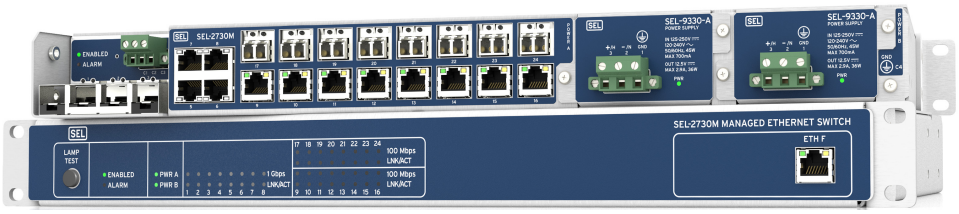
SEL-2730M
Managed Ethernet Switch

Instruction Manual



20250217

SEL SCHWEITZER ENGINEERING LABORATORIES

PM2730M-01

PM2730M-01

Table of Contents

This page intentionally left blank

List of Figures

List of Tables

Preface

Manual Overview

This instruction manual describes the functionality and use of the SEL-2730M Managed Ethernet Switch. It includes information necessary to install, configure, test, and operate this device.

An overview of the manual's layout and the topics that are addressed follows.

Preface. Describes the manual organization and conventions used to present information.

Section 1: Introduction and Specifications. Introduces SEL-2730M applications, connectivity, and use requirements. This section also lists specifications.

Section 2: Installation. Provides dimension drawings on the SEL-2730M and instructions for initializing the SEL-2730M.

Section 3: Managing Users. Explains how users are managed on the SEL-2730M.

Section 4: Job Done Examples. Provides three Job Done examples. These examples provide step-by-step configuration of the SEL-2730M for application in various SCADA and engineering access environments.

Section 5: Settings and Commands. Lists and describes all the SEL-2730M settings and commands.

Section 6: Testing and Troubleshooting. Provides guidelines for testing and troubleshooting the SEL-2730M.

Appendix A: Firmware and Manual Versions. Lists firmware and manual revisions.

Appendix B: Firmware Upgrade Instructions. Provides instructions to update the firmware in the SEL-2730M.

Appendix C: User-Based Accounts. Introduces user-based accounts and the benefits associated with using user-based accounts.

Appendix D: Lightweight Directory Access Protocol. Describes Lightweight Directory Access Protocol (LDAP) and its use in SEL products.

Appendix E: Syslog. Introduces the Syslog Protocol and its uses in SEL products.

Appendix F: Networking Fundamentals. Provides an overview of Windows Networking and network configuration.

Appendix G: Virtual Local Area Networks. Describes VLANs, their purpose, and how they should be used in control system environments.

Appendix H: Classless Inter-Domain Routing (CIDR). Explains CIDR and CIDR notation.

Appendix I: X.509. Explains the structure and use of X.509 certificates.

Appendix J: Accessing Port Information Through SNMP. Describes the mapping between ifIndex and SEL-2730M port number.

Appendix K: Cybersecurity Features. Describes the various features of the relay that impact cybersecurity.

Safety Information

⚠CAUTION
To ensure proper safety and operation, the equipment ratings, installation instructions, and operating instructions must be checked before commissioning or maintenance of the equipment. The integrity of any protective conductor connection must be checked before carrying out any other actions. It is the responsibility of the user to ensure that the equipment is installed, operated, and used for its intended function in the manner specified in this manual. If misused, any safety protection provided by the equipment may be impaired.

Dangers, Warnings, and Cautions

This manual uses three kinds of hazard statements, defined as follows:

⚠DANGER
Indicates a potentially hazardous situation that, if not avoided, **will** result in death or serious injury.

⚠WARNING
Indicates a potentially hazardous situation that, if not avoided, **could** result in death or serious injury.

⚠CAUTION
Indicates a potentially hazardous situation that, if not avoided, **may** result in minor or moderate injury or equipment damage.

Safety Symbols

The following symbols are often marked on SEL products.

	**⚠CAUTION** Refer to accompanying documents.	**⚠ATTENTION** Se reporter à la documentation.
	Earth (ground)	Terre
	Protective earth (ground)	Terre de protection
	Direct current	Courant continu

	Alternating current	Courant alternatif
	Both direct and alternating current	Courant continu et alternatif
	Instruction manual	Manuel d’instructions

Safety Marks

The following statements apply to this device.

Table 1 General Safety Marks

⚠CAUTION There is danger of explosion if the battery is incorrectly replaced. Replace only with Panasonic BR-1632A/DBN or equivalent recommended by manufacturer. See Owner's Manual for safety instructions. The battery used in this device may present a fire or chemical burn hazard if mistreated. Do not recharge, disassemble, heat above 100°C or incinerate. Dispose of used batteries according to the manufacturer’s instructions. Keep battery out of reach of children.	**⚠CAUTION** Une pile remplacée incorrectement pose des risques d’explosion. Remplacez seulement avec un Panasonic BR-1632A/DBN ou un produit équivalent recommandé par le fabricant. Voir le guide d’utilisateur pour les instructions de sécurité. La pile utilisée dans cet appareil peut présenter un risque d’incendie ou de brûlure chimique si vous en faites mauvais usage. Ne pas recharger, démonter, chauffer à plus de 100°C ou incinérer. Éliminez les vieilles piles suivant les instructions du fabricant. Gardez la pile hors de la portée des enfants.
Disconnect both power supplies before servicing.	Débranchez les deux blocs d’alimentation avant l’entretien.

Table 2 Other Safety Marks

⚠DANGER Disconnect or de-energize all external connections before opening this device. Contact with hazardous voltages and currents inside this device can cause electrical shock resulting in injury or death.	**⚠DANGER** Débrancher tous les raccordements externes avant d’ouvrir cet appareil. Tout contact avec des tensions ou courants internes à l’appareil peut causer un choc électrique pouvant entraîner des blessures ou la mort.
⚠DANGER Contact with instrument terminals can cause electrical shock that can result in injury or death.	**⚠DANGER** Tout contact avec les bornes de l’appareil peut causer un choc électrique pouvant entraîner des blessures ou la mort.
⚠WARNING Use of this equipment in a manner other than specified in this manual can impair operator safety safeguards provided by this equipment.	**⚠WARNING** L’utilisation de cet appareil suivant des procédures différentes de celles indiquées dans ce manuel peut désarmer les dispositifs de protection d’opérateur normalement actifs sur cet équipement.
⚠WARNING Have only qualified personnel service this equipment. If you are not qualified to service this equipment, you can injure yourself or others, or cause equipment damage.	**⚠WARNING** Seules des personnes qualifiées peuvent travailler sur cet appareil. Si vous n’êtes pas qualifiés pour ce travail, vous pourriez vous blesser avec d’autres personnes ou endommager l’équipement.
⚠WARNING Do not look into the fiber ports/connectors.	**⚠WARNING** Ne pas regarder vers les ports ou connecteurs de fibres optiques.
⚠WARNING Do not look into the end of an optical cable connected to an optical output.	**⚠WARNING** Ne pas regarder vers l’extrémité d’un câble optique raccordé à une sortie optique.

⚠WARNING Do not perform any procedures or adjustments that this instruction manual does not describe.	**⚠WARNING** Ne pas appliquer une procédure ou un ajustement qui n'est pas décrit explicitement dans ce manuel d'instruction.
⚠WARNING During installation, maintenance, or testing of the optical ports, use only test equipment qualified for Class 1 laser products.	**⚠WARNING** Durant l'installation, la maintenance ou le test des ports optiques, utilisez exclusivement des équipements de test homologués comme produits de type laser de Classe 1.
⚠WARNING Incorporated components, such as LEDs and transceivers are not user serviceable. Return units to SEL for repair or replacement.	**⚠WARNING** Les composants internes tels que les leds (diodes électroluminescentes) et émetteurs-récepteurs ne peuvent pas être entretenus par l'usager. Retourner les unités à SEL pour réparation ou remplacement.
⚠CAUTION Equipment components are sensitive to electrostatic discharge (ESD). Undetectable permanent damage can result if you do not use proper ESD procedures. Ground yourself, your work surface, and this equipment before removing any cover from this equipment. If your facility is not equipped to work with these components, contact SEL about returning this device and related SEL equipment for service.	**⚠CAUTION** Les composants de cet équipement sont sensibles aux décharges électrostatiques (DES). Des dommages permanents non-décelables peuvent résulter de l'absence de précautions contre les DES. Raccordez-vous correctement à la terre, ainsi que la surface de travail et l'appareil avant d'en retirer un panneau. Si vous n'êtes pas équipés pour travailler avec ce type de composants, contacter SEL afin de retourner l'appareil pour un service en usine.
⚠CAUTION In order to avoid losing system logs on a factory-default reset, configure the SEL-2730M to forward Syslog messages.	**⚠CAUTION** Pour éviter de perdre les enregistrements du système sur un redémarrage défini par défaut, configurer le SEL-2730M pour envoyer les messages de l'enregistreur du système (“Syslog”).

General Information

Examples

This instruction manual uses several example illustrations and instructions to explain how to effectively operate the SEL-2730M Managed Ethernet Switch. These examples are for demonstration purposes only; the firmware identification information or settings values these examples include may not necessarily match those in the present version of your SEL-2730M.

Trademarks

All brand or product names appearing in this document are the trademark or registered trademark of their respective holders. No SEL trademarks may be used without written permission.

SEL trademarks appearing in this manual are shown in the following table.

ACSELERATOR QuickSet®	Job Done®

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, Inc.
One Schweitzer Drive
Pullman, WA 99163-5603 U.S.A.

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

This page intentionally left blank

SECTION 1

Introduction and Specifications

Introduction

This section includes the following information about the SEL-2730M Managed Ethernet Switch.

Product Overview

The SEL-2730M Managed Ethernet Switch is designed for the harsh environments commonly found in the energy and utility industries. The SEL-2730M supports communications infrastructures built for engineering access, supervisory control and data acquisition (SCADA), and real-time data communication, and offers the same reliability found in SEL protective relays.

Product Features

- **Reliable.** Increase availability with the SEL-2730M, which is designed, built, and tested to function in harsh environments such as substations. Optional hot-swappable, dual power supplies allow connectivity to primary and backup power sources.
- **Flexible.** Maximize flexibility by using SEL-2730M ordering options to meet different network configurations. Order the SEL-2730M with Ethernet ports in combinations of copper, single-mode fiber, and multimode fiber. Add even more flexibility by using the four small form-factor pluggable (SFP) modules to change port configurations when network designs change.
- **Ease-of-Use.** Simplify configuration and maintenance with a secure web interface that allows convenient setup and management. Configure settings offline by using ACSELERATOR QuickSet SEL-5030 Software or through an exported settings file that can be imported later on the switch.
- **VLANs.** Segregate traffic and improve network organization and performance. Take advantage of IEEE 802.1Q-2005 VLANs to separate IEC 61850 GOOSE messages from other traffic with as many as 4094 VLANs.

- **Traffic Prioritization.** Support critical substation messaging by using IEEE 802.1Q-2005 VLAN and Priority Tagging Class of Service (CoS) traffic prioritization with four service levels and VLAN-based classification.
- **Rapid Spanning Tree Protocol (RSTP).** Use IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) to speed network recovery and convergence after a topology change caused by a link or device failure.
- **Bridge Protocol Data Unit (BPDU) Guard.** Improve network robustness by enabling BPDU Guard to disable a port when unexpected BPDUs are received.
- **Rate Limiting.** Prevent network storms by limiting the amount of broadcast, multicast, and/or unicast traffic on the network.
- **Multicast MAC Filtering.** Filter multicast traffic to reduce network load on end devices.
- **Port-Based MAC Security.** Use port-based MAC security to limit network access to authorized devices.
- **Time Synchronization.** Synchronize time by using network time protocol (NTP). Time-align events and user activity across your system.
- **Syslog.** Log events for speedy alerts, consistency, compatibility, and centralized collection. Use the switch to forward Syslog system and security logs to as many as three central servers.
- **MAC Address Table.** Download a comma-separated value table of MAC addresses. Use the table for troubleshooting and locating devices on the network.
- **Dynamic Host Configuration Protocol (DHCP).** Easily connect a laptop computer during initial setup by using settings that enable the front-panel 10/100BASE-T Ethernet port to function as a DHCP server.
- **Security and Monitoring.** Increase security by taking advantage of SNMPv3 and HTTPS features. SNMPv3 provides secure network management and is interoperable with existing network management systems (NMS). An HTTPS web interface provides secure and intuitive switch management. Map system and security events to configurable alarm contact behavior for alarming through an external system, such as an existing SCADA network.
- **Port Mirroring.** Monitor ingress and egress traffic for viewing network statistics and performing troubleshooting.
- **Port Monitoring.** Monitor port health for link flap and frame check sequence cyclic redundancy check (CRC) errors.
- **Port Configuration.** Use per-port configuration of settings such as speed, duplex, and auto-negotiation, which facilitates connection with other devices.
- **User-Based Accounts.** Provide user accountability and separate authorization levels for configuration and maintenance. Use LDAP or RADIUS with two-factor authentication for centralized user authentication.

Connections, Reset Button, and LED Indicators

Front Panel

Figure 1.1 shows the front panel of the SEL-2730M. The front panel includes all of the activity and status LED indicators of the device. There are link status and activity indicators for each of the 24 rear Ethernet ports. The front (local management) Ethernet port has link and activity indicators built into the port itself. In addition, there are status indications for the unit as a whole, as well as for the power supply and optional backup power supply.

NOTE
SEL-2730M fiber ports are 100 Mbps only; they will not operate at 10 Mbps.

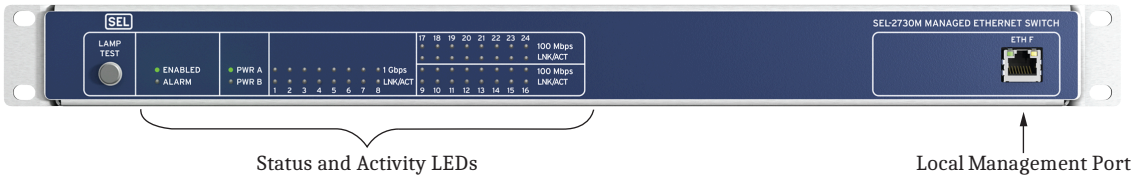


Figure 1.1 Front-Panel View

Status Indicators

Figure 1.2 shows the layout of the status indicators on the front of the SEL-2730M. After the device has turned on and is in a normal operating state, a red LED indicates a non-optimal condition needing operator attention.

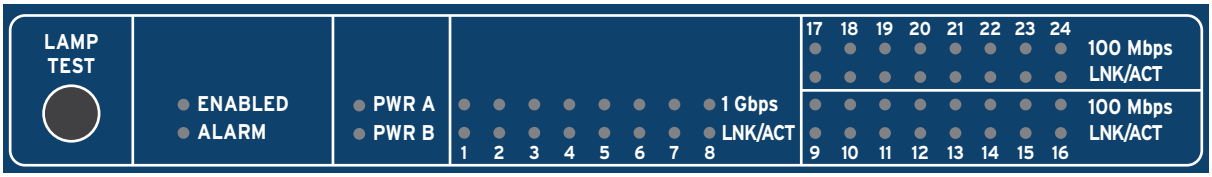


Figure 1.2 Close-Up of Front-Panel Status Indicators

Lamp Test

The **LAMP TEST** button illuminates all front-panel indicators when pressed.

General Status Indicators

The **ENABLED** indicator is green when the unit is "up" (has passed self-tests and is operational). This indicator is not illuminated during startup and if the unit fails self-test.

The **ALARM** indicator is not illuminated unless the unit asserts an alarm. Flashing red indicates a minor alarm, while solid red indicates a major alarm.

Power Supply Status Indicators

The **PWR A**/**PWR B** indicators will be green if the power supply is installed and healthy. If the unit detects a fault problem, the indicator will be red. If a power supply is not installed, the corresponding indicator will not be illuminated.

Ethernet Status Indicators

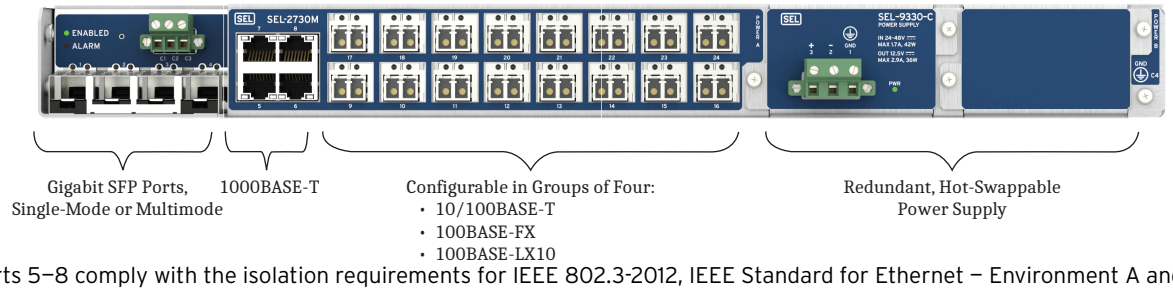
Each of the rear-panel Ethernet ports has a pair of corresponding LED indicators on the front panel: a yellow indicator above a green one. *Table 1.1* shows how to interpret the states of these LED indicators. Note that the connector for each port on the rear panel has built-in status indicators. As with the front-panel indicators, these include one green and one yellow LED, and these indicate link status similarly. This simplifies the detection of cabling errors when inserting and removing Ethernet cables from the rear of the unit.

Table 1.1 Ethernet Status Indicators

LED State	Ethernet
Solid Green	Link up
Blinking Green	Port activity
Solid Yellow	Full-Speed Link
Blinking Yellow	Collision[a]
Extinguished Yellow	Low-Speed Link

[a] Collision indication is not supported on the four 1000BASE-T ports.

Rear Panel



Ports 5–8 comply with the isolation requirements for IEEE 802.3-2012, IEEE Standard for Ethernet – Environment A and should be connected to devices that share the same main power supply phase.

Ports 17–20 can be configured with two 10/100BASE-T and two 100BASE-FX ports.

Figure 1.3 Rear-Panel View

The base-model SEL-2730M has four Gigabit Ethernet copper ports and sixteen 10/100 Mbps copper Ethernet ports, built as four-port modules. You can order each of the 10/100 Mbps copper port modules as single- or multimode fiber-optic ports to meet the unique requirements of your network. You can also add as many as 4 ports that use small form-factor pluggable (SFP) modules for a total of 24 ports. These SFP ports can be any combination of fiber-optic Gigabit Ethernet ports and 10/100/1000 copper ports.

NOTE

Fiber Ethernet devices connected to the fiber ports must match both the speed and sub-type (FX) of the SEL-2730M port.

Ethernet copper ports support Auto MDI/MDX and auto-negotiation for speed and duplex values. Gigabit fiber-optic SFP ports support auto-negotiation of speed, but only support the Gigabit speed. 100 Mbps fiber-optic ports support auto-negotiation of speed but only support the 100 Mbps speed.

NOTE
SEL-2730M fiber ports are 100 Mbps only; they will not operate at 10 Mbps.

Four Small Form-Factor Pluggable (SFP) Ports

Ports 1–4 are compatible with SEL copper, single mode, or multimode SFP fiber-optic modules. These modules are digitally signed and must be ordered from SEL. A list of SFP modules that the SEL-2730M supports is available on the SEL website at selinc.com.

Four Gigabit Ethernet Ports

Ports 5–8 support 10/100/1000 Mbps copper Ethernet.

Table 1.2 Gigabit Ethernet Port Pinout

Pin	Description
1	A+
2	A-
3	B+
4	C+
5	C–
6	B–
7	D+
8	D–

Sixteen Fast Ethernet Ports

You can order ports 9–24 in combinations of four-port groups of either copper or fiber. *Table 1.3* shows the pinout for the copper Ethernet option.

Table 1.3 10/100 Mbps Ethernet Port Pinout

Pin	Description
1	A+
2	A–
3	B+
4	N/C
5	N/C
6	B–
7	N/C
8	N/C

Redundant, Hot-Swappable Power Supplies

Optional redundant power supplies provide failover protection. Connect a separate power source to each power supply. If one source fails, the other continues to keep the switch operational. The power supply has an estimated mean time between failures (MTBF) of 3000 years. Power supply inputs are isolated from ground and polarity protected.

SEL-9330-A High-Voltage Power Supply (120–240 Vac, 125–250 Vdc)

Table 1.4 High-Voltage Power Supply Connections

Pin	Description
1	GND
2	–/N
3	+/H

SEL-9330-C Low-Voltage Power Supply (24–48 Vdc)

Table 1.5 Low-Voltage Power Supply Connections

Pin	Description
1	GND
2	–
3	+

The **POWER** terminal on the rear of the power supplies must connect to a source within the rated range of the SEL-2730M. The **POWER** terminals are isolated from the chassis ground. Use 1.5–2.5 mm (16–14 AWG) wire to connect to the **POWER** terminals.

Alarm Contact Output

One Form C output mechanical relay contact is provided on the rear panel for alarming. The alarm contact operates for one second to indicate a minor alarm. It indicates a major alarm by continuing to operate until removal of the failure source is manually acknowledged through the management interface.

Table 1.6 Alarm Contact Pinout

Pin	Description
C1	Normally Open
C2	Common
C3	Normally Closed

Table 1.7 Alarm Contact Ratings

Max Voltage	250 Vdc
Contact Protection	270 Vdc, 23 J MOV protected

Max Current	6 A
Pickup time	≤8 ms typical
Dropout time	≤8 ms typical

Software System Requirements

The device is primarily managed through the internal HTTPS server. This server requires a web browser capable of HTTPS communication. The official supported browsers are Google Chrome, Mozilla Firefox, and Microsoft Edge.

General Safety and Care Information

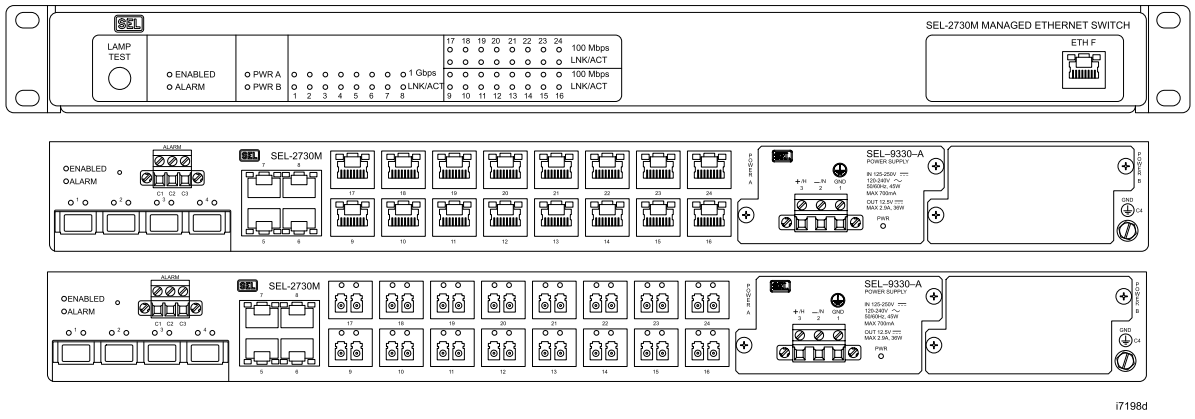
General Safety Notes

- The SEL-2730M is designed for restricted access locations. Access should be limited to qualified service personnel.
- The SEL-2730M should neither be installed nor operated in a condition this manual does not specify.

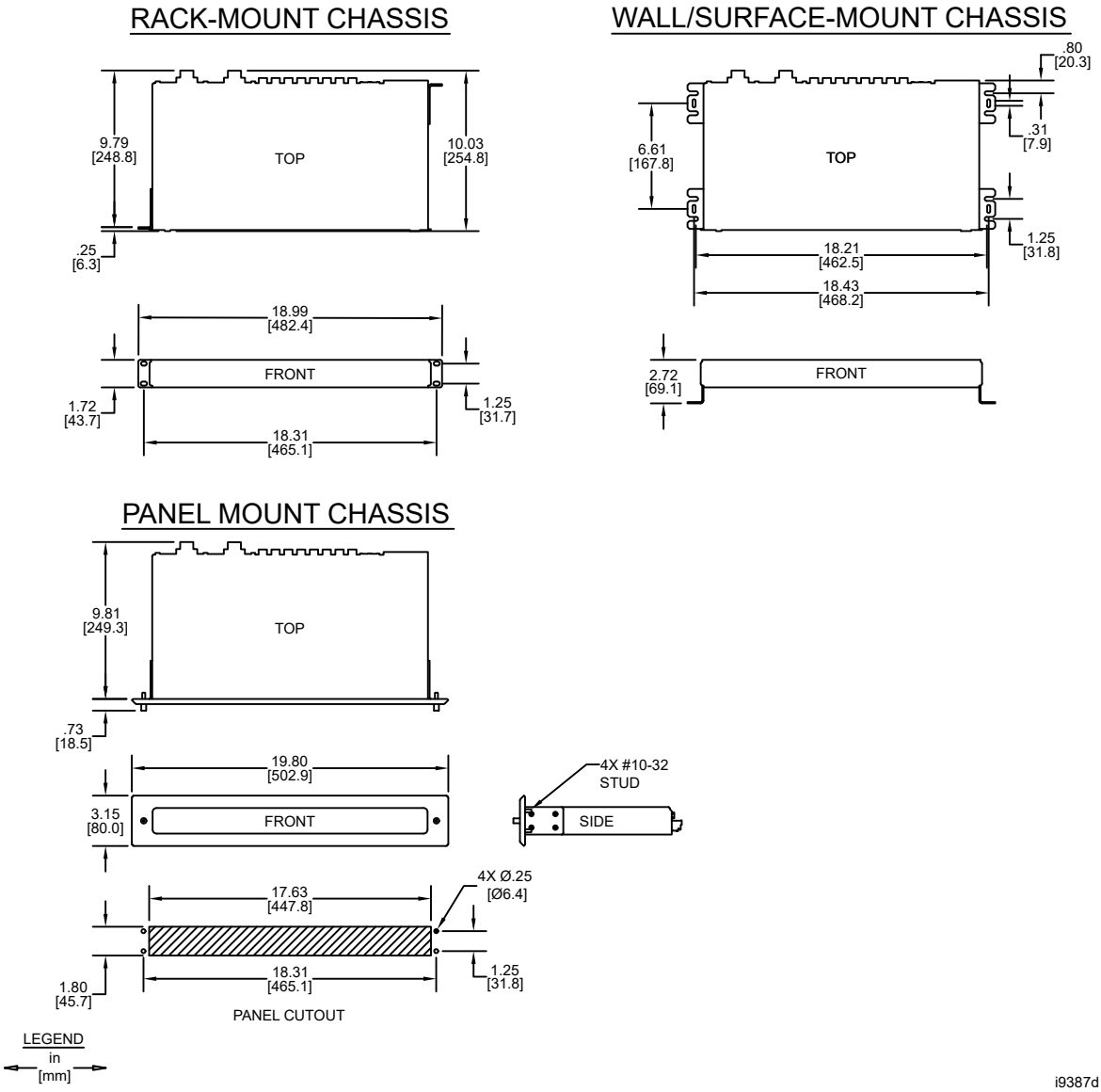
Cleaning Instructions

- The device should be de-energized (by removing the power connection to both the power and alarm connection) before cleaning.
- The case can be wiped down with a damp cloth. Solvent-based cleaners should not be used on plastic parts or labels.

Front- and Rear-Panel Diagrams



Dimension Drawing



Note: The SEL-2730M supports front, 19-inch rack-mount, panel-mount, and wall-mount installations.

Note: When using 915900533 wall-mount brackets, use appropriate fasteners for the wall location to which the unit is being mounted and install the device in a restricted area with wires down.

Note: When using the wall-mount brackets, insert one mounting screw in each bracket cutout, for a total of four mounting screws per switch.

Note: For torque recommendations, refer to Specifications on page 9.

Mounting Options

Mounting Instructions

The SEL-2730M comes with reversible mounting ears to support surface mount and front- and rear-panel installations. When mounting multiple SEL-2730M in the same rack, leave a one-unit space between each device to ensure proper heat dissipation.

Warranty

The SEL-2730M meets or exceeds the IEEE 1613 Class 1, IEC 61850-3, and IEC 60255 industry standards for communications devices in electrical substations for vibration, electrical surges, fast transients, extreme temperatures, and electrostatic discharge.

SEL manufactures the SEL-2730M through the use of the same high standards as those for SEL protective relays and backs it with the same 10-year worldwide warranty.

Specifications

Compliance

Designed and manufactured under an ISO 9001 certified quality management system

UL Listed to U.S. and Canadian safety standards
(File E220228; NRAQ/NRAQ7) (rack- and panel-mount configurations)

UKCA Mark

CE Mark

RCM Mark

General

Switching Properties

Switching Method:	Store and Forward
Switching Latency:	<35 µs
Switch Fabric Throughput:	19.2 Gbps
Priority Queues:	4
Maximum VLANs:	4094
MAC Learning Architecture:	Shared VLAN Learning (SVL)
VLAN ID Range:	1–4094
MAC Address Table Size:	8192 addresses

Warranty

10 years

Network Management

HTTPS Web User Interface

SNMPv1/SNMPv2c/SNMPv3

ACSELERATOR QuickSet SEL-5030 Software

Settings Import/Export

Third-Party Network Management Systems (NMS)

User-Based Accounts

Maximum Local Accounts:	256
Password Length:	8–72 characters
Password Set:	All printable ASCII characters
User Roles:	Administrator, Engineer, User Manager, Monitor

Syslog

Storage for 60,000 local Syslog messages.

Support for three remote Syslog destinations.

Processing and Memory

Processor Speed:	313 MHz
Memory:	512 MB
Storage:	512 MB

Communications Ports

Ethernet Ports

Ports:	24 rear, 1 front
Data Rate:	10, 100, or 1000 Mbps
Front Connector:	RJ45 Female
Rear Connectors:	RJ45 female or LC fiber (single-mode or multimode)
Standard:	IEEE 802.3-2012 IEEE 802.3-2012 excluding 10 Gbps and above IEEE 802.3-2008/Cor 1 IEEE 802.3bd IEEE 802.3bf

Fiber-Optic Ports

Multimode Option (to 2 km)

Maximum TX Power:	–14 dBm
Minimum TX Power:	–19 dBm
RX Sensitivity:	–30 dBm
System Gain:	11 dB
Source:	LED
Wavelength:	1300 nm
Connector Type:	LC (IEC 61754-20)

Single-Mode Option (to 15 km)

Maximum TX Power:	–8 dBm
Minimum TX Power:	–15 dBm
RX Sensitivity:	–25 dBm
System Gain:	10 dB
Source:	Laser
Wavelength:	1310 nm
Connector Type:	LC (IEC 61754-20)

Supported Small Form-Factor Pluggable (SFP) Fiber-Optic Ports

- 1000BASE-SX (300 m)
- 1000BASE-LX (10 km)
- 1000BASE-LX (20 km)
- 1000BASE-LX (30 km)
- 1000BASE-LX (40 km)
- 1000BASE-XD (50 km)
- 1000BASE-ZX (80 km)

Supported Small Form-Factor Pluggable (SFP) Copper Ports

10/100/1000BASE-T

For the most up-to-date list of qualified SFP modules, please contact the SEL application engineer in your region.

Digital Output

Rated Operational Voltage:	24–250 Vdc
Continuous Carry:	2 A

Power Supply

125–250 Volt Power Supply

Rated Supply Voltage:	125–250 Vdc; 120–240 Vac, 50/60 Hz
Input Voltage Range:	88–300 Vdc or 85–264 Vac
Maximum Burden:	AC: <60 VA DC: <45 W
DC Ripple:	<15% rated voltage
Peak Inrush:	8 A
Insulation:	3100 Vdc
Power Factor:	>75%
Isolated from Chassis Ground:	Yes
Input Voltage Interruptions:	50 ms @ 125 Vac/Vdc 100 ms @ 250 Vac/Vdc

24–48 Volt Power Supply

Rated Supply Voltage:	24–48 Vdc (polarized)
Input Voltage Range:	19.2–60.0 Vdc
Maximum Burden:	<42 W
DC Ripple:	<15% rated voltage
Peak Inrush:	18 A
Insulation:	3100 Vdc
Isolated from Chassis Ground:	Yes
Input Voltage Interruptions:	50 ms @ 48 Vdc 10 ms @ 24 Vdc

Recommended External Overcurrent Protection

Breaker Type:	Standard
Breaker Rating:	15 A at 250 Vdc
Current Breaking Capacity:	10 kA
Grounded Neutral Systems:	Device in series with the HOT or energized conductor
DC and Isolated Systems:	Device in series with both conductors

Fuse Ratings

Power Supply Fuse

SEL-9330-A:	2.5 A, 250 Vdc/300 Vac Time-lag T, 250 Vac/1500 A break rating
SEL-9330-C:	4.0 A, 150 Vdc Time-lag T, 250 Vac/ 1500 A break rating

Note: Fuses are not user-serviceable.

Alarm Contact Output

Per IEC 255-0-20:1974, Using Simplified Method of Assessment

Output Type:	Relay, Form C, break-before-make
Power Supply Burden:	<1 W maximum
Mechanical Life:	2000000 operations
Operational Voltage:	250 Vac/Vdc
Make:	30 A at 250 Vdc
Carry:	6 A continuous at 70°C
1 s Rating:	50 A
MOV Protection:	270 Vac, 23 J
Insulation Voltage:	300 Vdc
Pickup Time:	<8 ms
Dropout Time:	<8 ms

Breaking Capacity (10,000 Operations):

24 V	0.75 A	L/R = 40 ms
48 V	0.50 A	L/R = 40 ms
125 V	0.30 A	L/R = 40 ms
250 V	0.20 A	L/R = 40 ms

Cyclic Capacity (2.5 Cycle/Second):

24 V	0.75 A	L/R = 40 ms
48 V	0.50 A	L/R = 40 ms
125 V	0.30 A	L/R = 40 ms
250 V	0.20 A	L/R = 40 ms

Terminal Connections

Compression Screw Terminals

Power Wiring

Insulation:	300 V minimum
Size:	12–18 AWG
Tightening Torque	
Minimum:	0.6 Nm (5 in-lb)
Maximum:	0.8 Nm (7 in-lb)
Crimp Ferrule Recommended	

Alarm Wiring

Insulation:	300 V minimum
Size:	16–24 AWG
Tightening Torque	
Minimum:	0.5 Nm (4 in-lb)
Maximum:	0.6 Nm (5 in-lb)
Crimp Ferrule Recommended	

Mounting Ear Tightening Torque

Minimum:	2 Nm (18 in-lb)
Maximum:	4 Nm (35 in-lb)

Grounding Screw

Ground Wiring

Insulation:	300 V minimum
Size:	12 AWG
Length:	<3 m

Tightening Torque

Minimum:	0.9 Nm (8 in-lb)
Maximum:	1.4 Nm (12 in-lb)

Ring Terminal Recommended

Dimensions

1U Rack Mount

Height:	43.7 mm (1.72 in)
Depth:	232.1 mm (9.14 in)
Width:	482.5 mm (19 in)

1U Panel Mount

Height:	80.0 mm (3.15 in)
Depth:	261.9 mm (10.31 in)
Width:	502.9 mm (19.80 in)

Weight

1.96 kg (4.3 lb)

Environmental

Operating Temperature

–40° to +85°C (–40° to +185°F)

Relative Humidity

0% to 95% non-condensing

Altitude

2000 m

Atmospheric Pressure

80–110 kPa

Operating Environment

Pollution Degree:	2
Overvoltage Category:	II
Insulation Class:	I

Enclosure Protection

IEC 60529:2001 + A2:2013
Severity Level: IP20

Green Product

Compliant with the European Union's RoHS directive

Type Tests

Communication Product Testing

IEEE 1613-2009, Class 1*	KEMA certified
IEC 61850-3:2013	KEMA certified
IEC 61850-90-4	KEMA certified

* With SEL-C627-R or equivalent cables.

Electromagnetic Compatibility Emissions

Generic Emissions:	EN 60255-26:2013 EN 61850-3:2014 47 CFR Part 15 CISPR 11:2009 + A1:2010 CISPR 22:2008 EN 55011:2009 + A1:2010 EN 55022:2010 + AC:2011 EN 55023:2012 + AC:2013 Severity Level: Class A Canada ICES-001 (A) / NMB-001 (A)

Electromagnetic Compatibility Immunity

Conducted RF Immunity:	IEC 60255-26:2013 IEC 61000-4-6:2008 Severity Level: 10 Vrms
Electrostatic Discharge Immunity:	IEC 60255-26:2013 IEC 61000-4-2:2008 IEEE C37.90.3-2001 Severity Level: 2, 4, 8 kV contact; 4, 8, 15 kV air
Fast Transient/Burst Immunity:	IEC 60255-26:2013 IEC 61000-4-4:2011 Severity Level: Zone A
Magnetic Field Immunity:	IEC 60255-26:2013 IEC 61000-4-8:2009 Severity Level: 1000 A/m for 3 seconds, 100 A/m for 1 minute IEC 61000-4-9:2001 Severity Level: 1000 A/m IEC 61000-4-10:2001 Severity Level: 100 A/m
Power Supply Ripple:	IEC 60255-26:2013 IEC 61000-4-17:2008
Power Supply Dips and Interruptions:	IEC 60255-26:2013 IEC 61000-4-11:2004 IEC 61000-4-29:2000
Power Supply Gradual Shutdown and Startup:	IEC 60255-26:2013
Power Supply Discharge Capacitors:	IEC 60255-27:2013
Power Supply Reverse Polarity and Slow Ramp:	IEC 60255-27:2013
Radiated RF Immunity:	IEC 60255-26:2013 Severity Level: 10 V/m unmodulated 80 MHz–1 GHz, 1.4 GHz–2.7 GHz IEEE C37.90.2-2004 Severity Level: 20 V/m 80% AM, 0.5 s keyed, 80 MHz–1 GHz

Surge Immunity:
IEC 60255-26:2013
IEC 61000-4-5:2005
Severity Level: Zone A

Surge Withstand Capability:
IEC 60255-26:2013
Severity Level: 2.5 kV peak common mode, 1.0 kV peak differential mode
IEC 61000-4-18:2006
IEEE C37.90.1-2002
Severity Level: 2.5 kV oscillatory, 4 kV fast transient waveform

Environmental

Cold:
IEC 60255-27:2013
IEC 60068-2-1:2007
Severity Level: 16 hours at –40°C

Dry Heat:
IEC 60255-27:2013
IEC 60068-2-2:2007
Severity Level: 16 hours at +85°C

Damp Heat, Cyclic:
IEC 60255-27:2013
IEC 60068-2-30:2005
Severity Level: 25°C to 55°C
Relative Humidity: 93% to 95%
Duration: 6 cycles, 1 cycle/day

Damp Heat, Steady State:
IEC 60255-27:2013
IEC 60068-2-78:2002
Severity Level: 40°C
Relative Humidity: 93%
Duration: 4 days

Vibration (Front-Panel Mount Only):
IEC 60255-27:2013
IEC 60255-21-1:1988
Severity Level: Class 1 endurance, Class 2 response
IEC 60255-21-2:1988
Severity Level: Class 1 - shock withstand, bump, and Class 2 - shock response
IEC 60255-21-3:1993
Severity Level: Class 2 (quake response)

Safety

Dielectric Strength:
IEC 60255-27:2013
IEEE C37.90-2005
3600 Vdc on power supply and alarm contact; 2250 Vdc on Ethernet ports Type tested for 1 minute
IEEE 802.3-2012
2250 Vdc on electrical Ethernet ports Type tested for 1 minute
Ports 5–8 comply with Environment A requirements between ports
Ports 9–24 comply with Environment B requirements between ports

Impulse:
IEC 60255-27:2013
IEEE C37.90-2005
Severity Level:
Common Mode
5 kV power supply, alarm contact
2.4 kV Ethernet ports
Common Mode, Port to Port
5 kV power supply, alarm contact
Zero-Rated, Ethernet ports

Protective Bonding Resistance:
IEC 60255-27:2013
IEEE C37.90-2005

This page intentionally left blank

SECTION 2

Installation

Introduction

This section includes the following information:

Connecting to the Device

The device includes an HTTPS web server which provides configuration and management functions for use with an internet browser.

For the initial connection to a device, you will need to have the following:

- ➤ A computer with a wired Ethernet port
- ➤ An uncommissioned SEL-2730M
- ➤ One RJ45 Ethernet cable
- ➤ CA-signed X.509 certificate (optional, but recommended)

Physical Network

Connect the device to your computer as shown in *Figure 2.1*. Using a standard RJ45 Ethernet cable, connect the Ethernet port of your computer to the front Ethernet port (**ETH F**) of the device. The web management interface of an uncommissioned SEL-2730M can only be reached through the front Ethernet port. After commissioning, an additional IP interface can be configured. See *Network Settings on page 78* for information on enabling an additional IP interface.

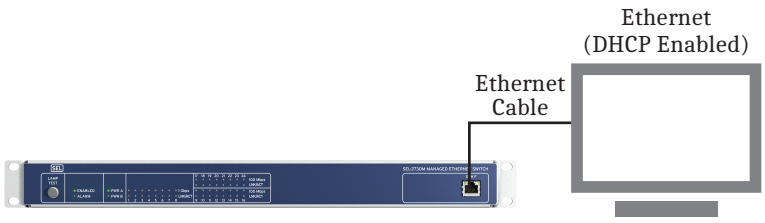


Figure 2.1 Commissioning Network

The default URL for the web server via the front port is https://192.168.1.2. However, if your computer is configured as a DHCP client, the SEL-2730M Captive Port feature sends the necessary network configuration information from the SEL-2730M to place your computer in the same subnet as the

SEL-2730M. This will direct any entered URL to the SEL-2730M. More information about the Captive Port feature can be found in *Network Settings on page 78*. If you prefer to use a static IP address, you can set these parameters yourself as described in *Configuring a Static IP Address in Microsoft Windows Networking on page 26*.

To set the network connection of your computer to be automatically configured, follow these steps:

Step 1. Open the Microsoft Windows Network Connections Control Panel applet. Do this by typing **ncpa.cpl** in the Windows Run dialog box, as shown in *Figure 2.2*. Selecting **OK** will open the **Network Connections** window, which contains a list of the network devices available on your computer.

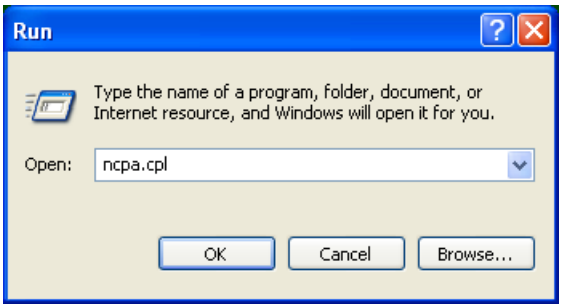


Figure 2.2 Open Network Connections With Run Command

Step 2. Right-click on the connection you will be using to communicate with the device and select the **Properties** option to show the connection properties window (see *Figure 2.3*). This connection may be labeled as **Local Area Connection**.

