SEL-5056

SDN Flow Controller

Instruction Manual

20200630

SEL SCHWEITZER ENGINEERING LABORATORIES

The information in this document is provided for informational use only and is subject to change without notice. Schweitzer Engineering Laboratories, Inc. has approved only the English language document.

This product is covered by the standard SEL 10-year warranty. For warranty details, visit selinc.com or contact your customer service representative.

Table of Contents

Appendix F: Learn and Lock Extension

List of Tables

List of Figures

Preface

Overview

Preface. Provides the manual overview, as well as safety and general information about the products.

Section 1: Introduction and Specifications. Introduces the SEL-5056 SDN Flow Controller. Summarizes functions and applications. Lists specifications, type tests, and ratings.

Section 2: Installation and Configuration. Discusses installation, commissioning, adoption, and administrative functions of the SEL-5056.

Section 3: OpenFlow. Explains SDN OpenFlow features supported by the SEL-5056.

Section 4: Topology, Configuration, and Telemetry. Describes how to program and configure SEL SDN technology.

Appendix A: Software and Manual Versions. Provides instructions for determining firmware version, firmware revision history, and manual revision history.

Appendix B: Events. Describes possible logs.

Appendix C: Protocol Match Criteria. Suggests the match criteria necessary for the most common control system protocols.

Appendix D: Application Permissions. Describes the permissions available on the representational state transfer (REST) interface.

Appendix E: Security. Provides the cybersecurity information.

Appendix F: Learn and Lock Extension. Describes the extension features and how to use the automation for commissioning, circuit provisioning, and network reset.

General Information

Copyrighted Software

The software included in this product may contain copyrighted software licensed under terms that give you the opportunity to receive source code. You may obtain the applicable source code from SEL by sending a request to:

Legal Department
GPL Compliance
Schweitzer Engineering Laboratories
One Schweitzer Drive
Pullman, WA 99163

Please include your return address, product number, and firmware revision.

Technical Support

We appreciate your interest in SEL products and services. If you have questions or comments, please contact us at:

Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163-5603 U.S.A.
Tel: +1.509.338.3838
Fax: +1.509.332.7990
Internet: selinc.com/support
Email: info@selinc.com

SECTION 1

Introduction and Specifications

Product Overview

Software-Defined Network

A software-defined network (SDN) is an architectural Ethernet network model that abstracts the network control plane from the network appliances that manage the data plane. An SDN has two main components:

- The flow controller
- The network appliance (SDN switch)

SEL-5056 SDN Flow Controller

The flow controller provides centralized configuration and situational awareness. It performs topology discovery, circuit provisioning, and telemetry monitoring. This constitutes what is called the control plane and includes everything that is necessary to teach the network appliances how to forward datagrams. The control plane has three main components:

- Match
- Action
- Counters

The Match component determines which control plane rules to apply to each packet entering a switch port. After the flow match determination, the Action component instructs the switch regarding what it does with the packet. Lastly, the Counters component includes sets of metrics you can use to monitor the overall status and health of the network.

Product Overview

The SEL-5056 SDN Flow Controller performs all commissioning and configuration proactively. Once the SEL-5056 configures the SDN switch, the SEL-5056 no longer needs to be online for proper network operations. The flow controller does provide detailed telemetry monitoring benefits when left online post-network configuration. There are many ways in which industrial or energy industry networks may benefit by using this SDN model, including the following:

- Reduced operational expenses because of central change control and monitoring.
- Better performance in latency and network fault-healing times.
- More efficient use of existing network assets.
- Greater situational awareness of exactly what devices are on the network and exactly what conversations each device is having.
- Improved cybersecurity with deny-by-default management and multi-layer packet inspection at each hop.

The SEL-5056 has a secure application programming interface (API), unlocking the programmability and enabling each organization to integrate the flow controller into their enterprise system and have interoperable software ecosystems.

Security

The SEL-5056 is designed for reliability and ease-of-use in the energy and utility industries. Use the SEL-5056 for central management and monitoring, including managing all deployed SDN switches as a single asset. The SEL-5056 supports strong deny-by-default cybersecurity access controls, cryptographically secure communications, and detailed log management.

Topology Discovery

Manage network topology through the SEL-5056, which discovers and displays deployed network components to ease configuration and monitoring. The SEL-5056 detects SDN switches, hosts, and links, displaying them in position of how each element connects to neighboring element. The SEL-5056 simplifies flow programming by collecting the desired network operations and automating the translation of those requirements to OpenFlow programming. This is called logical connections. The SEL-5056 has an extension that enables Learn and Lock for complete automation of commissioning and topology management, as well as complete automation of unicast circuit provisioning. The Learn and Lock extension found in the SEL-5056 enables the convenience of plug-and-play but with the purpose of engineering safety and reliability.

Host discovery is necessary before you can use logical connection automation. The SEL-5056 attempts to find unknown hosts by watching the traffic on the network and through user-directed discovery. The SEL-5056 uses both MAC and IP address information in circuit provisioning automation and removes the burden of data entry from the user.

Traffic Engineering

You can traffic-engineer and configure all deployed SDN switches through the use of the SEL-5056. Traffic engineering focuses on engineering planning, including how application-oriented communication is transmitted through the network and designed to fault tolerance. This engineering includes control over what constitutes the attributes of a traffic flow (Match), what forwarding instructions each network appliance applies to each packet as it passes through a node (Action), and the metrics collected from each switch for telemetry monitoring (Counters).

Fast Fault Recovery

Apply up-front engineering for fault tolerance, instructing each network appliance what to do when it detects a fault. This eliminates convergence times and heals faults on the next ingress packet. You can select logical connections to provide redundancy as part of the automated flow programming.

Network State Monitoring

Enable advanced analytics with the SEL-5056 network monitoring capabilities, which monitor all OpenFlow counters.

Programmatic Change Control

Use the SEL-5056 for network-wide management of change control. The SEL-5056 allows user access to all of the OpenFlow configurations and has a northbound API enabling broader software interoperability and unlocking capabilities your organization would want to develop. This level of access and control provides a fully programmable network infrastructure that can be purpose engineered to meet the demanding requirements of your critical infrastructure.

Extensions and Applications

The SEL SDN solution includes extensions and applications that bring added value to the system. Extensions are additional features in the SEL-5056. Refer to *Appendix F: Learn and Lock Extension* for more information about these extensions. Applications are standalone software applications that are installed and run separately from the SEL-5056 but work with the API of the SEL-5056 to gather information or orchestrate the configuration. SEL's suite of applications can be found on selinc.com under the product number SEL-5057.

Recommended Quick-Start Programming Steps

SEL has optimized the programming of SDN with the following three steps. Each step is described in this manual.

Step 1. Installing and commissioning the SEL-5056 and turning on and connecting the SDN switches to the computer running the SEL-5056

Step 2. Adopting all network elements

Step 3. Circuit provisioning by using logical connections

The adoption process is the act of identifying the physical assets and connections and authorizing those physical elements to be used in programming. Logical connections is automated circuit provisioning where the SEL-5056 calculates and configures the OpenFlow settings from simplified user instructions.

SEL-5056 Product Features

Robust Topology Discovery and Management. Automated, directed, and offline topology discovery and management capabilities provide full control of situational awareness and programmability with simplified network deployment options.

Circuit Provision Orchestration. Provides circuit provisioning through simply selecting the source and destination, as well as automated flow configuration and redundancy path planning.

Ease of Use. Simplifies complex settings by using an application-focused design to construct each network according to the applications running on the network.

Holistic Network Visibility. Allows viewing and management of network appliances as a single asset. Automated network topology discovery allows for near real-time situational awareness.

Learn and Lock. Fully automate commissioning and unicast circuit provisioning.

Scalable Network Deployments. Manages small or large networks with a single SEL-5056 installation.

Secure Configuration. Provides situational awareness and strong cybersecurity through user-based access controls, encrypted communication, and detailed audit logging.

Syslog. Performs log management through Syslog for centrally automated collection and redundancy.

Supported Operating System. Provides high-quality, service-focused performance with Microsoft Windows Server 2016 Standard.

X.509 Certificate. Supports secure, mutually authenticated communication between the switch and the flow controller and manages keys through X.509 certificates.

Central Authentication. Uses Lightweight Directory Access Protocol (LDAP) to centrally manage and authenticate authorized users.

Back Up and Restore. Generates backup images for incident recovery and quickly restores the system to the saved backup.

Secure Application Registration. Scale out the software ecosystem safely with secure application registration to the northbound API.

General Information

Communication

Use the SEL-5056 to commission, configure, and monitor the SEL SDN switches. The SEL-5056 can manage OpenFlow compatible switches of other suppliers. Interoperability between flow controllers and switches are compliant with OpenFlow 1.3 specifications.

SEL-5056 Requirements

The SEL-5056 is the preferred OpenFlow controller for the SEL SDN switches. All network configurations and settings are managed through the SEL-5056. The SEL-5056 is available for order either as a Windows application or preinstalled on an SEL-3355 Computer running Windows Server 2016 Standard.

Table 1.1 Minimum System Requirements

Operating system	Windows Server 2016 Standard
Hard disk drive	250 GB
Processor speed	2.5 GHz
RAM	8 GB
Screen resolution[a]	1920 x 1080
Browser	Google Chrome version 80

[a] Recommended.

Table 1.2 Software Requirements

.NET	4.6.2
WinPcap	4.1.3
Microsoft Visual C++ Redistributable	Version 12.0.30501.0

SEL-5056 Specifications

Operating System Support

Windows Server 2016 Standard

General

Protocols

OpenFlow 1.3
Transport Layer Security (TLS)
Syslog (UDP and TLS)
Hypertext Transfer Protocol Secure (HTTPS)
Secure REST
Lightweight Directory Access Protocol (LDAP) over StartTLS

Security

X.509 certificate
User-based accounts

Monitoring

Windows Event Viewer
Syslog

Browser

Google Chrome version 80 and higher (recommended)

SECTION 2

Installation and Configuration

SEL-5056 Service

Introduction

The SEL-5056 SDN Flow Controller runs as a Windows service. The SEL-5056 is configured through the settings tool found in the Windows tool tray. The service starts automatically upon startup of the Windows machine. You can stop it and start it manually by using the Windows Task Manager. The first time the SEL-5056 starts during installation, a commissioning window appears asking for the first user account to be created with the Security Administrator role. The SEL-5056 service can fail to run if the SEL-5056 settings are invalid or the configured port is already bound to another process.

Instructions

Installing the SEL-5056

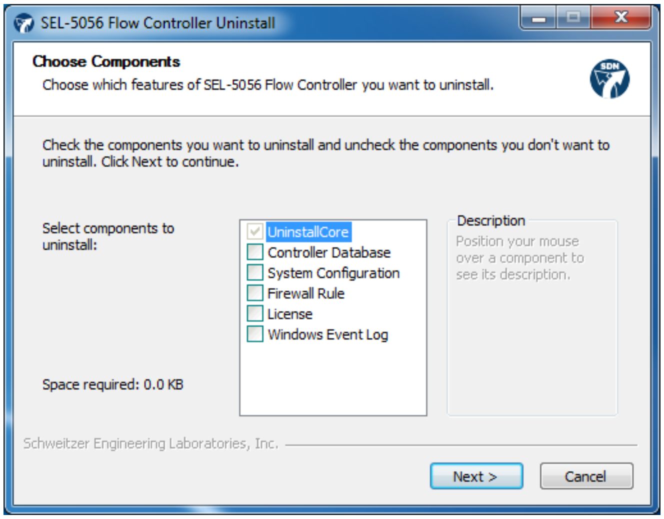
Copy the SEL-5056 installer to a location on your computer. Run the installer with Administrative permissions and follow the onscreen instructions.

If WinPcap is already installed with version 4.1.3 or higher, you can cancel its installation and proceed with the remainder of the SEL-5056 installation.

Upgrading the SEL-5056

To upgrade an existing version of the SEL-5056 on your computer, run the same installer as a new installation. The installer detects a version of the SEL-5056 already installed, and you will be prompted to uninstall the previous version before the installer can continue. You may want to back up the current database in case you need to revert back to the current version of the SEL-5056 at a later time. The SEL-5056 must be upgraded in the release order to maintain all configurations and settings.

After selecting **Yes** to uninstall the previous version, you are prompted to select which portions of the SEL-5056 you want to uninstall. Select all of the check boxes for a clean upgrade (i.e., all current configurations will be erased). To upgrade your current database while keeping all of your SDN configurations, do not select the **Controller Database** check box. To keep your current SEL-5056 settings, do not select the **System Configuration** check box.



SEL-5056 Flow Controller Uninstall

Choose Components

Choose which features of SEL-5056 Flow Controller you want to uninstall.

Check the components you want to uninstall and uncheck the components you don't want to uninstall. Click Next to continue.

Select components to uninstall:

- ☑ UninstallCore
- □ Controller Database
- □ System Configuration
- □ Firewall Rule
- □ License
- □ Windows Event Log

Description

Position your mouse over a component to see its description.

Space required: 0.0 KB

Schweitzer Engineering Laboratories, Inc.

Figure 2.1 SEL-5056 Flow Controller Uninstall Prompt

Downgrading the SEL-5056

The SEL-5056 does not support downgrading versions. If you want to downgrade your present version you can uninstall the software and install the desired version. You can then import any database configuration files you previously exported from this version. You cannot downgrade database configurations from newer versions to previous versions.

Uninstalling the SEL-5056

There are two methods for uninstalling the SEL-5056:

- ➤ Rerun the SEL-5056 installer
- ➤ Use the uninstall program tool in Windows

Starting the SEL-5056 Service

If the SEL-5056 service is not running, you can start the software by using one of the following options:

- ➤ The SEL-5056 Service Settings Tool
- ➤ The Windows Task Manager

Stopping and Restarting the SEL-5056 Service

You can use the Windows Services manager to stop or restart the SEL-5056 service, or you can select **Restart SEL-5056 Service** from the Settings Tool menu.

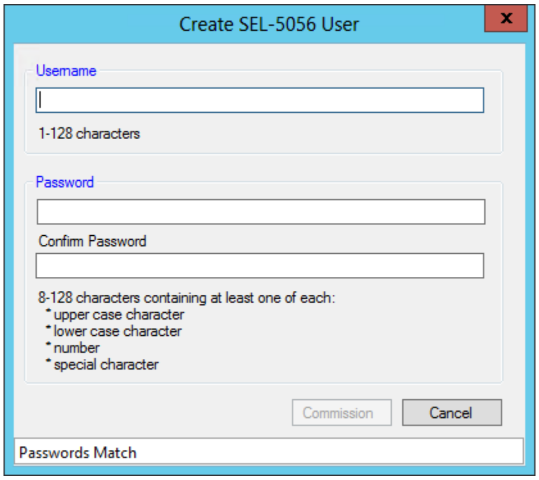
Commissioning the SEL-5056

The SEL-5056 service must be commissioned before first use. If the SEL-5056 is not commissioned, you must commission it before logging in. The SEL-5056 can be installed in a commissioned state if its database contains a user. The SEL-5056 must be recommissioned if the database is deleted.

A username and password are the only requirements for commissioning the SEL-5056. The username must be 1 to 128 printable ASCII characters, and the password must be 8 to 128 printable ASCII characters with at least one uppercase character, one lowercase character, one number, and one special character.

Steps

Step 1. A Create SEL-5056 User dialog box appears. If this does not automatically display, go to the SEL-5056 icon in the Windows tool tray, right-click it, and select **Settings**.



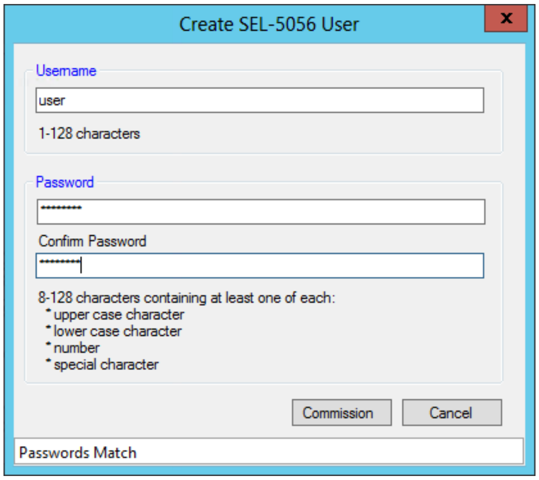
1-128 characters

8-128 characters containing at least one of each:
- upper case character
- lower case character
- number
- special character

Passwords Match

Step 2. Enter the username and password for the local Security Administrator account.

- ➢ Reenter the password into the Confirm Password box.
- ➢ If the username and password are correctly formatted, the Commission button is enabled.
- ➢ Select **Commission** to commission the SEL-5056.



Username: user

1-128 characters

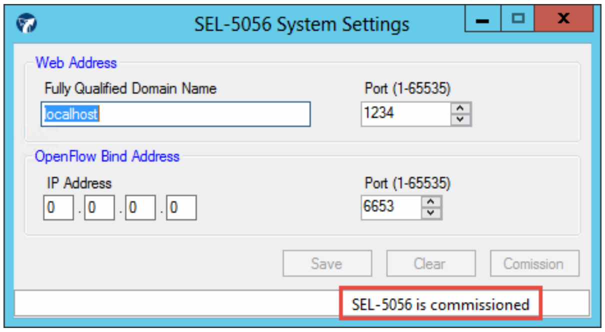
Password: ********

Confirm Password: ********

8-128 characters containing at least one of each:
- upper case character
- lower case character
- number
- special character

Passwords Match

If the commissioning is successful, “SEL-5056 is commissioned” displays at the bottom of the SEL-5056 System Settings window.



Web Address

Fully Qualified Domain Name: localhost

Port (1-65535): 1234

OpenFlow Bind Address

IP Address: 0 . 0 . 0 . 0

Port (1-65535): 6653

SEL-5056 is commissioned

Service Settings Tool

To access Settings Tool after commissioning, right-click the icon located in the notification area of the Windows taskbar, typically found on the right side and represented by an up arrow, and select **Settings**.

Accessing the SEL-5056 Web Interface Remotely

You can access the SEL-5056 web interface remotely by setting the web address fully qualified domain name (FQDN) to the IP of one of the interfaces on the host machine, or the name of the host machine, and the corresponding port to an unused port on the machine. For example, if the computer name is **mymachine.mydomainname** and you want to connect to Port 10001, set the hostname and port to the following:

- FQDN: **mymachine.mydomainname**
- Port: **10001**

You can log in to the SEL-5056 by using the following web address:

https://mymachine.mydomainname:10001/

The Firewall settings of the SEL-5056 host machine may need to be configured.

Service Settings

The Windows service has four configurable settings, listed in *Table 2.1*. Use the settings tool to view or modify these. The user must have Administrator permissions to modify these settings.

Table 2.1 SEL-5056 Service Settings

Setting Group	Setting Name	Description	Valid Values	Default Value
Web Address	Hostname	The hostname or IP address for hosting the web interface	localhost or the fully qualified domain name or IP address of one of the interfaces on the SEL-5056 host computer	localhost
	Port	The TCP/IP port of the web interface	1 to 65535	443
OpenFlow Bind Address	IP Address	The IP address to which the SEL-5056 binds to listen for OpenFlow messages	0.0.0.0 or the IP address of any interface on the SEL-5056 host computer	0.0.0.0
	Port	The TCP/IP port to which the SEL-5056 binds to listen for OpenFlow messages	1 to 65535	6653

If the web address hostname is localhost, the web interface can only be accessed on the SEL-5056 host machine. If the web address is not localhost, access the webpage from a remote machine by navigating to **https://[hostname]:[port]**, where Hostname is the web address hostname or FQDN and Port is the web address port. The SEL-5056 listens for OpenFlow messages and SEL SDN switch autodiscovery messages on all network interfaces that were present when the SEL-5056 service last started if the IP Address setting is left at 0.0.0.0. If the SEL-5056 is set to a specific OpenFlow Bind Address, the service only listens to OpenFlow connections on that address.

User Interface

All user access to the SEL-5056 is through a web interface. Google Chrome is the recommended browser to achieve the best graphics results. The web interface is described throughout this manual as part of each feature description. There is also an application programming interface (API) described later in the manual.

Configuration Storage

The SEL-5056 holds all settings of the SEL-5056 in a database. The database is stored in C:\ProgramData\SEL\SEL-5056\Database\.

Back Up and Restore

The SEL-5056 provides the capability to generate and export a backup copy of the database. This copy contains the configuration and public security certificates for all switches in the system. You can generate backups that are encrypted or plaintext. To create an encrypted backup, enter a password in the field before selecting the action button to generate a backup. To create a plaintext backup, leave the password field blank. SEL recommends saving the backup files on a separate machine. Service settings and licenses are not stored in the backup.

Restoring the SEL-5056 is as simple as importing a saved copy into the Backup/ Restore page in the web management interface. You can restore a database with a database of the same version or one version earlier than the current version of the SEL-5056 service. Once restored, the SEL-5056 removes all previous configurations and only has the configurations associated in the restored database. Backup and restore actions are managed through the web management interface.

To restore from an encrypted backup, enter the same password that was created when the file was generated, and then choose the backup .zip file and select **Restore**. To restore from a plaintext backup, leave the password field blank.

X.509 Certificates

The SEL SDN solution uses cryptographically secured communication and uses X.509 certificates to establish trust. *Figure 2.2* shows the trust relationships that must be established for the system to communicate.

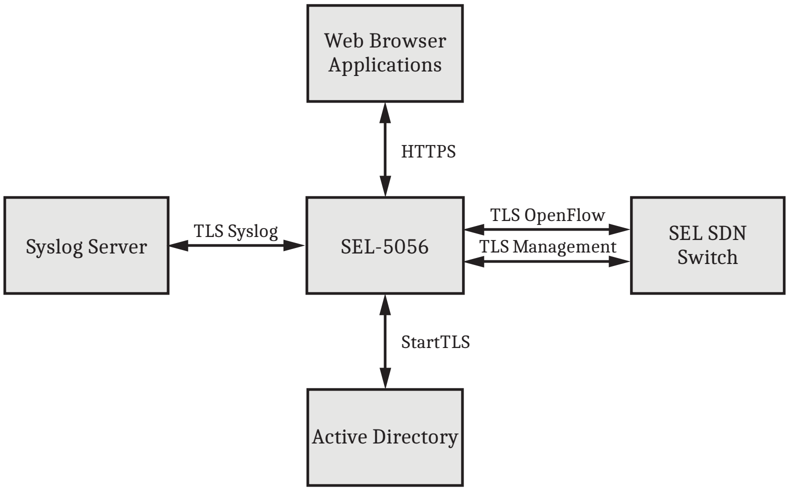


Figure 2.2 Secured Components

Certificates bind an identity to a set of cryptographic keys. The SEL-5056 uses Transport Layer Security (TLS) protocol for data transport. The SEL-5056 can self-generate all the certificates needed for operations, or you can upload external certificates to be used. When uploading certificates there are three options you can select:

1. Trusted
2. Web Server
3. Internal Certificate Authority (CA)

Trusted certificates are used for Syslog, Applications, and Active Directory. Web Server certificates are used for the SEL-5056 web server. Internal CA certificates are used to generate certificates used to commission SEL SDN switches.

Table 2.2 lists the SEL-5056-generated certificate profiles.

Table 2.2 SEL-5056 Certificate Profiles

Standard	X.509
Version	3
Validity period	20 years
Subject name	<root CA>
Public key algorithm	RSA
Certificate signature algorithm	SHA256 with RSA
Extensions	None
Supported file extensions for import	.pfx or .pem

Uploading Certificates

When uploading a new root certificate or web certificate that is generated by an external CA, you must upload a certificate that has the public and private portions of the certificate. When uploading a trusted certificate, only the public portion must be uploaded.

Certificate Usage When Adopting New Switches

When you adopt a new SEL SDN switch, the SEL-5056 generates two new Base64 encoded .pem certificates and sends the public and private portions of these certificates to the newly adopted switch. The first certificate is used for the OpenFlow connection between the controller and the switch; the switch uses this certificate to identify itself to the controller. The second certificate is used for the management interface between the SEL-5056 and the switch; this certificate is the communications channel the SEL-5056 uses for commissioning non-OpenFlow management. The SEL-5056 also sends the public portion of its own root certificate to every adopted switch, allowing the switch to securely communicate with and authenticate the controller. The controller stores a copy of the public portion of each certificate for each of the adopted switches, so it can securely communicate with and authenticate each switch.

Updating or Revoking Certificates

The SEL-5056 supports revoking certificates through the web interface. Certificates will also be revoked if they expire. To update the certificates used for the root or web, the SEL-5056 service requires a restart. To update a certificate used for OpenFlow or management interface between the SEL-5056 and an SEL SDN switch, you must unadopt and readopt the switch.

Parts of the Web Interface

The web interface is comprised of several pages, each containing a navigation menu, page title bars, a center pane, and a right pane. The currently logged in username and role of the user is displayed in the top right corner. The Submit button in the top right corner must be used to commit any setting changes to the database. Navigating away from the page before selecting Submit may result in the loss of changes. The software version is displayed at the bottom left corner on all pages.

Navigation Menu

The navigation menu running down the left side of the page contains links to each page available in the web interface. These pages are grouped into categories based on function, which can be either administration, network configuration, or diagnostics. Only the pages for the current category are displayed.

The navigation menu starts in the expanded view. In the condensed view, the navigation menu only shows the page icons.

Feedback Messages

The user interface (UI) uses toast messages to display any feedback messages from the SEL-5056. If the action was successfully submitted, the toast message is green and displays the Success message. If the toast message is red, there is an error and the message will explain the issue.

Table Columns (Except for the Flow Entries Page)

If an ⌄ icon is present to the right of a column name, one or more of the following actions may be available:

- ➤ Sort ascending
- ➤ Sort descending

The column for the action icons contains only the Hide Column action.

Resizing a Column

To resize a column, select either the left or right side of the column header cell and drag left or right.

Table Rows

Action Icons

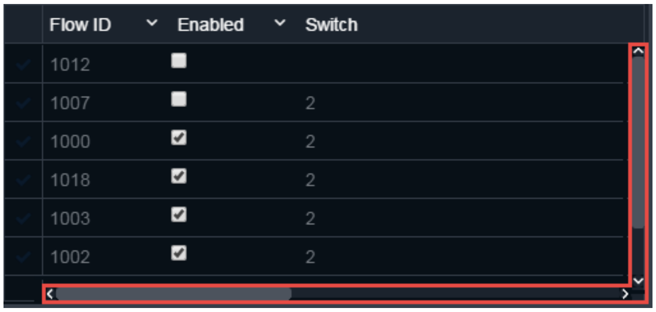
Table 2.3 Action Icons

Icon	Name	Description
🗑	Delete	Queues the entry to be deleted once the Submit button is selected
⤓	Keep Local Changes	Changes the updated configuration back to the values represented in your webpage. This is when another user has made changes to the configuration.
⤒	Take Server Changes	Takes the updated configuration and updates the webpage you are watching. This is when another user has made changes to the configuration.
📋	Copy	Creates an exact copy of all of the settings of the selected row and puts them into a new row of the table.
○	Undelete	Removes the delete action queued

If the Actions column is present, one or more of the action icons listed in *Table 2.3* may be available.

Scroll Bars

Each pane and table supports Scroll bars you can use to scroll vertically and horizontally across a table or pane that does not fit in the view. *Figure 2.3* provides an example view of the Scroll bars.



Flow ID ⌄	Enabled ⌄	Switch
1012	□	
1007	□	2
1000	☑	2
1018	☑	2
1003	☑	2
1002	☑	2

Figure 2.3 Web Interface Scroll Bars

Roles

Roles determine access to pages. You can have more than one role, but you can only log in with one role at a time. When attempting to access pages to which you do not have permissions, the SEL-5056 will ask you to log in again at the new role. To change roles, log out and log back in with the desired role. *Table 2.4* lists the three roles the SEL-5056 supports.

Table 2.4 Role List

Role	Description
Security Administrator	Create users, register applications, set usage policy, log settings, manage LDAP servers, back up, and restore
Permission Level 3	Network Engineering
Monitor	View status, events, logs, and diagnostics

Table 2.5 lists the roles permitted to access each SEL-5056 page.

Table 2.5 Role Permissions for Each Page

Menu	Page	Role[a]		
		Security Administrator	Permission Level 3	Monitor
Administration	Application Management	✔	✘	✘
	Authentication Services	✔	✘	✘
	Backup	✔	✘	✘
	Log Settings	✔	✘	✘
	My Account	✔	✔	✔
	Usage Policy	✔	✘	✘
	User Accounts	✔	✘	✘
	X.509 Certificates	✔	✘	✘
Configuration	Topology	✘	✔	✔
	Flow Entries	✘	✔	✘
	CST Entries	✘	✔	✘
	Group Entries	✘	✔	✘
	Meter Entries	✘	✔	✘
	Configuration	✘	✔	✘
	Adoption Settings	✘	✔	✘
	VID Reservation	✘	✔	✘
Diagnostics	Counters	✘	✔	✔

[a] Check = allowed; X = denied.

Time-Outs

You are automatically logged out after an amount of inactivity, depending on your logged-in role according to *Table 2.6*.

Table 2.6 Web Inactivity Time-out

Role	Time-out (Minutes)
Security Administration	15
Permission Level 3	
Monitor	No inactivity time-out

Undoing Settings Changes

Refreshing or navigating away from a page discards any changes you made after you last submitted the page.

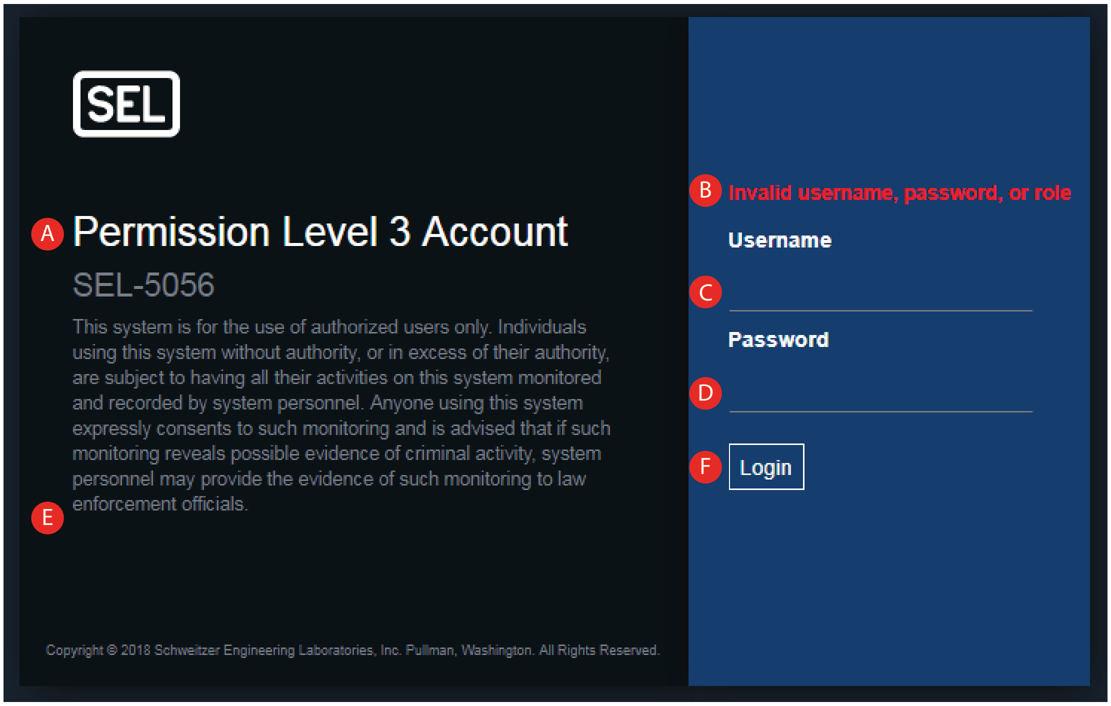
Using the Web Interface Concurrently

The SEL-5056 supports as many as 25 concurrent users. If one user edits an object on the same page as another user, the second user sees the change.

Landing and Login Pages

To log in to the SEL-5056, you must first select a role on the landing page and then establish your credentials in the login page. To change roles after you have selected one but before you log in, select the SEL logo in the top left to return to the role selection page.

Login Page (User)



Permission Level 3 Account

SEL-5056

This system is for the use of authorized users only. Individuals using this system without authority, or in excess of their authority, are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity, system personnel may provide the evidence of such monitoring to law enforcement officials.

Invalid username, password, or role

Copyright © 2018 Schweitzer Engineering Laboratories, Inc. Pullman, Washington. All Rights Reserved.

(A) **User Role:** User role the user is attempting to log in to.

(B) **Feedback Bar:** Displays any errors during feedback.

(C) **Username:** Input for username.

(D) **User Password:** Input for password.

(E) **Usage Policy:** Configured usage policy (see *Usage Policy on page 2.17*).

(F) **Login Button:** Submits user credentials to the controller.

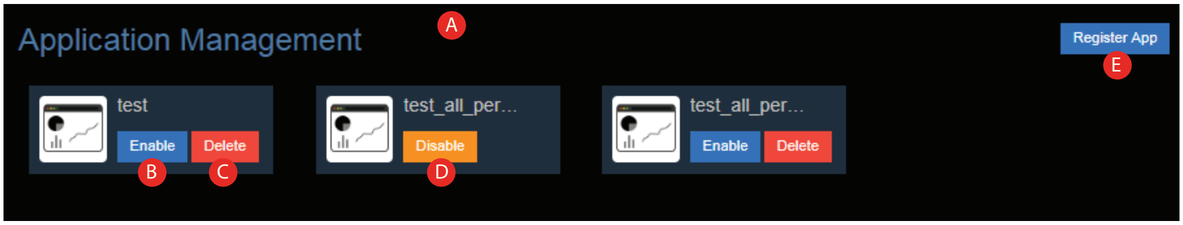
Figure 2.4 Login Credentials Page

SEL-5056 Administration Pages

Application Management

Use the Application Management page to register, enable, disable, and delete applications that connect to the SEL-5056 on the northbound representational state transfer (REST) API. You need the Security Administrator role to register applications. Applications that are registered or applications that use login credentials can access the SEL-5056 API.

Default View



(A) List of Registered Applications.

(B) **Enable Button:** Application is disabled, select **Enable** to enable.

(C) **Delete Button:** Delete the application and remove it from the SEL-5056.

(D) **Disable Button:** Application is enabled, select **Disable** to disable the application. The application can no longer perform any actions.

(E) **Register App Button:** A step in the application registration process.

Figure 2.5 Application Management Page

Application Settings Pane

If an application is selected in the list, the application settings pane appears on the right side of the window. The settings are divided into two tabs:

- Description (provided by the application at registration)
- Permissions (requested by the application at registration)

Instructions

Registering an Application

Settings

- Public X.509 certificate from the application
- URL to access the registration endpoint of the application

Steps

Step 1. Upload the public X.509 certificate to the X.509 Certificates page with a purpose of Trusted.

Step 2. Select the **Register App** button on the Application Management page and enter the URL for the registration endpoint of the application.

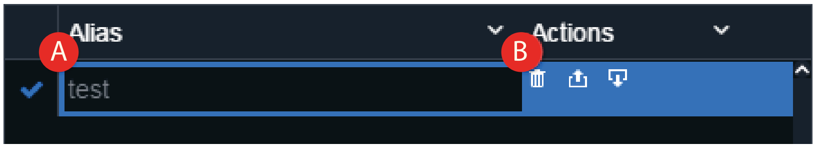
If the registration is successful, the application is added to the registration application list. Applications may have their own steps to register with the SEL-5056 and you must follow those before a mutual registration is successful.

Authentication Services

Use the Authentication Services page to configure LDAP configuration services. The SEL-5056 supports LDAP over SSL (StartTLS). The Security Administrator role is required to add authentication services.

Authentication Services Table

Figure 2.6 shows the configured authentication services.



	Alias	Actions
✓	test	

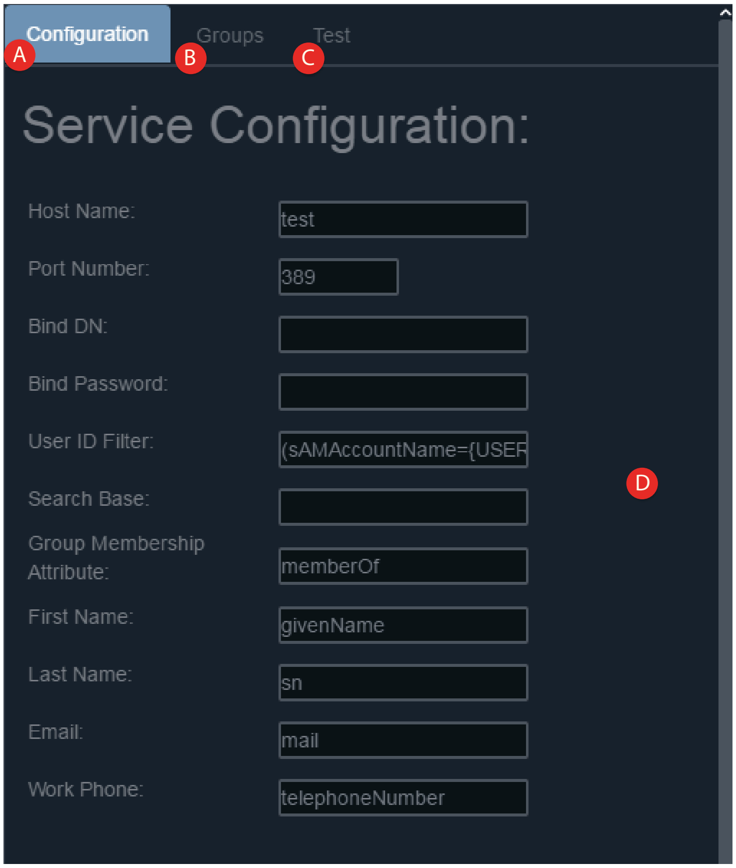
(A) **Authentication Services Setting:** Column for the name of the authentication service.

(B) **Actions Icons:** Set of available action icons.

Figure 2.6 Authentication Services Table

Authentication Services Settings

Figure 2.7 contains all settings for the LDAP authentication services.



Service Configuration:

Host Name:	test
Port Number:	389
Bind DN:	
Bind Password:	
User ID Filter:	(sAMAccountName={USER
Search Base:	
Group Membership Attribute:	memberOf
First Name:	givenName
Last Name:	sn
Email:	mail
Work Phone:	telephoneNumber

(A) **Configuration Tab:** Displays the Configuration settings for an authentication service.

(B) **Groups Tab:** Displays the group maps for an authentication service.

