type)**: The name of the Link Aggregation Group (LAG)
- **Optics**: The type of optic
- **Neighbor Name**: When LLDP is enabled, the name of the neighboring device, such as an AP or another switch or router
- **Incoming Multicast Packets**: The total number of incoming multicast data packets
- **Outgoing Multicast Packets**: The total number of outgoing multicast data packets
- **Incoming Broadcast Packets**: The total number of incoming broadcast data packets
- **Outgoing Broadcast Packets**: The total number of outgoing broadcast data packets
- **In Errors**: The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol
- **Out Errors**: The number of outbound packets that could not be transmitted because of errors
- **CRC Errors**: Indicates that the checksum calculated does not match between the data sender side and the received side. A CRC error usually indicates network transmission problems.
- **In Discard**: The number of inbound packets that were chosen to be discarded (even though no errors are detected) to prevent their being deliverable to a higher-layer protocol. One reason for discarding such a packet could be to free up buffer space.
- **Switch Name**: The name of the switch connected to the port
- **Switch Group**: The name of the switch group connected to the port

You can also filter the list of ports by the VLANs associated with them. Click  to set the filters.

> **NOTE**
> In this release only forming a LAG through the controller web user interface is supported. The system does not support configuring LAG interface detail through the controller web user interface. To configure detail settings for LAG after form it, you need to configure it through Switch console directly.

VIDEO
PoE Ports View. View PoE Information from SmartZone.
Click to play video in full screen mode.

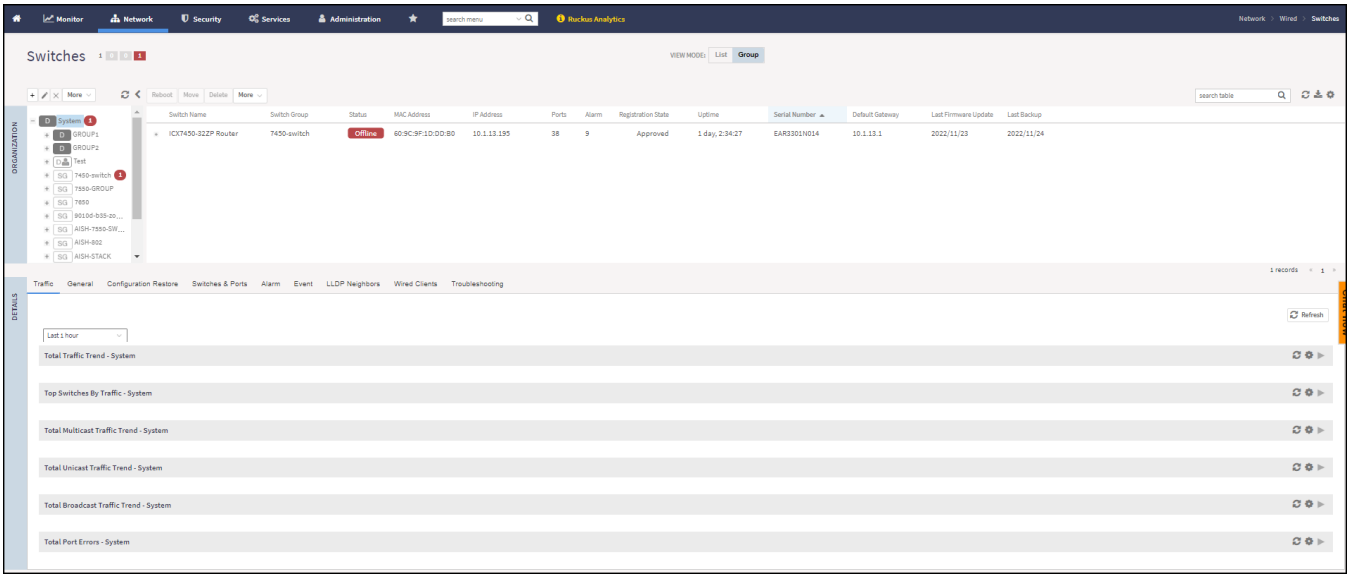
Viewing Switch Health

Health information displayed for a switch is based on memory usage and CPU usage statistics.

To view information on the health of a switch or the active controller of a stack, perform the following steps.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

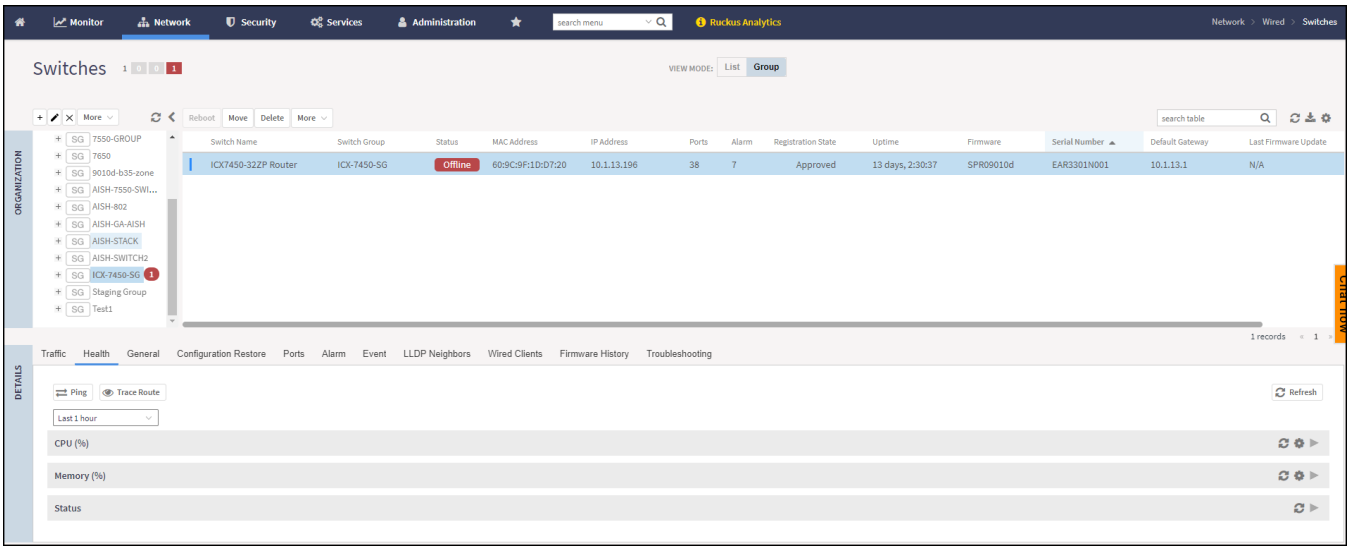
FIGURE 130 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**.

3. In the **Details** tab, click **Health** tab.

FIGURE 131 Health

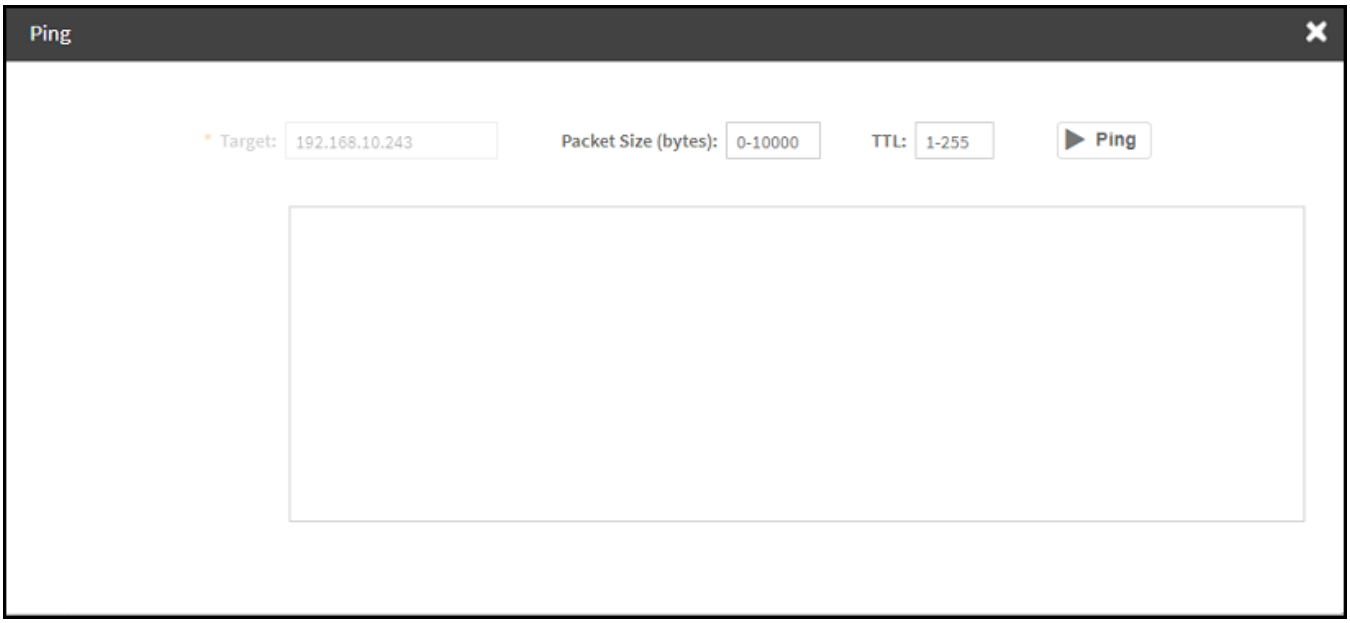


4. Click 

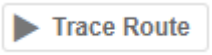
icon to display the **Ping** dialog box.

5. In the **Ping** dialog box, enter the IP address of the target switch, packet size, and TTL (Time to Live) value. Click Ping icon. In the below display window you can view that a packet is discarded from the network. As shown in the following example, after the ping, the page displays the number of data packets transmitted, received, and lost and the time required following the ping from the controller to the switch to establish communication.

FIGURE 132 Pinging the switch



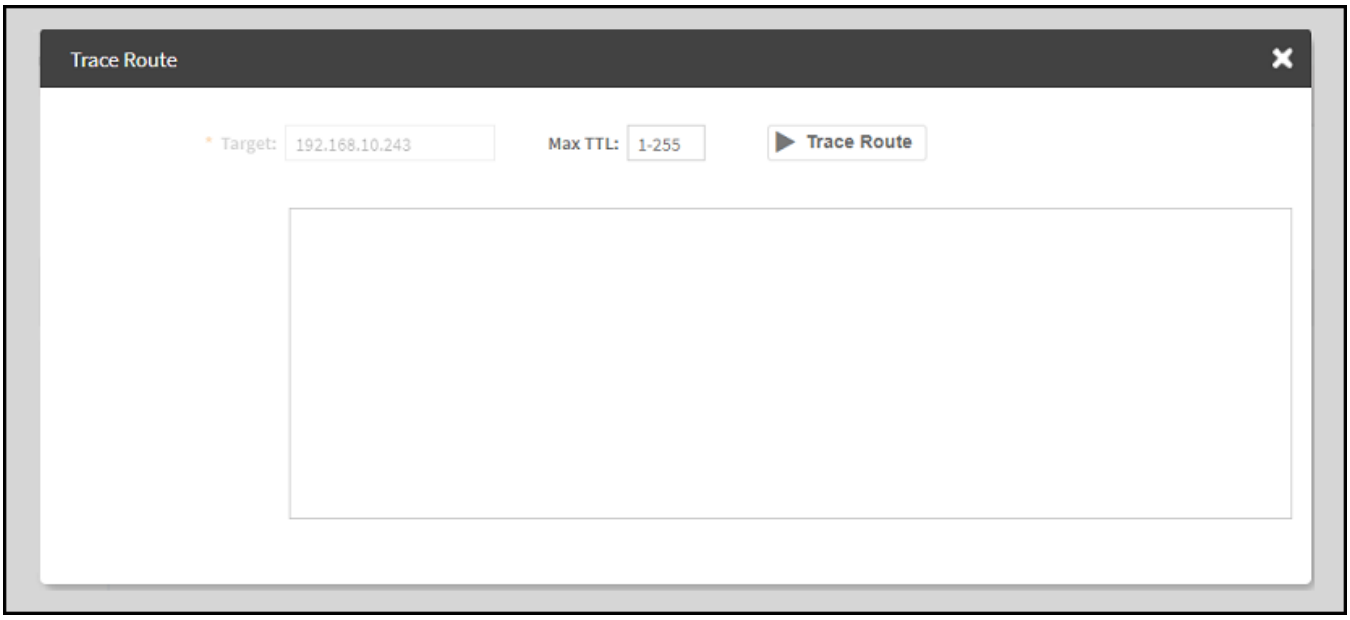
6. Click Trace Route icon to display the **Trace Route** dialog box.

7. On the **Trace Route** dialog box, enter the TTL (Time to Live) value. Click 

icon. In the below display window you can view that a packet is discarded from the network.

   As shown in the following example, the page displays the IP address of the hops the packet takes as it traverses the network between the switch and the controller.

   FIGURE 133 Tracing the packet route through the network

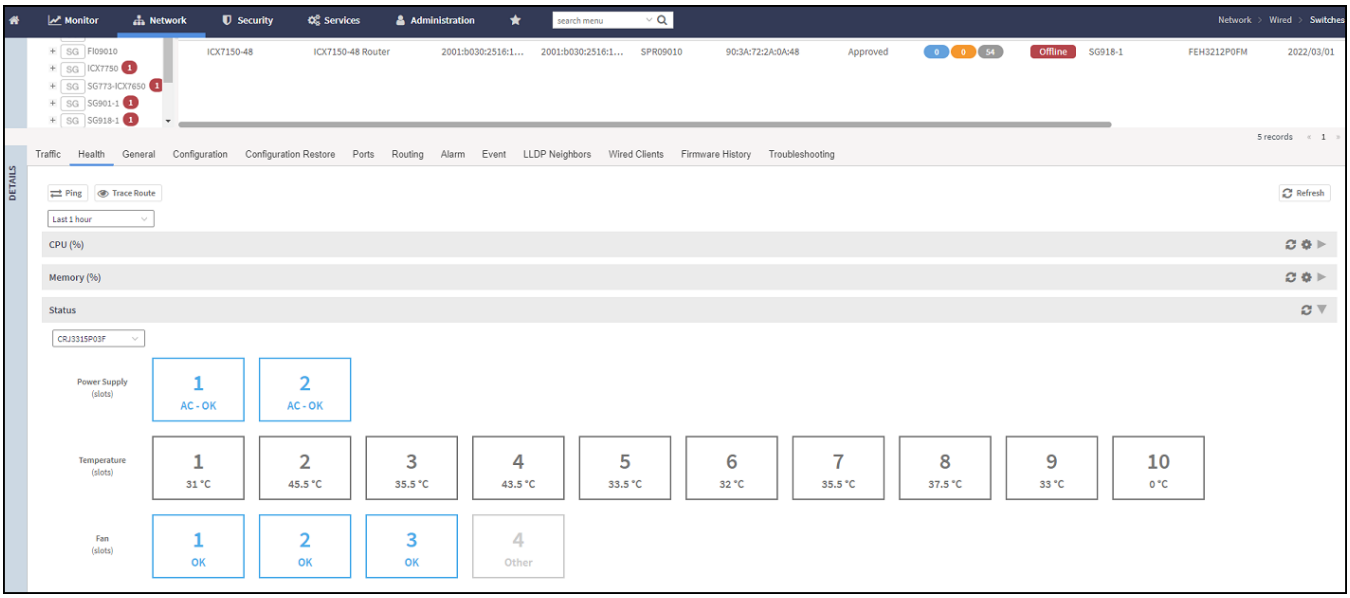


8. In the **Health** tab, from the drop-down menu 

select the duration for which you want to view the switch health.

   As shown in the following example, information on switch health is displayed on the **Health** Tab, based on your selections.

   FIGURE 134 Health Tab



   The following information is displayed based on the duration selected:

   - **CPU (%)**: The CPU usage of the switch, including the minimum, maximum, average, and current CPU usage trends of the switch.
   - **Memory (%)**: The memory usage of the switch, including the minimum, maximum, average, and current memory usage trends of the switch.
   - **Status**: The health status of the power supply, temperature, and the fans for up to four switch modules are displayed. OK indicates the parameter and components are in good health.

   You can click  to modify the display settings. You can view the trend as a graph or a table. You can also modify the display to reflect the switch name, MAC address, or IP address.

Viewing Alarms

Syslog messages from the switch are sent to the controller to periodically communicate switch health and status. It also brings your attention to issues that may need resolution at the switch level. You can view these details from the **Alarms** tab for individual switches, stacks and switch groups.

Syslog messages from the switch are categorized as **Major** and **Critical**, and are displayed as **events** in the controller. From these events, the following messages are displayed as **alarms** in the controller interface:

- Power Supply failure
- Fan failure
- Module Insertion or removal
- Temperature above the threshold warning

- Stack member unit failure
- PoE power allocation failure
- DHCP offer dropped message
- Port put into error disable state

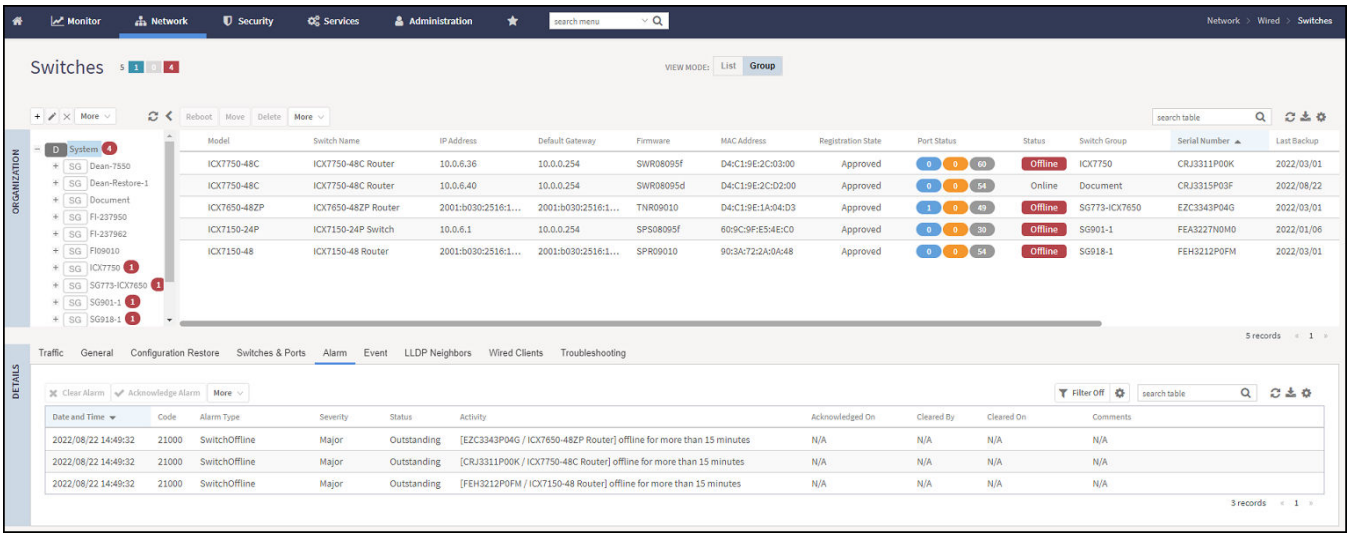
The remaining syslog messages which are categorized by other severity levels are listed in the `switchevent.log` file available in **Diagnostics** > **Application Logs**.