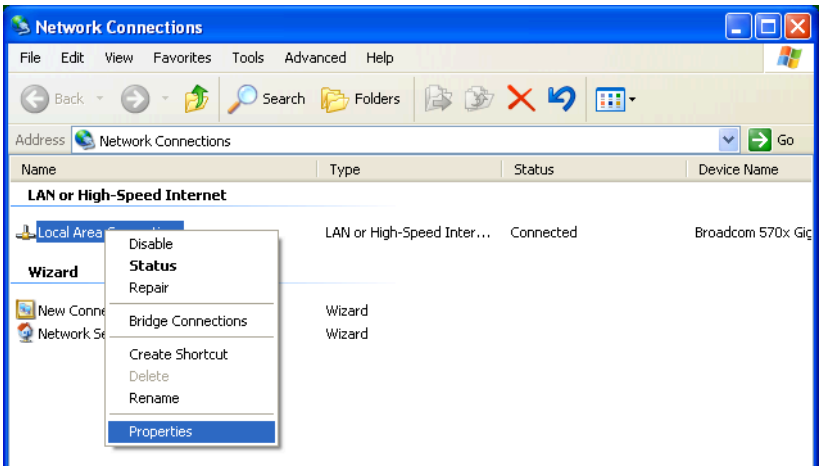


Figure 2.3 Open Connection Properties

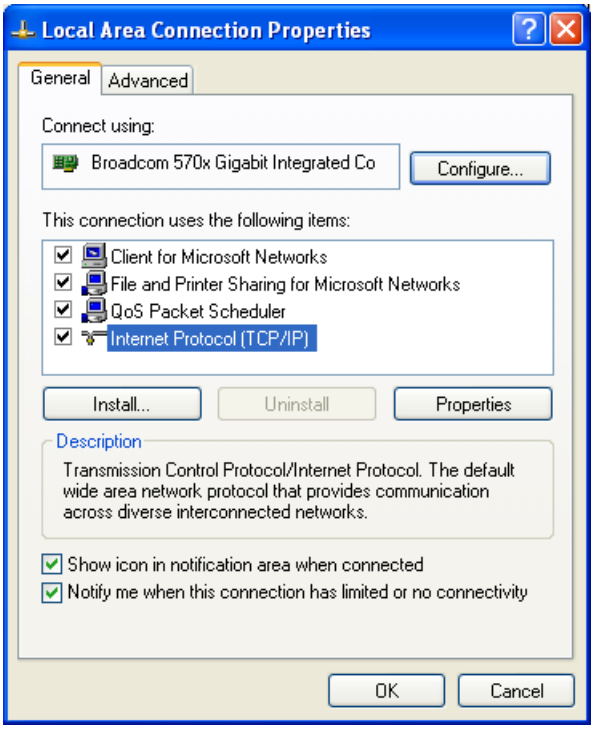


Figure 2.4 Local Area Connection Properties

Step 3. Select the **Internet Protocol (TCP/IP)** entry from the **This connection uses the following items** list (this entry is usually located last in the list). Select the **Properties** button to show the **Internet Protocol (TCP/IP) Properties** window (see *Figure 2.5*).

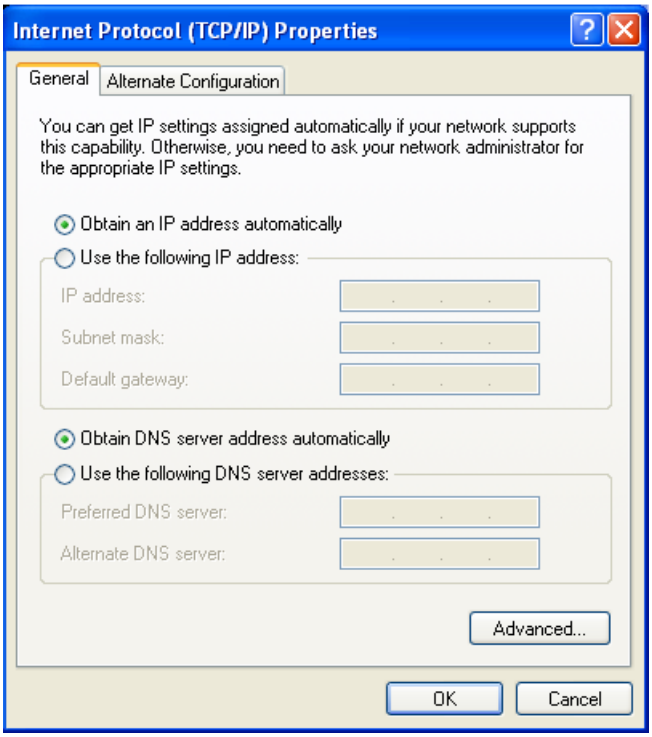


Figure 2.5 Configuring Automatic Network Configuration

Step 4. Select **Obtain an IP address automatically**. This is the usual setting for computers on a company network.

Step 5. Select **Obtain DNS server address automatically**. This is the usual setting for computers on a company network.

Step 6. Select the **OK** button.

Commissioning the Device

Configure the network connection of your computer as described in *Physical Network on page 17*. Using a standard RJ45 Ethernet cable, connect the Ethernet port of your computer to the front port **ETH F** of the SEL-2730M. Wait for the network connection to be configured, and then open your web browser and navigate to any URL (e.g., selinc.com)—the SEL-2730M will handle resolving the URL and connecting you to its web management interface.

NOTE
You may receive a certificate error from your browser. The message is dependent on the browser you are using. This error appears because the default certificate is a self-signed certificate and not signed by a trusted certificate authority (CA). You will need to create a certificate exception to access the device login page. Your browser will provide instructions for doing this. For information on creating an X.509 certificate to eliminate this error, see Section 5: Settings and Commands.

Step 1. In your browser's address bar, enter **https://192.168.1.2**. This will open the device Commissioning Page.

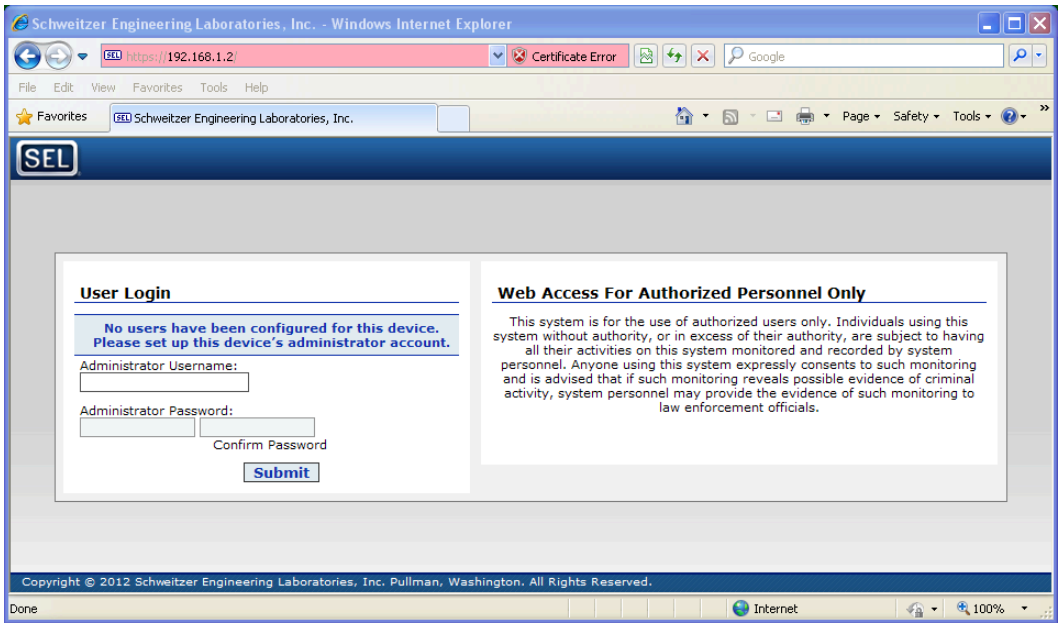


Figure 2.6 Device Commissioning Page

Step 2. Enter the account information for the first administrative user. This requires both a username and a password. The password must be entered twice to ensure that it is correctly typed, because the password characters are hidden.

Step 3. Select the **Submit** button to complete commissioning. When the page reloads, you will be able to log in as the administrative user to set up accounts and configure the system. *Navigating the User Interface on page 21* provides a general description of the web interface.

Navigating the User Interface

The device has an HTTPS interface to enable easy device configuration. This HTTPS interface can be accessed by opening your web browser and navigating to the device management address. By default this address is https://192.168.1.2.

When you log in to the device, you are presented with the Dashboard as shown in *Figure 2.7*. The Dashboard gives a quick overview of the status of the device. The features of the Dashboard are explained in greater detail later in this section.

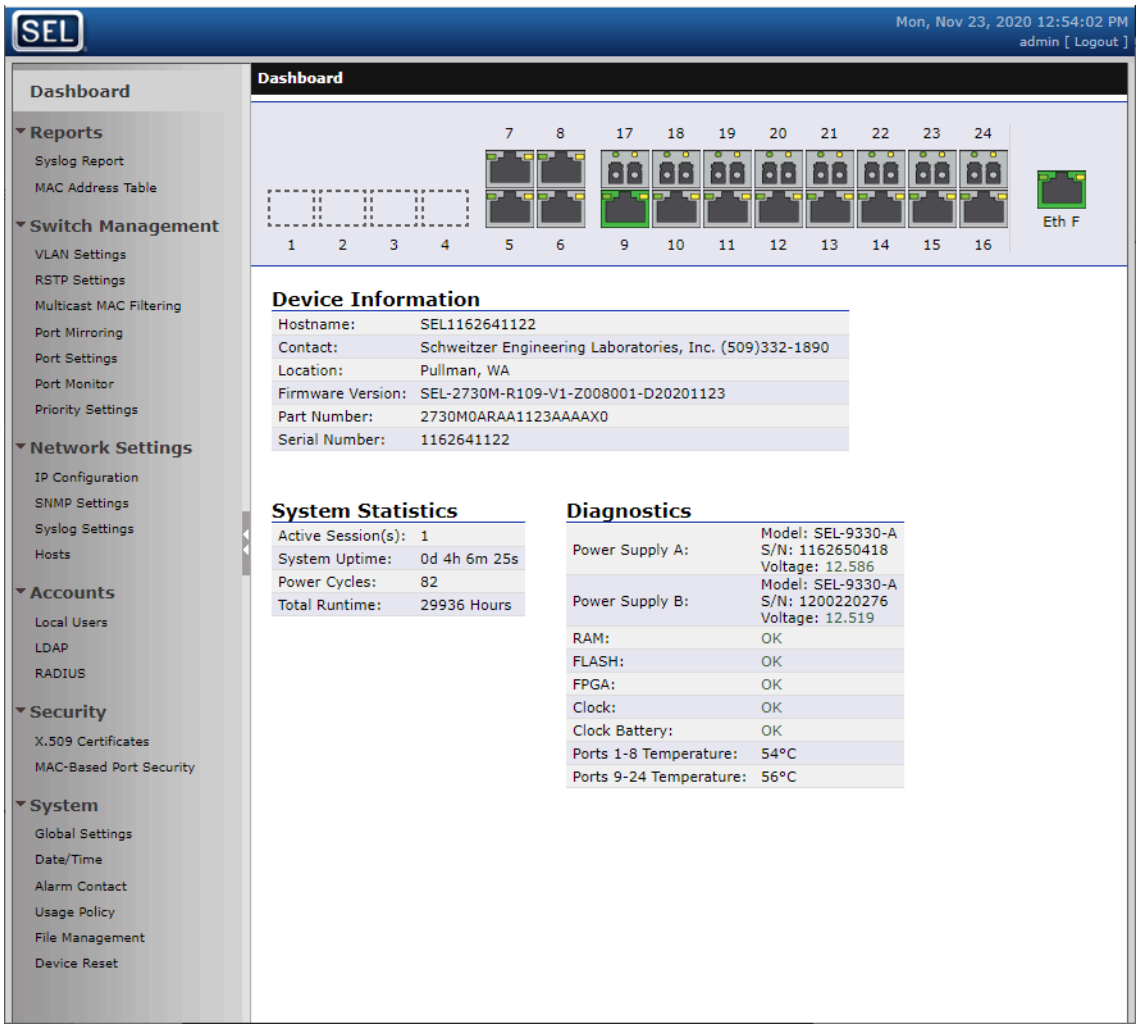


Figure 2.7 Device Dashboard and Navigation Menu

The far-left frame of the device web interface is the navigation panel. Selecting any link on this panel will take you to the associated page that includes all the settings and configurations for that part of the system. The navigation panel is always present on the web interface. One of the first tasks might be to create user accounts for personnel who will be configuring and maintaining the device. Selecting the **Local Users** link in the navigation panel will open the Accounts page as shown in *Figure 2.8*.

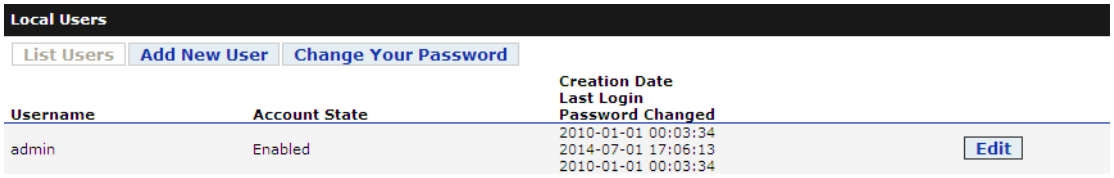


Figure 2.8 Local Users

The Local Users page shown in *Figure 2.8* shows the main panel of the web interface. This sample shows the single administrative user created when the device was configured. On this page, we can also see the status of each user account and details about the users.

The Local Users page has an **Add New User** button above the table. There is also an **Edit** button for each user in the table. Each user will also have a **Delete** button, except for that user when there is only one administrative user left. The last administrative user cannot be deleted.

Selecting the **Add New User** button will display the user form (see *Figure 2.9*) to allow changing the role, description, password, or enabled condition of a user. Selecting the **Edit** button will show the same form, without the username box.

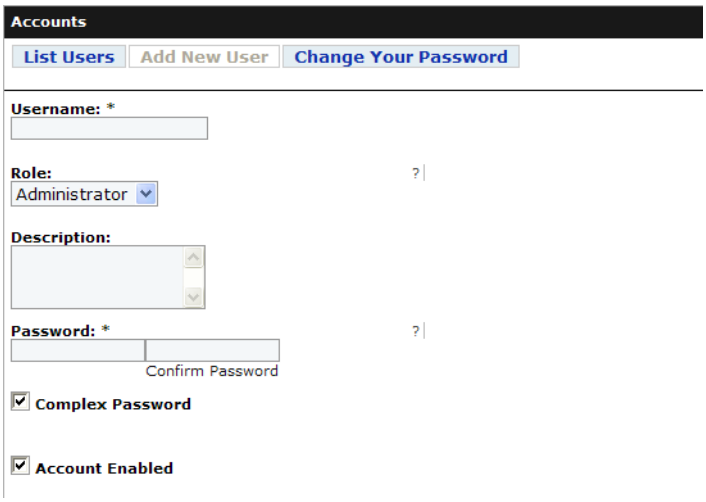


Figure 2.9 Adding a New User

Installing a New Web Certificate

The SEL-2730M comes configured with a self-signed X.509 certificate. SEL recommends installing a CA-signed X.509 certificate on the device. Perform the following instructions to install a new web certificate on the SEL-2730M.

Step 1. Navigate to the **X.509 Certificate** page.

Step 2. Select **Import** (at the top of the page).

Step 3. Add a **Certificate Alias** and a **Password** (if required).

Step 4. Select **Browse** and select the new web certificate.

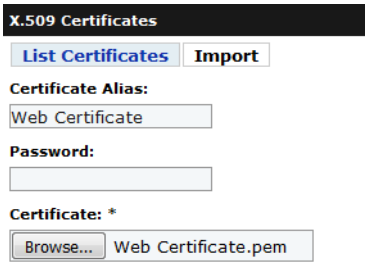


Figure 2.10 Uploading a New X.509 Certificate

Step 5. Select **Submit**. If the certificate is valid, it will appear in the list of certificates with an **Activate** button.

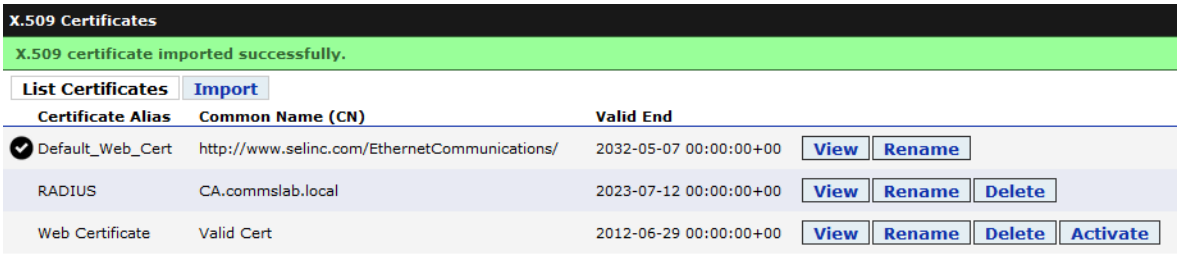


Figure 2.11 Successful Upload of a New X.509 Certificate

Step 6. Select **Activate** for the new certificate and then **Yes** to continue. The SEL-2730M begins refreshing the web interface; when the **Activating certificate** button turns green, select it to return to the web interface.

You can confirm that the X.509 certificate is presently active by navigating to the **X.509 Certificate** page.

There should now be a check mark (✔) to the left of the alias of the certificate that you activated. You may now remove the self-signed certificate by selecting the **Delete** button for the Default_Web_Cert certificate.

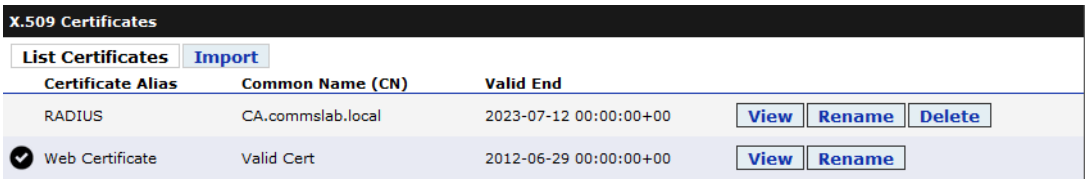


Figure 2.12 New Certificate Is Activated

Device Dashboard

The device Dashboard is the page that is displayed when a user logs in to the device. The Dashboard provides a quick overview of the state of the device. To access the Dashboard from another device webpage, select the **Dashboard** link on the left navigation panel.

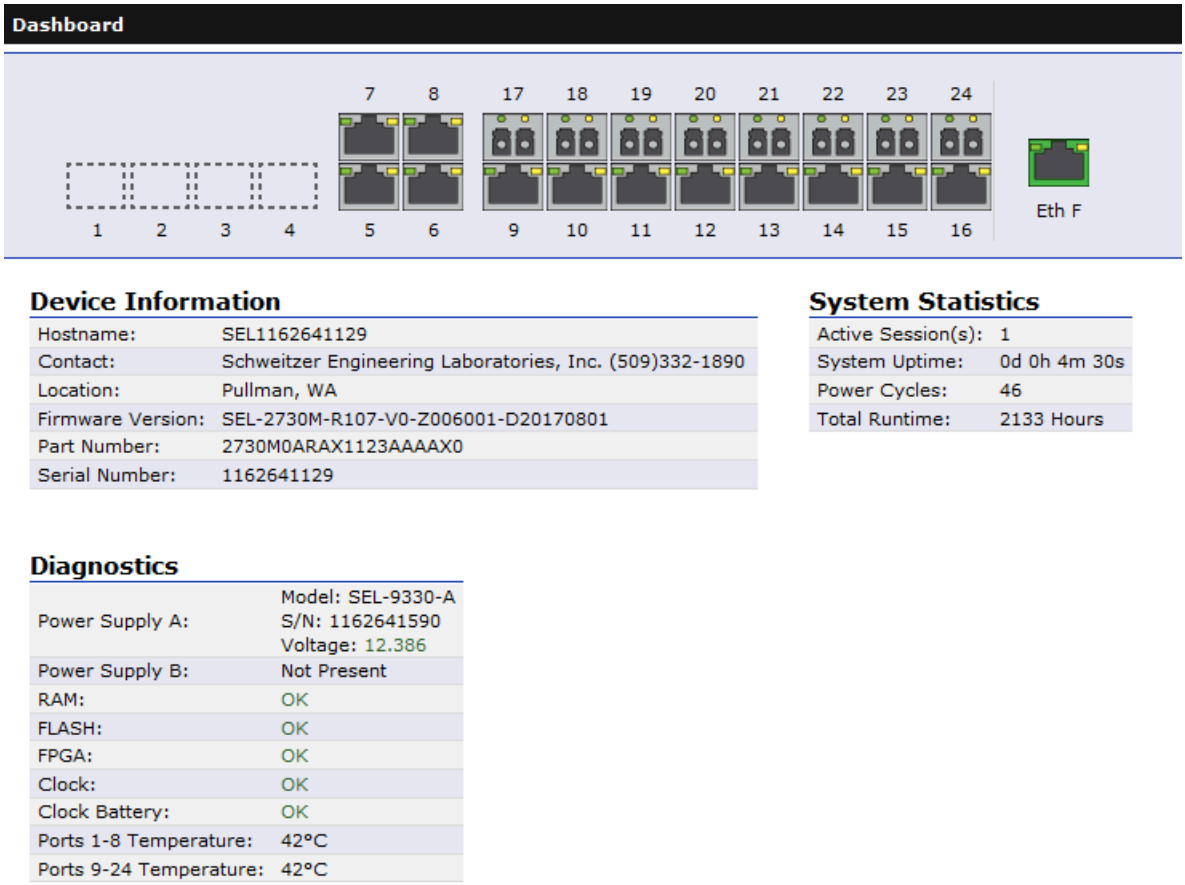


Figure 2.13 Device Dashboard

The system status and statistics information on the **Dashboard** page is updated periodically. The dashboard is broken into the following four categories.

- Network Interfaces
- Device Information
- System Statistics
- Diagnostics

Network Interfaces

The Network Interfaces section of the Dashboard contains icons representing each physical Ethernet network interface on the device. You can mouse over any of the network interface port icons to see the alias and current status information of the port. Selecting one of these icons will add a status area to the Dashboard and add a line to it containing the statistics for that interface. More information about network interface configuration can be found in *Section 5: Settings and Commands*.

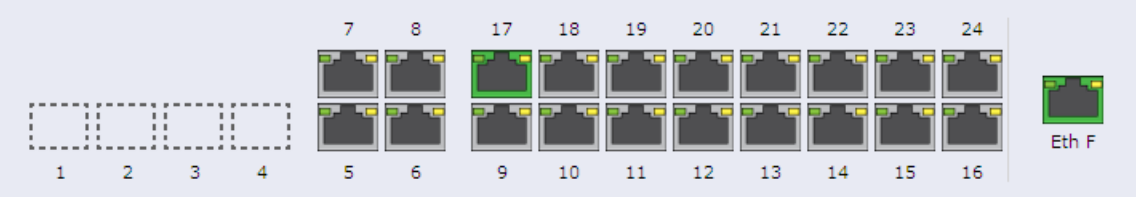


Figure 2.14 Network Interfaces

The network interface icons are color-coded to indicate the configuration state of that interface. The interface icon colors and their meanings can be found in *Table 2.1*.

Table 2.1 Network Interface Icon Colors

Interface Icon	Status
(Green)	Enabled (link up)
(Gray)	Enabled (link down)
(Dark Gray)	Disabled (not configured)

Device Information

This section of the Dashboard provides version information, including part number, serial number, and the firmware identification string. This information can be useful when technical support or firmware upgrades are necessary.

Device Information

Hostname:	SEL1162641129
Contact:	Schweitzer Engineering Laboratories, Inc. (509)332-1890
Location:	Pullman, WA
Firmware Version:	SEL-2730M-R107-V0-Z006001-D20170801
Part Number:	2730M0ARAX1123AAAAX0
Serial Number:	1162641129

Figure 2.15 Version Information

System Statistics

The System Statistics area (see *Figure 2.16*) of the Dashboard provides some basic statistics of device operations. This information can quickly help determine whether the device firmware is operating properly.

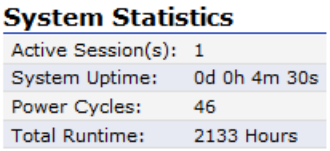


Figure 2.16 System Statistics

Table 2.2 explains the meaning of each of these statistics.

Table 2.2 System Statistics

Statistic	Meaning
Active Session(s)	Number of users currently logged on to the management web interface
System Uptime	How long the unit has been running since last turned on or restarted
Power Cycles	Number of times power has been cycled; increases by one every time the unit is powered up
Total Runtime	Total number of hours the unit has been powered up

Diagnostics

The Diagnostics section (see *Figure 2.17*) of the Dashboard provides simple status indications for the basic hardware systems of the SEL-2730M. This information can quickly help determine the health of the device hardware and that it is operating properly.

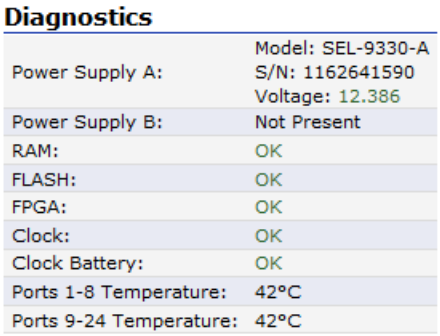


Figure 2.17 Diagnostics

Configuring a Static IP Address in Microsoft Windows Networking

To configure the SEL-2730M by using a static IP address, you will need to configure your computer to communicate on the 192.168.1.0/24 subnet. For a description of the Classless Inter-Domain Routing (CIDR) notation, see *Appendix H: Classless Inter-Domain Routing (CIDR)*.

NOTE

The instructions in this section are provided in the event you decide to use a static IP address to access the device instead of configuring your computer for DHCP.

Step 1. Start the Microsoft Windows Command Terminal.

1. Open the **Run** command (from the Start menu).
2. Type **cmd** in the text box.
3. Select **OK**.

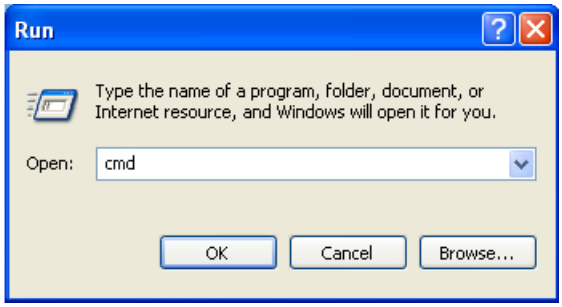


Figure 2.18 Open Terminal With Run Command

Step 2. In the command window, type **ipconfig <Enter>**. This will display the IP address and subnet mask that your Ethernet connection is configured for. The IP address must match 192.168.1.1 and the subnet mask must match 255.255.255.0. If these values are correct, you are ready to begin commissioning the device.

Step 3. If you need to configure your computer to communicate on the 192.168.1.0/24 subnet, open Microsoft Windows Network Connections.

1. Type **ncpa.cpl** in the **Run** command.
2. Select **OK**.

   The Network Connections window will open. This window contains a list of the network devices available on your computer.

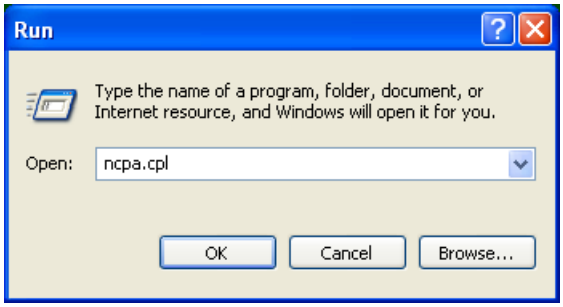


Figure 2.19 Open Network Connections With Run Command

Step 4. Right-click on the connection you will be using to communicate with the device, and select **Properties**. This connection may be labeled as **Local Area Connection**.

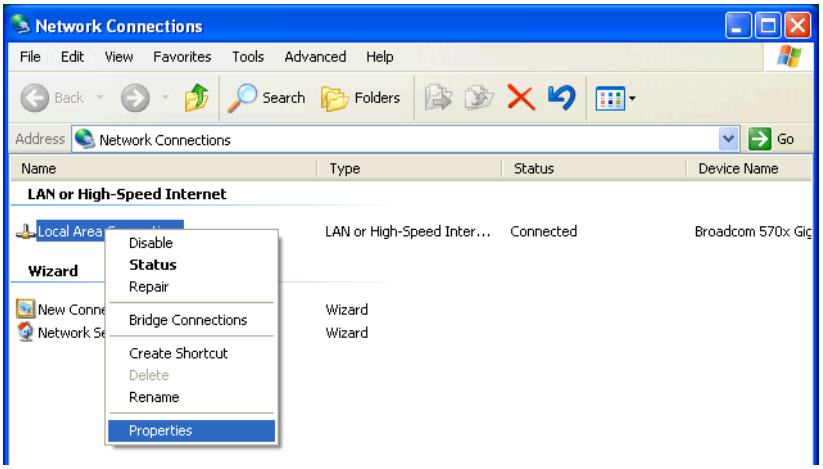


Figure 2.20 Open Connection Properties

Step 5. Select the **Internet Protocol (TCP/IP)** entry from the **This connection uses the following items** list (usually located last in the list). Select the **Properties** button.

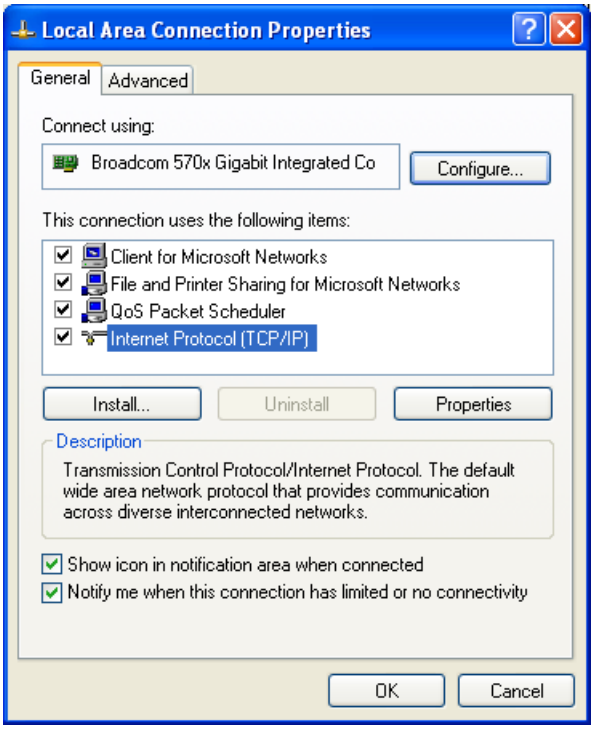


Figure 2.21 Local Area Connection Properties

Step 6. Select **Use the following IP address**. Enter **192.168.1.1** as the IP address and **255.255.255.0** as the Subnet mask, as shown in *Figure 2.22*. Select the **OK** button.

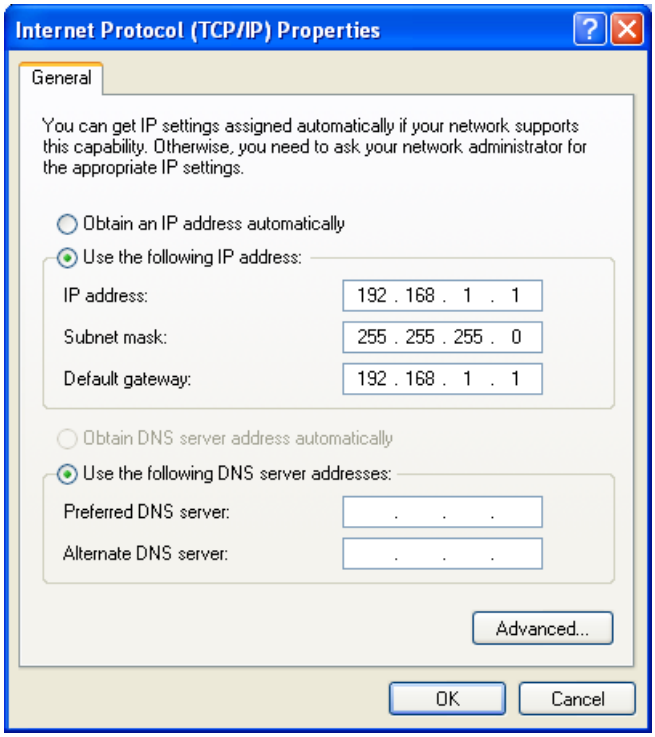


Figure 2.22 Internet Protocol (TCP/IP) Properties

Step 7. Select the **OK** button in the **Local Area Connection Properties** dialog box. The new settings will take effect once this is done.

Battery Change Instructions

The battery in the SEL-2730M is used to maintain power to the real-time clock so that the switch retains the time through power cycles. The battery is rated to last more than 10 years, but if you need to change the battery, use the following steps.

Step 1. Disconnect power from the SEL-2730M.

Step 2. Remove the SEL-2730M from the panel or rack.

Step 3. Ground yourself, your work station, and the SEL-2730M to the same ground.

Step 4. Unscrew the 11 top screws and remove the top cover.

The battery is located on the main board, near the power supply.

Step 5. Replace the battery.

Step 6. Reassemble the device and return it to service.

To test that the battery replacement was successful, apply power to the unit and log in to the web management interface. Check for major alarms indicating battery failure. If there are no alarms, navigate to the **Date and Time** webpage and reset the time on the device.

This page intentionally left blank

SECTION 3

Managing Users

Introduction

This section includes the following:

User-Based Accounts

The SEL-2730M has user-based access control to provide for greater authentication, authorization, and accountability. Individuals responsible for configuring, monitoring, or maintaining the device will have their own unique user accounts. User-based access controls are organized to answer, "Who did what and when?" and allow flexibility for detailed auditing. This structure also eases the burden of password management for the operators by only requiring users to remember their own personal passwords. This eliminates the need for each operator to remember a new password every time an employee leaves or no longer needs access as required in a global account structure.

Permissions of the device are organized into roles, and access is granted through role-based access controls (RBACs). The device has four roles: Administrator, Engineer, User Manager, and Monitor. User account privileges are based on the group (i.e., role) in which the user is a member. A brief overview of each role is provided below.

- Users with the Administrator role have full access to the device.
- Users with the Engineer role have access to most settings and information on the device. The main exception to this is user account management.
- Users with the User Manager role have access to manage users on the device. Access to other settings is restricted.
- Users with the Monitor role have read-only access to most of the device settings.

Adding a Local User

The device supports as many as 256 unique local user accounts. Use the following steps to create a new user account.

Step 1. Log in to the device with an account that is a member of either the Administrator or the User Manager group. The account you created during commissioning is one such account.

Step 2. Select the **Local Users** link from the navigation menu of the web management interface. This link will open the User Accounts page.

Step 3. Select **Add New User**.

Step 4. Enter the **Username**, **Role**, and **Password** of the new user. The password must be entered twice to confirm that it has been entered correctly.

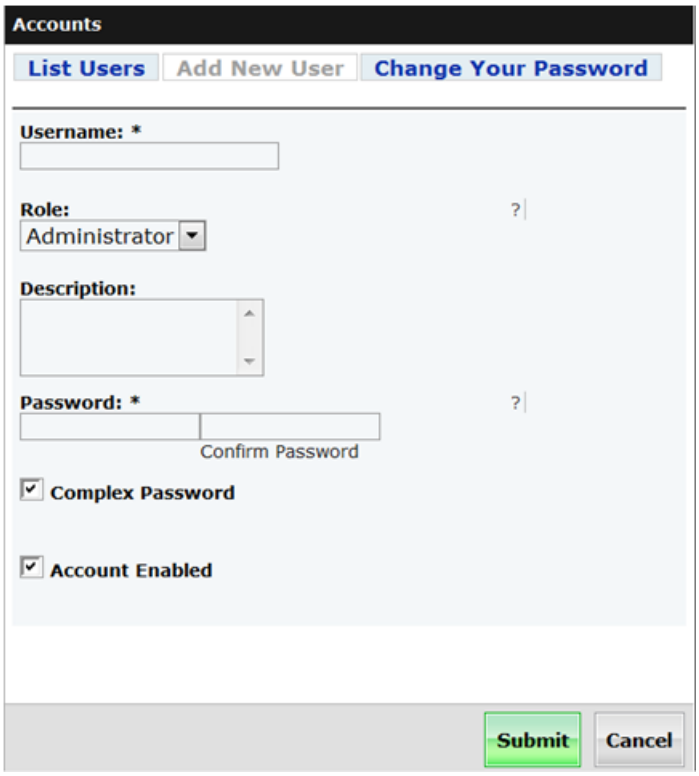


Figure 3.1 Add New User Form

Step 5. Select the **Submit** button. This will add the new user to the device.

Editing a Local User and Resetting a Password

The device provides an Administrator or User Manager user with the ability to edit account information for existing accounts. With this function, users can reset forgotten passwords, reassign group membership, and enable or disable an account. Perform the following steps to reset an account's password.

Step 1. Log in to the device with an account that is a member of the Administrator or User Manager group. The account you created during commissioning is one such account.

Step 2. Select the **Local Users** link from the navigation menu of the web management interface. This link will open the User Accounts page.

Step 3. Select the **Edit** button associated with the account that you want to edit. This step will open the Edit User form.

Step 4. To change the user's password, enter the new password, confirm the new password, and select the **Submit** button.

Removing a Local User

In the case where an employee leaves the company, you should remove the employee's account to prevent security breaches. The device allows for the easy removal of user accounts. Perform the following steps to remove an account.

Step 1. Log in to the device with an Administrator or User Manager account. The account you created during commissioning is one such account.

Step 2. Select the **Local Users** link from the navigation menu of the web management interface. This link will open the User Accounts page.

Step 3. Select the **Delete** button associated with the account that you want to remove.

Step 4. Verify that the user to be deleted is the correct user.

Step 5. Once verified, select **Yes**. If this person is not the correct user, select **No** to go back to the User Accounts page.

Enabling or Disabling a Local User

If an employee takes an extended leave of absence or has a temporary change in duties, the employee's account should be disabled to prevent unauthorized access to the device. Disabling the account will maintain the account information while preventing unauthorized access to the system during the absence. The account can be reactivated when the employee resumes normal duties. Perform the following steps to enable or disable a user's account.

Step 1. Log in to the device with an account that is a member of the Administrator or User Manager group. The account you created during commissioning is one such account.

Step 2. Select the **Local Users** link from the navigation menu of the web management interface. This link will open the User Accounts page.

Step 3. Select the **Edit** button associated with the account that you want to edit. This step will open the Edit User form.

Step 4. If an account is currently enabled, uncheck the **Account Enabled** button to disable the account. To enable an account that has been disabled, check **Account Enabled**.

Changing a User Password

Many organizations have policies requiring employees to change their system passwords at regular intervals. To aid with these policies, users on the device can change their own passwords. Perform the following steps to change your password.

Step 1. Log in to the device.

Step 2. Select the **Local Users** link from the navigation menu of the web management interface.

Users of the Monitor or Engineer group will only see a **Change Your Password** button. Users of the User Manager or Administrators group will see all user accounts of the device, as well as the same **Change Your Password** button.

Step 3. Select the **Change Your Password** button. This step will bring up the form to change your password. Enter your old password, new password, and select the **Submit** button to change your password.

Centralized User Accounts

The SEL-2730M supports two types of centralized authentication protocols: LDAP and RADIUS. Only one may be active at a time. When a user attempts to log in to the SEL-2730M, the SEL-2730M authenticates the account using the following order:

Local Users	OR	Local Users
LDAP (if enabled)		RADIUS (if enabled)

Each of the central authentication services can configure primary and backup servers. When using LDAP or RADIUS settings, the SEL-2730M attempts to contact the primary server first; if the response times out, the SEL-2730M either tries to contact the backup server. If any other error or rejection occurs, the SEL-2730M rejects the login attempt and stops processing the login.

Both protocols use the **Hosts** page to resolve Hostname settings into IP addresses and the **X.509** page for X.509 certificate management for EAP protocols. See *Edit Hosts on page 81* and *X.509 Certificates on page 88* for instructions on using those two pages.

LDAP

Lightweight Directory Access Protocol (LDAP) is used by many IT departments to manage the users and devices on their corporate networks.

LDAP is included in the SEL-2730M to provide a mechanism for centralized user management. With LDAP, users can be managed at a central server. When a user who does not have a local account requests access to the device, the device will consult the central directory to find their account and verify that they are authorized to access the unit, see *Figure 3.2*.

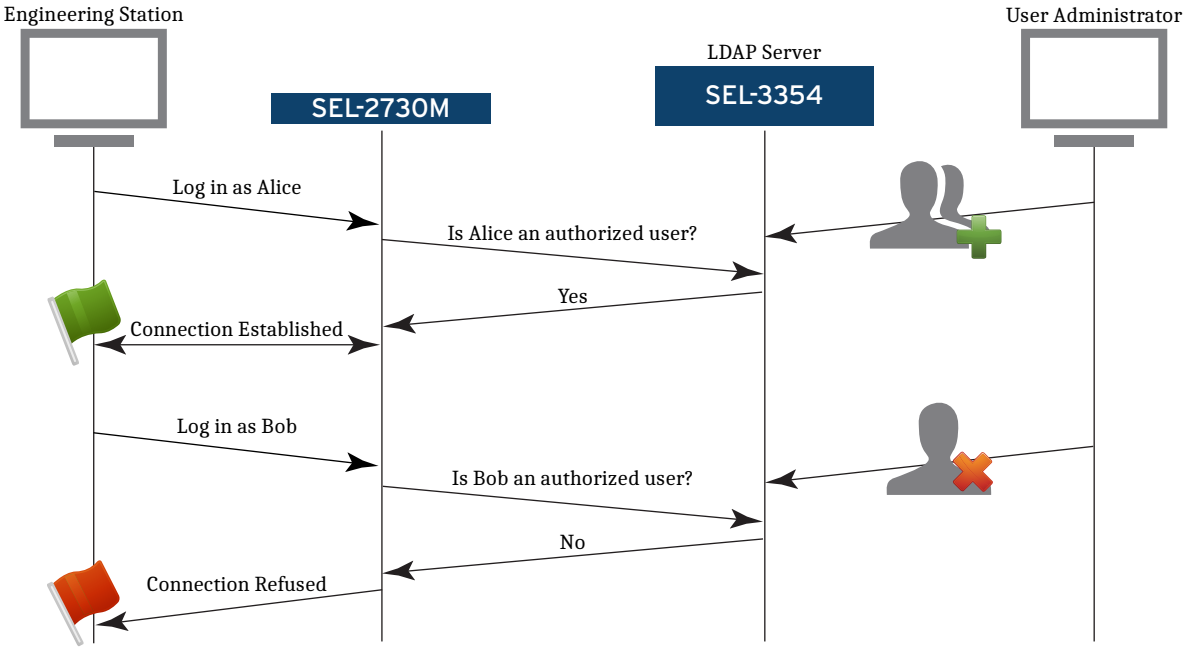


Figure 3.2 LDAP Login Process

To support this behavior, certain parameters must be configured in the SEL-2730M to allow it to communicate with your LDAP server. These parameters are configurable through the web interface. To configure LDAP on your device, access the web interface and log in using an account with administrative privileges.