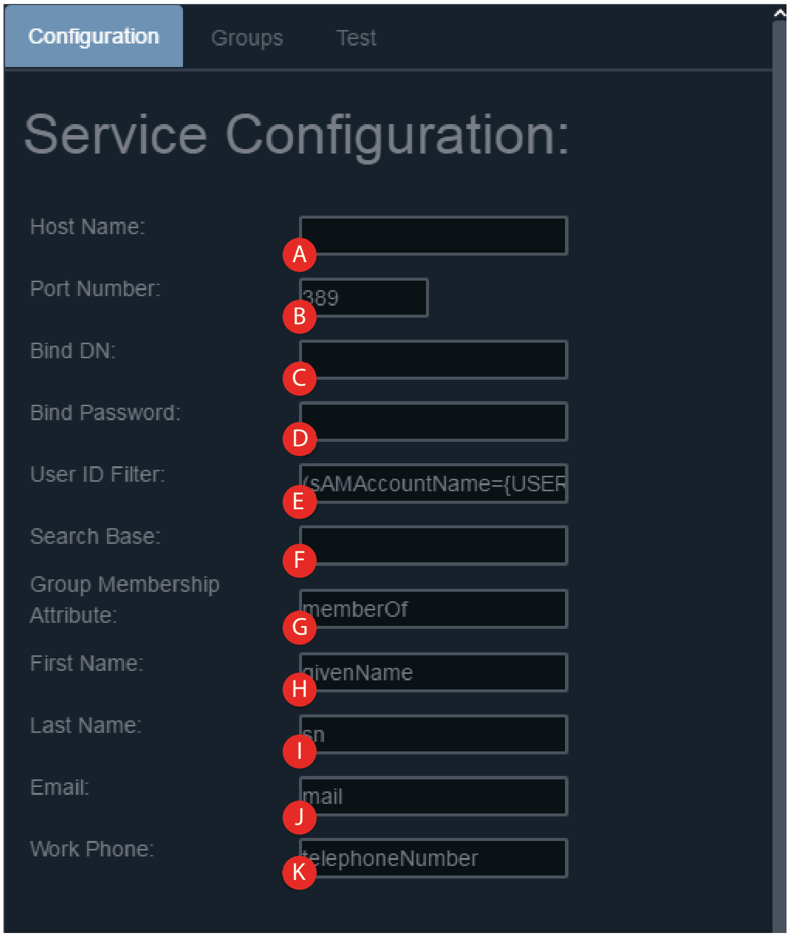
(C) **Test Tab:** Displays settings to perform a test to confirm success binds to the LDAP server.

(D) **Tab Settings:** Displays the settings for the tab.

Figure 2.7 Authentication Services Settings

Configuration Tab

Figure 2.8 contains all the configuration settings for the LDAP authentication services.



Service Configuration:

Host Name:

Port Number: 389

Bind DN:

Bind Password:

User ID Filter: (sAMAccountName={USER

Search Base:

Group Membership Attribute: memberOf

First Name: givenName

Last Name: sn

Email: mail

Work Phone: telephoneNumber

(A) **Host Name Setting:** Hostname of the LDAP server.

(B) **Port Number Setting:** Port number on which the LDAP server is listening.

(C) **Bind DN Setting:** Bind distinguished name.

(D) **Bind Password Setting:** Label that identifies users of the system.

(E) **User ID Filter Setting:** Subsection of the directory to search for authorized users.

(F) **Search Base Setting:** Label to search for associated memberships for the user.

(G) **Group Membership Attribute Settings:** Optional owner information.

(H) **First Name Attribute Setting:** Optional owner information.

(I) **Last Name Attribute Setting:** Optional owner information.

(J) **Email Attribute Setting:** Optional owner information.

(K) **Work Phone Attribute Setting:** Optional owner information.

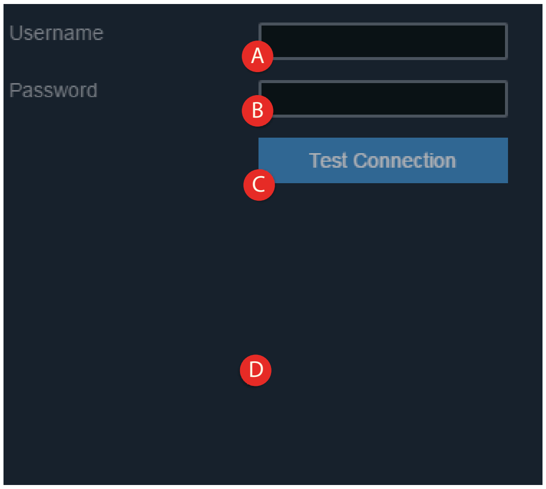
Figure 2.8 Authentication Services Configuration Tab

Groups Tab

The Groups tab contains settings for creating and managing group maps and mapping user distinguished names (DNs) to the SEL-5056 roles. Selecting the plus sign in the group mappings adds a new map. When selecting the plus sign in the map, you can select the roles in the SEL-5056 that you want to map to a distinguished name. Enter the full DN that you want to map the selected roles. Each DN can be only entered once and can be mapped to one or more roles in the SEL-5056.

Test Tab

This tab allows you to test the selected authentication service if the status is Success.



(A) **Username:** Username to test.

(B) **User Password:** Password of username to test.

(C) **Test Connection Button:** Starts the test service.

(D) **Test Results:** Displays the test results after running the test.

Figure 2.9 Authentication Services Test Service

An LDAP administrator is the best source for some of this information. See *Appendix D: Lightweight Directory Access Protocol (LDAP)* for a form you can give to the LDAP administrator to obtain this information. To delete an authentication service, a group mapping, or role from a group mapping, use the trash can action icon.

Log Settings

Use the Log Settings page to configure logging for Syslog and to the Window Event. When setting the severity threshold, the lower levels have a higher severity so when you select the desired severity level, all events at that severity and higher will be logged to the destination. When you use Syslog, there are two option with UDP delivery or TCP that uses TLS secure delivery. When using TCP/TLS, you must also have the X.509 certificate installed from the Syslog server as a trusted certificate into the SEL-5056.

Instructions

Adding a Syslog Server

Settings

Table 2.7 Settings for Adding a Syslog Server (Sheet 1 of 2)

Setting	ID	Description	Valid Values
Alias	1	Alias for the Syslog service	Alias to be displayed
Severity	2	Severity logging level	All levels defined in the Syslog RFC
IP Address	3	IP address of the Syslog server	Any IPv4 address

Table 2.7 Settings for Adding a Syslog Server (Sheet 2 of 2)

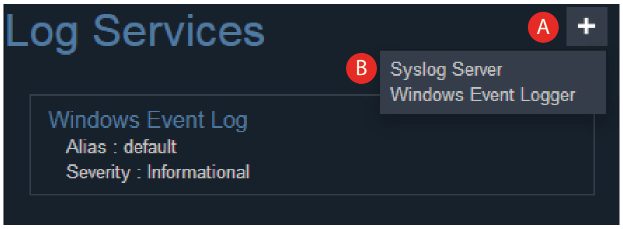
Setting	ID	Description	Valid Values
Port	4	Syslog port on the Syslog server	Any valid IP port (usually 514)
Message Format	5	Controls the format of the contents of the Syslog message	RFC 3164 (Traditional) or RFC 5424
Transport Method	6	IP protocol used	UDP or TLS

Steps

Step 1. Go to the Log Settings page.

Step 2. Select the Primary entry in the Logging table.

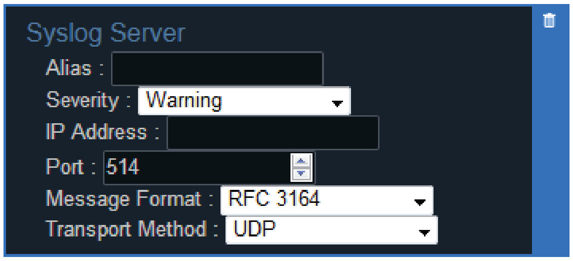
Step 3. Select the **Add** + icon (A) in the Log Services pane, and then select Syslog Server (B) from the menu to display a new Syslog Server Log Service box.



Windows Event Log
Alias : default
Severity : Informational

Step 4. Select the Syslog Server box to display a blue border around the box.

Step 5. Enter Settings (1) through (4) in the appropriate boxes.



Syslog Server
Alias :
Severity : Warning
IP Address :
Port : 514
Message Format : RFC 3164
Transport Method : UDP

Step 6. Select **Submit**.

Adding or Editing a Windows Event Log Service

You can only configure one web data or Windows event log service at one time. If one is already available, edit its settings.

Table 2.8 Settings for Adding or Editing a Web Data or Windows Event Log Service

Setting	Description	Valid Values
Alias	Alias to be displayed	Any valid text string
Severity	Severity logging level	One of the selectable choices from the drop-down menu

Steps to Add a Windows Event Log Service

Step 1. Go to the Log Settings page.

Step 2. Select the Primary entry in the Logging table.

Step 3. Select the Add New Log Service button.

Step 4. Select the Windows Event Logger.

Step 5. Use the following steps to populate the settings.

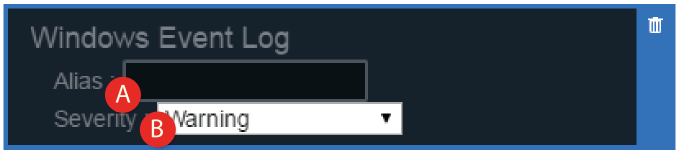
Steps to Edit a Windows Event Log Service

Step 1. Go to the Log Settings page.

Step 2. Select the Primary entry in the Logging table.

Step 3. Select the Log Service box to edit. When you select a box, the border turns blue.

Step 4. Enter settings into the appropriate boxes (A and B).



Windows Event Log

Alias :

Severity : Warning

Step 5. Select **Submit**.

User Account

You can access the My Account page by selecting your account icon in the top right of any page and from any role. The Security Administrator role is the only one that can add or delete accounts and change role permissions. All other roles can only change their own password. Follow the onscreen instructions to change your password. Security Administrators manage accounts and roles on the User Accounts page. Security Administrators can add, delete, change roles; change the password of any local account; and add external users to the roles mapped in the SEL-5056 through any configured LDAP server.

Usage Policy

The Usage Policy page allows you to change the use policy banner displayed on the login page.

This page intentionally left blank

SECTION 3

OpenFlow

Introduction

The SEL-5056 has powerful automation integrated into it, eliminating most direct OpenFlow programming. This section provides a reference for the supported OpenFlow 1.3 features in the SEL-5056. For details on OpenFlow, review the standard at opennetworking.org. The SDN switches used with the SEL-5056 also have OpenFlow specifications that must be reviewed because it is the combined support of both the flow controller and switch that dictates the overall system capabilities.

Software-Defined Network (SDN)

An SDN is a network architectural concept that abstracts the control plane from the data plane. Traditional networking integrates the operation of determining how to forward packets (control plane) and the action of forwarding the packets (data plane) into the same device. An SDN physically removes the determination of how to forward packets from each device and moves it to centralized software that determines how to forward packets for all devices in tandem.

This central software is referred to as the flow controller. The SEL-5056 is the SEL flow controller. The flow controller programs the SDN switches with match and action pairings, which the switch uses to forward packets. The switch acts like a large look-up table, which the switch uses to match and forward packets. Once a packet matches an entry, the switch executes actions for that match. This combination of match and action is called a flow entry.

Flow entries are the building blocks necessary for traffic engineering the network. Traffic engineering allows proactive configuration of how all packets travel through the network under normal or faulted conditions.

There are three main advantages to centralizing the control plane:

- Simplified application and monitoring of network policies
- Reduction in the complexity of the network appliance
- Increase in performance

OpenFlow is a common, open industry standard used for implementing an SDN. OpenFlow is a standard protocol used to communicate between the flow controller and the network appliance for configuration and monitoring. SEL uses the OpenFlow protocol to implement an SDN that supports OpenFlow 1.3.

SDN architectures consist of three main levels:

- Applications
- Flow controller
- Network appliance

Operations, administration, and management (OAM) applications implement automation, enforce policy, harvest network configuration and counters, and perform other system needs. The flow controller is the central software that provides visualization of the network and instructs network appliances on how they forward packets. Consider the flow controller as the network operating system that allows better situational awareness of the network. The network appliances are the switches that forward data from source to destination. *Figure 3.1* graphically represents this architecture.

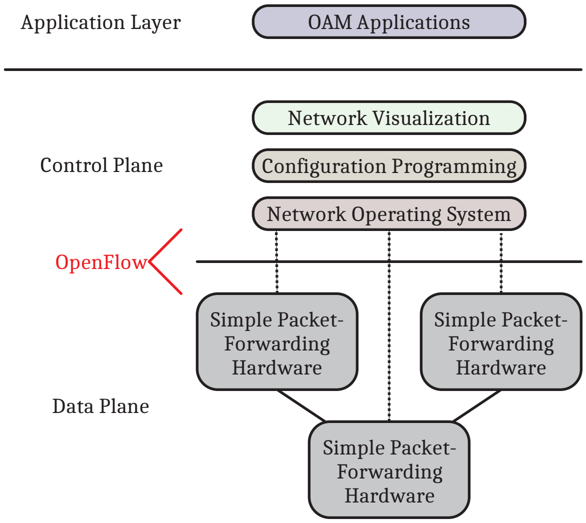

Application Layer
OAM Applications
Network Visualization
Control Plane
Configuration Programming
Network Operating System
OpenFlow
Simple Packet-Forwarding Hardware
Simple Packet-Forwarding Hardware
Data Plane
Simple Packet-Forwarding Hardware

Figure 3.1 SDN Architecture

Overview

The SEL-5056 uses the capabilities defined in the OpenFlow standard as the underlay technology managing the network operations, not traditional switch behavior. Technologies such as Spanning Tree Protocol (STP) and dynamic MAC learning are removed from the switch.

OpenFlow switches can be divided into the following five separate OpenFlow components:

- Ports, including queues
- Flow tables
- Flow entries, including instructions
- Group entries, including action buckets
- Meter entries, including meter bands

Traditionally, each setting requires a numeric value. For example, to specify the NTP UDP port for the UdpSrc match field, you must enter the value 123. Instead, the SEL-5056 allows you to use a friendly name, which is an alias for the numeric value. This allows you to enter either the friendly name NTP or the numeric value 123 as the value for the UdpSrc match field. Friendly names are listed where available.

Counters and Parameters

Table 3.1 lists the supported counters.

Table 3.1 Complete List of Supported Counters

Type of Counter	Name	Description
Port	Received Packets	Packet count received per port
	Transmitted Packets	Packet count transmitted per port
	Received Bytes	Byte count received per port
	Transmitted Bytes	Byte count transmitted per port
Flow Table	Active Count	Number of flow entries in the flow table
Flow Entry	Received Packets	Packet count applied to the flow entry
	Received Bytes	Byte count applied to the flow entry
	Duration	Elapsed time from when the flow entry was programmed or last modified (in milliseconds)
Group Entry	Packet Count	Packet count applied to the group entry
	Byte Count	Byte count applied to the group entry
	Reference Count	Number of flow entries referencing the group entry
	Duration	Elapsed time from when the group entry was programmed or last modified (in milliseconds)
Meter Entry	Input Packet Count	Packet count applied to the meter entry
	Input Byte Count	Byte count applied to the meter entry
	Reference Count	Number of flow entries referencing the meter entry
	Duration	Elapsed time from when the meter was programmed or last modified (in milliseconds)
Meter Band	In-Band Packet Count	Packet count applied to the meter band
	In-Band Byte Count	Byte count applied to the meter band

Terms

Table 3.2 lists the terms used in OpenFlow.

Table 3.2 List of Terms and Definitions (Sheet 1 of 2)

Term	Definition
Action	Part of the flow entry that controls how to forward packets
All port	The set of ports to flood a packet
Any port	The watch port when port liveness is not used
Clear-Actions	Clears the action set
Controller port	The alias for the port to the SEL-5056
Counters	One of the OpenFlow 1.3-defined counters listed in *Table 3.1*
Entry	An individual flow, group, or meter configuration
Flow controller	The network operating system
Flow ID	Identifies a flow entry
Flow table	One of the four flow tables that contains the flow entries
Friendly name	An alias for a numeric value
Ingress port	An alias for the physical port on which the packet arrived
Instruction	One of the instructions listed in *Table 3.12*
Instructions	The part of a flow entry used to control packet egress
Local port	The alias for the port to the SEL-2740S management interface
Match fields	Part of the flow entry that controls how to match packets
Meter	Rate limiting

Table 3.2 List of Terms and Definitions (Sheet 2 of 2)

Term	Definition
Northbound interface	Point of communication between users, applications, and the flow controller
OpenFlow	An open standard that defines the Southbound interface and forwarding capabilities of a switch
OpenFlow Port	Any of the ports defined in *Table 3.3*
OutPort	The value of the Output action
Port liveness	A port is live if the port link is active and not administratively disabled through port configuration
Priority queue	One of the four egress queues for each physical port
Set-Field action	An action that changes the contents of a packet
Southbound interface	Point of communication between the flow controller and the network appliances
Table-Miss entry	A flow entry with no match fields and a priority of 0 that matches packets that are not matched by any other flow entry in the flow table
Watch group	The group used to determine liveness in a fast failover action bucket
Watch port	The port used to determine liveness in a fast failover action bucket
Write-Actions	An instruction that contains actions that are added to the action set of a packet

Ports

OpenFlow ports represent all of the inputs and outputs in the OpenFlow packet processing environment. The SEL SDN switches support many different types of OpenFlow ports. *Table 3.3* lists the supported ports.

Table 3.3 SEL-2740S Port Types

Port	Description	Value	Friendly Name	Port Diagnostics	Valid InPort	Valid OutPort	Valid Watch Port
Physical	SEL-2740S, 20 data plane ports	1–20	Module Letter and Number	Yes	Yes	Yes	Yes
Physical	SEL-2742S, 12 data plane ports	1–12	N/A	Yes	Yes	Yes	Yes
Ingress	Alias for physical ingress port	0xfffffff8	Ingress	No	No	Yes	No
All	Forwards to all standard ports except the ingress port	0xfffffffc	All	No	No	Yes	No
Controller	Forwards packets to the SEL-5056	0xfffffffd	Controller	No	Yes	Yes	No
Local	Forwards to the management interface of the switch itself	0xfffffffe	Local	Yes	Yes	Yes	No
Any	The watch port used when there is no port liveness	0xffffffff	Any	No	No	No	Yes

Liveness

All physical ports have liveness, and a physical port is live if the port link is active and not administratively disabled through port configuration. Non-physical ports do not have liveness.

Priority Queues

The SEL-5056 supports setting all priority levels. The SDN switch will determine how many queues the egress port has and if the VLAN tag or the flow configuration is followed.

Port Settings

Using the SEL-5056 web interface, you may change the Port settings shown in *Table 3.4* for a physical port. Each of these settings may be True or False. These settings cannot be modified for a port that is disabled.

Table 3.4 Port Settings Based on Ordering Options

Setting	Default Value	Supported
Disable Port	False	Yes
Disable Receiving	False	Yes
Disable Transmitting	False	Yes
Disable Packet In Messages	False	Yes
Auto-Negotiation	True	Yes
Pause	Not Supported	No
Asymmetric Pause	Not Supported	No
10 Mbps Full-Duplex	True	Yes
10 Mbps Half-Duplex	True	Yes
100 Mbps Full-Duplex	True	Yes
100 Mbps Half-Duplex	True	Yes
1 Gbps Full-Duplex	True	Yes
1 Gbps Half-Duplex	True	Yes

Flow Tables

The SEL-5056 supports 256 tables and does not limit the number of flows that can be added to each table. The SEL-5056 writes flows to the switch and monitors to confirm if the configurations are accepted.

Table-Miss Entries

Table-Miss entries are flow entries that have a priority setting of 0 and no match fields. Because they have no match fields, Table-Miss entries match all packets. If the Table-Miss entry does not have an Output action, the packet is dropped.

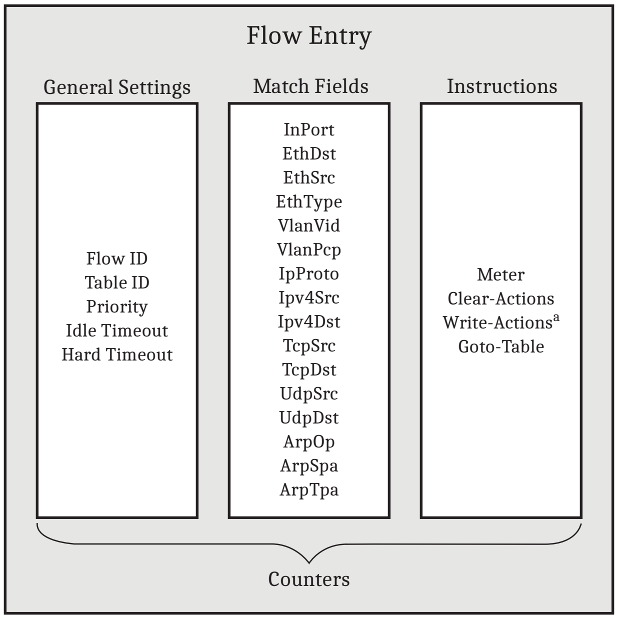
The SEL-5056 adds table-miss flows for SEL SDN switches. There are four table-miss flows, each with a meter to limit the rate of packets sent to the SEL-5056. These four flows are specific to ARP, GOOSE, Sampled Values, and all other Ethernet traffic. Do not adjust these flows when you want the SEL-5056 to automatically provide host discovery. If you do not want host discovery, these flows may be disabled or deleted.

Flow Entries

Flow entries are the heart of the OpenFlow system and control how packets are forwarded through their match fields and instructions. The switches use match fields to match packets to a flow entry and then executes the instructions in the flow entry. The SEL-5056 programs the flow tables in each switch in a proactive traffic engineering manner. Once programmed, the switches continue to operate as instructed with or without the flow controller online.

Flow entries have four parts (see *Figure 3.2*):

- General settings
- Match fields
- Instructions
- Counters



[a] This instruction contains actions.

Figure 3.2 Flow Entries Diagram

The primary purpose of flow entries is to match the packet to the conversation it belongs to so that the packet can be forwarded to the proper destination. By following this simple concept, only packets each end device wants to receive is delivered, optimizing processing and reducing noise. Therefore, a flow entry can be divided into two functions: an ingress function of matching a packet, and an egress function of controlling what to do with that matched packet. Match fields control the behavior of packets on ingress, and instructions control the behavior of packets on egress.

General Settings

Table 3.5 lists the general settings for flow entries.

Table 3.5 Flow Entry General Settings

Setting	Values	Description
Alias	User-defined string	Friendly name used to identify the flow when looking at the table and counters. Local to the SEL-5056 only.
Flow ID	Set by the controller	ID of the flow entry.
Table ID	0 to 3	Table ID to which the flow entry is programmed.
Priority	0 to 65535[a]	Setting used for selecting a flow entry when a packet matches multiple flow entries; in this case, the SDN switches selects the flow entry with the highest value.
Idle Timeout	0 to 65535	The flow entry is deleted if the set number of seconds has elapsed from when a packet was last applied to the flow entry; a value of 0 disables the time-out.
Hard Timeout	0 to 65535	The flow entry is deleted after the specified number of seconds; a value of 0 disables the time-out.
Check Overlap	True or False	If true, the SDN switches prohibits flow entries that have the same priority and may match the same in the same flow table; the SEL-5056 sets this to True for every flow entry; this is always enforced when using the SEL-5056.

[a] 100 to 64000 is recommended to prevent conflict with the SEL-5056 auto-generated default flow entries.

The Flow ID setting serves as a reference to a particular flow entry. The SEL-5056 sets this value after you have submitted a new flow entry. This value also serves to reference a flow entry in the list of flow entry counters. If both time-outs are set and either time-out expires, the SEL SDN switch deletes the flow. Modifying a flow entry resets the counters.

Match Fields

Table 3.6 lists the supported match fields. The available friendly names for each field are listed in *Table 3.7*. If you do not use match fields or if you use match fields but do not enter a value, the SEL-5056 programs the flow by using wildcards in these fields. Wildcards match all packets for the specific field. For some match fields, you can use an alias instead. If you use the alias of the host instead of the value, the flow entry updates if the underlying value changes. For example, if you use a host in the Ipv4DstByAlias match field, the SEL-5056 enters the IP address of the host. You cannot use a mask if you use the Alias version of a match field.

Table 3.6 Match Fields (Sheet 1 of 2)

Name	Valid Values[a]	Maskable	Aliasable	Prerequisites		Description
				Type	Value	
ArpOp	0 to 255	No		EthType	0x806	Address Resolution Protocol (ARP) Opcode
ArpSpa	Any valid IPv4 address	Yes	Yes	EthType	0x806	ARP source IPv4 address
ArpTpa	Any valid IPv4 address	Yes	Yes	EthType	0x806	ARP destination IPv4 address
EthDst	Any valid MAC address	Yes	Yes			Ethernet destination address
EthSrc	Any valid MAC address	Yes	Yes			Ethernet source address
EthType	0 to 65535	No				Ethernet type
InPort	Any valid InPort port for the switch	No	Yes			Switch input port

Table 3.6 Match Fields (Sheet 2 of 2)

Name	Valid Values[a]	Maskable	Aliasable	Prerequisites		Description
				Type	Value	
IpProto	0 to 255	No		EthType	0x800	IP Protocol
Ipv4Dst	Any valid IPv4 address	Yes	Yes	EthType	0x800	IPv4 destination address
Ipv4Src	Any valid IPv4 address	Yes	Yes	EthType	0x800	IPv4 source address
TcpDst	0 to 65535	No		IpProto	6	IPv4 TCP destination port
TcpSrc	0 to 65535	No		IpProto	6	IPv4 TCP source port
UdpDst	0 to 65535	No		IpProto	17	IPv4 UDP destination port
UdpSrc	0 to 65535	No		IpProto	17	IPv4 UDP source port
VlanPcp	0 to 7	No		VlanVid		VLAN priority code point (PCP)
VlanVid	None, Present, 0 to 4095; Present and 0 to 4095 for mask (see *VlanVid*)	Yes				VLAN virtual identifier (ID)

[a] If the field has a corresponding mask, the valid values are the same as the match field unless specified otherwise.

Table 3.7 Additional Friendly Names for Match Fields (Sheet 1 of 2)

Match Field	Friendly Name	Equivalent Value
ArpOp	Reply	2
	Request	1
EthType	ARP	0x806
	GOOSE	0x88b8
	GSE	0x88b9
	IPv4	0x800
	LLDP	0x88cc
	PRP	0x88FB
	PTP	0x88F7
	SEL87L	0x892b
	SV	0x88ba
IpProto	ICMP	1
	TCP	6
	UDP	17

Table 3.7 Additional Friendly Names for Match Fields (Sheet 2 of 2)

Match Field	Friendly Name	Equivalent Value
TcpSrc/TcpDst	DNP3	20000
	Fast Message	23
	FTP	21
	FTPDATA	20
	HTTP	80
	HTTPS	443
	LDAP	389
	MMS	102
	Modbus	502
	OpenFlow	6653
	SSH	22
	Synchrophasors	4712
	Telnet	23
UdpSrc/UdpDst	DNP3	20000
	DNS	53
	Fast Message	23
	MMS	102
	NTP	123
	SNMP	161
	SNMPTrap	162
	Synchrophasors	4713
	Syslog	514

The purpose of match fields is to differentiate traffic, thus allowing you to apply different instructions to different traffic. Flow entries overlap if one packet can match more than one flow at the same flow priority. The more match fields that are used, the more exclusive the flow is. The fewer match fields that are used, the more inclusive the flow is.

If all match fields match all equivalent packet fields, the flow entry is considered to match. *Table 3.8* lists the matching states. For a flow entry to match a packet, every match field must match, as shown in *Table 3.8*. If any match fields do not match, the flow entry does not match the packet and the SEL-2740S does not apply the packet to it.

Table 3.8 Matching States

If the match field is . . .	And the equivalent packet field is . . .	Then the effect on the match for this combination is . . .
Not present	Not present	Match
Not present	Present	Match
Present	Not present	No match
Present	Present, but has a different value than the match field value	No match
Present	Present and has the same value as the match field value	Match

Masking

Some match fields support an optional mask. A mask is applied as a bit mask to the corresponding match field value to allow a range of matching values. The match field must be present to use its corresponding mask. A bit value of 1 in the mask requires a match in that bit between the packet field value and match field value; a bit value of 0 in the mask is a wildcard match. For example, the combination of an EthDst value of 01:00:00:00:00:00 and a mask value of 01:00:00:00:00:00 matches all multicast packets because the 01 in the first byte of the mask means that the multicast bit of the Ethernet Destination of the packet must be 1 to match and the 00 in the remaining bytes are wildcard bytes that allow any value in that part of the Ethernet Destination address field of the packet. The mask has one requirement: if the mask has a 0 in a bit position, the Match Fields value must also have a 0 in that bit position, as shown in *Table 3.9*.

Table 3.9 Mask Matching Criterion

		Value Bit	
		0	**1**
Mask Bit	**0**	Packet bit ignored (wildcard)	Not allowed by OpenFlow
	1	Packet bit must be 0	Packet bit must be 1

While adding more match fields reduces the number of possible matching packets, adding a mask increases the number of possible matching packets. A mask of all one bits is the same as having no masking. The more the bits are set in the mask, the fewer possible packets that match (see *Table 3.10*).

Table 3.10 The Effect of Masking

Scenario	Effect
A match field with no masking	Only packets with the same packet value match
A match field with a mask with all bits set to 1	No masking
A match field with some but not all of the bits set to 1	A subset of all possible packet values match

By using masking, nonoverlapping matching can be combined to apply the same instructions to otherwise nonoverlapping packets. For IP addresses, masking works like traditional IP address masking. For example, using a mask for the Ipv4Dst field can combine subnets into the same flow entry. By using an Ipv4Dst value of 192.168.0.0 and a mask value of 255.255.0.0, all packets within the 192.168.0.0/16 value match the flow entry. Therefore, match fields differentiate packets, and masking associates packets.

VlanVid

The VlanVid match field can be used to match four states: no VLAN header, a VLAN header with any virtual ID (VID) (including 0 and 4095), a VLAN header with a particular VID, or a range of VIDs. If the VlanVid match field is not present, the flow entry matches both packets, with and without a VLAN header. *Table 3.11* lists the VlanVid match field values for each state.

Table 3.11 VlanVid Match Field and Mask Values

Condition to Match	VlanVid Value	VlanVid Mask
No VLAN header	None	NA
VLAN header with any VID (including 0 and 4095)	Present (0)	Present (0)
VLAN header with a particular VID	The specific VLAN ID	NA
A range of VLAN IDs	Calculated	Calculated

The mask can use the values 0 to 4095. The value Present can be used instead of 0.

VlanPcp

To use the VlanPcp match field, the VlanVid match field must be present and have a value of Present or 0 to 4095. This indicates that the VLAN header is present and therefore the VLAN PCP field is present.

Instructions and Actions

If the match fields represent the *if*, the instructions (and the possible included actions) represent the *then*. If a packet matches a flow entry, the switch applies the instructions of the flow entry to the packet. *Table 3.12* lists all of the supported instructions on the SEL SDN switches in order of instruction application.

Table 3.12 Supported Instructions in Order of Applied Priority

Instruction	Value	Description
Meter	Any valid Meter ID	Directs the packet to a meter
Clear-Actions	None	Removes all of the actions from the action set
Write-Actions	Zero or more of the actions listed *Table 3.13*	Merges the specified action(s) into the action set
Goto-Table	1–3 (value must be higher than the Table ID of the flow entry)	Sends the packet to the designated table to look for the next match

The Meter instruction sends the flow to the specified meter. If the meter drops the packet, packet processing for that packet stops. Write-Actions instruction actions are not applied to the packet immediately, but they are added to the action set of the packet. The action set is only applied to the packet when packet processing stops, so it does not affect any further matching against the packet. *Table 3.13* lists the supported actions of the Write-Actions instruction in the order the switch executes the actions. The Clear-Actions instruction clears the action set of actions added in previous flow tables. The Goto-Table instruction forwards the packet to another flow table for further matching. The specified table must have a higher Table ID than the Table ID of the present flow entry. Therefore, flow entries in Flow Table 3 cannot have Goto-Table instructions and flow entries in Flow Table 2 can only have a Goto-Table instruction for Flow Table 3.

Table 3.13 Supported Write-Actions Instruction Actions in Order of Applied Priority

Action	Value	Prerequisites	Description
PopVlan	None	See *Set-Field Actions*	Pops a VLAN header
PushVlan	0x8100	None	Pushes a VLAN header
SetVlanId	0 to 4095[a]	See *Set-Field Actions*	Sets the VLAN ID of the outermost VLAN header
SetVlanPcp	0 to 7	See *Set-Field Actions*	Sets the VLAN PCP of the outermost VLAN header
SetQueue	1 to 4	None	Sets the priority queue
Group by Alias or Group by Value	Any valid Group ID or alias	None	Sends the packet to the group represented by the Group ID or alias
Output by Alias or Output by Value	Any valid port listed in *Table 3.3* or the alias of an adopted port	None	Sends the packet out of the port represented by the port name or alias

[a] The value 0 indicates a priority-tagged packet. The value 4095 is reserved by IEEE 802.1Q.

The Output action sends the packet to the specified port, referred to as the OutPort. This OutPort can be any of the valid OutPorts listed in *Table 3.3*. The Output action is required for egress packets coming from the switch. If an OutPort action is never executed against a packet, the packet is dropped. This Output action may be present in the Group action instead of directly in the flow entry.

The Group action sends the packet to the specified group. The group can be any of the presently programmed groups on the switch. Groups are covered in *Group Entries on page 3.13*. *Set-Field Actions on page 3.12* explains the Set-Field actions, SetVlanId and SetVlanPcp. When adding a new VLAN header, the SEL SDN switch copies the VLAN ID and VLAN PCP fields from the previous VLAN tag to the new VLAN tag, if present, or sets them at 0, if not present. Use the SetVlanId and SetVlanPcp actions when using the pushVLAN action to set the fields in the header.

Set-Field Actions

To set the VLAN ID or VLAN PCP, a VLAN header must be present (see *Table 3.17*, rows 2 and 3). This requires that either the VlanVid match fields be present with a value of Present or of 0 to 4095, or that the PushVlan action also be present.

Adding, Modifying, and Deleting

You can add flow entries to a flow table if you do not exceed the limit of 1,024 flow entries in SEL SDN switches; other switches may have smaller or larger flow tables. This limit includes the default flows.

Modifying or deleting a flow entry may disrupt packets that are applied to that flow entry, including packet loss. If you delete a group or meter entry, all flow entries that reference that group or meter are also deleted. Flow entries with timeouts are deleted when the SDN switches resets or cycles power.

You can only program one flow entry with the same match fields and priority for each flow table. Adding another flow entry with the same match fields and priority removes the previous entry.

Additionally, you cannot program flow entries on the same flow table with different match fields and the same priority that match the same packets.

When you modify flows for in-band management, it is best to work from the farthest source point from the controller and then toward the controller. It is also best to modify one flow at a time to ensure control over execution order. Modifying a flow does not delete the flow entry on the switch if you are modifying the instruction set of the flow entry. Therefore, if there is an error, the flow should be at its last known good state.

Group Entries

The purpose of groups is to extend the capabilities of the Output action by defining a special relationship among a group of Output actions. Groups do not form any relationship among the ports of the Output actions in the action buckets of the group, but only form relationships among the OutPort actions themselves.

Groups are accessed through Write-Actions instruction, so they are a part of the egress control, not the ingress control, of a packet through packet processing; therefore, groups cannot be used to control how packets are matched, only how packets are forwarded by the switch. Group actions are not a replacement for the Output action; instead, Group actions extend the functionality of the Output action by providing a special relationship of aliasing, failover, reduplication, or link aggregation among the Output actions in the group. All groups should ultimately resolve to one or more Output actions. If a group does not resolve into an Output action, the packet is dropped. Some combination of chaining is also supported to combine the special relationship of groups to form a richer set of capabilities.

Group entries have three parts, as shown in *Figure 3.3*:

- ➤ General Settings
- ➤ Action Buckets
- ➤ Counters

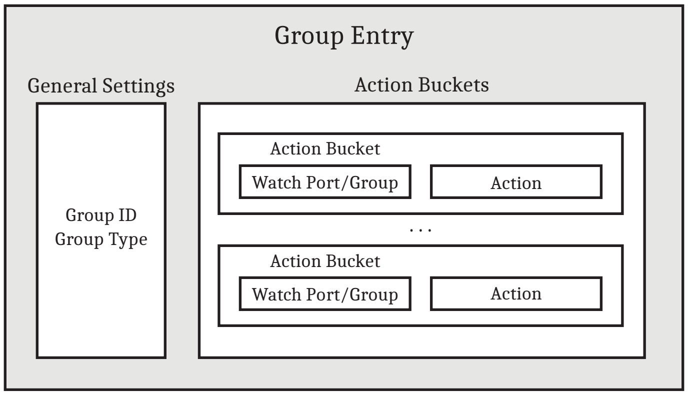


Figure 3.3 Parts of a Group Entry

General Settings

Table 3.14 lists the general settings for group entries.

Table 3.14 Group Entry General Settings

Setting	Values	Description
Group ID	0 to 4294967040	ID of the Group Entry
Group Type	Indirect, All, Select, Fast Failover	Type of the Group

Use the Group ID setting to reference the group in a Group action and for counters.

The SEL SDN switches support all four OpenFlow group types listed in *Table 3.15*.

Table 3.15 Group Type Parameters

Group Type	Number of Group Chaining	Packet Duplication	Liveness	Relationship
Indirect	2	No	No	Aliasing
All	2	Yes	No	Replication
Select	0	No	No	Aggregation
Fast Failover	2	No	Yes	Priority

Indirect groups can be used to alias a physical port by having all flow entries forward to an Indirect group that contains an Output action to the aliased physical port instead of having an Output action in each flow entry. This allows you to change the OutPort by modifying the Output action of the Indirect group instead of the Output action of each flow entry if the physical port to a device is changed. If group liveness is necessary, a Fast Failover group must be used instead. A Select group or an All group with one action bucket has the equivalent behavior of an Indirect group.

Figure 3.4 shows four flow entries with the same OutPort. If the OutPort must change, all four Output actions must be modified.

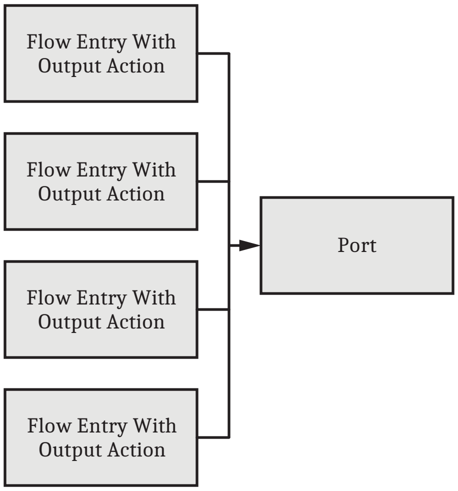

Flow Entry With Output Action
Flow Entry With Output Action
Flow Entry With Output Action
Flow Entry With Output Action
Port

Figure 3.4 No Port Aliasing

Figure 3.5 shows the same scenario by using an alias port. In this case, if the OutPort needs to change, only the Output action in the alias group must be changed.

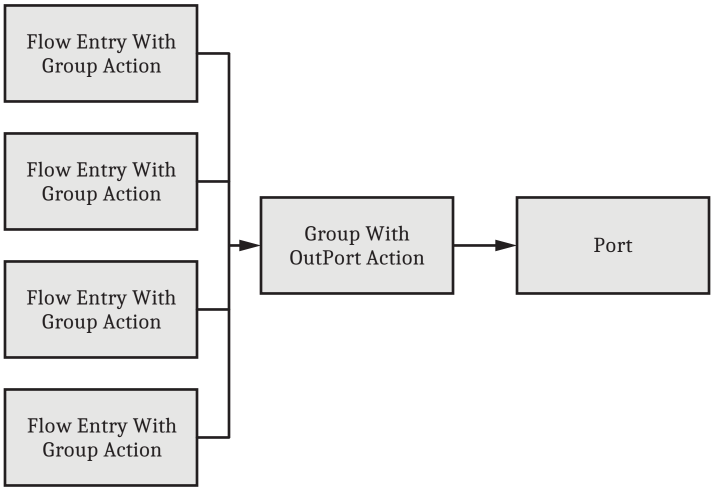

Flow Entry With Group Action
Flow Entry With Group Action
Flow Entry With Group Action
Flow Entry With Group Action
Group With OutPort Action
Port

Figure 3.5 Port Aliasing

The All group is used to replicate packets to a set of ports but not all ports (as occurs when using the All port). An All group with an action bucket for each standard port is equivalent to the All port.