The alarms generate for the switch also reflect in the **Monitor** > **Events and Alarms** > **Events** page.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**. In the **Details** tab, click **Alarm** tab.

FIGURE 135 Switches Alarms Tab



The following information is displayed in the **Alarms** tab:

- Date and Time: Displays the date and time when the alarm was triggered.
- Code: Displays the alarm code (see the Alarm and Reference Guide for your controller platform for more information).
- Alarm Type: Displays the type of alarm event that occurred (for example, switch reset to factory settings).
- Severity: Displays the severity level assigned to the events such as Critical, Major, Minor and Warning.
- Status: Indicates whether the alarm has already been cleared or still outstanding.
- Activity: Displays additional details about the alarm, such as how long was the switch offline for.
- Acknowledged On: Displays the date and time when the administrator acknowledge the alarm.
- Cleared By: Displays information about who cleared the alarm.
- Cleared On: Displays the date and time when the alarm was cleared.
- Comments: Displays administrator notes recorded during alarm management.

Click to export the alarms details to a CSV file. Check the default download folder of your web browser and look for a file named *alarms.csv* and view it using a spreadsheet application

Clearing an alarm removes the alarm from the list but keeps it on the controller's database. Select the alarm from the list and click **Clear Alarm**. The **Clear Alarm** page appears. Type your comments and select **Apply**.

Acknowledging an alarm lets other administrators know that you have examined the alarm. Click **Acknowledge Alarm** to acknowledge an alarm. After you acknowledge an alarm, it will remain on the list of alarms and will show the date and time that you acknowledged it.

You can also view alarms by their severity, status, date and time stamp. Click to apply filters.

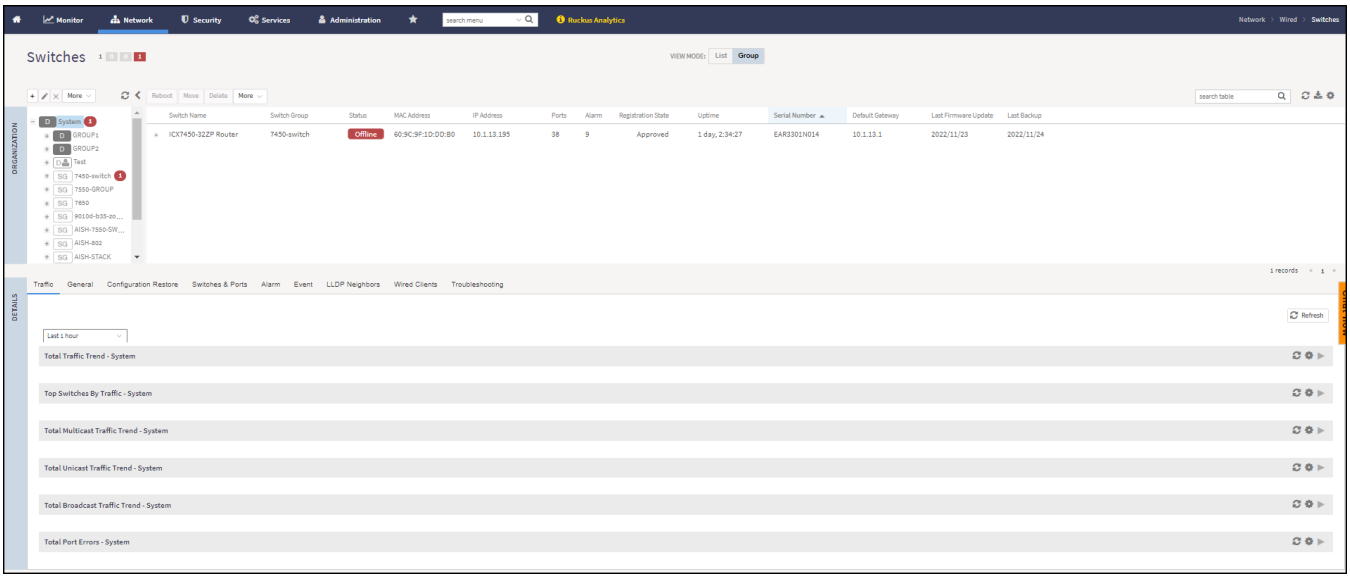
Viewing Events

Events are triggered by an occurrence or the detection of certain conditions in the switch. For example, when the temperature of the device reaches warning levels, or when the fan speed changes, an event is triggered. You can view these details from the **Events** tab for individual switches, stacks and switch groups.

The alarms generate for the switch also reflect in the **Monitor** > **Events and Alarms** > **Events** page.

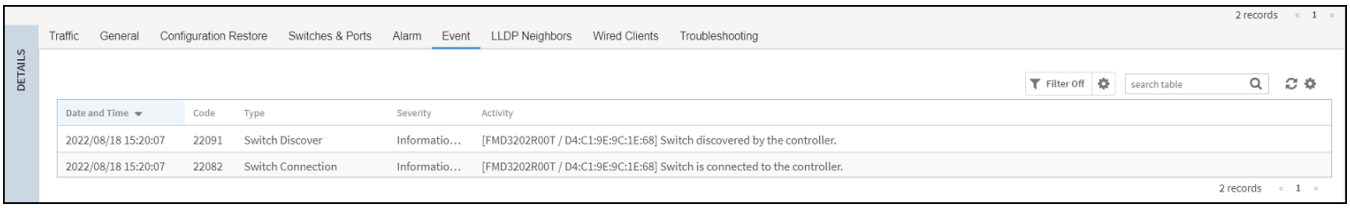
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 136 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**. In the **Details** tab, click **Events** tab.

FIGURE 137 Events Tab



The following information is displayed in the **Events** tab:

- Date and Time: Displays the date and time when the event occurred
- Code: Displays the event code (see the Alarm and Event Reference Guide for your controller platform more information)
- Type: Displays the type of event that occurred (for example, Switch configuration updated)
- Severity: Displays the severity level assigned to the events such as Critical, Debug, Informational, Warning, Major etc .
- Activity: Displays additional details about the event

Click  to export the events details to a CSV file. Check the default download folder of your web browser and look for a file named *events.csv* and view it using a spreadsheet application

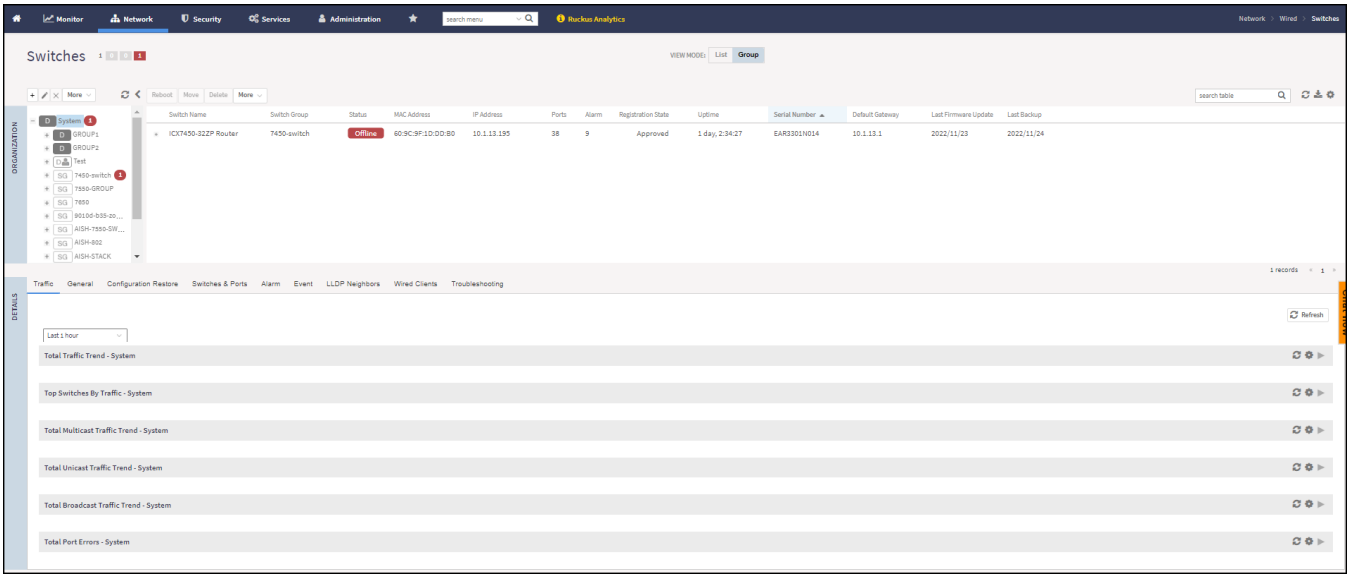
You can also view alarms by their severity, date and time. Click  to apply filters.

Viewing LLDP Neighbor Information

You can view information about the LLDP neighbors such as printers, VOIP devices, or other user equipment connected to the switch, in addition to the LLDP AP neighbors connected to the switch. Link layer discovery protocol or LLDP is used to discover and identify the clients.

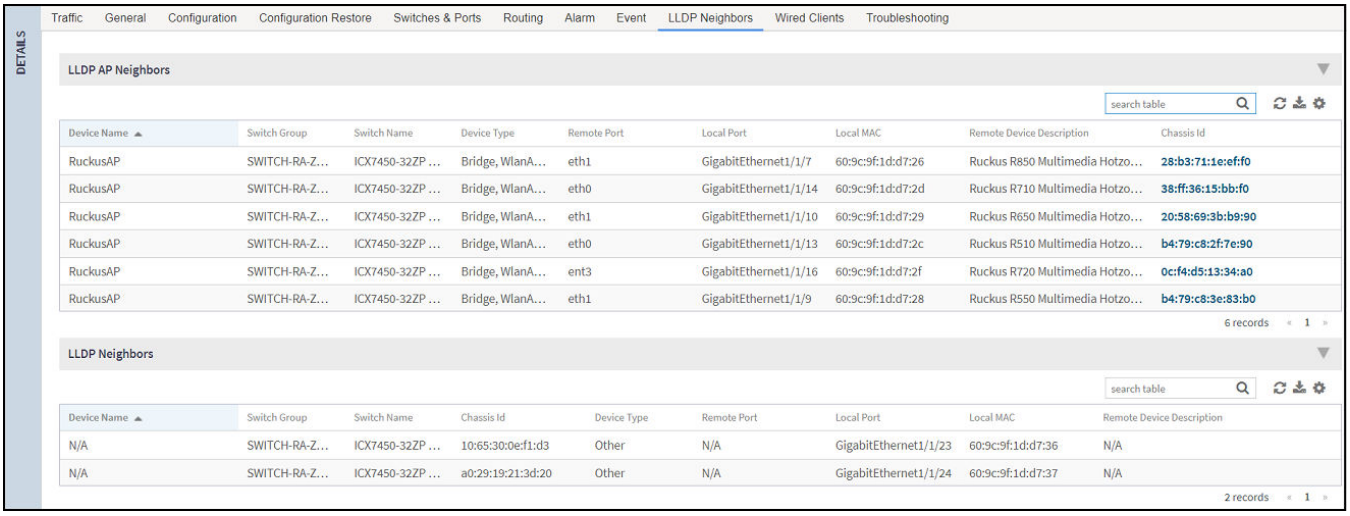
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 138 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**. In the **Details** tab, click **LLDP Neighbors** tab.

FIGURE 139 LLDP Neighbors Connected to the Switch



The following LLDP Neighbors information for switch is displayed in the **LLDP AP Neighbors** tab and **LLDP Neighbors** tab:

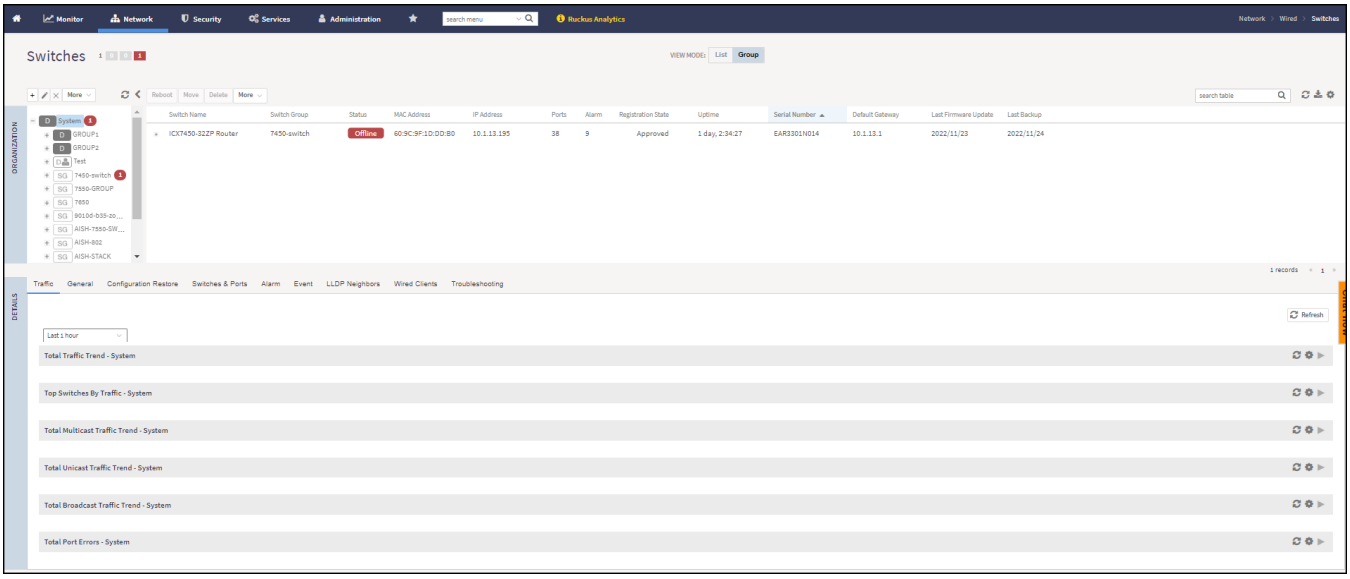
- Device Name: Displays the name of the LLDP neighbor or AP neighbor connected to the switch.
- Switch Group: The name of the group to which the switch belongs.
- Switch Name: The name of the switch or group.
- Device Type: Displays the name of the device type (for example, Router).
- Remote Port: Displays the remote port to which the device is connected.
- Local Port: Displays the local port the device is connected to.
- Local MAC: Displays the local MAC address of the device.
- Remote Device Description: displays the name of the remote device.
- Chassis Id: Display the chassis id information.

Viewing Traffic Trends in the Switch

You can view statistical information about how traffic is handled at the switch level. These details are available for individual switches, stacks and switch groups.

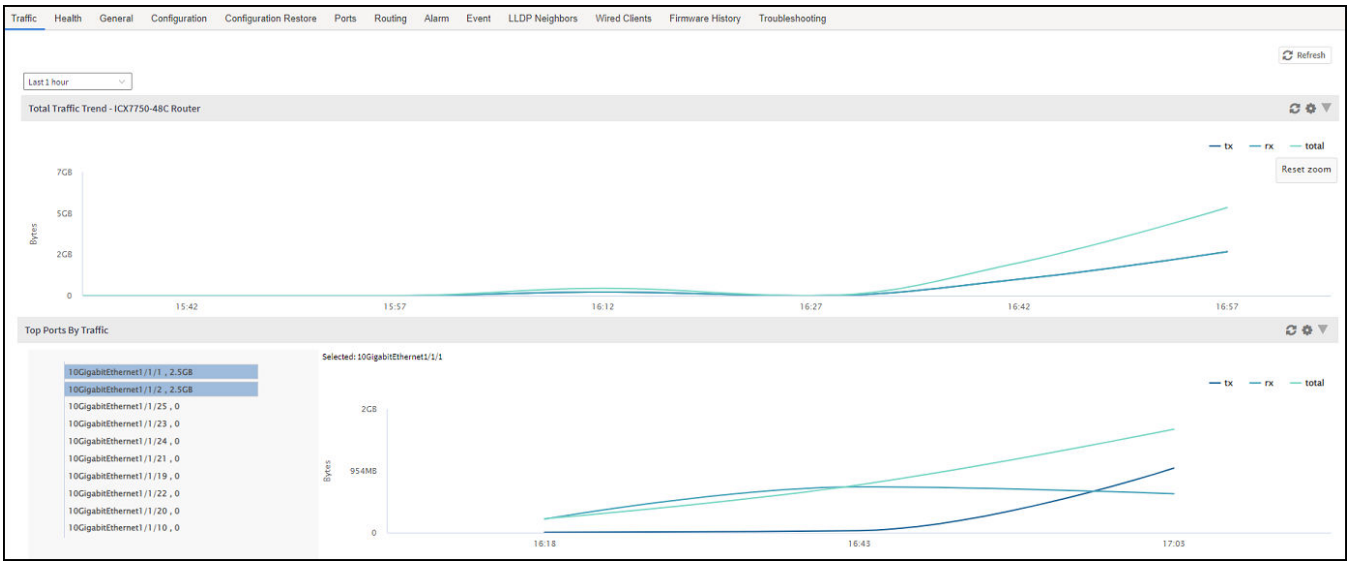
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 140 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**. In the **Details** tab, click **Traffic** tab.

FIGURE 141 Traffic Trend for a Switch



The following information is displayed in the **Traffic** tab. You can view the traffic trend for the last 1 hour or 24 hours:

- Total Traffic Trend: Provides a graphical representation of the network traffic usage over a period of time in the switch or switch group. It also indicates the amount of traffic or data transmitted (tx) and received (rx) by the group in MB, at a certain time and date.
- Top Switch by Traffic: Provides a graphical representation of the top switches that handled maximum network traffic over a period of time, in the switch group. You can click on the switch address to view the traffic trend. This trend is only available for switch groups.
- Top Ports by Traffic: Provides a graphical representation of the top ports that handled maximum network traffic over a period of time, for a switch. You can click on the port address to view the traffic trend. This trend is only available for individual switches.
- Total Multicast Traffic Trend: Provides a graphical representation of the multicast traffic usage over a period of time in the switch or switch group. It also indicates the total number of incoming multicast data packets (multicastIn) and total number of outgoing multicast packets (multicastOut) by the group in MB, at a certain time and date.
- Total Unicast Traffic Trend: Provides a graphical representation of the unicast traffic usage over a period of time in the switch or switch group. It also indicates the total number of incoming unicast data packet (unicastIn) and total number of outgoing unicast packet (unicastOut) by the group in MB, at a certain time and date.
- Total Broadcast Traffic Trend: Provides a graphical representation of the broadcast traffic usage over a period of time in the switch or switch group. it also indicates the total number of incoming broadcast data packets (broadcastIn) and total number of outgoing broadcast packets (broadcastOut) by the group in MB, at a certain time and date.
- Total Port Errors: Provides a graphical representation of the port errors over a period of time in the switch or switch group. It also indicates the total number of inbound packets that contained errors (inErr) and total number of outbound packets that could not be transmitted because of errors (outErr) by the group in MB, at a certain time and date.