SEL cannot guarantee that the device will be compatible with all possible LDAP server architectures and implementations. Commissioning and configuration of an LDAP server typically requires advanced knowledge of certificate authority hierarchies and centralized user group configurations. It is important that an organization's LDAP server administrators be involved during the design and implementation process to ensure that the device settings will be compatible with your organization's specific trust management infrastructure.

NOTE
This device is not compatible with LDAP deployments that permit commas in usernames.

Hosts

The device needs to know the name and IP address of your LDAP server to know how to contact it. Select **Hosts** from the navigation panel on your webpage to view and edit the **Hosts** settings, see *Figure 3.3*.

Figure 3.3 Host Settings

The Host Settings page provides a method to statically map IP addresses with external device hostnames such as your LDAP servers. To map an IP address to a hostname, select **Add Host**. The SEL-2730M supports as many as 64 hosts.

LDAP Certificates

LDAP requires X.509 authentication to create binds (authenticated connections) between the server and client. This is to ensure that attackers are not spoofing the authentication server to gain unauthorized access. The device requires that the root certificate of the LDAP server's certificate chain is stored locally.

LDAP Settings

Now that your device knows who and where your LDAP servers are, we can configure the device to access those servers. Select **Accounts / LDAP** in the navigation panel on your webpage to view the LDAP configuration (see *Figure 3.4*).

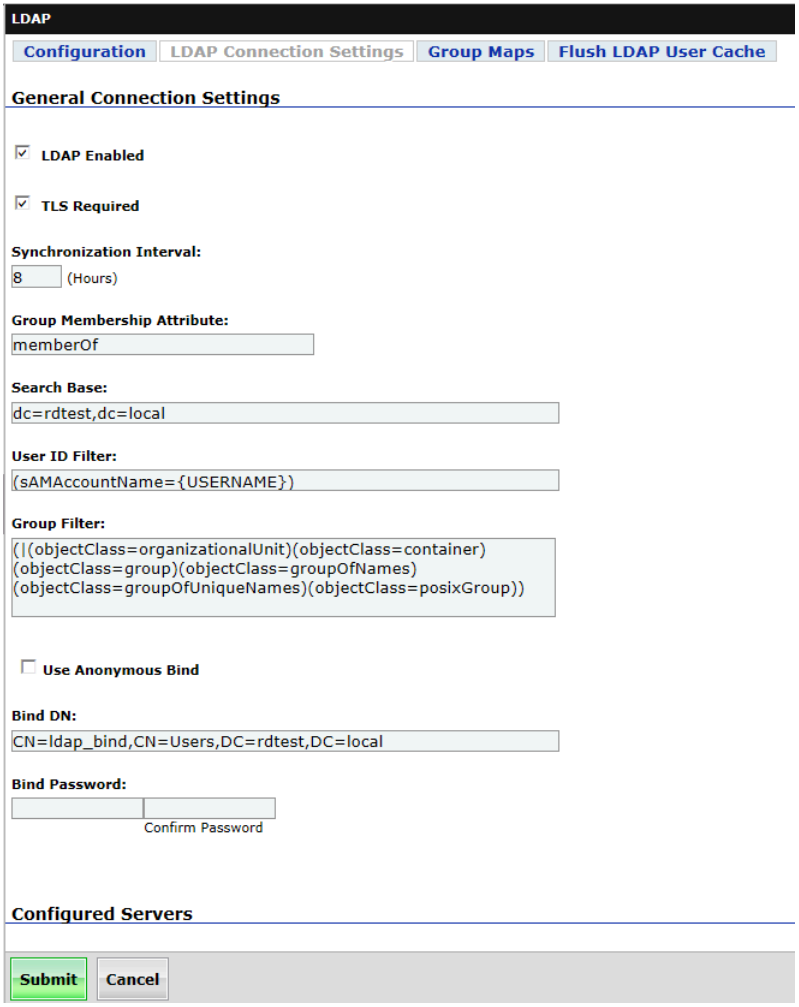


Figure 3.4 LDAP Configuration Summary

Figure 3.5 shows the LDAP Connection Settings form and all the options for communicating with your LDAP servers. To simplify configuration, we have included a form for your LDAP administrators to complete, which you can use to populate all the LDAP fields. This form is in *Appendix D: Lightweight Directory Access Protocol*.

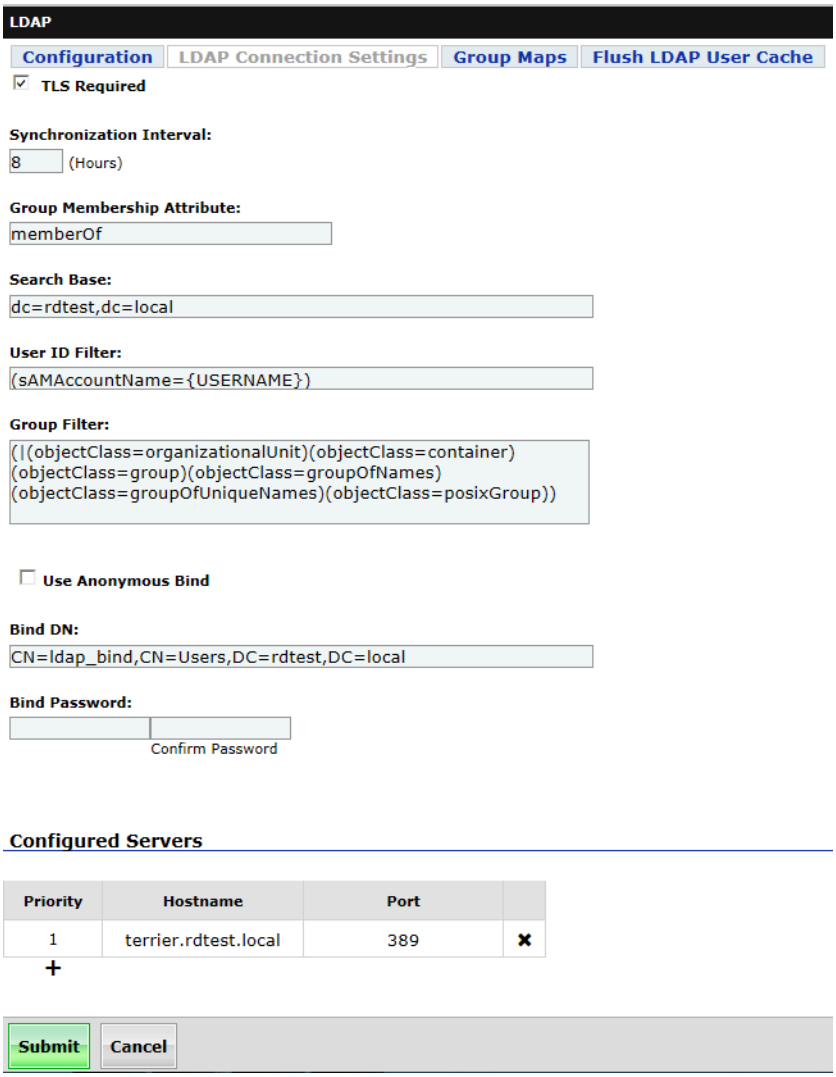


Figure 3.5 LDAP Communication Settings

The **LDAP Enabled** setting must be set checked to make centrally managed accounts available to the SEL-2730M for logins. When LDAP is enabled, if the credentials entered by the user are not found in the locally configured accounts on the SEL-2730M, it will next consult the enterprise directory by using LDAP to attempt to authenticate the user. If LDAP authentication is successful, the directory service will supply user attributes that indicate the privilege level of the user when logging in to this device.

The **TLS Required** setting determines whether the connection to the LDAP server will be protected by a TLS session. Using TLS requires that the LDAP server be provided with a suitable X.509 server certificate and that the SEL-2730M import a suitable CA or server certificate.

The **Synchronization Interval** setting exists to reduce the overhead associated with pulling account information from an LDAP server. The device locally caches the credentials and privileges of centralized users for the period of time configured. The synchronization interval is settable from 0 to 24 hours. If the

synchronization interval is set to 0, then the device will resynchronize on every login. The synchronization interval exists to speed up the login process. The SEL-2730M will continue to verify the authenticity of users against the central directory even if their privilege information is locally cached.

Group Membership Attribute, **Search Base**, **User ID Filter**, and **Group Filter** settings are used by the SEL-2730M to construct queries to the LDAP server to locate the user and then to verify his credentials. The exact form and content of these items must be carefully entered from information supplied by the LDAP administrator. Using the form in *Appendix D: Lightweight Directory Access Protocol* is recommended to collect this information.

NOTE

The Internet-Draft RFC 2307 specifies that the groupOfMembers object class can also be used as the convenient structural class for the LDAP entries of the group service. Such group entries can then have member attribute values specifying group membership in Distinguished Names (DNs). LDAP clients support such group entries and use the member attribute values for group membership resolution.

The LDAP clients also support group entries that use the groupOfUniqueNames object class and the uniqueMember attribute. However, using this object class and attribute is not recommended.

The existing method of defining the group entries with the posixGroup object class and the memberUid attribute is still supported.

The **Search Base** can be thought of as the root directory to begin your user search from. It is formed by listing all the components of the search base separated by commas going from the most specific component to the broadest component. In the figure above, the Search Base is configured as "DC=centralauth,DC=local." In this search base, DC refers to domain component. The domain components are later combined with "." to create the search domain. In this case, the search domain is centralauth.local. This search base can be interpreted to mean "search the directory residing on an LDAP server in the centralauth.local domain."

NOTE

The broader your search base, the more users/groups may be able to access the device. Broader search bases can take significantly more time to search than search bases that use more specific organizational units or groups.

One other common component of LDAP queries is CN. The component CN is short for "common name." It is a name that refers to a specific object that may or may not be unique. Examples of CNs are groups and user names.

The User ID and Group Member attributes are the LDAP labels that identify the usernames and groups of users of the system. If these are not correctly entered, the device will not be able to determine which LDAP fields to search for usernames or privileges. The User ID should be configured similar to (**sAMAccountName={USERNAME}**) or (**uid={USERNAME}**). In these examples, "sAMAccountName" or "uid" is the name of the attribute on the directory server that identifies the ownership of a user account. The {USERNAME} portion of the User ID is the variable that holds the username of the person attempting to log in to the device. For example, if the User ID were configured as (**sAMAccountName={USERNAME}**), and a person with the username **jsmith** were to attempt to log in to the device, then the device would search the LDAP directory for an entry with

a sAMAccountName attribute that contained a value of "jsmith". This field is extendable, so you can search for entries matching multiple criteria. For example, the search field "(&(sAMAccountName={USERNAME})(memberOf=cn=activeusers,dc=your,dc=domain))" would only allow access to users with a valid username who are members of the active users group of your domain.

The **Use Anonymous Bind** setting determines how the SEL-2730M accesses the LDAP server. The device supports both authenticated and anonymous binds to your LDAP servers. Authenticated binds use a service account to access the LDAP server. If the service account is revoked, or the password expires, the device will not be able to access the LDAP server, and centralized users will be unable to access the device. Anonymous binds forgo the use of service accounts. Find out from your LDAP administrator which method is preferred for your system.

If you do not use anonymous bind, you will need to supply the service account username in the **Bind DN** field, and you will need to supply the password in the Bind **DN Password** fields.

LDAP Servers

The **Configured Servers** section lists the LDAP servers that the SEL-2730M will use to authenticate logins.

To improve availability when the primary LDAP server may be inaccessible, the device supports accessing a secondary LDAP server. To add an LDAP server, select the plus (+) button below the Configured Servers table. This will add a new row to the table. Enter the hostname and port number of your server, and select **Submit** (see *Figure 3.6*).

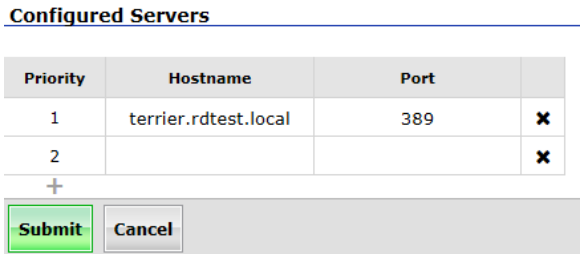


Figure 3.6 Adding an LDAP Server

LDAP servers are identified by their hostname and port numbers. Use Port 389 unless a different port number is specified by your LDAP administrator. This information should be obtained from your LDAP administrators using the form found in *Appendix D: Lightweight Directory Access Protocol*.

The device allows for two LDAP servers to be configured for redundancy and increased reliability. LDAP servers are assigned a priority and will be queried in their order of priority until the user accessing the device is found, or the list has been exhausted.

Group Mappings

The device has specific device roles that can be mapped to LDAP group memberships on the **Group Maps** tab. The view shown in *Figure 3.7* has a single group defined for administrators.

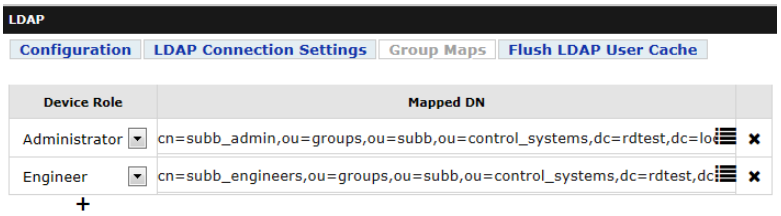


Figure 3.7 Group Mappings Showing a Single Group

Select the plus (+) button at the end of the table to configure a new group mapping in a new row of the table. On the new table row, select the device role from the drop-down list in the left column. You can enter the Mapped DN string yourself, or you can select the list icon at the end of the Mapped DN field. When you select the list icon, the SEL-2730M will query your LDAP server and then show a hierarchical tree of directory groups that can be searched using your Search Base. Scroll through the tree as necessary to find the correct group, select it with a mouse click, and select **Submit**. Opening a new row in the table is shown in *Figure 3.8*.

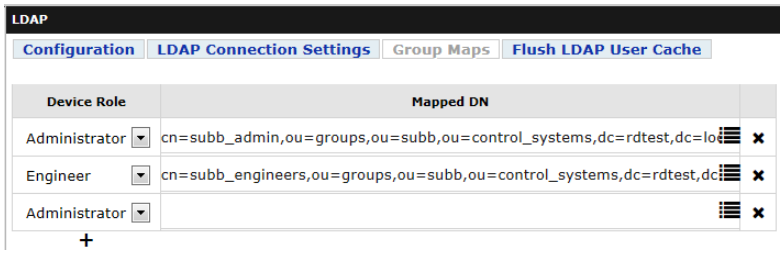


Figure 3.8 Adding a New Role

To expand the tree of groups for a row of the table, select the list icon at the right end of the **Mapped DN** field in the table. Selecting the icon again will close the tree of groups. *Figure 3.9* shows the tree of possible groups that appears after selecting the list icon.

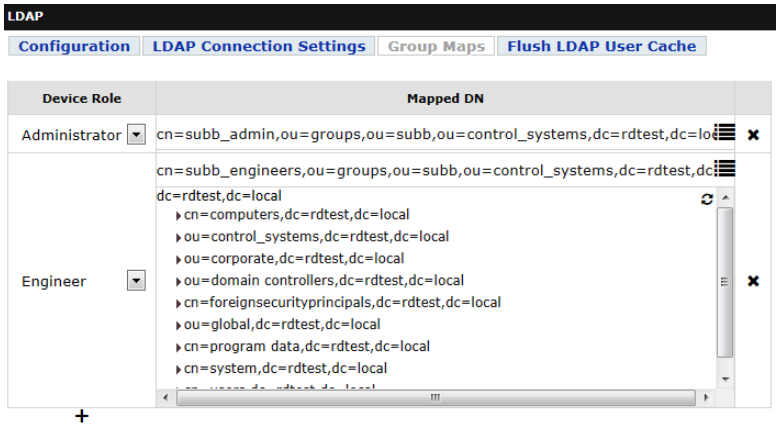


Figure 3.9 Selecting a Group From the Tree Display

If you cannot find an appropriate group, your server administrator may need to create new groups and assign members appropriate for these mappings. Work with your LDAP administrator to determine group mappings using the form found in *Appendix D: Lightweight Directory Access Protocol*.

The last tab on the LDAP page is Flush LDAP User Cache. Selecting the **Flush Cache** button flushes the LDAP user cache, which will cause all LDAP users to be logged out of the device and will force authentication information to be refreshed from the server on each account's next login.

RADIUS

The SEL-2730M supports the basic NAS client authentication functionality of the RADIUS protocol. By configuring the RADIUS settings, a user can log in using credentials not stored in the Local Users table on the SEL-2730M. The SEL-2730M also supports two-factor authentication through RADIUS.

There are three types of settings used by the RADIUS feature on the SEL-2730M:

- RADIUS Protocol settings (see RADIUS Protocol Settings) viewable on the **Configuration** page and configurable through the use of the **RADIUS Connection Settings** page under the RADIUS navigation menu link
- Hosts (required if a hostname is used in hostname setting in Configured Server) located on the **Hosts** page
- X.509 Certificates (required if an EAP Authentication Protocol is used) located on the **X.509 Certificates** page

SEL cannot guarantee that the device will be compatible with all possible RADIUS server architectures and implementations.

The **RADIUS** page on the SEL-2730M is divided into three tabs, as shown in *Figure 3.10*: **Configuration** for viewing RADIUS settings, **RADIUS Connection Settings** for configuring RADIUS settings, and **Download Dictionary** for downloading the RADIUS dictionary file. You can access these tabs by selecting on the **RADIUS** navigation menu item under **Accounts**.

Figure 3.10 RADIUS Webpage

RADIUS Protocol Settings

The RADIUS settings are divided into three categories: general, additional (for EAP protocols), and configured servers. *Figure 3.11* shows the RADIUS Connection Settings tab.

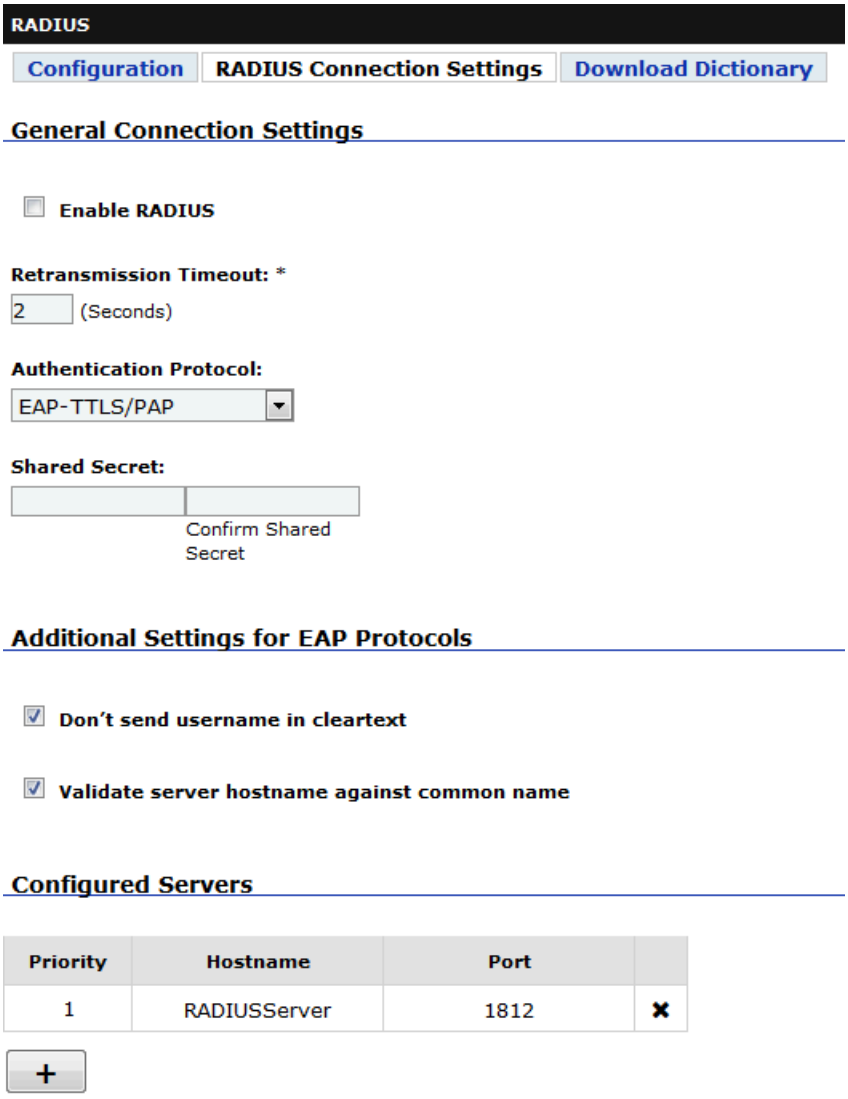


Figure 3.11 RADIUS Protocol Settings

General RADIUS settings that appear in the web interface, configuration file, and ACSELERATOR QuickSet SEL-5030 Software are listed in *Table 3.1*. Configuration file and QuickSet-only settings are listed in *Table 3.2*.

Table 3.1 General RADIUS Settings

Settings	Valid Values	Default	Feedback	Rules	Description
Enable RADIUS	Enabled, Disabled	Disabled	—	—	Enables RADIUS for authenticating users logging in to the SEL-2730M.
Retransmission Timeout	1–10 seconds	1 second	—	—	If the SEL-2730M does not receive a response from the active RADIUS server within the set Timeout amount of seconds, it makes another attempt (up to the value of the Attempts setting [see *Table 3.2*]). The total time-out period for a login attempt is Attempts * Retransmission Timeout * the number of configured RADIUS servers.
Authentication Protocol	PAP, EAP-PEAPv0/ MSCHAPv2, EAP-TTLS/ PAP	PAP	—	—	The authentication protocol that defines how the SEL-2730M authenticates with the RADIUS server. SEL recommends using an EAP protocol for enhanced security.
Shared Secret	1–128 printable ASCII characters		If RADIUS is enabled with no shared secret: `Shared secret is required because no shared secret previously configured.` If the shared secret is too long: `The shared secret can't be more than 128 characters.`	Required upon enabling RADIUS for the first time. The setting appears empty when the page loads. If the user does not successfully submit a new shared secret, the last shared secret continues to be used.	Shared secret between the SEL-2730M and the RADIUS server. This value must be the same between the SEL-2730M and the RADIUS server. SEL recommends using long shared secrets.
Confirm Shared Secret	Same as shared secret		If different than shared secret: `The shared secret and confirm shared secret settings do not match.`	Must be identical to the shared secret.	—

Table 3.2 General RADIUS Settings (XML/QuickSet Only)

Settings	Valid Values	Default	Feedback	Rules	Description
Attempts	1–10	3	—	—	Number of authentication attempts to make to the RADIUS server. If the SEL-2730M does not receive a response within the time-out period, the SEL-2730M sends another identical request. The SEL-2730M may not receive a response for various reasons, including the RADIUS server being offline or unreachable or the request packet being discarded or lost by the network.
Anonymous ID	1–128 printable ASCII characters	anonymous	—	—	Value sent as the username if **Don't send username in cleartext** is enabled.

EAP protocols also have two additional settings, as listed in *Table 3.3*. SEL recommends enabling these settings if the RADIUS server supports them. These do not apply if the PAP authentication protocol is selected.

Table 3.3 Additional Settings for EAP Protocols

Setting	Valid Values	Default	Feedback	Rules	Description
Don't send username in cleartext	Enabled, Disabled	Disabled	—	—	The username is normally sent in clear text in the User-Name attribute or Identity field (for EAP protocols). If this setting is enabled, then the SEL-2730M sends "anonymous" instead of the username (see **Anonymous ID** in *Table 3.2*).
Validate server hostname against common name	Enabled, Disabled	Enabled	—	—	As part of setting up the TLS connection, the RADIUS server sends a certificate to the SEL-2730M. One of the attributes of this certificate is the common name. If this setting is enabled, the SEL-2730M checks the server hostname as entered into the hostname setting on the **RADIUS** page and the common name in the X.509 certificate and rejects any login attempt from that RADIUS server if they are not identical.

Configured server settings are listed in *Table 3.4*. There are no default values for the Hostname or Port setting.

Table 3.4 Configured Servers Settings

Setting	Valid Values	Feedback	Rules	Description
Hostname	The hostname as listed in the host table or the IP address	—	—	The address at or through which the SEL-2730M may reach the RADIUS server. The hostname only needs to be present on the **Hosts** page when the SEL-2730M is contacting that RADIUS server.
Port	1–65535 (typically 1812)	—	—	The UDP port at or through which the SEL-2730M can reach the RADIUS server.

At least the primary server (Priority 1) must be configured. You can optionally add a backup server (Priority 2). The SEL-2730M first attempts to contact the primary server (Priority 1), and if no responses are received, it attempts to contact the backup server (Priority 2) if one is configured. If no servers are configured during the time RADIUS is enabled, then the feedback is as follows:

```
At least one configured server required
```

You can enter a hostname, as entered in the **Hosts** page, or an IP address, into the **Hostname** setting and the appropriate authentication port into the **Port** setting. This is typically **1812**. To add a backup server, select the plus (+) button and enter the hostname and port. The hostname does not have to be present on the **Hosts** page when entered, but the SEL-2730M skips any server with a hostname that is not present on the **Hosts** page. The primary and backup server information must be unique (i.e., the hostname and either the IP address that the hostname resolves to or the port must be different). If the configured servers are identical, the feedback is as follows:

```
Configured servers must be unique. Either the hostname, and
their resolved IP addresses, or the ports must be different
```

Select the ✖ button to delete a server.

SEL-User-Role VSA

Similar to logging in through LDAP or through a Local User, the user does not select their role. The RADIUS server determines the user role through the reply message. To successfully authenticate a user, the RADIUS server must return the user role in the format accepted by the SEL-2730M. This format is defined by an SEL vendor attribute SEL-User-Role, which can be downloaded by selecting **Download Dictionary** at the top of the **RADIUS** page.

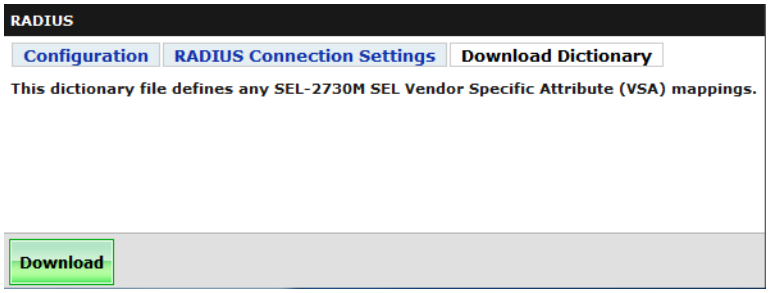


Figure 3.12 Download Dictionary

Setting up RADIUS

On the SEL-2730M

When enabling RADIUS, you must configure the RADIUS Shared Secret setting (configured on the RADIUS server) and have at least one configured server with a defined Hostname or IP address and the UDP port. If you are using a hostname, add the appropriate hostname and IP address to the **Hosts** page. If you are using an EAP protocol, you must have the appropriate X.509 certificate added to the **X.509 Certificate** page. To enable RADIUS, select the **Enable RADIUS** check box on the **RADIUS** page, configure the settings, and select **Submit**. RADIUS is then enabled and ready for the next login attempt.

On the RADIUS Server

The RADIUS server must be configured with the same shared secret and configured to return the appropriate SEL-User-Role attribute for each user.

RADIUS Attributes

In addition to the RADIUS attributes defined by the authentication protocol, the SEL-2730M supports three other attributes, listed in *Table 3.5*. These appear in each request message to the RADIUS server.

Table 3.5 Additional Request Attributes

Attribute	Value
NAS-IP-Address	The IP address of the port through which the SEL-2730M contacts the server (i.e., the IP address of the front- or rear-panel ports)
NAS-Identifier	The hostname setting as configured on the **IP Configuration** page
Calling-Station-Id	The IP address of the user logging in to the SEL-2730M

For example, if a user on a computer with an IP address of 172.16.0.150 attempts to log in to an SEL-2730M with a hostname of SEL1162641127, which then contacts the RADIUS server through an interface/port with an IP address of 172.16.1.100, the NAS-IP-address, NAS-Identifier, and Calling-Station-Id in the request message are 172.16.1.100, SEL1162641127, and 172.16.0.150, respectively.

Communications

Using PAP as an example, when a user attempts to log in to the SEL-2730M, the SEL-2730M sends an Access-Request to the RADIUS server with the username and the hashed password. When using EAP protocols, certificates are exchanged so that the RADIUS communications are encrypted. If the RADIUS server authenticates the users, it replies with an Access-Accept message that includes the user role of the user in the SEL-User-Role VSA. The RADIUS server may respond with additional attributes, which the SEL-2730M ignores. The SEL-2730M then accepts the login attempt, logging in the user with the user role specified in the SEL-User-Role VSA returned by the RADIUS server. The login attempt is rejected if the RADIUS server returns any other message, such as an Access-Reject message, or if the Access-Accept message does not contain a valid user role in the SEL-User-Role VSA. If the RADIUS server does not respond, the SEL-2730M attempts to contact the backup server (if configured). If the SEL-2730M received no responses, the login is rejected. *Figure 3.13* shows an example of this process for an authorized user with the user role of Engineer (Alice) and an unauthorized user (Bob).

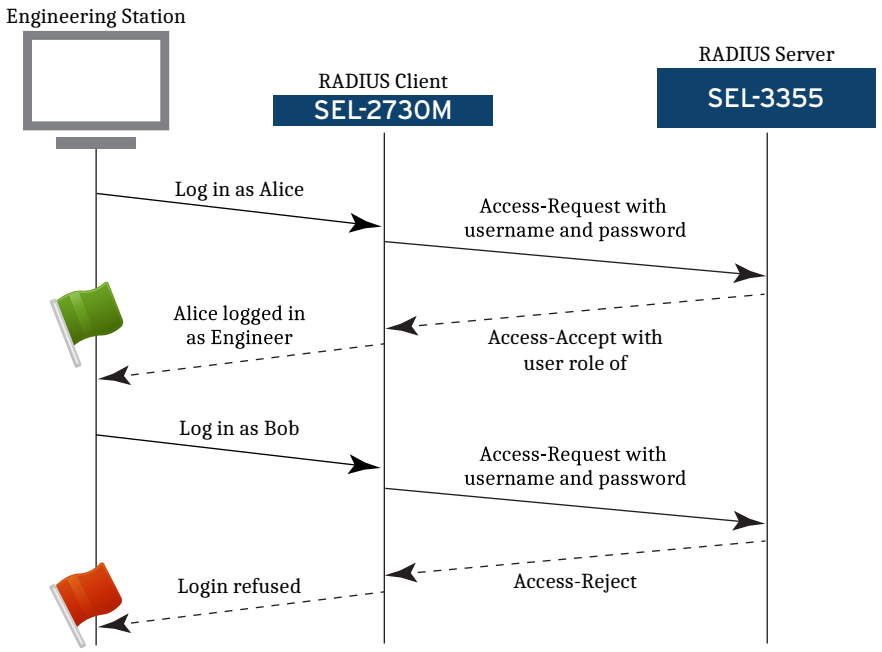


Figure 3.13 RADIUS Login Process (One-Factor)

When two-factor authentication is used, the user first generates or receives a token. This may be on a keychain or a smart phone. The user then appends this token to their password when logging in to the SEL-2730M. The SEL-2730M contacts the RADIUS server with the username and the password (i.e., the combination of the user's password and the token). The RADIUS server may proxy the request to another server to perform the two-factor authentication. *Figure 3.14* shows an example of the two-factor login process.

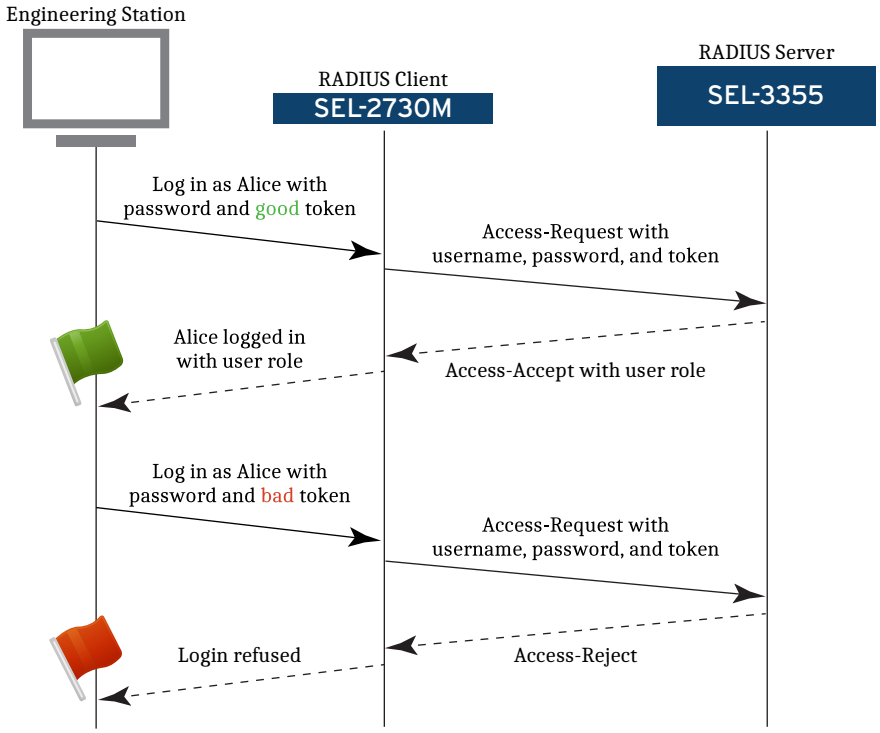


Figure 3.14 RADIUS Login Process (Two-Factor)

Events

If the SEL-2730M does not receive a response within the time-out period, the SEL-2730M logs the following event:

```
Rejected login attempt because no response from the RADIUS
server received within the retransmission timeout
```

The SEL-2730M rejects the login attempt if all attempts time out.

The RADIUS server authenticates and logs a user in by responding to the SEL-2730M request with a user role in the response. The user role must be one of the four supported on the SEL-2730M. If there is no user role in the response accept message, the SEL-2730M rejects the login attempt and sends the following event:

```
Rejected login attempt by user <username> because RADIUS server
<priority> replied without an SEL-User-Role attribute
```

If the user role is not recognized, the SEL-2730M rejects the login attempt and sends the following event:

```
Rejected login attempt by user <username> because RADIUS server
<priority> replied with an SEL-User-Role attribute containing
an unrecognized user role
```

The SEL-2730M attempts to use the primary server (Priority 1) first. If all attempts to contact the primary RADIUS server fail, and the backup server (Priority 2) is configured, the SEL-2730M logs the following event and then attempts to contact the backup server (Priority 2):

```
Active RADIUS server is now 2
```

At the next login attempt, the SEL-2730M again attempts to connect to the primary server (Priority 1) first.

The EAP authentication protocols have additional optional checks. During the initial handshake, the RADIUS server sends its X.509 certificate. If the user has enabled the **Validate server hostname against common name** setting, and the hostname does *not* match the common name, the SEL-2730M rejects the login attempt and logs the following event:

```
Rejected login attempt because the common name in the X.509
certificate sent by the RADIUS server <priority> did not match
the hostname of the RADIUS server on the RADIUS page
```

If the certificate sent by the RADIUS server has an authority issue, the SEL-2730M rejects the login attempt and logs the following event:

```
Reject login attempt because RADIUS server <priority> sent
an X.509 certificate with an unknown or untrusted certificate
authority
```

If the X.509 time is incorrect (e.g., expired), the SEL-2730M rejects the login attempt and logs the following event:

```
Rejected login attempt because RADIUS server <priority> sent an
expired or not yet valid X.509 certificate
```

If a user enables, disables, or modifies one or more RADIUS settings, the SEL-2730M logs the following events:

```
<username> at <user_ip> enabled RADIUS
```

```
<username> at <user_ip> disabled RADIUS
```

```
<username> at <user_ip> modified RADIUS settings
```

For a complete list of all events including those for RADIUS, see *Appendix E: Syslog*.

SECTION 4

Job Done Examples

Introduction

This section contains Job Done examples for the SEL-2730M. All Job Done examples assume that the device has already been commissioned.

- Example 1: *Create VLANs to Effectively Manage Network Traffic on page 49*
- Example 2: *Configure RSTP Network Topology on page 54*
- Example 3: *SNMP Monitoring From a Central Location on page 55*

Job Done Example 1

Create VLANs to Effectively Manage Network Traffic

VLANs provide benefits such as segmentation of network traffic at the message and network level. For Engineering Access applications, such as Telnet and SSH, VLANs can segregate Engineering Access between a workstation and a relay, and thus force traffic through a firewall device to perform packet inspection to ensure the traffic is allowed between network segments. VLANs also provide benefit in limiting traffic to a specific broadcast domain. For example, broadcast and multicast traffic will only be sent to devices within the same VLAN, limiting the traffic load of devices that may not need to receive this type of traffic from other devices. Grouping devices into VLANs can help improve network performance. With IEC 61850 GOOSE messaging, messages are assigned to a VLAN and are only sent to other devices within the VLAN associated with the GOOSE message.

Identifying the Problem

Your objective is to create VLANs to separate devices and GOOSE messages to effectively and securely manage network traffic. *Figure 4.1* is the logical network diagram that was provided to you, and your job is to configure VLANs on the SEL-2730M to implement this network configuration.

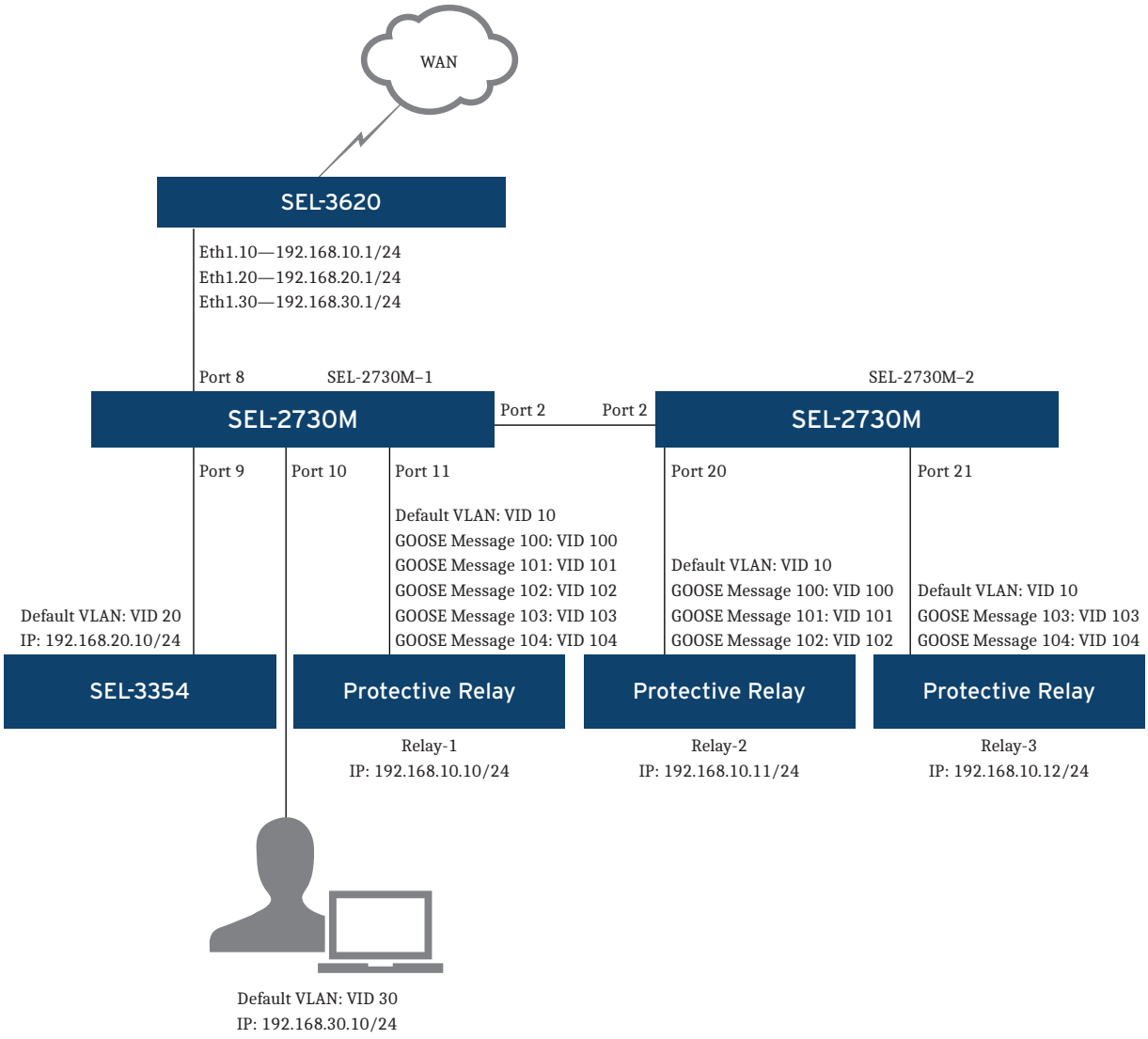


Figure 4.1 Network Diagram

The following VLANs are needed to support this configuration.

Table 4.1 VLANs for Job Done Example 1

VLAN ID	VLAN Name
10	Relay LAN
20	SCADA LAN
30	Engineering Access LAN
100	GOOSE Message 100
101	GOOSE Message 101
102	GOOSE Message 102
103	GOOSE Message 103
104	GOOSE Message 104

Access between VLANs 10, 20, and 30 are firewalled using an SEL-3620 to perform packet inspection. The SEL-3620 is configured with three sub-interfaces on Eth1 to provide routing between each VLAN segment. VLANs 100–104 are used specifically for GOOSE messaging and therefore do not require routing to the SEL-3620. The VLAN configuration in this Job Done example allows GOOSE messaging between relays as follows:

- Relay-1: Send/Receive GOOSE messages with VIDs 100–104
- Relay-2: Send/Receive GOOSE messages with VIDs 100–102
- Relay-3: Send/Receive GOOSE messages with VIDs 103–104

Configure VLANs on SEL-2730M-1

Step 1. Log in to the SEL-2730M–1 web management interface and navigate to Global Settings.

Step 2. Check VLAN-aware and select the **Submit** button.

Step 3. Navigate to VLAN Settings and select the plus (+) button beneath the VLAN table to add a new VLAN.

Step 4. Enter the configuration in *Table 4.2*. You may see feedback such as "A port can only exist in the untagged column for one VLAN." when entering the information for each VLAN. You can ignore these prompts because the SEL-2730M automatically updates the VID to 1 to remove duplicates when you submit the page.