The Select group is used for link aggregation. Packets are applied to the group, and the group allocates the packets to ports by using a round-robin allocation. *Figure 3.6* shows an example of a Select group applying packets to four ports. The same OutPort can be added to multiple buckets to increase the allocation of packets to that OutPort. Ports that are not live are skipped.

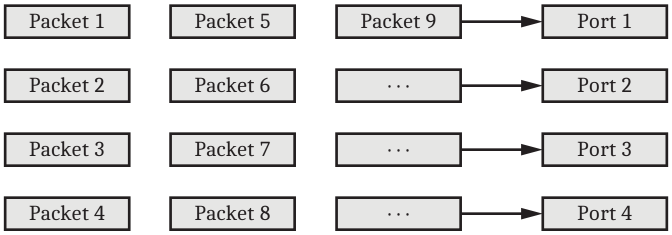


Figure 3.6 Allocating Packets in a Select Group

The Fast Failover group provides redundancy by using liveness to send a packet from an ordered list of ports or groups. *Figure 3.7* shows how the packet is applied in a Fast Failover group with a primary action bucket and two backup action buckets.

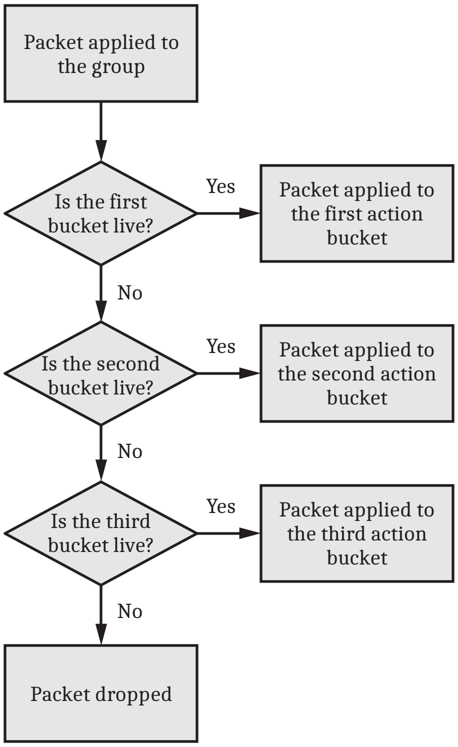

Packet applied to the group
Is the first bucket live?
Yes
Packet applied to the first action bucket
No
Is the second bucket live?
Yes
Packet applied to the second action bucket
No
Is the third bucket live?
Yes
Packet applied to the third action bucket
No
Packet dropped

Figure 3.7 Applying a Packet to a Fast Failover Group

Action Buckets

A Group entry may contain zero or more action buckets depending on the group type. *Table 3.16* lists all of the parameters per group type for Watch port, Watch group, supported actions, and the maximum number of action buckets.

The SEL SDN switch treats each set of actions in an action bucket as its own Action Set, which is the same as how the SEL SDN switch treats the action set of Write-Actions Instruction actions. A group with no action buckets drops the packet. The actions in an action bucket operate the same as their Write-Actions instruction action equivalents except that the SEL SDN switch applies the actions immediately in the same order as the Write-actions instruction actions show in *Figure 3.8*. Because the action set of a packet through the flow tables is applied before the packet is sent to a group entry, action bucket actions are applied after the SEL SDN switch has applied all of the Write-Actions instruction actions to the packet. If an action bucket forwards a packet to another group, the SEL SDN switch applies the actions of the second action bucket to the packet after applying the actions of the first action bucket and the action of the Write-Actions instruction of the flow entry. For example, if the flow entry and the action bucket both contain a PushVlan, the egressing packet contains two VLAN tags.

There are no prerequisites for action bucket actions. If the action bucket contains a PopVlan, SetVlanId, or SetVlanPcp action without a PushVlan action and the packet did not have a VLAN tag when sent to the group (for example, if the Write-Actions Instruction action set contains a PopVlan action), the switch discards the packet.

Table 3.16 Action Bucket

Group Type	Action Buckets Supported	Valid Watch Port	Valid Watch Group	Supported Actions
Indirect	1	Any	Any	Output, Group
All	30	Any	Any	Output, Group, PushVlan, PopVlan, SetQueue, SetVlanVid, SetVlanPcp
Select	30	Any[a]	Any	Output
Fast Failover[b]	30	Any Watch port listed in *Table 3.3*	Group ID of a Fast Failover group on the switch or Any	Output, Group, PushVlan, PopVlan, SetQueue, SetVlanVid, SetVlanPcp

[a] Although the watch Port must be Any, action buckets with a downed OutPort are automatically skipped.

[b] Either the watch port or watch group may be Any, but not both.

The role of the action bucket depends on the group. For the Indirect group, the action bucket action specifies the aliased port or group. The action buckets in an All group represent points of duplication, either through a Group or Output action. Application of a packet to an All group applies the packet to every action bucket, regardless of liveness. This group may be used for redundancy schemes that involve packet reduplication.

Action buckets in a Select group determine how to allocate packets applied to the group. Each action bucket represents a point of allocation. The example group in *Figure 3.6* contains four action buckets, each with an Output action for each of the ports in the Select group, i.e., 1, 2, 3, and 4. The action buckets in a Select group have implicit liveness. If the OutPort is live, the action bucket is live and the switch applies packets to the bucket. If the OutPort is no longer live, the switch skips that bucket. The Select group may also be used for redundancy. Fast Failover groups use the action buckets to provide a prioritized list of primary and backup connections to handle link failure. The first action bucket represents how to forward the packet during normal conditions, and the remaining action buckets represent how to forward the packet during failover conditions.

All group types, except the Select group type, support two levels of chaining. This means that a packet may be programmed to pass through as many as three groups before an Output action. A group cannot reference itself in an action bucket, within chained Group action buckets, or in a loop.

If an action bucket contains both a group and an Output action, only the Group action is applied, regardless of liveness or contents.

For the All, Select, and Indirect groups, the Watch Port and Watch Group settings must be Any (0xffffffff, see *Table 3.3*). Only Fast Failover groups may have a non-Any Watch group or Watch port; at least one must be a valid value other than Any. The SEL-2740S uses watch groups or watch ports to determine if an action bucket has liveness. If either the watch port or watch group is live, the action bucket is considered live. A Failover Group action bucket that uses a watch group besides Any cannot have a Group action that also has an action bucket that also uses a watch group besides Any.

Liveness

Liveness is an important concept for groups and ports. As shown in *Table 3.16*, only the Fast Failover group and the physical ports have liveness. A Fast Failover group is live if at least one of its action buckets is live. A Fast Failover action bucket is live if either the OutPort of the Watch Port setting or the group of the

Watch Group setting is also live. Because only Fast Failover groups can be live, only a Fast Failover group can be used as a watch group. The watch port or watch group does not have to match the value of the group or Output action.

When the switch sends a packet to a Fast Failover group, the group checks the first action bucket for liveness. If the OutPort in the Watch Port setting is live or the group in the watch group is live, the action bucket is live and the switch applies the packet to the action bucket. If the first action bucket is not live, the second bucket is checked, and so on. If no action buckets are live, the packet is dropped.

Group Action Bucket Actions

Actions in group entry action buckets are executed immediately as an action set in the order listed in *Figure 3.8* when a packet is sent to the action bucket. These actions occur after the switch has applied all of the Write-Actions instruction actions to the packet. If an action bucket forwards a packet to another group, the switch applies the actions of the second action bucket to the packet after the actions of the first action bucket and the Write-Actions instruction of the flow entry.

Adding, Modifying, and Deleting Group Entries

The SEL-5056 does not limit the number of groups or action buckets but when it attempts to write the configuration to the switch, the switch may reject it if the number of groups or action buckets has been exceeded.

You cannot delete a group entry if another group references that group entry. If you delete a group entry, all flow entries that reference that group entry are also deleted. Modifying, unless modifying the action bucket set of the group entry or deleting group entries, may result in traffic disruption, including packet loss.

Meter Entries

Meters provide rate limiting for flows. The SEL-5056 does not limit the number of meters but the SDN switch will. The SEL-5056 also supports an optional burst size. The rate and burst size may be in packets per second (PPS) or Kbps.

General Settings

Table 3.17 lists the meter entry general settings. Meter ID 64 is reserved for SEL-5056 use.

Table 3.17 Meter Entry General Settings

Setting	Valid Values	Description
Meter ID	1 to 256	ID of the meter entry
Measurement Type	Kbps or PPS	Defines the unit of measurement for the Rate and Burst Size meter band settings
Set Burst Size	True or False	If True, the meter band burst size is user-defined; if False, the minimum value is used

Meter Band

The Rate and Burst Size settings are listed in *Table 3.18* and depend on the Measurement Type setting of the meter band. The Burst Size setting defines the size of the meter, and the range of accepted values depends on the Meter Rate setting. If no burst size is set, or if it is set to a value below the minimum, Burst Size defaults to a minimum value as determined by the equation shown in *Table 3.18*. Using this minimum value with bursty traffic may cause traffic loss even though the traffic rate is much lower than the meter rate. Burst Size is in bytes if the Rate setting is in Kbps, and packets if the Rate setting is in PPS.

Table 3.18 Meter Band Settings

Setting	Measurement Type	Minimum Value	Maximum Value
Rate	Kbps	1	110000
	PPS	1	624999
Burst Size[a]	Kbps	1632 / (1 – [Rate[b] / 125,000,000])	16,777,215 / (1 – [Rate[b] / 125,000,000])
	PPS	256 / (1 – [Rate / 625,000])	16,777,215 / (1 – [Rate / 625,000])

[a] Required if Set Burst Size is True.

[b] Convert the rate to Bps.

Modifying and Deleting Meter Entries

If you modify or delete a meter entry, all flow entries referencing that meter entry are also deleted.

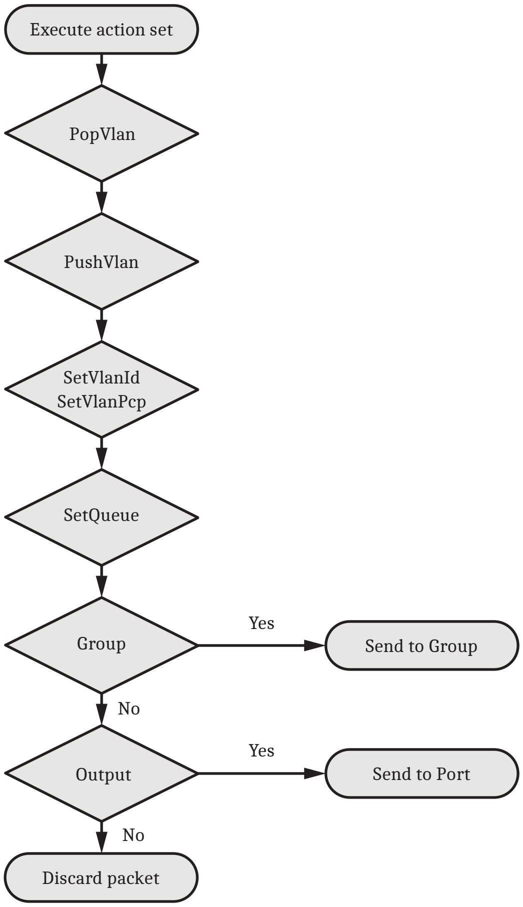


Figure 3.8 Action Set Execution Order

SECTION 4

Topology, Configuration, and Telemetry

This section covers the configuration and diagnostics of the SEL SDN system.

Introduction

The SEL SDN system manages the physical and logical network elements through a deny-by-default network access control and proactive traffic-engineered circuit provisioning with redundancy. This architecture removes the flow controller from being a single point of failure because the network will continue to operate as instructed if the flow controller goes offline. All physical and logical elements are deny by default. You must adopt (or approve) all switches, hosts, ports, and links in order to use them for circuit provisioning automation. Direct OpenFlow programming is accepted at any time. The SEL-5056 SDN Flow Controller has automation to remove the burden of direct OpenFlow programming and use automated circuit provisioning through logical connections or Learn and Lock. Logical connections are the circuit provisioning automation built into the SEL-5056. Logical connections perform the path planning and OpenFlow programming for the user. Users only select the source, destination, and the communication service type elements. Learn and Lock is the automation where the SEL-5056 learns the devices that are on the system and the conversations all devices are attempting to have and provisions the network to allow conversations to happen through fully automated measures or through supervised approval processes.

The physical network is broken into three types of network objects in the SEL-5056:

- Nodes
- Ports
- Links

These are referred to as operational objects and are listed in *Table 4.1*. Nodes consist of anything that communicates and affects communication, such as hosts, switches, and other network appliances, but the nodes do not include media converters or other transparent devices that do not create traffic. Links represent the cables between any two nodes across which traffic can pass (i.e., the physical connection). Ports are where the links connect to the nodes.

Table 4.1 Three Types of Network Objects

Object	Description
Node	Network device or hosts
Port	Physical port
Link	Virtual connection representing the cable(s) between two nodes

Network View

The SEL-5056 automates the discovery of the physical attributes so you do not need to enter them manually. The SEL-5056 has the ability to enter an offline host by selecting the port on the switch that the host will be attached to once deployed. This allows communications circuits to be provisioned before the device is connected. *Table 4.2* shows the four ways that the SEL-5056 discovers the physical elements.

Table 4.2 Network Discovery Processes

Process	Purpose	Method
Beacon	Discover links between two OpenFlow switches	Send out a Link Layer Discovery Protocol (LLDP) packet out of each OpenFlow switch port and watch for them to enter another OpenFlow switch port.
Host discovery	Discover hosts and ports	Forward Table-Miss flow entry traffic to the SEL-5056 and discover hosts through the controller that is receiving a packet from a host or a packet to a host. User-directed host discovery allows the operator to enter an IP address for the SEL-5056 to discover.
Autodiscovery	Discover uncommissioned OpenFlow switches	Forward autodiscovery packets to the SEL-5056.
Offline Host	Circuits can be provisioned before host is available	User configuration

A node cannot be separated from its port in a network. A device can have more than one port with the same MAC address, and a MAC address should be globally unique; therefore, if two links forward traffic with the same MAC address into a switch, those two links belong to the same node. The SEL-5056 autodiscovers switches and hosts on the network and the ports belonging to each host and switch. Silent hosts, or hosts for which other flow entries are matching all device traffic, do not appear in the Topology view. In this case, a port may appear to be up, but it has no connected link. When traffic is sent to an unknown host and hits the table-miss flow sending the packet to the controller, the controller uses Address Resolution Protocol (ARP) for the destination out of every active switch port that does not have an identified host on it already. If a host has more than one port and each port has a different MAC address, the host appears as more than one node in the Network view.

Object Management

Operational objects are representations of how the SEL-5056 understands the physical layout of the network. Once the SEL-5056 finds an operational host object with an IP address, the SEL-5056 watches the port status and ARPs for the active status of the device. If the port goes down or the host stops responding to the ARP requests, the SEL-5056 removes the host from the Topology view if the host is not adopted. If the host is adopted, it considers the host to be offline. If the host is only discovered by its MAC address, the host is monitored by the port status of the switch to which it is directly connected. Hosts with multiple addresses on the same port causes the SEL-5056 to use the last address discovered for liveness and logical connection circuit provisioning automation.

The configuration object represents a collection of settings for one of the four object types. The configuration object is independent of a specific operational object, so configuration objects can be independently created, modified, and deleted. You associate the configuration object with the operational object through adoption or, if changing the configuration object associated with the operational object, through a configuration change. You configure an operational object either by configuring the configuration object or by directly modifying the operational object, depending on the setting. Settings associated with the configuration object can therefore be created, modified, or deleted in the configuration object before or after adoption. Unadoption disassociates the configuration and operational objects.

For example, you can create an SEL-2740S configuration object, populate the object with OpenFlow entries, and then adopt an SEL-2740S with the configuration object. The SEL-5056 then commissions and programs the SEL-2740S to match the OpenFlow programming of the configuration object. Subsequent changes made to the configuration objects are synchronized with the SEL-2740S as long as the SEL-5056 can communicate with the SEL-2740S, or as soon as communications are reestablished between the SEL-5056 and SEL-2740S. If you want to replace the SEL-2740S with another SEL-2740S, unadopt the configuration object from the present SEL-2740S and then adopt the new SEL-2740S with the configuration object. The SEL-5056 then configures the same OpenFlow and IP address settings onto the new SEL-2740S. Other settings (SEL-2740S OpenFlow port settings or the IP settings of a host, for example) are not configuration object settings, so they cannot be reapplied to another operational object through the configuration object.

An operational object must be compatible with the configuration object to which it will be applied. *Table 4.3* lists types of operational objects and compatible configuration object types.

Table 4.3 Compatible Configuration and Operational Objects

Operational Object	Compatible Configuration Object
Host	Generic node
Non-SEL-2740S OpenFlow switch	Generic node
SEL-2740S OpenFlow switch	SEL-2740S node
SEL-2742S OpenFlow switch	SEL-2742S node
Port	Port
Link	Link

Only one configuration object can be applied to an operational object.

Once a configuration object is used to adopt an operational object, all the settings are written to the real device. When settings changes are made later, all settings are immediately written to the real device.

Display Name

Each type of operational object has an established display format. *Table 4.4* and *Table 4.5* list these for nodes, ports, and links, respectively.

Table 4.4 Operational Node Display Format (Default)

Type	Display Format
SEL-5056 host machine	Controller (unique, but may be modified in the Configuration objects > Node page)
Host (end device)	Host:<IP Address or Ethernet MAC Address>[a]
SEL-2740S	OpenFlow:<Datapath ID> where Datapath ID equals the identification on the bottom of the SEL-2740S chassis

[a] The IP address is displayed if the host has one. Otherwise, the Ethernet MAC address is displayed.

Table 4.5 Operational Port Display Format

Type	Display Format
Port on a host (end device)	IP: <IP Address> if IP address discovered for the host else MAC: <MAC Address>
Port on an OpenFlow switch	OpenFlow:<Datapath ID>:<Port Name>(<Port ID>) where Datapath ID equals the identification on the bottom of the SEL-2740S chassis, Port Name is based on the Module ID and relative port number, and Port ID

All objects can be renamed through the Configuration Object page after adoption. All operational nodes, ports, and links can have an alias assigned to them. These aliases become the display names for these attributes. This includes in the counter diagnostics and flows, which can use these aliases by including the qualifier "by alias" in the corresponding match field. Write-actions can also use these aliases when you send the packet to a group.

Attributes

The SEL-5056 collects and displays attributes depending on the source. These attributes are automatically gathered and displayed. These can be found by selecting the appropriate object on the Topology page. Attributes are listed in the right-most pane.

Table 4.6 Attributes

Category	Type	Description	Location
Ethernet Information	MAC Address	MAC address of the node	Switch Node, Host Node, Host Port
GOOSE Information	Destination	Destination MAC address of the GOOSE message	Host Node (if publishing GOOSE)
	Provider Info VID	VID of the GOOSE message	
	Source Address	Source MAC address of the GOOSE message	
IP Information	Address	IP address of the node	Host Node, Host Port
OpenFlow Information	Datapath ID	Datapath ID of the switch	Switch Node, Host Node (if non-Switch OpenFlow node)
Switch Information	Primary IP	IP address of the primary address to use when the Flow Controller communicates with the switch	Switch Node
	Datapath ID	Datapath ID of the switch	
	Alternate IP	IP address of the alternate network interface of the switch	
	Serial Number	Serial number of the SEL-2740S	

GOOSE Attributes

When creating a GOOSE logical connection, the SEL-5056 requires that the GOOSE attribute be present for the selected (start) node. The SEL-5056 then automatically enters the appropriate value for EthSrc into the flow entries of the logical connection.

Managing Dual-Homed Devices

Hosts can have multiple network interfaces. The SEL-5056 allows for the Topology manager to merge these multiple interfaces together into a single host. To perform such a merge, adopt the first node that was discovered and its first port.

Then select the second node that displays with the second port of the same node and select **Merge**, as shown in *Figure 4.1*. A host should not be merged if you want to use logical connections to or from that device or if the host operates the ports in Failover mode. In the latter case, use SEL Relay Failover Mode instead.

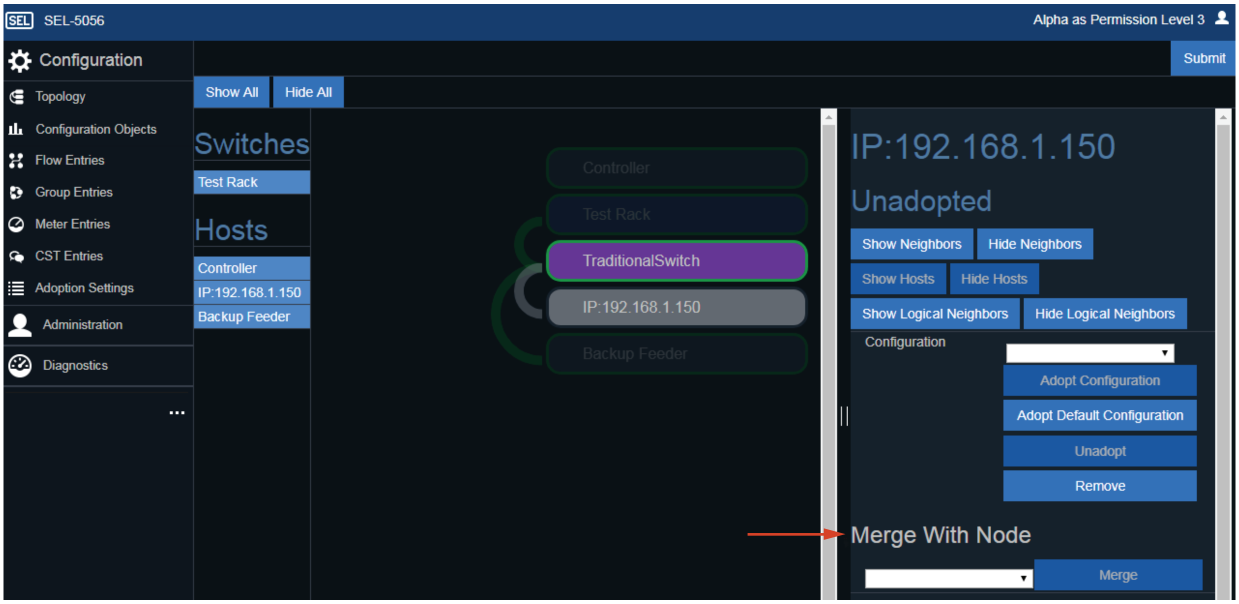


Figure 4.1 Merging Dual-Homed Hosts

Managing Devices in Failover Mode

The SEL-5056 supports the ability to configure logical connections to SEL relays running in Failover mode. This means that the relay has two network interfaces and communicates out of one until it fails because of an interface or link failure, at which time the relay starts communicating out of the other interface. Flows in an SDN must handle the delivery to or receive a packet from both interfaces for every flow to which the relay is communicating.

When the SEL-5056 has determined both interfaces of the relay, it is possible to make logical connections and for the SEL-5056 to automate the delivery of the same packet to both interfaces. Logical connections created with CSTs with type multicast cannot be used with devices in SEL Relay Failover mode. This allows the acceptance of the packet from either interface. To set up this pairing, perform the following steps:

Step 1. After the SEL-5056 discovers the SEL relay host, adopt it with your choice of configuration node.

Step 2. Adopt the link that the SEL-5056 discovered. This is the active link of the relay that is presently communicating to a switch.

Step 3. Select the host that is the SEL relay and expand it to show the ports.

Do this by selecting the name of the node.

Step 4. Select the port of the node to show the settings on the right side, as seen in *Figure 4.2*.

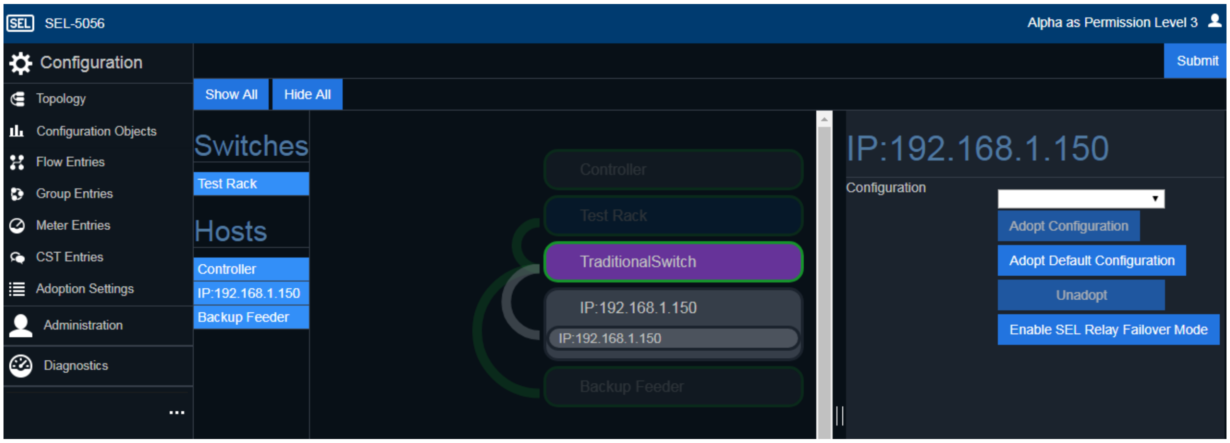


Figure 4.2 Configuring SEL Relay Failover Mode

Step 5. Select **Enable SEL Relay Failover Mode** to place a double ring around the port.

Step 6. Select **Discover Alternate Link** to temporarily disable the first adopted link, allowing the SEL-5056 to discover the second link to the same relay so that it can also be adopted. After a few seconds, the SEL-5056 will move the link back to the first live one.

Managing Devices That Do Not Respond to ARP Probes With an SPA Value of 0.0.0.0

The SEL-5056 uses ARP probes to check the status of discovered devices. The SEL-5056 uses the standard sender protocol address (SPA) value of 0.0.0.0. However, in some rare cases, devices do not respond to ARP requests if the SPA value is not in the subnet. You can change the IP address that the SEL-5056 uses to probe for devices by using the Controller ARP Source IP Address setting in the Adoption Settings page (see *Adoption Settings on page 4.52*). The value should be in the same subnet as all discovered hosts but not an IP address that is used anywhere else.

Managing Traditional Switches

In many cases, the network has traditional switches to which the hosts are connected. These non-SDN switches are connected to the SDN switches. This results in a topology showing multiple hosts connected to the same port of the SEL SDN switch. Represent this more clearly by adding a traditional switch node, as shown in *Figure 4.3*. You may configure the alias of the TraditionalSwitch and any attached ports. Traditional switch nodes are required when you want to use multicast logical connections to multiple endpoints behind a traditional switch on the same OpenFlow port.

There is a port for each connection to another device. Flow programming and logical connections work through these nodes as they would if the host connects directly to the SDN switch. To use logical connections, all links, ports, and nodes must be adopted. Path planning with logical connections is weighted, if possible, to use all SDN paths instead of paths that include traditional switch nodes. However, if the only paths are through traditional nodes, the switches use these paths. The SEL-5056 cannot manage redundancy through traditional switches because the traditional switch manages its own control plane. As the SEL-5056 discovers more hosts on the same SDN switch port, it places and displays these behind the traditional switch node automatically. You can remove and create traditional switch nodes as necessary by selecting the SDN switch port to which the traditional switch port is connected and selecting the **Add Traditional Switch** button in the right-side Configuration pane.

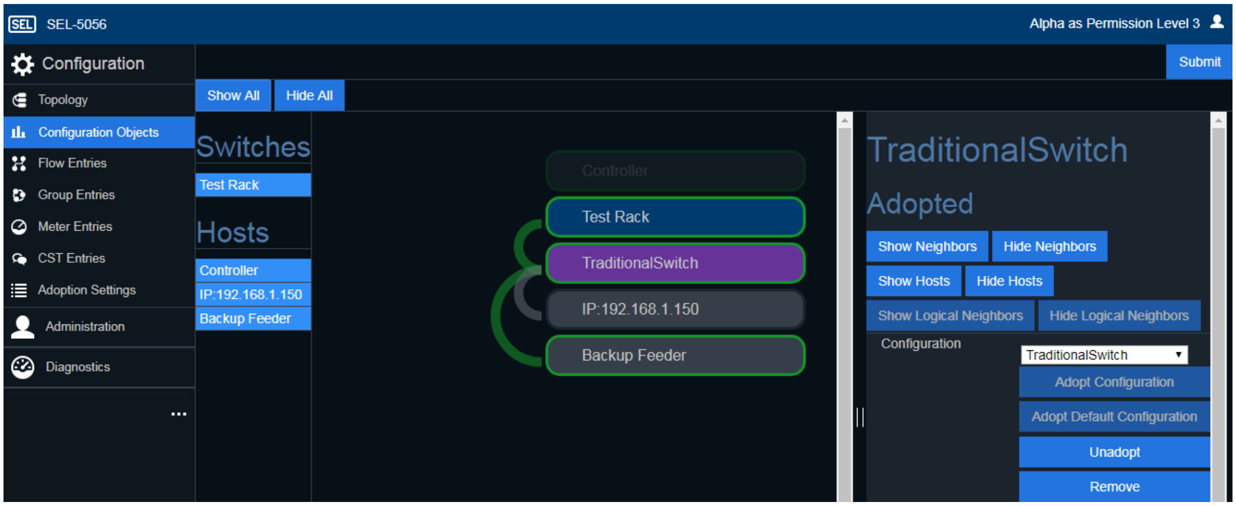


Figure 4.3 Displaying Traditional Switches

Managing SDN-Traditional Switch Network Tie Points

You can connect a traditional switch network to an SDN network by using two links. The SEL-5056 then automatically uses both paths between the two networks when creating logical connections. The SEL-5056 does not program entries to manage the RSTP Bridge Protocol Data Units (BPDUs).

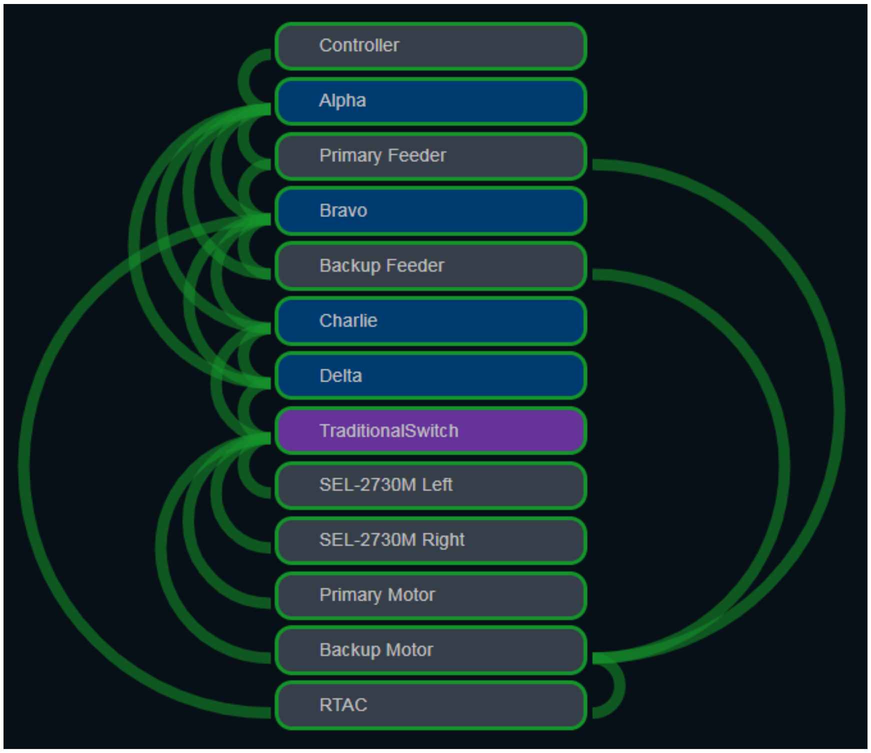
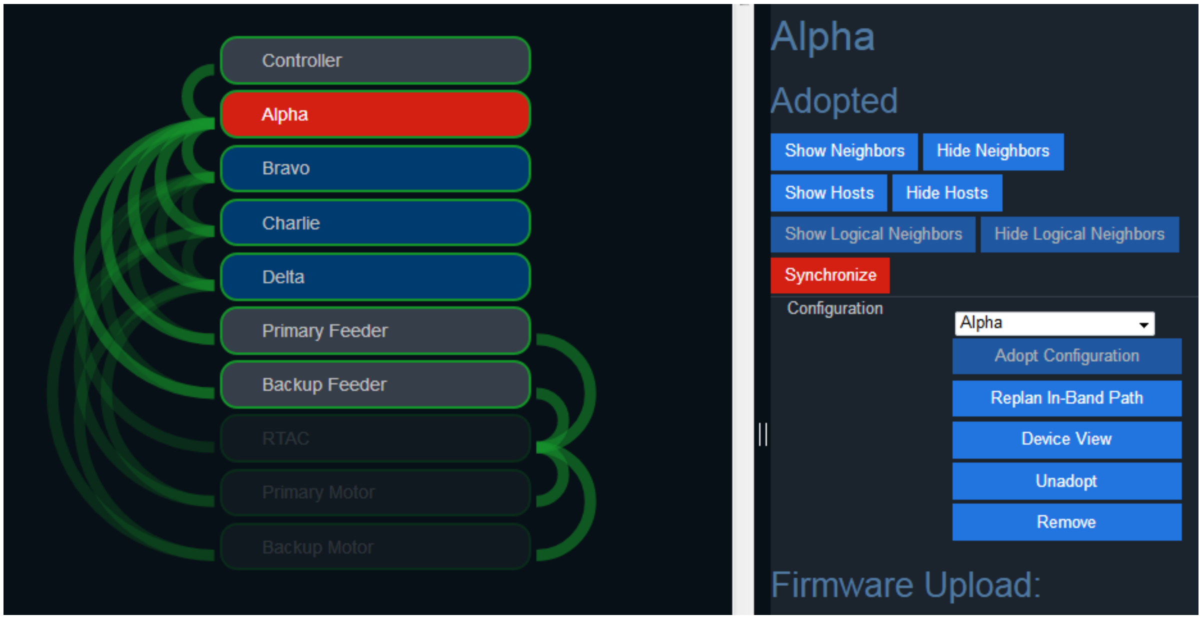


Figure 4.4 Example of a Tie Point That Uses Two Traditional Switches

For more information about SDN-traditional switch networks, see the SEL application guide “Setting Up a Fully Redundant RSTP-to-SDN Tie Point” (AG2017-28), available at selinc.com.

Synchronizing OpenFlow Switches

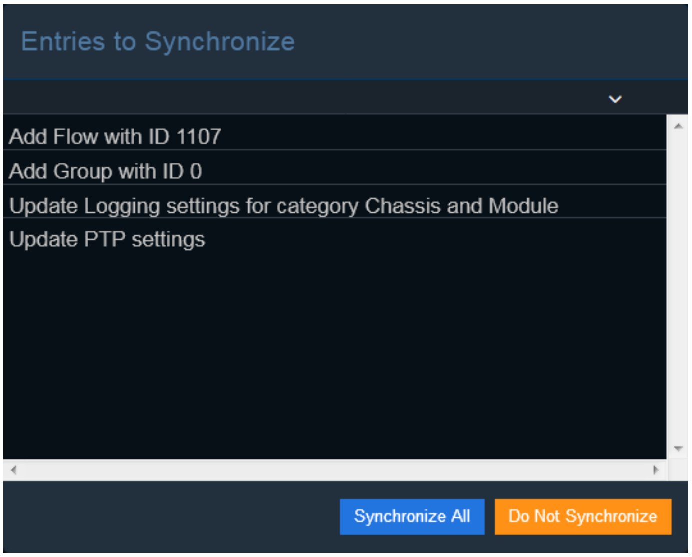
The SEL-5056 monitors the OpenFlow programming and device settings as reported by an OpenFlow switch. If there is a mismatch, the SEL-5056 marks the OpenFlow switch as unsynchronized. User-initiated activities, such as creating LCs or manually adding OpenFlow entries, do not cause a mismatch. When synchronizing, the SEL-5056 adds, modifies, or deletes entries on the OpenFlow switch to eliminate the mismatch. A node may appear as unsynchronized during adoption but this will clear when the configuration has finished, you do not need to synchronize on adoption. When the SEL-5056 detects an unsynchronized OpenFlow switch, the switch appears red in the Topology view and a Synchronize button appears in the Node Options pane.



Configuration Alpha

Figure 4.5 Example of an Unsynchronized SEL-2740S

Step 1. Select the **Synchronize** button to display the list of OpenFlow entries (which the SEL-5056 must add, modify, or delete) or changes to other settings (such as Log settings) on the SEL-2740S to eliminate mismatch.



Add Flow with ID 1107
Add Group with ID 0
Update Logging settings for category Chassis and Module
Update PTP settings

Figure 4.6 Example List of Unsynchronized SEL-2740S OpenFlow Entries

Step 2. Select the **Synchronize All** button to start the synchronization process. The Entries to Synchronize window closes.

Select **Do Not Synchronize** if you do not want to make any changes. The switch remains unsynchronized.

Programming the Network

The SEL SDN system uses OpenFlow as the underlay control plane. This means the switches do not have spanning tree or MAC tables, and flow tables are what manage traffic. The SEL-5056 is the SEL flow controller for programming and monitoring OpenFlow switches. This programming consists of three types of entries:

- Flow
- Group
- Meter

OpenFlow programming provides an open and interoperable way to provision communication circuits in an Ethernet network and give in-depth telemetry data for improved situational awareness. The SEL-5056 configures the forwarding behavior of OpenFlow switches, and it can program them through the use of a network-wide view. Flow entries are switch-specific. The SEL-5056 is flexible to provide the user access to every OpenFlow or automates the OpenFlow configuration through logical connections or even automate logical connection programming through the Learn and Lock extension.

Manual Programming

Manual programming allows you to control the full range of OpenFlow capabilities. You create the necessary and complete flow programming entries for the network to function correctly, and you use the SEL-5056 to program the OpenFlow switches. Manual programming does not rely on the topology shown in the Topology view.

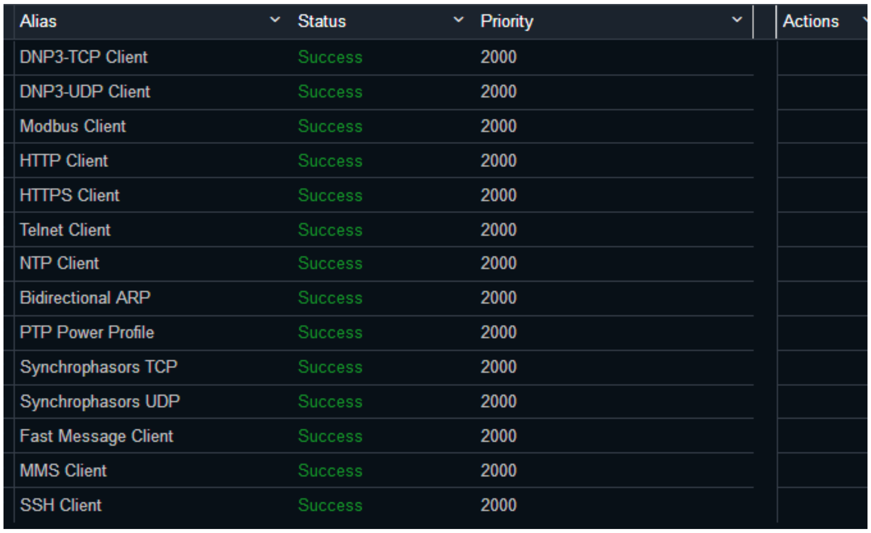
Logical Connection Programming

Logical connections allow the user to define the conversation between source and destination(s) and the SEL-5056 automates the translation of this conversation into all the OpenFlow programming. This removes the burden of detailed OpenFlow programming from the end user and now the user simply defines the conversations they want to allow on the network and the SEL-5056 programs all the OpenFlow in all the switches on behalf of the user. Logical connection programming is a simple three-part process:

1. Adopt links, hosts, and switches.
2. Define the communication service type (CST).
3. Select the start and endpoint(s) for a conversation.