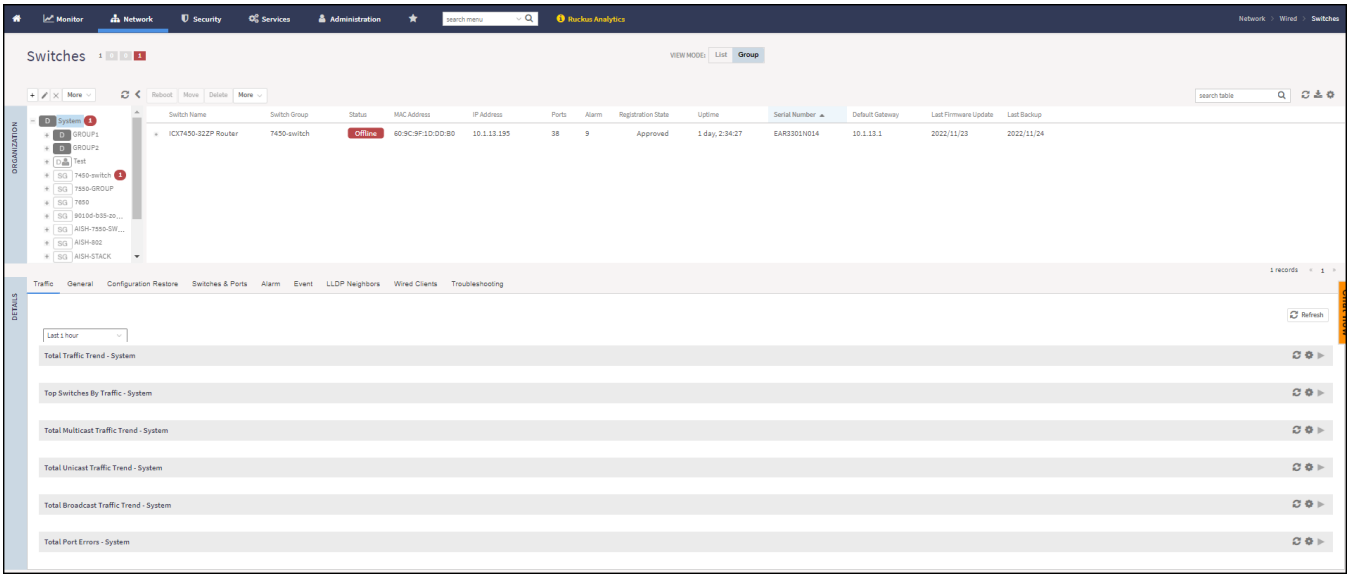
Viewing Firmware History of the Switch

You can view the detailed status and result of the firmware update to a switch. You can also view a history of firmware upgrades that were previously carried out on the switch.

You must have upgraded the firmware of the switch as described in Scheduling a Firmware Upgrade for Selected Switches on page 40

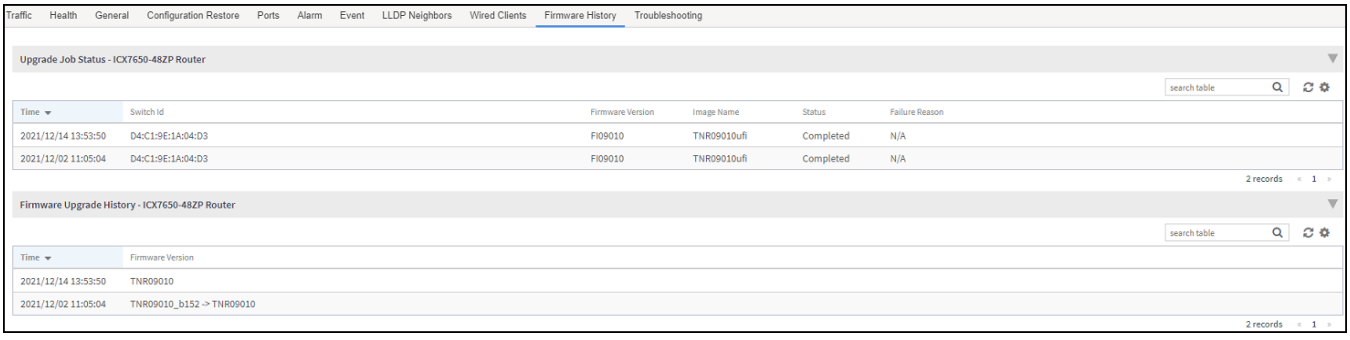
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 142 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**. In the **Details** tab, click **Firmware History** tab.

FIGURE 143 Viewing Firmware History



You can verify the status of the upgrade from the **Upgrade Job Status** section which displays the time, switch ID, firmware version, image name, status and failure reasons (if any) for the upgrade.

The **Firmware Upgrade History** section displays the time of the pervious upgrade operations, and firmware versions to which the upgrade was done.

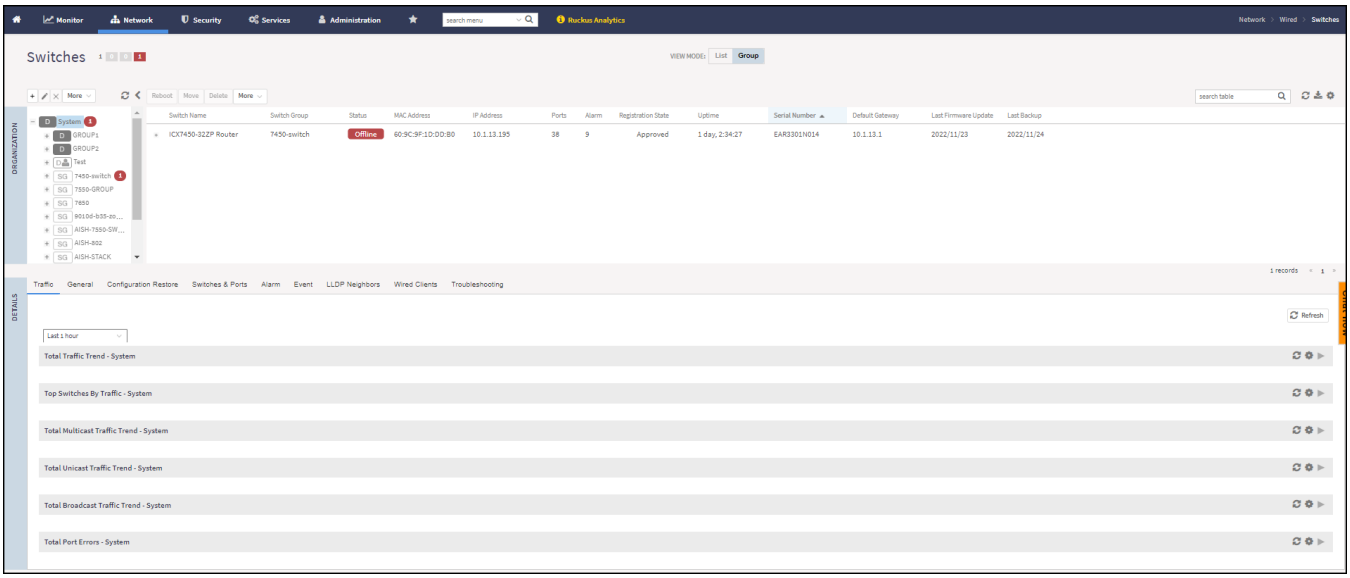
Deleting the Firmware Upgrade Schedules

If you schedule a firmaware upgrade, and if the firmware upgrade is not executed or is in progress then this feature allows you to cancel the firmware upgrade. However, it must be noted that if the switch is copying or downloading the firmware, the controller will not be able to cancel the process.

To delete the firmware upgrade process, perform the following steps.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 144 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**. In the **Details** tab, click **More** > **Delete Firmware Schedules**.

FIGURE 145 Upgrade in Progress

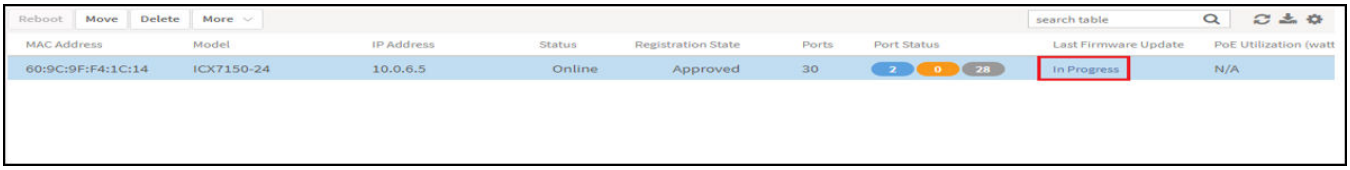
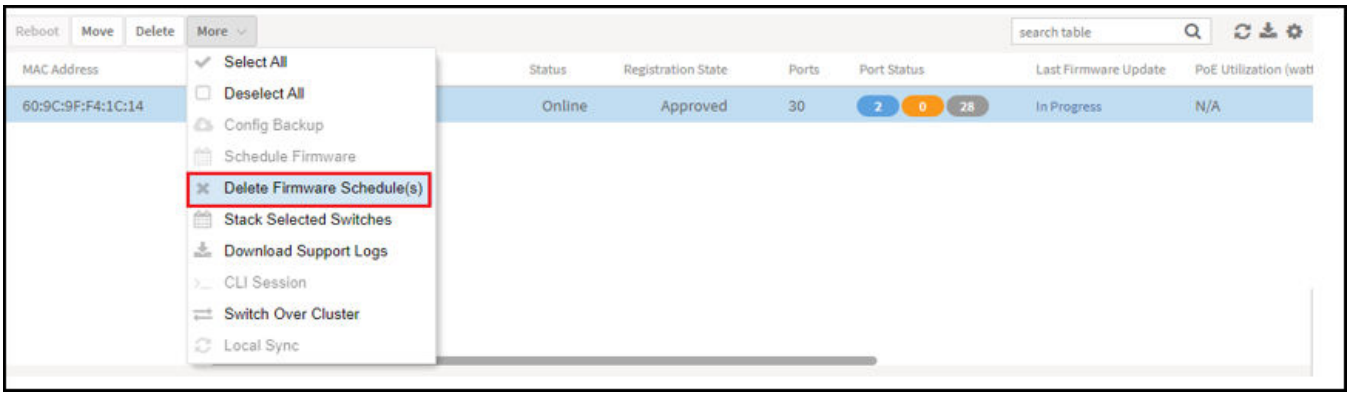
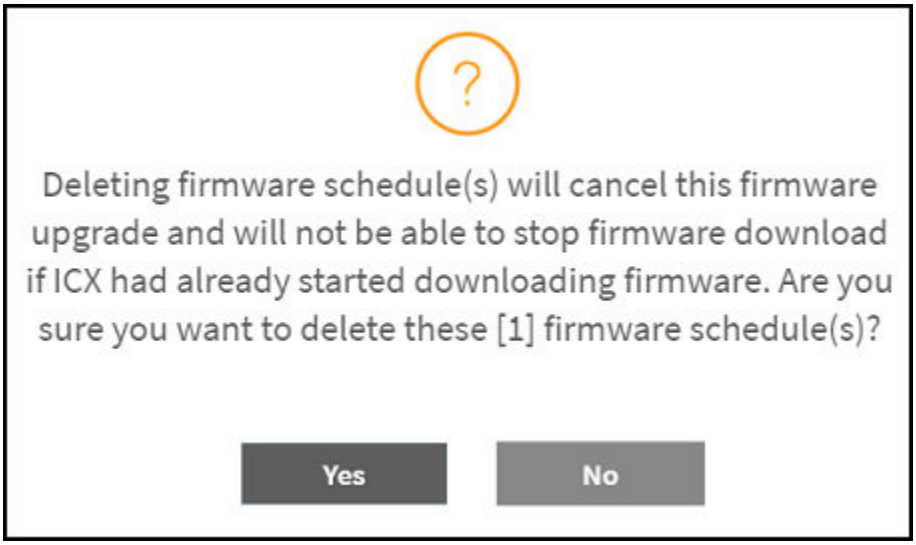


FIGURE 146 Deleting Firmware Upgrade Schedule(s)



A warning message is displayed before you cancel the upgrade.

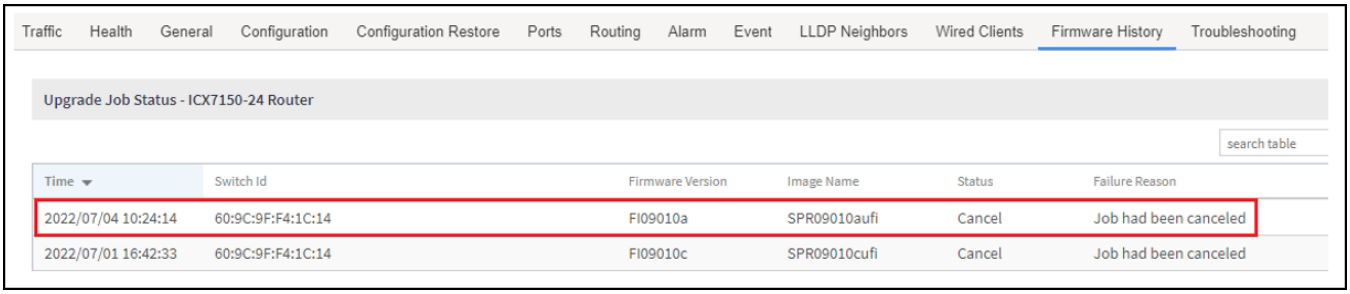
FIGURE 147 Warning Message before deleting



3. Click **Yes** to delete the firmware schedule.
4. A **Switch firmware schedule(s) deleted successfully** message dialog box is displayed, click **OK**.

5. In the **Organization** tab, select the **Switch** and in the **Details** tab, select the **Firmware History** tab. In the **Upgrade Job Status** tab confirm that the schedule is canceled.

FIGURE 148 Confirming the deletion



Configuring the Group Firmware Settings

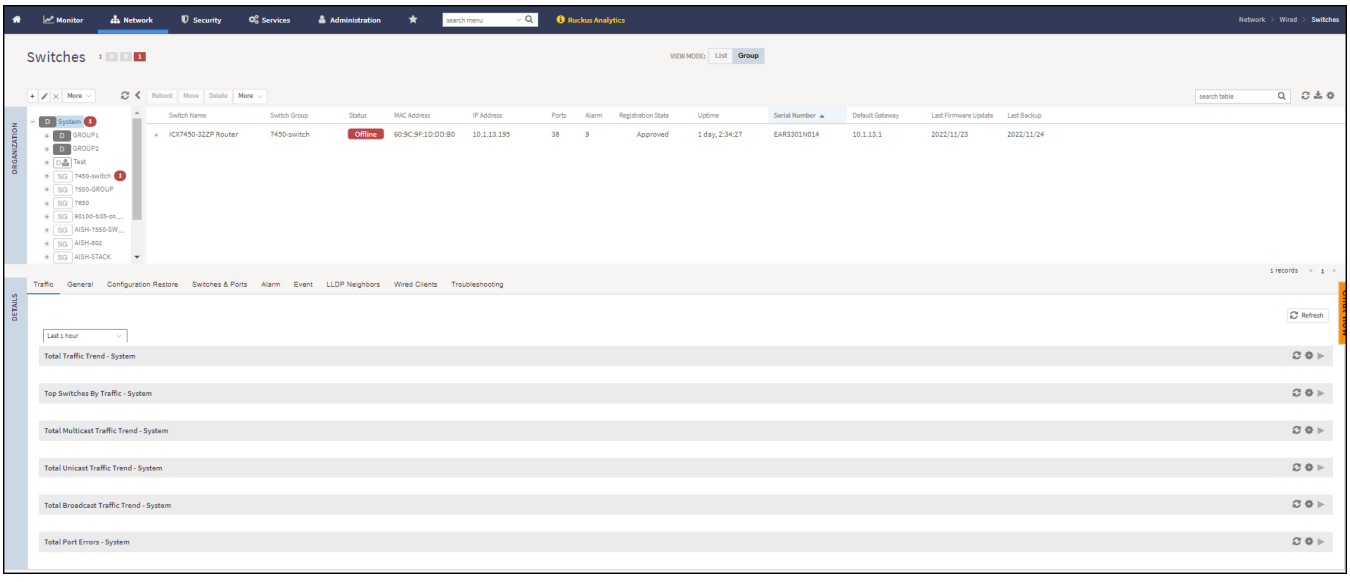
The Group Firmware Settings allows the user to select default firmware for the switch group. The newly joined switch is upgraded to the selected firmware in the switch group.

NOTE
The default firmware selection at group level does not trigger upgrade for the existing switches in the switch group, it only triggers upgrade for newly joined switch(es)

Complete the following steps to perform the firmware upgrade of newly added switch in the switch group to the default firmware version.