Table 4.2 VLAN 10 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
10	Relay LAN	2, 8	11

Step 5. Select the plus (+) button again to add a new VLAN.

Step 6. Enter the configuration in *Table 4.3*.

Table 4.3 VLAN 20 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
20	SCADA LAN	8	9

Step 7. Select the plus (+) button again to add a new VLAN.

Step 8. Enter the configuration in *Table 4.4*.

Table 4.4 VLAN 30 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
30	Engineering Access LAN	8	10

Step 9. Select the plus (+) button again to add a new VLAN.

Step 10. Enter the configuration in *Table 4.5*.

Table 4.5 VLAN 100 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
100	GOOSE Message 100	2, 11	None

Step 11. Select the plus (+) button again to add a new VLAN.

Step 12. Enter the configuration in *Table 4.6*.

Table 4.6 VLAN 101 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
101	GOOSE Message 101	2, 11	None

Step 13. Select the plus (+) button again to add a new VLAN.

Step 14. Enter the configuration in *Table 4.7*.

Table 4.7 VLAN 102 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
102	GOOSE Message 102	2, 11	None

Step 15. Select the plus (+) button again to add a new VLAN.

Step 16. Enter the configuration in *Table 4.8*.

Table 4.8 VLAN 103 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
103	GOOSE Message 103	2, 11	None

Step 17. Select the plus (+) button again to add a new VLAN.

Step 18. Enter the configuration in *Table 4.9* and select **Submit** to create all the new VLANs.

Table 4.9 VLAN 104 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
104	GOOSE Message 104	2, 11	None

The completed VLAN configuration on SEL-2730M–1 is displayed in *Figure 4.2*.

VID	VLAN Name	Tagged Ports	Untagged Ports	
1	Default		1-8,12-24	✖
10	Relay LAN	2,8	11	✖
20	SCADA LAN	8	9	✖
30	Engineering Access LAN	8	10	✖
100	GOOSE Message 100	2,11		✖
101	GOOSE Message 101	2,11		✖
102	GOOSE Message 102	2,11		✖
103	GOOSE Message 103	2,11		✖
104	GOOSE Message 104	2,11		✖

Figure 4.2 SEL-2730M-1 VLAN Configuration

Configure VLANs on SEL-2730M–2

Step 1. Log in to the SEL-2730M–2 web management interface and navigate to Global Settings.

Step 2. Check VLAN-aware and select the **Submit** button.

Step 3. Navigate to VLAN Settings and select the plus (+) button beneath the VLAN table to add a new VLAN.

Step 4. Enter the configuration in *Table 4.10*.

Table 4.10 VLAN 10 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
10	Relay LAN	2	20, 21

Step 5. Select the plus (+) button again to add a new VLAN.

Step 6. Enter the configuration in *Table 4.11*.

Table 4.11 VLAN 100 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
100	GOOSE Message 100	2, 20	None

Step 7. Select the plus (+) button again to add a new VLAN.

Step 8. Enter the configuration in *Table 4.12*.

Table 4.12 VLAN 101 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
101	GOOSE Message 101	2, 20	None

Step 9. Select the plus (+) button again to add a new VLAN.

Step 10. Enter the configuration in *Table 4.13*.

Table 4.13 VLAN 102 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
102	GOOSE Message 102	2, 20	None

Step 11. Select the plus (+) button again to add a new VLAN.

Step 12. Enter the configuration in *Table 4.14*.

Table 4.14 VLAN 103 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
103	GOOSE Message 103	2, 21	None

Step 13. Select the plus (+) button again to add a new VLAN.

Step 14. Enter the configuration in *Table 4.15* and select **Submit** to create all the new VLANs.

Table 4.15 VLAN 104 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
104	GOOSE Message 104	2, 21	None

The completed VLAN configuration on SEL-2730M–2 is displayed in *Figure 4.3*.

VID	VLAN Name	Tagged Ports	Untagged Ports	
1	Default		1-19,22-24	✖
10	Relay LAN	2	20-21	✖
100	GOOSE Message 100	2,20		✖
101	GOOSE Message 101	2,20		✖
102	GOOSE Message 102	2,20		✖
103	GOOSE Message 103	2,21		✖
104	GOOSE Message 104	2,21		✖

Figure 4.3 SEL-2730M-2 VLAN Configuration

Job Done Example 2

Configure RSTP Network Topology

Rapid Spanning Tree Protocol (RSTP) is designed to provide loop-free redundant paths to end devices. Without RSTP, network loops would be present on the network and communications would be impacted by Ethernet frames circulating endlessly throughout the network. RSTP ensures a loop-free network and provides an alternative path to take in the event of a network failure.

Identifying the Problem

Your objective is to configure the RSTP settings of the SEL-2730M devices in the network diagram pictured in *Figure 4.4*. SEL-2730M-1 has been chosen to be the root bridge in the network topology and is connected to two SEL-2730M devices, providing redundant communications paths for end devices. SEL-2730M-2 and SEL-2730M-3 are connected to each other, providing a redundant communications path. End devices connected to either SEL-2730M-2 or SEL-2730M-3 have two communications paths available. One is listed as the Active RSTP Link, and the other is listed as the Blocking RSTP Link. The Active RSTP Links are the paths that communications follow unless there is a link or device failure impacting those communications paths. In the event of such a failure, the Blocking RSTP Link becomes active. Without RSTP, the network topology depicted in the figure below would have a loop, which would be detrimental to the network.

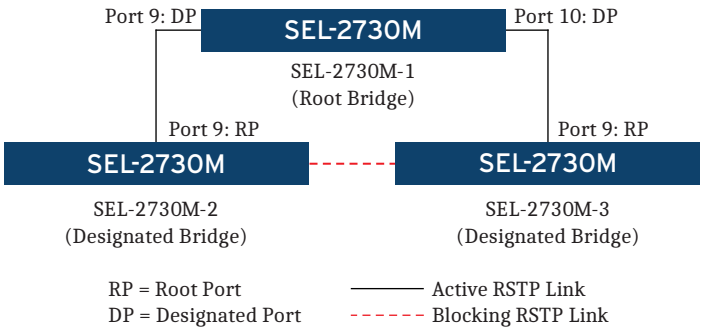


Figure 4.4 RSTP Network Topology

The root bridge is the logical center of the network. There is always exactly one root bridge at any given time within the network. The root bridge of the network is determined by selecting the device with the lowest bridge ID. RSTP selects the lowest bridge ID by comparing the bridge priority first and selecting the lowest value. If two devices have equal lowest bridge priority values, then the MAC addresses are compared next and the device with the lowest MAC address will be selected as the root bridge. To guarantee that a device will be the root bridge within the network, the bridge priority value must be set to a lower value than all other RSTP-capable devices in the network. Careful network planning is crucial when deciding on the selection of the root bridge.

Configure RSTP on SEL-2730M-1

Step 1. Log in to SEL-2730M-1 and make sure RSTP is enabled on the Global Settings page. RSTP is enabled by default.

Step 2. Navigate to RSTP Settings under Switch Management and select **Edit RSTP Settings**.

Step 3. Because SEL-2730M-1 is the root bridge in the spanning tree topology, the bridge priority must be set to a lower value than any other switch participating in the spanning tree topology. For this example, set the Bridge Priority value for SEL-2730M-1 to 8192. Leave the remaining settings on this page at their default settings.

Step 4. The following message should now be displayed at the top of the RSTP Settings page when the device determines it is the Root Bridge in the spanning tree topology.

NOTE
It may take a few seconds for the status of the spanning tree topology to refresh and the message to appear.

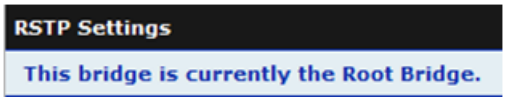


Figure 4.5 RSTP Root Bridge Notification

Job Done Example 3

SNMP Monitoring From a Central Location

Simple Network Management Protocol (SNMP) provides a method to monitor devices from a central location. SNMP capable devices respond to authorized SNMP requests with information providing insight on the network topology, network and system statistics, and hardware configuration of a device. SNMP capable devices can also be configured to send SNMP events, called traps, to a central location providing event monitoring and correlation across the network infrastructure.

Identifying the Problem

Your objective is to configure the SNMP settings of the SEL-2730M to allow SNMP requests from a network management system (NMS), and to also configure SNMP traps to be sent to the NMS. *Figure 4.6* is the logical network diagram that was provided you, and your job is to configure the SNMP settings on the SEL-2730M to implement this SNMP configuration. It is assumed that the NMS has already been configured with the SNMP configuration required to allow this communication to occur. SNMPv3 is used in this example, but the steps to configure SNMPv1 and SNMPv2c are very similar (see *Add v1/v2c Profile on page 82*).

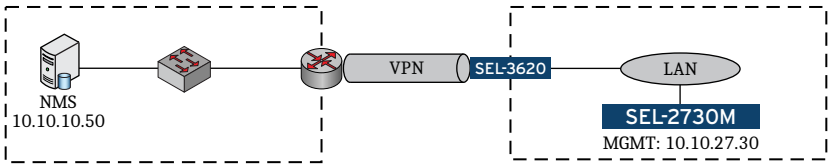


Figure 4.6 SNMP Network Diagram

Configure SNMP on the SEL-2730M

Step 1. Log in to the SEL-2730M web management interface and navigate to IP Configuration under Network Settings. Make sure SNMP is listed under Services under the Mgmt interface. If SNMP is not listed, you will need to enable SNMP by editing the network interface and selecting SNMP.

Step 2. Navigate to SNMP Settings under Network Settings and select **Edit Hosts**. The Edit Hosts page allows you to limit access to the SNMP service of the SEL-2730M by entering allowed hosts or networks. In this example, we will be limiting access to only allow the NMS with an IP address of 10.10.10.50. Enter the configuration shown below and select **Submit**.

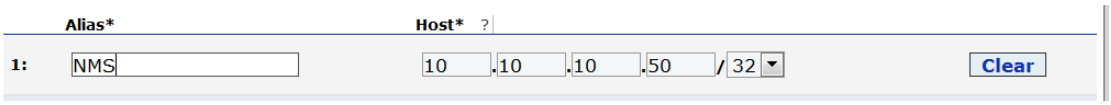


Figure 4.7 Edit Hosts Configuration

Step 3. Select the **Add v3 Profile** tab at the top of the SNMP Settings page. Configure the SNMPv3 settings as shown below (enter an **Authentication Password** and **Encryption Password** of your choice) and select **Submit**. These settings must match the SNMPv3 configuration on the NMS.

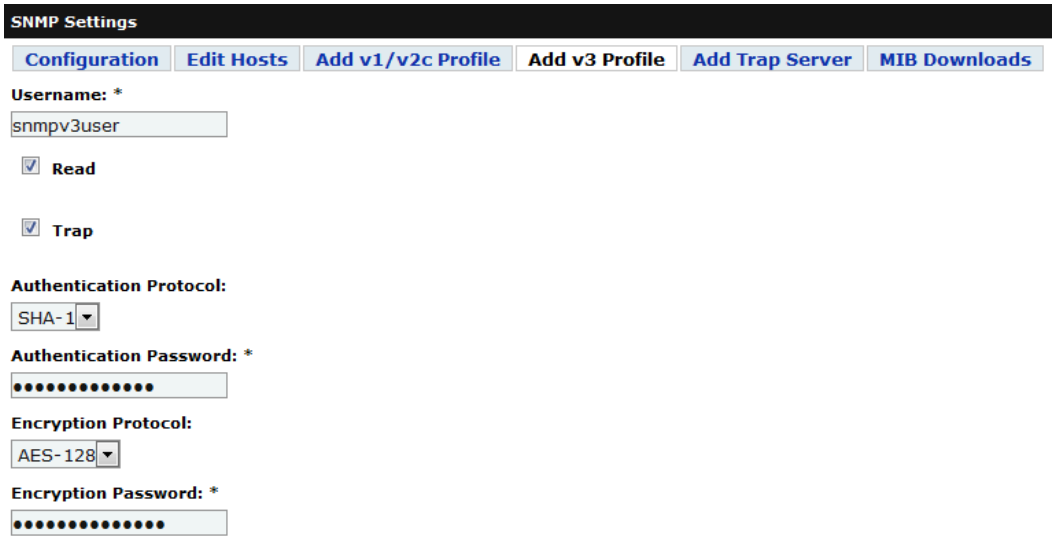


Figure 4.8 SNMPv3 Profile

Step 4. Select the **Add Trap Server** tab at the top of the SNMP Settings page and configure the settings as shown below. This configuration will send Authentication, Configuration, Port Security, and Rapid Spanning Tree Protocol SNMP traps to the NMS at 10.10.10.50.

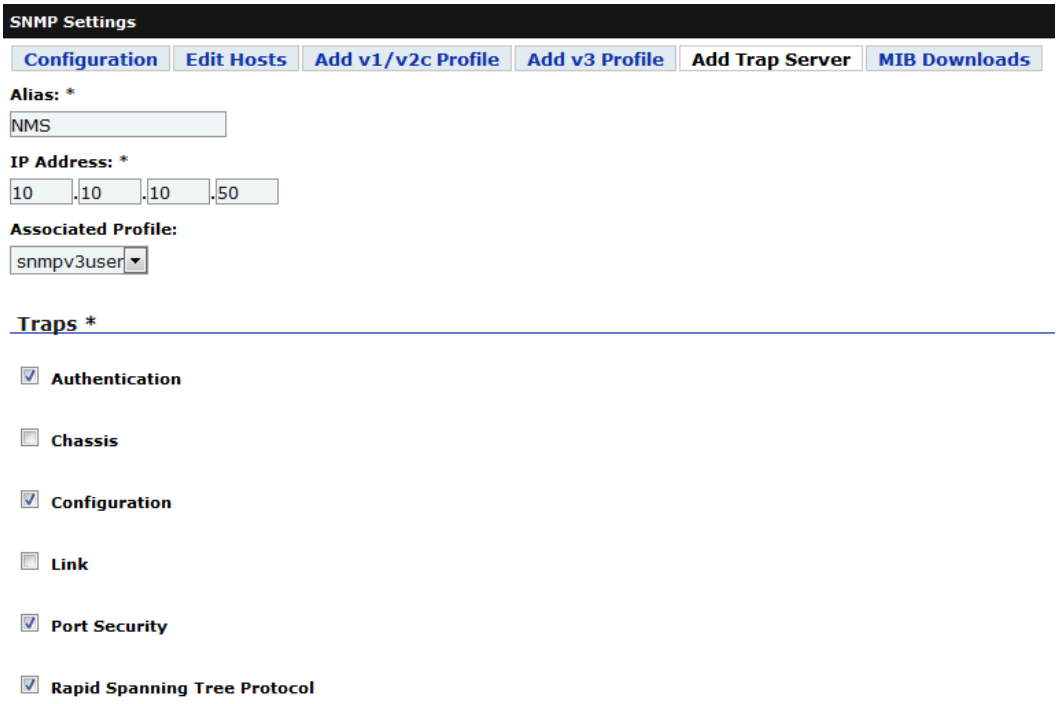


Figure 4.9 Add Trap Server

This page intentionally left blank

SECTION 5

Settings and Commands

Introduction

This section explains the settings and commands of the device.

Reports

Syslog Report

The SEL-2730M uses the Syslog message format to record event data. The device has storage for 60,000 of these messages. The device can also forward Syslog messages to three destinations.

The Syslog message format includes five fields:

- Severity
- Facility
- Tag name
- Timestamp
- Message

A message can have seven different severity ratings, ranging from informational to emergency. There are three possible facilities on the device: user, system, and security. The Tag field indicates which part of the system generated the message. The Timestamp and Message fields include the time stamp of when the message was generated and the message description. For more information about Syslog, refer to *Appendix E: Syslog*.

Select the **Syslog Report** link from the navigation panel to show the local system logs of the device (see *Figure 5.1*).

Syslog Report

Download | Acknowledge Selected | Acknowledge All

Acknowledged	ID	Timestamp	Tag	Severity	Facility	Message
☐	203	2012-05-23 17:17:13.62045+00	Login	Notice	SECURITY	Login to web: successful by admin at 10.203.16.99
☐	202	2012-05-23 17:05:46.550265+00	Login	Notice	SECURITY	Login to web: successful by admin at 10.203.16.33
☐	201	2012-05-23 16:14:30.115179+00	Login	Warning	SECURITY	User account admin timeout
☐	200	2012-05-23 15:13:45.046505+00	Login	Notice	SECURITY	Login to web: successful by admin at 10.203.16.33
☐	199	2012-05-21 21:10:39.343696+00	Login	Warning	SECURITY	User account admin timeout
☐	198	2012-05-21 21:09:09.563439+00	Login	Warning	SECURITY	User account admin timeout
☐	197	2012-05-21 20:57:38.354901+00	Login	Warning	SECURITY	User account admin timeout
☐	196	2012-05-21 20:09:58.326443+00	X509Config	Notice	SECURITY	X.509 certificate 10_203_17_37: certificate import completed successfully
☐	195	2012-05-21 20:09:49.763052+00	X509Config	Notice	SECURITY	X.509 certificate import started by admin at 10.203.16.99
☐	194	2012-05-21 20:09:11.619253+00	Login	Notice	SECURITY	Login to web: successful by admin at 10.203.16.99
☐	193	2012-05-21 20:07:59.413534+00	X509Config	Notice	SECURITY	X.509 certificate 10.203.17.37_1551976384052061911 8: certificate import completed successfully
☐	192	2012-05-21 20:07:49.812102+00	X509Config	Notice	SECURITY	X.509 certificate import started by admin at 10.203.16.99
☐	191	2012-05-21 20:07:28.515184+00	Login	Notice	SECURITY	Login to web: successful by admin at 10.203.16.99
☐	190	2012-05-21 19:56:50.885204+00	X509Config	Notice	SECURITY	X.509 certificate 10.203.17.37_1551976384052061911 8: certificate import completed successfully
☐	189	2012-05-21 19:56:42.438428+00	X509Config	Notice	SECURITY	X.509 certificate import started by admin at 10.203.16.99
☐	188	2012-05-21 19:55:33.082309+00	Login	Notice	SECURITY	Login to web: successful by admin at 10.203.16.99
☐	187	2012-05-21 19:16:01.546277+00	Login	Warning	SECURITY	User account admin timeout
☐	186	2012-05-21 19:10:31.368248+00	Login	Warning	SECURITY	User account admin timeout
☐	185	2012-05-21 18:41:02.189467+00	X509Config	Notice	SECURITY	X.509 certificate 10: certificate import completed successfully
☐	184	2012-05-21 18:41:00.903044+00	Login	Warning	SECURITY	User account admin timeout
☐	183	2012-05-21 18:11:49.446583+00	X509Config	Notice	SECURITY	X.509 certificate import started by admin at 10.203.16.99
☐	182	2012-05-21 18:11:01.192239+00	X509Config	Notice	SECURITY	X.509 certificate 10: certificate import completed successfully
☐	181	2012-05-21 18:10:50.86625+00	X509Config	Notice	SECURITY	X.509 certificate import started by admin at 10.203.16.99
☐	180	2012-05-21 18:10:32.750324+00	X509Config	Notice	SECURITY	X.509 certificate 10.203.17.37_1551976384052061911 8: certificate import completed successfully
☐	179	2012-05-21	Login	Notice	SECURITY	Login to web: successful by admin at 10.203.16.99

Displaying Records 0 - 50 of 203 | Records Per Page: 50 | << | < | Page 1 | > | >>

Figure 5.1 Sample Syslog Report

Device system logs are displayed in the order of their generation. Select a field label at the top of the list to reorder the messages according to the value of that field. For example, selecting the Severity label reorders the list by severity.

Event messages in the device have two states: unacknowledged and acknowledged. These two states exist to make identification of abnormal event generation easier. Large numbers of unacknowledged messages can indicate high levels of activity on the device.

Message acknowledgment also assists with log documentation. In your periodic examination of logs, acknowledge existing logs. When you examine logs in the future, the previously acknowledged logs limit the logs of concern to only those logs the device has generated since the last examination.

Select the **Acknowledge Selected** button to acknowledge selected system logs. All system logs can be acknowledged by selecting the **Acknowledge All** button. You cannot remove system logs from the device without issuing a factory-default reset.

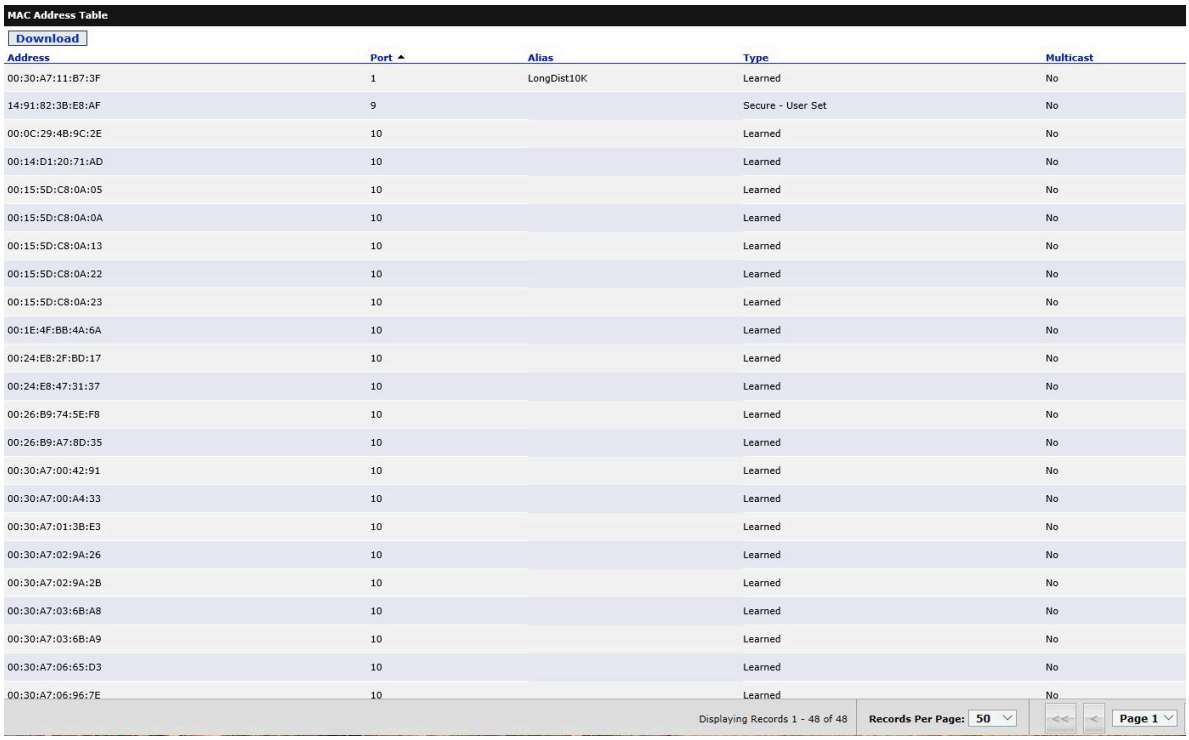
The **Download** button allows you to save log messages in an offline format.

MAC Address Table

The SEL-2730M can report the device MAC Address attached to each port. The report can be sorted by:

- Address
- Port
- Alias
- Type
  - Learned: Learned by the switch
  - Static: Manually input multicast MAC filter
  - Secure - User Set: Manually input by user on MAC-based port security
- Multicast

The report can also be downloaded into a comma-separated value table for local storage or export.



MAC Address Table

Download

Address	Port	Alias	Type	Multicast
00:30:A7:11:B7:3F	1	LongDist10K	Learned	No
14:91:82:3B:E8:AF	9		Secure - User Set	No
00:0C:29:4B:9C:2E	10		Learned	No
00:14:D1:20:71:AD	10		Learned	No
00:15:5D:C8:0A:05	10		Learned	No
00:15:5D:C8:0A:0A	10		Learned	No
00:15:5D:C8:0A:13	10		Learned	No
00:15:5D:C8:0A:22	10		Learned	No
00:15:5D:C8:0A:23	10		Learned	No
00:1E:4F:BB:4A:6A	10		Learned	No
00:24:E8:2F:BD:17	10		Learned	No
00:24:E8:47:31:37	10		Learned	No
00:26:B9:74:5E:F8	10		Learned	No
00:26:B9:A7:8D:35	10		Learned	No
00:30:A7:00:42:91	10		Learned	No
00:30:A7:00:A4:33	10		Learned	No
00:30:A7:01:3B:E3	10		Learned	No
00:30:A7:02:9A:26	10		Learned	No
00:30:A7:02:9A:2B	10		Learned	No
00:30:A7:03:6B:A8	10		Learned	No
00:30:A7:03:6B:A9	10		Learned	No
00:30:A7:06:65:D3	10		Learned	No
00:30:A7:06:96:7E	10		Learned	No

Displaying Records 1 - 48 of 48 Records Per Page: 50 Page 1

Figure 5.2 Sample MAC Address Table Report

Select a field label at the top of the report to reorder the messages according to the value of that field. For example, selecting the Address label reorders the list by Address first and Port second.

The **Download** button allows you to save the table output in an offline format.

Switch Management

VLAN Settings

When the device is not in VLAN-aware mode, VLAN settings can be viewed but not modified. To modify VLAN settings, make sure VLAN-aware mode is enabled and the account accessing the device has the appropriate role assigned. Refer to *Global Settings on page 91* for information on enabling VLAN-aware mode. The switch supports a shared VLAN learning (SVL) architecture, so the MAC addresses of hosts are learned and shared across all VLANs. Therefore, the switch expects that each host has a unique MAC address, even if those hosts are on different VLANs. Using SVL reduces flooding when learning MAC addresses, which in turn reduces network burden.

Table 5.1 VLAN Settings

Field Name	Values	Default	Description
VID	1 to 4094	N/A	The VLAN Identifier (VID) identifies the VLAN in IEEE 802.1Q-2005 tagged frames.
VLAN Name	0 to 64 characters	N/A	User-defined name of the VLAN.
Tagged Ports	Available ports	N/A	Tagged ports determines which ports can ingress and egress frames for the VLAN. Tagged ports are sometimes called Trunk Ports. Tagged ports can be used to connect to a VLAN-aware device, or to another switch.
Untagged Ports	Available ports	N/A	Untagged ports tags all untagged frames with the VID of the VLAN they are associated with when ingressing from the ports and untags all tagged frames when egressing to the ports. Untagged ports are used to connect to non-VLAN-aware devices.

VLAN View

The **VLAN View** page (*Figure 5.3*) shows a table that provides a VLAN-centric view of the configuration of VLANs and the member ports. The fields of the table can be edited, and the **Submit** button at the bottom of the page used to apply the finished set of changes to the configuration of the VLANs. In the VLAN view, groups of VLANs with similar settings are shown as a VID range.

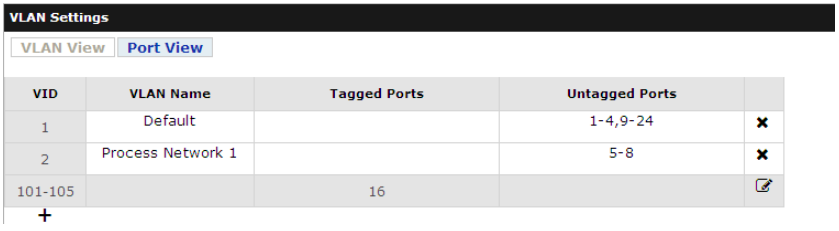


Figure 5.3 VLAN View

To edit a VLAN entry, select the table item to be changed and edit the data. The affected table item will be highlighted, and an undo link will appear next to it to allow you to revert the change. Selecting the **Submit** button at the bottom of the page will apply all the edited changes to the VLAN configuration. *Figure 5.4* shows an example where several fields have been edited but not yet applied.

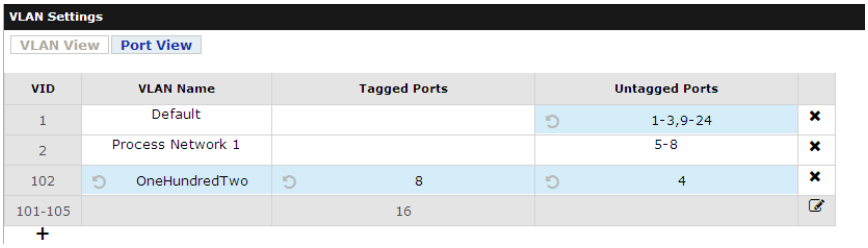


Figure 5.4 Editing VLAN Settings

To delete a VLAN entry, select the ✖ button in the last column of the table.

To edit a VLAN in a group, select the edit ( ) button in the last column of the entry, enter the VLAN number, and then make the necessary changes in the table row that is added for that VLAN. *Figure 5.5* shows how to select the VLAN that you wish to edit.

Figure 5.5 Editing a VLAN Within a Range

To delete a VLAN group (single row of the VLAN table), select the **Port View** tab and delete the affected VID range from the **Allowed VIDs** column for the affected ports.

Tagged Ports

The **Tagged Ports** column lists those ports that can send or receive frames for a given VLAN to another VLAN-aware switch or device. Devices capable of IEEE 802.1Q-2005 VLAN tagging, such as switches and GOOSE-capable IEDs, transmit frames with a VID assigned to the frame. This is commonly referred to as VLAN tagging. For the device to allow a frame with a VLAN tag to be sent or received from a port, that port must be configured as a **Tagged Port** for the VLAN indicated by the tag.

One example of using VLAN tagging is to create a trunk link between switches. A trunk link is a physical link between two switches that can pass traffic among multiple VLANs. *Figure 5.6* shows an example of two switches using port 1 as a trunk link carrying VLANs 100, 101, and 102. To configure this, each switch would need to add Port 1 as a **Tagged Port** for VLANs 100, 101, and 102.

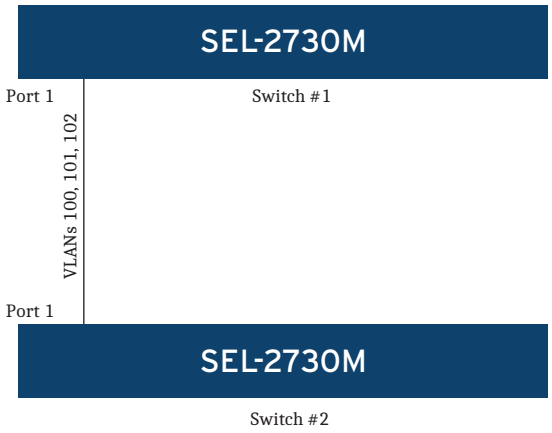


Figure 5.6 Switch Trunk Link

Another example of using VLAN tagging is with the IEC 61850 GOOSE protocol. IEDs tag GOOSE messages with a VID. For these GOOSE messages to be sent or received with another switch, you must configure the port used to connect to the other switch or VLAN-aware device as a **Tagged Port** for the VID tag of the GOOSE frame. In the example shown in *Figure 5.7*, two IEDs use GOOSE messages tagged with VIDs 200, 201, and 202 to communicate through the switch. In this example, the configuration of the switch must have Ports 9 and 10 listed as **Tagged Ports** for VLANs 200, 201, and 202 for the GOOSE messages to pass through the switch between the two VLAN-aware IEDs.

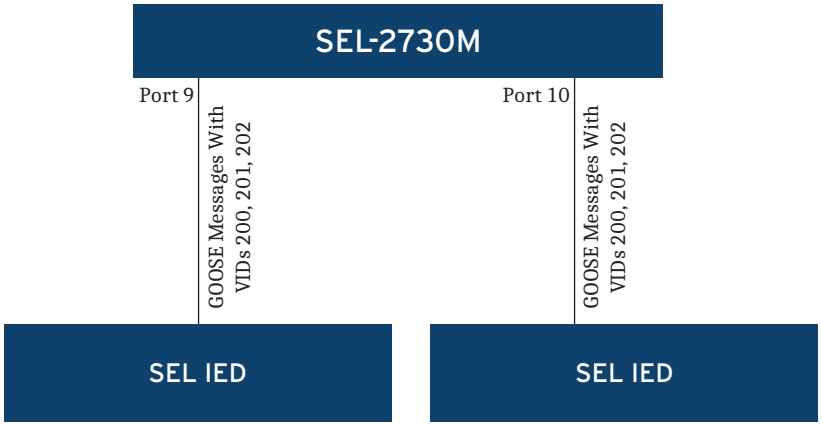


Figure 5.7 GOOSE Message

Untagged Ports

Devices that are not VLAN-aware can still participate in a VLAN if the switch is configured to associate their traffic with a VLAN. Their network frames need to be assigned a VID associated with other devices within the same VLAN. Untagged ports perform two actions: (1) they receive untagged frames from devices connected to the port and apply the VID of the VLAN to which the port is assigned, and (2) they transmit untagged frames to the devices. Each port can be assigned as an **Untagged Port** in one only VLAN.

In the example shown in *Figure 5.8*, an engineer must log in to the SEL IED to perform maintenance. Communications from the SEL-3355 to the SEL IED are untagged, and the ports must be in the same VLAN for the two devices in this example to communicate. VLAN 7 is used in this example, but any valid VLAN could be used. In this example, Ports 11 and 12 must be set as **Untagged Ports** for VLAN 7, for untagged frames to pass between the two devices. By default, all ports are assigned to VLAN 1.

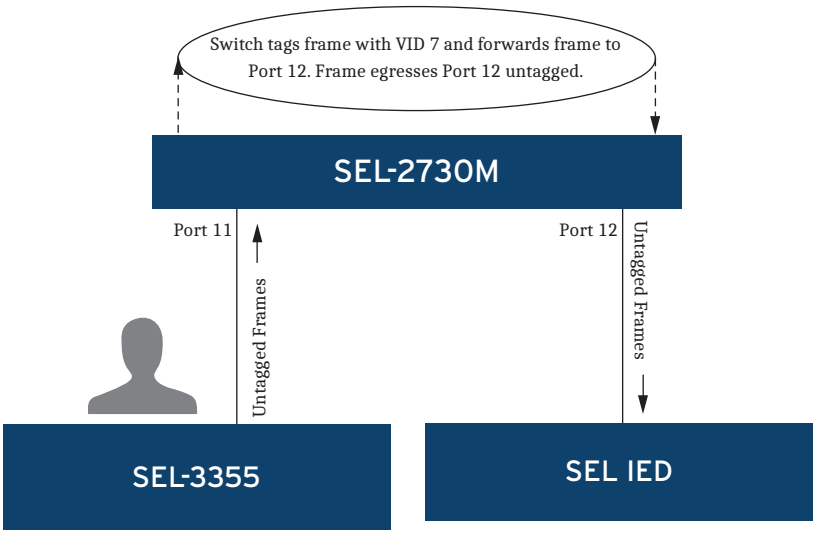


Figure 5.8 Untagged Ports

Port View

The **Port View** page (see *Figure 5.9*) provides a port-centric view of the VLAN configuration of each port. This page provides an alternative view of the VLAN configuration for each port.

VLAN Settings

VLAN View | Port View

Ports	Default VID	Allowed VIDs
1	7	
2	1	
3	1	
4	1	
5	1	
6	1	
7	1	
8	1	
9	1	
10	1	

Figure 5.9 Port View

Add New VLAN

Use the following steps to create a new VLAN on the device.

Step 1. Log in to the device with an Engineer or Administrator account.

Step 2. Navigate to the **VLAN Settings** page. When no VLANs have yet been configured, all ports are assigned as untagged ports to VLAN 1, the default VLAN.

Step 3. To create a new VLAN, select the plus (+) button beneath the VLAN table. A new row will be added to the end of the VLAN table.

Step 4. Assign a **VID**, optionally enter a **VLAN Name**, and assign the port(s) based on your required configuration. The VLAN settings table above describes each field.

Rapid Spanning Tree Protocol (RSTP) Settings

Communications networks are typically designed with ring and mesh topologies and interconnecting switches to provide network redundancy. RSTP is designed to support these network topologies and provide loop-free redundant paths to end devices. Without these protocols, network loops would be present on the network and Ethernet frames circulating endlessly throughout the network would impact communications. RSTP ensures a loop-free network and provides an alternative path in the event of a network failure.

RSTP is enabled by default on this device. You can disable RSTP through the Spanning Tree Mode setting on the Global Settings page. Exercise caution when disabling RSTP, because doing so could introduce network loops.

If RSTP is disabled, the following message displays at the top of the RSTP Settings page.

Figure 5.10 RSTP Disabled

Settings can be modified while RSTP is disabled; these settings are not active until you enable RSTP through the Spanning Tree Mode setting in Global Settings.

Configuration

Figure 5.11 shows the RSTP configuration of the device.

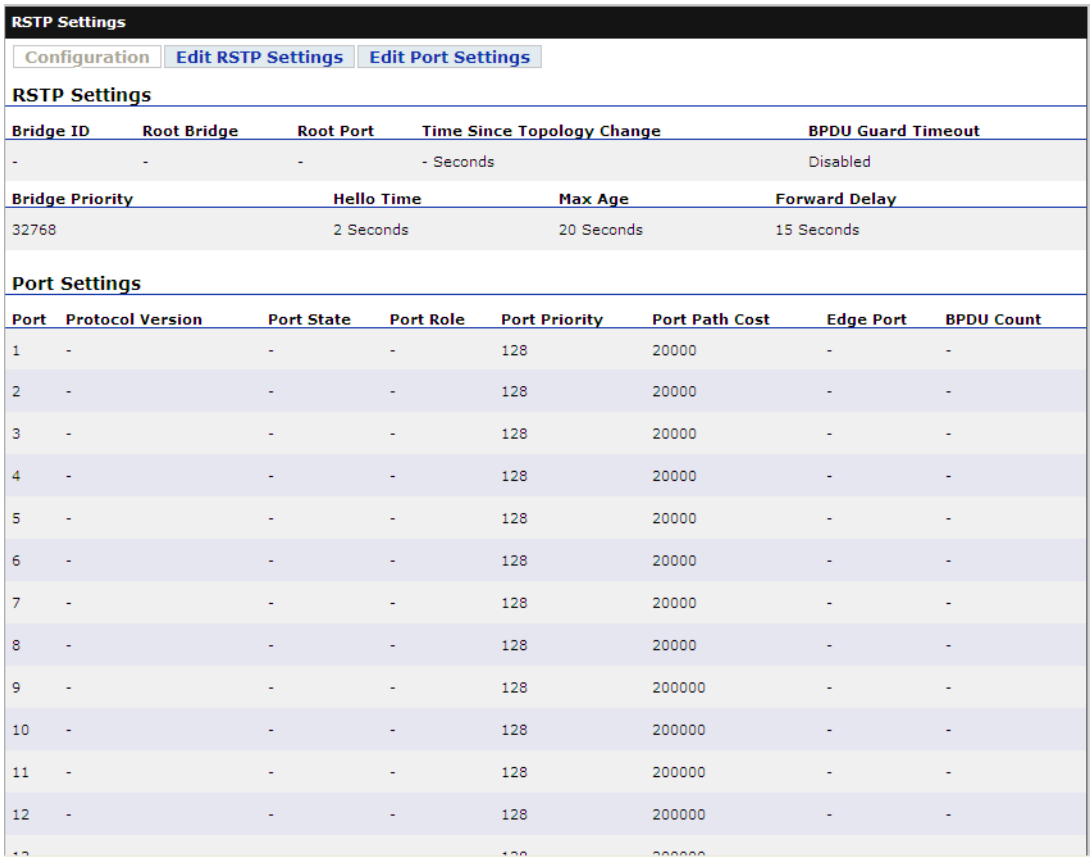


Figure 5.11 RSTP Configuration Page

Bridge ID

The Bridge ID field consists of a combination of the bridge priority and the bridge MAC address. Each RSTP-capable device in the network has a unique bridge ID that RSTP uses to determine the root bridge.

Root Bridge

The root bridge is the logical center of the network. There is always exactly one root bridge at any given time within the network. Determination of the root bridge of the network occurs through RSTP selection of the device with the lowest bridge ID. RSTP selects the lowest bridge ID by comparing the bridge priority first and selecting the lowest value. If two devices have equal bridge priority values, then RSTP next compares the MAC addresses and selects the device with the lowest MAC address as the root bridge. To guarantee a device will be the root bridge within the network, the bridge priority value must be set to a lower value than all other RSTP-capable devices in the network. Careful network planning is crucial to selection of the root bridge.

The following message displays at the top of the **RSTP Settings** page when the device is the root bridge in the spanning tree topology.

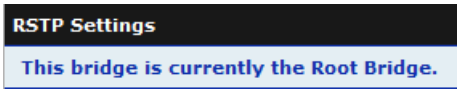


Figure 5.12 Root Bridge Notification

Root Port

The root port is a port with the shortest path to the root bridge. All RSTP-enabled devices must have exactly one root port with the exception of the root bridge, which does not have a root port. If the device is the root bridge, the root port does not apply and the device displays –.

Time Since Topology Change

The device displays the time since the last topology change occurred. Common scenarios for a topology change occurring are when a spanning tree port changes state, or either a power cycle or decommissioning procedure removes a spanning tree device from the topology.

BPDU Guard Timeout

This interval is the time that a port configured with BPDU Guard will be disabled before the SEL-2730M attempts to reenable it after the SEL-2730M receives a BPDU on that port.

Bridge Priority

The bridge priority consists of two components; the bridge priority and the MAC address.

Hello Time

The hello time is the interval in which the device sends bridge protocol data units (BPDUs).

Max Age

The max age is the maximum number of hops from the root that an SEL-2730M accepts a BPDU. If the number of hops from the root bridge (Message Age) is greater than this setting, the SEL-2730M discards the BPDU.

Forward Delay

The forward delay is the time that a port must spend in the listening and learning states before transitioning to forwarding.

The max age and forward delay derive from the root bridge. If the device is not the root bridge in the spanning tree topology, the device derives these settings from the root bridge.

Editing RSTP Settings

RSTP Settings are made on the **RSTP Settings** page. The **Edit RSTP Settings** tab (*Figure 5.13*) is used to edit settings that are common to all ports, and the **Port Settings** tab (*Figure 5.14*) is used to set the **STP Mode**, the **Port Priority**, and **Path Cost** for each port.

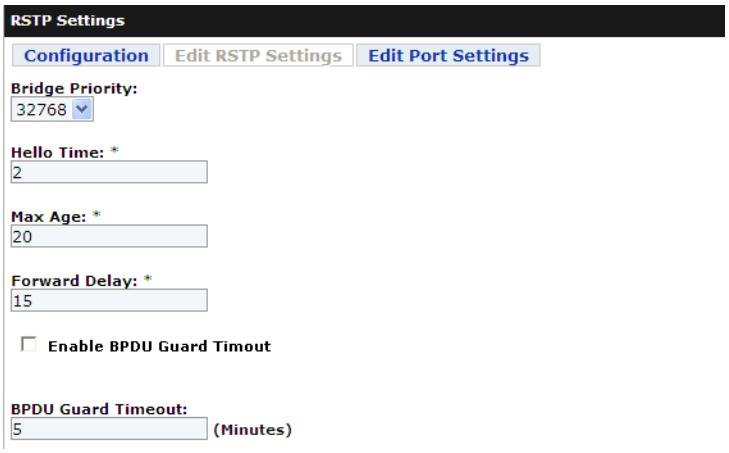


Figure 5.13 Common RSTP Settings

Figure 5.14 shows the **Port Settings** dialog used to set those RSTP parameters that are individual for each port.