The SEL-5056 automates the path planning by using the shortest path and when redundancy is selected will path plan multiple paths and proactively provision these alternate paths for the circuit.

Logical programming can be a replacement for, or a complement to, manual programming. Logical programming automates the creation of groups and flow entries. The user with the required role (see *Roles on page 2.9*) can access and modify all entries, including the entries created by logical programming.



Alias	Status	Priority	Actions
DNP3-TCP Client	Success	2000	
DNP3-UDP Client	Success	2000	
Modbus Client	Success	2000	
HTTP Client	Success	2000	
HTTPS Client	Success	2000	
Telnet Client	Success	2000	
NTP Client	Success	2000	
Bidirectional ARP	Success	2000	
PTP Power Profile	Success	2000	
Synchrophasors TCP	Success	2000	
Synchrophasors UDP	Success	2000	
Fast Message Client	Success	2000	
MMS Client	Success	2000	
SSH Client	Success	2000	

Figure 4.7 Default CSTs

CSTs

A CST defines how to identify a packet that belongs to a specific conversation. This typically is done by including TCP or UDP port numbers, VLAN tags or any unique identifier of the conversation. When programming logical connections with a CST, the source and destination addresses are added along with the physical input and output ports. CSTs are designated as one-way or bidirectional.

When you select bidirectional, the SEL-5056 automates the configuration of flows for Ethernet communications from a source to a destination and from the destination back to the source so you do not need to create two circuits; both will be programmed for you on the first action. The appropriate values in the match criteria are automatically flipped to simplify the process. For example, if the TcpDst match field is present in the CST, the value of TcpDst becomes the value for TcpSrc in the return packet. Logical connections can also be used with redundancy. This is an N-1 link redundancy, which means that the SEL-5056 programs flows that can handle any single link failure between a switch-to-switch hop. The SEL-5056 programs any available redundancy into logical connections. If no redundant links exist in any given switch-to-switch hop, path planning shows an absence of redundancy by coloring links yellow in the Topology view. After the SEL-5056 programs the logical connections, a link displays on the right side of the stack view in the Topology page. Select this new link to show the status of the logical connection and to see the path that the logical connection takes through the network.

The SEL-5056 uses CSTs to match traffic for a logical connection. A CST consists of a user-supplied list of match fields, a priority setting, Cast Type (see *Table 4.7*), Proactive Failover, and SetQueue settings. The user may add any match field except for InPort. If the match field added is the same as one of the ones added by the LC (*Table 4.8*), the user-supplied match field value overrides the value supplied by the LC.

Table 4.7 Cast Type

Type	Description
Unicast	Programs a connection from source to destination.
Bidirectional Unicast	Programs two connections, from source to destination and then from destination to source reversing the match fields as applicable.

Proactive failover can be enabled independent of the cast type. When enabled, the SEL-5056 attempts to program N-1 redundancy for every link. If there is a redundant path for some but not all links, the SEL-5056 will program redundancy for those links. Selecting the logical connection in the topology shows whether redundancy was programmed for a link. The SetQueue settings set the priority queue for the flow entries programmed for the logical connection.

There are two types of logical programming designed to support unicast and multicast flows. *Table 4.8* shows the difference in configuration between these logical programming options.

Table 4.8 OpenFlow Components Used in Logical Programming

Flow Entry Component	Unicast[a]	Multicast
Match Fields	If CST contains the Match Field EthType with value IPv4: InPort + Ipv4Src + Ipv4Dst + CST match fields If CST contains the Match Field EthType with value ARP: InPort + ArpSpa + ArpTpa + CST match fields Else: InPort + EthSrc + EthDst + CST match fields	InPort + EthSrc + CST match fields
Priority	CST Priority setting	

[a] Unidirectional or bidirectional.

Default CSTs

The SEL-5056 has default CSTs for many common protocols for use in making logical connections. You can use these CSTs immediately for setting up logical connections. Ipv4Dst and Ipv4Src match fields are automatically added to the line circuits (LCs) made from IP-based CSTs. ArpTpa and ArpSpa are automatically added to LCs, created by using the bidirectional ARP CST (see *Table 4.9*). Default CSTs cannot be modified or deleted.

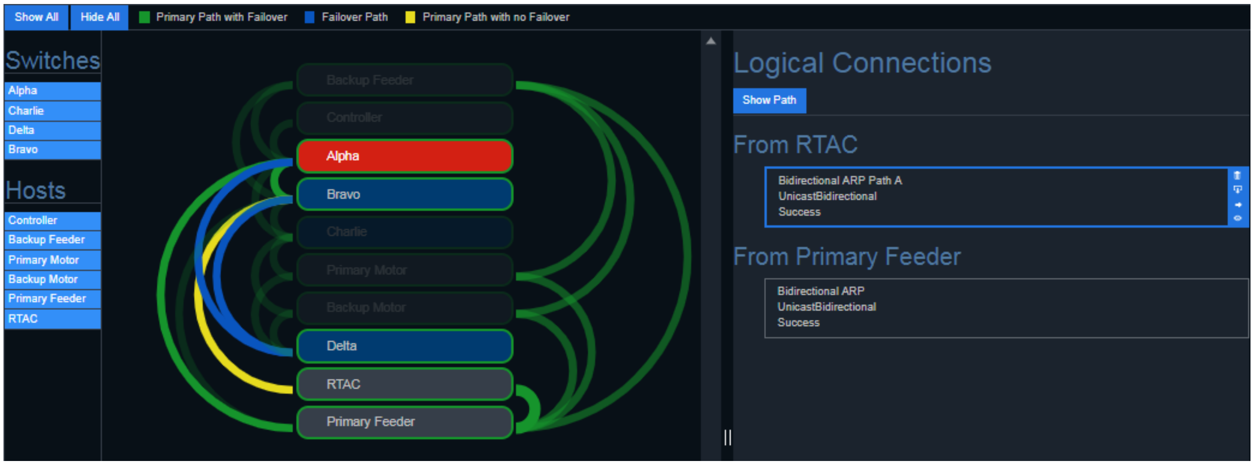
Table 4.9 Default CSTs

Alias	Match Fields		Cast Type[a]
	Type	Value	
ARP	EthType	ARP	Bidirectional Unicast
DNP3-TCP Client	TcpDst	20000	Bidirectional Unicast
DNP3-UDP Client	UdpDst	20000	Bidirectional Unicast
HTTP Client	TcpDst	HTTP	Bidirectional Unicast
HTTPS Client	TcpDst	HTTPS	Bidirectional Unicast
ICMP	IpProto	ICMP	Bidirectional Unicast
MMS Client	TcpDst	MMS	Bidirectional Unicast
Modbus Client	TcpDst	502	Bidirectional Unicast
NTP Client	TcpDst	NTP	Bidirectional Unicast
Power Profile PTP	EthType EthDst	PTP 011B19000000	Multicast
SSH Client	TcpDst	SSH	Bidirectional Unicast
Synchrophasors TCP	TCP	Synchrophasors	Bidirectional Unicast
Synchrophasors UDP	UDP	Synchrophasors	Bidirectional Unicast
Telnet/Fast Message Client	TcpDst	23	Bidirectional Unicast

[a] All default CSTs have Proactive Failover enabled.

Logical Connections With Redundancy

CSTs define if redundancy is built for the logical connections that use the CST. When you use CSTs with redundancy in logical connection programming, the communications finds a primary and a secondary path to deliver the packet to its destination at each hop. This means that any single link lost on the path delivering the packet heals and continues to operate. When programming these logical connections, you are able to see the primary and failover path that the packet takes at each hop. *Figure 4.8* shows this. The key displays across the top.



Bidirectional ARP Path A
UnicastBidirectional
Success

Bidirectional ARP
UnicastBidirectional
Success

Figure 4.8 Displaying Path Planning

Manual Programming Versus Logical Programming

Use logical connections whenever possible because this groups all the OpenFlow programming together for the entire circuit and you simplify the initial configuration, change management, and decommissioning efforts through the entire communications circuit life cycle. You manage the circuit not the OpenFlow settings and allow the SEL-5056 automation to manage the OpenFlow settings for you.

Management Traffic

The SEL-5056 configures each switch and then monitors the events and statistics of each switch. The SEL-5056 is throttled to collect the logs and diagnostics from one switch every 10 seconds. This means that the network load on the CPU that the controller is running on is fixed and does not scale with increased network size. This helps ensure that the in-band (IB) management does not impact operational flows.

IB Redundancy

When a switch is first adopted, the SEL-5056 attempts to program the IB management connection with redundancy based on the currently adopted topology. To replan the connection, such as after adopting further paths to improve the redundancy, select the **Replan In-Band Path** button (see *Figure 4.13*) and the SEL-5056 replans the connection and adds link redundancy if possible. This redundancy extends to all links that have a redundant path.

Default Adoption Flow Entries

The SEL-5056 enters new default flows and groups to each switch it adopts. These default flows are intended to preserve the communications between the SEL-5056 and the switch it is adopting. There are two options for adopting the switch, in-band and out-of-band (OOB), but the flows automatically programmed into the switches maintain the same purpose. These default flows have alias names beginning with **SEL-5056:**. These names should not be changed. The default priorities of these default flows are 0, 1, 60000, and 65000. Flows programmed above and below these priorities are in danger of interfering with or being overruled by the default adoption rules. To avoid interference, always use flow priorities that fall between 2 and 59999.

Managing PTP

Managing Precision Time Protocol (PTP) Power Profile network configurations through the use of the SEL-5056 is accomplished in two steps.The first step is validating that each SDN switch has PTP enabled. The second step is configuring OpenFlow programming to send Sync and Announce messages from the PTP master clock to each PTP client. Using logical connections and the default PTP CST is the best way to accomplish this programming.

The SEL-5056 assists the user by doing the following:

- Adding a flow entry to forward P2P traffic to the local port as part of the default adoption flow entries.
- Adding a Layer 2 PTP CST to the default CSTs that you can use to create the LC to forward Sync and Announce messages to PTP masters and PTP clients (see *Table 4.9*).
- Providing a Global Enable/Disable setting to turn PTP on and off for the entire switch through the configuration object settings. By default, PTP is disabled.

For each potential master, use the PTP Power Profile CST (or one you created) to create an LC between itself and every other master and all clients. Because the SEL SDN switch must also be syntonized to meet Power Profile performance, a copy of the PTP packet also is sent to the switch processor automatically.

SEL-5056 Configuration Pages

Topology

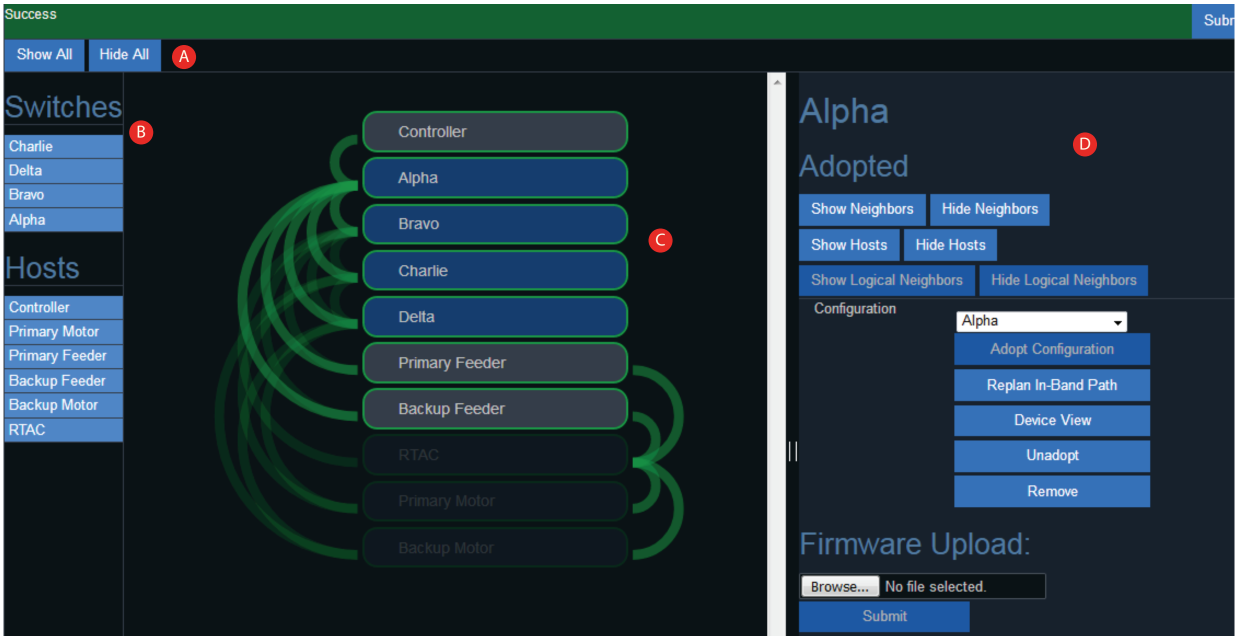
Use the Topology page to view the physical and logical state of the network and provision communication circuits.

Views

Navigation Menu

Select **Topology** (under the Configuration menu) to access the Topology page.

Topology Page



(A) **Topology View Buttons:** Manage the view of the network.

(B) **Switch Toggle List:** Lists switches in the network.

(C) **Topology View:** Shows the currently configured view of the network.

(D) **Object Options Pane:** Shows the settings and information about the currently selected topology object.

Figure 4.9 Topology Page

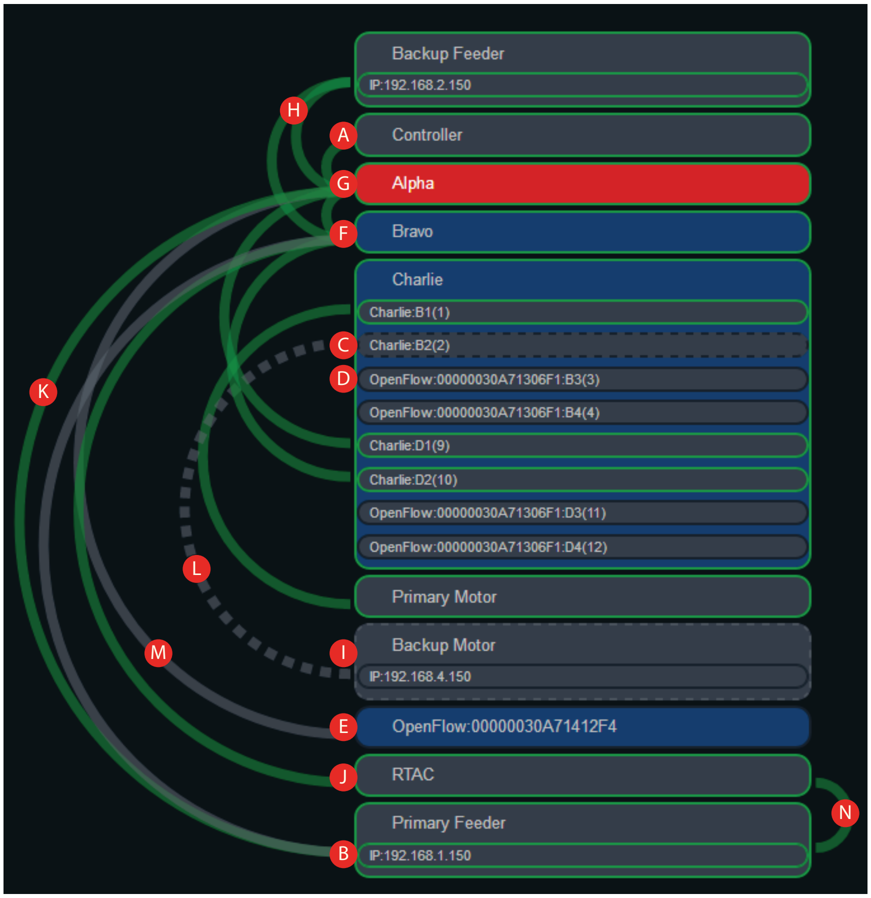
The Switch toggle list allows you to quickly add and remove a switch from the current Topology view. You can select more than one switch; a selected switch displays in the Topology view.

Use the Topology view buttons located in the menu drop-down to manage how objects in the Topology view display. *Table 4.10* lists the buttons and their functions.

Table 4.10 Topology View Buttons

Name	Effect on the Topology View
Show All	Shows all nodes, links, and logical connections; selects all switches in the Switch toggle list (*Figure 4.10*)
Hide All	Hides all switch nodes (except for unadopted host and uncommissioned OpenFlow switch nodes)
Show Neighbors	Shows all nodes attached to the selected node
Hide Neighbors	Hides all nodes attached to the selected node
Show Hosts	Shows all hosts
Hide Hosts	Hides all hosts
Show Logical Neighbors	Shows all nodes and links attached by logical connections to the selected node
Hide Logical Neighbors	Hides all nodes and links attached by logical connections to the selected node
Remove Selected	Removes the selected node from view
Show Path	Shows the path for the selected logical connection

Topology View



(A) **Controller:** The node representing the SEL-5056 host machine.

(B) **Up Adopted Port:** An SEL-2740S port that is up.

(C) **Down Adopted Port:** An SEL-2740S port that is down.

(D) **Unadopted Port:** A port that is part of an unadopted node and is unadopted itself.

(E) **Unadopted SEL SDN Switch Node:** An SEL-2740S that has been detected but not adopted.

(F) Adopted SEL SDN switch node

(G) Unsynchronized SEL SDN switch node

(H) Two Ports in Failover Mode

(I) **Offline Host:** A host that has been detected but not configured.

(J) **Adopted Online Host:** A host that has been adopted and is connected and online.

(K) **Up Adopted Link:** A physical link that has been adopted and is live.

(L) **Down Adopted Link:** A physical link that has been adopted and is down.

(M) **Up Unadopted Link:** A physical link that has been detected but not configured.

(N) **Logical Connection:** A logical connection between a source and a destination node.

Figure 4.10 Topology View

You can select and drag any node up and down to change its order in the list.

A display format, listed in *Table 4.11*, indicates the state of each node. The controller node is always adopted and up.

Table 4.11 Border Display Format for Different Node Statuses

Border Display Format		Adoption Status	
		Adopted	Unadopted
Link Status	Up	Solid green	Solid uncolored
	Down	Dashed uncolored	

The color of the node indicates whether the node is an SEL SDN switch node. See *Table 4.12* for a color key. *Object Management on page 4.2* explains node types.

Table 4.12 Fill Color for Different Node Types

Type	Fill Color of Node
SEL SDN switch	Blue
Controller	Gray
Host	Gray
Generic	Gray

A display format, listed in *Table 4.13*, indicates the state of each link. Unadopted links, when down, do not display in the Topology view.

Table 4.13 Display Format for Links

Display Format		Adoption Status	
		Adopted	Unadopted
Link Status	Up	Solid green	Solid uncolored
	Down	Dashed uncolored	Does not display in the Topology view

Logical connections are always colored green, regardless of status.

The contents of the option window depend on the type of element you select. There are five possible option pane views, depending on which of the following elements you select:

- SEL SDN switch node
- Host node (adopted and unadopted)
- Port
- Physical link
- Logical connection

Node View

Nodes have two display states: expanded and collapsed. Selecting a node name toggles between the two display states. In the expanded view, you can select individual ports and the links from each port display. In the collapsed view, all the links are collected together.

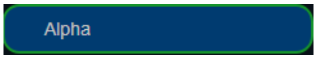
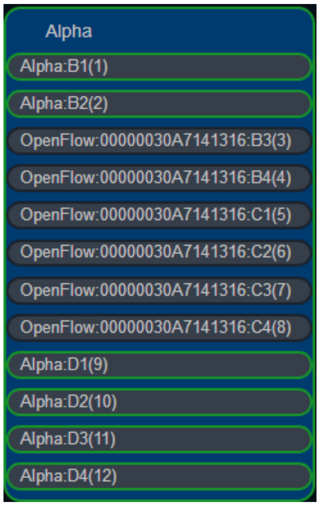


Figure 4.11 Collapsed Node View



Alpha

Alpha:B1(1)

Alpha:B2(2)

OpenFlow:00000030A7141316:B3(3)

OpenFlow:00000030A7141316:B4(4)

OpenFlow:00000030A7141316:C1(5)

OpenFlow:00000030A7141316:C2(6)

OpenFlow:00000030A7141316:C3(7)

OpenFlow:00000030A7141316:C4(8)

Alpha:D1(9)

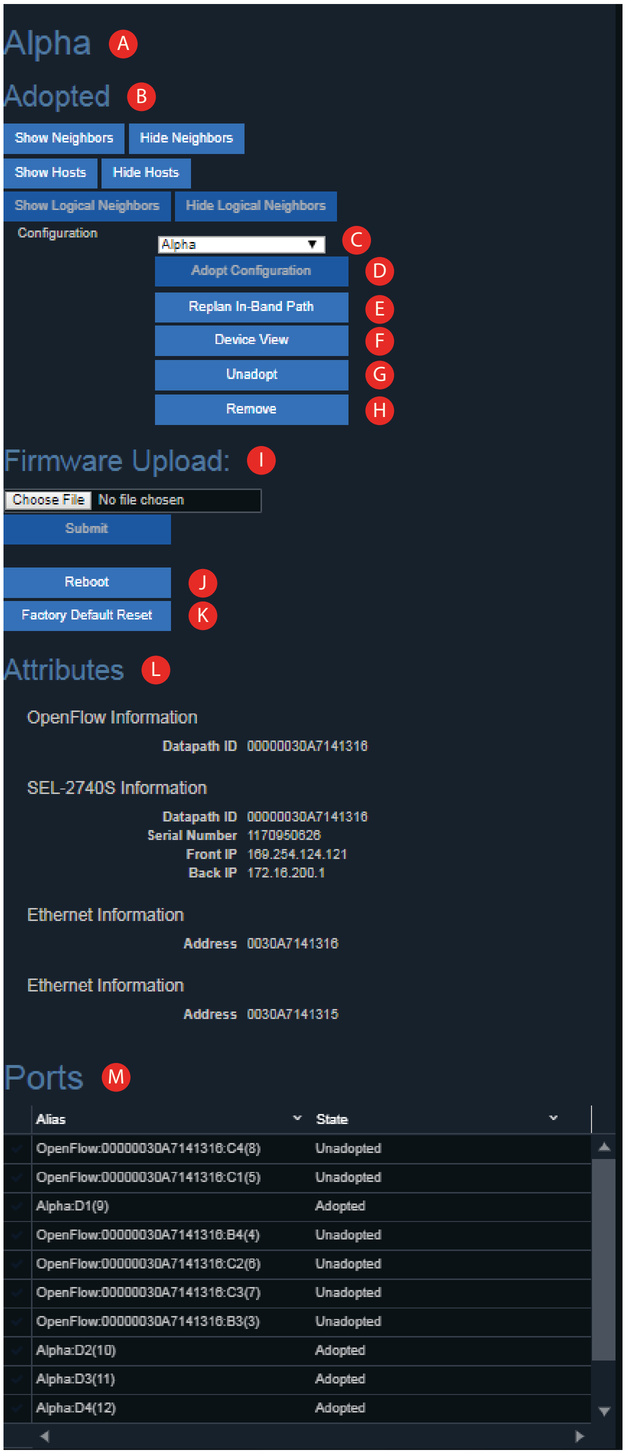
Alpha:D2(10)

Alpha:D3(11)

Alpha:D4(12)

Figure 4.12 Expanded Node View

SEL SDN Switch Node Options Pane



OpenFlow Information

Datapath ID 00000030A7141316

SEL-2740S Information

Datapath ID 00000030A7141316
Serial Number 1170950626
Front IP 169.254.124.121
Back IP 172.16.200.1

Ethernet Information

Address 0030A7141316

Ethernet Information

Address 0030A7141315

Alias	State
OpenFlow:00000030A7141316:C4(8)	Unadopted
OpenFlow:00000030A7141316:C1(5)	Unadopted
Alpha:D1(9)	Adopted
OpenFlow:00000030A7141316:B4(4)	Unadopted
OpenFlow:00000030A7141316:C2(6)	Unadopted
OpenFlow:00000030A7141316:C3(7)	Unadopted
OpenFlow:00000030A7141316:B3(3)	Unadopted
Alpha:D2(10)	Adopted
Alpha:D3(11)	Adopted
Alpha:D4(12)	Adopted

Figure 4.13 SEL SDN Switch Node Options Pane

(A) **Name:** Displays the node name in the alias or in the operational node display format (see *Table 4.4* and *Table 4.5*).

(B) **Adoptions Status:** Shows whether the node is adopted, unadopted, or disconnected.

(C) **Configuration Node:** The configuration node applied to the SEL SDN switch operational node; blank if not yet configured.

(D) **Adopt Configuration Button:** Applies (or replaces, if another configuration node has already been applied) the configuration node you selected to the SEL SDN switch you selected.

(E) **Replan In-Band Path:** Recreates the IB management logical connection with N-1 link redundancy.

(F) **Device View Button:** Opens a new tab or window on the SEL SDN switch Device View page (see *SEL SDN Switch Device View, Local Syslog Events, and Alarms Pages on page 4.55*).

(G) **Unadopt Button:** Unadopts the node, removing the configuration object from the operational object; the SEL-5056 attempts to uncommission the SEL SDN switch.

(H) **Remove Button:** Removes the node from the Topology view; the node appears again if it sends traffic.

(I) **Firmware Upload:** Upload new firmware to the selected switch.

(J) **Reboot Button:** Resets the switch if the SEL-5056 can communicate with the switch over the management channel.

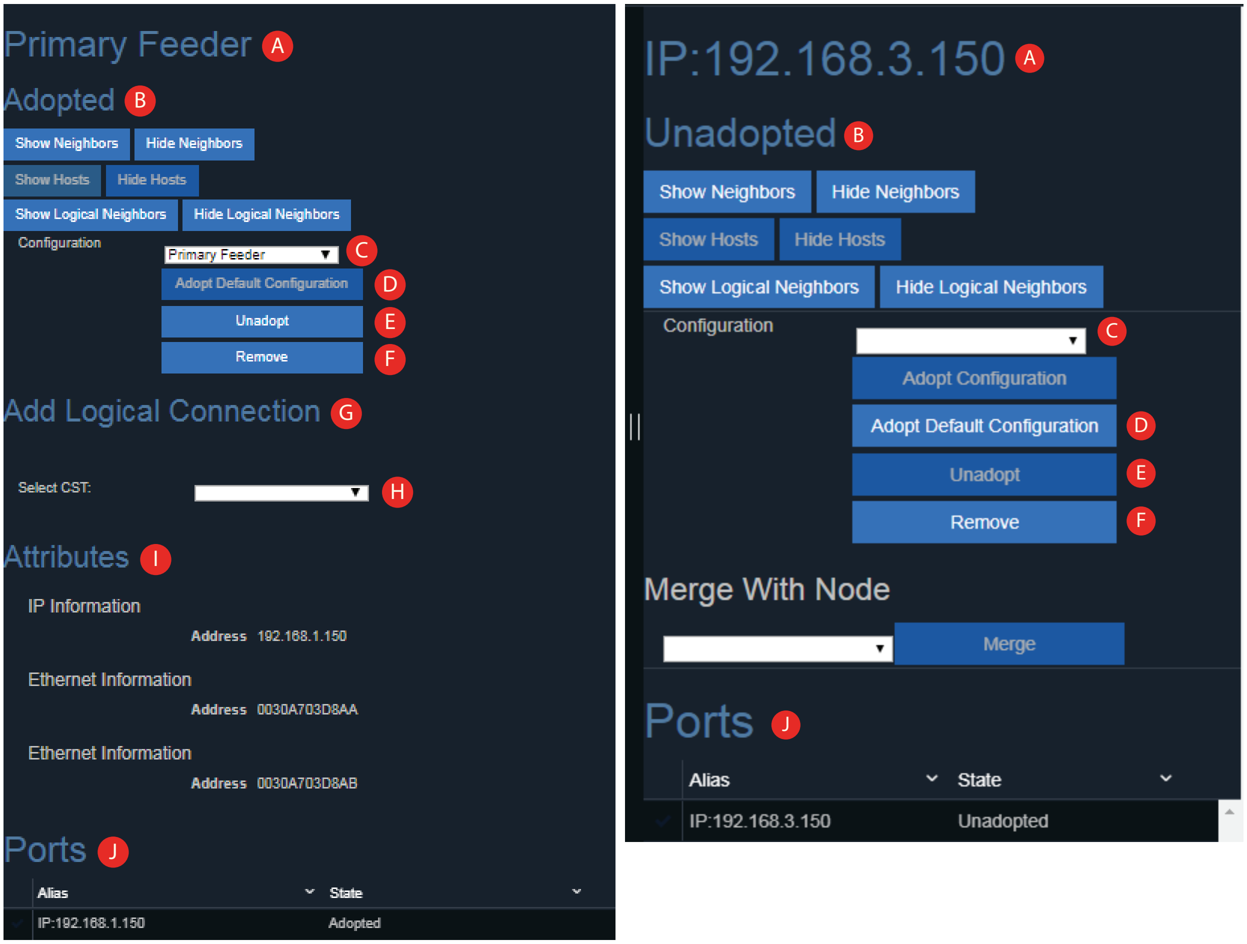
(K) **Factory Default Reset Button:** Performs a factory-default reset of the switch if the SEL-5056 can communicate with the switch over the management channel.

(L) **Attributes:** List of attributes for the SEL SDN switch.

(M) **Ports:** List of ports and their states.

(N) **Add Hosts:** Adds a host node to the selected switch port to enable offline configuration.

Host Node Options Pane



IP Information

Address 192.168.1.150

Ethernet Information

Address 0030A703D8AA

Ethernet Information

Address 0030A703D8AB

Alias	State
IP:192.168.1.150	Adopted

Alias	State
IP:192.168.3.150	Unadopted

Adopted Host Node Options Pane **Unadopted Host Node Options Pane**

(A) **Name:** Displays the node name either in the alias or in the operational node display format (see *Table 4.4*).

(B) **Adoption Status:** Unadopted, adopted, or disconnected.

(C) **Configuration Object Setting:** Allows you to select a configuration node to apply to the operational host node; blank if not yet configured.

(D) **Adopt Default Configuration:** Creates a configuration node with default settings; you can modify this on the Configuration Objects page.

(E) **Unadopt Button:** Unadopts the node.

(F) **Remove Button:** Changes the state of the node to Disconnected (if adopted) or removes the node from the Topology View (if not adopted) or reappears on the Topology View (if not adopted) if it sends traffic.

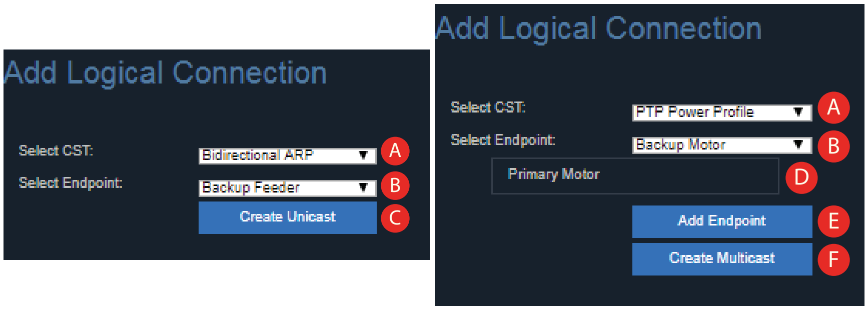
(G) **Add Logical Connection:** Settings for adding a new logical connection from the selected node.

(H) **Select CST:** The CST used for the logical connection from the CST Entries page. If a CST with cast type Unicast or Bidirectional Unicast is selected, the Add Unicast Logical Connection settings are shown (see the left side of *Figure 4.15*). If a CST with cast type Multicast is selected, the Add Multicast Logical Connection settings are shown (see the right side of *Figure 4.15*).

(I) **Attributes:** List of attributes for the SEL-2740S.

(J) **Ports:** List of ports and their states.

Figure 4.14 Host Node Options Pane



Add Logical Connection

Select CST: Bidirectional ARP

Select Endpoint: Backup Feeder

Add Logical Connection

Select CST: PTP Power Profile

Select Endpoint: Backup Motor

Primary Motor

Add Unicast Logical Connection **Add Multicast Logical Connection**

(A) **Select CST:** The CST used for the logical connection from the CST Entries page. If a CST with cast type of Unicast or Bidirectional Unicast is selected, the Add Unicast Logical Connection settings (on the left side of this figure) are shown. If a CST with cast type of Multicast is selected, the Add Multicast Logical Connection settings (on the right side of this figure) are shown.

(B) **Select Endpoint:** The endpoint for the logical connection; the selected node is the start point.

(C) **Create Unicast Button:** Submits the Unicast Logical Connection settings.

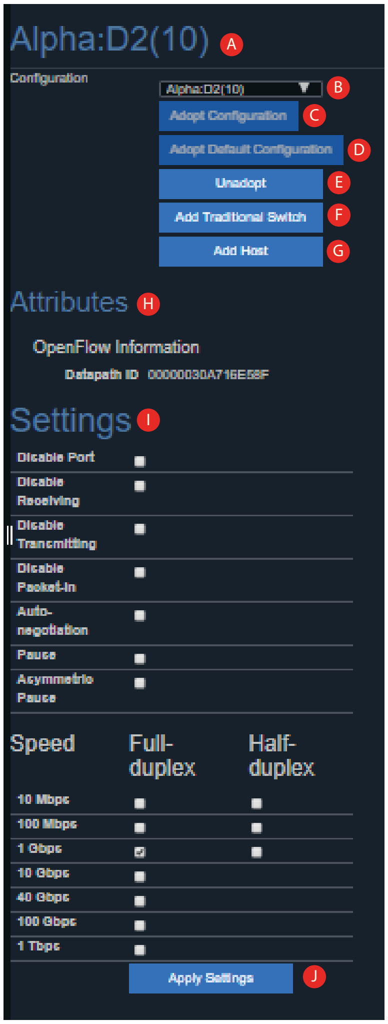
(D) **Endpoint List:** Determines the list of endpoints selected in (B).

(E) **Add Endpoint Button:** Adds an endpoint to the multicast logical connection.

(F) **Create Multicast Button:** Submits the Multicast Logical Connection settings.

Figure 4.15 Add Logical Connection Subpane

SEL-2740S Port Options Pane



OpenFlow Information

Datapath ID 00000030A716E58F

Disable Port	□
Disable Receiving	□
Disable Transmitting	□
Disable Packet-In	□
Auto-negotiation	□
Pause	□
Asymmetric Pause	□

Speed	Full-duplex	Half-duplex
10 Mbps	□	□
100 Mbps	□	□
1 Gbps	☑	□
10 Gbps	□	
40 Gbps	□	
100 Gbps	□	
1 Tbps	□	

(A) **Name:** Displays the node name in either the configuration port alias (A in *Figure 4.28*) or in the operational port display format (*Table 4.5*).

(B) **Configuration Object Setting:** Allows the user to select a configuration node to apply to the operational host node; shows the configuration node applied to the SEL-2740S operational node; blank if not yet configured.

(C) **Adopt Configuration Button:** Applies (or replaces if another configuration node has already been applied) the selected configuration node to the select port.

(D) **Adopt Default Configuration:** Have the SEL-5056 create a new generic configuration node object and adopt the selected host with it.

(E) **Unadopt Button:** Unadopt selected port.

(F) **Add Traditional Switch Button:** Add a traditional switch to the selected port (see *Managing Traditional Switches on page 4.6*).

(G) **Add Host:** Add a host node for offline configuration

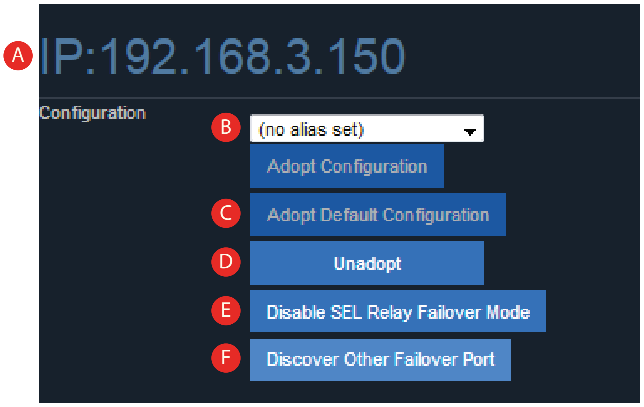
(H) **Attributes:** List of attributes for the selected SEL-2740S port.

(I) **OpenFlow Port Settings:** Displays the OpenFlow Port settings listed in *Table 3.4*.

(J) **Apply Settings Button:** Apply the OpenFlow port settings.

Figure 4.16 SEL-2740S Port Options Pane

Host Port Options Pane


A
IP:192.168.3.150
Configuration
B
(no alias set)
Adopt Configuration
C
Adopt Default Configuration
D
Unadopt
E
Disable SEL Relay Failover Mode
F
Discover Other Failover Port

(A) **Name:** Displays the node port name.

(B) **Configuration Drop-Down Menu:** Allows you to select a configuration node to apply to the operational host node; shows the configuration node applied to the SEL-2740S operational node; blank if not yet configured.

(C) **Adopt Default Configuration:** Applies (or replaces, if another configuration node has already been applied) the selected configuration node to the selected port.

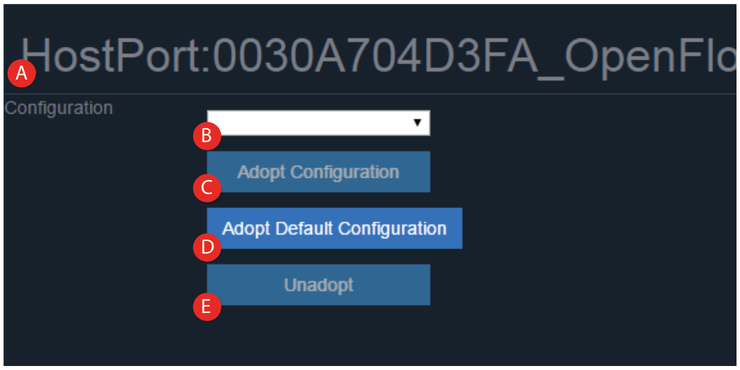
(D) **Unadopt:** Allows the removal or changing of the configuration node associated with the host node.

(E) **Enable or Disable SEL Relay Failover Mode:** Allows the binding of two links to work as one during communication with SEL relays operating in failover mode.

(F) **Discover Other Failover Port Button:** The SEL-5056 attempts to find the other failover link by using OpenFlow port settings to disable the currently active link for a short period of time. (Appears when SEL Relay Failover mode is enabled.)

Figure 4.17 Host Port Options Pane

Link Options Pane



(A) **Name:** Displays the node name in either the configuration link object alias or in the Operational node display format (*Table 4.4*).

(B) **Configuration Drop-Down Menu**: Allows you to select a configuration node to apply to the operational host node; shows the configuration node applied to the SEL-2740S operational node; blank if not yet configured.