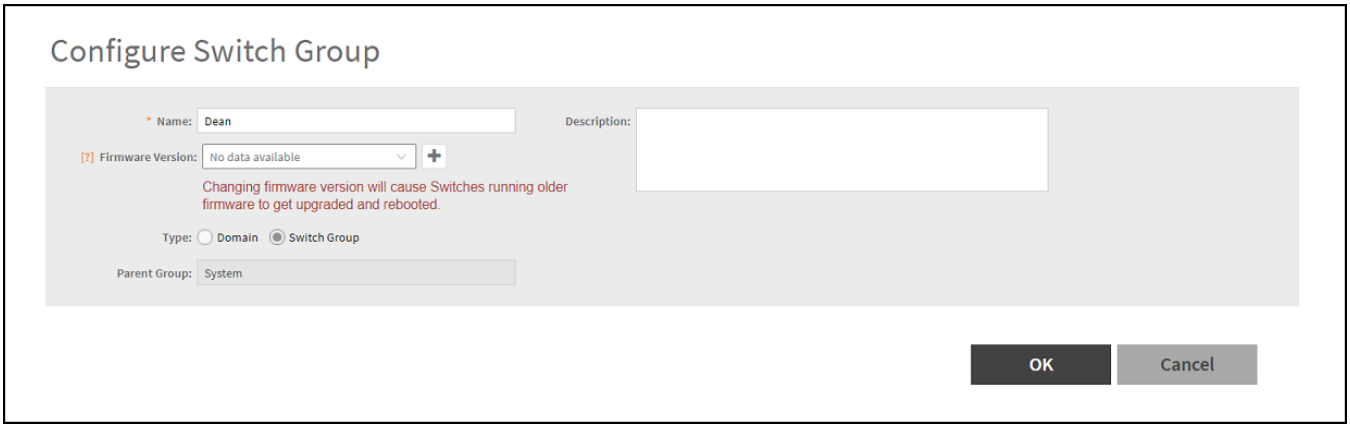
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 149 Switches



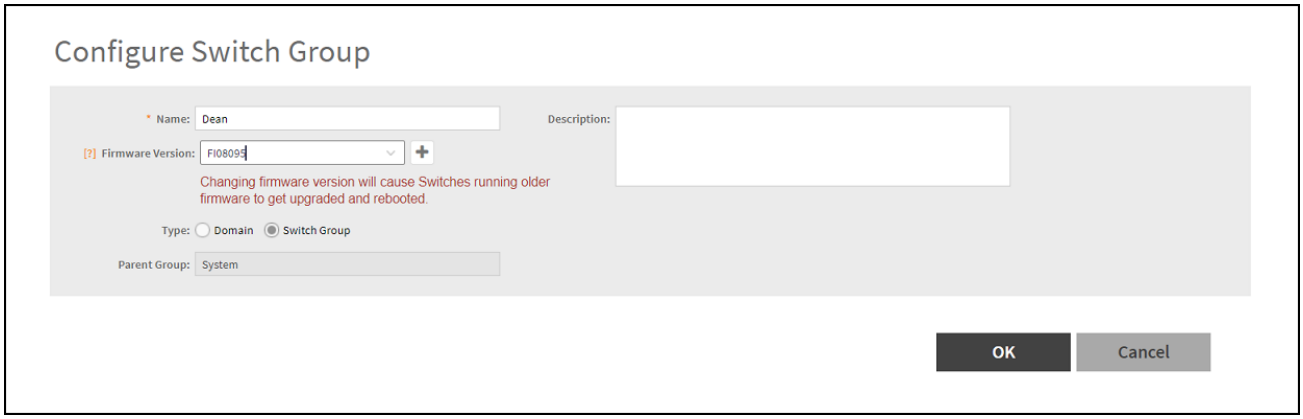
2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** that you want to configure, and click  icon to display the **Configure Switch Group** dialog box.

FIGURE 150 Configuring the Switch with Default Version



3. Complete the following fields:
   - **Name**: Type the name of the switch group that you want to create.
   - **Description**: Enter a brief description for the switch group .
   - **Firmware version**: Select firmware version from the list or retain the default firmware version.

     FIGURE 151 Configuring the switch with Firmware version



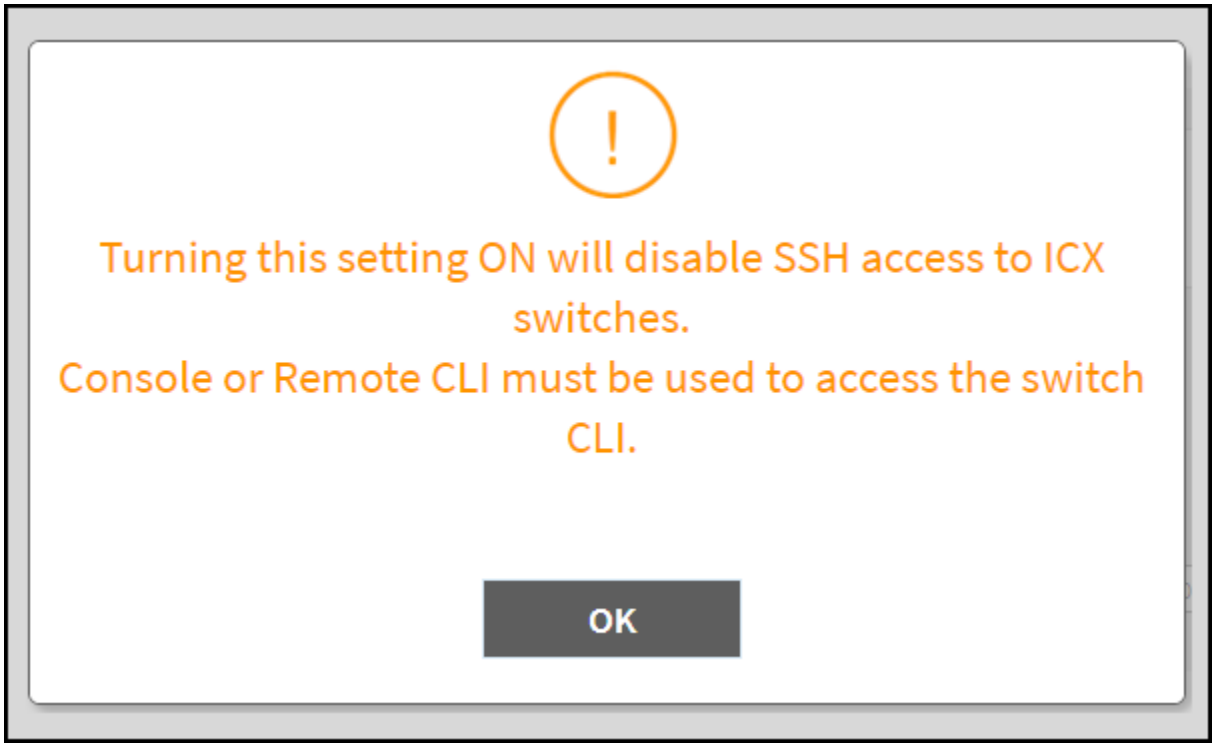
     NOTE
     The group firmware settings requires switches to be running SmartZone 5.2.1 or later.

   - **Type**: Select **Switch Group**.
   - **Parent Group**: Displays the parent group under which the switch group resides.
   - **Two Factor Authentication**: Switch **ON** to use the **Console CLI** or **Remote CLI** to access the **Switches**.

     NOTE
     Turning ON this feature will disable the SSH access to the switches.

     A **message** dialog box is displayed, click **OK**.

FIGURE 152 Two Factor Authentication Message



- **Backup Schedule**: Allows you to schedule the backup. From the **Interval** drop-down list, select the type of backup such as **Daily**, **Weekly**, or **Monthly**. If the backup selected is **Daily**, you can configure **@Hour** , and **Minute** fields. If the backup selected is **Weekly**, you can configure the **Every** (day of the week), **@Hour** , and **Minute** fields. If the backup selected is **Monthly**, you can configure **Every** (date), **@Hour** , and **Minute** fields.

  NOTE
  The default backup time for scheduling a **Daily** backup is 3:30 a.m. The backup schedule is configured on the level one switch group.

4. Click **OK**.

Accessing the switch CLI through SmartZone (Remote CLI)

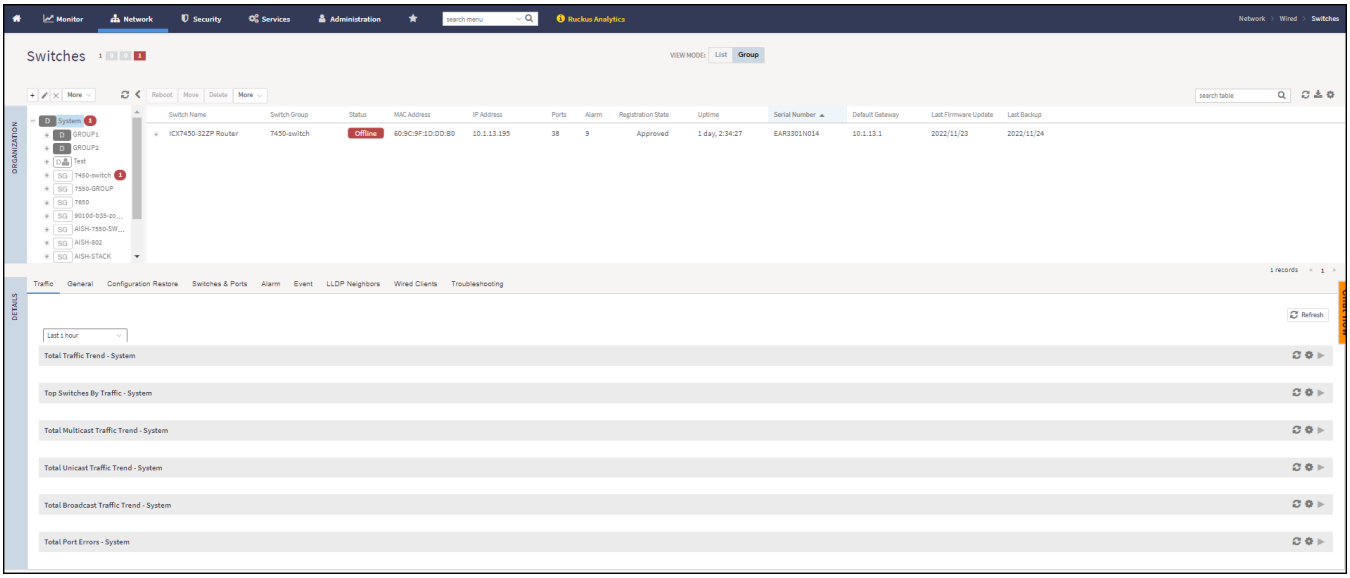
SmazrtZone 5.2.1 introduces this essential feature that allows you to directly access the Switch CLI prompt from the controller web interface. The Remote CLI allows you to establish a secured connection between controller and switch that can span over Internet, and eliminate the need to open VPN connection to switch's network when trying to access CLI through SSH or Telnet.

NOTE
This feature can be accessed by only the System Super-Admin in 5.2.1 release.

The administrator must complete the following steps to access a CLI session.

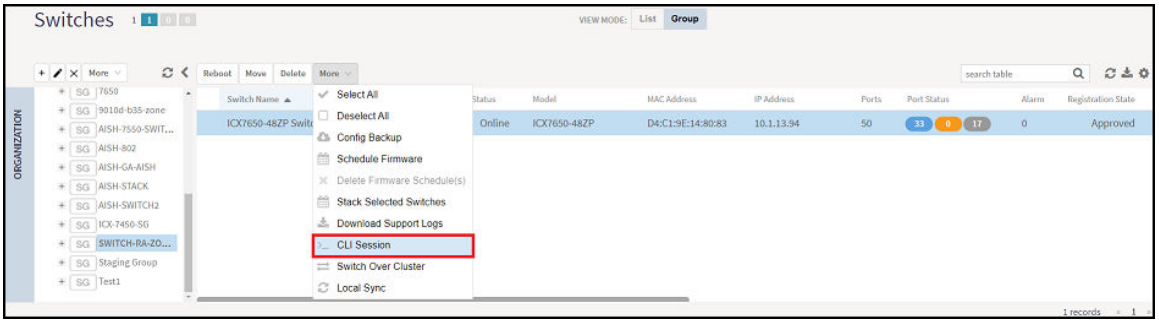
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 153 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**.
3. Click **More** > **CLI session** to display the **CLI command** window.

FIGURE 154 Selecting CLI Session



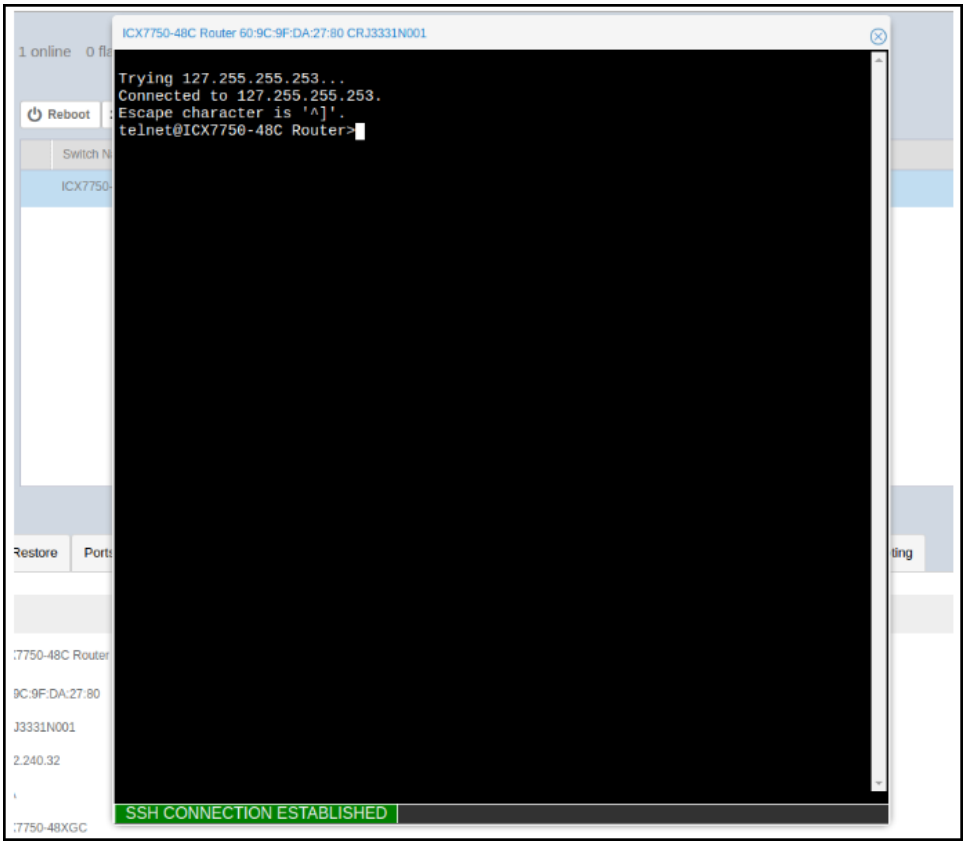
4. Enter the administrator password.

   After login, it takes approximately five seconds to set up a secure session within the secure tunnel established between switch and controller to access switch.

   A CLI Window is displayed.

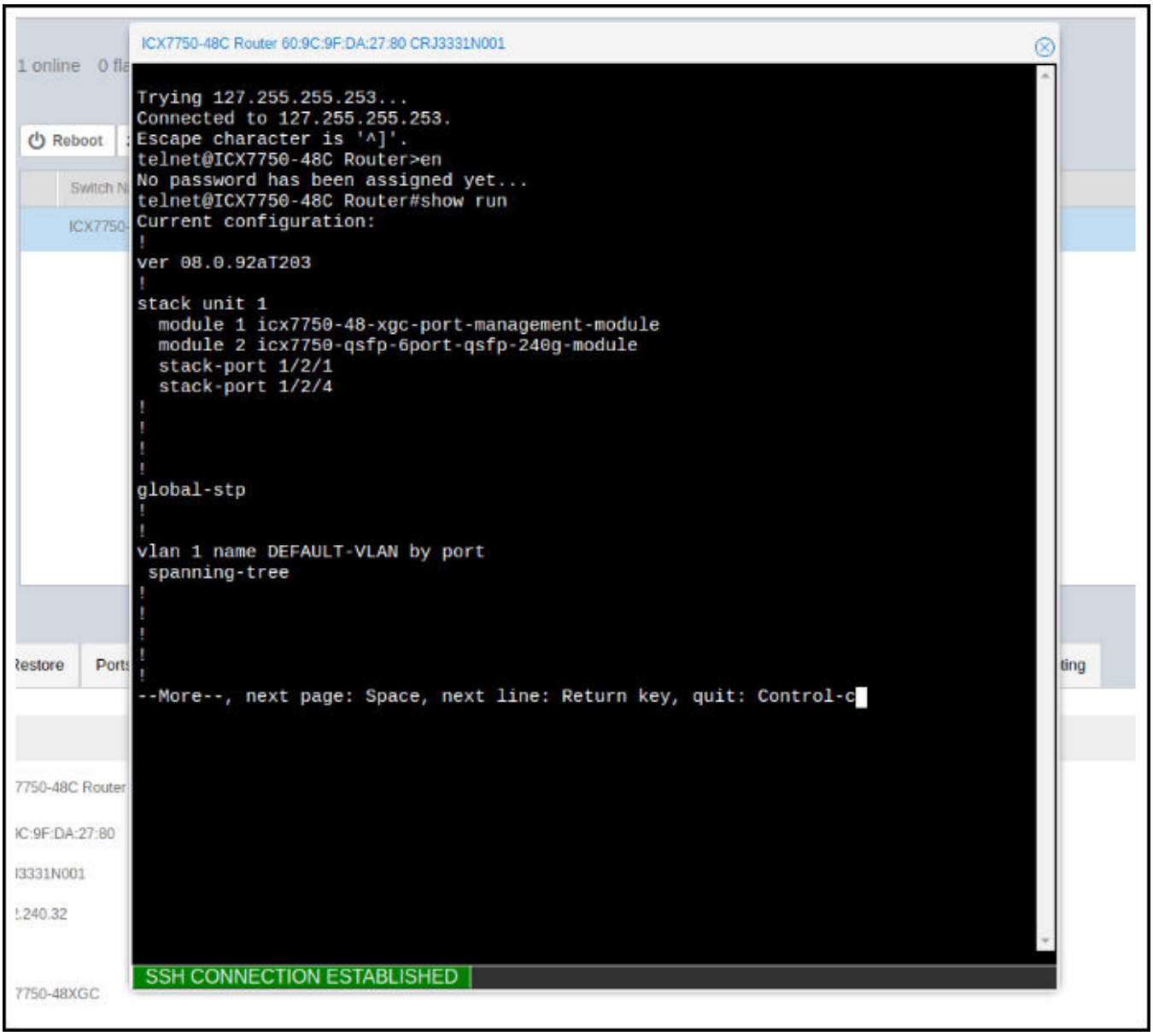
   NOTE
   You do not need to enable telnet server on ICX switches to use Remote CLI.
   However, if telnet authentication is enabled on the switch, you will be prompted to enter the credentials when opening CLI session via SmartZone. The credentials depend on the type of authentication defined on the switch (local user, RADIUS etc.).

FIGURE 155 Accessing Switch Through the CLI Sesion



5. Press the **Spacebar** to skip to the next page, press **Enter** to display the next line, or press **Ctrl + C** to exit.