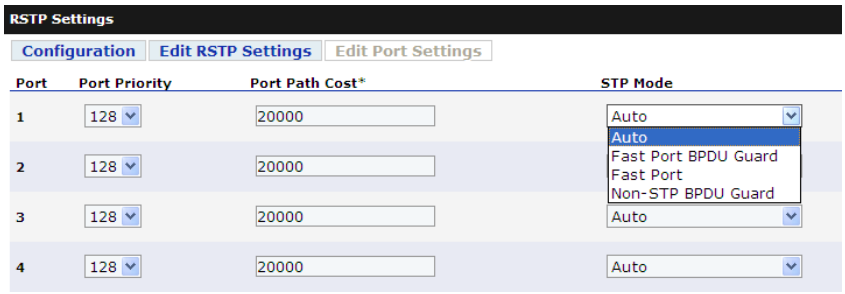


Figure 5.14 Port RSTP Settings

Table 5.2 RSTP Settings

Field Name	Values	Default	Description
BPDU Guard Timeout	1–60 min	5 min	The amount of time that port configured with BPDU Guard will be disabled after receiving a BPDU frame.
Bridge Priority	0–61440 in increments of 4096	32768	Bridge priority determines the root bridge. The bridge with the lowest value becomes the root bridge.
Hello Time	1–10 s	2 s	Interval in which device sends BPDUs.
Max Age	6–40	20	Maximum number of hops before a BPDU is discarded.
Forward Delay	4–30 s	15 s	The time that a port must spend in the listening and learning states before transitioning to forwarding.

Port Settings

Table 5.3 Port Settings

Field Name	Values	Default	Description
Priority	0–240	128	Port priority determines which port the device selects as a root port when there is a tie between two ports. The port with the lower value will become the root port.
Path Cost	1–200000000	Based on port speed	Path cost helps determine which path the device selects to a root bridge. The device selects paths with the lowest overall cost first.
STP Mode	Auto, Fast Port BPDU Guard, Fast Port, Non-STP BPDU Guard	Auto	See below.

Switches communicate RSTP through BPDU frames that travel between adjacent switches. These frames allow switches to determine the root switch, as well as the state and role of each port on that root. RSTP is faster than STP because it uses a proposal/agreement mechanism to quickly move a port into the forwarding state, thereby quickly enabling communication through that port. When ports connect to an end device that does not participate in RSTP, the proposal/agreement mechanism is unavailable, and the switch must rely on STP timers (in this case, the Forward Delay). With the default Forward Delay value of 15, the switch takes longer than 15 seconds to transition the port into the forwarding state. Because no BPDUs have been received, the port is considered an edge port. After this time-out, the port remains in the forwarding state (i.e., as an edge port) until the link status toggles or the switch changes its root port at which time the switch reinitiates the slow transition into the forwarding state. If a BPDU ingresses into the port, the switch then removes the edge port status.

To prevent this slow transition into the forwarding state, you can configure the STP Mode to be either Fast Port BPDU Guard, Fast Port, or Non-STP BPDU Guard. In these modes, each port transitions quickly to the forwarding state, but behaves differently in how it reacts to received BPDUs and whether the switch sends BPDUs out of that port. In Fast Port BPDU Guard or Fast Port mode, the switch still sends out BPDU packets; in Non-STP BPDU Guard mode, the switch does not send BPDUs out of the port.

BPDU Guard prevents devices connected to the port from affecting the spanning tree of the switch. If the switch receives a BPDU on a port with BPDU Guard enabled, the switch disables that port, preventing traffic from passing to and from the port. Enabling this setting on every port not connected to another RSTP switch can help protect against miswirings and malicious attacks to the spanning tree.

The differences among the four modes are summarized in *Table 5.4*. Ports of RSTP switches connected to other RSTP switches should be in Auto STP Mode. Non-STP BPDU Guard mode is recommended for connections to non-RSTP switches.

Table 5.4 STP Mode

STP Mode	Switch Sends BPDUs Out the Port?	Switch Shuts Off Port if it Receives a BPDU?	Moves Instantly Into the Forwarding State?	For Connecting to...
Auto	Yes	No	No	RSTP switches
Fast Port BPDU Guard	Yes	Yes	Yes	End devices
Fast Port	Yes	No	Yes	End devices
Non-STP BPDU Guard	No	Yes	Yes	End devices

Multicast MAC Filtering

The SEL-2730M uses multicast MAC filtering to subscribe multicast traffic to a group of selected ports. When a multicast frame ingresses a port, the device inspects the multicast address to see if it matches any configured multicast MAC filter. If no match occurs, the device sends the frame to all ports within the same VLAN. If a match does occur, the device sends the frame to only the member ports the device configuration specifies within the same VLAN.

Use the following steps to create a multicast MAC filter on the device.

Step 1. Log in to the device with an Engineer or Administrator account.

Step 2. Navigate to the **Multicast MAC Filtering** page and select **Add Filter**. The following page will display.

Figure 5.15 Add New Filter

Step 3. Enter the multicast MAC address on which you would like to filter and the member ports.

Step 4. Select **Submit** to add the multicast MAC filter.

Port Mirroring

You would typically use port mirroring for troubleshooting network problems and for monitoring traffic on a selected source port through the use of a network protocol analyzer attached to a target port. Port mirroring mirrors the network traffic the device sends and receives on the source port to the target port. This allows the use of a non-intrusive troubleshooting technique for gathering network traffic information for a connected port.

The device can mirror network traffic from multiple source ports to one target port. The source port may be any physical port on the device except the target port that the device uses for mirroring and the front Ethernet management port (**ETH F**).

The source port may be selected as ingress, egress, or for passage of both types of traffic to the target port.

The target port cannot receive ingress traffic while in the monitoring session.

In *Figure 5.16*, the device has been configured to mirror both ingress and egress traffic from Port 9 to Port 16. To configure port mirroring, navigate to the **Port Mirroring** page and select **Enable Port Mirroring**. Select the source port, target port, and the traffic you want mirrored to the target port, by selecting either **Mirror Ingress Traffic** or **Mirror Egress Traffic**. You can also select both to mirror ingress and egress traffic from the source port to the target port.

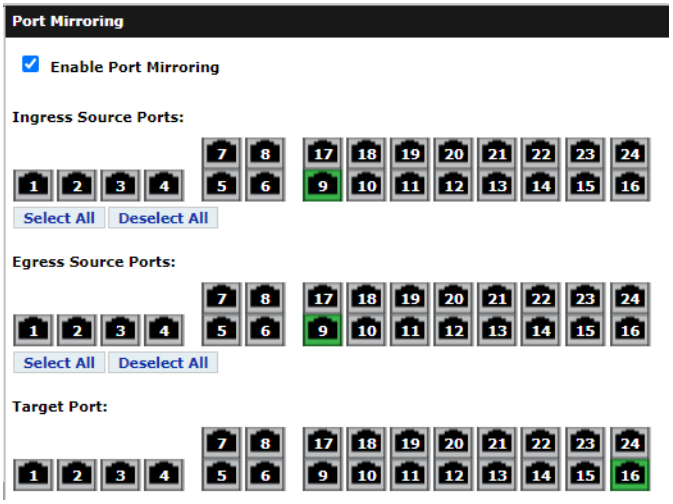


Figure 5.16 Port Mirroring

Port Monitor

Link flap is a situation in which a physical interface on the switch continually goes up and down. Rx Checksum is a count of the frame check sequence errors. The **Port Monitor** page provides you the ability to change the monitoring mode, threshold limits, and actions. Each port can be configured with two different modes (see *Figure 5.17*) and four actions (see *Figure 5.18*). The default settings are to monitor for both situations and log to the syslog. The monitoring period is fixed at sixty seconds. The port will be disabled if the threshold is reached inside of the monitoring period. A user can enable the port from the port settings page or the port monitoring page. A reboot of the device will automatically enable any disabled ports.

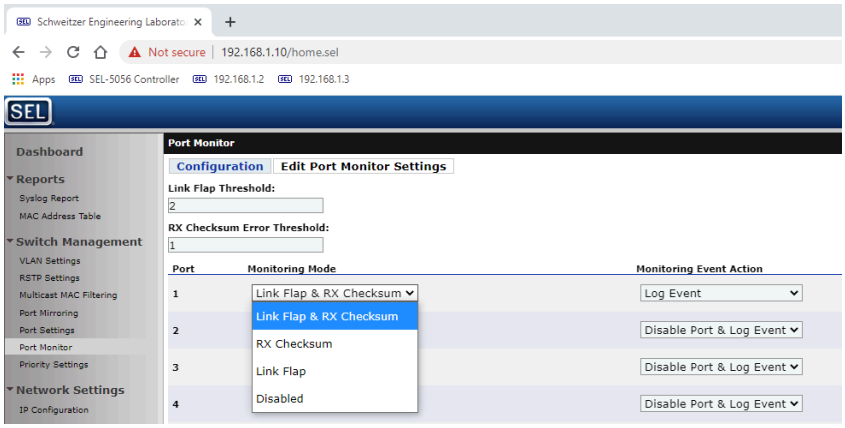


Figure 5.17 Port Modes

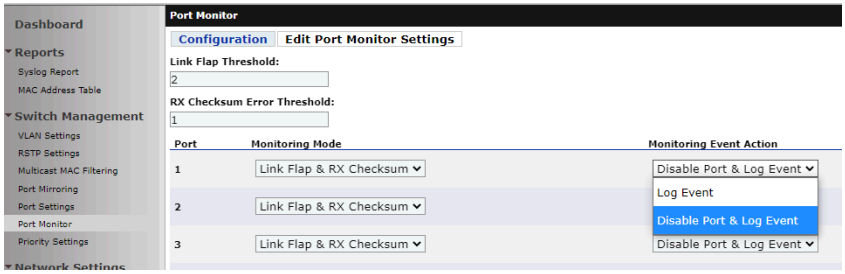


Figure 5.18 Port Actions

Port Settings

The **Port Settings** page provides you the ability to enable and disable ports, set an alias for a port, configure port speed and duplex mode, and configure Rating Limiting protection. The device configures fiber ports automatically to their maximum speed and sets these to full duplex. The device sets copper ports to Auto as their default setting for speed and duplex values, but you can configure these as necessary.

Rate Limiting

The SEL-2730M allows you to set the maximum data rate for either ingress (incoming) or egress (outgoing) traffic for any of the device ports slider controls on the **Switch Management/Port Settings** page. This allows you to prevent malicious or faulty devices from flooding your network and blocking access to network resources. *Figure 5.19* shows how limiting can be configured for each port.

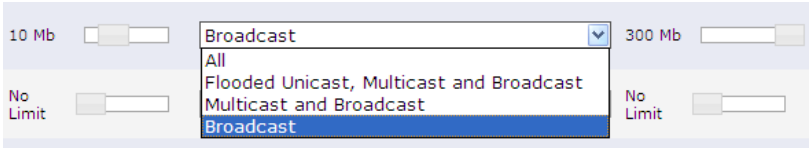


Figure 5.19 Setting Rate Limiting on the Port Settings Page

The Ingress Rate limit can be set using a slider control to **1**, **5**, **10**, **20**, **30**, **42**, **50**, **75**, **100**, **150**, or **300** Mbps, as appropriate for the link speed of the port, or can be set to **No Limit**. For the Ingress traffic, the limit can be set to **All** traffic, **Broadcast**, or mixes of unicast, broadcast, and multicast. The Egress Rate is applied to the overall rate (all traffic from the port).

Priority Settings

Priority settings control the egress order of frames out of a port by using the transmission policy and the assigned priority of each frame, which is based on the priority code point (PCP), differentiated service code point (DSCP), or a default value.

Settings

There are three groups of settings (described in *Table 5.5*): one to control the order in which frames are transmitted from a port, one to configure the PCP-to-priority mapping, and one to configure the DSCP-to-priority mapping.

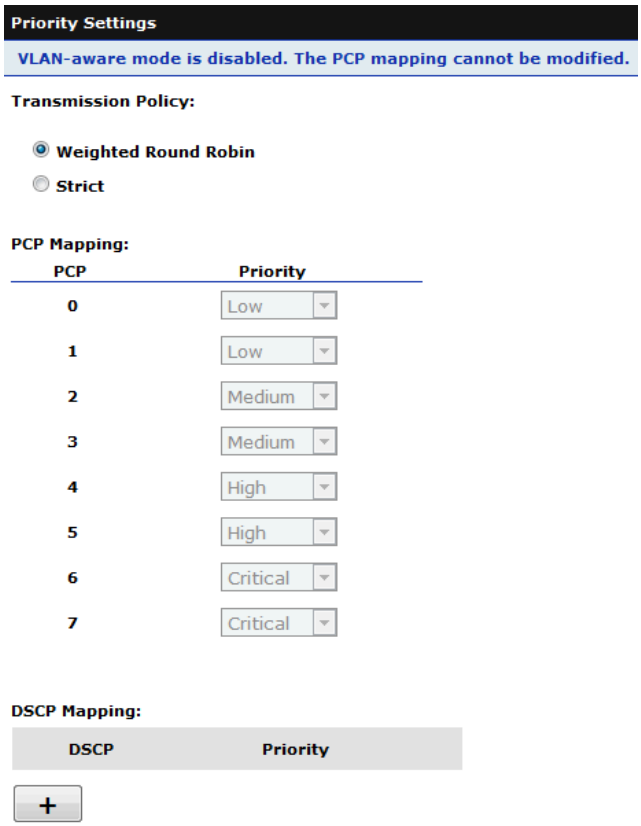


Figure 5.20 Priority Settings Page (Default Settings)

Table 5.5 Priority Settings

Setting	Valid Values	Default Value	Rules	Description
Transmission Policy	Weighted Round Robin, Strict	Weighted Round Robin	—	Sets the transmission policy for all SEL-2730M ports.
PCP Mapping	Priority: Low, Medium, High, Critical	See *Table 5.6*	Disabled if VLAN-aware is disabled.	Sets the priority for each PCP value for all SEL-2730M ports.
DSCP Mapping	DSCP: 0–63 Priority: Low, Medium, High, Critical	Empty	If the DSCP Mapping table is empty, then the DSCP field is ignored (ToS Inspection disabled). Otherwise, DSCP values not explicitly specified are mapped to Low.	Sets the priority for each DSCP value for all SEL-2730M ports.

The SEL-2730M supports two transmission policies to decide which packet to egress first when packets of more than one priority are waiting to egress: strict and weighted round robin (WRR). Strict always egresses higher-priority packets before lower-priority packets, and WRR uses an 8:4:2:1 allocation. Packets of the same priority egress in the order in which the SEL-2730M adds them to the queue.

There are eight PCP values (0–7) defined by IEEE 802.1D and IEEE 802.1Q. The PCP Mapping setting is a fixed table with a row for each possible PCP value. If VLAN-aware is enabled, you can modify the priority for each PCP value. By default, the SEL-2730M assigns the PCP to the priority listed in *Table 5.6*. This mapping applies to all SEL-2730M ports.

Table 5.6 Default PCP-to-Priority Mapping

PCP	Priority
0	Low
1	
2	Medium
3	
4	High
5	
6	Critical
7	

There are 64 DSCP values (0–63). The DSCP uses the Type of Service (ToS) field in the IP header as defined by the DiffServ standard RFC2475. If the DiffServ-to-Queue Mapping table is empty, the SEL-2730M ignores the DSCP field in the packet (ToS Inspection is disabled). To add a new mapping point, select the plus (+) button, select a DSCP value from 0–63 that is not already present and a Priority of Low, Medium, High, or Critical (as shown in *Figure 5.21*). Select the ✖ button to remove a mapping point.

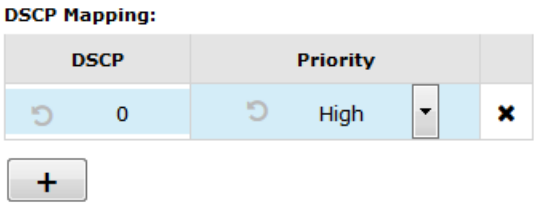


Figure 5.21 Adding a DSCP Mapping Point

The SEL-2730M does not have an explicit ToS Inspection setting. Instead, the SEL-2730M enables ToS Inspection automatically if the DSCP mapping has at least one row, and disables ToS Inspection automatically if the DSCP mapping has zero rows.

Priority Behavior

Internally, the SEL-2730M supports the following four priority levels, listed in descending order of precedence:

- Critical
- High
- Medium
- Low

The SEL-2730M determines the priority of a packet at ingress using one of the three sources listed in *Table 5.7*. The VLAN PCP and ToS fields support more than four values, so the SEL-2730M must map those values to its internal four priority levels. *Table 5.7* lists what sources use which mappings.

Table 5.7 Priority Sources

Source	Mapping
PCP field	PCP
ToS field	DSCP
Port Default	None; always Low

The SEL-2730M uses the process shown in *Figure 5.22* to determine the priority of a packet. As shown, the ToS field is used only for tagged IP packets if VLAN-aware is disabled and ToS Inspect is enabled.

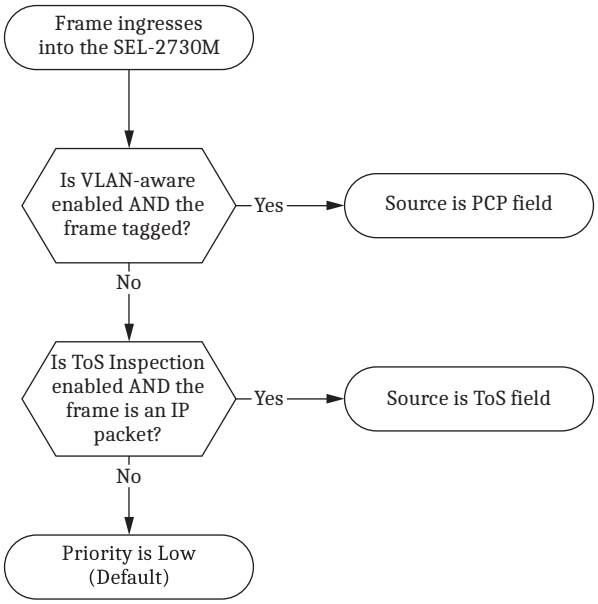


Figure 5.22 Priority Determination for a Frame

The SEL-2730M supports four priority queues, one for each priority level. When the SEL-2730M forwards a frame to a port for egress, it places the frame in the appropriate priority queue based on the priority assigned at ingress (see *Figure 5.22*). The priority of a packet only determines into which priority queue the packet is placed. The transmission policy setting determines which packet to egress first when packets of more than one priority are waiting to egress. Packets of the same priority egress in the order in which they were forwarded to the port. The transmission policy considers the priority of packets only and not their priority source (as shown in *Table 5.7*).

The SEL-2730M does not modify the ToS field of an IP packet or the PCP field of a frame that was already tagged at ingress. If the SEL-2730M tags a packet, it sets the PCP field to 0 unless the packet is an IP packet and the ToS Inspection is enabled, in which case the SEL-2730M sets the PCP field based on the priority mapped to the DSCP value of the frame, as shown in *Table 5.8*.

Table 5.8 DSCP Mapped Priority to PCP

Priority Mapped to DSCP Value of the Packet	Value Written to PCP Field at Egress
Low	0
Medium	2
High	4
Critical	6

Network Settings

IP Configuration

The **IP Configuration** page provides the configuration options for the IP settings of the device. ETH F is used for initial commissioning and local access. A second IP interface, under the **Mgmt** section of the page, can be configured to access the device over a local or remote network, as shown in *Figure 5.23*.

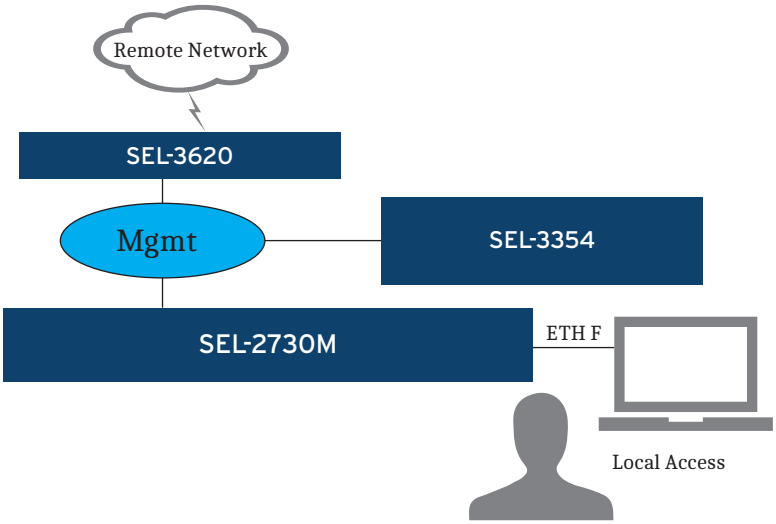


Figure 5.23 IP Configuration

The Mgmt interface is a logical interface accessible through the switch fabric ports. Ports 1–24 are considered the switch fabric ports. **ETH F** is used for local management access and is not considered a switch fabric port. **ETH F** does allow web management or SNMP access if these services are enabled for the front port.

The Mgmt interface is used for services such as remote management of the device, sending Syslog or SNMP traps, and receiving SNMP requests. You can reach the Mgmt interface through the use of devices within the same subnet, or through a router configured with an interface on the same subnet as the Mgmt interface.

Table 5.9 Global IP Settings

Field Name	Values	Default	Description
Hostname[a]	1–63 characters	SEL<SERIAL#>	The unique name identifying the device on the network.
Domain Name[a]	0–253 characters	N/A	The domain name of which the device is a member.
Default Gateway	Unicast network address	N/A	The IP address of the device used to transfer packets to another network. If this setting is left blank, the device will not be able to communicate outside of the local subnet.

[a]The Hostname and Domain Name combined length must be less than 255 characters.

Table 5.10 ETH F Network Interface Settings

Field Name	Values	Default	Description
Alias	1–32 characters	ETH F	A name that is associated with the network interface.
Enabled	Enabled, Disabled	Enabled	Administratively enables or disables the interface.
IP Address	Unicast IP address	192.168.1.2/24	IP address of the interface. The device uses classless inter-domain routing (CIDR) notation to assign the subnet mask.[a]
HTTPS	Enabled, Disabled	Enabled	Enables or disables HTTPS on the interface.
Captive Port	Enabled, Disabled	Enabled	Enables or disables captive port on the interface.
SNMP	Enabled, Disabled	Disabled	Enables or disables the ability to read status data on the SNMP interface.

[a]The IP address and subnet for ETH F cannot be the same as any of the switch ports or of the Management Network Interface.

When captive port is enabled on **ETH F**, the device provides an IP configuration to connected devices that are configured for DHCP. The IP configuration the device issues sets the connected device to use the **ETH F** IP address as the default gateway and DNS server. The configuration of the DNS server on the device resolves any DNS queries to the **ETH F** IP address. This redirects all traffic from connected devices to the **ETH F** IP address. This configuration is useful in the event the **ETH F** IP address is unknown.

Enable the Captive Port feature by connecting a computer configured for DHCP to **ETH F**. Making this connection causes the device to issue the IP configuration for your computer that permits the use of this feature. Simply open your web browser and navigate to any site (e.g., selinc.com); the device resolves this query to the **ETH F** IP address and redirects you to the web management interface of the device. Some devices cache webpages; if the webpage does not appear, try a different webpage or clear the web cache for that web address.

Table 5.11 Mgmt Network Interface Settings[a]

Field Name	Values	Default	Description
Alias	1–32 characters	Mgmt	A name that is associated with the network interface.
Enabled	Enabled, Disabled	Disabled	Administratively enables or disables the interface.
IP Address	Unicast IP address	N/A	IP address of the interface. The device uses classless inter-domain routing (CIDR) notation to assign the subnet mask.
VLAN ID	1–4094	1	The VLAN with which to associate the interface. The VLAN must be present to be selected as the management VLAN. This setting is not visible when the device is not in VLAN-aware mode.
HTTPS	Enabled, Disabled	Disabled	Enables or disables HTTPS on the interface.
SNMP	Enabled, Disabled	Disabled	Enables or disables SNMP on the interface.

[a] If you put the management port on a nondefault VLAN, the switch must restart to complete the settings change.

SNMP Settings

The device supports SNMPv1, SNMPv2c, and SNMPv3 read-only operations. Use SNMP to monitor device health, status, and to gather data. *Figure 5.24* shows the SNMP Settings page.

The SNMP Engine ID for the SEL-2730M is a sequence of 11 bytes consisting of 80 00 7C 4F 03, followed by the MAC address of the unit. Example: For a unit with MAC address of 00:30:A7:04:5A:CF, the SNMP engine ID would be (shown in hexadecimal) : 80 00 7C 4F 03 00 30 A7 04 5A CF.

Figure 5.24 SNMP Settings Page

SNMP is disabled by default. You must enable SNMP on the Mgmt interface for the device to respond to SNMP communications. Refer to *IP Configuration on page 78* for information on how to enable SNMP.

The **Permitted Hosts** section on the page displays the hosts or networks allowed SNMP communications with the device. The device will accept SNMP requests from all IP addresses, unless configured otherwise. The Permitted Hosts list provides the option to limit SNMP communications from known IP address ranges. The Edit Hosts page provides the interface to update the Permitted Hosts list.

The **SNMP Profiles** section on the page displays the SNMP profiles configured on the device. The device requires an SNMP profile for it to respond to SNMP requests. The Add v1/v2c Profile and Add v3 Profile pages provide the interfaces from which you can add SNMP profiles. The SNMP manager requesting SNMP information from the device must be configured with the matching SNMP profile information for the device to respond to the SNMP requests. The device supports as many as eight SNMP profiles.

The **Trap Servers** section on the page displays the SNMP trap servers to which the device is configured to send SNMP traps. An SNMP profile with trap permission is necessary prior to configuring a trap server. The Add Trap Server page provides the interface from which you can add a trap server. The SNMP manager must be configured with the matching SNMP trap profile for the SNMP manager to accept the SNMP traps.

Descriptions follow for each of the pages under SNMP Settings.

Edit Hosts

The **Edit Hosts** page allows you to add or remove hosts or networks from the Permitted Hosts list. Perform the following steps to add a host or network:

Step 1. From the **SNMP Settings** page, select **Edit Hosts**. This will take you to the page shown in *Figure 5.25*.

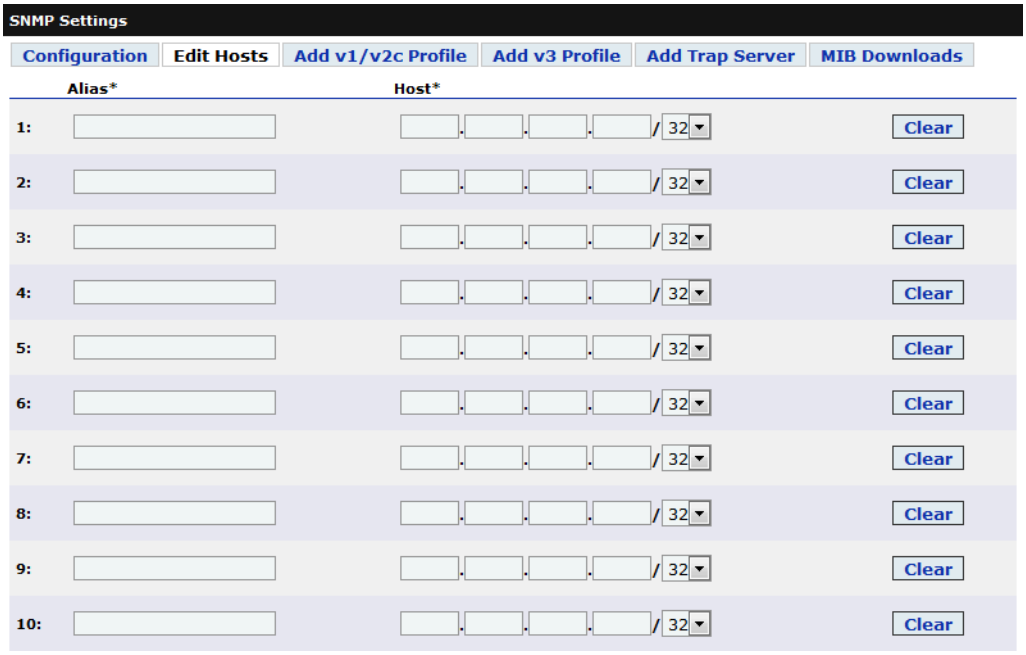


Figure 5.25 Edit Hosts

Step 2. Enter the alias you would like to use for the host or network you will be adding.

Step 3. Enter either the host IP address or network ID under the **Host** field.

Host IP addresses use a /32 CIDR notation. For example, if the IP address of the SNMP manager for which you would like to allow SNMP access to this device is 192.168.10.10, you would enter 192.168.10.10/32 into the **Host** field. A network ID could also be specified to allow access from the network segment that the SNMP manager is on, e.g., 192.168.10.0/24.

Step 4. The **Edit Hosts** page allows you to enter as many as 16 entries on this page.

Step 5. Select **Submit** to complete.

Table 5.12 Edit Hosts Settings

Field Name	Values	Default	Description
Alias	1–32 characters	N/A	A name that is associated with the host or network.
Host	Host IP address (e.g., 192.168.10.10/32) or Network ID (e.g., 192.168.10.0/24)	N/A	IP address or network allowed access to the SNMP service of the device.

Add v1/v2c Profile

The **Add v1/v2c Profile** page allows you to add an SNMPv1/SNMPv2c profile. You may use v1/v2c version formatted reads. Traps use v2c version formatting. Perform the following steps to add an SNMPv1/SNMPv2c profile:

Step 1. From the **SNMP Settings** page, select **Add v1/v2c Profile**. This will take you to the page shown in *Figure 5.26*.

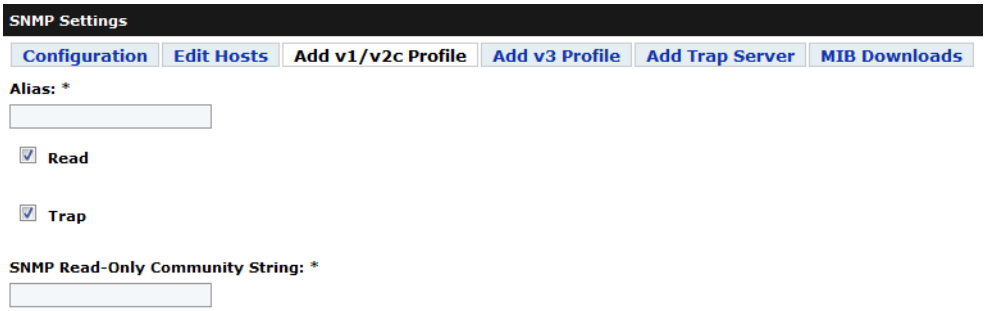


Figure 5.26 Add v1/v2c Profile

Step 2. Enter the **Alias** you would like to use for the SNMP profile.

Step 3. Select whether the SNMP profile should have **Read**, **Trap**, or both permissions.

Step 4. Enter the **SNMP Read Only Community String**.

Step 5. Select **Submit** to add the SNMP profile.

Add v3 Profile

The **Add v3 Profile** page allows you to add an SNMPv3 profile. Perform the following steps to add an SNMPv3 profile:

Step 1. From the **SNMP Settings** page, select **Add v3 Profile**. This will take you to the page shown in *Figure 5.27*.

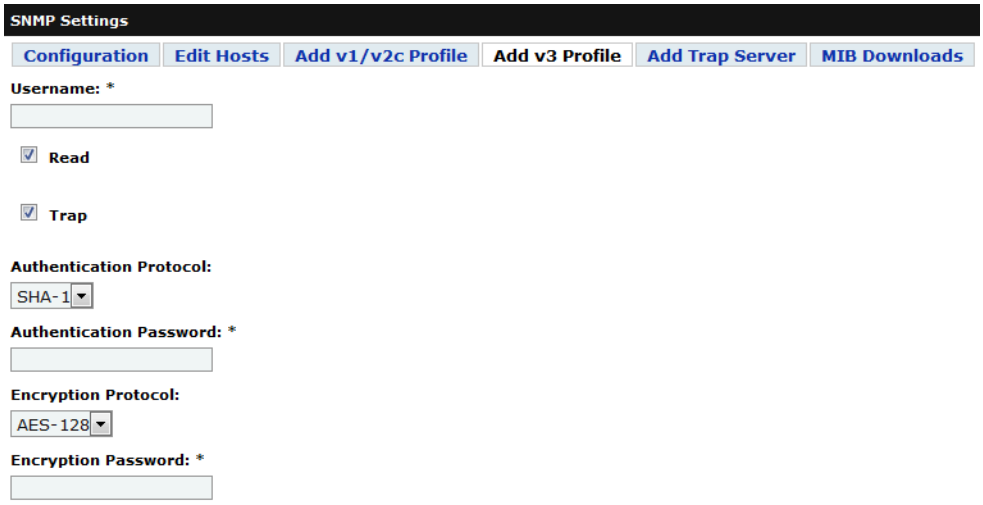


Figure 5.27 Add v3 Profile

Step 2. Enter the **Username** you would like to use for the SNMPv3 user.

Note: SNMPv3 provides optional authentication and encryption to ensure a secure SNMP communications channel. SHA-1 Authentication Protocol and AES-128 Encryption Protocol is recommended. SNMPv1/SNMPv2c provides mutual authentication through the use of a preshared key and the SNMP Read Only Community String, but SNMP communication, including the community string, is not encrypted and appears as plaintext.

NOTE
The encryption algorithm DES is deprecated and should not be used for an encryption protocol. Migrate all systems to AES-128.

Step 3. Select whether the SNMP user should have **Read**, **Trap**, or both permissions.

Step 4. Specify the **Authentication Protocol**, **Authentication Password**, **Encryption Protocol**, and **Encryption Password**.

Step 5. Select **Submit** to add the SNMP profile.

Table 5.13 SNMPv1/SNMPv2c Profile Settings

Field Names	Values	Default	Description
Alias	1–64 characters	N/A	SNMPv1/SNMPv2c alias
Read	Enabled, Disabled	Enabled	Profiles with read permission selected can read SNMP information from the device
Trap	Enabled, Disabled	Enabled	Profiles with trap permission selected can be configured to send SNMP traps from the device
SNMP Read Only Community String	1–128 characters	N/A	The read-only community string used to authenticate SNMP sessions

Table 5.14 SNMPv3 Profile Settings

Field Name	Values	Default	Description
Username	1–64 characters	N/A	SNMPv3 username
Read	Enabled, Disabled	Enabled	Profiles with read permission selected can read SNMP information from the device
Trap	Enabled, Disabled	Enabled	Profiles with trap permission selected can be configured to send SNMP traps from the device
Authentication Protocol	None, MD5, SHA-1	SHA-1	Authentication protocol to use for authenticating SNMP messages between this SNMP user and SNMP manager
Authentication Password	8–128 characters	N/A	Cannot be the same as the Encryption Password
Encryption Protocol	None, DES[a], AES-128	AES-128	Encryption protocol to use for encrypting SNMP messages between this SNMP user and SNMP manager
Encryption Password	8–128 characters	N/A	Cannot be the same as the Authentication Password

[a] Do not use DES for the encryption protocol.

Add Trap Server

The **Add Trap Server** page allows you to add SNMP trap servers to which the device sends SNMP traps. At least one SNMP profile with trap permission is necessary; otherwise, the page returns the error `At least one SNMP profile must be configured with the Allow Traps permission`.

The device sends traps to all configured trap servers through the use of the SNMP information for the selected profiles. The trap server must have the corresponding information for the profiles to authenticate and accept the traps.

The device supports as many as three trap servers. Perform the following steps to add a trap server:

Step 1. From the **SNMP Settings** page, select **Add Trap Server**. This will take you to the page shown in *Figure 5.28*.

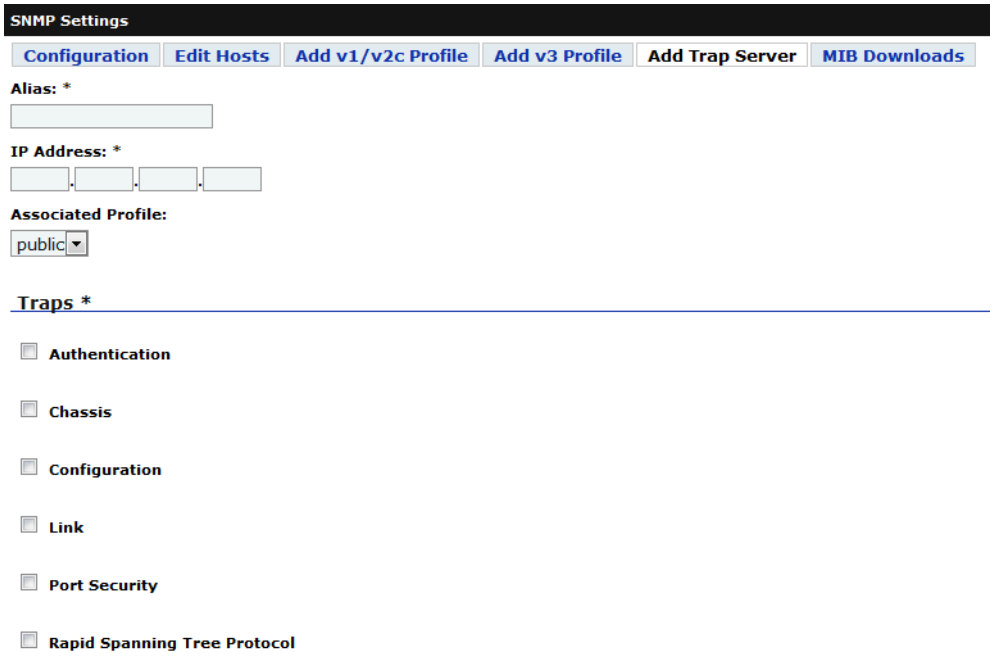


Figure 5.28 Add Trap Server

Step 2. Enter the **Alias** and **IP address** of the trap server to which you would like to send SNMP traps.

Step 3. Select the SNMP profile from the drop-down box whose identity you would like to use to send SNMP traps.

Step 4. Select the SNMP traps you would like to send to the trap server by checking one or more trap categories under **Traps**.

Step 5. Select **Submit** to add the SNMP trap server.

Table 5.15 SNMP Trap Server Settings

Field Name	Values	Default	Description
Alias	1–128 characters	N/A	A name that is associated with the SNMP trap server.
IP Address	Host IP address	N/A	The IP address of the SNMP trap server.
Associated Profile	A list of SNMP profiles with the trap permission	N/A	Any one SNMPv1/SNMPv2c or SNMPv3 profile created on the SEL-2730M.
Traps	See *Table 5.16*.	N/A	The SEL-2730M sends SNMP traps to the configured trap server when an event occurs within selected trap categories.

SNMP traps are categorized based on the type of system event that occurs. Each category is listed below with an explanation of the event types that fall within each category. When an SNMP trap is selected, the device will send that SNMP trap to the configured trap server when an event that falls within the category occurs.

Table 5.16 SNMP Trap Categories

Category	Description
Authentication	Authentication-related events
Chassis	Physical hardware-related events
Configuration	Configuration events related to settings changes
Link	Back port events related to link up/link down status
Port Security	MAC-based port security violations
Rapid Spanning Tree Protocol	RSTP-related events, such as topology changes

MIB Downloads

SNMP Management Information Base (MIB) modules contain definitions and other information about the properties of services and resources of the device. The MIB Downloads page provides a brief description of the MIBs the device uses to provide information through SNMP. You can download MIBs through this page by selecting the **Download** button.

Syslog Settings

Syslog is a specification that describes both the method and format in which the device stores logs locally and routes them to a collector. The device logs many different types of events such as system startup, log in attempts, and configuration changes. The device can send log information to as many as three remote destinations and store as many as 60,000 event logs locally in nonvolatile memory. Each destination, including the local device, has a configurable logging threshold. The device logs all configuration changes to Syslog. For more information about Syslog, refer to *Appendix E: Syslog*.

Select the **Syslog Settings** link from the navigation menu to configure the Syslog settings for the device. The **Syslog Settings** page (see *Figure 5.29*) allows you to configure the logging threshold for local logging and remote Syslog destinations, which determines what severity levels are logged. *Table 5.17* lists what severity levels are logged for each logging threshold. See *Appendix E: Syslog* for a list of Syslog events and their associated severity levels.

Table 5.17 Severity Levels

Logging Threshold	Severity Levels Logged
Alert (Highest Severity)[a]	Alert
Critical[a]	Alert, Critical
Error	Alert, Critical, Error
Warning	Alert, Critical, Error, Warning
Notice	Alert, Critical, Error, Warning, Notice
Informational (Lowest Severity)	Alert, Critical, Error, Warning, Notice, Informational

[a] Not available for Local Logging Threshold.

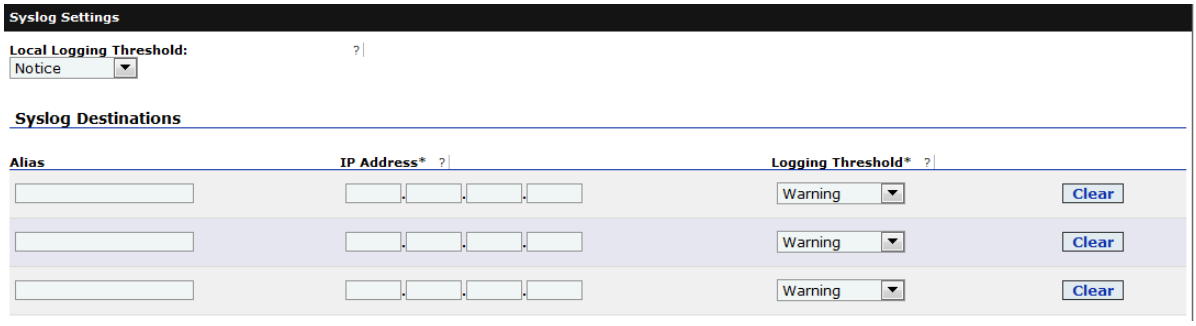


Figure 5.29 Syslog Settings

Table 5.18 Syslog Threshold Values

Field Name	Values	Default	Description
Local Logging Threshold	Error Warning Notice Informational	Notice	Controls the severity levels logged to the device (see *Table 5.17*).

Setting the logging threshold too low can result in the device generating many logs. Setting the logging threshold too high can result in the device failing to record important messages.

The settings under Syslog Destinations are to configure remote Syslog destinations. You can configure as many as three remote destinations. To configure the device to send Syslog events to a remote Syslog server, enter the **Alias** and **IP Address** of the remote Syslog server, and select the logging threshold of the Syslog events to be sent to the remote Syslog server.