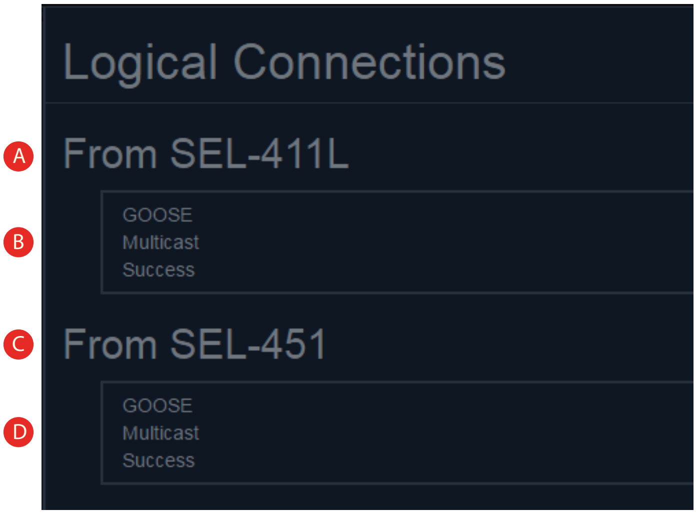
(C) **Adopt Configuration Button:** Configures to a selected configuration node.

(D) **Adopt Default Configuration:** Creates a configuration node with default settings; you can modify this on the Configuration Objects page.

(E) **Unadopt Button:** Unadopts the node.

Figure 4.18 Link Options Pane

Logical Connections Options Pane



Logical Connections

From SEL-411L

GOOSE
Multicast
Success

From SEL-451

GOOSE
Multicast
Success

(A) **From Node A:** Displays the name of Node A.

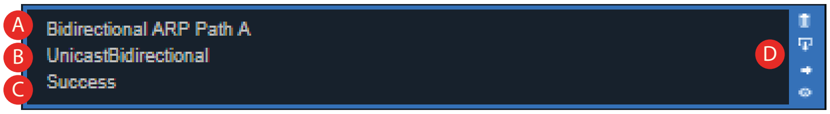
(B) **Logical Connections List From Node A:** Lists logical connections from Node A.

(C) **From Node B:** Displays the name of Node B.

(D) **Logical Connections List From Node B:** Lists logical connections from Node B.

Figure 4.19 Logical Connection Options Pane

Logical Connection Box



Bidirectional ARP Path A
UnicastBidirectional
Success

(A) **CST Name:** Displays the name of the CST for a logical connection.

(B) **Communications Type:** Displays the communications type of the logical connection, whether unicast or multicast (for unicast, shows whether it is bidirectional).

(C) **Status:** Displays the logical connection status (see *Table 4.15*).

(D) **Actions:** Displays a list of actions for the logical connection (see *Table 4.18*).

Figure 4.20 Logical Connection Box

The color of the unselected Logical Connection box indicates its state (see *Table 4.14*). When you select this box, its color can be blue or green.

Table 4.14 Logical Connection Color Key

State	State
Gray	Applied
Blue	Added, but not yet submitted
Green	Select the Action ⟳ icon to move to the applied state
Red	Set to be deleted when the page is submitted

The logical connection may have one of three statuses, listed in *Table 4.15*.

Table 4.15 Logical Connection Status Message

Status	Description
Success	The logical connection was created and the OpenFlow entries were successfully created.
Failure	The logical connection was not created, or the OpenFlow entries were not successfully created.
Error	There is an error in the submission of the logical connection. The error message will attempt to describe what is wrong.

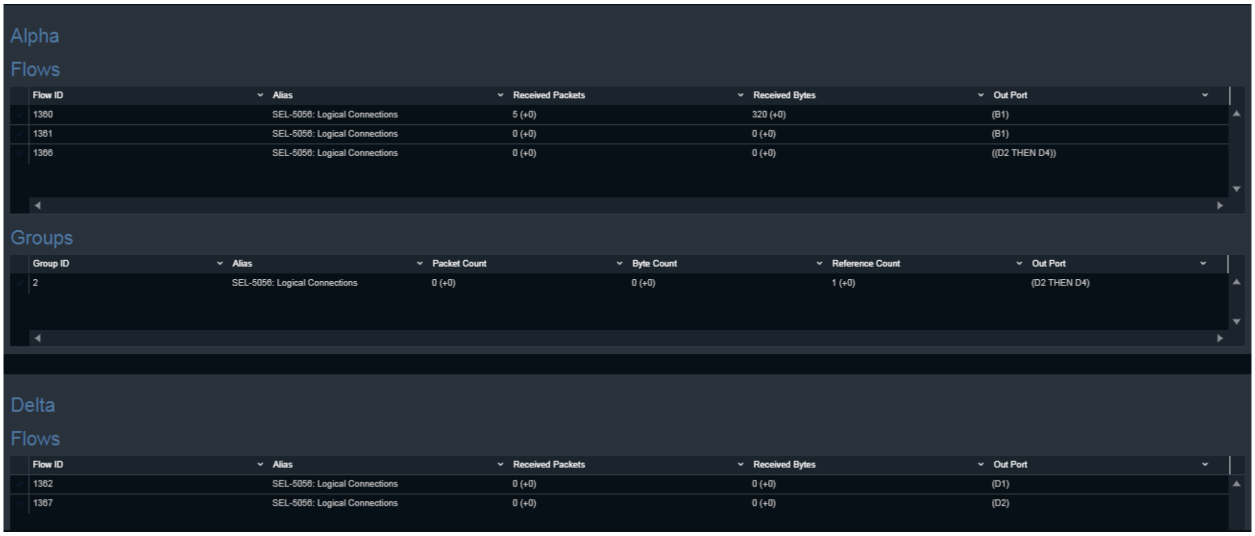
One or more of the actions shown in *Table 4.16* may be available for a logical connection.

Table 4.16 Logical Connection Actions

Action	Icon	Description	When Present
Delete	🗑	Delete the logical connection (you must select **Submit** to complete)	Always
Resubmit	⇩	Re-create the logical connection (may lead to traffic disruption)	Always
Path Toggle	➡	Toggled between the path from each source port	When the source device is in SEL Relay Failover mode
Detailed View	👁	List of flow and group entries on each switch for the logical connection	When the logical connection is successfully created

Logical Connection Detailed View

Accessed through the Detailed View action in the Logical Connections box. The Logical Connection Diagnostics view shows all the flow and group entries and their diagnostics used by the logical connections.



Alpha

Flows

Flow ID	Alias	Received Packets	Received Bytes	Out Port
1360	SEL-5056: Logical Connections	5 (+0)	320 (+0)	(B1)
1361	SEL-5056: Logical Connections	0 (+0)	0 (+0)	(B1)
1366	SEL-5056: Logical Connections	0 (+0)	0 (+0)	((D2 THEN D4))

Groups

Group ID	Alias	Packet Count	Byte Count	Reference Count	Out Port
2	SEL-5056: Logical Connections	0 (+0)	0 (+0)	1 (+0)	(D2 THEN D4)

Delta

Flows

Flow ID	Alias	Received Packets	Received Bytes	Out Port
1362	SEL-5056: Logical Connections	0 (+0)	0 (+0)	(D1)
1367	SEL-5056: Logical Connections	0 (+0)	0 (+0)	(D2)

Figure 4.21 Detailed View

Instructions

Restarting an SEL SDN Switch

Step 1. Go to the Topology page.

Step 2. Select the SEL SDN switch to restart. The Option window displays the SEL SDN switch Node Options pane.

Step 3. Select the **Reboot** button.

Step 4. Select the **Reboot Device** button in the Reboot Confirmation window that appears.

Factory-Default Resetting an SEL SDN Switch

Step 1. Go to the Topology page.

Step 2. Select the SEL SDN switch to perform the factory-default reset. The Option window displays the SEL SDN switch Node Options pane.

Step 3. Select the **Factory Default Reset** button.

Step 4. Select the **Factory Default Reset Device** button in the Factory Default Reset Confirmation that appears.

Uploading Firmware to an SEL SDN Switch

Step 1. Go to the Topology page and select the switch on which you want to upgrade the firmware.

Step 2. Select **Choose File** and then select the firmware file.

Step 3. Select the **Submit** button to start the firmware upgrade process.

Step 4. Select the **Device View** button to view the status of the firmware upgrade.

Adopting an SEL SDN Switch

Requirements

You must create an SEL SDN switch configuration node object before adoption.

Steps

Step 1. Go to the Topology page.

Step 2. Select on the SEL SDN switch you want to adopt. The Option window shows the SEL SDN switch Node Options pane.

Step 3. Select the SEL SDN switch configuration node from the Configuration setting. The Adopt Configuration button is enabled.

Step 4. Select the **Adopt Configuration** button. The Feedback bar displays Success to indicate the successful application of the configuration node. The adoption process starts.

Step 5. Wait until the alarm contact pulses (about 30 to 60 seconds).

After selecting the **Adopt** button, the process may take a minute or longer to complete, depending on the speed of the SEL-5056 host machine. When complete, the selected object becomes adopted, the appropriate ports appear, and the Adoption State is Adopted. The SEL-5056 has four stages of adoption. The first stage sets the IP address, subnet mask, and default gateway of the switch. These settings are pulled from the configuration node being used for adoption and are applied to the in-band or out-of-band adoption interface being used. The second stage starts once the SEL SDN switch applies the new addresses from stage one and the SEL-5056 establishes communications on the REST interface by using TCP Port 443 to upload the new certificates, set the time, and complete the administrative OpenFlow configurations. In the third stage, the SEL-5056 waits for the switch to communicate with the SEL-5056 through the use of OpenFlow and once this happens, SEL-5056 also connects to the REST interface again. In this third stage, all the final network addressing and cybersecurity trust management is used. In the final stage, the SEL-5056 programs all the OpenFlow flows and completes all the other settings for the configuration node.

Adopting an Object

Use this instruction to adopt a host, link, or port.

Steps

Step 1. Go to the Topology page.

Step 2. Select the object to adopt. The Option window displays the appropriate options pane.

Step 3. Then either:

- ➢ Select the configuration object from the Configuration setting and
- ➢ Select the Set Configuration button

Or (if using the default configuration)

- ➢ Select the Adopt Default Configuration button

Creating a Logical Connection

Requirements

- ➤ The source and destination node(s) are adopted
- ➤ A path of adopted links exists between the source and destination node(s)
- ➤ A CST has been created

Settings

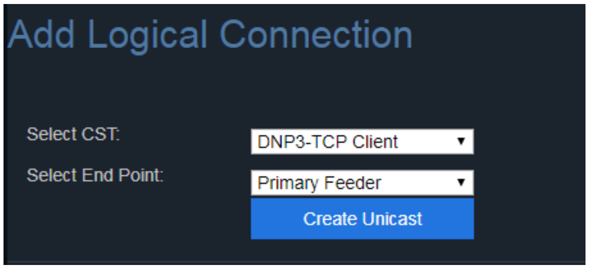
Table 4.17 Settings for Creating a Unicast Logical Connection

Setting	ID	Description	Valid Values
CST	1	Alias of the CST entry to use for the logical connection	Any of the CST profiles on the CST Editor page that have not already been used to create a logical connection between the source (2) and destination (3) nodes
Source Node	2	Source node for the traffic	Any of the adopted nodes in the Topology view
Destination Node	3	Destination node for the traffic	Any of the adopted nodes or SEL-2740S switches in the Topology view that are not the source node (2). A unicast LC can only have one destination node. The destination node may be in SEL Relay Failover mode.

Steps

Step 1. Go to the Topology page and select the source host node from which you want to provision a new circuit.

Step 2. Select the CST you want to use. The CST dictates if it is unicast or multicast and if it is bidirectional and with redundancy.



Add Logical Connection

Select CST: DNP3-TCP Client

Select End Point: Primary Feeder

Step 3. Select the endpoint from the drop-down menu.

Step 4. Select the **Create Unicast** button. A link displays between the two devices on the right side of the nodes in the Topology view. Multicast logical connections work the same way with the addition that you can select multiple end points before creating the circuit.

Step 5. Select the **Submit** button.

The appropriate flows should also be added to the Flow Entries table of each of the switches in the path between the source and the destination. You may create many logical connections before hitting submit in the top right corner of the user interface. All logical connections are queued and only configured in the switches when the Submit button is selected. If you navigate away from the Topology page before selecting Submit, the logical connections not programmed but in queue are removed and not configured.

If you do not have the real host yet and want to provision the network to support the communications before the host is plugged into the network, perform the following steps:

Step 1. Expand the switch to display all the ports by selecting the name of the switch.

Step 2. Select an unused port on the switch to which the host will be plugged in and select **Add Host** from the right pane.

Step 3. Enter the name and addresses to be used for this host in the model that pops up and then select **Submit**. You will see the new host node displayed in the topology. Now you can create logical connections for this host.

Logical Connection Page

The logical connection page displays all the logical connections configured on the network. The source, destination, and CST appears for each logical connection. You can delete or replan each logical connection from this page, and this page supports multi-select.

The Learn and Lock extension uses the Proposed and Filtered tabs when supervised learning is used. The Proposed tab shows all the logical connections that have been learned and waiting your approval before being programmed and the Filtered tab shows all the logical connections that were learned but declined during a Learn and Lock session. The Filtered logical connections can be removed, which enables them to be learned again during the next session. You can select all actions from the menu option for each tab.

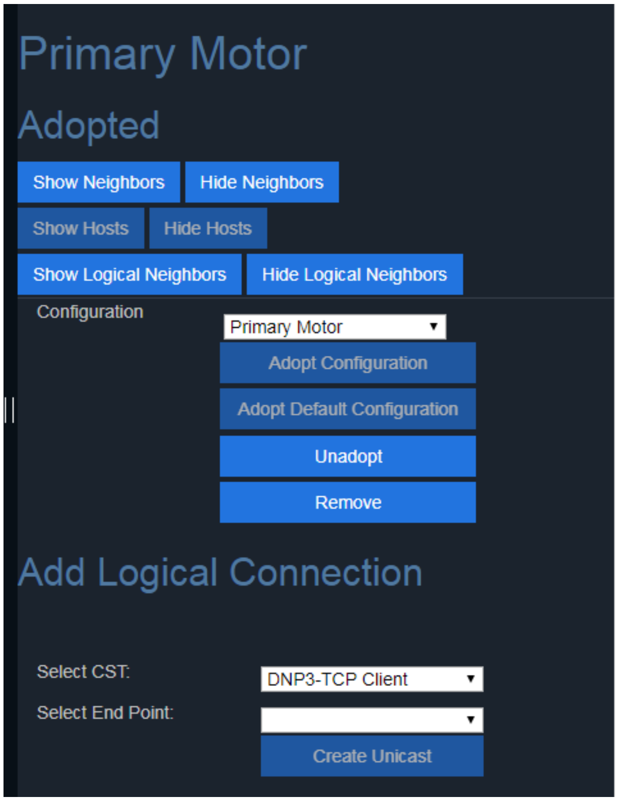
Unadopting an Object

Use these instructions to unadopt a host, link, or an SEL SDN switch. You cannot directly unadopt ports. Ports are automatically unadopted along with their attached nodes. The SEL-5056 automatically attempts to uncommission (i.e., perform a factory-default reset) the SEL SDN switch. If the SEL-5056 cannot communicate with the switch, attempt a factory-default reset of the switch by using the pinhole reset button.

Steps

Step 1. Go to the Topology page.

Step 2. Select the object you want to unadopt.



Configuration: Primary Motor

Select CST: DNP3-TCP Client

Select End Point:

Step 3. Select the **Unadopt** button.

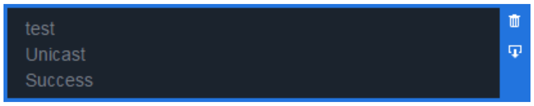
Resubmitting a Logical Connection

You can resubmit a logical connection instead of deleting and re-adding it. The SEL-5056 incorporates any changes to the CST or topology when re-creating the logical connection.

Step 1. Go to the Topology page.

Step 2. Select the logical connection to resubmit. The Logical Connection Options pane displays with a blue border.

Step 3. Select the **Logical Connection** box.



test
Unicast
Success

Step 4. Select **Resubmit** (⭳). The logical connection may briefly disappear and then reappear. There is no need to select **Submit**.

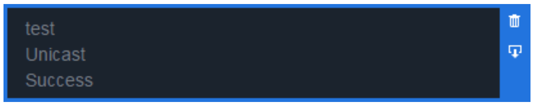
Deleting a Logical Connection

Steps

Step 1. Go to the Topology page.

Step 2. Select the logical connection to delete. The Logical Connection Options pane displays with a blue border.

Step 3. Select the **Logical Connection** box.


test
Unicast
Success

Step 4. Select the **Delete** 🗑 icon. The border turns red.

Step 5. Select **Submit**.

After you successfully delete the logical connection, the logical connection disappears.

The appropriate flow and group entries are deleted from the Flow and Group tables.

Removing a Node

To remove any unwanted nodes, follow these steps.

Steps

Step 1. Go to the Topology page.

Step 2. Select the node to delete. The Node Options pane displays.

Step 3. Select the **Remove** button. The node disappears from the Topology view.

After you successfully remove a node, the node disappears. If the node is still physically there and active, it will return to the Topology view.

Accessing the SEL SDN Switch Device View

You do not need to adopt the SEL SDN switch to access the Device View.

Steps

Step 1. Go to the Topology page.

Step 2. Select the switch you want to view. The switch Node Options pane appears.

Step 3. Select the **Device View** button.

The Device View opens in a new browser tab or window.

Configuration Objects

Use the Configuration Objects page to create and modify the configuration node, port, and link objects.

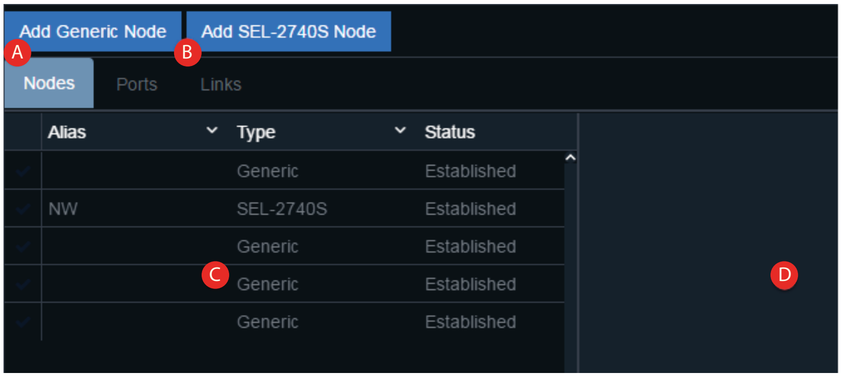
Views

Navigation Menu

Select **Configuration Objects** (under the Configuration menu) to access the Configuration Objects page.

Configuration Objects Page

The Configuration Node view displays when you select the Nodes tab.



	Alias	Type	Status
✓		Generic	Established
✓	NW	SEL-2740S	Established
✓		Generic	Established
✓		Generic	Established
✓		Generic	Established

(A) **Add Generic Node Button:** Adds an entry in the Node Configuration Object table for non-OpenFlow switch nodes.

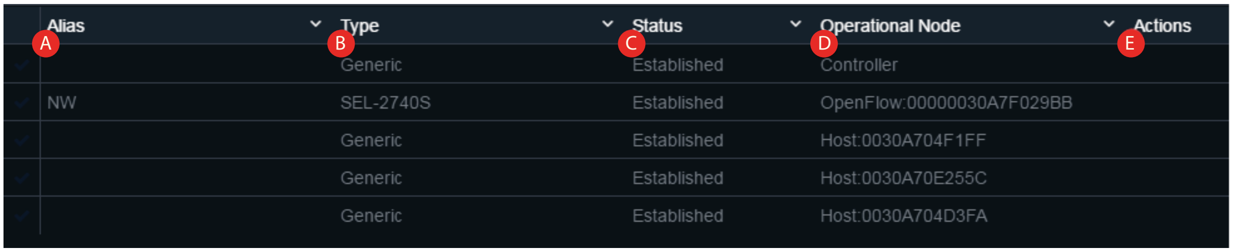
(B) **Add SEL-2740S Node Button:** Adds an entry in the Node Configuration Object table for an SEL-2740S switch.

(C) **Configuration Node Table:** Table of node configuration objects.

(D) **Configuration Node Option Pane:** Shows additional settings for the node you selected in the Node Configuration Object table.

Figure 4.22 Configuration Node Tab

Configuration Node Table



	Alias	Type	Status	Operational Node	Actions
✓		Generic	Established	Controller	
✓	NW	SEL-2740S	Established	OpenFlow:00000030A7F029BB	
✓		Generic	Established	Host:0030A704F1FF	
✓		Generic	Established	Host:0030A70E255C	
✓		Generic	Established	Host:0030A704D3FA	

(A) **Alias:** Alias for the configuration node.

(B) **Type:** Type of configuration node: Generic or SEL-2740S.

(C) **Status:** Status of configuration node: configured or established.

(D) **Operational Node:** Operational node currently configured with the configuration node.

(E) **Actions:** Set of available action icons for the entry.

Figure 4.23 Configuration Node Table

The operation node has display formats according to the Operational Node.

Table 4.18 Types of Configuration Nodes

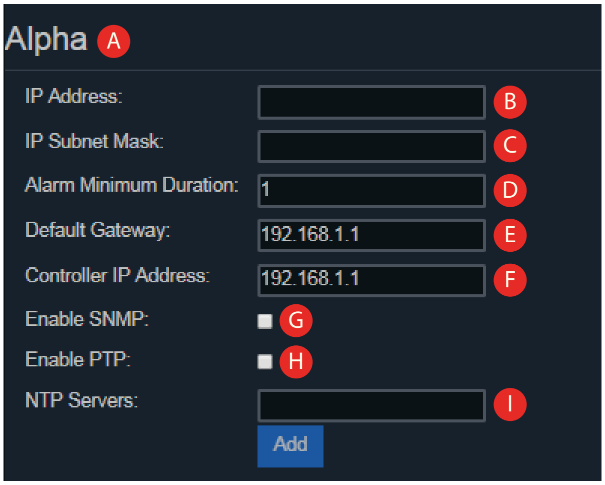
Type	Description
Generic	Used for non-SEL SDN switches
SEL-2740S	Used for SEL-2740S switches
SEL-2742S	Used for SEL-2742S switches

The configuration node will be in one of two states, listed in *Table 4.19*.

Table 4.19 States of a Configuration Node

State	Description
Established	Configuration node has been created and applied to an operational node
Configured	Configuration node has been created but not yet applied to an operation node

Configuration Node Settings Options Pane Displayed for SEL SDN Switches



Alpha

IP Address:

IP Subnet Mask:

Alarm Minimum Duration: 1

Default Gateway: 192.168.1.1

Controller IP Address: 192.168.1.1

Enable SNMP: □

Enable PTP: □

NTP Servers:

(A) **Display Name:** Display name for the configuration node.

(B) **IP Address:** IP address to give the operation node on adoption.

(C) **IP Subnet Mask:** The subnet mask to give the operation node on adoption.

(D) **Alarm Minimum Duration:** Number of seconds to latch during a minor alarm.

(E) **Default Gateway:** Default gateway assigned to the SEL-2740S during adoption; if blank, it uses the setting in the Network Settings page.

(F) **Controller IP Address:** OpenFlow controller IP address assigned to the SEL-2740S during adoption; if blank, it uses the setting in the Adoption Settings page.

(G) **Enable SNMP:** Enable or disable SNMP.

(H) **Enable PTP:** Enable or disable PTP P2P TC mode.

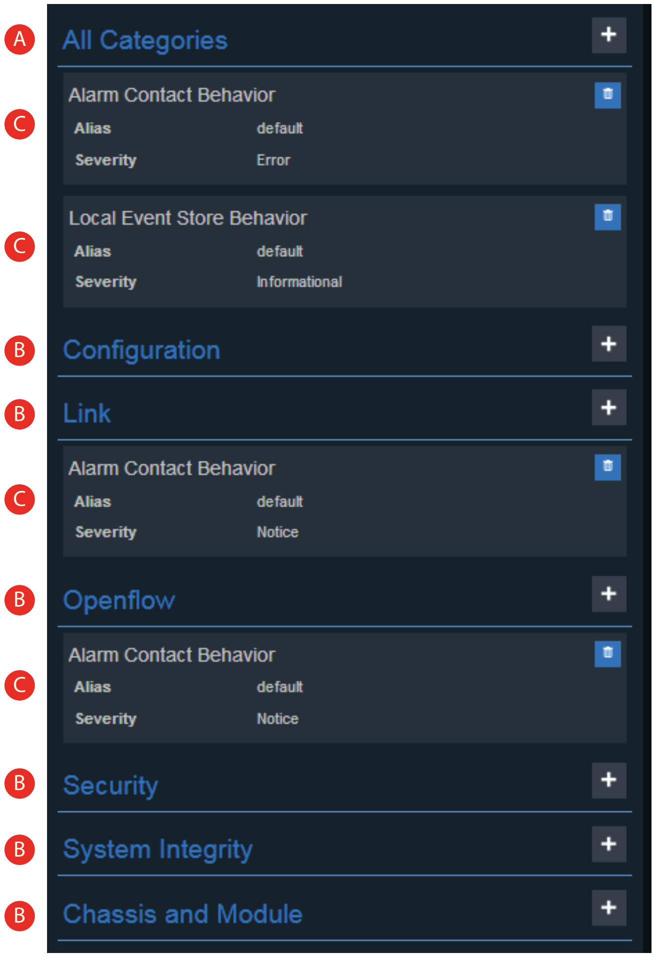
(I) **NTP Servers:** List of NTP servers in order of priority.

(J) **Add Button:** Add the IP address in (H) to the bottom of the list of NTP servers.

Figure 4.24 SEL-5056 Configuration Node Settings Options Pane

Configuration Node Log Services Pane

This pane contains all the logging settings for the SEL SDN switch except for the alarm contact duration.



All Categories +

Alarm Contact Behavior
Alias default
Severity Error

Local Event Store Behavior
Alias default
Severity Informational

Configuration +

Link +

Alarm Contact Behavior
Alias default
Severity Notice

Openflow +

Alarm Contact Behavior
Alias default
Severity Notice

Security +

System Integrity +

Chassis and Module +

(A) **All Categories:** Enable logging of event messages of the specified severity for the selected log service type for all individual categories (Configuration, Link, OpenFlow, etc.).

(B) **Individual Categories:** Enable logging of event messages of the specified severity for the selected log service type for an individual category.

(C) **Individual Log Settings:** Configurations for each log category

Figure 4.25 Configuration Node Log Services Pane

Configuration Node Log Service Boxes

There are three types of log services.

Table 4.20 Log Service Types

Name	Description
Syslog Server	Settings for sending Syslog reports to a remote Syslog server
Alarm Contact Behavior	Settings for behavior of the alarm contact
Local Event Store Behavior	Settings for storing local events

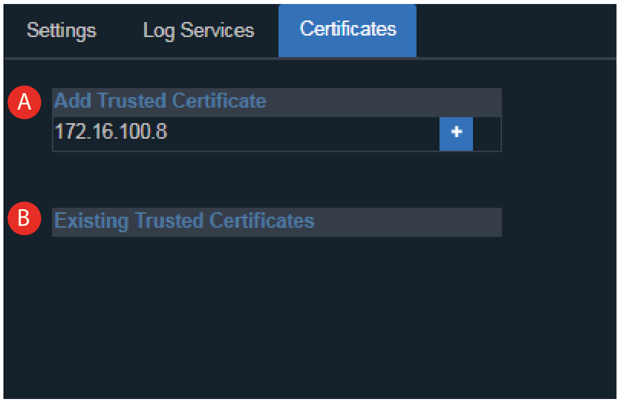
Each category may have more than one log setting of each log service type. Each individual log setting can be assigned an alias, and log settings with the same alias are grouped together. The following rules govern how log settings within a group are considered:

- If there is only one log setting for a given log service type and it is in the All Categories category, all the individual categories operate as if they had the same settings applied directly (i.e., using the All Categories category is a shortcut for applying the same settings to all individual categories).
- If there is a log setting for a given log service type in one or more individual categories (i.e., *not* in the All Categories category), only those applicable individual categories apply to the log service for that group. All other individual categories are not affected.
- If there is a log setting for a given log service type in both the All Categories category *and* one or more individual categories, only those applicable individual categories apply to the log service for that group (i.e., the presence of the setting in one or more individual categories *overrides* its presence in the All Categories category). The remaining individual categories still operate according to the log settings that are in the All Categories category.

Only one event will occur if more than one log setting of either the Alarm Contact Behavior or Local Event Store Behavior log service type is added to a category.

Configuration Node Certificates Pane

When using additional services that support cryptography like LDAP and Syslog, use the Configuration Node Certificates pane to import the public certificates that the switch will use to communicate to the servers.



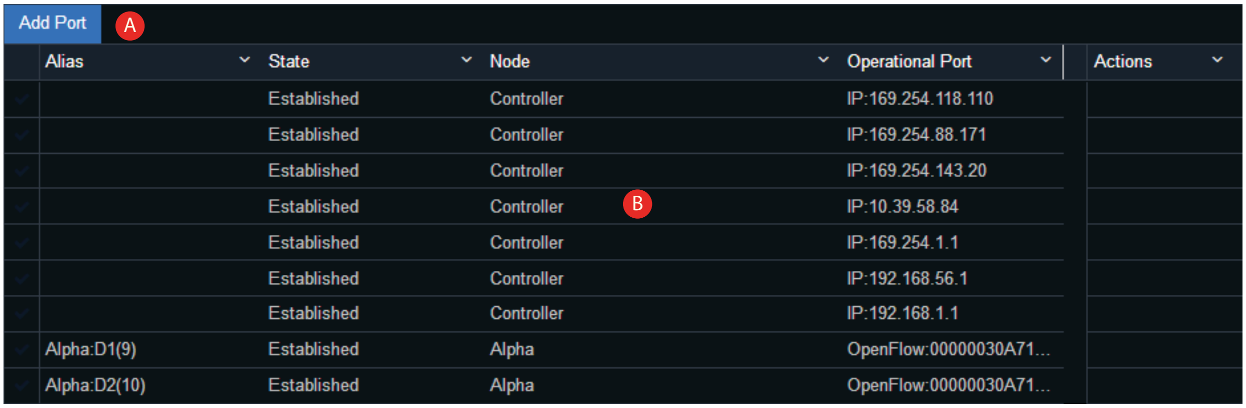
(A) **Add Trusted Certificate:** Upload the certificate with the corresponding common name.

(B) **Existing Trusted Certificates:** Uploaded certificates on the SEL SDN switch.

Figure 4.26 Configuration Node Certificates Pane

Configuration Port Tab

Select the Ports tab to display the Configuration Node view.



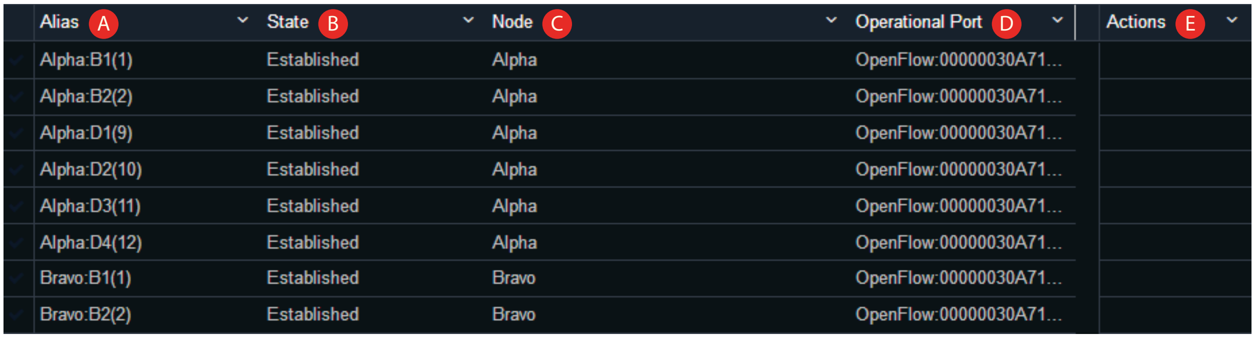
Alias	State	Node	Operational Port	Actions
	Established	Controller	IP:169.254.118.110	
	Established	Controller	IP:169.254.88.171	
	Established	Controller	IP:169.254.143.20	
	Established	Controller	IP:10.39.58.84	
	Established	Controller	IP:169.254.1.1	
	Established	Controller	IP:192.168.56.1	
	Established	Controller	IP:192.168.1.1	
Alpha:D1(9)	Established	Alpha	OpenFlow:00000030A71...	
Alpha:D2(10)	Established	Alpha	OpenFlow:00000030A71...	

(A) **Add Port Button:** Adds a configuration port to the Configuration Port table.

(B) **Configuration Port Table:** Displays a table of configuration port objects.

Figure 4.27 Configuration Port Tab

Configuration Port Table



Alias	State	Node	Operational Port	Actions
Alpha:B1(1)	Established	Alpha	OpenFlow:00000030A71...	
Alpha:B2(2)	Established	Alpha	OpenFlow:00000030A71...	
Alpha:D1(9)	Established	Alpha	OpenFlow:00000030A71...	
Alpha:D2(10)	Established	Alpha	OpenFlow:00000030A71...	
Alpha:D3(11)	Established	Alpha	OpenFlow:00000030A71...	
Alpha:D4(12)	Established	Alpha	OpenFlow:00000030A71...	
Bravo:B1(1)	Established	Bravo	OpenFlow:00000030A71...	
Bravo:B2(2)	Established	Bravo	OpenFlow:00000030A71...	

(A) **Alias:** Alias for the configuration node.

(B) **State:** Status of the configuration node: configured or established.

(C) **Node:** The configuration node containing the port.

(D) **Operational Port:** Operational node currently configured with the configuration node.

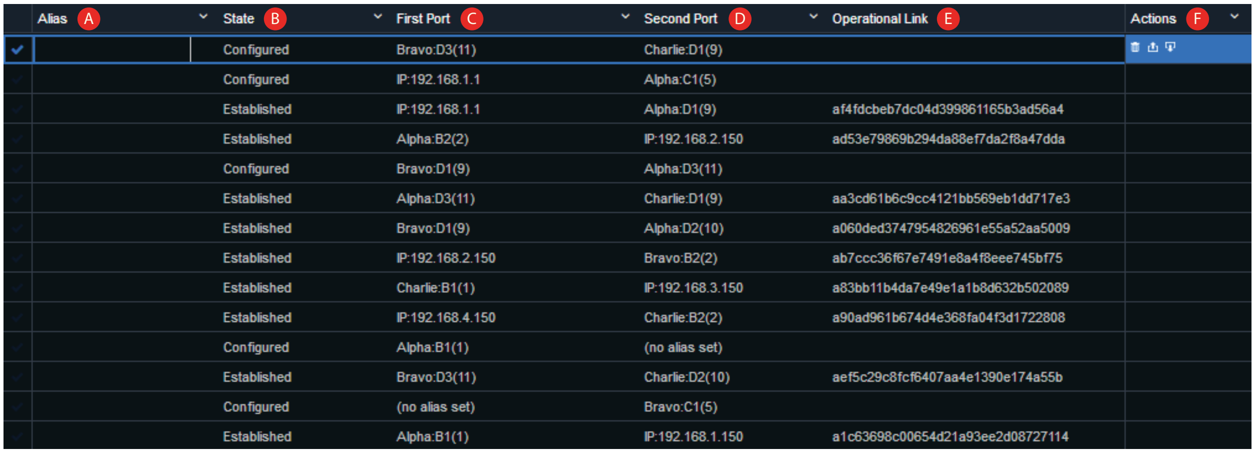
(E) **Actions:** Set of available action icons for the entry.

Figure 4.28 Configuration Port Table

Configuration Link Tab

Select the Links tab to view all the links discovered and their status. Links are intended to be managed by the discovery service and other configurations.

Configuration Link Table



	Alias A	State B	First Port C	Second Port D	Operational Link E	Actions F
✓		Configured	Bravo:D3(11)	Charlie:D1(9)		🗑 ⇪ ⇩
✓		Configured	IP:192.168.1.1	Alpha:C1(5)		
✓		Established	IP:192.168.1.1	Alpha:D1(9)	af4fdcbeb7dc04d399861165b3ad56a4	
✓		Established	Alpha:B2(2)	IP:192.168.2.150	ad53e79869b294da88ef7da2f8a47dda	
✓		Configured	Bravo:D1(9)	Alpha:D3(11)		
✓		Established	Alpha:D3(11)	Charlie:D1(9)	aa3cd61b6c9cc4121bb569eb1dd717e3	
✓		Established	Bravo:D1(9)	Alpha:D2(10)	a060ded3747954826961e55a52aa5009	
✓		Established	IP:192.168.2.150	Bravo:B2(2)	ab7ccc36f67e7491e8a4f8eee745bf75	
✓		Established	Charlie:B1(1)	IP:192.168.3.150	a83bb11b4da7e49e1a1b8d632b502089	
✓		Established	IP:192.168.4.150	Charlie:B2(2)	a90ad961b674d4e368fa04f3d1722808	
✓		Configured	Alpha:B1(1)	(no alias set)		
✓		Established	Bravo:D3(11)	Charlie:D2(10)	aef5c29c8fcf6407aa4e1390e174a55b	
✓		Configured	(no alias set)	Bravo:C1(5)		
✓		Established	Alpha:B1(1)	IP:192.168.1.150	a1c63698c00654d21a93ee2d08727114	

(A) **Alias:** Alias for the configuration link.

(B) **State:** Status of the configuration link (configured or established).

(C) **First Port:** One of the ports at the end of the link.

(D) **Second Port:** The port at the other end of the link.

(E) **Operational Link:** Operational link currently configured with the configuration link.

(F) **Actions:** Set of available action icons for the entry.

Figure 4.29 Configuration Link Table

Instructions

Creating a Generic Configuration Node

Steps

Step 1. Go to the Configuration Objects page.

Step 2. Select the **Add Config Node** button. A new green row displays at the bottom of the list.

Step 3. *Optional Step*. Add the display name (1) in the Display Name column.

Step 4. Select **Submit**.

Creating and Editing an SEL-2740S or SEL-2742S Configuration Node

Requirements

Creating an SEL-2740S configuration node is required for adoption of an SEL-2740S.

Settings

The default gateway controller IP address may be preconfigured on the Adoption Settings page. NTP server setting configuration is also in this section.

Table 4.21 Settings for Creating an SEL-2740S Configuration Node (Sheet 1 of 2)

Setting	Valid Values
Alias[a]	1 to 32 printable ASCII characters
IP Address	Valid unicast IPv4 address
IP Subnet Mask	Valid IPv4 mask

Table 4.21 Settings for Creating an SEL-2740S Configuration Node (Sheet 2 of 2)

Setting	Valid Values
Alarm Minimum Duration	1 to 30
Default Gateway[b]	Valid unicast IPv4 address
Controller IP Address[b]	The IPv4 address of any interface on the SEL-5056
Enable SNMP	True
Enable PTP	True
NTP Servers	Any three NTP server IP addresses
Log Settings	For Alarm Contact Behavior or Local Event Store Behavior log services
Certificates	Any trusted certificate from the X.509 page
Alternate IP Address	IP address and subnet mask to set on the second switch interface. This is the alternate interface that is not used for adoption.

[a] Optional setting.

[b] May be preconfigured in the Default Adoption Settings page.

You can change any of the SEL-2740S Configuration Node settings, regardless of whether the configuration node is currently applied to an SEL-2740S operational node. Modifying IP settings of an IB managed SEL-2740S may lead to a loss of connectivity.