FIGURE 156 Example of Paging Display



6. Enter the **exit** command to quit the CLI session.

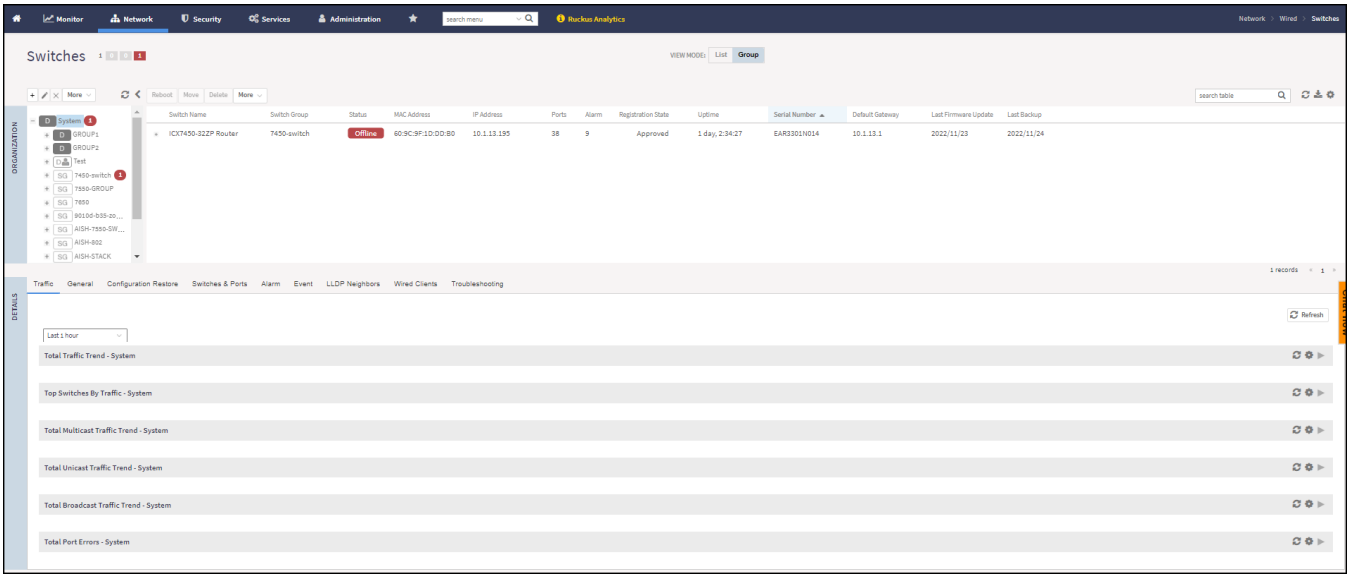
Viewing PoE Utilization and Health Status of the Switch

Prior to SmartZone 5.2.1, the controller provided the power supply status and PoE utilization for a stack unit. Beginning with SmartZone 5.2.1, the controller provides a view of the PoE utilization in watts, and health status such as the power supply, temperature and fan status of each member in the stack unit.

Complete the following steps to view the health status of each member in the stack unit.

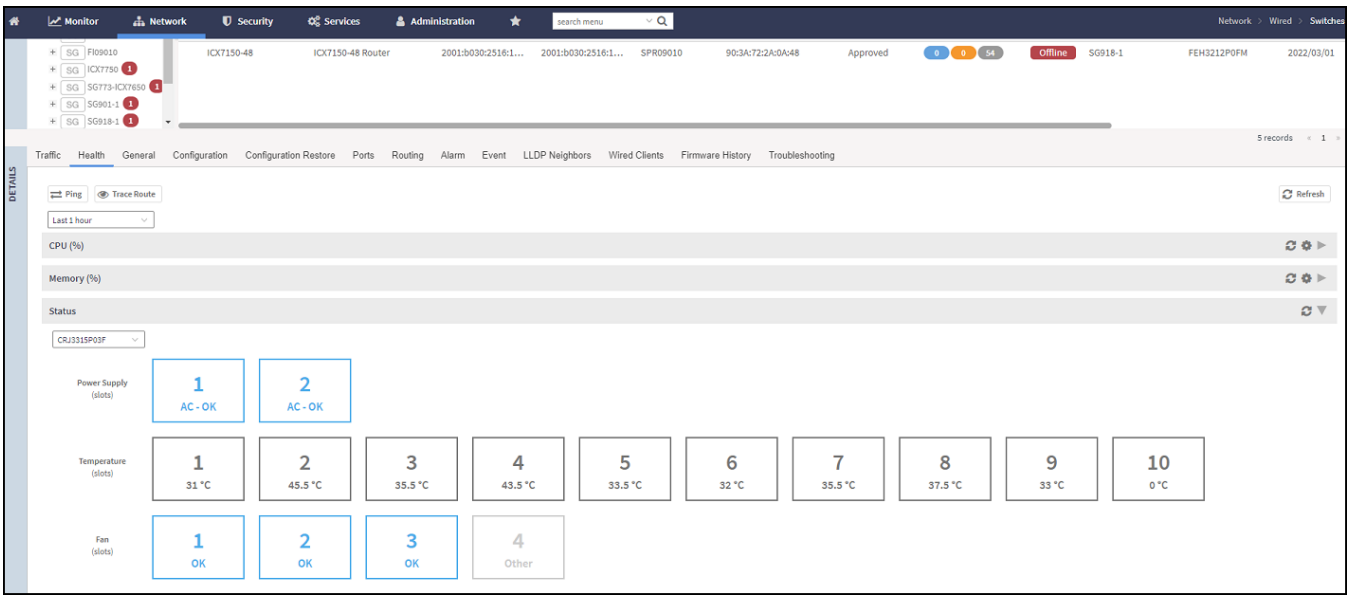
1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

FIGURE 157 Switches



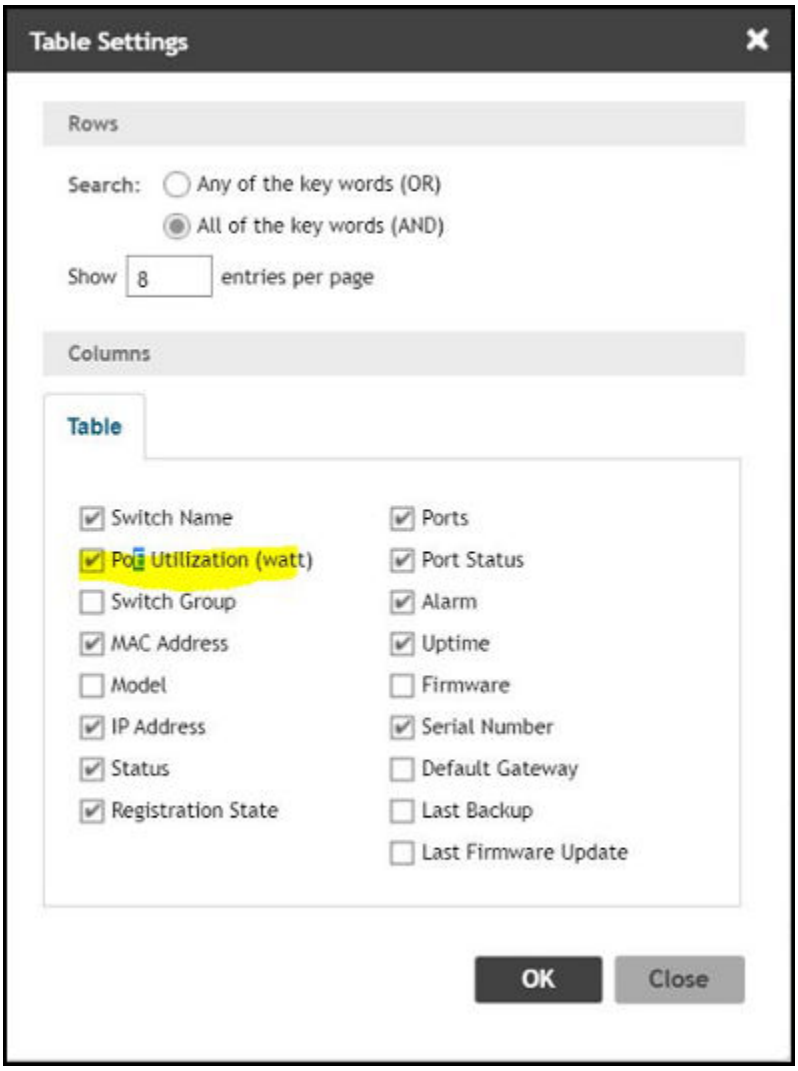
2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**.
3. In the **Details** tab, click **Health** tab. In the **Status** tab you can view the health status, such as the power supply, temperature, and fan status of the stack switch.

FIGURE 158 Viewing the Health Status of Stack Switch



4. To enable the PoE Utilization, In the **Organization** tab, click icon at the top right to display the **Table Settings** dialog box.

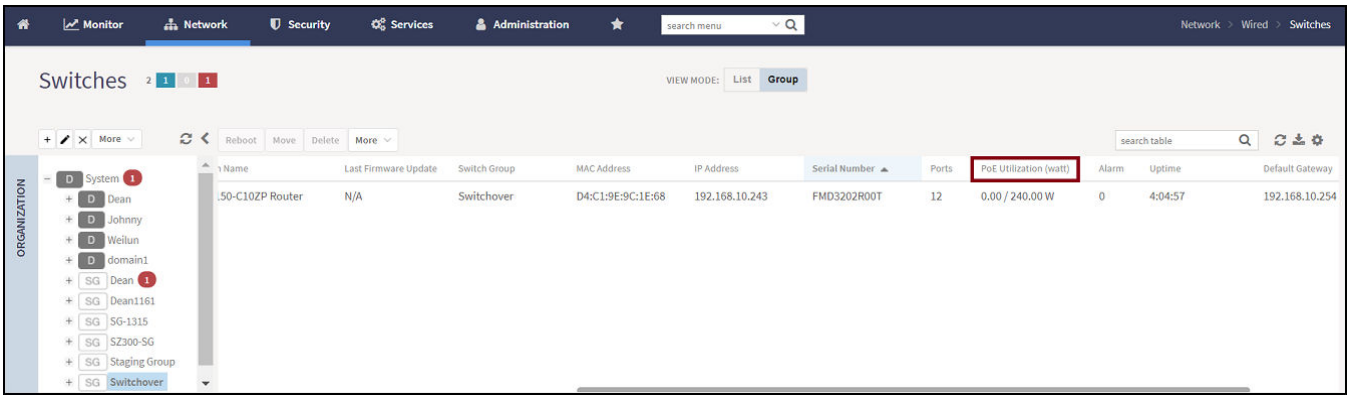
FIGURE 159 Enabling the PoE Utilization



5. Select the **PoE Utilization (watt)** from the table.
6. Click **OK**.

7. In the **Organization** tab, select the **Switch**, to view the **PoE Utilization (watt)** field listed in the table.

FIGURE 160 Viewing the PoE Utilization Field



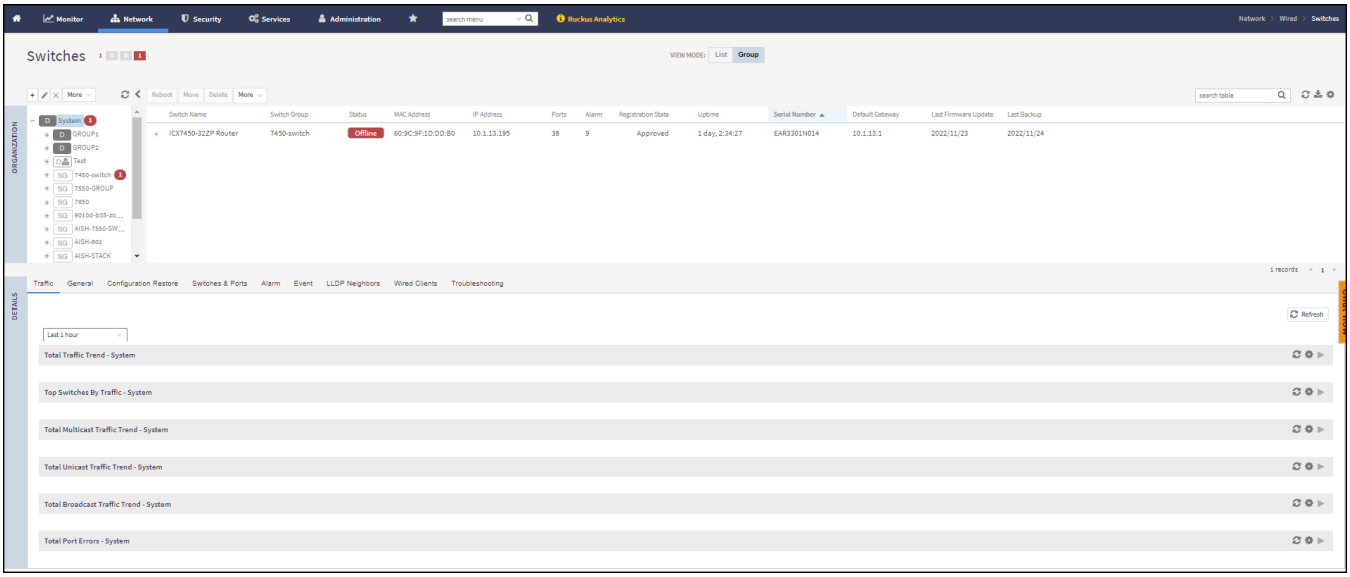
Ability to Convert Standalone Switch to Stack

This feature allows the Standalone switch to convert into a stack by adding member switches.

Complete the following steps to convert standalone switch into stack.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

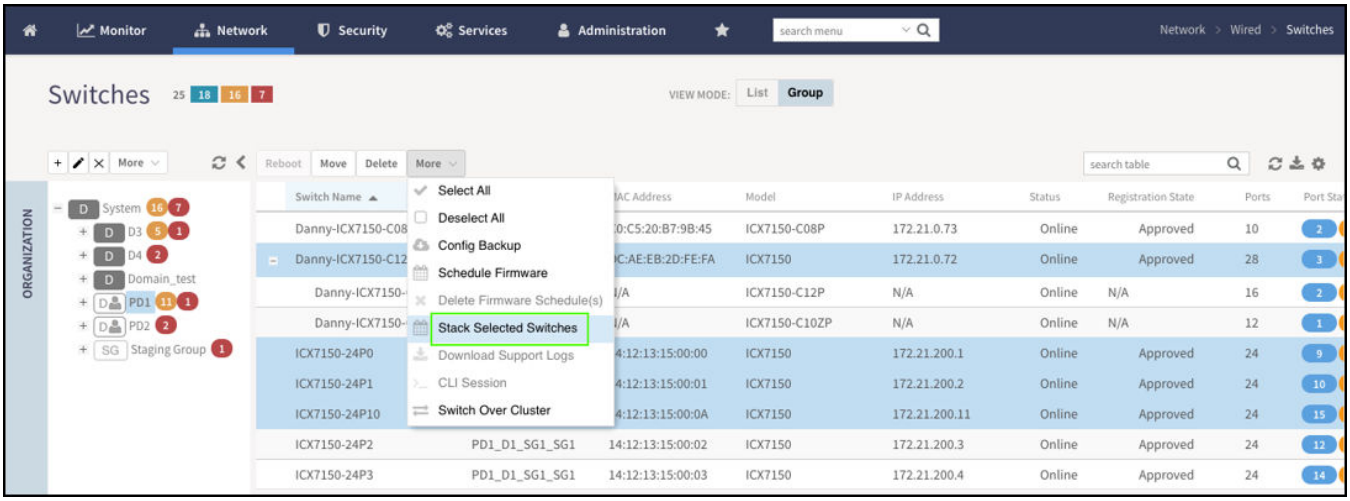
FIGURE 161 Switches



2. In the **Organization** tab, click a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**.

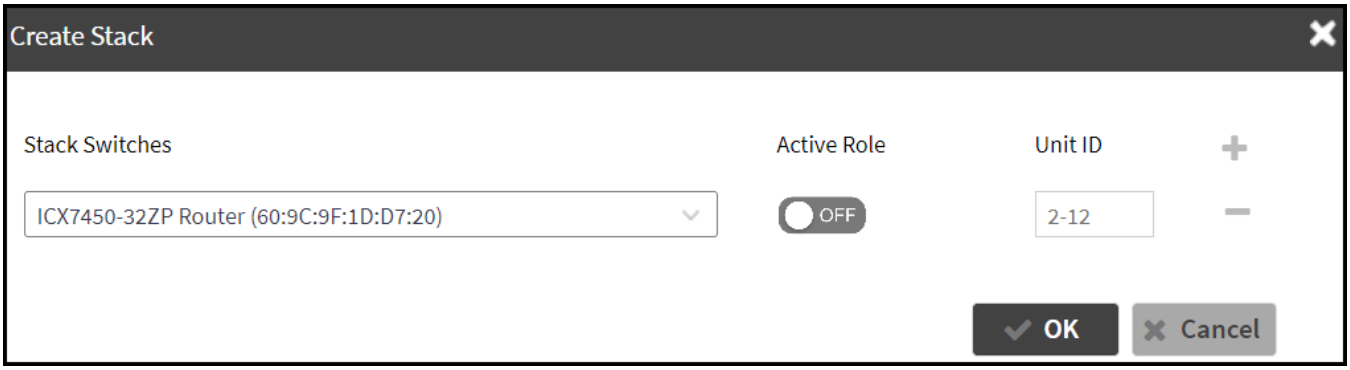
3. To add stanalone switch to the stack, click **More** > **Stack Selected Switches**

FIGURE 162 Stack Selected Switches



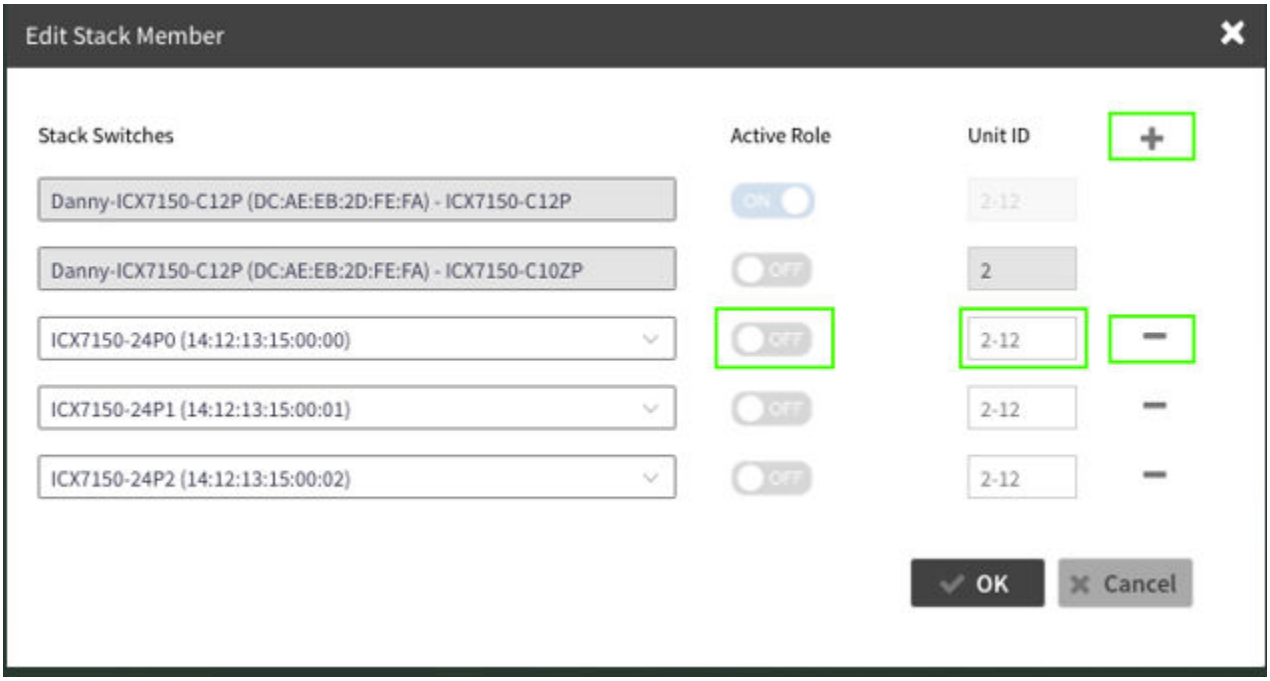
The **Create Stack** dialog box is displayed. Turn **Active Role** ON.