Table 5.19 Syslog Destination Settings

Field Name	Values	Default	Description
Alias	0–32 characters		A name that is associated with the Syslog destination.
IP Address	Unicast IP Address		The IP address of the Syslog destination.
Logging Threshold	Alert Critical Error Warning Notice Informational	Warning	Controls the severity levels logged to the device (see *Table 5.17*).

Hosts

To map an IP address to a host name, select the **Add Host** button. This shows the Add Host form (see *Figure 5.30*).

Figure 5.30 Add Hosts Form

Populate the Add Host form with the correct host name and IP address of an LDAP or RADIUS server. The SEL-2730M supports as many as 64 hosts.

Accounts

Local Users

Use the **Local Users** page to add, remove, and update local user accounts for the device. Refer to *Section 3: Managing Users* for more information regarding local user accounts.

Security

X.509 Certificates

HTTPS (SSL/TLS) connections require authentication to confirm that the server with which you are communicating is the correct server. This authentication is through X.509 certificates. By default, the device has a self-signed X.509 certificate that can cause your web browser to issue a security alert. This security alert will require a security exception for authentication to continue. To prevent this security alert from appearing, install a CA-signed X.509 certificate on the device. If your web browser has been configured to trust the CA issuing and signing the certificate, the X.509 certificate will be trusted and the security alert will no longer appear.

The device supports one X.509 certificate that is used for HTTPS communications between the client web browser and the web server running on the device. The X.509 Certificates page has options to view, rename, export, import, and regenerate the X.509 certificate. Descriptions follow for each of these options.

LDAP and RADIUS also use X.509 certificates.

View

This option provides a detailed view of the installed certificate.

Rename

This option provides a form for renaming the certificate. The Certificate Name can contain as many as 128 characters.

Figure 5.31 Renaming Certificates

Import

This option provides a form to import a certificate generated or signed externally to the device. You must enter the password for the private key during import if the private key is encrypted.

For more information on X.509 certificates, see *Appendix I: X.509*.

MAC-Based Port Security

MAC-based port security has two modes: Static and Dynamic. Static mode has a source MAC list for each port and only allows incoming packets from MAC addresses on the list for the given port. Once a MAC address is listed for a port running in Static mode, that MAC address is not allowed on any other port regardless of what mode that port is operating in. Dynamic mode also has a MAC list but instead of per port like Static mode, the Dynamic mode list is for the switch. Dynamic mode configuration is still performed per port but the MAC addresses authorized per port are allowed on any port operating in Dynamic mode or unsecure mode. Static mode is sometimes referred to in the industry as "sticky" and Dynamic mode as "non-sticky" MAC filtering. When enabling MAC-based port security, the MAC table for the port is flushed and authorized MAC lists must be configured. When changing from Static to Dynamic modes, the authorized MAC list for that port is retained and those MAC addresses are added to the Dynamic authorized MAC list. When changing from Dynamic mode to Static mode, the MAC list is flushed for that port but the Dynamic MAC list is retained. When using the automated learning modes, it may be possible to drop the first ingress packet. The device provides two methods of dynamically building the MAC filter for a port and an additional method to statically assign MAC addresses to the filter. The methods for dynamically building the MAC filter for a port include count lock and time lock. You can use all methods independently or in conjunction to build the MAC filter for the port.

For example, you can specify that you would like to learn five MAC addresses for the port and lock in the configuration. You can also specify that you would like to learn five MAC addresses for ten minutes, and the configuration will either lock after five addresses have been learned, or ten minutes have elapsed. You can also choose to statically configure the MAC filter on the port by manually entering one or more MAC addresses.

MAC-Based Port Security Configuration

Select the **Edit** button for the port on which you would like to configure MAC-based port security. This will open the MAC security configuration form for the port.

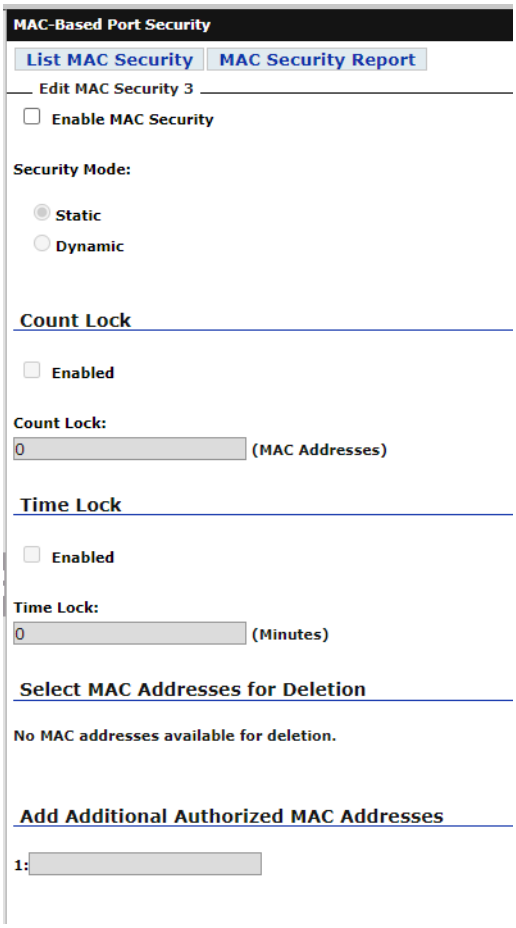


Figure 5.32 MAC-Based Port Security

Enable MAC Security

Selecting this will enable MAC security for the port and allow editing of the fields on the form. Configure the MAC security filter based on your configuration needs. The fields on the form are described in *Table 5.20*.

Table 5.20 MAC Security Fields

Field Name	Values	Description
Count Lock	0–1000 MAC Addresses	The number of MAC addresses that will be added to the filter.
Time Lock	0–1440 Minutes	Time period in which new MAC addresses may be added to the filter.
Select MAC Addresses for deletion	Unicast MAC Address	Field to remove MAC addresses from the filter.
Add additional whitelist MAC Addresses	Unicast MAC Address	Field to add MAC addresses to filter.
Mode	Static or Dynamic	MAC filter mode on which the port will operate.

The device supports a maximum of 1000 MAC address entries across all ports.

MAC Security Report

The **MAC Security Report** page provides an overall view of the status of each port and the MAC addresses locked on each port.

System

Global Settings

Web Settings

The web settings allow for modification of settings related to the web management interface of the device.

Table 5.21 Web Settings

Field Name	Values	Default	Description
Language	English, Spanish	English	The default language for the device.
Maximum Sessions	1–20	5	Maximum number of concurrent web user sessions.
Sessions Timeout	1–60 minutes	5	Amount of time a user's session is inactive before the device terminates the session.

The device automatically selects the language used for the web management interface based on an Accept-Language request-header field from the requesting client web browser. The device defaults to the highest-priority supported language the requesting client web browser lists. In the event of a tie in priorities of supported languages or if none of the requested languages are supported, the language defaults to the Language setting configured in the Global Settings. The SEL-2730M transmits Syslog messages and SNMP traps in the language specified through the Language setting in Global Settings.

System Contact Information

The system contact information settings provide fields for defining a system contact and system location.

Table 5.22 System Contact Information Settings

Field Name	Values	Default	Description
Contact	0–128 characters	Schweitzer Engineering Laboratories, Inc. (509) 332-1890	Contact information for the device.
Location	0–128 characters	Pullman, WA	Location of the device.

Table 5.23 Features

Field Name	Values	Default	Description
VLAN-aware	Enabled, Disabled	Disabled	Determines the operational mode of the device with respect to VLANs .
Spanning Tree Mode	RSTP, Off	RSTP	Configures the spanning tree mode for the device. The device does not provide network loop prevention if this setting is disabled.
LLDP	Enabled, Disabled	Enabled	Enables or disables Link Layer Discovery Protocol (LLDP) on the device.

Date/Time

The date and time functions of the device allow accurate timekeeping for time-stamping internally generated system events. The date and time of the device can be manually set, or the device can synchronize its internal clock to Network Time Protocol (NTP) servers over the network. One benefit of synchronizing time by using NTP is that all devices synchronized to the NTP servers share the same time, and event correlation across multiple systems is possible. Having the same time reference for time-stamped events makes auditing system and security events across multiple systems easier to manage.

Manually Updating Date/Time

The device provides an extensive time zone list to allow you to select the time zone appropriate for your location. Identification of many of these time zones is according to cities that lie in those zones, while common time zone names, such as Coordinated Universal Time (UTC), identify others. Time zone selection is important in how the SEL-2730M determines daylight-saving adjustments. To select a time zone, find the appropriate time zone entry in the **Time Zone** drop-down list, and select the **Submit** button.

Note: Updating the time zone or time may cause the web management session to expire. You will need to log back onto the device after changing the time zone or time.

In installations where NTP sources are unavailable, manual date and time configuration is necessary. To manually configure the date and time of the device, select the current date from the calendar, enter the current time, and select the **Submit** button.

NTP

NTP is a method for synchronizing system clocks over IP networks. NTP typically maintains accuracies of 10 ms across public networks and 200 μs or better in private networks under ideal conditions.

NTP uses a hierarchical, layered "stratum" system of clock source levels. Stratum numbering begins with zero at the top and increments with layers from the reference clock. The stratum scheme exists to prevent cyclical dependencies in the hierarchy. A lower stratum number for the NTP source does not necessarily mean it is more accurate.

The SEL-2730M uses NTP version 4.0 and is backward-compatible with older versions, including NTPv3 and NTPv2, but not NTPv1.

To use NTP as the time source for the device, you must select **Enable NTP Client** and specify at least one NTP Server, as shown in *Figure 5.33*. Replace 192.168.100.1 with the IP address of your NTP server, and select the **Submit** button.

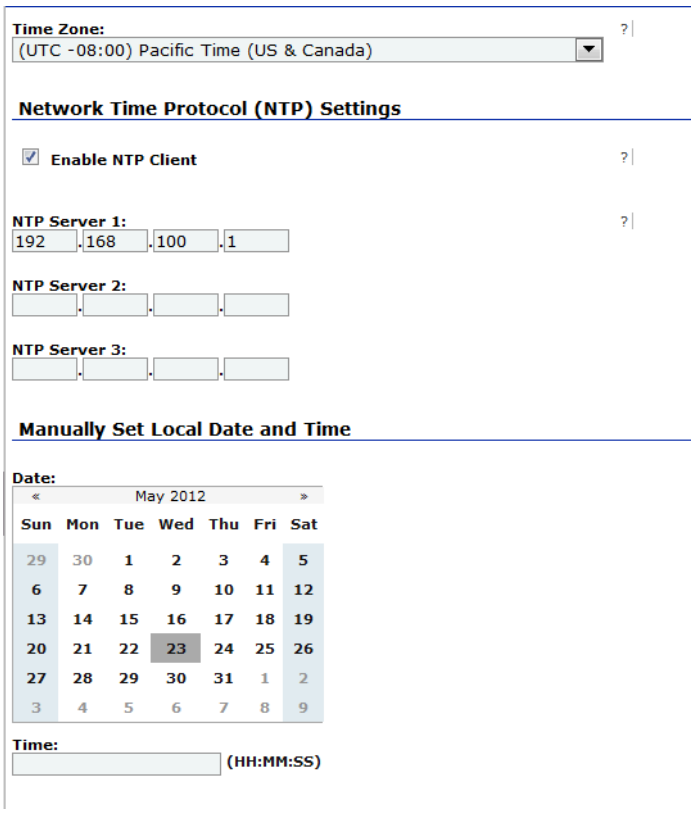


Figure 5.33 Date/Time Settings

Alarm Contact

Each SEL-2730M has one alarm contact output that can be used to alert system personnel about system- or security-related events. The events are divided into seven categories (described in *Table 5.24*) that can either be configured with one of three alarm contact behaviors (described in *Table 5.25*) or disabled so that the SEL-2730M does not operate the alarm contact for those events. The alarm contact on and off duration for latching and pulsing are configurable, as described in *Table 5.27*. These durations apply to all pulsing and latching events.

Settings

There are three groups of settings: one to enable the event categories (see *Table 5.24*), one to select the alarm contact behavior (see *Table 5.25*), and one for the on and off durations (see *Table 5.27*).

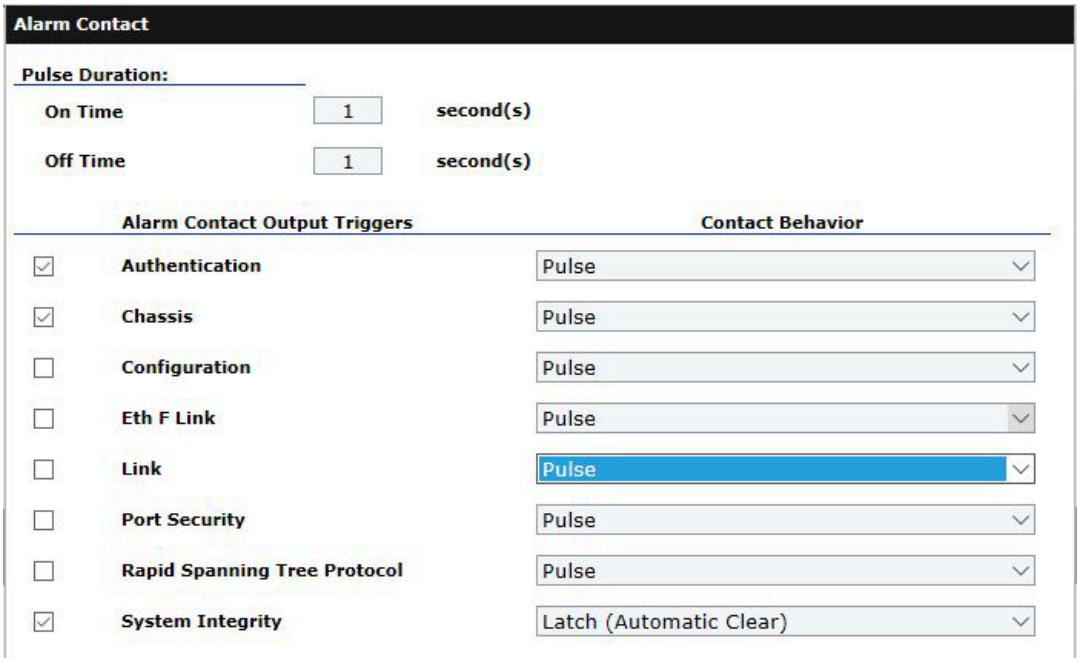


Figure 5.34 Alarm Contact Page (Default Settings)

Table 5.24 Alarm Contact Categories

Category	Default Enable Setting	Default Contact Behavior	Description
Authentication	Enabled	Pulse	Authentication-related events
Chassis	Enabled	Pulse	Physical hardware-related events
Configuration	Disabled	Pulse	Configuration events related to settings changes
Eth F Link	Disabled	Pulse	Front-port interface events related to link up/link down status.
Link	Disabled	Pulse	Interface events related to link up/link down status
Port Security	Disabled	Pulse	MAC-based port security violations
Rapid Spanning Tree Protocol	Disabled	Pulse	RSTP-related events, such as topology changes
System Integrity	Enabled	Latch (Automatic Clear)	System event, such as component failure or a part number change (also referred to as Major Alarms)

Table 5.25 Alarm Contact Behaviors

Behavior	Description
Pulse	The alarm contact asserts for the on time and then deasserts for the off time.
Latch (Manual Clear) or Latch (Automatic Clear)	The alarm contact asserts for at least as long as the on time. The alarm contact then deasserts for at least as long as the off time after the user manually clears the alarm via the web interface for both types of latches. Automatically clearing latches are automatically cleared if the underlying cause of the event is resolved. If cleared during the on time period, the alarm contact deasserts immediately after the on time expires.

The Latch (Automatic Clear) behavior depends on the category of the alarm, as shown in *Table 5.26*.

Table 5.26 Latch (Automatic Clear) Behavior

Alarm Category	Alarm Is Automatically Cleared When...
Authentication Chassis Configuration	Alarm is manually cleared. SEL-2730M is turned off and back on
Eth F Link	Front port is up
Link	All enabled back ports are up[a]
Port Security Rapid Spanning Tree Protocol	Alarm is manually cleared SEL-2730M is turned off and back on
System Integrity	Alarm is manually cleared[b] SEL-2730M is turned off and back on[b] The underlying cause is corrected (e.g., the battery is replaced)

[a] Latching is caused by at least one port being down but enabled. The Latch will remain asserted until all links are up and On Time and Off Time shall be honored. For example, if 10 ports lose their link (link down), and 5 of those ports recover their link, the alarm remains latched. Once the last five ports recover their link, the alarm autoclears as the On Time and Off Time are honored.

[b] The alarm reasserts if the underlying cause is still present during the next diagnostics cycle, e.g., if the battery is still missing.

Table 5.27 Pulse Duration Settings[a]

Setting	Default	Range	Description
On Time	1 s	1–10 s	Minimum duration for which the alarm contact asserts.
Off Time	1 s	1–10 s	Minimum duration for which the alarm contact deasserts.

[a] These apply to latching events as well as pulsing events.

To enable a category, select the check box to the left of the category name. To change the behavior of the alarm contact for that category, use the drop-down box to the right of the category name.

System Integrity alarms representing diagnostics are pooled once per cycle. If the alarm is manually cleared and the underlying cause persists, the configured alarm contact behavior event reoccurs.

For both Link Alarms (Link: Eth F or Link: Ports 1–24), there are no warnings to the user when they enable a Link alarm when the physical port is disabled. For example, if Link alarm for Eth F is enabled but in the IP Configuration, the physical Eth F is disabled, the user will not be warned and Eth F will never trigger a Link alarm. This is true for Ports 1–24 as well. If Ports 13–24 are physically disabled and the Link alarm for Ports 1–24 are enabled, the user is not warned that some ports are physically disabled, but alarms occur for port activity on the physically enabled Ports 1–12.

Alarm Contact Behavior

If no other event in an enabled event category occurs while the alarm contact is pulsing or latching, the alarm contact follows the behavior described in *Table 5.25*.

If more than one event occurs during the on or off time of a latch or pulse, the alarm contact operates according to the following rules:

- A latching event always interrupts a pulse, regardless of whether the on or off time has expired.
- Pulsing events are ignored during the on time of a pulse or a latch.
- If one or more pulsing events occur during the off time of a pulse or a latch, or if one or more latching events occur and are cleared during the off time of the latch, the alarm contact pulses once more after the off time has expired.
- During a latching event, the alarm contact always asserts for at least the on time and remains asserted until all latching events are cleared, including all latching events that occurred during the on time of the original latching event.
- Once in the off time of a latch, the alarm contact remains deasserted until at least the off time expires, regardless of any pulsing or latching events that occur during this time.

To unambiguously differentiate between a latching event and a pulsing event, use a manually clearing latch behavior. Events are also logged to the Syslog Report page and sent to any configured Syslog servers regardless of the alarm contact settings or behavior.

Usage Policy

The device presents a usage policy to all users accessing the login page. This policy notifies users of what constitutes the appropriate use of this device, what actions are taken to ensure the device is not used inappropriately, and what actions will be taken if abuse is discovered. The device comes with the following default usage policy:

> *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 activity to law enforcement officials.*

The usage policy is configurable from 0 to as many as 4095 characters. Select the **Usage Policy** link from the navigation menu to modify the usage policy.

File Management

File management provides an interface from which you can import and export settings, as well as perform firmware upgrades and download diagnostics reports. Exporting system settings is useful for providing device configuration backups for disaster recovery, as well as creating a template configuration that you can use in commissioning large numbers of devices. For example, if all devices share the same configuration, except for a few device-specific configuration items such as hostname and IP address, the configuration can be created once and then exported as a template. When the configuration file is imported into a new device, only a couple of changes are necessary before the device is fully configured.

Export Settings

Settings can be exported either encrypted or unencrypted in XML format. The encrypted settings export is useful for creating an encrypted copy of the device configuration as a device backup. You can use this backup for disaster recovery purposes in the event the configuration on the device must be restored. The other option is to export the device settings in unencrypted XML format, which allows for offline editing.

Note: Settings files should be stored in a secure location, because they contain sensitive information.

The **Export Settings** page provides an interface to export settings to either an encrypted or unencrypted settings file. Follow the steps below to export a settings file:

Step 1. Log in to the device and browse to the **File Management** page.

You should be on the **Export Settings** page shown in *Figure 5.35*.

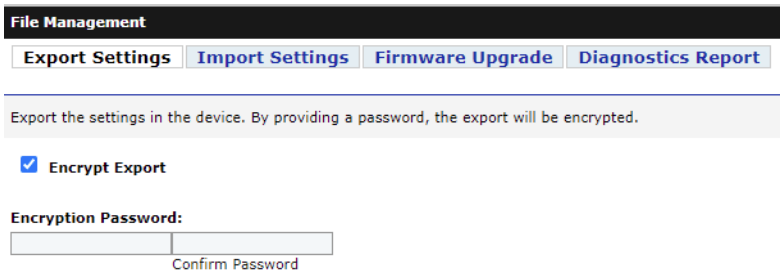


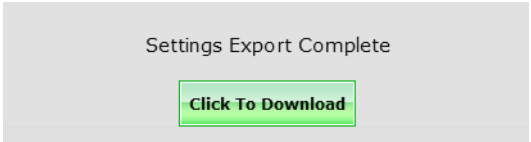
Figure 5.35 Export Settings Page

Step 2. If you would like to export settings in an encrypted format, select the **Encrypt Export** check box and select an encryption password for use in encrypting the settings file. You must use this password when you perform an import of the encrypted settings file, so be sure you store the password in a secure location.

If you would like to export settings in an unencrypted format, clear the **Encrypt Export** check box.

Step 3. Select the **Export** button.

Step 4. The settings export will initialize and show the export progress for each module. The device will present you with the following message when the export is complete.



Step 5. Select the **Click to Download** button. Your browser then downloads the file from the SEL-2730M.

Diagnostics Report

A diagnostics report provides system status, diagnostics, and crash logs to SEL for analysis. Diagnostic reports are encrypted to protect sensitive information.

Step 1. Log in to the device and browse to the **File Management** page.

Step 2. Select **Diagnostics Report**.

Step 3. Select **Generate**.

Step 4. Select **Click to Download** (see *Figure 5.36*) to download the hostname_diagnostics.log file that you can share with your SEL representative.

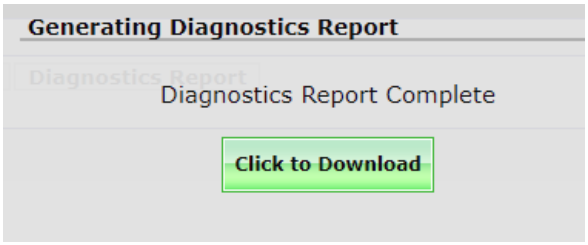


Figure 5.36 Diagnostics Report Complete

Import Settings

Figure 5.37 Import Settings Page

The **Import Settings** page provides an interface to import settings from either an encrypted or unencrypted settings file. Perform the following to import a settings file:

Step 1. Log in to the device and browse to the File Management page.

Step 2. Select the **Import Settings** tab at the top of the page.

> **⚠WARNING**
> Importing settings will replace the current settings and reboot the device.

Step 3. Select **Choose File** and browse to the location of the settings file you would like to import.

Step 4. If the file was encrypted during the export process, enter the encryption password into the **Password** field. If the file was not encrypted during the export process, leave the **Password** field blank.

Step 5. Select the **Import** button.

Firmware Upgrade

The **Firmware Upgrade** page provides an interface from which you can upgrade device firmware. Refer to *Appendix B: Firmware Upgrade Instructions* for more information on the firmware upgrade procedure.

Device Reset

Device Reboot

The device reboot function turns the device off and back on. All communication through the device is lost while the device restarts.

Factory Reset

The device provides the factory-reset function to restore the unit to its factory configuration. You should only use this feature when you decommission the device. The factory-reset function erases the device log files and returns device settings back to the factory-default values. After a factory reset, you must recommission the device. Refer to *Section 2: Installation* for details on commissioning the device.

This page intentionally left blank

SECTION 6

Testing and Troubleshooting

Introduction

This section provides the following guidelines for testing and troubleshooting the device.

Testing Philosophy

Device testing can be divided into three categories: acceptance, commissioning, and maintenance. The categories are differentiated by when they take place in the life cycle of the product and by test complexity. The following paragraphs describe when you should perform each type of test, the goals of testing at that time, and the functions that you need to test at each point.

This information is intended as a guideline for testing a device.

Acceptance Testing

Perform acceptance testing when qualifying the SEL-2730M for use in an Ethernet-based communications network that supports critical systems.

Goals of Acceptance Testing

- ➤ Ensure that the device meets published critical performance specifications.
- ➤ Ensure that the device meets the requirements of the intended application.
- ➤ Improve your familiarity with device capabilities.

What to Test

Acceptance test all settings parameters critical to your intended application. SEL performs detailed acceptance testing on all SEL-2730M models and versions. It is important for you to perform acceptance testing on the SEL-2730M if you are unfamiliar with device operating theory or settings. Such testing helps you ensure that the device settings are correct for your application.

Commissioning Testing

Perform commissioning testing when installing a new device. Commissioning testing is performed on each unit installed.

Goals of Commissioning Testing

- Ensure that power connections are correct.
- Ensure that the alarm output connection is correct.
- Ensure that the device functions with your settings according to your expectations.

What to Test

Perform commissioning testing on all connected Ethernet ports, fiber ports, and alarm contacts.

SEL performs a complete functional check of each device before shipment. Device commissioning tests should verify that the power supply, Ethernet cables, fiber cables, and alarm contacts are connected properly.

Maintenance Testing

The SEL-2730M does not require regular maintenance testing.

LED Indicators

The SEL-2730M has extensive self-test capabilities. You can determine the status of your device by using the indicator lights located on the front or rear panels. These indicators are provided to show whether the device is enabled, whether an alarm condition exists, whether the power supplies are healthy, and to show the speed and link state for each of the communications interfaces. *Figure 6.1* shows the locations of the LED indicators. The rear-panel indicators corresponding to the ones on the front panel operate identically.

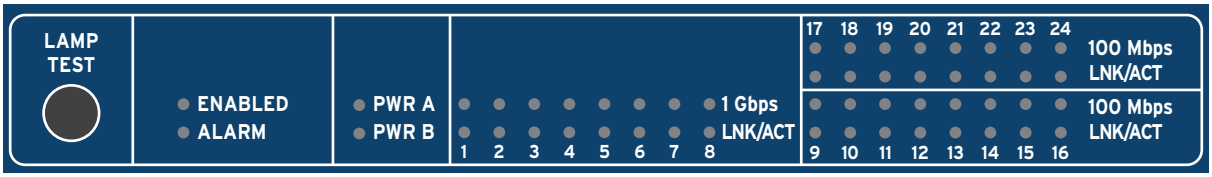


Figure 6.1 Close-Up of Front-Panel Status Indicators

Table 6.1 describes the system status indicators. On the front panel, these are located next to the **LAMP TEST** button.

Table 6.1 System Status Indicators

Indicator	Green Condition	Red Condition
ENABLED	Normal operation	—
ALARM	—	When the alarm contact operates or watchdog timer expires. System is halted or booting, or an error condition has occurred.
PWR A	Power supply installed and working properly	Power supply has failed or is not energized. This will only display when the other power supply is installed and energized.
PWR B	Power supply installed and working properly	Power supply has failed or is not energized. This will only display when the other power supply is installed and energized.

The communications interface indicators in *Table 6.2* are located in two groups, one for Ports 1–8, and the other for Ports 9–24. Ports 1–8 are 1 Gbps ports. The yellow **1 Gbps** speed indicator is illuminated when the port is operating at full speed. When the port is operating at a reduced speed, the indicator is not illuminated. Ports 9–24 are 100 Mbps ports. The yellow **100 Mbps** speed indicator is illuminated when these ports are operating at 100 Mbps, and not illuminated when operating at a reduced speed. For all of these ports (1–24), the same two indicators are provided at the port connector on the rear panel.

Table 6.2 Communications Interface Indicators

Indicator	Not Illuminated Condition	Illuminated Condition
1 Gbps	Port is operating at a reduced speed or is unconnected.	Port is operating at its full speed of 1 Gbps.
100 Mbps	Port is operating at a reduced speed or is unconnected.	Port is operating at its full speed of 100 Mbps.
LNK/ACT	Port is unconnected.	Green when port is connected. Blinks to indicate data traffic in either direction.

Device Dashboard

While the device status indicator lights are useful for getting status information at a quick glance, they will only alert you to simple normal vs. abnormal operating conditions. For more detailed diagnostic information, visit the Dashboard page by selecting the **Dashboard** link from the navigation panel. See *Device Dashboard on page 23* for more information.

Troubleshooting

Inspection Procedure

Complete the following procedure before disturbing the device. After you finish the inspection, refer to *Table 6.3*.

Step 1. If the web interface is accessible, record the part number, serial number, and firmware version from the Dashboard Device Information table.

Step 2. Record a description of the problem encountered.

Step 3. Examine the System Statistics and Diagnostics tables and record any values that are unusual.

Step 4. Measure and record the power supply voltage at the power input terminals.

Step 5. Record the state of the LED indicators.

Table 6.3 Troubleshooting Procedure

Problem	Possible Causes	Solution
The **PWR A** and **PWR B** indicators are both dark	Input power is not present.	Verify that input power is present and that the power supply assembly is fully inserted.
The login page is inaccessible	The computer trying to connect to the web interface is not on the correct network.	Verify the physical and logical connection between the management computer and the SEL-2730M. Configure the IP address of the management computer to the same network as the SEL-2730M, or set the computer network interface to autoconfigure the network by using DHCP as described in *Section 2: Installation*.
	The **ETH F** network interface on the SEL-2730M is not enabled.	Insert a small tool such as a paperclip into the pinhole reset above Port 2 on the rear panel of the device, and depress the reset button for 5 seconds. This will enable the interface and turn on the Captive Port feature to allow you to connect to the management interface by using **ETH F**. See *Section 2: Installation* for details.
No Syslog messages	The Syslog server is not reachable from the network containing the SEL-2730M.	Ensure that the Syslog server IP address is valid and reachable. If the Syslog server is on another network, ensure that a network gateway is configured and available to route the Syslog traffic.
	No Syslog servers defined or the logging threshold is unexpectedly high.	Navigate to the Network Settings/Syslog Settings page and ensure that the proper Syslog IP address and Logging Threshold settings are made there.
A user cannot log in	The user's account is missing.	Log in to the SEL-2730M as an administrator and verify the details for the subject account on the Accounts/Local Users page.
	The user's password is incorrect.	Check that Caps Lock is not active on the computer logging in. If necessary, reset the user's account from the Local Users page.

If You Forget Your SEL-2730M IP Address

If you forget the IP address for which your SEL-2730M is configured, but do not want to perform a full factory reset, the Captive Port feature provides you access to the web management interface.

To activate the Captive Port feature on **ETH F**, while the SEL-2730M is powered on, insert a tool such as a straightened paper clip into the pinhole reset hole above Port 2 on the rear panel and press the recessed reset button for 5 seconds. This enables the front Ethernet port and turns on the Captive Port feature.

The Captive Port feature provides special DHCP and DNS servers to the computer connected to **ETH F**. The DHCP server assigns the computer an IP address adjacent to the IP address of your SEL-2730M, so the computer will be on the same subnet and capable of communicating with it. This also sets the DNS server for the computer to the IP address of your SEL-2730M. Once this occurs, any DNS requests from the computer resolve to the SEL-2730M, so that browsing to any host, such as selinc.com, results in opening the web management interface of your SEL-2730M.

If You Forget Your Administrative Account Password

Use of the Captive Port feature to gain access to your SEL-2730M reestablishes network communication with it, but you must still know the credentials for an administrative account. If you have lost all administrative account credentials, you must perform a full factory-default reset.

Turn off power to your SEL-2730M, insert a tool such as a straightened paper clip into the pinhole reset hole above Port 2 on the rear panel, and press the recessed reset button. Holding the button depressed, apply power. After five seconds, release the recessed reset button.

Wait for the green **ENABLED** LED on the front panel to illuminate, indicating that your SEL-2730M has reset to factory-default settings and is ready. **ETH F** will be enabled, the Captive Port feature will be on, and the IP address for the unit will be 192.168.1.2. You can access the Commissioning page by entering a hostname, such as selinc.com, or you can browse directly to the IP address for the unit at https://192.168.1.2.

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

This page intentionally left blank

APPENDIX A

Firmware and Manual Versions

Firmware

Determining the Firmware Version

To determine the firmware version, log in to the web interface and check the Dashboard page. The Device Information section displays the Firmware Identification (FID) number.

The firmware version will be either a standard release or a point release. A standard release adds new functionality to the firmware beyond the specifications of the existing version. A point release is reserved for modifying firmware functionality to conform to the specifications of the existing version.

A standard release is identified by a change in the R-number of the device FID number.

Existing firmware:

FID=SEL-2730M-**R100**-V0-Z001001-Dxxxxxxxx

Standard release firmware:

FID=SEL-2730M-**R101**-V0-Z001001-Dxxxxxxxx

A point release is identified by a change in the V-number of the device FID number.

Existing firmware:

FID=SEL-2730M-R100-**V0**-Z001001-Dxxxxxxxx

Point release firmware:

FID=SEL-2730M-R100-**V1**-Z001001-Dxxxxxxxx

The Z-number indicates which ACSELERATOR QuickSet SEL-5030 Software version to use.

The date code is after the D. For example, the following is firmware version number R100, release date June 11, 2012.

FID=SEL-2730M-R100-V0-Z001001-**D20120611**

Revision History

Table A.1 lists the firmware versions, revision descriptions, and corresponding instruction manual date codes.

Starting with revisions published after March 1, 2022, changes that address security vulnerabilities are marked with "[Cybersecurity]". Other improvements to cybersecurity functionality that should be evaluated for potential cybersecurity importance are marked with "[Cybersecurity Enhancement]".

Table A.1 Firmware Revision History

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-2730M-R112-V3-Z010001-D20250217	Includes all of the functions of SEL-2730M-R112-V2-Z010001-D20240626 with the following addition: ➤ Addressed an issue where under certain conditions the SFP ports did not transition to the proper RSTP states.	20250217
SEL-2730M-R112-V2-Z010001-D20240626	Includes all of the functions of SEL-2730M-R112-V1-Z010001-D20240130 with the following addition: ➤ Addressed an issue where the static MAC security was not generating a log when an authorized MAC address was connected to the wrong port.	20240626
SEL-2730M-R112-V1-Z010001-D20240130	Includes all of the functions of SEL-2730M-R112-V0-Z010001-D20230630 with the following addition: ➤ Addressed an issue in handling mismatched RSTP Hello times in a superior switch.	20240130
SEL-2730M-R112-V0-Z010001-D20230630	➤ Added compatibility support for the RTAC Web Proxy. ➤ Updated settings import to disable ports while applying settings. ➤ Updated RSTP to move a port into blocking when it receives a disputed BPDU. ➤ Enhanced RSTP resiliency during network storms.	20230630
SEL-2730M-R111-V0-Z010001-D20230220	➤ [Cybersecurity Enhancement] Added Dynamic MAC-based security mode support.	20230227
SEL-2730M-R110-V1-Z009001-D20250217	Includes all of the functions of SEL-2730M-R110-V0-Z009001-D20210830 with the following addition: ➤ Addressed an issue where under certain conditions the SFP ports did not transition to the proper RSTP states.	20250217
SEL-2730M-R110-V0-Z009001-D20210830	➤ Changes to the VLAN ID or IP address of management interfaces now take effect when the change is submitted. ➤ Added support for auto-negotiation on 1000BASE-X fiber (SFP) ports. ➤ Modified the firmware to make the status of a mirror port target available in the SNMP interface MIB. ➤ Addressed an issue in the System Time Change Syslog message where both UTC and local time were used to describe a manual time change. ➤ Updated the syslog report page to display syslog time stamps in the local time zone. ➤ Removed support for DES encryption protocol option in SNMPv3. ➤ Added a diagnostics report, which will generate a report to help SEL diagnose field issues.	20210830
SEL-2730M-R109-V3-Z008001-D20210826	Includes all the functions of SEL-2730M-R109-V2-Z008001-D20210301 with the following addition: ➤ Addressed an issue in all prior versions of R109 firmware, where under certain network conditions, some SEL-2730M switches may stop processing management traffic and management interfaces may become unresponsive. The device remains in this state until it is restarted.	20210830
SEL-2730M-R109-V2-Z008001-D20210301	Includes all the functions of SEL-2730M-R109-V1-Z008001-D20201123 with the following addition: ➤ Addressed an issue with RADIUS logins where the first login attempt for a given user, whether valid or invalid, could show the dashboard with a partial display in read-only mode.	20210301

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-2730M-R109-V1-Z008001-D20201123	Includes all the functions of SEL-2730M-R109-V0-Z008001-D20201117 with the following additions: ➤ Added a downgrade blocker for the new MOT for the two fiber + two copper ports option. Firmware versions earlier than R109-V1 will not work on this hardware variant. ➤ Added support for an additional copper SFP module.	20201123
SEL-2730M-R109-V0-Z008001-D20201117	➤ Updated to allow selection of multiple ports to mirror. ➤ Added port monitor feature to optionally detect and disable ports with unstable links. ➤ Updated third-party software components. ➤ Addressed an issue present in firmware releases R108-V0 and R108-V1 where, in isolated cases, a device set to a system time prior to 2019 and generating a large volume of syslog messages could experience eventual failure. ➤ Revised so the re-enable port button on the RSTP page is no longer visible for view-only users. ➤ Added support for SEL-supplied copper 10/100/1000BASE-T SFP modules. ➤ Added new ordering option for two fiber-optic ports and two copper ports in a specific bank of four ports. ➤ Updated so ARP responses are limited to enabled, and connected Ethernet interfaces with the appropriate IP address. ➤ Addressed TCP SACK vulnerability. ➤ Addressed jQuery cross site scripting vulnerability.	20201117
SEL-2730M-R108-V1-Z007001-D20200709	Includes all the functions of SEL-2730M-R108-V0-Z007001-D20181228 with the following addition: ➤ Addressed an issue that could cause some SEL-2730M Managed Ethernet Switches to stop processing management traffic under certain network conditions.	20200709
SEL-2730M-R108-V0-Z007001-D20181228	➤ Addressed an issue with the power supply not automatically clearing an alarm once power has been restored. ➤ Added Bridge MIB support. ➤ Added MAC Address table download. ➤ Addressed an issue with the link alarms on the back port automatically clearing. ➤ Created a new Eth F link alarm category for the front port. ➤ Updated third-party software components. ➤ Addressed a security issue with SNMPv3 authentication. ➤ Increased security requirements for cryptography in web browser sessions. Removed TLS v1.0 support permanently. ➤ Addressed an issue where SNMP settings are repeatedly updated, consuming available settings memory and causing the user interface to become unresponsive.	20181228
SEL-2730M-R107-V3-Z006001-D20200714	Includes all the functions of SEL-2730M-R107-V2-Z006001-D20180824 with the following addition: ➤ Addressed an issue that could cause some SEL-2730M Managed Ethernet Switches to stop processing management traffic under certain network conditions.	20200709
SEL-2730M-R107-V2-Z006001-D20180824	Includes all the functions of SEL-2730M-R107-V1-Z006001-D20171031 with the following addition: ➤ Addressed an issue caused by an interaction between the device firmware and the flash hardware.	20180824

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-2730M-R107-V1-Z006001-D20171031	Includes all the functions of SEL-2730M-R107-V0-Z006001-D20170801 with the following additions: ➤ Added RADIUS protocol support. ➤ Enhanced Entity MIB support. ➤ Added UCD MIB support. ➤ Increased diagnostics refresh rate. ➤ Improved RSTP convergence with legacy devices. ➤ Removed TLS v1.0 support. ➤ Updated third-party software components.	20171031
SEL-2730M-R107-V0-Z006001-D20170801	**Note:** This firmware was not production released.	—
SEL-2730M-R106-V1-Z005001-D20180824	Includes all the functions of SEL-2730M-R106-V0-Z005001-D20170314 with the following addition: ➤ Addressed an issue caused by an interaction between the device firmware and the flash hardware.	20180824
SEL-2730M-R106-V0-Z005001-D20170314	➤ Added configurable PCP priority mappings. ➤ Added support for ToS awareness and priority mapping. ➤ Added configurable alarm contact behavior. ➤ Added port alias capabilities on the dashboard. ➤ Updated third-party software components.	20170314
SEL-2730M-R105-V1-Z004001-D20160812	Includes all the functions of SEL-2730M-R105-V0-Z004001-D20160330 with the following addition: ➤ Addressed issue which in previous firmware caused improper RSTP convergence in SFP ports when multiple switches turn on at the same time. ➤ Updated cryptographic library by removing weaker algorithm support.	20160812
SEL-2730M-R105-V0-Z004001-D20160330	➤ Enhanced SNMP to allow operation on the front port. ➤ Improved SFP validation alarm. ➤ Improved RSTP convergence when many ports are disabled.	20160330
SEL-2730M-R104-V1-Z003001-D20141023	Includes all the functions of SEL-2730M-R104-V0-Z003001-D20141014 with the following addition: ➤ Made improvements for manufacturability.	20141014
SEL-2730M-R104-V0-Z003001-D20141014	**Note:** This firmware was not production released. ➤ Removed support for MD5 from TLS/SSL. ➤ Improved fiber ports handling of link state when remote-end device is power cycled and RSTP is enabled. ➤ Improved SEL-2730M RSTP link state handling of rapid-link up/down events. ➤ Improved configuration of disabled fiber ports upon application of device power. ➤ Updated OpenSSL to mitigate the POODLE vulnerability. ➤ Updated web interface to remove host header vulnerability. ➤ Disallowed downgrade below R104 to prevent backward compatibility issues with updated hardware.	20141014
SEL-2730M-R103-V0-Z003001-D20140814	➤ Increased number of VLANs from 256 to 4094. ➤ Enhanced configuration UI for VLAN configuration of ports. ➤ Removed VLAN setting from Multicast MAC Filtering page. ➤ Increased MTU value to 1632 bytes for interoperability with PRP. ➤ Support SNMPv1 requests. ➤ Fixed Traffic disruption on port mirroring settings change. ➤ Fixed GOOSE issue with non-STP BPDU Guard setting on port. ➤ Updated third-party software components.	20140814

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-2730M-R102-V0-Z002001-D20131204	➤ Added support for centrally managed user accounts using LDAP . ➤ Added BPDU Guard feature to protect network topology against unexpected BPDUs. ➤ Added per-port rate limiting features to suppress storms. ➤ Added Far End Fault Indication (FEFI) to better support redundant links. ➤ Removed support for SSLv2. ➤ Fixed intermittent issue with validation of SFP modules.	20131204
SEL-2730M-R101-V0-Z001001-D20121206	➤ Significantly improved performance of RSTP on link changes. ➤ Improved tolerance to connection of incorrect fiber type.	20121206
SEL-2730M-R100-V0-Z001001-D20120611	➤ Initial version.	20120611

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 revisions are listed first.