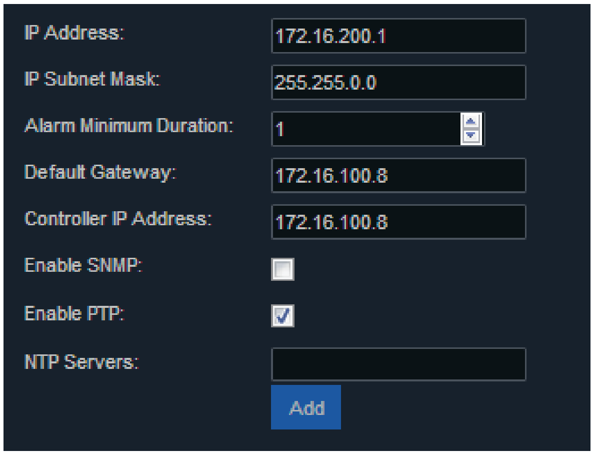
Steps to Create an SEL-2740S Configuration Node

Step 1. Go to the Configuration Objects page.

Step 2. Select the **Add SEL-2740S Node** button. A new green row appears at the bottom of the list.

Step 3. *Optional Step*. Enter the alias in the Display Name column.

Step 4. In the options pane, enter the settings as shown in the following example.



IP Address: 172.16.200.1

IP Subnet Mask: 255.255.0.0

Alarm Minimum Duration: 1

Default Gateway: 172.16.100.8

Controller IP Address: 172.16.100.8

Enable SNMP: □

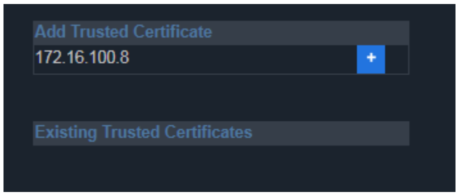
Enable PTP: ☑

NTP Servers:

Step 5. *Optional step for Log settings*. Select the **Log Services** tab and add log services.

Step 6. *Optional step for uploading certificates*. Select the **Certificates** tab. For each certificate, select the + next to the corresponding common name of the certificate.

Step 7. *Optional step for setting the alternate IP address.* Select the plus sign and enter the desired IP address and subnet to set the second interface. Services like Syslog and SNMP use this interface if configured to do so.



172.16.100.8

Step 8. Select **Submit**.

The configuration node is uncolored.

Steps to Edit an SEL-2740S Configuration Node

Step 1. Go to the Configuration Objects page.

Step 2. Select the SEL-2740S configuration node with the correct operational node.

Step 3. In the Configuration Node Options pane, configure the Configuration settings as required.

To delete a trusted certificate, select the **Delete** button (🗑) next to the certificate in the Existing Trusted Certificates list.

Step 4. Select **Submit**.

You may need to synchronize the SEL-2740S.

Adding an Alarm Contact Behavior or Local Event Store Behavior Log Service

The log services for a connected, adopted SEL-2740S can be changed at any time.

Steps to Add a Logger

Step 1. Go to the Configuration Objects Nodes page.

Step 2. Select the appropriate row that matches the alias in the Configuration Objects Nodes table and select the **Log Services** tab in the configuration pane.

Step 3. Select the + icon and **Alarm Contact Behavior** or **Local Event Store Behavior** in the desired category.

Step 4. Enter the Alias setting.

Step 5. Select the desired Severity value from the **Severity** drop-down menu.

Step 6. Select Submit. The feedback bar should say “Success.”

Editing the Alias of a Configuration Object

You may edit the alias on any object at any time. Select the current name in the user interface and make the edits.When you have finished, select **Submit**.

Deleting a Configuration Object in the Configured State

The state of the configuration object must be configured and not established.

Steps

Step 1. Go to the Configuration Objects page.

Step 2. The default active tab is the Nodes tab. If the configuration object type is port, select the Ports tab; if it is link, select the Links tab.

Step 3. Select the object you want to delete.

Step 4. Select the Delete 🗑 icon in the Actions column in the row. The row turns red.

Step 5. Select Submit.

After you successfully delete a configuration object in the configured state, the configuration object is removed from the appropriate Configuration table.

Flow Entries

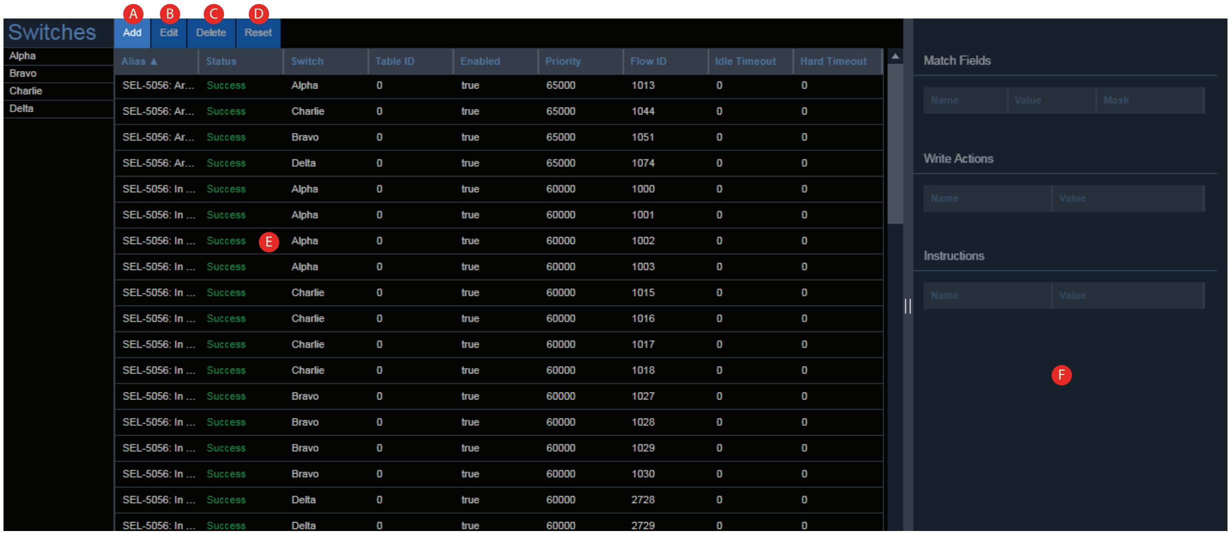
Use the Flow Entries page to manage OpenFlow flow entries directly. The SEL-5056 attempts to minimize the amount of direct work required at the OpenFlow level and provides powerful automation to manage the low-level OpenFlow settings for you. When setting the OpenFlow configuration, refer to the OpenFlow standard version 1.3 for details on each setting. The SEL-5056 uses the same nomenclature and syntax as the standard for easy reference.

Views

Navigation Menu

Select **Flow Entries** (under the Configuration menu) to access the Flow Entries page.

Flow Entry Page



Alias ▲	Status	Switch	Table ID	Enabled	Priority	Flow ID	Idle Timeout	Hard Timeout
SEL-5056: Ar...	Success	Alpha	0	true	65000	1013	0	0
SEL-5056: Ar...	Success	Charlie	0	true	65000	1044	0	0
SEL-5056: Ar...	Success	Bravo	0	true	65000	1051	0	0
SEL-5056: Ar...	Success	Delta	0	true	65000	1074	0	0
SEL-5056: In ...	Success	Alpha	0	true	60000	1000	0	0
SEL-5056: In ...	Success	Alpha	0	true	60000	1001	0	0
SEL-5056: In ...	Success	Alpha	0	true	60000	1002	0	0
SEL-5056: In ...	Success	Alpha	0	true	60000	1003	0	0
SEL-5056: In ...	Success	Charlie	0	true	60000	1015	0	0
SEL-5056: In ...	Success	Charlie	0	true	60000	1016	0	0
SEL-5056: In ...	Success	Charlie	0	true	60000	1017	0	0
SEL-5056: In ...	Success	Charlie	0	true	60000	1018	0	0
SEL-5056: In ...	Success	Bravo	0	true	60000	1027	0	0
SEL-5056: In ...	Success	Bravo	0	true	60000	1028	0	0
SEL-5056: In ...	Success	Bravo	0	true	60000	1029	0	0
SEL-5056: In ...	Success	Bravo	0	true	60000	1030	0	0
SEL-5056: In ...	Success	Delta	0	true	60000	2728	0	0
SEL-5056: In ...	Success	Delta	0	true	60000	2729	0	0

(A) **Add Button:** Adds a new entry to the Flow Entries table.

(B) **Edit Button:** Edit the selected flow entry.

(C) **Delete Button:** Delete the selected flow entry.

(D) **Reset Button:** Reset the flow entry counters for the selected flow entry.

(E) **Flow Entry Table:** Lists flow entries on all OpenFlow switches the SEL-5056 manages.

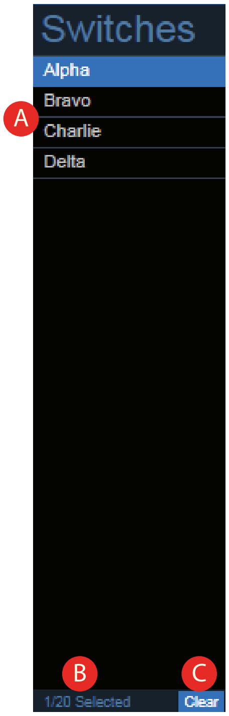
(F) **Flow Entry Option Pane:** Shows additional settings for a flow entry that is currently selected.

(G) **Copy:** Copy the flow attributes to a new entry for use on another switch

Figure 4.30 Flow Entry Page

Switches Filter View

The Switch toggle list lets you quickly add and remove a switch from the current Topology view.



(A) List of switches.

(B) Number of switches selected.

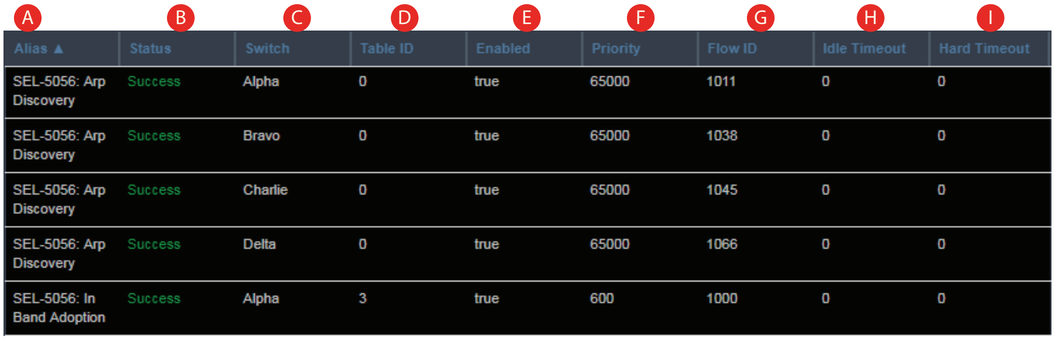
(C) Clear Button.

Figure 4.31 Switch Toggle List

To select all switches, clear all switches or select the **Clear** button. If you select one or more switches, only the flow entries of those switches are displayed along with any flow entries that are modified since the filter was applied. You can select as many as 20 switches from the menu at a time.

Flow Entry Table

The flow entry table uses pagination to load only a subset of the applicable flow entries. You can continuously scroll down to see more. You can also select a column (except for Switch) to sort in descending or ascending order.



Alias ▲	Status	Switch	Table ID	Enabled	Priority	Flow ID	Idle Timeout	Hard Timeout
SEL-5056: Arp Discovery	Success	Alpha	0	true	65000	1011	0	0
SEL-5056: Arp Discovery	Success	Bravo	0	true	65000	1038	0	0
SEL-5056: Arp Discovery	Success	Charlie	0	true	65000	1045	0	0
SEL-5056: Arp Discovery	Success	Delta	0	true	65000	1066	0	0
SEL-5056: In Band Adoption	Success	Alpha	3	true	600	1000	0	0

(A) **Alias:** Friendly name for the flow entry.

(B) **Status:** Indicates the status of the entry (see Table 4.41).

(C) **Switch:** Assigned switch of the flow entry.

(D) **Table ID:** Flow Table setting of the flow entry (see Section 3).

(E) **Enabled:** Sets whether the flow entry should be pushed to or removed from the SEL-2740S.

(F) **Priority:** Priority setting of the flow entry (see Section 3).

(G) **Flow ID:** Unique flow entry identifier the SEL-5056 assigns (see Section 3).

(H) **Idle Timeout:** Time-out to remove entry (see Section 3).

(I) **Hard Timeout:** Time-out to remove entry (see Section 3).

Figure 4.32 Flow Entry Table

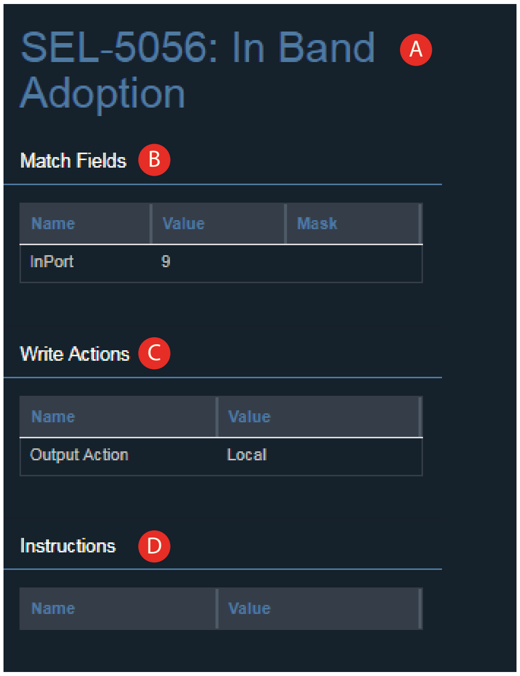
A flow entry will have one of four statuses, listed in *Table 4.22*.

Table 4.22 Flow Entry Status

Status	Description
Success	The flow entry was successfully programmed on the SEL-2740S
Failure	The flow entry was unsuccessfully programmed on the SEL-2740S
In Progress	The flow entry is currently being programmed on the SEL-2740S, or no switch setting is set
[blank]	The flow entry was added since the last submission of the page

Flow Entry Options Pane

The Flow Entry options pane shows the current match fields, write actions, and instructions for the selected flow entry.



SEL-5056: In Band Adoption

Match Fields

Name	Value	Mask
InPort	9	

Write Actions

Name	Value
Output Action	Local

Instructions

Name	Value

(A) **Alias:** Alias of the selected flow entry.

(B) **Match Fields:** See *Flow Entries on page 3.6*.

(C) **Write-Actions List:** See *Flow Entries on page 3.6*.

(D) Instructions List

Figure 4.33 Flow Entry Options Pane

Modal View

The values of a flow entry are added or modified in a modal window.

To add a flow entry, select the **Add** button or the A key. To modify a flow entry, select the **Edit** button or the E key to cause the modal window to appear.

The modal window has four tabs:

- Flow for general settings that appear in the table itself
- Match Fields for match fields
- Write actions for the actions
- Other instructions for Clear-action, Goto-table, and Meter instructions

Required fields are prepopulated with default values, where applicable. Other values have default values but are not required. If the value is incorrect, the setting is surrounded by a red box. Settings without values contain the text Optional. Settings with Optional are not processed.

Some match fields have more than one setting. Match fields may have no values in any of the boxes, a value in the Value setting, values in both the Value and Mask settings (if present), or a value in the By Alias setting (if present).

For Write-Actions and other instructions with both a By Alias and By ID/Value settings, you can use one or the other or neither, but not both.

Instructions

Adding, Editing, and Deleting a Flow Entry

Requirements

The SEL-5056 requires that flow entries do not overlap.

Steps to Add a Flow Entry

Flow entries are submitted to the switch only as a complete unit. Create a flow entry through the use of the **Add Flow** button.

You can therefore do the following:

Step 1. Select the **Add Flow** button.

Step 2. Program each setting of the flow entry according to desired configuration and do not select the **Submit** button after each setting.

Step 3. Select **Submit** to commit the entire flow entry only after all configurations of the flow are set.

Steps to Edit a Flow Entry

You can change any part of a flow entry (except for the Flow ID).

Steps to Delete a Flow Entry

Step 1. Go to the Flow Entries page.

Step 2. Select the flow entry to delete from the Flow Entry table.

Step 3. Select the **Delete** button in the Actions column or press the D key.

Step 4. Select **Delete** in the confirmation window.

Group Entries

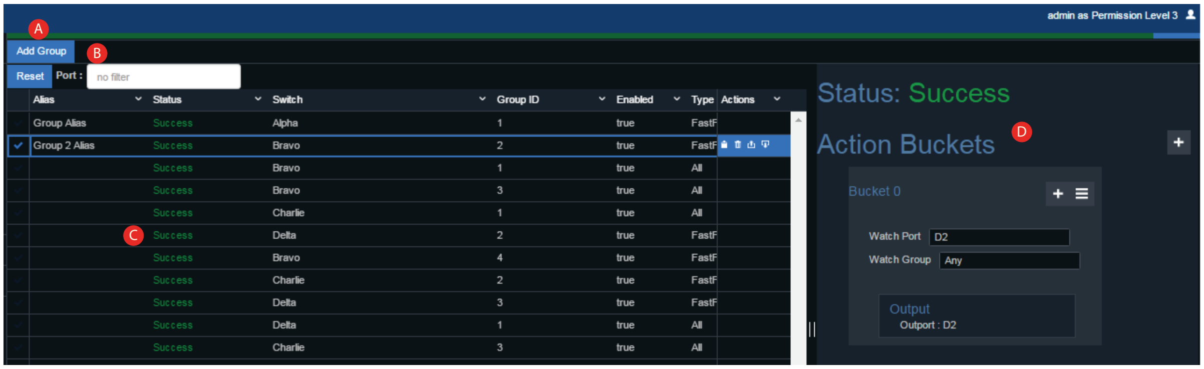
Use the Group Entries page to manage group entries.

Views

Navigation Menu

Select **Group Entries** (under the Configuration menus) to access the Group Entries page.

Group Entries Page



Port : no filter

	Alias	Status	Switch	Group ID	Enabled	Type	Actions
	Group Alias	Success	Alpha	1	true	FastF	
✓	Group 2 Alias	Success	Bravo	2	true	FastF	
		Success	Bravo	1	true	All	
		Success	Bravo	3	true	All	
		Success	Charlie	1	true	All	
		Success	Delta	2	true	FastF	
		Success	Bravo	4	true	FastF	
		Success	Charlie	2	true	FastF	
		Success	Delta	3	true	FastF	
		Success	Delta	1	true	All	
		Success	Charlie	3	true	All	

Status: Success

Action Buckets

Watch Port D2
Watch Group Any

Output
Outport : D2

(A) **Add Group Button:** Adds a new entry to the Group Entries table.

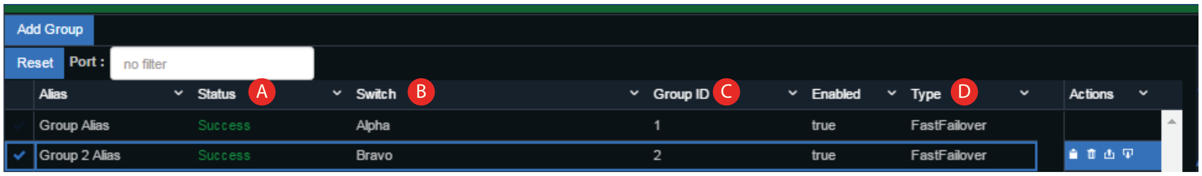
(B) **Switch Filter Settings:** Filters the flow entries listed in the Group Entries table by Switch and Port setting.

(C) **Group Entry Table:** Lists group entries on all OpenFlow switches the SEL-5056 manages; filtering is based on the Filtering settings.

(D) **Group Entry Option Pane:** Shows additional settings for the entry you selected in the Group Entry table.

Figure 4.34 Group Entries Page

Group Entry Table



Port : no filter

	Alias	Status	Switch	Group ID	Enabled	Type	Actions
	Group Alias	Success	Alpha	1	true	FastFailover	
✓	Group 2 Alias	Success	Bravo	2	true	FastFailover	

(A) **Status:** Indicates the status of the entry.

(B) **Switch:** Assigned switch of the Group entry.

(C) **Group ID:** Group ID setting assigned when adding the group.

(D) **Type:** Group Type.

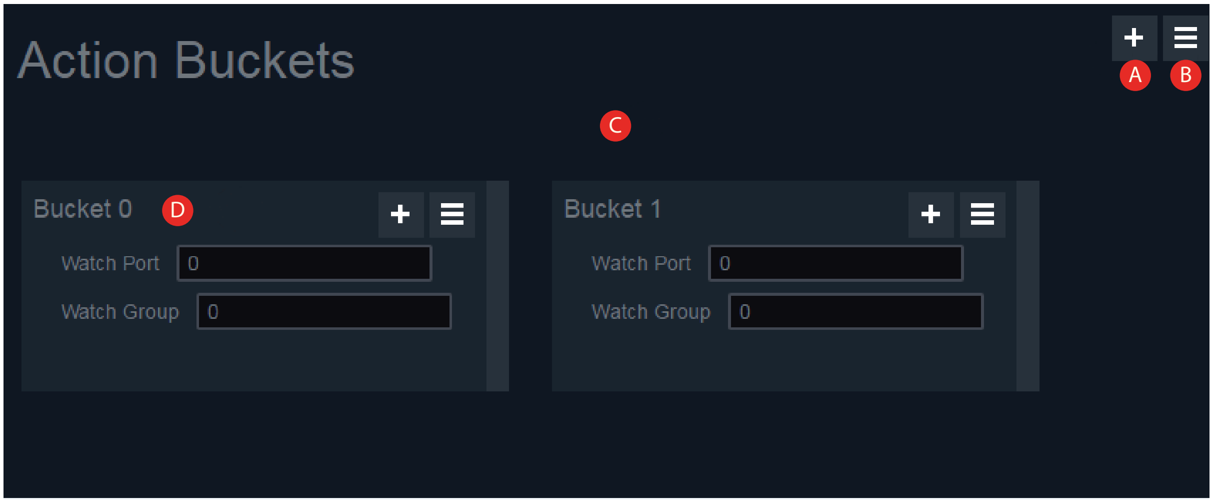
Figure 4.35 Group Entry Table

A flow entry can have one of the four statuses listed in *Table 4.23*.

Table 4.23 Statuses of a Group Entry

Status	Description
Success	The group entry was successfully programmed on the switch
Failure	The group entry was unsuccessfully programmed on the switch
In Progress	The group entry is currently being programmed on the switch, or no Switch setting is set
[blank]	The group entry was added since the last submission of the page

Group Bucket Pane



(A) **Add Action Bucket Button:** Button for adding a new action bucket to the Action Bucket list.

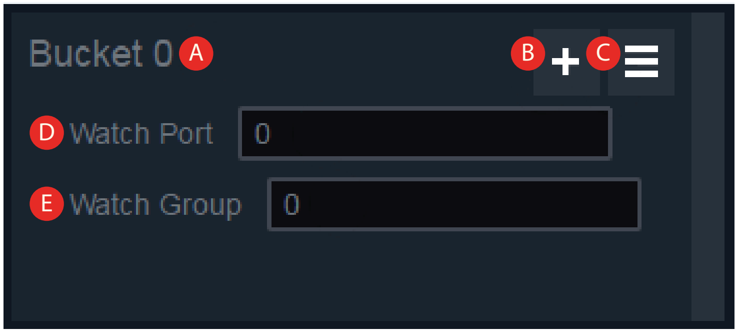
(B) **Action Bucket List Options:** Menu to copy and paste action buckets.

(C) **Action Bucket List:** List of action buckets.

(D) **Action Bucket Box:** An individual action bucket.

Figure 4.36 Group Bucket Pane

Action Bucket Box



(A) **Bucket ID:** Order of bucket priority in the Action Bucket list.

(B) **Add Action Button:** Menu of available actions to add to the action bucket.

(C) **Action Bucket Options:** Menu to copy and paste actions and to delete the action bucket.

(D) **Watch Port:** Liveness of the desired port (see *Action Buckets on page 3.16*).

(E) **Watch Group:** Liveness of the desired group (see *Action Buckets on page 3.16*).

Figure 4.37 Action Bucket Box

Instructions

Adding, Editing, and Deleting a Group Entry

Steps to Add a Group Entry

Step 1. Select the **Add Group** button.

Step 2. Configure Group Type and add desired Action Buckets.

Step 3. Assign the group to the specified switch.

Steps to Edit a Group Entry

Step 1. Select the Group from the Group list.

Step 2. Change to your desired configuration.

Step 3. Select the **Submit** button.

Steps to Delete a Group Entry

Step 1. Select the group from the Group list.

Step 2. Select the **Delete** 🗑 icon in the Action list.

Step 3. Select the **Submit** button.

Rearranging Action Buckets

Action buckets are arranged in order of priority in the Group Bucket pane. Action bucket priority matters for the Fast Failover groups because liveness testing occurs in the order of bucket priority.

Meter Entries

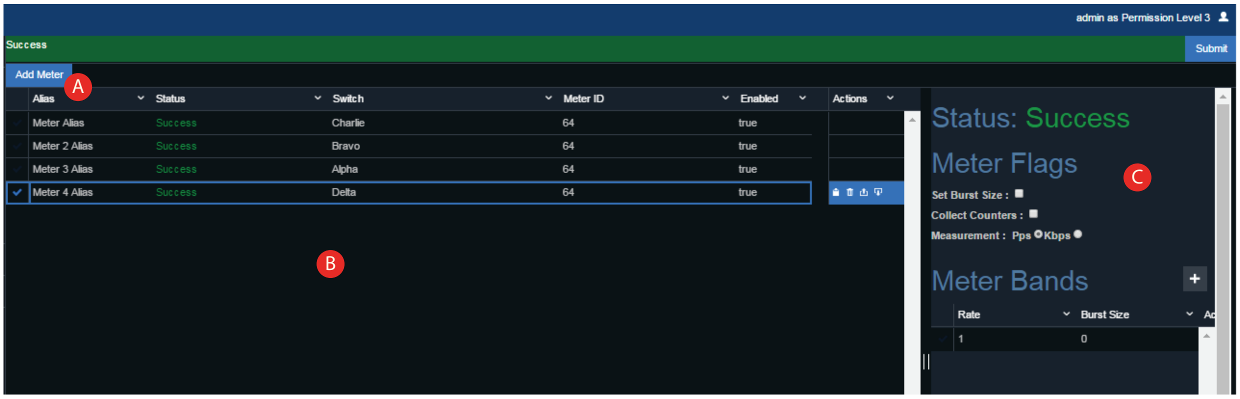
Use the Meter Entries page to manage meter entries, including their meter bands.

Views

Navigation Menu

Select **Meter Entries** (under the Configuration menu) to access the Meter entries page.

Meter Entries Page



	Alias	Status	Switch	Meter ID	Enabled	Actions
	Meter Alias	Success	Charlie	64	true	
	Meter 2 Alias	Success	Bravo	64	true	
	Meter 3 Alias	Success	Alpha	64	true	
✓	Meter 4 Alias	Success	Delta	64	true	

Status: Success

Meter Flags

Set Burst Size : □

Collect Counters : □

Measurement : Pps ○ Kbps ●

Meter Bands +

Rate	Burst Size	Ac
1	0	

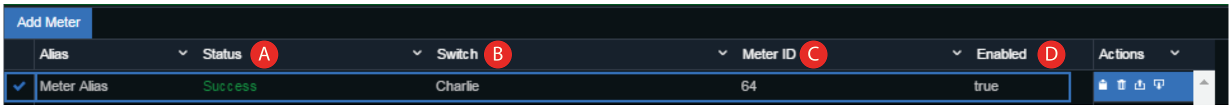
(A) **Add Meter Button:** Create a new Meter entry.

(B) **Meter Entry Table:** Table of meter entries.

(C) **Meter Entry Options Pane:** Additional settings for the entry you selected in the Meter Entry table.

Figure 4.38 Meter Entries Page

Meter Entry Table



Add Meter

	Alias	Status	Switch	Meter ID	Enabled	Actions
✓	Meter Alias	Success	Charlie	64	true	

(A) **Status:** Indicates the status of the entry.

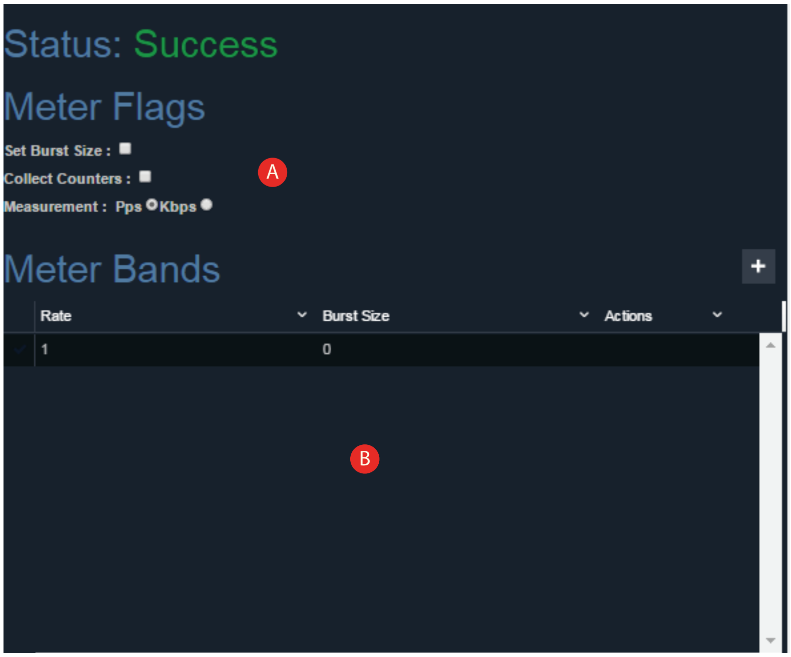
(B) **Switch:** Assigned switch of the Meter entry.

(C) **Meter ID:** Value used to identify the meter

(D) **Enabled:** Toggle for whether the Meter entry should be pushed or removed from the SEL-2740S.

Figure 4.39 Meter Entry Table

Meter Entry Options Pane



Status: Success

Meter Flags

Set Burst Size : □

Collect Counters : □

Measurement : Pps ○ Kbps ●

Meter Bands

Rate	Burst Size	Actions
1	0	

(A) **Meter Flags:** Configuration options for the meter.

(B) **Meter Bands Table:** Table of meter bands for the meter entry you selected.

Figure 4.40 Meter Entry Options Pane

Instructions

Adding, Editing, and Deleting a Meter Entry or Band

Steps to Add a Meter Entry

Step 1. Select the **Add Meter** button.

Step 2. Make the required edits to the Meter entry.

Step 3. Select the **Submit** button.

Steps to Edit a Meter Entry

Step 1. Select the meter entry you want to edit.

Step 2. Make the required edits to the meter entry.

Step 3. Select the **Submit** button.

Steps to Delete a Meter Entry

If you delete a meter entry from an OpenFlow switch, the OpenFlow switch also deletes any flow entries referencing the meter entry in the meter instruction.

Any affected flow entries therefore have a Failure status.

Step 1. Select the meter entry you want to delete.

Step 2. Select the **Delete** 🗑 icon on the Actions list.

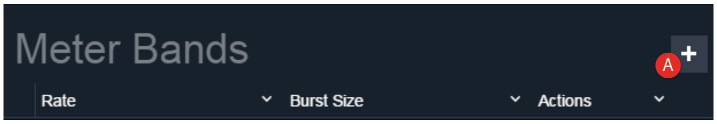
Step 3. Select the **Submit** button.

Steps to Add a Meter Band

Step 1. Go to the Meter Entries page.

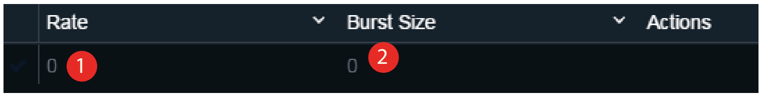
Step 2. Select the meter entry to which you are adding a meter band.

Step 3. Select the **Add** + icon (A) in the Meter Entry Options pane. A new row is added to the Meter Bands table.



Rate	Burst Size	Actions

Step 4. Enter the Rate (1) and Burst Size (2).



Rate	Burst Size	Actions
0	0	

Step 5. Select the **Submit** button to have the SEL-5056 add the meter band to the Meter entry.

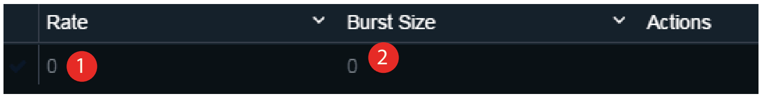
Steps to Edit a Meter Band

Step 1. Go to the Meter Entries page.

Step 2. Select the meter entry to edit the meter band.

Step 3. Select the meter band you want to edit.

Step 4. Edit the Rate (1) or Burst Size (2).



Rate	Burst Size	Actions
0	0	

Step 5. Select the **Submit** button to have the SEL-5056 apply the Meter Band settings changes.

Steps to Delete a Meter Band

Step 1. Go to the Meter Entries page.

Step 2. Select the meter entry to delete a meter band.

Step 3. Select the meter band you want to delete.

Step 4. Select the **Delete** 🗑 icon. The meter band is removed from the table.

Step 5. Select the **Submit** button to have the SEL-5056 apply the deletion of the meter band.

Enabling and Disabling a Meter Entry

Disabling a meter entry deletes the meter from the switch.

Steps

Step 1. Go to the Meter Entries page.

Step 2. Locate the meter entry you want to enable or disable.

Step 3. Select the Enabled check box to program the meter entry to the switch, or clear the Enabled check box to delete the meter entry from the switch.

Step 4. Select **Submit**.

CST Entries

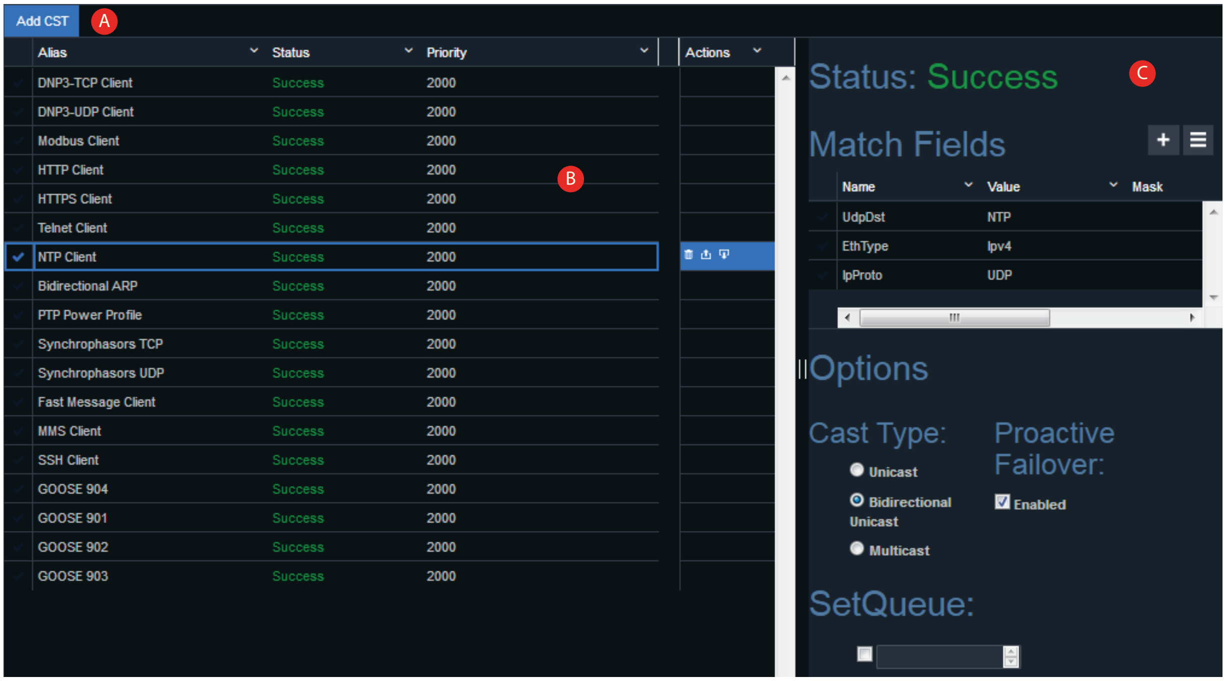
Use the CST Entries page to manage the CSTs used in logical programming.

Views

Navigation Menu

Select **CST Entries** (under the Configuration menu) to access the CST Entries page.

CST Entries Page



	Alias	Status	Priority	Actions
	DNP3-TCP Client	Success	2000	
	DNP3-UDP Client	Success	2000	
	Modbus Client	Success	2000	
	HTTP Client	Success	2000	
	HTTPS Client	Success	2000	
	Telnet Client	Success	2000	
✓	NTP Client	Success	2000	
	Bidirectional ARP	Success	2000	
	PTP Power Profile	Success	2000	
	Synchrophasors TCP	Success	2000	
	Synchrophasors UDP	Success	2000	
	Fast Message Client	Success	2000	
	MMS Client	Success	2000	
	SSH Client	Success	2000	
	GOOSE 904	Success	2000	
	GOOSE 901	Success	2000	
	GOOSE 902	Success	2000	
	GOOSE 903	Success	2000	

Status: Success

Match Fields

Name	Value	Mask
UdpDst	NTP	
EthType	Ipv4	
IpProto	UDP	

Options

Cast Type:
○ Unicast
● Bidirectional Unicast
○ Multicast

Proactive Failover:
☑ Enabled

SetQueue:
□

(A) **Add CST Button:** Button for creating a new CST entry in the CST table.

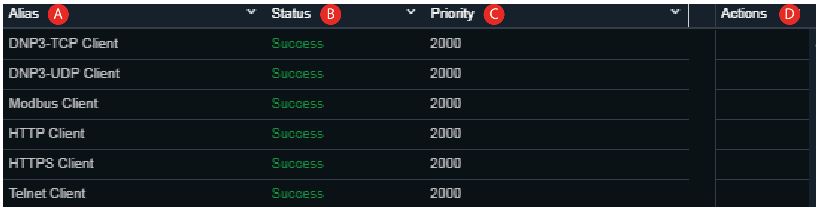
(B) **CST Table:** Table displaying configured CSTs.

(C) **CST Option Pane:** Additional settings for the selected CST entry in the CST table.

Figure 4.41 CST Entries Page

CST Table

The CST table always contains at least the default CSTs. Default CSTs cannot be deleted or edited.



Alias	Status	Priority	Actions
DNP3-TCP Client	Success	2000	
DNP3-UDP Client	Success	2000	
Modbus Client	Success	2000	
HTTP Client	Success	2000	
HTTPS Client	Success	2000	
Telnet Client	Success	2000	

(A) **Alias:** Friendly name for the CST.

(B) **Priority:** Priority value assigned to all flow entries created by the logical connection that uses this CST.

(C) **Status:** Indication of the state of the entry.

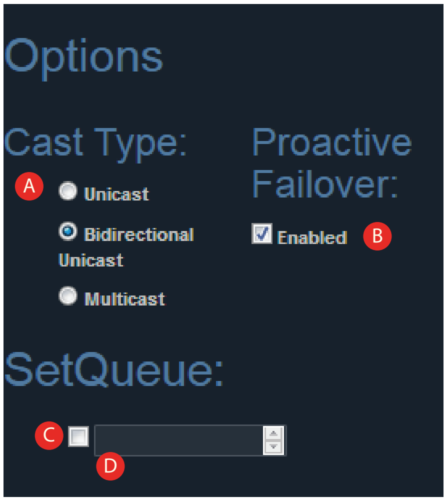
(D) **Actions:** List of actions to copy, paste, and delete.

Figure 4.42 CST Table

Match Field List

The Match Field list is the same as the Match Fields table on the Flow Entries page, except that the InPort field is absent from the Match Fields list.

Options



Options

Cast Type:

○ Unicast

● Bidirectional Unicast

○ Multicast

Proactive Failover:

☑ Enabled

SetQueue:

□

(A) **Cast Type:** See *Table 4.24*.