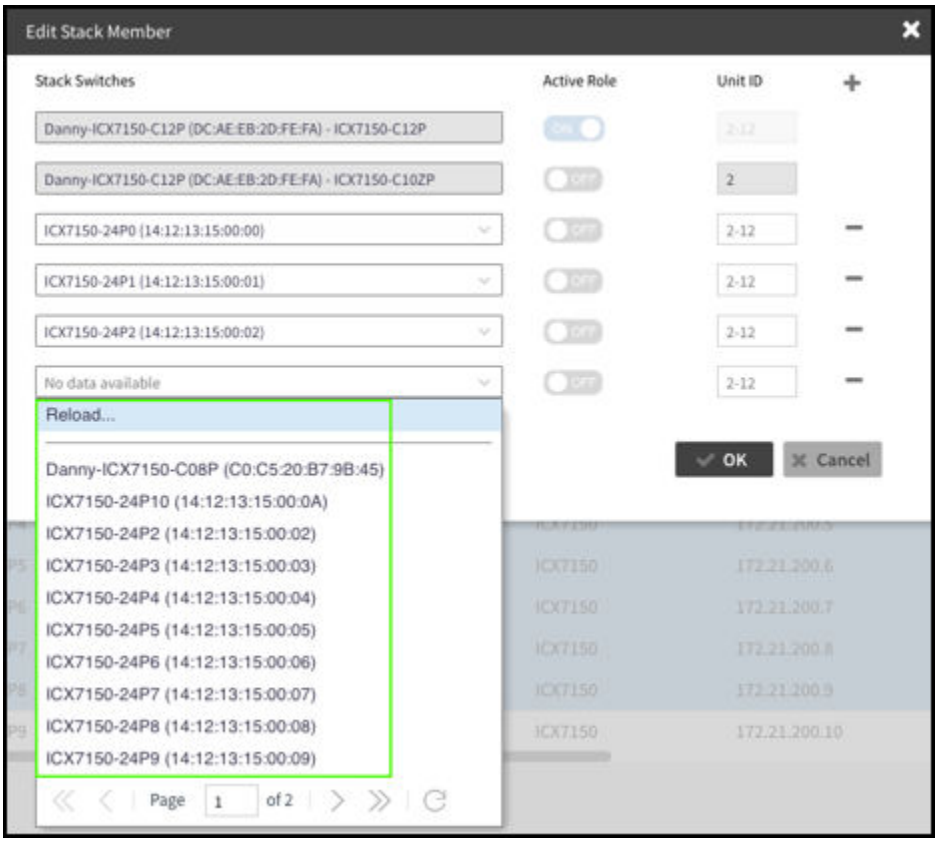
FIGURE 163 Create Stack Dialog Box



4. In the **Edit Stack Member** page, click **+** or **-** to add or remove the stack entry. A RUCKUS stack contains from two to 12 units configured in a ring or linear topology. The units in a stack are from the same model family; that is, a stack can be an ICX 7150 stack, an ICX 7250 stack, an ICX 7450 stack, an ICX 7650 stack, or an ICX 7850 stack.

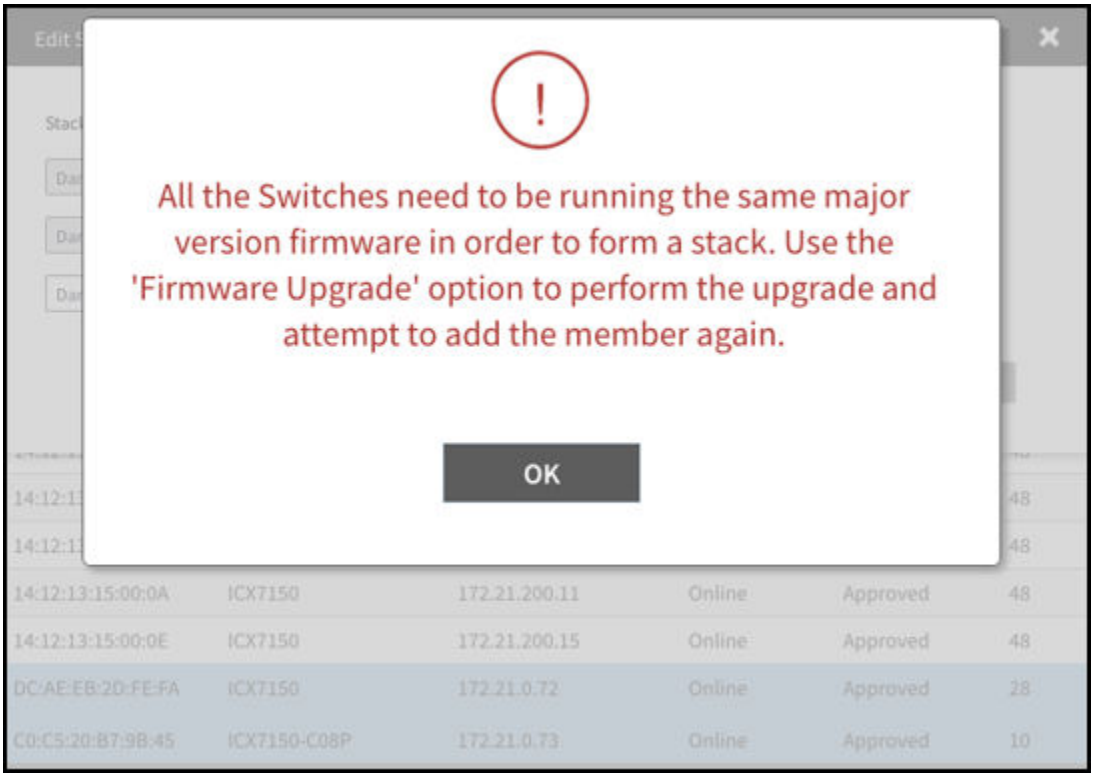
   NOTE
   Initially for 09.0.00, the ICX 7150 and ICX 7250 platforms are limited to a maximum of eight units in a stack.




Edit Stack Member
Stack Switches
Active Role
Unit ID
Danny-ICX7150-C12P (DC:AE:EB:2D:FE:FA) - ICX7150-C12P
Danny-ICX7150-C12P (DC:AE:EB:2D:FE:FA) - ICX7150-C10ZP
ICX7150-24P0 (14:12:13:15:00:00)
ICX7150-24P1 (14:12:13:15:00:01)
ICX7150-24P2 (14:12:13:15:00:02)
No data available
2-12
OK
Cancel
Reload...
Danny-ICX7150-C08P (C0:C5:20:B7:9B:45)
ICX7150-24P10 (14:12:13:15:00:0A)
ICX7150-24P2 (14:12:13:15:00:02)
ICX7150-24P3 (14:12:13:15:00:03)
ICX7150-24P4 (14:12:13:15:00:04)
ICX7150-24P5 (14:12:13:15:00:05)
ICX7150-24P6 (14:12:13:15:00:06)
ICX7150-24P7 (14:12:13:15:00:07)
ICX7150-24P8 (14:12:13:15:00:08)
ICX7150-24P9 (14:12:13:15:00:09)
Page 1 of 2

5. Click **OK**.

NOTE
If stack and switch are running different version of an image, an error message is displayed.



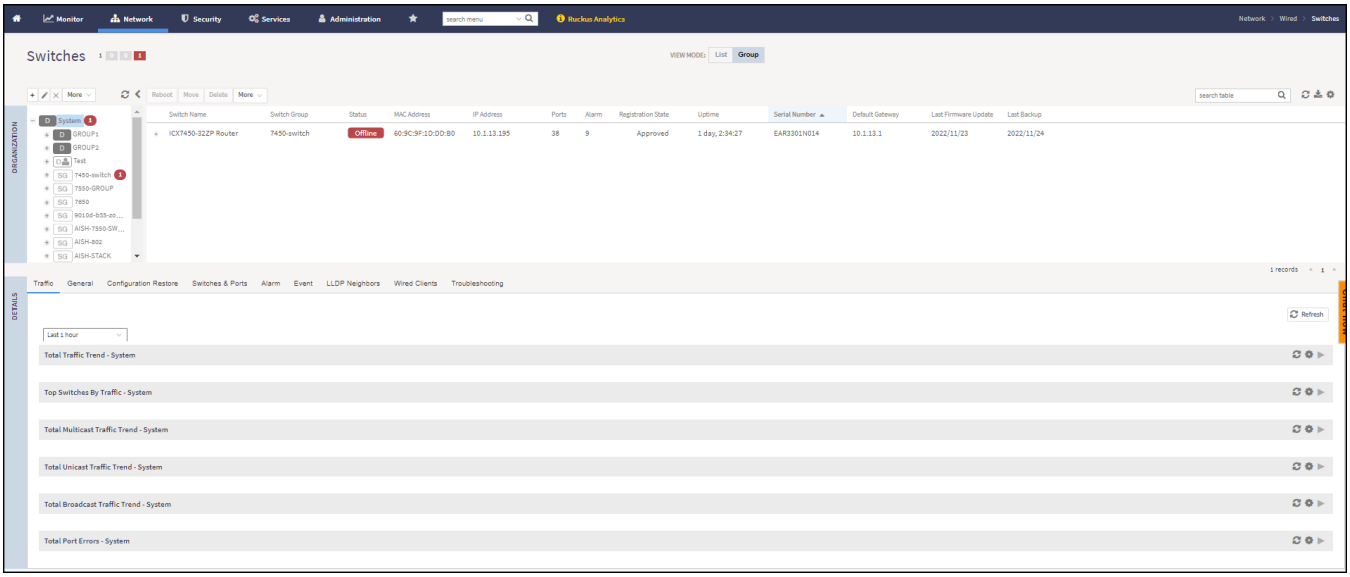
Troubleshooting Switch Issues

You can troubleshoot issues related to wired and wireless clients connected to the switch at the system level from the **Troubleshooting** tab. You can use Remote operations, Client Connectivity and Custom Events to troubleshoot issues with switches or switch groups.

To access the **Troubleshooting** tab do the following:

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

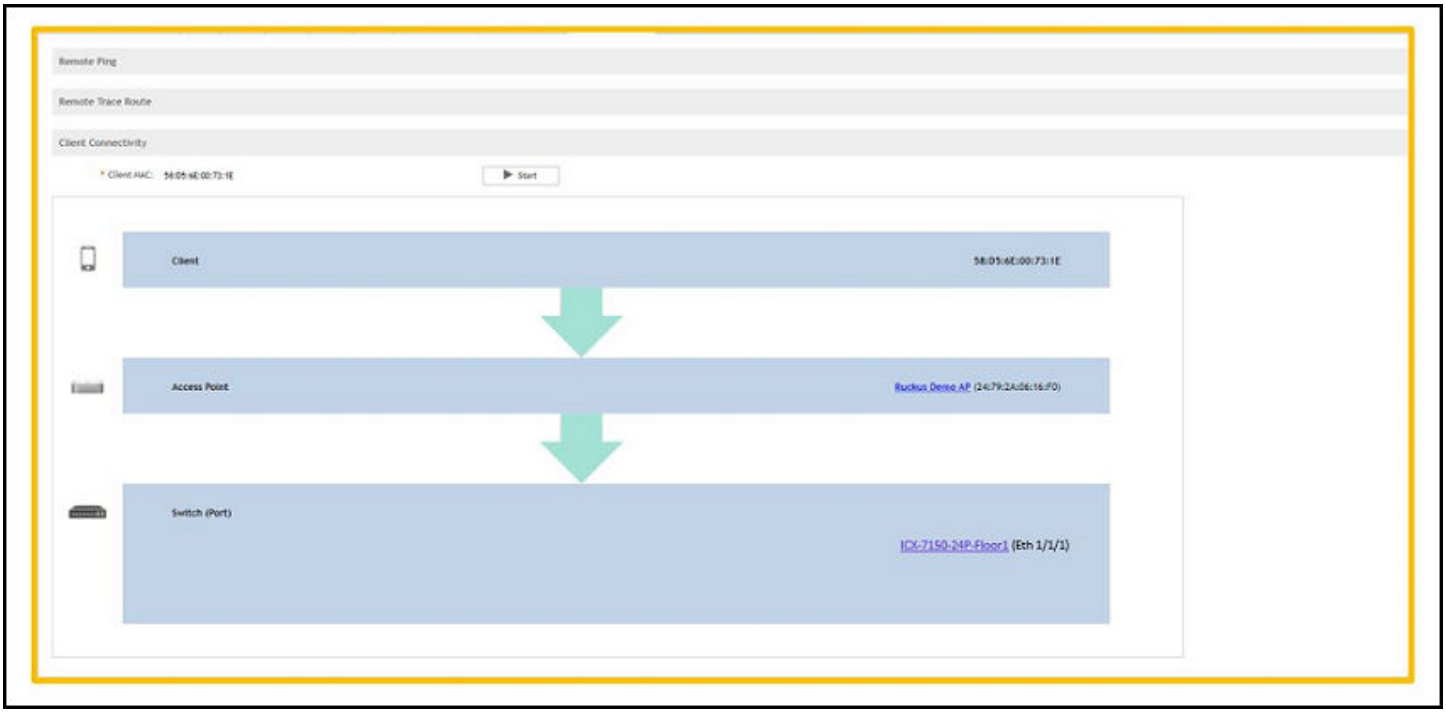
FIGURE 164 Switches



2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**.
3. Click **Troubleshooting** tab.

To troubleshoot issues with an AP client, use the MAC address of the client on the **Troubleshooting** tab of a switch or switch group. Once you enter the MAC address of the client, SmartZone displays how the client is connected to the network, including the AP, the switch, and the switch port on which the client MAC is learned. As an example, if a printer is connected to an AP, which in turn is connected to a switch that is managed by a SmartZone controller, you can troubleshoot any connectivity issues between the devices from the **Troubleshooting** tab by providing the MAC address of the printer.

FIGURE 165 Client MAC Search



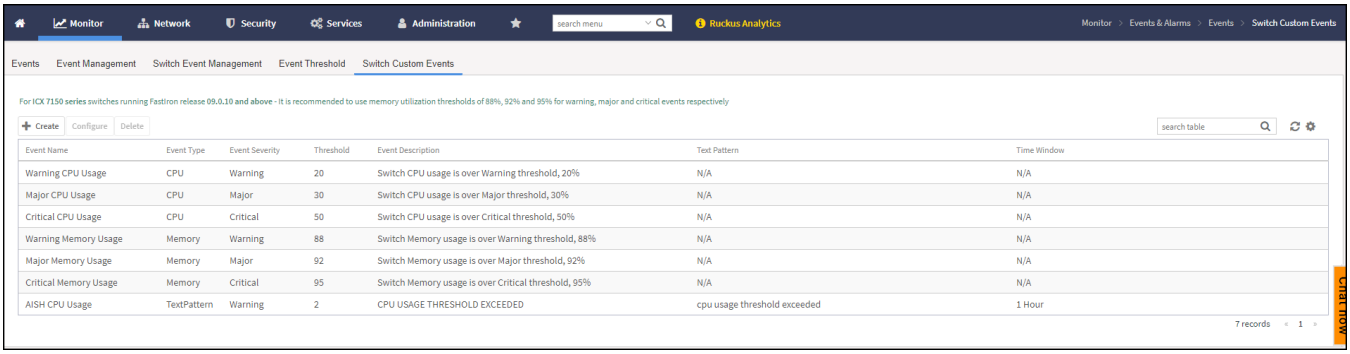
Troubleshooting Using Custom Events

You can create custom events to define failure scenario and use them to generate troubleshoot switch issues.

To access the **Switch Custom Events** window do the following:

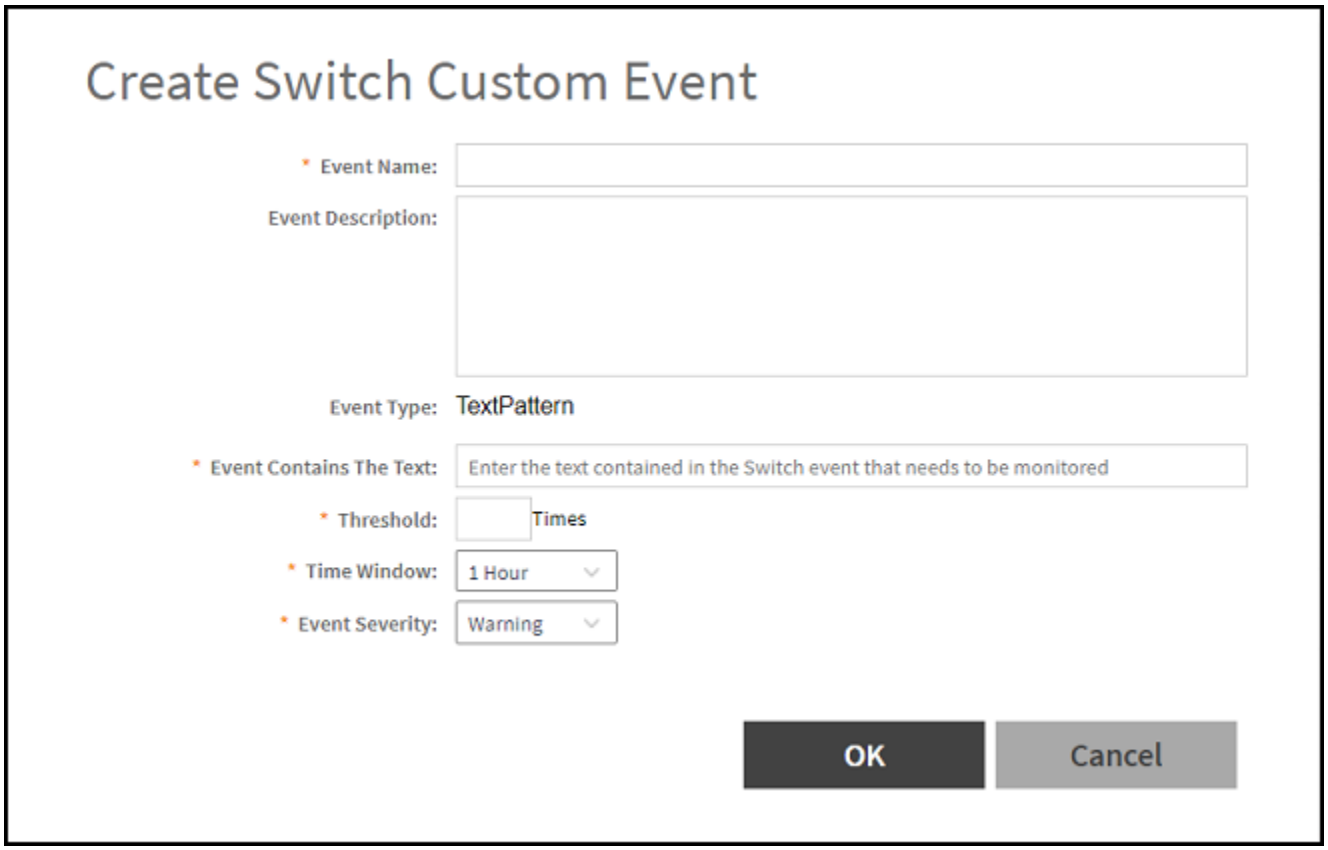
1. On the menu, click **Monitor** > **Events and Alarms** > **Events** > **Switch Custom Events** to display the **Switch Custom Events** window.