Table A.2 Instruction Manual Revision History

Date Code	Summary of Revisions
20250217	Section 5 ➤ Updated *Table 5.10: ETH F Network Interface Settings*. Appendix A ➤ Updated for firmware versions R110-V1 and R112-V3.
20250116	Section 1 ➤ Removed DIN-rail mount information in *Dimension Drawing*.
20240626	Appendix A ➤ Updated for firmware version R112-V2.
20240130	Appendix A ➤ Updated for firmware version R112-V1.
20231020	Section 1 ➤ Updated *Switching Latency* in *Specifications*. Section 2 ➤ Updated *Commissioning the Device.* Section 3 ➤ Updated *LDAP*.
20230630	Appendix A ➤ Updated for firmware version R112-V0.
20230227	Appendix A ➤ Revised R111-V0 firmware summary.
20230220	Section 1 ➤ Updated *Compliance* in *Specifications*. Section 5 ➤ Updated *MAC-Based Port Security* in *Security*. ➤ Updated *Figure 5.32: MAC-Based Port Security*. ➤ Updated *Table 5.20: MAC Security Fields*.

Date Code	Summary of Revisions
	Appendix A ➤ Updated for firmware version R111-V0. **Appendix E** ➤ Updated *Table E.3 Event Logs*. **Appendix K** ➤ Added *Appendix K: Cybersecurity Features*.
20221027	**Section 1** ➤ Added UKCA Mark to *Specifications*.
20211227	**Section 1** ➤ Updated *Figure 1.3: Rear-Panel View*. ➤ Updated *SEL-9330-A High-Voltage Power Supply (120–240 Vac, 125–250 Vdc)*, *SEL-9330-C Low-Voltage Power Supply (24–48 Vdc)*, *Front- and Rear-Panel Diagrams*, and *Specifications*.
20210830	**Section 1** ➤ Updated *Product Features*. **Section 5** ➤ Added *Hosts*. ➤ Updated *File Management*. ➤ Updated *Figure 5.34: Export Settings Page*. ➤ Added *Diagnostics Report*. **Appendix A** ➤ Updated for firmware versions R109-V3 and R110. **Appendix E** ➤ Updated *Table E.3: Event Logs*.
20210727	**Section 1** ➤ Updated *Dimension Drawing*. ➤ Updated *Specifications*.
20210630	**Section 1** ➤ Updated *Electromagnetic Compatibility Emissions* in *Specifications*.
20210625	**Section 1** ➤ Updated *Dimension Drawing*. ➤ Updated notes in *Dimension Drawing*.
20210324	**Section 1** ➤ Updated UL listing in *Specifications*.
20210301	**Section 2** ➤ Updated Connecting to the Device. **Appendix A** ➤ Updated for firmware version R109-V2. **Appendix J** ➤ Updated *Table J.1 SEL-2730M Port Number to ifIndex Mapping*.
20201203	**Section 1** ➤ Updated UL listing in *Specifications*.
20201123	**Section 2** ➤ Updated *Figure 2.7: Device Dashboard and Navigation Menu*. **Appendix A** ➤ Updated for firmware version R109-V1.
20201117	**Section 1** ➤ Added port monitoring. ➤ Updated compliance statement for *Figure 1.3: Rear-Panel View*.

Date Code	Summary of Revisions
	Section 3 ➤ Added note regarding Internet-Draft RFC 2307. **Section 4** ➤ Changed *Figure 4.4: RSTP Network Topology* to reflect port number changes. **Section 5** ➤ Added Port Monitor section. **Section 6** ➤ Updated *Table 6.1: System Status Indicators*. **Appendix A** ➤ Updated for firmware version R109. **Appendix E** ➤ Updated Port Mirror log messages in *Table E.3: Event Logs*. ➤ Added Port Monitor log messages to *Table E.3: Event Logs*.
20200805	**Section 1** ➤ Updated *Figure 1.1: Front-Panel View* and *Dimension Drawing*. **Section 2** ➤ Updated *Figure 2.1: Commissioning Network*.
20200709	**Section 1** ➤ Updated list of supported browsers in *Software System Requirements*. **Appendix A** ➤ Updated for firmware versions R107-V3 and R108-V1.
20200402	**Section 1** ➤ Added UL MX certification to *Specifications*.
20190805	**Section 1** ➤ Updated *Specifications*.
20190429	**Appendix A** ➤ Added a new entry under firmware version R108.
20181228	**Section 1** ➤ Added MAC Address Download to *Product Features*. **Section 2** ➤ Updated *Figure 2.7: Device Dashboard and Navigation Menu*. **Section 5** ➤ Added NTP version information. ➤ Updated *Figure 5.30: Alarm Contact Page (Default Settings)*. ➤ Updated *Table 5.24: Alarm Contact Categories*. ➤ Updated *Table 5.26: Latch (Automatic Clear) Behavior*. **Appendix A** ➤ Updated for firmware version R108. **Appendix E** ➤ Updated *Table E.3: Event Logs*.
20180824	**Appendix A** ➤ Updated for firmware versions R106-V1 and R107-V2.
20180622	**Section 1** ➤ Added *Supported Simple Form Factor Pluggable (SFP) Fiber-Optic Ports* in *Specifications*.
20180228	**Section 1** ➤ Updated *Communication Product Testing* in *Specifications*.

Date Code	Summary of Revisions
20171207	**Section 1** ➤ Added RoHS compliance to *Environmental* in *Specifications*.
20171031	**General** ➤ Added *Appendix J: Accessing Port Information Through SNMP*. **Section 1** ➤ Added a note regarding isolation requirements to *Figure 1.3: Rear-Panel View*. ➤ Added RCM Mark to *Compliance* in *Specifications*. ➤ Updated *24/48 Volt Power Supply* under *General > Power Supply* in *Specifications*. ➤ Updated *Power Supply Fuse Ratings* under *General* in *Specifications*. ➤ Updated *Type Tests* in *Specifications*. **Section 2** ➤ Added *Installing a New Web Certificate*. ➤ Updated *System Statistics* in *Device Dashboard*. **Section 3** ➤ Added *RADIUS* to *Centralized User Accounts*. **Section 4** ➤ Updated *Configure VLANs on SEL-2730M-1* and *Configure VLANs on SEL-2730M-2* in *Job Done Example 1*. ➤ Updated *Identifying the Problem* in *Job Done Example 2*. **Section 5** ➤ Updated *Table 5.1: VLAN Settings*, *Table 5.2: RSTP Settings*, *Table 5.3: Port Settings*, *Table 5.18: Syslog Threshold Values*, *Table 5.19: Syslog Destination Settings*, and *Table 5.23: Features*. ➤ Updated *Figure 5.8: Port View*. ➤ Updated *IP Configuration* and *SNMP Settings* in *Network Settings*. ➤ Added *Table 5.4: STP Mode*, *Table 5.17: Severity Settings*, and *Table 5.26: Latch (Automatic Clear) Behavior*. **Section 6** ➤ Updated *Table 6.1: System Status Indicators*. ➤ Updated *Device Dashboard*. **Appendix A** ➤ Updated for firmware version R107-V1. **Appendix C** ➤ Updated *Logging In With SEL User-Based Accounts*. **Appendix E** ➤ Updated *Table E.1: Syslog Message Severities Reported by the SEL-2730M*. ➤ Added *RADIUS* messages to *Table E.3: Event Logs*. **Appendix F** ➤ Updated *Date Link Layer (Layer 2)* and *Transport Layer (Layer 4)* in *OSI Model*.
20170731	**Section 1** ➤ Updated *Type Tests* in *Specifications*.
20170314	**General** ➤ Updated open-source software components to current revisions. **Section 1** ➤ Updated *Connections, Reset Button, and LED Indicators*, *Software System Requirements*, and *Specifications*. **Section 2** ➤ Updated *Figure 2.7: Device Dashboard and Navigation Menu*. **Section 5** ➤ Updated *Switch Management*. ➤ Updated *Table 5.5: ETH F Network Interface Settings*. ➤ Added *Priority Settings*. ➤ Updated *Alarm Contact*.

Date Code	Summary of Revisions
	Appendix A ➤ Updated for firmware version R106-V0.
20160812	**Appendix A** ➤ Updated for firmware version R105-V1.
20160330	**Section 1** ➤ Updated *Specifications*. **Section 4** ➤ Updated *Table 4.2: VLAN 10 Configuration*, *Table 4.3: VLAN 20 Configuration*, and *Table 4.4: VLAN 30 Configuration*. **Appendix A** ➤ Updated to include information on point releases. ➤ Updated for firmware version R105-V0. **Appendix B** ➤ Updated to include information on point releases.
20160218	**Preface** ➤ Updated *Safety Information*. ➤ Added *Trademarks*. **Section 1** ➤ Moved *Open Source Software* to *Preface*. ➤ Updated *Table 1.7: Alarm Contact Ratings*. ➤ Updated *Specifications*.
20150901	**Preface** ➤ Updated *General Safety Marks*. **Section 1** ➤ Added *Open Source Software* subsection. **Section 2** ➤ Added *Battery Change Instructions* subsection.
20150630	**Section 1** ➤ Updated *Specifications*.
20150522	**Section 1** ➤ Updated *Specifications*.
20150325	**Section 1** ➤ Updated *Status Indicators*. **Section 3** ➤ Updated *Figure 3.3– Figure 3.9*. **Section 4** ➤ Updated *Figure 4.2*. ➤ Updated *Job Done Example 3*.
20141218	**Preface** ➤ Updated *Safety Information* **Section 1** ➤ Updated *Specifications*.
20141014	**Appendix A** ➤ Updated for firmware version R104.
20140814	**Section 1** ➤ Updated *Product Features*. ➤ Updated *Specifications*.

Date Code	Summary of Revisions
	Section 2 ➤ Updated *Navigating the User Interface*. ➤ Updated *Device Dashboard*. **Section 4** ➤ Updated *Configure VLANs on SEL-2730M–1*. ➤ Updated *Configure VLANs on SEL-2730M–2*. **Section 5** ➤ Updated *VLAN Settings*. ➤ Updated *Figure 5.14 Add New Filter*. **Section 6** ➤ Updated *Figure 6.2 Device Dashboard*. **Appendix A** ➤ Updated for firmware version R103.
20140425	**Section 1** ➤ Updated *Specifications*.
20131204	**Section 1** ➤ Updated *Product Features*. ➤ Updated *Figure 1.3: Rear-Panel View*. ➤ Updated *Communications Ports* in *Specifications*. **Section 2** ➤ Updated *Figure 2.12: Version Information*. **Section 3** ➤ Added LDAP functionality description and settings. **Section 5** ➤ Updated *Figure 5.13: Port Mirroring*. **Appendix A** ➤ Updated for firmware version R102. **Appendix D** ➤ New appendix with information about LDAP. **Appendix I** ➤ Updated *X.509 Certificates*. ➤ Updated *Digital Signatures*. ➤ Updated *Public Key Infrastructure*.
20130429	**Section 1** ➤ Updated *Figure 1.3: Rear-Panel View*. ➤ Updated Power Supply in *Specifications*.
20130416	**Section 1** ➤ Updated *Specifications*.
20121206	**Appendix A** ➤ Updated for firmware version R101.
20120611	➤ Initial version.

APPENDIX B

Firmware Upgrade Instructions

Introduction

These instructions guide you through the process of upgrading firmware in the device. The firmware upgrade will be either a standard release or a point release. A standard release adds new functionality to the firmware beyond the specifications of the existing version. A point release is reserved for modifying firmware functionality to conform to the specifications of the existing version.

A standard release is identified by a change in the R-number of the device firmware identification (FID) number.

Existing firmware:

FID=SEL-2730M-**R100**-V0-Z001001-Dxxxxxxxx

Standard release firmware:

FID=SEL-2730M-**R101**-V0-Z001001-Dxxxxxxxx

A point release is identified by a change in the V-number of the device FID number.

Existing firmware:

FID=SEL-2730M-R100-**V0**-Z001001-Dxxxxxxxx

Point release firmware:

FID=SEL-2730M-R100-**V1**-Z001001-Dxxxxxxxx

The release date is after the D. For example, the following is firmware version number R100, release date June 11, 2012.

FID=SEL-2730M-R100-V0-Z001001-**D20120611**

Firmware Files

SEL-2730M firmware upgrade files have a tar.gz file name extension. An example firmware filename is install_2730M_R100.tar.gz.

The firmware packages are cryptographically signed to enable the device to recognize official SEL firmware. Any uploaded files that cannot be verified as being produced by SEL will not be processed.

Firmware Upgrade Procedure

To perform an upgrade you will need the appropriate firmware upgrade file and access to an administrative account on the device. Upgrade the device firmware by uploading a file from a personal computer to the device via the web interface. All firmware updates are logged. Perform the following steps to upgrade the SEL-2730M firmware:

Step 1. Log in using an account with administrative-level privileges. Nonadministrative accounts cannot perform firmware upgrades.

Step 2. Select the **File Management** link from the navigation panel. This will show the File Management page, where firmware upgrades may be performed.

Step 3. In the **File Management** window, select the **Firmware Upgrade** button, which will show the version of the currently running firmware and allow you to choose the upgrade file to upload to the unit (see *Figure B.1*).

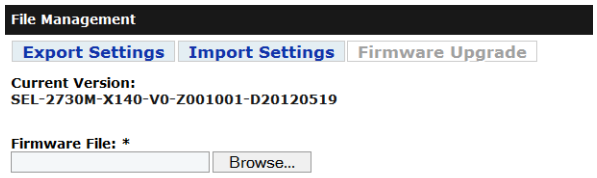


Figure B.1 File Management

Step 4. Enter the path name for the upgrade file. To locate the file instead using the Windows file browser, select the **Browse** button, navigate to the location where the upgrade file is stored, select it, and select **Open**.

Step 5. Select the **Upgrade** button at the bottom of the page to upload and install the new firmware. The **Upgrading Firmware** status display will appear and periodically update the progress of the upgrade operation as it proceeds. Firmware update takes about 10 minutes to complete.

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

APPENDIX C

User-Based Accounts

Introduction

Local accounts are the engineering access accounts that reside on SEL products. SEL has historically used global accounts such as ACC and 2AC and a password associated with each to control access to SEL devices. With global accounts, every user has the same login credentials (username and password), which weakens the security of the system. To strengthen authentication, authorization, and accountability, this SEL product uses a user-based account structure.

Benefits of User-Based Accounts

User-based accounts allow for a stronger security posture than global accounts. One of the drawbacks of global accounts is that when an individual's privileges are revoked, either everyone who uses that account is temporarily without access or there exists an unauthorized individual with secret knowledge that individual can use or sell for malicious purposes. User-based accounts correct this problem with the ability to disable or remove one individual's account without affecting access for anyone else.

Similarly, when password changes are required, either because of a compromised system, routine maintenance, or regulatory requirements, users will not need to remember several new and different global passwords. They will only need to remember their own personal password changes. This increases security by reducing the need to write passwords down and by reducing the chance that an unauthorized individual might obtain an active password.

Three key parts of strong access control are authentication, authorization, and accountability. Authentication is the process of verifying that users are whom they claim to be. This is very difficult to do reliably with global accounts because of the nature of shared passwords. User-based accounts allow for the reliable authentication of individual users of a system. This creates more trust that those who access the system are whom they claim to be.

Authorization is the process of granting privileges to users of a system. You can perform authorization with global accounts when the accounts are organized into access roles, such as with ACC and 2AC. However, unless you have many roles (and, therefore, a large number of shared passwords), it is difficult to assign privileges granularly to global accounts. You can use user-based accounts to assign specific privileges to users of a system.

Accountability is the idea that individual users can be held responsible for their actions on a system. The lack of authentication with global accounts creates too much opportunity to cast doubt on one's activities, making accountability difficult to enforce. The ability to clearly authenticate a user to the individual level allows all actions to be assigned to specific users. Accountability is very important to event tracking and forensic investigations.

Administration of User-Based Accounts

This product comes unconfigured from the factory. This means that there are no user accounts installed. To access the product, you must create an initial account through the commissioning page. This account is authorized to add, remove, enable, and disable system users. Only the individual who creates this account should have knowledge of this account password.

It is possible to create other accounts that can manage users. Only those users with a need to manage user accounts should be a member of the User Manager or Administrator group.

The SEL-2730M stores user accounts in nonvolatile memory. This allows the device to maintain account status through power cycles and other unexpected events.

Acceptable Use Banner

Prior to logging in to this SEL product, any potential user will see a use banner. The use banner is a programmable message indicating what constitutes appropriate use of this device and potential consequences for abusing this device. The default use banner for SEL products is the same as the recommended use banner for the National Institute of Standards and Technology:

> *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 activity to law enforcement officials.*

Logging in With SEL User-Based Accounts

Upon connection to this SEL product, the SEL-2730M directs the user to a login page with a banner and a login prompt. The login prompt includes fields for entering a username and the corresponding password. To log in to the SEL-2730M, the user must enter a valid username and the appropriate password. Usernames are case insensitive and unique to each individual with authority to access the device. Users who enter valid usernames and matching passwords have access to the device.

The SEL-2730M rejects a login attempt and returns an error if the username and corresponding password do not match a local user or if the LDAP or RADIUS server rejects the login attempt (if configured). After three failed login attempts within a one-minute period, this SEL product disallows access attempts with the locked username for 30 seconds. Additionally, the SEL-2730M pulses the alarm contact for one second to provide an alert to the control center that a failed login attempt has occurred (if the Authentication alarm contact category is enabled and set to Pulse). These security features are designed to prevent and slow down password guessing attacks. Login failure can occur if the username or password

is incorrect or the user's account is disabled. Check the spelling of the username and password if an access attempt fails. If you are certain that you entered the username and password correctly, contact your system administrator to verify that your account has not been disabled.

Passphrases

Passphrases provide a user the ability to create strong and easy-to-remember passwords that protect access to a system. A strong passphrase includes many different characters from many different character sets. Longer passphrases provide greater security than shorter passphrases. SEL user-based accounts support complex passphrases that must include at least one character from each of the following character sets.

- Uppercase letters
- Lowercase letters
- Digits
- Special characters

Additionally, passphrases must be at least eight characters in length. Spaces are allowed in passphrases.

Users with administrative access can set or change passphrases for any user of the system. Users without administrative access can only change their own passphrases. For the protection of your account, this SEL product will never display, transmit, or store a passphrase in clear text.

This page intentionally left blank

APPENDIX D

Lightweight Directory Access Protocol

SEL-2730M LDAP Client Implementation

LDAP allows the SEL-2730M to bind with existing centralized account directories, such as Microsoft Active Directory, for user authentication and authorization. SEL's specific LDAP implementation uses the StartTLS method for securing LDAP data from the device to the centralized account server. See *Figure D.1* for information about the LDAP interaction between the SEL LDAP client and the centralized server.

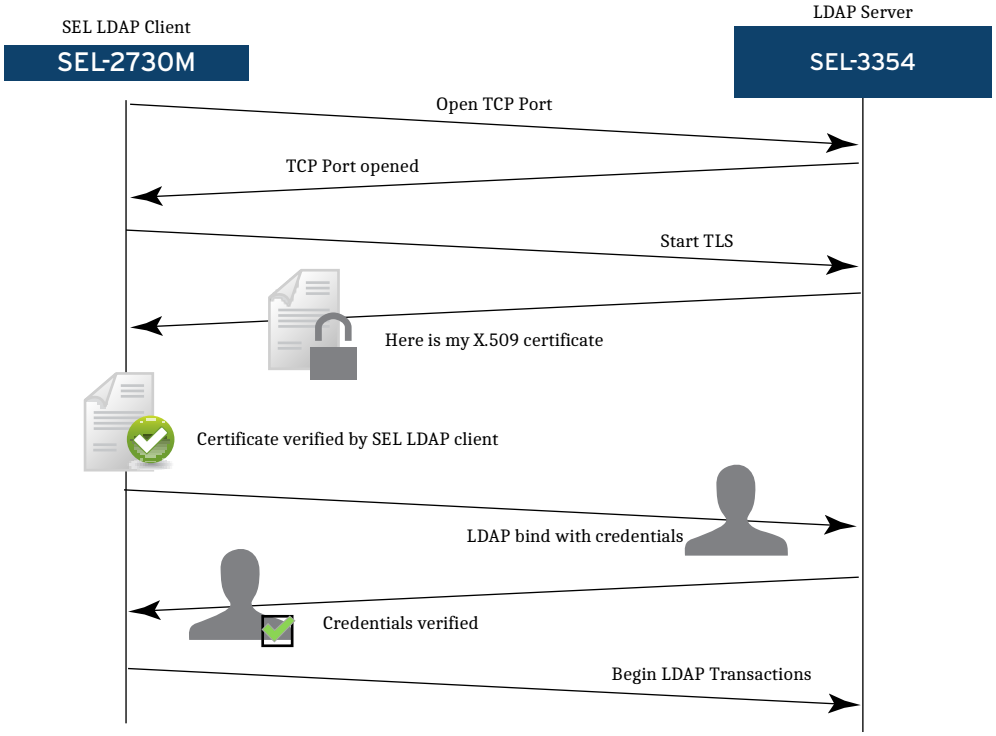


Figure D.1 LDAP Transaction

Certificate Chain

When an SEL device receives an X.509 certificate from an LDAP server during a StartTLS exchange prior to LDAP bind, you will need to have the certificate chain stored locally. The certificate chain, also known as the certification path, is a list of certificates used to authenticate the LDAP server. The chain, or path, begins with the certificate of the LDAP server (the one the SEL device receives), and each certificate in the chain is signed by the certificate authority (CA) identified by the next certificate in the chain. The chain terminates with a root CA certificate. The root CA certificate is always signed by the CA itself. The signatures of all certificates in the chain must be verified by the SEL LDAP

client until the root CA certificate is reached. The Distinguished Name (DN) of the X.509 certificate the LDAP server uses to authenticate to the SEL LDAP client must match the LDAP server name (i.e., LDAP server "3354.x509.local" must match its certificate DN "3354.x509.local").

LDAP Settings Form

LDAP Hosts
(Input these settings on the Hosts page, need at least one):

Hostname:	IP Address:
Hostname:	IP Address:

LDAP Settings
(Input these settings on the LDAP Settings page):

TLS Required (Yes/No):	Synchronization Interval (Hours):

Search Base:

User ID Attribute:

Group Member Attribute:

Bind DN (optional, if left blank will use anonymous binds):

Bind DN Password (optional, required only if not using anonymous binds):

LDAP Servers
(Input these settings on the LDAP Settings page, need at least one):

Hostname:	Port Number:
Hostname:	Port Number:

Device Roles
(Required to map user privileges, input these settings on the LDAP settings page):

Administrator Group/User DN:

Engineer Group/User DN:

User Manager Group/User DN

Monitor Group/User DN

APPENDIX E

Syslog

Introduction

The Syslog Protocol, defined in RFC 3164, provides a transport to allow a device to send system event notification messages across IP networks to remote Syslog servers. Syslog is commonly used to send system logs such as security events, system events, and status messages useful in troubleshooting, auditing, and event investigations. The Syslog packet size is limited to 1024 bytes and is formatted into three parts: PRI, HEADER, and MSG.

1. **PRI**: The priority part of a Syslog packet is a number enclosed in angle brackets that represents both the Facility and Severity of the message. The Priority value is calculated by multiplying the Facility numerical code by 8 and adding the numerical value of the Severity. For example, a kernel message (Facility = 0) with a Severity of Emergency (Severity = 0) would have a Priority of 0. Also, a "local use 4" message (Facility = 20) with a Severity of Notice (Severity = 5) would have a Priority value of 165. In the PRI part of the Syslog message, these values would be placed between the angle brackets as <0> and <165> respectively.

Higher severities have lower numerical codes, as shown in *Table E.1*.

Table E.1 Syslog Message Severities Reported by the SEL-2730M

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

The Facility code (*Table E.2*) defines from which application group the message originated.

Table E.2 Syslog Message Facilities

Numerical Code	Facility
0	Kernel messages
1	User-level messages
2	Mail system
3	System daemons
4	Security/authorization messages[a]
5	Messages generated internally by Syslog

Numerical Code	Facility
6	Line printer subsystem
7	Network news subsystem
8	UUCP subsystem
9	Clock daemon[b]
10	Security authorization messages[a]
11	FTP daemon
12	NTP subsystem
13	Log audit[a]
14	Log audit[b]
15	Clock daemon[b]
16	Local use 0 (local 0)
17	Local use 1 (local 1)
18	Local use 2 (local 2)
19	Local use 3 (local 3)
20	Local use 4 (local 4)
21	Local use 5 (local 5)
22	Local use 6 (local 6)
23	Local use 7 (local 7)

[a]Various operating systems have been found to use Facilities 4, 10, 13, and 14 for security/ authorization, audit, and alert messages that seem to be similar.

[b]Various operating systems have been found to use both Facilities 9 and 15 for clock (cron/at) messages.
Source: www.faqs.org/rfcs/rfc5424.html

2. **HEADER**: The header of a Syslog packet contains the time stamp and the source of the message. The IP address or the hostname defines the source of the message originator. Time stamps are based on the time of the originating host, so it is critical to have time synchronized across devices for the entire network to accurately perform log analysis and event correlation.
3. **MSG**: The message part of a Syslog packet contains the source program that triggered the message and the human-readable body of the message.

A sample Syslog message has been provided below. This particular message shows an invalid login attempt on July 09, 2009, at 08:17:29 to "myhostname" for user root from the IP address 192.168.1.1. The priority of this message is 34.

```
<34>Jul 09 2009 08:17:29 myhostname Invalid login attempt by:
root at 192.168.1.1
```

The Syslog message has been divided into each respective part as shown here.

PRI	HEADER	MSG
<34>	Jul 09 2009 08:17:29 myhostname	Invalid login attempt by: root at 192.168.1.1

Remote Syslog Servers

Syslog messages are stored locally and optionally sent to remote Syslog servers. The local buffers are circular in nature so that newer messages overwrite older messages after the buffer is filled. Support for multiple remote Syslog servers provide the added benefits of centralized logging including larger storage capacity, centralized event analysis and correlation, and archival of event logs. In *Figure E.1*, remote devices are configured to send Syslog messages to the remote Syslog server on the other end of the VPN tunnel. Syslog compatible devices are able to send logs to the central Syslog server in this example for centralized logging, reporting, and event correlation. The Syslog Protocol uses User Datagram Protocol (UDP) port 514 to send Syslog messages to remote Syslog servers.

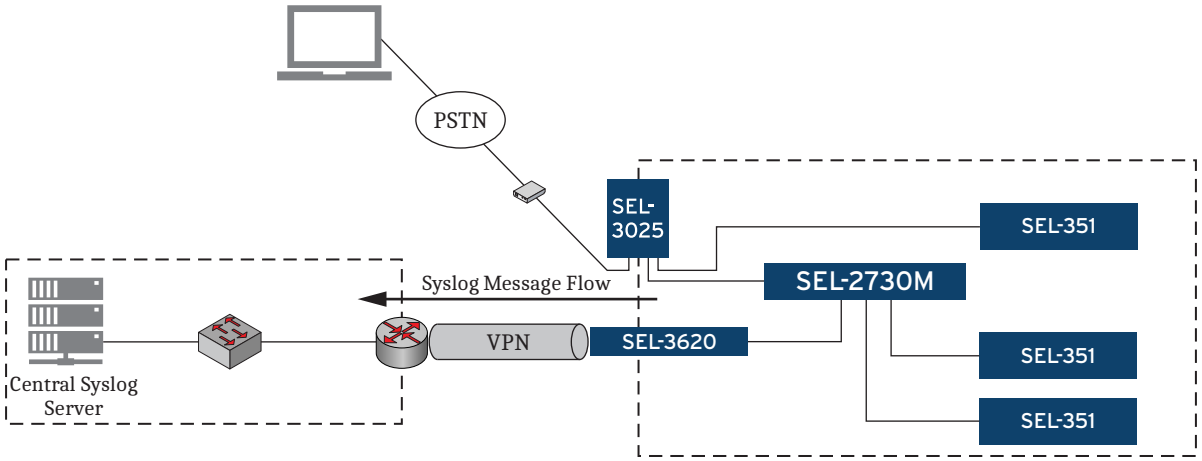


Figure E.1 Central Syslog Server

Open-Source Syslog Servers

Most Linux and UNIX distributions include a native Syslog server that can be used for a central Syslog server solution. Syslog-ng (www.balabit.com) is also an excellent solution with added functionality that can be used if not already included in your distribution. Syslog server solutions for Microsoft Windows are typically commercial or have limited feature sets if offered at no charge.

SEL-2730M Event Logs

The SEL-2730M records and time-stamps all events in the Syslog format consistent with the Syslog description from RFC 3164. *Table E.3* lists all of the events that the SEL-2730M logs and the record that is generated with each of these events.

Log messages may contain words or phrases in brackets such as {username}. This notation indicates that this is a variable that will be replaced with the value being logged. For example, the {username} in Syslog message `User account {username} locked out due to consecutive failed login attempts` would be replaced with the actual username that was locked out.

Table E.3 Event Logs (Sheet 1 of 6)

Message	Tag Name	Severity	Facility
Commissioning			
Device commissioned by {username} at {IP address}	Commissioning	Notice	SECURITY
User Configuration			
User {username}: created by {username} at {IP address}	UserConfig	Warning	SECURITY
User {username}: deleted by {username} at {IP address}	UserConfig	Warning	SECURITY
User {username}: enabled by {username} at {IP address}	UserConfig	Notice	SECURITY
User {username}: disabled by {username} at {IP address}	UserConfig	Notice	SECURITY
User {username}: password set by {username} at {IP address}	UserConfig	Warning	SECURITY
User {username}: attributes changed by {username} at {IP address}	UserConfig	Notice	SECURITY
Login			
Login to {interface}: successful by {username} at {IP address}	Login	Notice	SECURITY
Login to {interface}: failed from {IP address}	Login	Notice	SECURITY
Logout {interface}: {username} at {IP address}	Login	Notice	SECURITY
User account {username} locked out due to consecutive failed login attempts	Login	Warning	SECURITY
User account {username} timeout	Login	Warning	SECURITY
LDAP			
LDAP: settings changed by {username} at {IP address}	LDAPConfig	Warning	SECURITY
LDAP: enabled by {username} at {IP address}	LDAPConfig	Warning	SECURITY
LDAP: disabled by {username} at {IP address}	LDAPConfig	Warning	SECURITY
LDAP Search Base: changed by {username} at {IP address}	LDAPConfig	Warning	SECURITY
LDAP User ID Attribute: changed by {username} at {IP address}	LDAPConfig	Warning	SECURITY
LDAP Group Membership Attribute: changed by {username} at {IP address}	LDAPConfig	Warning	SECURITY
LDAP Synchronization Interval: changed by {username} at {IP address}	LDAPConfig	Warning	SECURITY
LDAP Bind DN: changed by {username} at {IP address}	LDAPConfig	Warning	SECURITY
LDAP Bind DN Password: changed by {username} at {IP address}	LDAPConfig	Warning	SECURITY
LDAP Server {hostname}: created by {username} at {IP address}	LDAPConfig	Warning	SECURITY
LDAP Server {hostname}: deleted by {username} at {IP address}	LDAPConfig	Warning	SECURITY
LDAP Server {previous_hostname} Hostname: changed to {post_hostname} by {username} at {IP address}	LDAPConfig	Warning	SECURITY
LDAP Server {hostname} Port: port number changed by {username} at {IP address}	LDAPConfig	Warning	SECURITY
LDAP Group Mapping: {privilege level} mapping created by {username} at {IP address}	LDAPConfig	Warning	SECURITY
LDAP Group Mapping: {privilege level} mapping deleted by {username} at {IP address}	LDAPConfig	Warning	SECURITY
LDAP User Attribute Mappings: changed by {username} at {IP address}	LDAPConfig	Warning	SECURITY

Message	Tag Name	Severity	Facility
LDAP: Unable to connect to server at {hostname}:{port}	LDAP	Error	SECURITY
LDAP: {hostname}:{port} does not respond	LDAP	Error	SECURITY
LDAP: LDAP version used by server {hostname}:{port} is not supported	LDAP	Error	SECURITY
LDAP: Unable to start TLS session with {hostname}:{port}	LDAP	Error	SECURITY
LDAP: The certificate presented by {hostname}:{port} is invalid	LDAP	Error	SECURITY
LDAP: The hostname of the certificate presented by {hostname}:{port} does not match	LDAP	Error	SECURITY
LDAP: The issuing authority of the certificate presented by {hostname}:{port} is untrusted	LDAP	Error	SECURITY
LDAP: The certificate presented by {hostname}:{port} is expired	LDAP	Error	SECURITY
LDAP: Search base entry not found on server {hostname}:{port}	LDAP	Error	SECURITY
LDAP: User ID Filter syntax invalid for server {hostname}:{port}	LDAP	Error	SECURITY
LDAP: Group Filter syntax invalid for server {hostname}:{port}	LDAP	Error	SECURITY
LDAP: Group Filter search on server {hostname}:{port} returned no groups	LDAP	Error	SECURITY
LDAP: No Group Mappings set for server {hostname}:{port}	LDAP	Error	SECURITY
LDAP: Bind DN authentication failed on server {hostname}:{port}	LDAP	Error	SECURITY
LDAP: An error occurred during authentication or authorization on server {hostname}:{port}	LDAP	Error	SECURITY
LDAP: One or more of the user-configured DNs for server {hostname}:{port} contains syntax errors.	LDAP	Error	SECURITY
LDAP: Server {hostname}:{port} returned a DN that was longer than 4096 bytes. That DN was ignored.	LDAP	Error	SECURITY
LDAP: An error occurred during Bind DN authentication on server {hostname}:{port}	LDAP	Error	SECURITY
LDAP: An error occurred when searching for a DN on the server {hostname}:{port}	LDAP	Error	SECURITY
LDAP: An error occurred when searching for the user's DN on the server {hostname}:{port}	LDAP	Error	SECURITY
Miscellaneous Configuration			
Usage Policy: changed by {username} at {IP address}	Config	Notice	SECURITY
System Contact Information: changed by {username} at {IP address}	Config	Notice	USER
Port Mirror			
Port Mirroring enabled on {target_port} by {username} at {user_ip}	PortMirrorConfig	Notice	USER
Port Mirroring disabled on {target_port} by {username} at {user_ip}	PortMirrorConfig	Notice	USER
Port Mirroring target port changed from {previous_target_port_id} to {new_target_port_id} by {username} at {user_ip}	PortMirrorConfig	Notice	USER
Port Mirroring source ports changed by {username} at {user_ip}	PortMirrorConfig	Notice	USER
Port Monitor			
Port {port #} exceeded link flap threshold	PortMonitor	Error	SYSTEM
Port {port #} detected {x} RX Checksum Errors within monitor window	PortMonitor	Notice	SYSTEM

Message	Tag Name	Severity	Facility
Port {port #} disabled: exceeded link flap threshold	PortMonitor	Error	SYSTEM
Port {port #} disabled: exceeded RX Checksum Error rate limit	PortMonitor	Error	SYSTEM
Port {port #} restored by {username} at {user_ip}	PortMonitor	Notice	USER
Settings changed by {username} at {user_ip}	PortMonitorConfig	Notice	SECURITY
Ports			
Port Settings: changed by {username} at {IP address}	Config	Notice	SYSTEM
Port {number} changed link state to up	Link Up/Down	Notice	SYSTEM
Port {number} changed link state to down	Link Up/Down	Notice	SYSTEM
Front Port changed link state up	Link Up/Down	Notice	SYSTEM
Front Port changed link state down	Link Up/Down	Notice	SYSTEM
Rate Limiting Settings: changed on port {number} by {username} at {IP address}.	RateLimitingConfig	Notice	USER
Firmware			
Firmware update from {previous version} to {current version} succeeded	Firmware	Warning	SYSTEM
Uploaded firmware update package is corrupted; unable to decrypt the firmware update package or validate the signature on the firmware update package	Firmware	Error	SYSTEM
Firmware: reversion to previous version initiated by {username} at {IP address}	Firmware	Warning	USER
The firmware update from {0} to new version failed with an error of {code}. Please contact Schweitzer Engineering Laboratories, Inc. for assistance.	Firmware	Critical	SYSTEM
Firmware: update to new version initiated by {username} at {IP address}	Firmware	Notice	USER
VLAN Configuration			
VLAN {VID}: updated by {username} at {IP address}	VLANConfig	Notice	USER
VLAN-aware mode disabled by {username} at {IP address}	VLANConfig	Notice	USER
VLAN-aware mode enabled by {username} at {IP address}	VLANConfig	Notice	USER
VLAN {VID}: created by {username} at {IP address}	VLANConfig	Notice	USER
VLAN {VID}: deleted by {username} at {IP address}	VLANConfig	Notice	USER
Multicast MAC Filtering			
Static Multicast MAC Group {number}: updated by {username} at {IP address}	StaticMulticastMAC	Notice	USER
Static Multicast MAC Group {number}: deleted by {username} at {IP address}	StaticMulticastMAC	Notice	USER
Static Multicast MAC Group {number}: created by {username} at {IP address}	StaticMulticastMAC	Notice	USER
Port Mirroring			
Port Mirroring Source Ports: changed by {username} at {IP address}	PortMirroringConfig	Notice	USER
Port Mirroring disabled on {port} by {username} at {IP address}	PortMirroring	Notice	USER
Port Mirroring enabled on {port} by {username} at {IP address}	PortMirroring	Notice	USER

Message	Tag Name	Severity	Facility
Port Mirroring target port changed from none to {port} by {username} at {IP address}	PortMirroringConfig	Notice	USER
Port Mirroring target port changed from {port} to none by {username} at {IP address}	PortMirroringConfig	Notice	USER
Spanning Tree			
Spanning Tree: {hostname} has become the root bridge	SpanningTree	Notice	SYSTEM
Spanning Tree: Configuration changed by {username} at {IP address}	SpanningTree	Notice	USER
Spanning Tree: Port {number} transitioned from {1} to {2}	SpanningTree	Informational	SYSTEM
Spanning Tree: Port {number} transitioned from {1} to {2}	SpanningTree	Notice	SYSTEM
RSTP			
BPDU received, port {port_number} disabled.	SpanningTree	Notice	SYSTEM
BPDU Guard timeout reached. Port {port_number} enabled.	SpanningTree	Notice	SYSTEM
BPDU Guard overridden by {username} at {IP address} Port {port_number} enabled.	SpanningTree	Notice	SYSTEM
Class of Service Configuration			
Class of Service queuing changed from {previous value} to {current value} by {username} at {IP address}	Config	Notice	USER
MAC-Based Port Security			
MAC-Based Port Security: configuration changed on port {0} by {username} at {IP address}	Config	Notice	SECURITY
MAC addresses locked due to time lock expiration	PortSecurity	Notice	SYSTEM
Maximum number of MAC addresses learned	PortSecurity	Error	SYSTEM
Maximum number of learned MAC addresses reached. Configuration locked.	PortSecurity	Notice	SYSTEM
Unauthorized address {MAC address} on port {port number}	PortSecurity	Critical	SECURITY
Address table overflow resulting from hash collision when attempting to insert {MAC address} on port {port number}	PortSecurity	Error	SYSTEM
Excessive unauthorized activity on port {port}	PortSecurity	Warning	SYSTEM
Unauthorized activity cleared on port {port}	PortSecurity	Notice	SYSTEM
Alarm Contact			
Alarm Contact: configuration changed by {username} at {IP address}	Alarm Contact	Notice	USER
X.509 Certificate			
X.509 certificate generation started by {username} at {IP address}	X509Config	Notice	SECURITY
X.509 certificate {alias} has expired; communications requiring X.509 based authentication may have stopped	X509Config	Alert	SYSTEM
X.509 certificate {alias} Alias: certificate changed to {new alias} by {username} at {IP address}	X509Config	Notice	USER
X.509 certificate {alias} will expire in {number} days; communications requiring X.509 based authentication may be affected when it expires	X509Config	Critical	SYSTEM
X.509 certificate {alias} will expire in {number} days; communications requiring X.509 based authentication may be affected when it expires	X509Config	Warning	SYSTEM
X.509 certificate {alias}: certificate generation completed successfully	X509Config	Notice	SECURITY

Message	Tag Name	Severity	Facility
X.509 certificate {alias} will expire in {number} days; communications requiring X.509 based authentication may be affected when it expires	X509Config	Notice	SYSTEM
X.509 certificate {alias}: certificate import completed successfully	X509Config	Notice	SECURITY
X.509 certificate import failed	X509Config	Warning	SECURITY
X.509 certificate import started by {username} at {IP address}	X509Config	Notice	SECURITY
X.509 certificate generation failed	X509Config	Warning	SECURITY
X.509 certificate {alias}: certificate exported by {username} at {IP address}	X509Config	Notice	USER
Networking Configuration			
Global Network Settings: changed by {username} at {IP address}	NetworkConfig	Notice	USER
Network Interface {alias}: changed by {username} at {IP address}	NetworkConfig	Notice	USER
Captive Port			
Captive Port: disabled by {username} at {IP address}	CaptivePortConfig	Notice	USER
Captive Port: enabled by {username} at {IP address}	CaptivePortConfig	Notice	USER
Hosts			
Host Settings: Added host {new_hostname} with IP address {ip_address} by {username} at {IP address}.	HostConfig	Notice	USER
Host Settings: Changed hostname {old_hostname} with IP address {old_ip_address} to {new_hostname} with IP address {new_ip_address} by {username} at {IP address}.	HostConfig	Notice	USER
Host Settings: Removed host {old_hostname} with IP address {ip_address} by {username} at {IP address}.	HostConfig	Notice	USER
SNMP			
SNMP Settings: changed by {username} at {IP address}	SNMPConfig	Informational	USER
Syslog			
Syslog Settings: changed by {username} at {IP address}	SyslogConfig	Notice	USER
Syslog Destination {number}: created by {username} at {IP address}	SyslogConfig	Notice	USER
Syslog Destination {number}: deleted by {username} at {IP address}	SyslogConfig	Warning	USER
Syslog Destination {number} Settings: modified by {username} at {IP address}	SyslogConfig	Warning	USER
Local Syslog Event Queue contains >= 90% unacknowledged events	Syslog	Critical	SYSTEM
Local Syslog Event Queue contains <= 80% unacknowledged events	Syslog	Notice	SYSTEM
Local Syslog Event Queue contains >= 75% unacknowledged events	Syslog	Warning	SYSTEM
Local Syslog Event Queue contains <= 65% unacknowledged events	Syslog	Notice	SYSTEM
Syslog events acknowledged by {username} at {IP address}	Syslog	Notice	USER
The {0} event queue overflowed	Syslog	Critical	SYSTEM
The {0} event queue left the overflow condition. Approximately {number} events were lost.	Syslog	Notice	SYSTEM

Message	Tag Name	Severity	Facility
Date/Time			
Time Zone: changed from {0} to {1} by {username} at {IP address}	DateTimeConfig	Notice	USER
System Time: changed from {0} to {1} by {username} at {IP address}	DateTimeConfig	Notice	USER
Time Source: set to {0} by {username} at {IP address}	DateTimeConfig	Notice	USER
NTP: server mode enabled by {username} at {IP address}	DateTimeConfig	Notice	USER
NTP Server {priority}: created by {username} at {IP address}	DateTimeConfig	Notice	USER
NTP Server {priority}: deleted by {username} at {IP address}	DateTimeConfig	Notice	USER
NTP: server mode disabled by {username} at {IP address}	DateTimeConfig	Notice	USER
System Time: synchronized via NTP	DateTime	Notice	SYSTEM
System Time: lost synchronization to external source	DateTime	Warning	SYSTEM
System Time: manually synchronized to external source by {username} at {IP address}	DateTime	Notice	USER
Configuration File Import and Export			
Configuration file import started by {username} at {IP address}	ImportExport	Notice	USER
Configuration file import successful	ImportExport	Notice	USER
Configuration file import failed	ImportExport	Warning	USER
Configuration file export started by {username} at {IP address}	ImportExport	Notice	USER
Configuration file export successful	ImportExport	Notice	USER
Configuration file export failed	ImportExport	Warning	USER
Device Reset			
Device initialization completed	Power	Notice	SYSTEM
Device reset because of hardware watchdog	Power	Critical	SYSTEM
Device rebooted by {username} at {IP address}	Power	Error	USER
Device factory reset initiated by {username} at {IP address}	Commissioning	Notice	SECURITY
Device factory reset initiated through pinhole button	PushbuttonReset	Notice	USER
Front management port reset initiated through pinhole button	PushbuttonReset	Alert	USER
RADIUS			
{username} at {IP address} enabled RADIUS	RADIUSConfig	Warning	SECURITY
{username} at {IP address} disabled RADIUS	RADIUSConfig	Warning	SECURITY
{username} at {IP address} modified RADIUS settings	RADIUSConfig	Notice	SECURITY
Rejected login attempt because no response from the RADIUS server received within the retransmission timeout	RADIUS	Warning	SECURITY
Active RADIUS server is now {priority}	RADIUS	Notice	SECURITY
Rejected login attempt by user {username} because RADIUS server {priority} replied without an SEL-User-Role attribute	RADIUS	Error	SECURITY
Rejected login attempt by user {username} because RADIUS server {priority} replied with an SEL-User-Role attribute containing an unrecognizable user role	RADIUS	Error	SECURITY

Message	Tag Name	Severity	Facility
Rejected login attempt because the common name in the X.509 certificate sent by the RADIUS server {priority} did not match the hostname of the RADIUS server on the RADIUS page	RADIUS	Error	SECURITY
Rejected login attempt because RADIUS server {priority} sent an X.509 certificate with an unknown or untrusted certificate authority	RADIUS	Error	SECURITY
Rejected login attempt because RADIUS server {priority} sent an expired or not yet valid X.509 certificate	RADIUS	Error	SECURITY
Diagnostics			
Diagnostic report generated by {username} at {IP address}	Diagnostics	Notice	USER

APPENDIX F

Networking Fundamentals

Introduction

A telecommunications network can be as simple as two devices linked together for information sharing or as complex as the internet involving many devices serving a multitude of purposes. In either case, networking devices need a common model for interconnectivity across a diverse set of communications media, manufacturer equipment, protocols, and applications. The International Organization for Standardization (ISO) developed the Open Systems Interconnection (OSI) model to serve this purpose. The OSI model has been in use for decades as a reference model that describes the fundamental concepts and approach to interconnecting heterogeneous systems by abstracting the model into seven logical layers. This appendix introduces networking fundamentals and illustrates how device communication occurs across disparate networks.