(B) **Proactive Failover Enable:** Enable or disable N-1 for link redundancy.

(C) **SetQueue Enable:** Enable or disable SetQueue. Disable uses the default value of 2.

(D) **SetQueue Value:** See *Priority Queues on page 3.5*.

Figure 4.43 CST Options

Table 4.24 Communications Service Cast Types

Type	Description
Unicast	One-way point-to-point communication
Bidirectional Unicast	Bidirectional point-to-point communication
Multicast	Point-to-multipoint communication

Instructions

Creating a CST

Settings

Table 4.25 CST Entry Settings

Setting	ID	Description	Valid Values
Alias	1	Alias of the CST you want to delete	Any alias listed in the CST table
Priority	2	Priority setting for each flow entry programmed using this CST	0 to 65535[a]
Match Fields	3	List of match fields	OpenFlow matches available

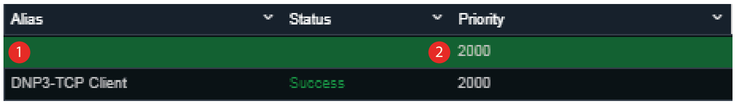
[a] The default value for Priority is 2000 (to avoid overlapping with the default priority of 1000 for flow entries added directly to the flow entries table).

Steps to Add a CST

Step 1. Go to the CST Entries page.

Step 2. Select the **Add CST** button.

Step 3. Enter the Alias (1) and Priority settings (2) in the table.



Alias	Status	Priority
1		2 2000
DNP3-TCP Client	Success	2000

Step 4. Enter the match fields into the Match Fields table, and select the cast type, priority, and redundancy.

Step 5. Select **Submit**.

Editing a CST

You can modify any of the settings of a CST. Modifying the match fields of a CST automatically updates any flow entries programmed by a logical connection through the use of the CST. Changing the Alias field does not update the CST Name in the Logical Connection box.

Deleting a CST

You cannot delete a CST that is in use by a logical connection. Once all logical connections are deleted, the CST can be deleted.

Steps

Step 1. Go to the CST Entries page.

Step 2. Select the CST entry in the CST table that has the alias.

Step 3. Select the **Delete** 🗑 icon in the Actions column.

Step 4. Select the **Submit** button.

Adoption Settings

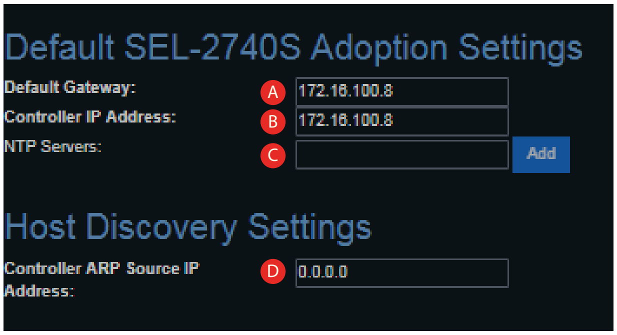
Use the Adoption Settings page to manage the default Adoption and NTP settings that the SEL-5056 will use for each new SEL SDN switch configuration object.

Views

Navigation Menu

Select **Adoption Settings** (under the Configuration menu) to access the Adoption Settings page.

Page View



Default SEL-2740S Adoption Settings

Default Gateway: 172.16.100.8

Controller IP Address: 172.16.100.8

NTP Servers:

Host Discovery Settings

Controller ARP Source IP Address: 0.0.0.0

(A) **Default Gateway:** Default gateway assigned by the controller to any new switch configuration node.

(B) **Controller IP Address:** Default controller IP address assigned by the controller to any new switch configuration node.

(C) **NTP Servers:** As many as three default NTP server addresses assigned to any new switch configuration node.

(D) **Controller ARP Source IP Address:** The ARP SPA value in ARP probe messages used by the SEL-5056 to check the host status.

Figure 4.44 Adoption Settings Page

VID Reservation

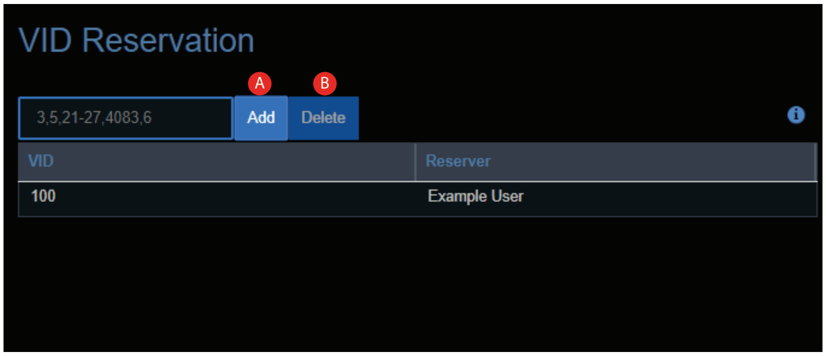
Use the VID Reservation page to reserve VIDs to prevent possible overlap between the device VIDs and the SEL-5056 VIDs that are used for coloring packets. The SEL-5056 uses a VID for failover to Failover mode devices and point-to-multipoint traffic delivery. The SEL-5056 starts at VID 4094 and then counts down to 1. Reserved VIDs either from the user or the SEL-5056 are listed in the VID Reservations page. VlanVid values from user-defined CSTs are automatically added to this list.

Views

Navigation Menu

Select **VID Reservation** (under the Configuration menu) to access the VID Reservation page.

VID Reservation Page


VID Reservation

VID	Reserver
100	Example User

(A) Add VLAN VID reservation

(B) Delete VLAN VID reservation

Figure 4.45 VID Reservation Table

Instructions

Adding VIDs

You can enter a single VID, multiple noncontiguous VIDs, or a range of VIDs. For example, **3, 5, 21–27, 4083, 6** would reserve the following VIDs: 3, 5, 21, 22, 23, 24, 25, 26, 27, 4083, and 6. Regardless of how the VIDs are entered, each VID is its own row on the VID Reservation page. You may reserve any value between 1 and 4094.

Steps

Step 1. Go to the VID Reservation page.

Step 2. Enter VID to be reserved and select **Add**.

Deleting a User-Reserved VID

Steps

Step 1. Select the row with the appropriate VID.

Step 2. Select **Delete**.

Reserving an Already Controller-Reserved VID

To prevent the SEL-5056 from using a VID, reserve the VID. If the SEL-5056 has already reserved the VID, delete the VID from the table, reserve the VID, and then resubmit any LCs that use the VID.

SEL-5056 Diagnostic Pages

Counters

Use the Counters pages to view OpenFlow counters reported by the SEL SDN switch. There are no configurable settings on the Counters pages.

Views

Navigation Menu

Select **Counters** (under the Diagnostics menu) to access the Counters page. Select the Counters link to display the statistics pages, as shown in *Figure 4.46*.

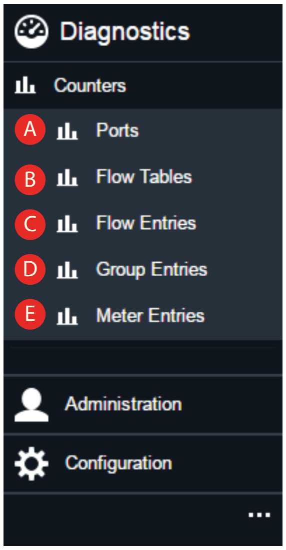


Figure 4.46 Statistics Page Navigation Menu Link With Pages

Table 4.26 Counters Pages

ID	Name	Description
A	Ports	Port Counters
B	Flow Tables	Flow Table Counters
C	Flow Entries	Flow Entry Counters
D	Group Entries	Group Entry and Action Bucket Counters
E	Meter Entries	Meter and Meter Entry Counters

SEL SDN Switch Device View, Local Syslog Events, and Alarms Pages

Device View

The Device View page contains chassis, module, and port information and diagnostic of the SEL SDN switch. When the switch is selected in the Topology page of the SEL-5056 user interface, the Device View button appears on the right pane. Each switch has its own device view design and device statistics and diagnostic displayed, Review the switch manual for the details.

APPENDIX A

Software and Manual Versions

Software

Determining the Software Version

The software version number displays on the bottom left of each webpage after the user has successfully logged into the SEL-5056.

Revision History

Table A.1 lists the lists the SEL-5056 software versions, revision descriptions, and corresponding instruction manual date codes.

Table A.1 SEL-5056 Software Revision History (Sheet 1 of 2)

Software Version Number	Summary of Revisions	Manual Date Code
2.2.0.0	➤ Added support for offline host configuration. ➤ Enhanced the way automated host discovery works to avoid Windows IP address conflicts. ➤ Enhanced adoption process to remove synchronization. ➤ Updated open source libraries and security patches. ➤ Updated the user interface to allow flows to be copied and arrow keys to work on all tables. ➤ Enhanced the user interface to display the links and hosts more accurately. ➤ Enhanced topology management discovery of links between SDN and traditional switch nodes. ➤ Added support for user-directed host discovery. ➤ Added Learn and Lock extension. ➤ Added support to adopt SEL SDN switches on any port. ➤ Removed licensing requirements. ➤ Added support for setting both IP addresses in SEL SDN switches. ➤ Increased alias length to 128 characters. ➤ Added support for Relay Failover mode on Layer 2-only hosts. ➤ Added support for specifying the preferred IP address on hosts with multiple addresses. ➤ Enhanced the adoption flows to improve host discovery.	20200630
2.1.0.0	➤ Added support for application registration. ➤ Changed supported OS to Windows Server 2016 Standard. ➤ Added support for redundancy for IB management connection. ➤ Improved performance of the user interface rendering for the Flow entries page through pagination and modal view. ➤ Added support for logical connections to and from switches.	20190614

Table A.1 SEL-5056 Software Revision History (Sheet 2 of 2)

Software Version Number	Summary of Revisions	Manual Date Code
2.0.0.0	➤ Added redundancy support for point-to-multipoint logical connections. ➤ Enhanced PTP logical connections to automatically send PTP packets to Local for Power Profile support. ➤ Added TLS syslog support. ➤ Added support for reserving VIDs and viewing VIDs reserved by the SEL-5056. ➤ Logical connections now reuse group entries. ➤ A 192.168.1.1 or 169.254/16 address is no longer required for adoption. ➤ Added detailed view for logical connections. ➤ Addressed an issue where an authorized SEL-5056 Security Administrator could elevate privileges on the host Windows operating system and execute arbitrary code.	20190118
1.4.0.0	➤ Reduced the time required for switch adoptions and programming. ➤ Added support for PTP transparent clocks. ➤ Added user approval process for OpenFlow configuration synchronization. ➤ Added support for the SEL-2740S VLAN Group action bucket actions.	20180401
1.3.0.0	➤ Improved the capability to use logical connections and automate redundancy for unicast traffic. ➤ Added functionality to automate the discovery and binding of SEL relay failover mode. ➤ Enhanced host discovery to include active discovery and online monitoring. ➤ Added support for using the OFPGC_MODIFY and OFPFC_MODIFY commands in OpenFlow. ➤ Enhanced topology manager support for multiple hosts per switch port. ➤ Added support for multiple hosts per port. ➤ Enhanced license support.	20171222
1.2.0.0	➤ Enhanced to support backup and restore functionality. ➤ Improved logical connections. ➤ Expanded the use of aliases for flows, groups, meters, matches, and diagnostics. ➤ Enhanced topology manager for active discovery and improved information gathering. ➤ Added the ability to use Communication Service Types (CST) in flow programming. ➤ Improved adoption process and default conditions. ➤ Added multiple user interface enhancements. ➤ Improved feedback and error messages.	20170414
1.0.0.0	➤ Initial version.	20161104

Instruction Manual

The date code at the bottom of each page of this manual reflects the creation or revision date.

Table A.2 lists the instruction manual versions and revision descriptions. The most recent instruction manual version is listed first.

Table A.2 Instruction Manual Revision History[a]

Date Code	Summary of Revisions
20200630	➤ Initial version.

[a] Information about changes to earlier versions of the SEL-5056 instruction manual is available in the SEL-2740S/SEL-5056 instruction manual with the 20191114 date code.

APPENDIX B

Events

The Syslog Protocol is used to convey event notification messages. Both the SEL SDN switch and the SEL-5056 SDN Flow Controller create Syslog messages as defined in RFC 3164 and RFC 5424 through the use of either UDP or TCP/TLS.

This section lists the logs the SEL-5056 generates. The SEL-5056 does also collect the logs from the SEL SDN switches and can generate and send those logs as Syslogs. To know what Syslogs the SEL SDN switch can generate and therefore what Syslogs the SEL-5056 will generate when those logs are collected from the switch, refer to the SEL SDN switch manuals.

Syslog Message Format

The Syslog message is divided into five parts: priority, timestamp, source, tag, and message. The Syslogs forwarded by the SEL-5056 (for both itself and any managed SEL SDN switches) are formatted as follows:

```
<priority> timestamp hostname tag: message
```

For example:

```
<131> Jul 19 10:15:54 ROBEMEINNB TopologyManager: Disconnected
OperationalLink     OpenFlow:00000030A733EEF6:B1(1)_OpenFlow:
00000030A733EEF6:B4(4) has reconnected and is now Adopted
```

The priority is calculated from the severity and facility of the message by the following equation:

Priority = Facility • 8 + Severity

Table B.1 and *Table B.3* list the possible values for severity and facility used by the SEL-5056 and SEL-2740S.

Table B.1 Syslog Severity Levels

Code	Severity
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Informational

Table B.2 Syslog Facility Levels

Code	Facility
1	User
3	System
4	Security/Authorization

The SEL SDN switch and SEL-5056 send out Syslogs for the given Syslog severity in the Syslog Server settings as well as any Syslogs with a higher severity level (which corresponds to a lower severity code). For example, if the user configures a Syslog server with a severity level of Warning (Code 4), the SEL-5056 sends out Syslogs with that severity, as well as Syslogs with severity levels of Error, Critical, Alert, and Emergency (Codes 3, 2, 1, and 0, respectively).

The hostname in the Syslog message is the hostname of the SEL-5056 host computer, whether the SEL-5056 created the event or the SEL-5056 collected the event from the SEL SDN switch. The hostname in the Syslog messages sent directly from the SEL SDN switch to Syslog servers is its IP address.

Event Messages

Table B.3 lists the available Syslog messages and their corresponding tag, severity, and facility for the SEL-5056.

Table B.3 SEL-5056 Event Logs (Sheet 1 of 6)

Message	Tag	Severity	Facility
The application named '{applicationName}' has been activated successfully	Application Registration	Informational	User
The application named '{applicationName}' registered successfully	Application Registration	Informational	User
Commissioning failed	CommissioningManager	Warning	User
Commissioning succeeded	CommissioningManager	Informational	User
Application {application} executed action {action} on {id} from IP address {ipAddress}	DataBroker	Notice	User
Application {application} executed unbound action {action} from IP address {ipAddress}	DataBroker	Notice	User
Application {application} failed to execute unbound action {action} from IP address {ipAddress}	DataBroker	Notice	User
Application {application} modified configuration object {id} from IP address {ipAddress}	DataBroker	Notice	User
Applicaton {application} failed to execute action {action} on {id} from IP address {ipAddress}	DataBroker	Notice	User
Permission denied to user owned object {objectId} for user {username} in role {role} from module {module} to {permissionsList}	DataBroker	Notice	User
User {user} with role {role} and module {module} executed action {action} on {id} from IP address {ipAddress}	DataBroker	Notice	User
User {user} with role {role} and module {module} executed unbound action {action} from IP address {ipAddress}	DataBroker	Notice	User
User {user} with role {role} and module {module} failed to execute action {action} on {id} from IP address {ipAddress}	DataBroker	Notice	User
User {user} with role {role} and module {module} failed to execute unbound action {action} from IP address {ipAddress}	DataBroker	Notice	User

Table B.3 SEL-5056 Event Logs (Sheet 2 of 6)

Message	Tag	Severity	Facility
User {user} with role {role} modified configuration object {id} from IP address {ipAddress}	DataBroker	Notice	User
(0) {node} {tag}: {message}	DeviceManagement	Emergency	User
(1) {node} {tag}: {message}	DeviceManagement	Alert	User
(2) {node} {tag}: {message}	DeviceManagement	Critical	User
(3) {node} {tag}: {message}	DeviceManagement	Error	User
(4) {node} {tag}: {message}	DeviceManagement	Warning	User
(5) {node} {tag}: {message}	DeviceManagement	Notice	User
(6) {node} {tag}: {message}	DeviceManagement	Informational	User
Cannot create management interface to {node}	DeviceManagement	Informational	User
Failed to plan path for trust request	DeviceManagement	Informational	User
Failed to receive events for node {node}	DeviceManagement	Informational	User
Failed to set time for node {node}	DeviceManagement	Informational	User
Failed trust request for node {node}	DeviceManagement	Informational	User
Settings applied to node {node}	DeviceManagement	Informational	User
Successful trust request for node {node}	DeviceManagement	Informational	User
Unable to communicate with node {node}	DeviceManagement	Informational	User
Unadopting device {node} because unable to commission the device	DeviceManagement	Informational	User
Log delivery was not confirmed to behavior {behaviorType} for event with id {monotonicId}	EventBus	Notice	User
Updated event category {eventCategory}	EventBus	Notice	User
The IP address the controller is listening on does not exist on any of the network interfaces of this machine.	OpenFlowDriver	Error	User
Unable to validate OpenFlow certificate	OpenFlowDriver	Warning	User
Data transaction failed due to error. May have failed to delete flows or groups	OpenFlowPlugin	Error	User
Failed to delete flow due to error '{error}	'OpenFlowPlugin	Error	User
Failed to delete group due to error '{error}	'OpenFlowPlugin	Error	User
Flow entry with ID {flowCookie} inconsistent between controller and node {node}	OpenFlowPlugin	Warning	User
Flow entry with ID {flowCookie} missing from node {node}	OpenFlowPlugin	Warning	User
OpenFlow port {portId} on switch {switchId} is down	OpenFlowPlugin	Warning	User
Adding flow entry with ID {flowCookie} to node {node}	OpenFlowPlugin	Informational	User
Adding group with ID {groupId} to node {node}	OpenFlowPlugin	Informational	User
Adding meter with ID {meterId} to node {node}	OpenFlowPlugin	Informational	User
Deleting flow entry with ID {flowCookie} from node {node}	OpenFlowPlugin	Informational	User
Deleting group entry with ID {groupId} from node {node}	OpenFlowPlugin	Informational	User
Deleting meter entry with ID {meterId} from node {node}	OpenFlowPlugin	Informational	User
Flow {displayName} with Id {cookie} disabled due to hard timeout on switch	OpenFlowPlugin	Informational	User
Flow {displayName} with Id {cookie} disabled due to idle timeout on switch	OpenFlowPlugin	Informational	User
Modifying flow entry with ID {flowCookie} from node {node}	OpenFlowPlugin	Informational	User
Modifying group entry with ID {groupId} from node {node}	OpenFlowPlugin	Informational	User
Modifying meter entry with ID {meterId} from node {node}	OpenFlowPlugin	Informational	User
OpenFlow port {portId} on switch {switchId} is up	OpenFlowPlugin	Informational	User

Table B.3 SEL-5056 Event Logs (Sheet 3 of 6)

Message	Tag	Severity	Facility
Failed to delete one or more flows due to error '{error}	'PathProgrammer	Error	User
An error occurred with the restored database {error}	Persistence	Error	System
Database corruption prevented database upgrade. Please contact SEL for further assistance.	Persistence	Error	System
Database file accessed while locked	Persistence	Error	System
Insufficient disk space for data storage. Free additional disk space.	Persistence	Critical	System
The database present when the {appName} started was incompatible with this version of the {appName}.The database was renamed and a new database created.	Persistence	Error	System
Selected database was corrupt. Now attempting to restore previous database	Persistence	Error	System
The current database was generated by {appName} version {dbVersion}. The current {appName} version is {currentVersion}. Please upgrade the {appName} to the version the database was generated with or higher.	Persistence	Error	System
The database was created by {dbsApp}. It is not compatible with {runningApp}.	Persistence	Error	System
Created new database	Persistence	Informational	System
Restored database	Persistence	Informational	System
Application {application} from IP address {ipAddress} has been denied permission to {permissionList}	SecurityManager	Warning	Security
Denied permission for user {username} in role {role} from module {module} to {permissionsList}	SecurityManager	Warning	Security
Invalid token presented to the rest interface IP address {ipAddress}	SecurityManager	Warning	Security
Session for user {user} has ended	SecurityManager	Warning	Security
Authenticated user {username} in role {role} from IP address {ipAddress}	SecurityManager	Notice	Security
Unable to authenticate user from IP address {ipAddress}	SecurityManager	Notice	Security
Unable to update password for {username}	SecurityManager	Informational	Security
Received LLDP packet from an adopted 2740s device with datapath {dataPathId}	Sel2740SDiscovery	Warning	User
An unhandled exception occurred with message {message} and stack trace {stackTrace}	SEL-5056	Error	User
System Startup Completed in {bootSeconds} seconds	SEL-5056	Informational	User
Username {oldUsername} was renamed to {newUsername} due to discovery of duplicate case insensitive usernames in the local user database	SEL-5056	Informational	User
Node {node} requires additional synchronization	Synchronization	Warning	User
Node {node} requires synchronization	Synchronization	Warning	User
Node {node} no longer requires synchronization	Synchronization	Informational	User
Device {type} {nodeId} disconnected	TopologyManager	Alert	User
Adopted {type} {nodeId}	TopologyManager	Informational	User
Adopted reconnected {type} {nodeId}	TopologyManager	Informational	User
Found unadopted {type} {nodeId}	TopologyManager	Informational	User
Removed disconnected {type} {nodeId}	TopologyManager	Informational	User
Unadopted {type} {nodeId}	TopologyManager	Informational	User
User {useraname} add abstract node added to port {portId}	TopologyManager	Informational	User
User {useraname} merged Nodes {firstNodeId} and {secondNodeId}	TopologyManager	Informational	User
Certificate with common name {commonName} and thumbprint {thumbprint} internally {revokeState}	TrustAuthority	Warning	User
User {username} failed to import certificate for purpose {purpose}	TrustAuthority	Warning	User

Table B.3 SEL-5056 Event Logs (Sheet 4 of 6)

Message	Tag	Severity	Facility
User {username} revoked certificate {thumbprint}	TrustAuthority	Warning	User
User {username} uploaded certificate {thumbprint} for {certificatePurpose}	TrustAuthority	Notice	User
Failed to find valid network interface information.	Utilities	Error	User
A corrupt packet was received.	Utilities	Informational	User
Error deserializing OFDP packet.	Utilities	Informational	User
An adopted node could not be found for ip '{ip}'	Learn and Lock	Error	User
Auto Adoption has completed	Learn and Lock	Informational	User
Auto Adoption failed for operational host '{name}' for the following reason: {reason}	Learn and Lock	Error	User
Auto Adoption failed for operational link '{name}' for the following reason: {reason}	Learn and Lock	Error	User
Auto Adoption failed for operational switch '{name}' for the following reason: {reason}	Learn and Lock	Error	User
Out of IP Addresses	Learn and Lock	Error	User
There are '{nodecount}' pending nodes remaining after auto adoption and there should not be any	Learn and Lock	Error	User
Auto Adoption has started	Learn and Lock	Informational	User
The Learn and Lock task named '{taskname}' has completed	Learn and Lock	Informational	User
Auto Adoption cannot use a 2740S config node for operational node '{displayname}' in this Learn and Lock session	Learn and Lock	Error	User
Auto Adoption could not build a config node for operational node '{displayname}'	Learn and Lock	Error	User
Auto Adoption cannot use a generic config node for operational node '{displayname}' in this Learn and Lock session	Learn and Lock	Error	User
Auto synchronization for switch {displayName} failed for reason {reason}	Learn and Lock	Informational	User
Replanning in-band management logical connection with id '{id}'	Learn and Lock	Informational	User
Logical Connection Learning has completed	Learn and Lock	Informational	User
Could not create a logical connection because the communication service type '{cstname}' failed to save for the following reason: {reason}	Learn and Lock	Error	User
Could not find a pair of config nodes for source ip '{srcip}' and destination ip '{dstip}' : '{reason}'	Learn and Lock	Informational	User
Logical Connection Learning has created a Communication Service Type named '{displayName}'	Learn and Lock	Informational	User
Logical Connection Learning has created a Logical Connection with id '{id}'	Learn and Lock	Informational	User
Logical Connection Learning has started	Learn and Lock	Informational	User
An operational node could not be found for ip '{ip}' with additional packet info: {packetinfo}	Learn and Lock	Error	User
Replanning of in-band management logical connections has completed	Learn and Lock	Informational	User
Replanning of in-band management logical connections has started	Learn and Lock	Informational	User
Detection of SEL Relay Failover devices has completed	Learn and Lock	Informational	User
Detection of SEL Relay Failover devices has started	Learn and Lock	Informational	User
Switch {displayName} in need of synchronization will now be automatically synchronized	Learn and Lock	Informational	User
The Communication Service Types '{firstCst}' and '{secondCst}' have the same priority and were both determined to match traffic	Learn and Lock	Error	User
Failed to delete one or more flows due to error '{error}'.	PathProgrammer	Error	User

Table B.3 SEL-5056 Event Logs (Sheet 5 of 6)

Message	Tag	Severity	Facility
Received LLDP packet from an adopted 2740s device with datapath {dataPathId}	Sel2740SDiscovery	Warning	User
Auto Adoption ended manually for reason {reason}	Learn and Lock	Informational	User
Auto Adoption ended manually by user {user}	Learn and Lock	Informational	User
The controller is not in the same subnet as the starting and ending IP addresses	Learn and Lock	Warning	User
Auto Adoption is unadopting the switch '{displayname}' to retry adoption	Learn and Lock	Informational	User
Outstanding synchronizations blocking has completed	Learn and Lock	Informational	User
Outstanding synchronizations blocking has started	Learn and Lock	Informational	User
Cannot delete a Learn and Lock session while another Learn and Lock session is active.	Learn and Lock	Error	User
CSV file creation failed with message {message}	Learn and Lock	Informational	User
'{username}' has deleted Learn and Lock session '{sessionId}	'Learn and Lock	Informational	User
An inactive session with id '{id}' could not be found	Learn and Lock	Informational	User
The Learned Logical Connection {llcDisplayName} has changed state from {priorState} to {newState}	Learn and Lock	Informational	User
{phase} cannot be interrupted	Learn and Lock	Warning	User
Adoption failed for host {displayName}	Learn and Lock	Informational	User
Adoption failed for link {displayName}	Learn and Lock	Informational	User
Adoption failed for switch {displayName}	Learn and Lock	Informational	User
Adoption has been initiated for host {displayName}	Learn and Lock	Informational	User
Adoption has been initiated for link {displayName}	Learn and Lock	Informational	User
Adoption has been initiated for switch {displayName}	Learn and Lock	Informational	User
Adoption succeeded for host {displayName}	Learn and Lock	Informational	User
Adoption succeeded for link {displayName}	Learn and Lock	Informational	User
Adoption succeeded for switch {displayName}	Learn and Lock	Informational	User
Logical Connection Learning has completed automatically	Learn and Lock	Informational	User
Logical Connection Learning ended manually by user {user}	Learn and Lock	Informational	User
Logical Connection Learning has completed by timeout	Learn and Lock	Informational	User
Could not find the learned logical connection with Id '{id}' in the current Learn and Lock session	Learn and Lock	Error	User
Generic {udpTcp} Logical Connection may be created from {sourceIP} to {destIP} due to: {fragmentOrHighPort}	Learn and Lock	Informational	User
A logical connection was not proposed because the packet has ethertype '{ethertype}' - Packet Information: {packetInfo}	Learn and Lock	Informational	User
A logical connection was not proposed because the packet has IP protocol '{ipProto}' - Packet Information: {packetInfo}	Learn and Lock	Informational	User
A logical connection was not proposed because the source IP address {srcIp} and destination IP address {dstIp} are outside the learning region - Packet Information: {packetInfo}	Learn and Lock	Informational	User
A logical connection was not proposed because the packet has an IP address of '{ip}' for both the source and destination address - Packet Information: {packetInfo}	Learn and Lock	Informational	User
A logical connection was not proposed because it is either already proposed or it is filtered - Packet Info: {packetInfo}	Learn and Lock	Informational	User
One or more nodes failed auto synchronization. User must manually synchronize node(s) before Learn and Lock can continue on to Logical Connection Learning.	Learn and Lock	Warning	User

Table B.3 SEL-5056 Event Logs (Sheet 6 of 6)

Message	Tag	Severity	Facility
Network reset has completed automatically	Learn and Lock	Informational	User
Host '{displayname}' was not unadopted	Learn and Lock	Error	User
Network reset has started	Learn and Lock	Informational	User
Switch '{displayname}' was not unadopted	Learn and Lock	Error	User

This page intentionally left blank

APPENDIX C

Protocol Match Criteria

Introduction

SDN is a deny-by-default network architecture so only the traffic engineered communications are forwarded. When using the SEL SDN solution it is highly recommended to use the logical connection automation to perform circuit provisioning. To use logical connections each individual conversation you want to provision on the network must have its own CST. These CSTs are the match criteria defining how to identify a packet as belonging to the specific conversation you are provisioning. This appendix explains how to collect the necessary information for matching protocols and to match a list of common network protocols.

Overview

Each protocol may have multiple message types carrying out different functions for that protocol. A message type is the smallest unit of a protocol that the switch can distinguish based on the supported match fields of the switch and the packet fields defined by the protocol. For example, unicast Network Time Protocol (NTP) has two message types, one type for the request and one type for the reply; the reason for this is that the User Datagram Protocol (UDP) ports are different for each message, so you can use match fields to distinguish between the messages.

Be aware that some intermediate devices, such as routers, can modify the packet fields. Always design match fields based on how the packets appear on ingress to the switch. Some protocols, such as Virtual Private Network (VPN), encapsulate packets. Only the outermost packet fields are used for matching.

Layer Type

Traffic can be divided into three general categories and three subcategories for IP Layer traffic, based on the layer of the traffic:

- Layer 2
- Address Resolution Protocol (ARP)
- IP Layer
  - IP only
  - Transmission Control Protocol (TCP)/IP
  - UDP/IP

Layer 2

Layer 2 traffic is often only matchable on the source and destination media access control (MAC) address, EthType, physical ports, and VLAN tags.

ARP

A software-defined network (SDN) has three ARP match fields: ArpOp, ArpSpa, and ArpTpa. ARP packets can be treated as point-to-point traffic instead of multicast traffic by matching on these ARP field and using the IP addresses of the hosts. The logical connections automate the configuration of these addresses into the circuit when you provision it.

IP Layer

IP traffic can be divided into three categories:

- IP Layer traffic
- TCP/IP traffic
- UDP/IP traffic

IP Layer protocol can be distinguished by the IP Protocol field. The TCP/IP and UDP/IP Layer protocols can be distinguished by TCP/IP and UDP/IP source and destination ports respectively.

Pure IP traffic, such as Internet Control Message Protocol (ICMP), resides directly on top of the IP header and has no ports on which to match. These applications are distinguished from each other by the IP Protocol field. TCP/IP and UDP/IP traffic each have a specific IP code, so they are only distinguished based on source and destination port numbers, not the IP Protocol value.

Prerequisites

Prerequisites required based on the OpenFlow standard are entered for you when using the SEL-5056.

Unique Match Fields

Unique match fields are useful for differentiating traffic. For example, at the IP Layer, this would be the IpProto match field; for UDP/IP traffic, this would be the UdpDst or UdpSrc match fields. For Layer 2, the destination Ethernet address is often set by the protocol, as in the case for Spanning Tree Protocol (STP) and GOOSE.

Directionality

Protocols can be further divided by directionality into two types: unidirectional and bidirectional. Unidirectional protocols only travel from source to destination; bidirectional protocols have one flow that travels from source to destination and another flow that travels from destination to source. Bidirectional flows may require a different message type if the protocol (for example, NTP) uses a request and reply method for communication. For unicast IP traffic, bidirectional ARP flows are also required.

Cast Type

Traffic can also be divided into unicast, broadcast, and multicast. Broadcast and multicast traffic can sometimes be modeled as unicast if the conversation is only between two devices, such as with an ARP request and reply, or with an IEC 61850 GOOSE message with only one subscriber. SEL SDN solutions allow you to control the destinations of each packet. When logical connections are used, only the destinations that want to process the packet see the packet, eliminating unwanted noisy traffic from the network. The system owner, not the packet attributes, now controls the casting of packets and not dictated by packet attributes. You can now send unicast to multiple destinations, such as your intrusion detection system or backup devices, and you can manage the multicast traffic without complex VLAN management.

This page intentionally left blank

APPENDIX D

Application Permissions

Table D.1 shows the generally allowed functions listed in the Permissions tab of an enabled application in the Application Management Page. These are the permissions third-party software applications use.

Table D.1 Application Permissions (Sheet 1 of 6)

Permission	What the Application Is Allowed to Do
Permission Tag : Factory Default Reset	One of the permissions required to factory-default reset an SEL-2740S
Permission Tag : Firmware Upgrade	One of the permissions required to firmware update an SEL-2740S
Permission Tag : Reboot	One of the permissions required to restart an SEL-2740S
Permission Tag : Replan Controller Route	Replan the IB management logical connection to/from a switch
Permission Tag : Engineer	One of the permissions required to factory-default reset an SEL-2740S One of the permissions required to firmware update an SEL-2740S One of the permissions required to restart an SEL-2740S
Permission Tag : Monitor	Read-only access on an SEL-2740S
Permission Tag: Administrator	Perform administrative role tasks on an SEL-2740S
Permission Tag : Read Data Type : Role	Perform engineering role tasks on an SEL-2740S
Permission Tag : Create Data Type : User	Create users
Permission Tag : Read Data Type : User	One of the permissions required to update users Read users
Permission Tag : Update Data Type : User	One of the permissions required to update users Update users
Permission Tag : Delete Data Type : User	Delete users One of the permissions required to update users
Permission Tag : Create Data Type : Auth Service	Create authentication services
Permission Tag : Read Data Type : Auth Service	One of the permissions required to update created authentication services Read created authentication services
Permission Tag : Update Data Type : Auth Service	One of the permissions required to update created authentication services Update created authentication services
Permission Tag : Delete Data Type : Auth Service	Delete created authentication services One of the permissions required to update created authentication services
Permission Tag : Create Data Type : Auth Service Group	Create authentication service groups
Permission Tag : Read Data Type : Auth Service Group	One of the permissions required to update authentication service groups Read authentication service groups
Permission Tag : Update Data Type : Auth Service Group	One of the permissions required to update authentication service groups Update authentication service groups
Permission Tag : Delete Data Type : Auth Service Group	Delete authentication service groups One of the permissions required to update authentication service groups

Table D.1 Application Permissions (Sheet 2 of 6)

Permission	What the Application Is Allowed to Do
Permission Tag : Read Data Type : Security Manager Settings	One of the permissions required to update maximum login attempts, lockout seconds, and login attempt windows Read maximum login attempts, lockout seconds, and login attempt windows
Permission Tag : Update Data Type : Security Manager Settings	One of the permissions required to update maximum login attempts, lockout seconds, and login attempt windows Update maximum login attempts, lockout seconds, and login attempt windows
Permission Tag : Subscribe Data Type : Security Manager Settings	One of the permissions required to update maximum login attempts, lockout seconds, and login attempt windows
Permission Tag : Change Own Password	Change the current user password
Permission Tag : Auth Service . Test User Authenticate	Test an authentication service
Permission Tag : Auth Service . Get Available Groups	Get the authentication groups for an authentication service
Permission Tag : Backup	Backup an SEL-5056 database
Permission Tag : Restore	Restore an SEL-5056 database
Permission Tag : Read Data Type : Certificate Information	Get a certificate in PEM format One of the permissions required to revoke a X.509 certificate by its purpose One of the permissions required to revoke an X.509 certificate One of the permissions required to revoke an X.509 certificate by its thumb print Read X.509 Certificates
Permission Tag : Revoke	One of the permissions required to revoke a X.509 certificate by its purpose One of the permissions required to revoke an X.509 certificate One of the permissions required to revoke an X.509 certificate by its thumb print
Permission Tag : Replace	One of the permissions required to revoke a X.509 certificate by its purpose One of the permissions required to revoke an X.509 certificate One of the permissions required to revoke an X.509 certificate by its thumb print Upload an X.509 certificate
Permission Tag : Read Data Type : Event Category	One of the permissions required to update event categories Read event categories
Permission Tag : Update Data Type : Event Category	One of the permissions required to update event categories Update event categories
Permission Tag : Subscribe Data Type : Event Category	One of the permissions required to update event categories
Permission Tag : Read Data Type : Event Type	Read event categories
Permission Tag : Read Data Type : Locale String	Read strings
Permission Tag : Read Data Type : Rest Settings	One of the permissions required to update usage policy, maximum number of concurrent sessions, and session timeout Read usage policy, maximum number of concurrent sessions, and session timeout
Permission Tag : Update Data Type : Rest Settings	One of the permissions required to update usage policy, maximum number of concurrent sessions, and session timeout Update usage policy, maximum number of concurrent sessions, and session timeout
Permission Tag : Subscribe Data Type : Rest Settings	One of the permissions required to update usage policy, maximum number of concurrent sessions, and session timeout
Permission Tag : Update License	Upload a new SEL-5056 license

Table D.1 Application Permissions (Sheet 3 of 6)

Permission	What the Application Is Allowed to Do
Permission Tag : Read Licensing	Read SEL-5056 license
Permission Tag : Read Data Type : System Message	Read system messages
Permission Tag : Create Data Type : Preference	One of the permissions required to add or modify a user preference One of the permissions required to update created Communication Service Types (CST)
Permission Tag : Read Data Type : Preference	Get the value of a user preference One of the permissions required to add or modify a user preference Read user preferences
Permission Tag : Update Data Type : Preference	One of the permissions required to add or modify a user preference
Permission Tag : Delete Data Type : Preference	Delete user preferences
Permission Tag : Read Data Type : Application Link	Read registered applications
Permission Tag : Create Data Type : Application Link	Create registered applications
Permission Tag : Delete Data Type : Application Link	Delete registered applications
Permission Tag : Initiate Application Registration	Have the SEL-5056 contact a URL for application registration
Permission Tag : Enable Application Link	Enable an application
Permission Tag : Disable Application Link	Disable an application
Permission Tag : Create Data Type : Config Node	Create hosts and switches
Permission Tag : Read Data Type : Config Node	One of the permissions required to create logical connections One of the permissions required to reset the counters for a flow entry One of the permissions required to resubmit a logical connection One of the permissions required to update created hosts and switches Read created hosts and switches
Permission Tag : Update Data Type : Config Node	One of the permissions required to update created hosts and switches Update created hosts and switches
Permission Tag : Delete Data Type : Config Node	Delete created hosts and switches One of the permissions required to update created hosts and switches
Permission Tag : Create Data Type : Config Link	Create links
Permission Tag : Read Data Type : Config Link	One of the permissions required to update created links Read created links
Permission Tag : Update Data Type : Config Link	One of the permissions required to update created links Update created links
Permission Tag : Delete Data Type : Config Link	Delete created links One of the permissions required to update created links
Permission Tag : Create Data Type : Config Port	Create ports
Permission Tag : Read Data Type : Config Port	One of the permissions required to update created ports Read created ports

Table D.1 Application Permissions (Sheet 4 of 6)

Permission	What the Application Is Allowed to Do
Permission Tag : Update Data Type : Config Port	One of the permissions required to update created ports Update created ports
Permission Tag : Delete Data Type : Config Port	Delete created ports One of the permissions required to update created ports
Permission Tag : Read Data Type : Operational Network Node	Get nodes by IP address One of the permissions required to remove a host or switch One of the permissions required to reset the counters for a flow entry One of the permissions required to send a PACKET OUT from a switch port Read detected hosts and switches
Permission Tag : Read Data Type : Operational Network Port	One of the permissions required to add a traditional switch Read detected ports
Permission Tag : Read Data Type : Operational Network Link	Read detected links
Permission Tag : Read Data Type : Network Settings	One of the permissions required to update default adoption settings and default ARP SPA IP address Read default adoption settings and default ARP SPA IP address
Permission Tag : Update Data Type : Network Settings	One of the permissions required to update default adoption settings and default ARP SPA IP address Update default adoption settings and default ARP SPA IP address
Permission Tag : Subscribe Data Type : Network Settings	One of the permissions required to update default adoption settings and default ARP SPA IP address
Permission Tag : Adopt Object	Adopt a host or switch with a preconfigured host or switch object Adopt a host with default settings Adopt a port with a preconfigured port object Adopt a port with default settings Adopt link with default settings
Permission Tag : Unadopt Object	Unadopt a host or switch Unadopt a link Unadopt a port
Permission Tag : Disconnect Object	One of the permissions required to remove a host or switch
Permission Tag : Replace Object	One of the permissions required to remove a host or switch
Permission Tag : Topology Discovery Hinting	Disable SEL Relay Failover mode from a port Enable SEL Relay Failover mode for a port One of the permissions required to add a traditional switch One of the permissions required to detect the other port of an SEL relay device
Permission Tag : Perform Synchronization	One of the permissions required to add a traditional switch
Permission Tag : Create Data Type : Flow	Create flow entries
Permission Tag : Read Data Type : Flow	One of the permissions required to reset the counters for a flow entry Read flow entries
Permission Tag : Update Data Type : Flow	Update flow entries
Permission Tag : Delete Data Type : Flow	Delete flow entries
Permission Tag : Create Data Type : Group	Create group entries

Table D.1 Application Permissions (Sheet 5 of 6)

Permission	What the Application Is Allowed to Do
Permission Tag : Read Data Type : Group	Read created group entries
Permission Tag : Update Data Type : Group	Update created group entries
Permission Tag : Delete Data Type : Group	Delete created group entries
Permission Tag : Create Data Type : Meter	Create meter entries
Permission Tag : Read Data Type : Meter	One of the permissions required to update created meter entries Read created meter entries
Permission Tag : Update Data Type : Meter	One of the permissions required to update created meter entries Update created meter entries
Permission Tag : Delete Data Type : Meter	Delete created meter entries One of the permissions required to update created meter entries
Permission Tag : Read Data Type : Flow Stats	Read flow entry diagnostics
Permission Tag : Read Data Type : Meter Stats	Read meter diagnostics
Permission Tag : Read Data Type : Group Desc	Read group entry descriptions
Permission Tag : Read Data Type : Group Stats	Read group diagnostics
Permission Tag : Read Data Type : Table Stats	Read flow table diagnostics
Permission Tag : Read Data Type : Port Stats	Read port diagnostics from OpenFlow
Permission Tag : Read Data Type : Meter Descriptions	Read meter descriptions
Permission Tag : Read Data Type : Synchronization Request	Nodes that are not synchronized Read nodes to synchronize
Permission Tag : Read Data Type : Received Packet	Read collected packet in packets
Permission Tag : Reset Flow Counters	One of the permissions required to reset the counters for a flow entry
Permission Tag : Set Flow Mod	Modify the OpenFlow settings of an OpenFlow port One of the permissions required to detect the other port of an SEL relay device One of the permissions required to reset the counters for a flow entry
Permission Tag : Perform Synchronization	One of the permissions required to detect the other port of SEL relay device
Permission Tag : Send Packet Out	One of the permissions required to send a PACKET OUT from a switch port
Permission Tag : Create Data Type : Logical Connection	One of the permissions required to create logical connections One of the permissions required to resubmit a logical connection One of the permissions required to send a PACKET OUT from a switch port
Permission Tag : Read Data Type : Logical Connection	Get path plan for a logical connection Get the OpenFlow entries for a logical connection Get the OpenFlow counters for a logical connection One of the permissions required to resubmit a logical connection Read created logical connections

Table D.1 Application Permissions (Sheet 6 of 6)

Permission	What the Application Is Allowed to Do
Permission Tag : Update Data Type : Logical Connection	No effect
Permission Tag : Delete Data Type : Logical Connection	One of the permissions required to delete created logical connections One of the permissions required to resubmit a logical connection
Permission Tag : Create Data Type : Communication Service Type	Create CSTs
Permission Tag : Read Data Type : Communication Service Type	One of the permissions required to create logical connections One of the permissions required to resubmit a logical connection One of the permissions required to update created CSTs Read created CSTs)
Permission Tag : Update Data Type : Communication Service Type	One of the permissions required to update created CSTs Update created CSTs
Permission Tag : Delete Data Type : Communication Service Type	Delete created CSTs One of the permissions required to update created CSTs
Permission Tag : Activate Logical Connection	One of the permissions required to create logical connections One of the permissions required to delete created logical connections One of the permissions required to resubmit a logical connection
Permission Tag : Read Data Type : Vlan Vid Reservation	One of the permissions required to create logical connections One of the permissions required to delete created logical connections One of the permissions required to resubmit a logical connection Read reserved VIDs
Permission Tag : Delete Data Type : Vlan Vid Reservation	Delete reserved VIDs
Permission Tag : Reserve Vlan Vid Permission	Reserve a VID

APPENDIX E

Security

Introduction

This appendix covers the security features of the SEL-5056.