   FIGURE 166 Switch Custom Events



2. Click + Create icon to display the **Create Switch Custom Event** dialog box.

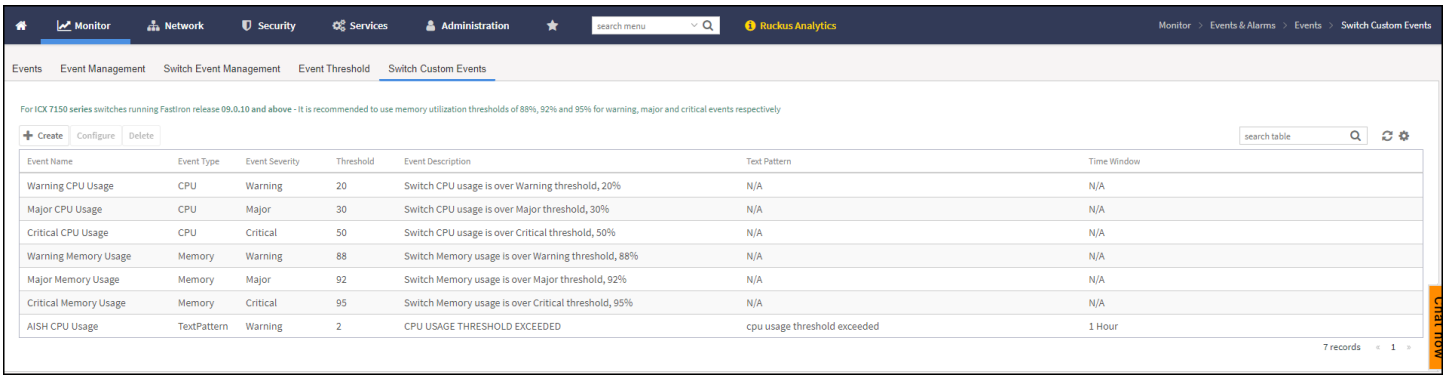
FIGURE 167 Creating Switch Custom Event



3. Complete the following fields:
   - Event Name: Enter the name.
   - Event Description: Enter a brief description.
   - Event Type: By default, **TextPattern** is selected.
   - Event Contains The Text: Enter the text contained in the switch event that needs to be monitored.
   - Threshold: Enter the threshold value between 0 to 255.
   - Time Window: Select from the drop down list, select the required time.
   - Event Severity: Select from the drop down list, select **Major** or **Critical** or **Warning**.
4. Click **OK**.

For example, you can create a "system is unusable" event with the following settings. Based on this event definition and configuration, if any switch sends this message thrice in one hour, the controller triggers a Custom Event. You can view the "system unavailable" event from the **Switch Custom Events** page. For more information on custom events, see #unique_80.

FIGURE 168 Troubleshooting switch issues through custom events



NOTE

It is quite common that entry level switches like ICX 7150 use up 70-80% of the available memory. You can modify the thresholds for memory usage custom events to a higher limit in such cases.

VIDEO

Switch Custom Troubleshooting Demo Verify client to WLAN to switch assignment (Switch Client Troubleshooting).
Click to play video in full screen mode.

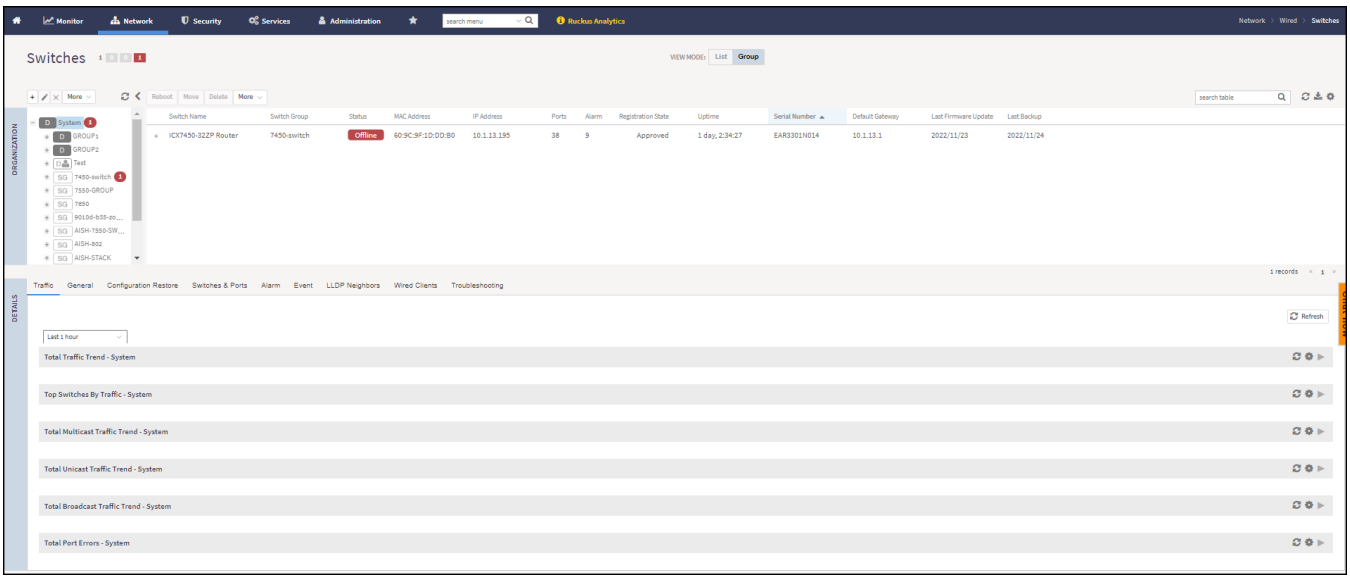
Troubleshooting Using Remote Operations

You can use the **Remote Ping** and **Remote Trace Route** options to identify issues with individual switches.

Follow these steps to troubleshoot switch issues using remote ping and traceroute.

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

   FIGURE 169 Switches

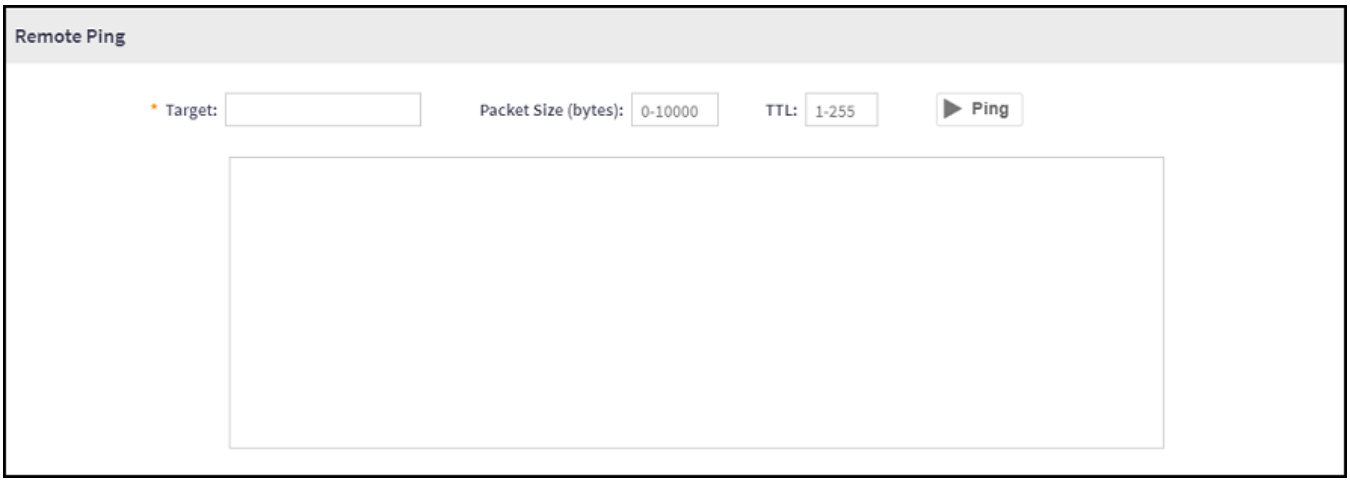


2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**.
3. In the **Details** tab, click **Troubleshooting** tab.
4. In the **Remote Ping** tab, click to display the **Remote Ping** fields.
5. Complete the following fields:
   - **Target**: Enter the IP address of the destination (target) you are checking.
   - **Packet Size**: Enter the packet size from 0-10000.
   - **TTL** (Time to Live): Enter the Time to Live from 1-255.

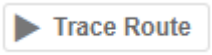
6. Click Ping icon. In the below display window you can view that a packet is discarded from the network.

   The controller pings the switch at the destination IP address provided. As shown in the following example, the results displayed include the number of data packets transmitted, received, and lost and the time required for the controller to ping the switch to establish communication.

   FIGURE 170 Pinging the switch



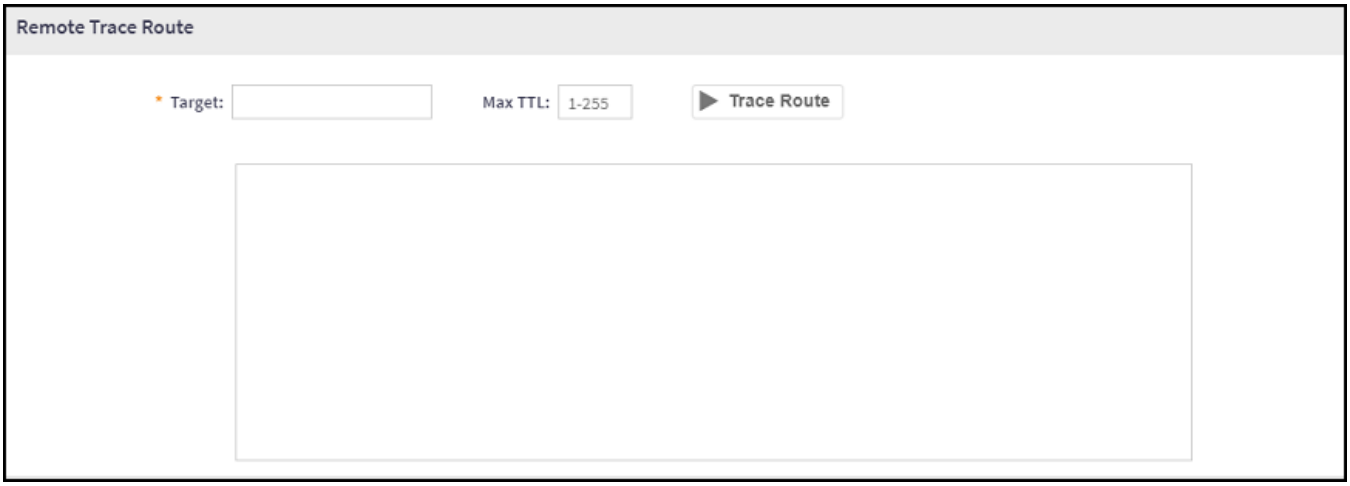
7. In the **Remote Trace Route** tab, click to display the **Remote Trace Route** fields.
8. Complete the folowing fields:
   - **Target**: Enter the IP address of the destination (target) you are checking.
   - **Max TTL**: Enter the Maximum Time to Live from 1-255.

9. Click 

icon. In the below display window you can view that a packet is discarded from the network.

   As shown in the following example, the **Remote Trace Route** page displays the IP address of the hops the packet traverses through the network between the switch and the controller.

   FIGURE 171 Tracing the packet route through the network



10. In the **Blink LED** tab, click ▼ to display the **Blink LED** fields.

    NOTE
    The Blink LED can be applied to either a single switch, or to switch in the stack by selecting an option **All**, or selecting a particular unit-id from the list.

- In **Seconds** field, enter the time in seconds and click ▶ Blink icon to enable blinking of port LEDs on switches.

    NOTE
    The value in seconds ranges from 15-120. By deafult, it is 15.

FIGURE 172 Applying Blink LED to Single Switch

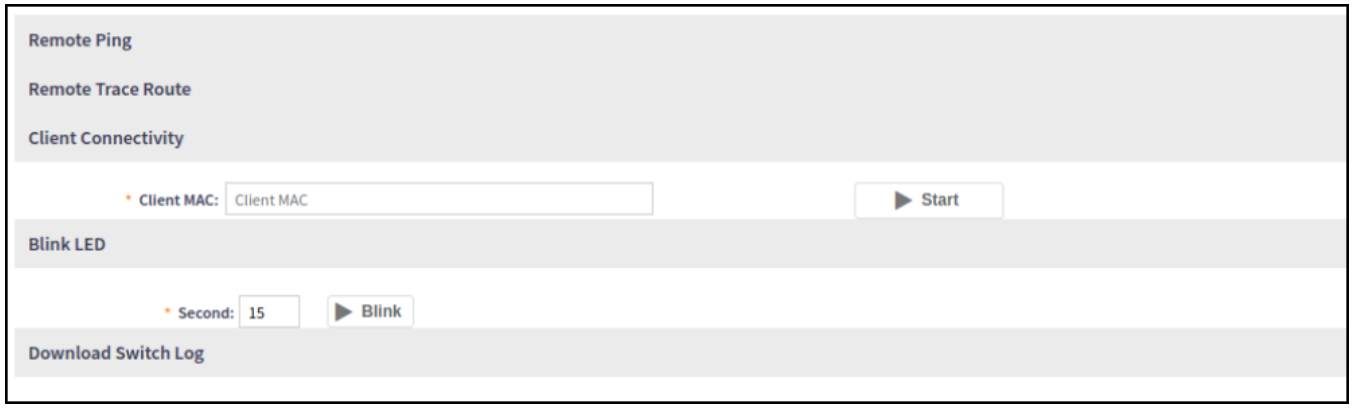
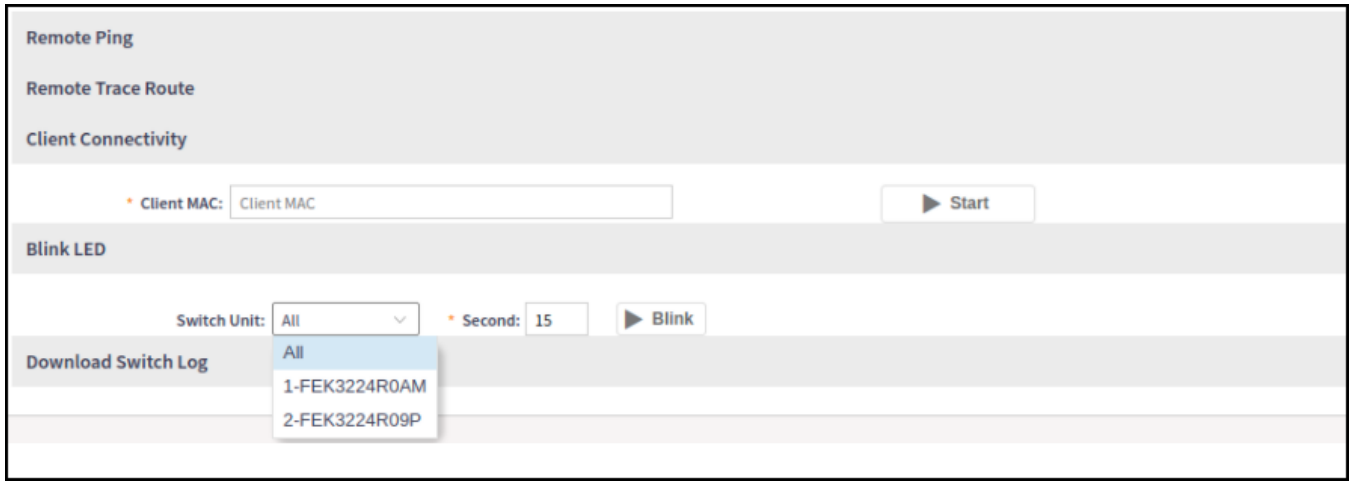


FIGURE 173 Applying Blink LED to Switch on Stack

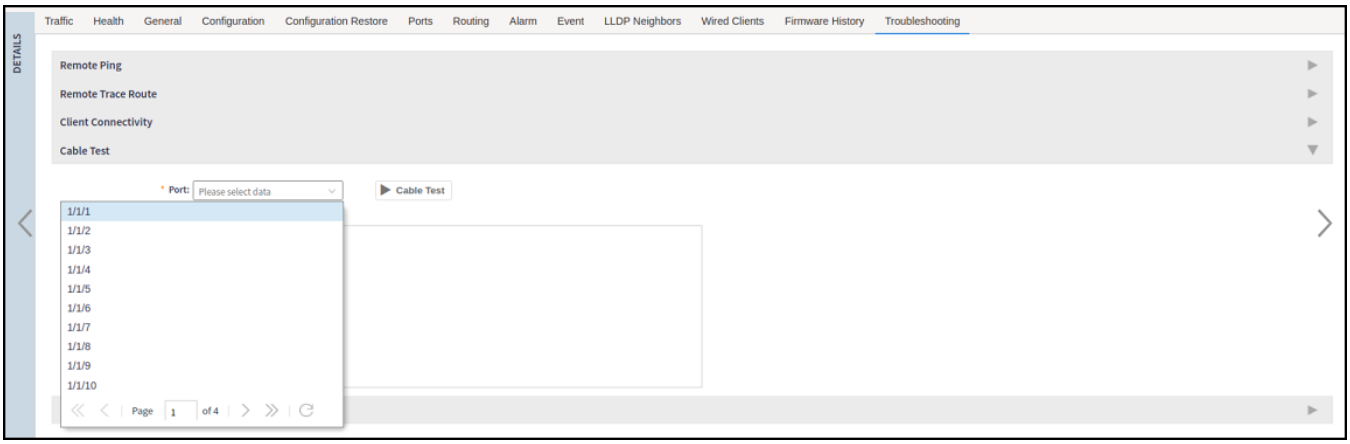


Cable Testing on ICX Ports

1. On the menu, click **Network** > **Wired** > **Switches** to display the **Switches** window.

2. In the **Organization** tab, select a **Domain** > **Switch Group** or **Switch Group** and select the **Switch**.
3. In the **Details** tab, click **Troubleshooting** tab.
4. In the **Cable Test** tab, click icon to display the **Cable Test** fields.