Security Environment

Figure E.1 shows the interfaces for the SEL-5056 and the connections to other services including the SEL SDN switch, the user components, and how these components interact with each other. *Figure E.2* shows an example of where some of the interfaces labeled in *Figure E.1* may appear in a network. It is assumed that the SEL-5056 is installed on a trusted computer and the operating system is maintained. Access controls to the user interface of the SEL-5056 should be limited to only those that have a need to know and least privileges. It is also assumed that commissioning is done on a trusted network so the passing of original trust credentials is protected.

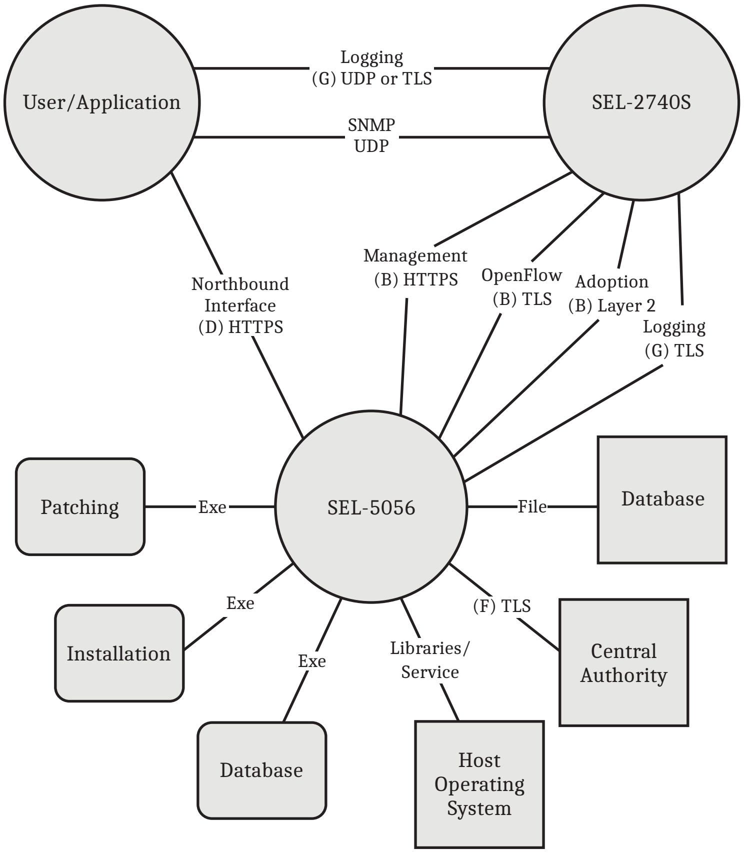


Figure E.1 SDN System Diagram

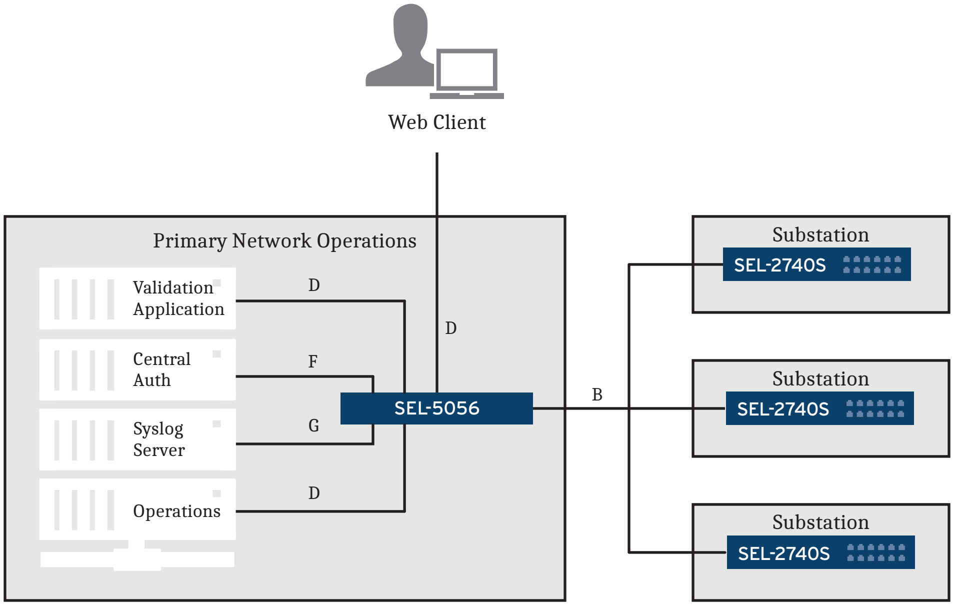


Figure E.2 Example SDN Diagram

SEL-5056 Version Information

The latest version of the SEL-5056 is downloaded from the SEL website on the SEL-5056 product page. An active SEL account is required to download the software. The SEL-5056 installer is digitally signed by SEL and the service that is installed is the "SEL-5056 Service." Program files are installed C:\Program Files (x86)\SEL\SEL-5056 and the operational files are installed C:\ProgramData\SEL\SEL-5056. Release notes are included in the manual revisions and SEL's security vulnerability disclosure procedures are documented at selinc.com/support/security-notifications/.

SEL-5056 Communications

There are two points of communication between the SEL SDN switch and the SEL-5056: OpenFlow and the management interface.

OpenFlow

OpenFlow is the protocol that defines the message type contents between an SDN controller and an SDN switch. The controller uses OpenFlow to program the switches, and the switches use OpenFlow to report counters and errors back to the controller. The SEL SDN switch only supports OpenFlow over Transport Layer Security (TLS). TLS uses X.509 certificates from the switch and the SEL-5056. The SEL-5056 uses the public key it obtains from a switch to confirm the identity of that switch. The certificates are configured as part of the commissioning and adoption process. The certificates are stored in the SEL-5056 database and will be included as part of the backup files so safe handling of the backup files is recommended.

Management

The management interface is a representational state transfer (REST) interface that enhances the SEL-5056 and SEL SDN switch communications interface to cover functionality not supported by OpenFlow. Such functionality includes exchanging X.509 certificates, ejecting modules, factory decommissioning the SEL SDN switch, and collecting Syslogs. The user communicates with the SEL-5056 through the northbound interface (NBI), which then communicates with the switch through the management interface. Communication is secured through the use of HTTPS.

Open Ports

Table E.1 lists all open ports on the SEL-5056 and SEL-2740S.

Table E.1 Summary of Open Ports (Sheet 1 of 2)

Component	Port	Interface
SEL-5056	6653[a]	OpenFlow
	443[a]	NBI

Table E.1 Summary of Open Ports (Sheet 2 of 2)

Component	Port	Interface
SEL-2740S	443	Management
	161[b]	SNMP (read-only)
	3002[c]	Adoption

[a] This can be modified through the SEL-5056 settings.

[b] If enabled.

[c] Closed after the commissioning process is complete.

The SEL SDN switch adoption process uses Layer 2 multicast packets, so no ports are used.

User and SEL-5056 Communications

The user has a single point of contact for communicating with the SEL-5056 through the northbound REST interface by using a browser and making an HTTPS connection.

SEL-5056 Component

Account Management

Default Accounts

The SEL-5056 has no default account. Upon installation of the SEL-5056, the user creates an account with Security Administrator privileges. This account can be deleted, but at least one local Security Administrator account must always be present. This account allows a user to access the SEL-5056 if other accounts are disabled and the Lightweight Directory Access Protocol (LDAP) server is unavailable.

User Accounts

Any local user account can be deleted as long as one Security Administrator account is still active locally. After three unsuccessful login attempts, the IP address locks out for 5 minutes. Login failures are logged.

User Roles

The user uses a single role to log in and only has access to the services that role authorizes. If the user wants to change roles, the user must use the new role and reauthenticate. For example, although a user may have both Security Administrator and Monitor access, the user can only log in either as a Security Administrator or as a Monitor at any one time and must reauthenticate to change roles.

Passwords

Complex passwords are required for local user accounts that are a minimum of eight characters long and include at least one uppercase letter, one lowercase letter, one number, and one special character. All printable characters, including a space, are supported in the password. Passwords are salted and hashed in the database.

Authorization Services

The SEL-5056 supports LDAP to provide authorization services. It supports StartTLS through the use of the locally stored public certificate of the LDAP server and imported into the SEL-5056.

Applications

Additional grant types are available for registered applications. The public certificate of the application must be imported as a trusted certificate and the application must be registered and enabled to obtain or to continue to use an OAuth token. Communications are over HTTPS.

Network Interfaces

Besides the OpenFlow and management interfaces that users can use to communicate with the SEL SDN switch, the SEL-5056 also has interfaces for the RESTful NBI that provides web interface and authorization services.

RESTful NBI

The NBI is a REST interface transported over HTTPS through the use of a single certificate within the SEL-5056, and the user either imports this certificate or it is generated internally. The REST client authenticates the SEL-5056 by using this certificate. The web user interface uses the NBI to communicate with the SEL-5056. The northbound REST interface on the SEL-5056 uses OAuth 2.0 authentication for any service requesting connection. A Resource Owner Password Credentials grant is provided as follows:

> Client ID: “password-client”
> Client Secret: “Rest Interface”

This credential allows connection to the interface and after connection, the service must supply a unique and configurable username and password to read or write any data to the REST interface.

The REST interface uses OData v4 and provides a notification interface with SignalR. The SEL-5056 requires no credentials for commissioning.

Logging

You can store logs in the Windows Logger or on a Syslog server, depending upon whether you have configured these. The SEL-5056 collects the Syslogs generated by the switch and sends these to the Syslog servers and Windows Logger.

Database

The database, stored on the same computer as the SEL-5056, contains all SEL-5056 settings, including flow entries and passwords. The passwords are salted and hashed. except for the LDAP bind user passwords that are stored in plaintext, as LDAP requires.

The SEL-5056 accesses the database through a database manager. A service created the database, so Administrator privileges are necessary to access it. The user can use the SEL-5056 to back up and restore the database, and when the SEL-5056 is uninstalled, the user can either preserve or delete the database.

Time

Several parts of the SDN are time-sensitive, and these would therefore be affected by network issues. The certificates the SEL-5056 and switch both use are time-sensitive. OpenFlow flow entries can also have time-outs, and these could not be refreshed if the controller connection were unavailable.

Certificate Management

The SEL-5056 performs certificate management, so such management does not rely on the operating system.

Final Authority

The SEL-5056 is the final authority for switch configuration, including all OpenFlow-related functionality. If the switch configuration varies from normal parameters, the SEL-5056 logs it and notifies the user if the OpenFlow configuration on an OpenFlow node differs from the expected configuration.

Installation/Maintenance

Users can update and patch the SEL-5056 by installing an updated version. You can restore the SEL-5056 to a factory-default state by deleting the database. All SEL-5056 software is digitally signed.

SEL SDN Switch Component

Account Management

The SEL SDN switches do not have either user accounts or passwords. A Java Web Token (JWT) replaces user accounts for accessing the device through the management interface.

Network Interfaces

The SEL SDN switches have no user interface and only supports communication through the OpenFlow, SNMP, PTP, and the management interface. The SEL SDN switches have SNMP and PTP disabled by default. OpenFlow and the REST management interface cannot be disabled.

Installation/Maintenance

The SEL SDN switches come preinstalled with firmware. Users can use the SEL-5056 to update the firmware. If an SEL SDN switch must be replaced, you can use the SEL-5056 to apply the configuration. When an SEL SDN switch must be removed from service, you can decommission it, removing all device configuration and restoring factory-default settings either through the SEL-5056 or through the front pushbutton reset.

Certificates

The SEL SDN switch trusts the certificate authority (CA). The SEL SDN switch stores its certificates locally. *Table E.2* lists the possible certificates on the switch.

Table E.2 Certificates on the SEL-2740S

Interface	Certificates
OpenFlow	Public/Private[a]
Management	Public/Private CA Public Certificate
Autodiscovery	Self-Signed Private[b]

[a] For both the switch and the SEL-5056.

[b] Deleted when adopted by the SEL-5056.

Recommendations

The following items are suggested security recommendations.

Turn Off Domain Name System

The SEL-5056 only requires domain name system (DNS) for LDAP hostname resolution. You could instead use a host file to eliminate the need for DNS on the SEL-5056 host machine and therefore eliminate the need for DNS as an attack vector.

Manage OS

The SEL-5056 manages the SDN. If the SEL-5056 host machine OS is compromised, the network or network configuration is at risk. Use best practices to make the SEL-5056 host machine OS as secure as possible.

Hard Drive Encryption

The SEL-5056 persists on the hard drive of the host computer. Although the OS has controls in place to prevent unauthorized access, these controls are only active when the OS is running. An attacker could boot the host machine under an alternative OS and gain access to the database for information retrieval or modification. Using hard drive encryption helps prevent unauthorized access to the database of the SEL-5056.

Standalone Host Machine for the SEL-5056

Although the SEL-5056 can run in a virtual machine, running the SEL-5056 on a standalone host machine provides the best and most secure performance.

Because reductions in running services make the machine more secure, installing the SEL-5056 on a standalone machine reduces the number of services the host machine requires. Nonessential services should be disabled.

Security Support

Contact SEL security with any additional questions or concerns at:

Tel: +1.509.332.1890
Email: security@selinc.com

Technical Support

We appreciate your interest in SEL products and services. If you have questions or comments, contact us at:

Schweitzer Engineering Laboratories, Inc.
2350 NE Hopkins Court
Pullman, WA 99163-5603 U.S.A.
Tel: +1.509.338.3838
Fax: +1.509.332.7990
Internet: selinc.com/support
Email: info@selinc.com

APPENDIX F

Learn and Lock Extension

Extension Overview

The Learn and Lock extension provides the functionality to help simplify the network topology discovery and communications circuit provisioning. This extension commissions and adopts switches; discovers and adopts hosts and links; and provisions Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Address Resolution Protocol (ARP) and Internet Control Message Protocol (ICMP) communications with minimal user interaction. The primary functions automated in the Learn and Lock extension include the following:

- Network reset: Removes of all previous configurations and returns the system to an initial state.
- Topology management: This is called Auto Adoption, and this feature discovers and adopts switches, hosts, and links.
- Communication circuit provisioning: This is called Logical Connection Learning, and this feature learns what ARP, TCP, UDP, and ICMP conversations each adopted host is attempting to have and provisions logical connections.

The Learn and Lock extension is initiated by an authorized user with Permission Level 3 privileges. Use caution when using the SEL-5056 SDN Flow Controller features during the Learn and Lock session because changes may impact the operations of the Learn and Lock extension. Only one Learn and Lock session can run at a time and only one of the three Learn and Lock functions can operate in the session at a time. A Learn and Lock session allows the user to choose which of the three functions to run as part of the session. When running multiple functions in a single session, the session starts with the Network Reset, next the Auto Adoption, and finishes with the Logical Connection Learning. You can start, stop, and manage Learn and Lock sessions through the menu on the Topology page, as shown in *Figure F.1*.

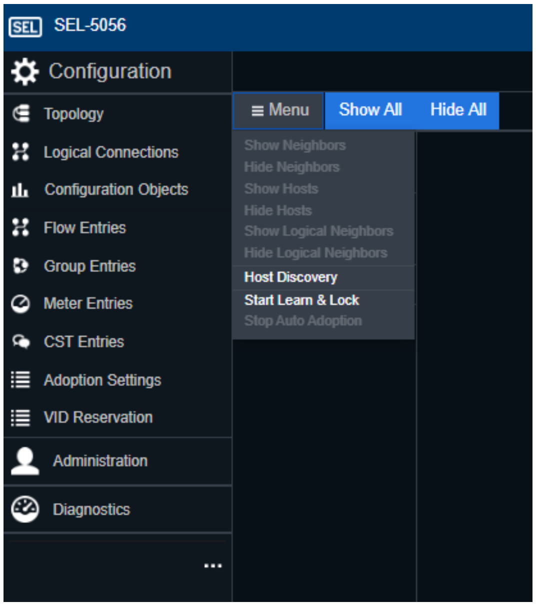


Figure F.1 Learn and Lock Menu

Extension Details

Network Reset

The Learn and Lock extension can perform a network reset. This feature resets all network elements managed by the SEL-5056 and clears configurations in the following order:

- Deletes all logical connections except for the in-band management logical connections
- Deletes all flows, groups, and meters, except for the ones used for in-band management
- Unadopts all SDN switches, traditional switches, hosts, and links
- Deletes all configuration nodes, configuration links, and configuration ports
- Removes all Learn and Lock session history

This process interrupts communications on the system and brings the network to the deny-by-default factory-default state. When you are using in-band management, the reset feature unadopts switches starting with the furthest switch away from the SEL-5056 to the closest.

To initiate a network reset, use the drop-down menu on the Topology page and select **Start Learn and Lock Session**. Then, confirm the network reset function is active. Optionally, you can also select the Auto Adoption and Logical Connection Learning functions to activate after the network reset is completed. The network rest function is completed when all the elements are unadopted and deleted. The Learn and Lock session ends at this point if the network reset is the only function selected for the session. The network rest function autotransitions to Auto Adoption when that function is also enabled for the same session. Logical Connection Learning cannot follow a network reset without running Auto Adoption first.

Topology Management—Auto Adoption

The Learn and Lock extension can perform Auto Adoption. This feature discovers switches, hosts, and links on the network and adopts them. New configuration nodes are created when hosts and switches are discovered. The name of the configuration node is the IP address for hosts and the DataPath ID for SDN switches. All links discovered are adopted. This feature discovers dual-attached nodes running SEL Relay Failover mode and replans in-band management logical connections after all switches are adopted to confirm the most optimum control plane path is configured.

One prerequisite before starting an Auto Adoption session is that you must create an SEL SDN switch template to use in the session. Creating this template is the same as creating a configuration node for the SEL SDN switch and is used to set the configurations for all Auto Adopted switches. You must fill in the IP address field for the template; however, the IP address field value is not used, so use zeros for the octets that you have set for the range (e.g., 192.168.1.0 if you have a /24 range). To start an Auto Adoption session, start a Learn and Lock session and enable the Auto Adoption feature. To configure Auto Adoption, enter a switch configuration node with the desired settings and use this as a template for the settings that will be used for all discovered switches. These settings include the default gateway, subnet, flow controller address, PTP, NTP, SNMP, log services, alarm, and certificate settings. Then, enter the desired values for the remaining settings. *Table F.1* lists these remaining settings.

Table F.1 SEL SDN Switch Auto Adoption Management Configurations

Name	Default Value	Minimum	Maximum	Description
Maximum Switch Count	Unlimited	1	Unlimited	The maximum number of SEL SDN switches that can be adopted. Note the maximum number of switches the SEL-5056 can adopt is also controlled by the license.
Maximum Host Count	Unlimited	1	Unlimited	The maximum number of hosts that can be adopted.
Minimum IP address	192.168.1.2	Any valid IPv4 address	Must be lower than the Maximum IP address setting	The first IP address that is used to adopt the first SEL SDN switch discovered.
Maximum IP address	192.168.1.254	Must be greater than the Minimum IP address setting. All addresses between the minimum and maximum addresses are available for use in the extension.	Any valid IPv4 address that is in the same subnet and is higher than the configured minimum	The maximum value of the IP address that is used to adopt discovered SEL SDN switches. Once this value is reached, the topology management feature does not adopt any more switches.
SEL SDN Switch Template	Blank	N/A	N/A	Selection for the configuration node to use as the template for all discovered and adopted switches.

When the maximum switch or host count is set to Unlimited, the Auto Adoption session operates until a user terminates the session. The user can terminate the topology management session at any time. When you have designated the maximum number of switches and hosts to be adopted, autoadoption stops as soon as the maximum adopted nodes are reached for both switches and hosts. If the topology management session is terminated because the maximum number of nodes is reached or the operator manually terminates the session, any in-process adoption of nodes and links between nodes complete. When you conclude the Auto Adoption function, all in-band management logical connections between the flow controller, each switch in the network, and each host adopted by the current Auto Adoption session is checked if they are dual-connected for SEL Relay Failover mode. During the Auto Adoption session, any switches that have a synchronization event are automatically synchronized. The Learn and Lock extension provides status indicators, allowing the operator to monitor the progress of the Auto Adoption session. If the Learn and Lock session is canceled, the Auto Adoption process stops immediately, and in-band management replanning and SEL Relay Failover discovery is not performed.

Unicast Logical Connection Learning

Learn and Lock sessions have the option to enable unicast Logical Connection Learning. This is where the Learn and Lock extension learns unicast conversations that are being attempted between the hosts within the learning region and configures the logical connections to allow those conversations to take place. Only one Logical Connection Learning session is active at a time.

Learning regions define which devices the flow controller proposes new logical connections for when new conversations are discovered. When a Learn and Lock session is initiated with both Auto Adoption and Logical Connection Learning, the learning region includes any device that was adopted as part of the Auto Adoption session. When Auto Adoption is not enabled as part of the Learn and Lock session but Logical Connection Learning is, all unicast conversations discovered within the learning region are proposed for logical connection programming.

Logical connection programming has three modes to select from:

1. Autoaccept all
2. Autoaccept ARP and prompt for UDP, TCP, and ICMP
3. Prompt for everything

When autoaccept is selected, the SEL-5056 programs the logical connection as soon as the conversation is learned. When a mode is selected that has prompts, conversations are proposed to the user for acceptance before being programmed.

When the mode options that include user prompting are selected, the user has the option to accept or decline the proposed logical connection. Once accepted, the logical connection is immediately programmed. When the user declines a proposed logical connection, the learned conversation is remembered and the system does not propose this conversation again to the user even in follow-up Learn and Lock sessions. The user can delete the declined logical connections, which allows those conversations to be learned and proposed to the user again.

Figure F.2 shows the states of the conversations that are learned in a Learn & Lock session.

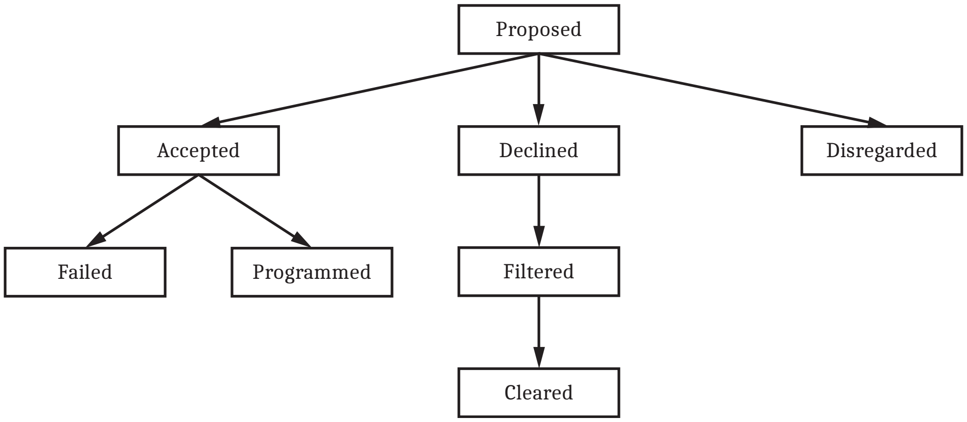


Figure F.2 Logical Connections States

Proposed logical connections are unicast conversations discovered by the Learn and Lock session that are waiting for the user to accept or decline. The proposed logical connections display what source, destination, and CST will be used to configure the communication circuit so the user can make an informed decision if they want this circuit programmed.

Accepted logical connections are communications circuits discovered during the Learn and Lock session that the user has approved to be programmed. When the Learn and Lock sessions are autoaccepted, all discovered logical connections immediately enter this stage, skipping the proposed stage.

Programmed logical connections are accepted learned communication circuits during a Learn and Lock session that successfully have been configured in the network. No user interaction is required; accepted logical connections transition to this stage once configured. This is the final stage of the circuit within the Learn and Lock extension, and any changes to this circuit is performed through the settings in the SEL-5056.

Failed logical connections are accepted learned communication circuits that have failed to be configured on the network. Monitor the error messages and logs generated by the SEL-5056 and the SEL SDN switches to investigate why the circuit was unable to be configured.

Declined logical connections are communications circuits discovered during the Learn and Lock session that the user has declined to program. This stage is only possible when Learn and Lock sessions are set to prompt for acceptance.

Filtered logical connections are filters put in place for the Learn and Lock extension to not propose or program this circuit on future Learn and Lock sessions. The Learn and Lock extension automatically transitions declined learned logical connections to this stage.

Cleared logical connections remove the filter for the logical connection, enabling the circuit to be learned and proposed or configured in future Learn and Lock sessions. This is a user action to clear the filter on a learned logical connection that previously has been declined.

Disregarded logical connections are proposed logical connections in a Learn and Lock session that the user neither accepted nor declined. Disregarded circuits are not programmed and not filtered so they are learned again in future Learn and Lock sessions.

Declined logical connections can be removed by navigating to the Connection Management page in the user interface and deleting the declined logical connections or selecting **Delete All Declined**. All modes conclude the session with a results report of all conversations that were learned during the session and their final state (either programmed or declined). From this report, the user can change the status of any conversations. Any logical connections in the proposed state when the Logical Connection Learning session has concluded are removed and not programmed. Communication learning is completed by either the user manually stopping the process or by the session timer expiration. You can set the user-configurable session timer to a duration between five minutes and one week.

When the Learn and Lock extension learns a new communication, the extension attempts to match it against existing communication service types (CSTs). When TCP communications are learned with a destination port less then 32768 and no existing CST match is available, the Learn and Lock extension makes a new bidirectional CST at priority 2000 with the destination TCP port included in the match criteria and all the OpenFlow prerequisites. When a new UDP communications are learned the same process is followed except a unidirectional circuit is programmed. The name for this logical connection is formatted as follows: LCL_TCP_BIDIR_<port>, where <port> is the destination port. If the learned port number is greater than or equal to 32768, the same process is followed unless the CST does not include the TCP or UDP port destination and the priority is set to 1900. This CST will include the name LCL_TCP_BIDIR_GENERIC.

Learned communication logical connections are not configured because of the following:

- The EtherType is not ARP or IPv4 with a TCP, UDP, or ICMP IP protocol
- The location of the destination address is unknown
- The user declined the proposed logical connection

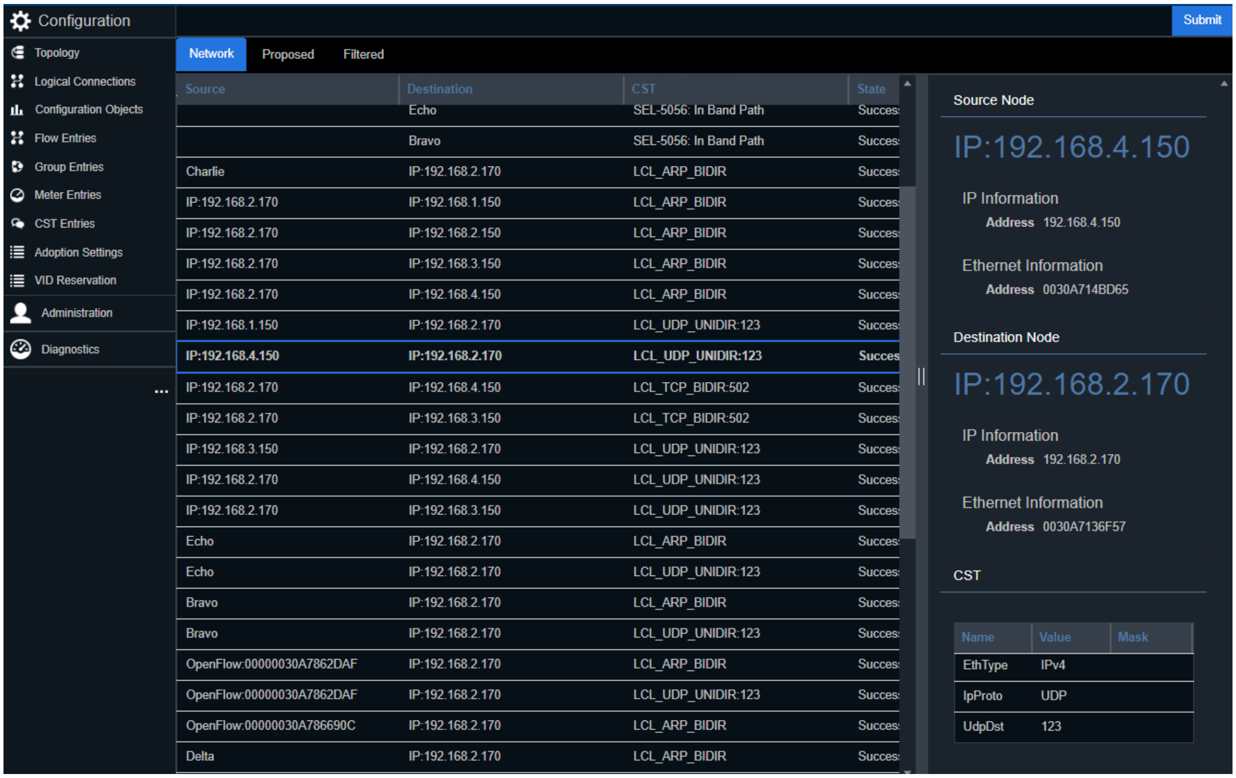
You can delete an entire communications Logical Connection Learning session. Use the session ID to delete the entire session and all configured logical connections.

Reporting

The Learn and Lock extension is the part of the SEL-5056 that logs all configuration and topology management actions in Windows Event Viewer and through Syslog. The topology management phase of the extension provides status indicators. The Logical Connection Learning displays all learned logical connections in the Connection Management page of the user interface, designating the source, destination, and CST used. The Learn and Lock extension also supports exporting the session to comma-separated value (CSV) format. This export is only available after the Learn and Lock session is completed. The SEL SDN switches have reporting in addition to the SEL-5056 logging. This report includes the following:

- The session ID
- The user who initiated the learning session
- The time stamps for when each stage of the Learn and Lock session started and stopped
- The list of network elements adopted
- The logical connections learned regardless of their state listed by source, destination, and CST as well as their current state

Learning sessions are exported through CSV-formatted reports. *Figure F.3* shows the Logical Connection page in the user interface. This is where the logical connections status is displayed and where you can move a learned logical connection between states.



Source	Destination	CST	State
	Echo	SEL-5056: In Band Path	Succes
	Bravo	SEL-5056: In Band Path	Succes
Charlie	IP:192.168.2.170	LCL_ARP_BIDIR	Succes
IP:192.168.2.170	IP:192.168.1.150	LCL_ARP_BIDIR	Succes
IP:192.168.2.170	IP:192.168.2.150	LCL_ARP_BIDIR	Succes
IP:192.168.2.170	IP:192.168.3.150	LCL_ARP_BIDIR	Succes
IP:192.168.2.170	IP:192.168.4.150	LCL_ARP_BIDIR	Succes
IP:192.168.1.150	IP:192.168.2.170	LCL_UDP_UNIDIR:123	Succes
IP:192.168.4.150	**IP:192.168.2.170**	**LCL_UDP_UNIDIR:123**	**Succes**
IP:192.168.2.170	IP:192.168.4.150	LCL_TCP_BIDIR:502	Succes
IP:192.168.2.170	IP:192.168.3.150	LCL_TCP_BIDIR:502	Succes
IP:192.168.3.150	IP:192.168.2.170	LCL_UDP_UNIDIR:123	Succes
IP:192.168.2.170	IP:192.168.4.150	LCL_UDP_UNIDIR:123	Succes
IP:192.168.2.170	IP:192.168.3.150	LCL_UDP_UNIDIR:123	Succes
Echo	IP:192.168.2.170	LCL_ARP_BIDIR	Succes
Echo	IP:192.168.2.170	LCL_UDP_UNIDIR:123	Succes
Bravo	IP:192.168.2.170	LCL_ARP_BIDIR	Succes
Bravo	IP:192.168.2.170	LCL_UDP_UNIDIR:123	Succes
OpenFlow:00000030A7862DAF	IP:192.168.2.170	LCL_ARP_BIDIR	Succes
OpenFlow:00000030A7862DAF	IP:192.168.2.170	LCL_UDP_UNIDIR:123	Succes
OpenFlow:00000030A786690C	IP:192.168.2.170	LCL_ARP_BIDIR	Succes
Delta	IP:192.168.2.170	LCL_ARP_BIDIR	Succes

Source Node

IP:192.168.4.150

IP Information
Address 192.168.4.150

Ethernet Information
Address 0030A714BD65

Destination Node

IP:192.168.2.170

IP Information
Address 192.168.2.170

Ethernet Information
Address 0030A7136F57

CST

Name	Value	Mask
EthType	IPv4	
IpProto	UDP	
UdpDst	123	

Figure F.3 Logical Connection Learning Screen

The Network tab on the logical connection page shows all the circuits provisioned on the network using logical connections. The logical connections displayed include any provisioned through the Learn and Lock extension and circuits manually provisioned. The Proposed tab shows all the learned logical connections in the current Learn and Lock session and waits for the user to accept or decline each circuit. The action menu is located at the top of the table, and there is also a filter option to see the logical connections in each state. The last tab is the Filtered tab, which shows all the learned logical connections on the current and previous Learn and Lock sessions that have been declined and now are filtered from being learned or programmed.

IP Multicasting

The Learn and Lock extension allows IP multicast learning to be enabled as part of the Logical Connection Learning feature. This is off by default, and if enabled, the Learn and Lock extension programs the IP multicast to be delivered to every host in the learning region. The CST created is formatted as <TCP or UDP>_<source ip>_<destination MAC>. The Logical Connection Learning checks to confirm the destination MAC starts with 01: and is a TCP or UDP IP protocol.

Saved Sessions

The Learn and Lock extension saves session data. To export saved session data, select the session of interest and export it to CSV. This export report has time-stamped log history about the session, devices that were adopted, and circuits that were provisioned.

Diagnostics

The Learn and Lock extension displays diagnostics in the message banner on the user interface and provides messages in toasts on the user interface to update the user what stage the Learn and Lock session is currently operating in and what actions are being taken. The Connection Management page displays all the logical connections learned and allows actions to be taken on each logical connection.

Reporting and Logging

The Learn and Lock extension uses the same logging services as the SEL-5056. Based on the SEL-5056 configuration, the Learn and Lock extension logs to the Windows event viewer and the configured Syslog servers.