FIGURE 174 Clicking Troubleshooting Tab



5. Select a port from the **Port** drop down list.

   NOTE
   To execute the cable test, port speed must be set to **Auto**.

   Image

6. Click  icon.

7. A **Cable Test Message** dialog box is displayed, click **OK**.

FIGURE 175 Warning Message for Confirmation

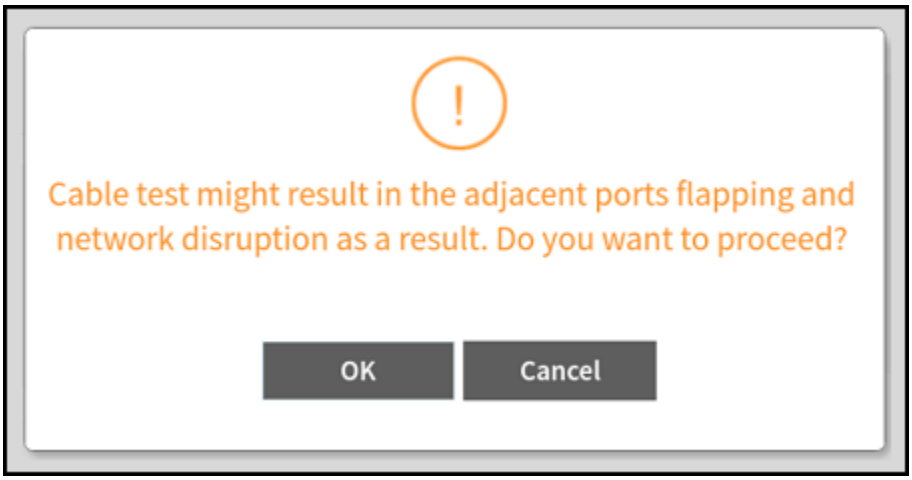


FIGURE 176 Testing Network Connectivity

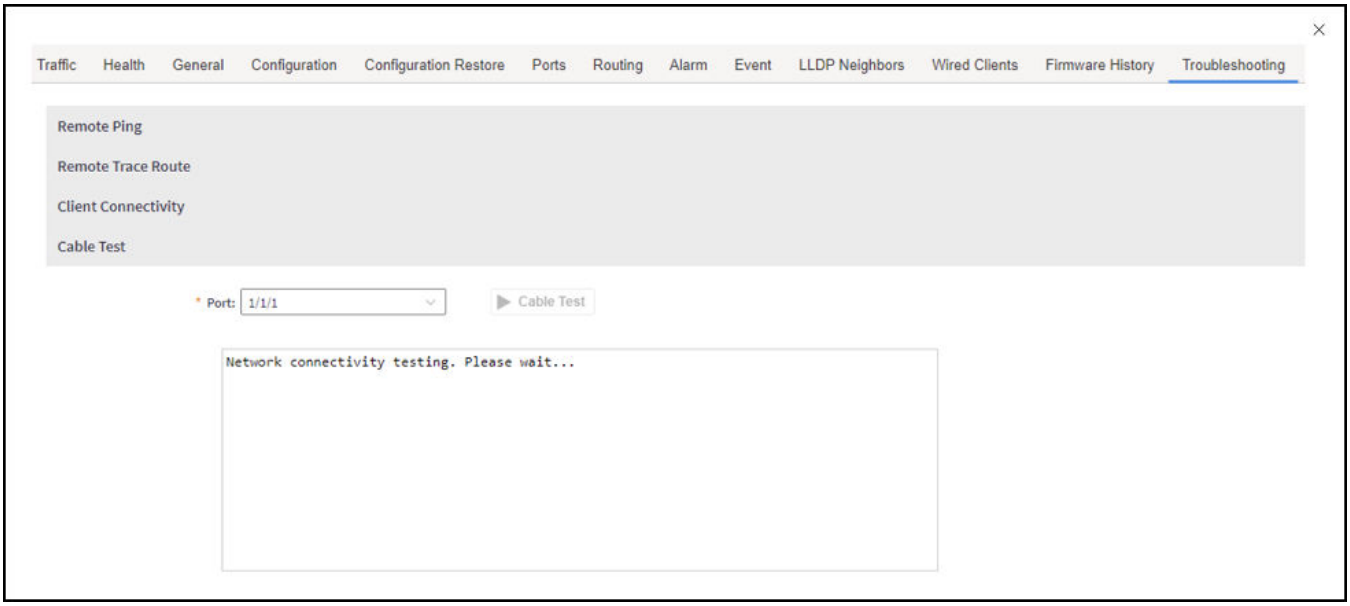
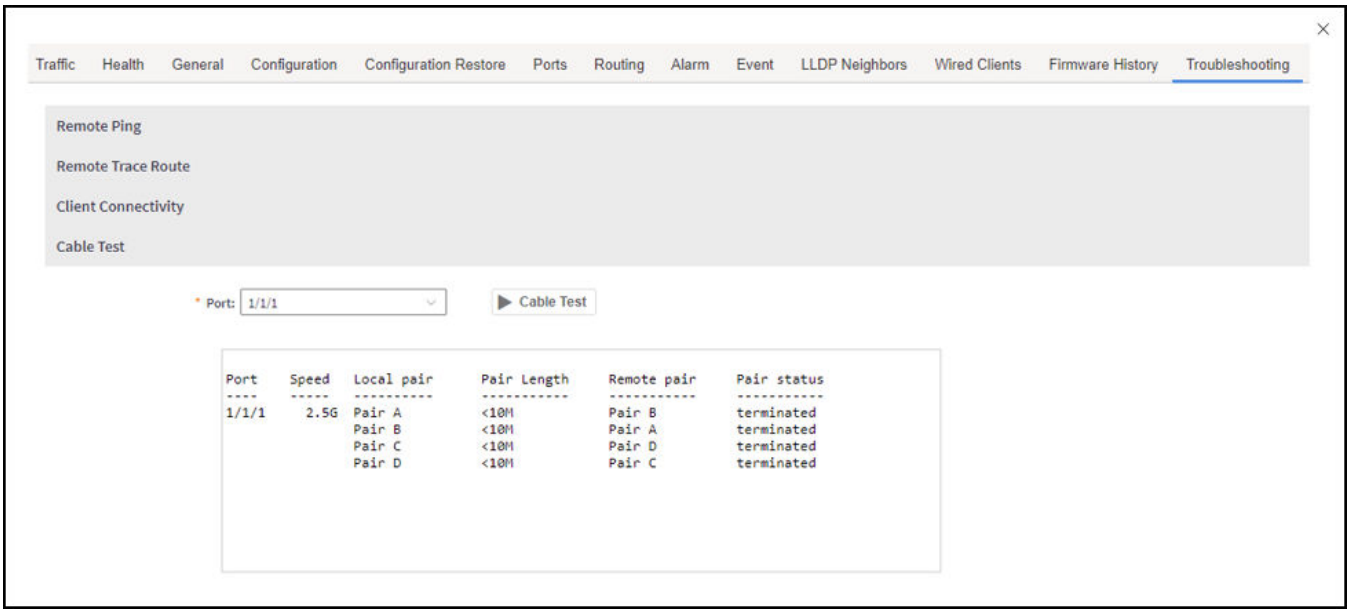


FIGURE 177 Viewing the Cable Test Report



8. If the selected port has the port speed set to **Fixed**, then an error message is displayed as below.

FIGURE 178 Displaying Error Message



Viewing Switches on the Dashboard

The wired dashboard displays detailed information about the health of the switch and displays charts illustrating traffic trends.

1. On the menu, click **Monitor** > **Dashboard** > **Wired** to display the **Dashboard** window.
2. In the **Health** tab, click System icon to display the connected switches.

   The **Settings-Health Dashboard** page is displayed.

3. From the **View Mode** , select either **Topology** or **Ball** view to be displayed on the dashboard.

FIGURE 179 Viewing Wired Dashboard - Ball



FIGURE 180 Viewing Wired Dashboard - Topology

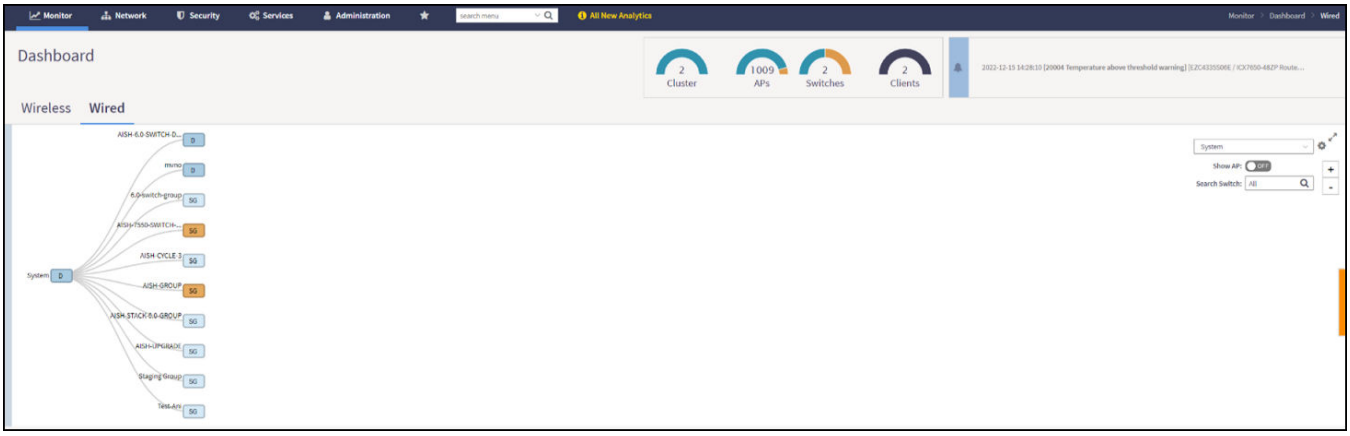


FIGURE 181 Showing Wired Devices Using Topology View Mode

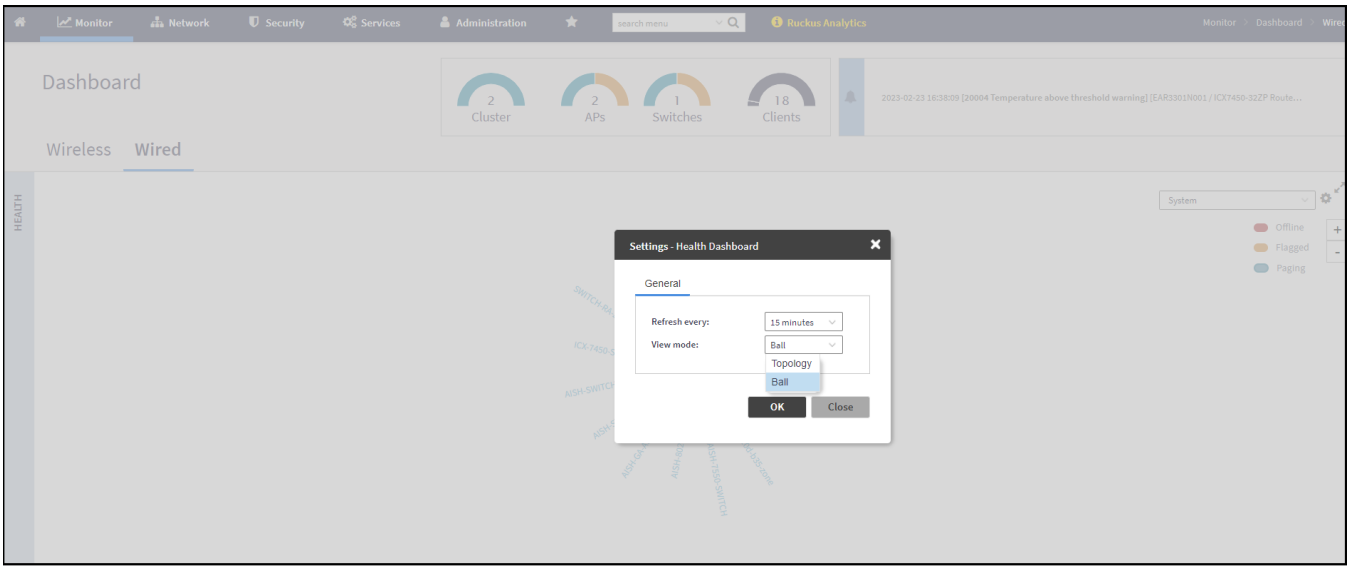
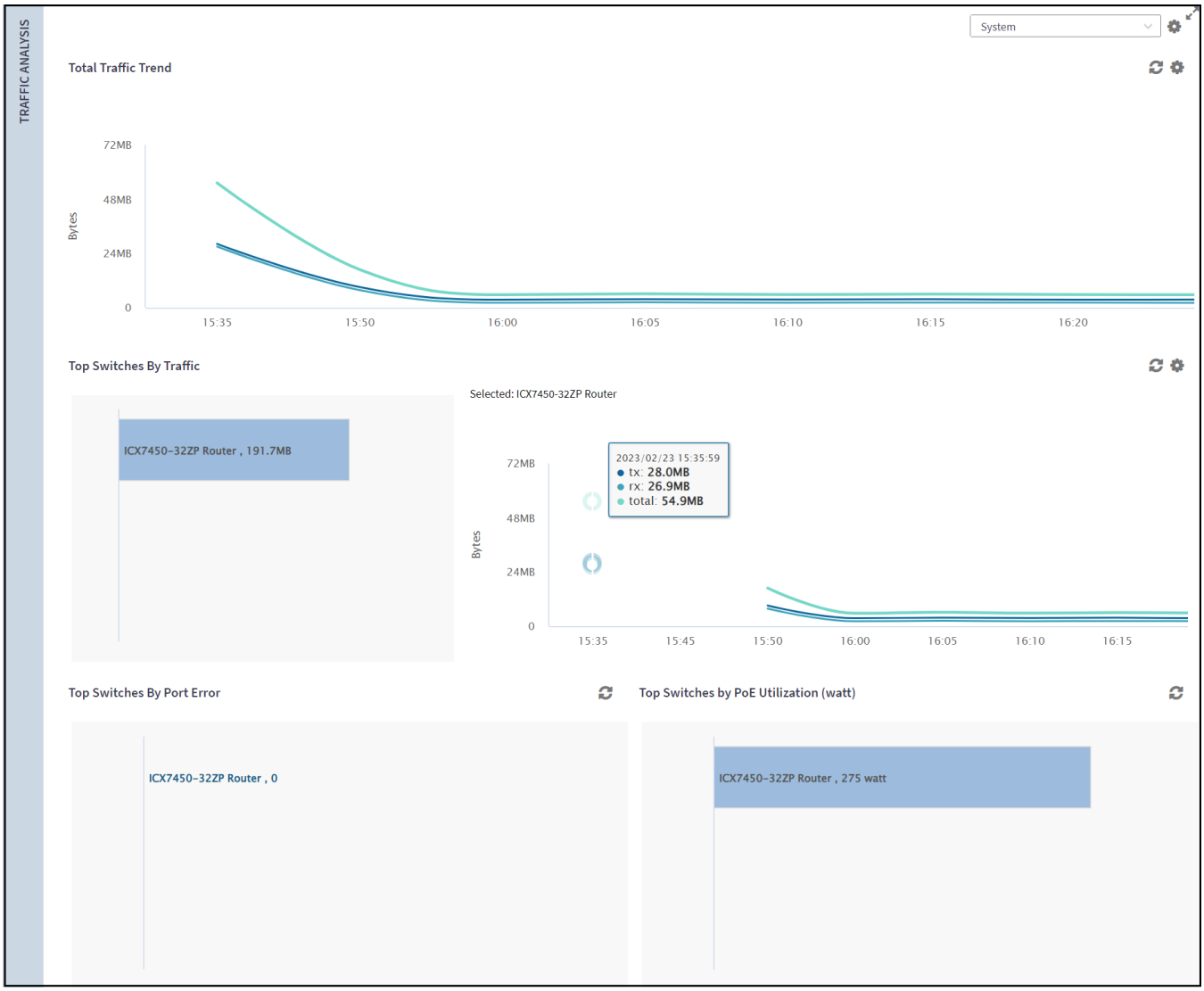


FIGURE 182 Viewing Traffic Analysis



The **Health** tab displays the number of switches that are online, offline, and flagged.

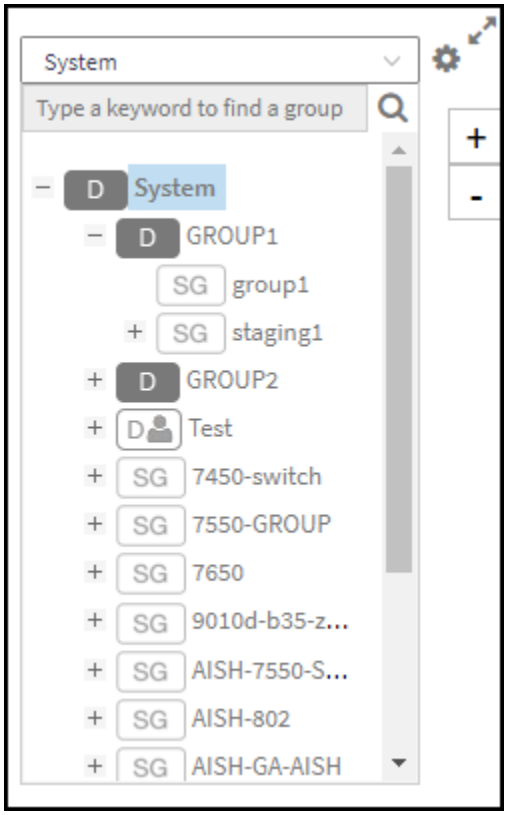
The **Traffic Analysis** tab displays the following information:

- Total Traffic Trend
- Top Switches By Traffic
- Top Switches By Port Error
- Top Switches by PoE Utilization (watt)

In the topology view mode, the **Health** pane consists of a filter combo box to display domain, sub-domain and switch group in the topology view. If you pause the pointer on a link in the topology view, the highlighted link shows the port and LAG information. If you pause the pointer on a device, the highlighted device shows device information such as name, model, MAC address, and IP address (for the switch only).

NOTE
The **Health** dashboard refreshes automatically every 15 minutes to show the latest topology view.

FIGURE 183 Showing Elements on the Health Dashboard



1 - Filter

2 - Topology Type Switch Button

3 - Search Bar



© 2023 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
https://www.commscope.com