OSI Model

The OSI model consists of seven conceptual layers, as shown in *Figure F.1*. Each layer is relatively independent of the other layers and only needs to know how to communicate with the adjacent layers. This independence has allowed manufacturers to develop implementations at their respective OSI layers and still be interoperable with implementations at completely different layers. For example, a program interfacing at the Application Layer does not need to know if the data being transmitted will traverse over a Cat 5 cable, serial, or radio physical medium.

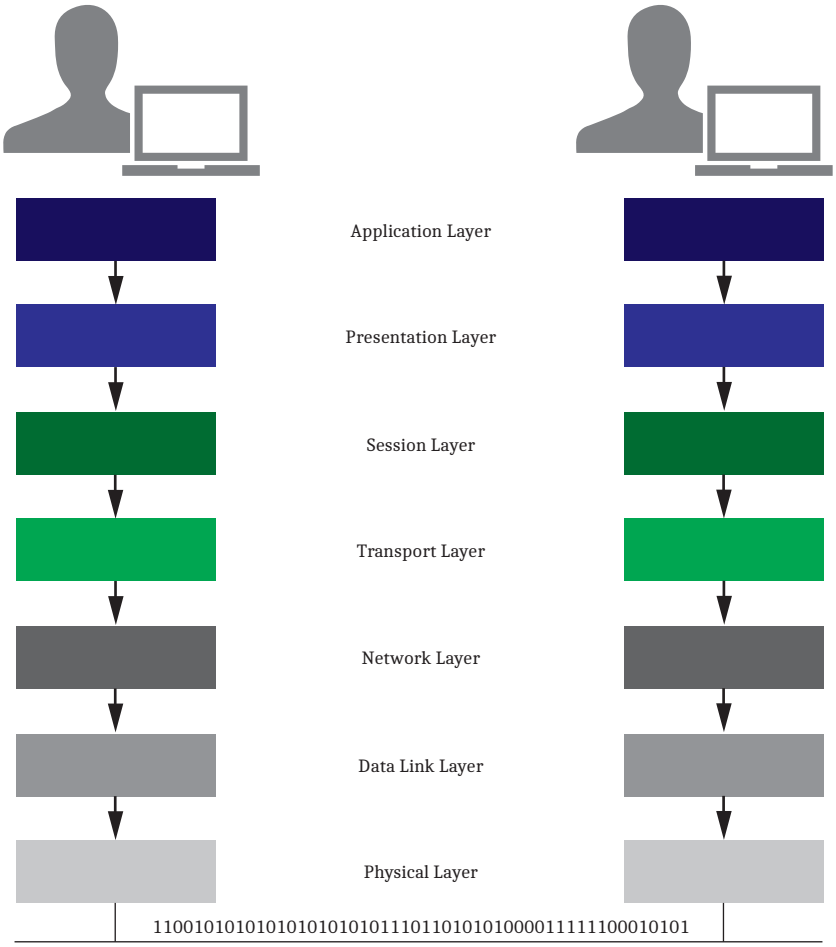


Figure F.1 OSI Model

Physical Layer (Layer 1)

The primary responsibility of the Physical Layer is transmitting data across a communications medium from one device to another. This layer defines the electrical and mechanical interfaces such as the hardware network interface cards use in interfacing with the physical medium that carries the bit stream. A Physical Layer device simply transmits or receives data and lacks any knowledge of the data that it transmits. Copper and fiber are both examples of physical media in common use. Network hubs and repeaters are devices common to this layer.

Data Link Layer (Layer 2)

The Data Link Layer is responsible for providing transit of data across physical mediums by controlling access control, data framing, and error detection, as well as providing physical addressing. Directly connected devices (*Figure F.2*) communicate at this layer without the need for a Layer 3 device, such as a router.

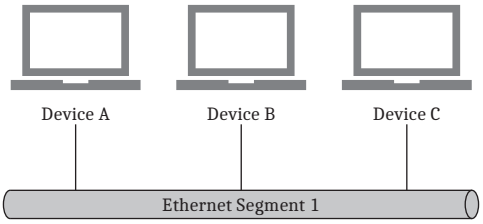


Figure F.2 Ethernet Segment

MAC addresses are physical addresses that are embedded into the hardware and determine how devices should identify each other uniquely on the same network segment.

At this layer, devices organize data they receive into frames that encapsulate the data from higher layers. *Figure F.3* depicts an example of an Ethernet frame.

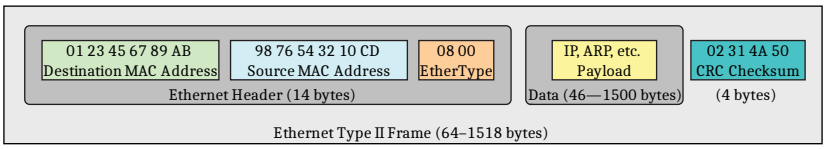


Figure F.3 Ethernet Frame

The Ethernet frame in *Figure F.3* includes the following components:

- Ethernet Header: Includes the source and destination MAC addresses that determine which devices are communicating on the network. Also included is the EtherType, which defines the type of Ethernet framing used.
- Data: The data field includes the payload type as well as the actual data transmitted.
- CRC Checksum: The CRC checksum provides error checking to verify that the data were not corrupted during transit.

Network Layer (Layer 3)

The Network Layer is responsible for transmitting data from one device to another device that is on a separate network segment. The separate network segment could be within close proximity, such as within the same building, or in a completely different country, as seen with the internet.

Addressing, routing, fragmentation, and error handling are all functions of the Network Layer.

Layer 3 addressing is different from Layer 2 addressing, in that Layer 3 addresses are logical. Logical addresses are hardware-independent, unlike MAC addresses that are assigned to specific hardware. The Network Layer manages mappings between these logical addresses and physical addresses. Address Resolution Protocol (ARP) performs this mapping in IPv4 networks.

The most common Layer 3 addressing scheme is IP addressing. IP addresses are 32-bit addresses, commonly denoted in dotted-decimal notation, that identify devices across different network segments.

Table F.1 shows an example IP address of 192.168.254.1 in dotted-decimal notation, with the equivalent 32-bit binary notation. Each 8-bit octet value is equivalent to the decimal value in the dotted-decimal notation. For example, the first binary octet of 11000000 is equivalent to 192 in the first octet of the dotted-decimal notation.

Table F.1 Sample IP Address

Dotted-Decimal Notation	192.168.254.1
32-Bit Binary Notation	11000000.10101000.11111110.00000001

Routing is necessary to define the traffic's path between two networks. In *Figure F.4*, there are two IP networks, 192.168.254.0/24 and 10.10.10.0/24, with a router between the two networks. The router provides the ability for Device A, Device B, and Device C to communicate with Device D, Device E, and Device F. Without this router, these devices would not be able to communicate with each other. Device A, Device B, and Device C can all communicate among each other without the need for a router, as described in *Data Link Layer (Layer 2) on page 136*. The same is true for communication among Device D, Device E, and Device F.

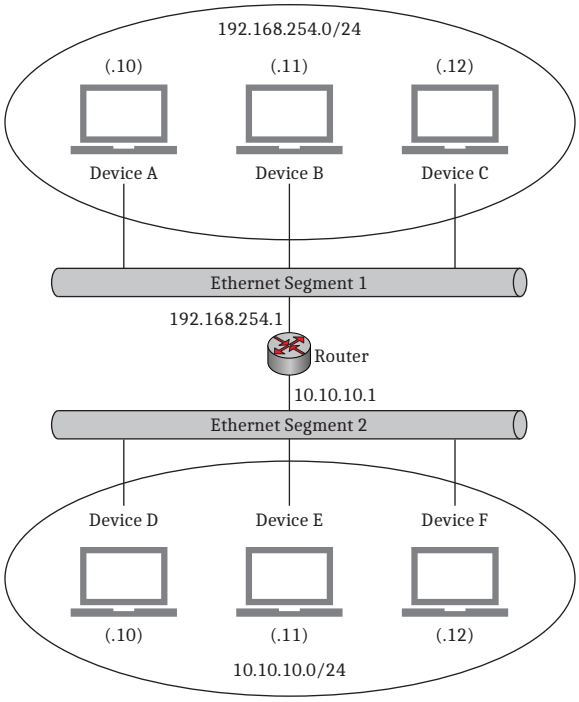


Figure F.4 Layer 3 IP Network

Transport Layer (Layer 4)

When data arrive at a network device that the Network Layer determines is the final destination, the Network Layer formats the data and passes the information to the Transport Layer. This layer is responsible for processing level addressing, segmentation, connection management, and flow control.

Flow control manages the amount of data transmitted between communicating devices so that the sending device does not send more data than the receiving device can process.

Each Transport Layer protocol handles error recovery differently, but it typically involves requesting data retransmission if a device detects an error.

Transmission Control Protocol (TCP) is the Transport Layer protocol the TCP/IP suite uses to provide reliable, end-to-end communication. The suite also includes User Datagram Protocol (UDP) as a connectionless protocol, meaning that data transmission occurs with no guarantee of successful delivery.

Connection-Oriented Versus Connectionless

Connection-oriented protocols, such as TCP, establish a connection between the sending device and the receiving device prior to data transmission. These protocols make the connection between two devices through a three-way handshake (*Figure F.5*). The three steps in the handshake are as follows:

1. The sending device sends a synchronization (SYN) packet to the receiving device.
2. The receiving device sends back a synchronization/ acknowledgment (SYN/ACK) packet to the sending device.
3. The sending device completes the three-way handshake by sending an acknowledgment (ACK) to the receiving device.

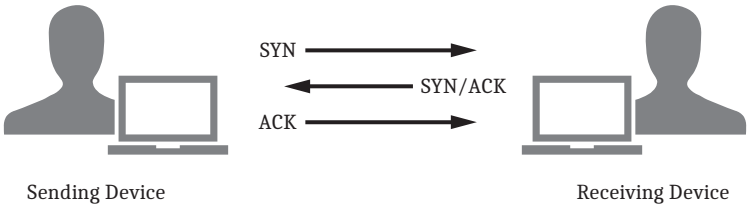


Figure F.5 TCP Three-Way Handshake

At the completion of the three-way handshake, a connection is established and the two devices can begin transmitting and receiving data. The connection is maintained between the two devices throughout the session, providing a reliable connection and verification of data transmission.

In a connectionless protocol, such as UDP, there is no established connection prior to data transmission. There is also no retained connection at any point during data transmission. The protocol is connectionless, so routing information must accompany each data packet to provide information on how the data should traverse the network. Connectionless protocols provide no means for data transmission verification and are often referred to as unreliable protocols for this reason.

Session Layer (Layer 5)

The Session Layer handles session establishment, management, and termination between two end-user software application processes. This is the first layer that switches focus from the actual networking details and deals primarily with sessions consisting of service requests and responses that occur between applications installed on communicating devices.

Presentation Layer (Layer 6)

The Presentation Layer provides for standard data presentation so that applications can exchange data in a meaningful manner across a network. The sending device converts data into a standard format for transmission on the network. The receiving device converts the data sent in this standard format to a format recognizable by the application of the receiving device. This processing occurs transparently to ensure that the receiving device can read the data from the sending device.

Application Layer (Layer 7)

The Application Layer is the layer closest to the end user of a system. Software applications provide a means for end users to interface with a device to transmit and receive data. The Application Layer provides the interface between the end user and software applications that a system uses to process data over the network. Application Layer protocols define rules for communicating with network applications in a standardized format.

APPENDIX G

Virtual Local Area Networks

VLANs are logical groupings of devices that communicate with one another as though they are part of the same broadcast domain on a physical network segment. Devices within the same broadcast domain can send data directly to other devices within the same broadcast domain without sending traffic through a routing device. *Figure G.1* illustrates a network with two broadcast domains. Device A, Device B, and Device C are all within Broadcast Domain A and can communicate directly with one another. Similarly, Device C, Device E, and Device F are all within Broadcast Domain B and can communicate directly with one another. For devices to communicate between Broadcast Domains A and B, data must pass through the router. In this network configuration, all devices on the 2nd floor must be part of Broadcast Domain A, and all devices on the 1st floor must be part of Broadcast Domain B. This might work well in some configurations, but using VLANs provides the flexibility to assign a device to a broadcast domain regardless of the physical location.

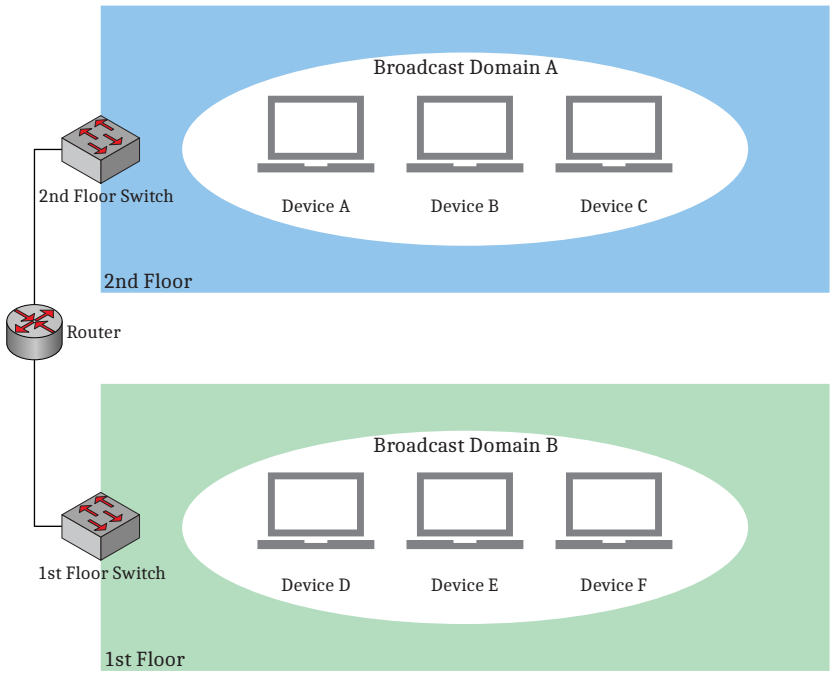


Figure G.1 Network Illustration Not Using VLANs

Figure G.2 shows the same physical network using VLANs. Broadcast Domain A now consists of Device A and Device D without requiring Device A to physically move to the 2nd floor. This can be useful when assigning VLANs to functional or departmental roles within an organization. Let's assume VLAN 10 was created for the Human Resources department that contains network resources spread throughout the 1st and 2nd floors. Without the use of VLANs, all network resources for the Human Resources department would need to be physically located on the same floor. As you can see in *Figure G.2*, VLAN membership is independent of physical location.

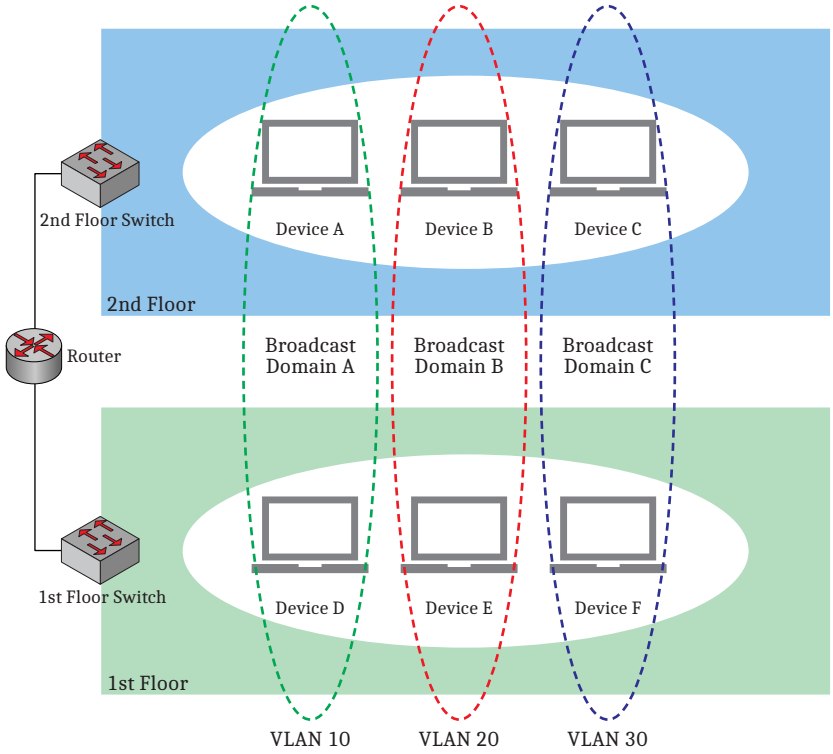


Figure G.2 Network Illustration Using VLANs

VLANs also increase network performance in large broadcast domains. As the name implies, broadcast domains "broadcast" certain types of traffic to every device within the respective broadcast domain. As the number of devices increases within the broadcast domain, so does the amount of network traffic, which causes network congestion. By separating certain devices into different VLANs, the broadcast traffic is also separated and isolated to each VLAN. While this separation provided by VLANs is great for isolating broadcast traffic, VLANs should not be confused as a security mechanism for secure network segregation. Highly secure networks should use a switch independent of the switch used by a less secure network. For example, it is not recommended to include a publicly accessible DMZ network segment on the same switch as an internal LAN segment. While these two network segments may be on completely different networks and separated using a VLAN for the DMZ network segment and a VLAN for the LAN network segment, there are attacks that could bypass this network separation.

APPENDIX H

Classless Inter-Domain Routing (CIDR)

CIDR was developed as a method to help alleviate the exhaustion of IPv4 addresses available on the internet and to reduce and simplify global routing tables across internet routers.

CIDR is an addressing scheme that allows for better use of IP addresses that traditionally fell into the old Class A, B, and C address schemes. In the traditional address scheme, Class A, B, and C addresses were categorized with 8, 16, and 24 bits, respectively, for the subnet mask. The smallest block of IP addresses in this addressing scheme is 254. This led to unused and wasted addresses in scenarios where someone needed 10 IP addresses but had to purchase the entire Class C block of 254 usable addresses. In situations where someone needed more than 254 addresses, they either had to purchase another Class C block or jump to a Class B or Class A network. The jump from Class C (254 usable addresses) to Class B (65,534 usable addresses) to Class A (16,777,214 usable addresses) provided no middle ground for IP addressing.

The solution was to allow network bits other than 8, 16, and 24, which resulted in providing that middle ground in the addressing scheme. For example, someone who needed only 10 IP addresses could be given a block of 14 usable IP addresses through the use of 28 network bits instead of 24 in the subnet mask.

CIDR allows blocks of contiguous addresses to be combined through route aggregation to create a larger classless set of IP addresses. It is then possible to summarize these aggregated routes into routing tables, resulting in fewer route advertisements.

In the following example, we would need to advertise a route for each classful network.

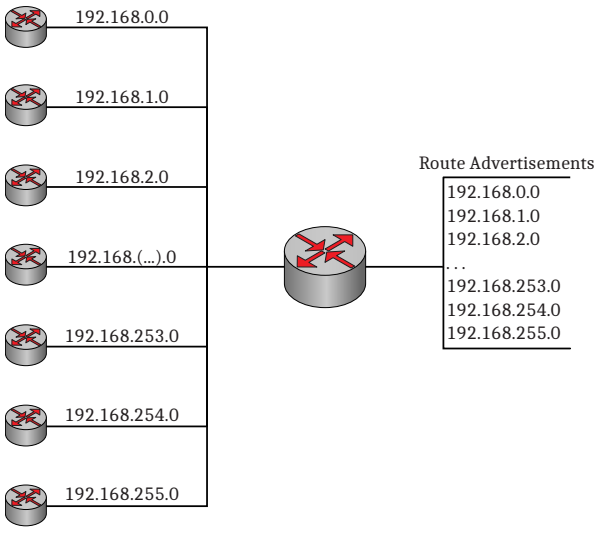


Figure H.1 Classful Route Advertisements

By using CIDR notation, we can use route aggregation to combine multiple routes, as seen below. High-level route entries can represent many lower-level routes in the global routing table, simplifying routing and management of route tables.

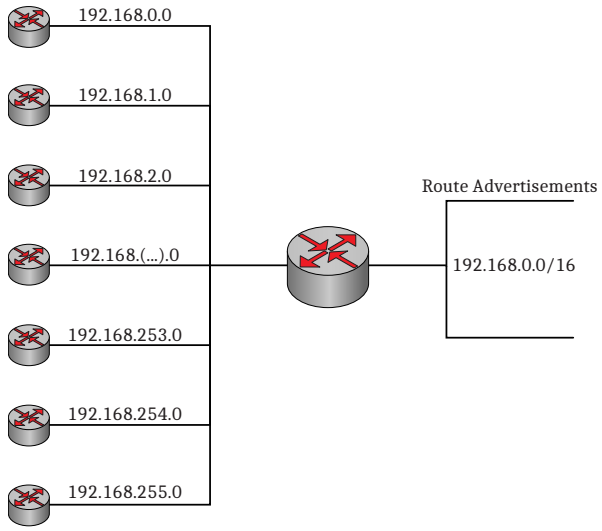


Figure H.2 CIDR Route Advertisements

CIDR has carried over to use in private network RFC 1918 addresses, through the use of CIDR notation when defining the subnet mask and in simplifying internal routing tables. CIDR notation uses the format where the network ID and associated subnet mask are listed as xxx.xxx.xxx.xxx/n. The value *n* is the number of leftmost bits set to a value of "1" in the mask. A traditional classful depiction of a network ID and subnet mask would be as follows:

- Network ID: 192.168.1.0
- Subnet Mask: 255.255.255.0 (dotted-decimal notation)

To take the above example and convert it to CIDR notation, you would need to count the number of leftmost bits set to a value of "1" in the binary notation of the subnet mask. The binary notation of the subnet mask of 255.255.255.0 would be 11111111.11111111.11111111.00000000. There are 24 bits set to a value of "1", so *n* would equal 24. The CIDR notation would be 192.168.1.0/24. The table below provides additional information about CIDR and the equivalent dotted-decimal notation.

Table H.1 CIDR to Dotted-Decimal Mapping

Subnet Mask (CIDR)	Subnet Mask (Dotted Decimal)	# of Bits for Network ID	# of Bits for Host ID	# of Hosts per Network
/1	128.0.0.0	1	31	2,147,483,646
/2	192.0.0.0	2	30	1,073,741,822
/3	224.0.0.0	3	29	536,870,910
/4	240.0.0.0	4	28	268,435,454
/5	248.0.0.0	5	27	134,217,726
/6	252.0.0.0	6	26	67,108,862
/7	254.0.0.0	7	25	33,554,430

Subnet Mask (CIDR)	Subnet Mask (Dotted Decimal)	# of Bits for Network ID	# of Bits for Host ID	# of Hosts per Network
/8	255.0.0.0	8	24	16,777,214
/9	255.128.0.0	9	23	8,388,606
/10	255.192.0.0	10	22	4,194,302
/11	255.224.0.0	11	21	2,097,150
/12	255.240.0.0	12	20	1,048,574
/13	255.248.0.0	13	19	524,286
/14	255.252.0.0	14	18	262,142
/15	255.254.0.0	15	17	131,070
/16	255.255.0.0	16	16	65,534
/17	255.255.128.0	17	15	32,766
/18	255.255.192.0	18	14	16,382
/19	255.255.224.0	19	13	8,190
/20	255.255.240.0	20	12	4,094
/21	255.255.248.0	21	11	2,046
/22	255.255.252.0	22	10	1,022
/23	255.255.254.0	23	9	510
/24	255.255.255.0	24	8	254
/25	255.255.255.128	25	7	126
/26	255.255.255.192	26	6	62
/27	255.255.255.224	27	5	30
/28	255.255.255.240	28	4	14
/29	255.255.255.248	29	3	6
/30	255.255.255.252	30	2	2

This page intentionally left blank

APPENDIX I

X.509

Introduction

In cryptography, X.509 is an International Telecommunication Union standard for public key infrastructure (PKI). X.509 specifies formats for public key certificates and validation paths for authentication. The SEL-2730M uses X.509 certificates in the web server for secure device management, and for IPsec authentication.

Public Key Cryptography

Public key cryptography is distinguished by the use of asymmetric keys instead of the more traditional symmetric keys. Asymmetric keys are mathematically related so that whatever one key encrypts, the other key must be used to decrypt. There is no way to derive one key from knowledge of its paired key. These key pairs are known as public and private keys. The private key must be kept secret, while the public key can be distributed freely. This allows for many methods of protecting and authorizing messages that are not possible with symmetric key cryptography.

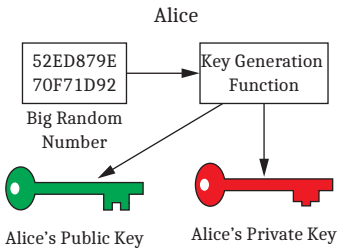


Figure I.1 Asymmetric Keys

Symmetric key cryptography, which has been used in various forms for thousands of years, uses a single key that both encrypts and decrypts the message. This key must be shared between the sender and receiver in advance. If the key cannot be shared securely, the confidentiality of any transmission encrypted with that key cannot be known.

In public key cryptography, the encryption key is not the same as the decryption key. If a message is encrypted with the publicly known key, only the private key can be used to decrypt it. This private key is known only to the owner of the key pair. Only the sender and the intended receiver will know the message, ensuring confidentiality.

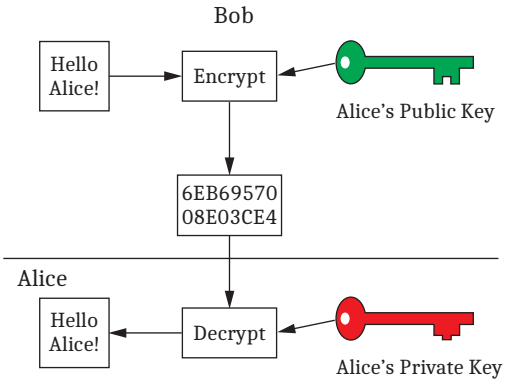


Figure I.2 Confidentiality With Asymmetric Keys

Public key cryptography is much more computation-intensive than symmetric key cryptography. This makes it infeasible to send large amounts of data, or secure a series of transmissions, using this technology. Public key cryptography offers confidentiality and the corresponding ability to exchange symmetric keys securely and confidentially. This is known as hybrid cryptography and is one way that IPsec uses public key cryptography.

You can also use public key cryptography for authentication. Do this by using a private key, rather than the public key, as the encryption key. The public key you use to decrypt the message will identify the sender. This is known as an electronic signature.

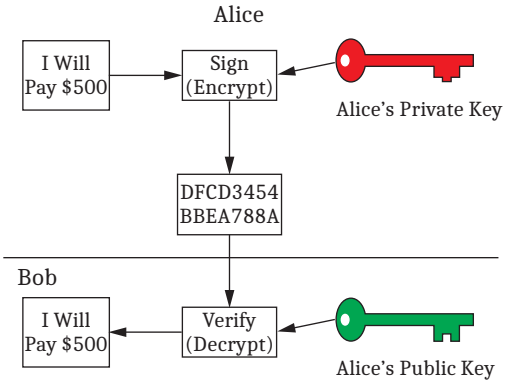


Figure I.3 Authentication With Asymmetric Keys

X.509 Certificates

Digital certificates, also known as public key certificates, provide a formal method for associating pairs of asymmetric keys with their owners. You can use these electronic documents, through the use of digital signatures, to bind public keys to their owners.

Digital Signatures

A digital signature is a more formal method of authenticating data than an electronic signature. They can be compared to the wax seals that were placed on envelopes before email was available. To create a digital signature of data, you would first compute a hash of the data to be signed and then encrypt that

hash with the signer's private key. You would then attach this signature to the data to be signed. To verify the authenticity of the data, the receiver's system first separates data and signature. The receiver computes a hash of the data and then uses the issuer's public key to decrypt the signature. We compare these two hashes and, if they match, we know the data are authentic.

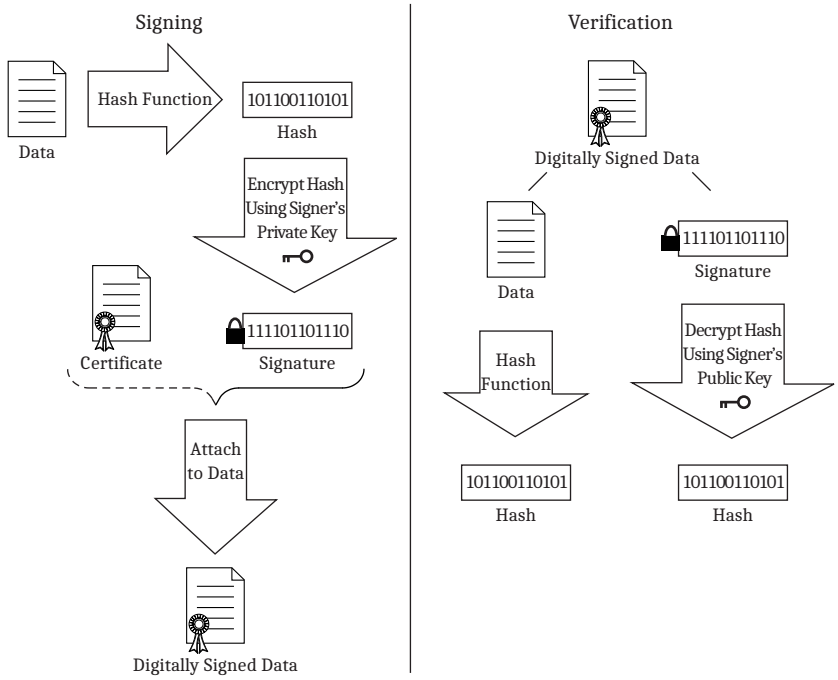


Figure I.4 Digital Signatures

Public Key Infrastructure

One of three common uses for digital certificates is in a public key infrastructure (PKI). PKI is a formal, hierarchical system where a digital certificate may contain the signature of one or a chain of more trusted certificate issuers. At the top of the PKI hierarchy is the most trusted certificate, a root certificate. A root certificate is self-signed, highly protected, and should only be used to sign CA certificates. Root certificates have to be manually made trusted by a system administrator, or they must be included by the software vendor in a cache of trusted root certificates. Most modern operating systems, such as Microsoft Windows preload a collection of root certificates for commonly used (and trusted) certificate authorities (e.g., VeriSign, Thawte, etc.) in the "Trusted Root" certificate store. If a root certificate is compromised, we must assume all certificates below it to be compromised as well.

A certificate authority (CA) is an entity that issues, or signs, other certificates. To obtain a certificate, an entity (the 'subject') will generate a key pair, and send the public key and proof of identity to a CA. The CA will verify the identity of the requester and issue the certificate containing the subject's identity, the public key, and the CA's digital signature. A CA is responsible for saying "yes" these people are whom they claim to be and this is their public key. CAs are authenticated by other CAs or by a root certificate.

An attacker can subvert this process. This can happen when an attacker steals the private key of a CA or of a party to whom a certificate was issued. It can also happen when an attacker impersonates another party when requesting a certificate. In either case, this can result in the issuance of untrustworthy certificates. An attacker might also steal a subject's private key. In such cases, these certificates must be revoked by the issuing authority.

Web of Trust

Another of the three common uses of digital certificates is in the web of trust. This is a less formal method of authentication than PKI provides, but is still in common use. The largest use of the web of trust model is in Pretty Good Privacy (PGP) used for email security. This model is very similar to PKI in that a trusted third party is verifying the authenticity of a certificate. The difference is that this trusted third party is not a CA, but rather a person who endorses the authenticity of another person. Signing the public key of the person requiring endorsement (or trust) with the endorser's (trusted entity) own private key establishes a web of trust. *Figure I.5* below illustrates a simple example of a web of trust. If Alice trusts Bob, and Bob trusts Charlie, then Alice implicitly trusts Charlie.

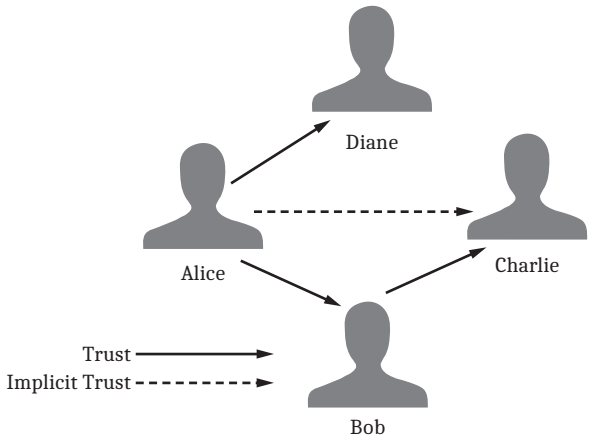


Figure I.5 Web of Trust

Simple Public Key Infrastructure

The third common use of digital certificates is in the simple public key infrastructure (SPKI). This model evolved from the need to limit the complexity inherent in PKI and the web of trust. There is no trusted third party in SPKI because the owner and issuer of the certificate are the same entity. For SPKI to be secure, certificates must be preshared among all entities who communicate on that system. This ensures that all knowledge for security decisions resides locally.

Online Certificate Status Protocol (OCSP)

In consideration of the case where an authentic certificate has been stolen, there are methods to revoke certificates. One method is the certificate revocation list (CRL). The CRL method has a few problems that allow a revoked certificate to still be used. This arises from the lag associated with producing CRLs. Also, a certificate will be accepted by default, even if revoked, if the CRL is not accessible.

The online certificate status protocol (OCSP) was created to fix some of these problems. OCSP requires less bandwidth than CRLs and enables near real-time status checks to verify a certificate's status. OCSP also allows a certificate to be denied by default if the OCSP server is not accessible.

OCSP is a request/response protocol that provides real-time revocation status information for X.509 certificates. When an OCSP-enabled certificate is presented to an application, such as a web browser, the browser uses OCSP to check the certificate and ensure it is valid before proceeding with the session. OCSP uses the following response indicators to help determine the certificate revocation status:

- Good: Indicates that the certificate is valid and has not been revoked
- Revoked: Indicates that the certificate has been revoked
- Unknown: Indicates that the responder does not know about the certificate being requested

The system performs a real-time revocation check for each certificate so that if a certificate is compromised or for some other reason requires revocation, it will no longer appear as valid.

Sample X.509 Certificate

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 1 (0x1)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,

OU=Certification Services Division,

CN=Thawte Server CA/Email=server-certs@thawte.com

Validity

Not Before: Aug 1 00:00:00 1996 GMT

Not After: Dec 31 23:59:59 2020 GMT

Subject: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,

OU=Certification Services Division,

CN=Thawte Server CA/Email=server-certs@thawte.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)

Modulus (1024 bit):

00:d3:a4:50:6e:c8:ff:56:6b:e6:cf:5d:b6:ea:0c:

68:75:47:a2:aa:c2:da:84:25:fc:a8:f4:47:51:da:

85:b5:20:74:94:86:1e:0f:75:c9:e9:08:61:f5:06:

6d:30:6e:15:19:02:e9:52:c0:62:db:4d:99:9e:e2:

6a:0c:44:38:cd:fe:be:e3:64:09:70:c5:fe:b1:6b:

29:b6:2f:49:c8:3b:d4:27:04:25:10:97:2f:e7:90:

6d:c0:28:42:99:d7:4c:43:de:c3:f5:21:6d:54:9f:

5d:c3:58:e1:c0:e4:d9:5b:b0:b8:dc:b4:7b:df:36:

3a:c2:b5:66:22:12:d6:87:0d

Exponent: 65537 (0x10001)

X509v3 extensions:

X509v3 Basic Constraints: critical

CA:TRUE

Signature Algorithm: md5WithRSAEncryption

07:fa:4c:69:5c:fb:95:cc:46:ee:85:83:4d:21:30:8e:ca:d9:

a8:6f:49:1a:e6:da:51:e3:60:70:6c:84:61:11:a1:1a:c8:48:

3e:59:43:7d:4f:95:3d:a1:8b:b7:0b:62:98:7a:75:8a:dd:88:

4e:4e:9e:40:db:a8:cc:32:74:b9:6f:0d:c6:e3:b3:44:0b:d9:

8a:6f:9a:29:9b:99:18:28:3b:d1:e3:40:28:9a:5a:3c:d5:b5:

e7:20:1b:8b:ca:a4:ab:8d:e9:51:d9:e2:4c:2c:59:a9:da:b9:

b2:75:1b:f6:42:f2:ef:c7:f2:18:f9:89:bc:a3:ff:8a:23:2e:

70:47

APPENDIX J

Accessing Port Information Through SNMP

The port status and other port information and diagnostics can be accessed remotely though the ifTable (1.3.6.1.2.1.2.2) in the IF MIB. *Table J.1* shows the relationship between the port number and the ifIndex of the ifTable.

Table J.1 SEL-2730M Port Number to ifIndex Mapping

SEL-2730M Port Number	ifIndex R100–R108-V1	ifIndex R109 and Later
1	22	20
2	21	19
3	20	18
4	19	17
5	18	16
6	16	14
7	17	15
8	15	13
9	14	12
10	13	11
11	12	10
12	11	9
13	10	8
14	9	7
15	8	6
16	7	5
17	27	25
18	28	26
19	29	27
20	30	28
21	23	21
22	24	22
23	25	23
24	26	24

For example, to find the port status (ifOperStatus) of Port 1, you would look at the ifEntry with an ifIndex of 22 (1.3.6.1.2.1.2.2.1.8.22).

This page intentionally left blank

APPENDIX K

Cybersecurity Features

Introduction and Security Environment

Product Function

The SEL-2730M is an Ethernet-managed switch. The security features of the SEL-2730M provide secure communications between the user interface and the computer used to interact with the device for configuration and monitoring and are focused on maintaining the availability and integrity of the LAN operations.

Security Requirements

The SEL-2730M was designed for a security model that includes hardware, firmware, the user interface, data plane, and control plane. The SEL-2730M has controls at each of these layers to protect the integrity of the device operations. This security model relies on other devices to monitor the logs, alarms, and health of the product. The data plane and control plane prioritize interoperability for Ethernet and rapid spanning tree protocols.

Version Information

Obtaining Version Information

The device firmware identification (FID) number can be obtained through the web user interface and the SNMP Entity MIB. The SEL-2730M firmware is provided in a single digitally signed file. The SEL-2730M will validate the digital signature before upgrading its firmware.

Integrity Indicators

The SEL-2730M protects the integrity of the operating firmware through validation of digital signatures.

Commissioning and Decommissioning

Commissioning

No service accounts are used on the SEL-2730M and on the first startup, the landing page of the user interface requires the input of the first administrator username and password. See *Commissioning the Device on page 20* for more information.

Secure Operation Recommendations

SEL recommends enabling only the user access on the interface of the product you intend to use. By default, only the front port is enabled. SEL also recommends collecting the logs from the SEL-2730M centrally on a server that can collect the syslogs and monitor the alarm contact.

Decommissioning

To remove all settings and return the device to its factory default state, see *Factory Reset on page 99* for more information.

External Interfaces

Ports and Services

The SEL-2730M has one front port that is used only for the management of the switch itself. There are 24 ports that you can use for management and data plane packet forwarding on the rear of the device. All physical ports are enabled by default, but the SEL-2730M has settings that allow any port to be disabled, as well as settings to enable web-based engineering access and SNMP on the front or back ports. By default, only the web-based engineering access is enabled on the front port and SNMP is disabled on both.

Logical Ports

IP Port Default	Network Protocol	Default Port State	Port Configurable	Purpose
80	HTTP	Enabled on ETH F	No	Redirect to HTTPS port for web user interface
443	HTTPS	Enabled on ETH F	No	Web user interface
161	SNMP	Disabled	No	SNMP read-only

File System Interfaces

The SEL-2730M is an embedded device operating on a single firmware image and does not support any external file systems. You can export and import device settings by using an active and authorized user through the user interface.

Access Controls

Privilege Levels

See *Appendix C: User-Based Accounts* for more information.

Centrally Managed Accounts (if Supported)

See *Appendix D: Lightweight Directory Access Protocol* for more information.

Local Accounts (or Access Levels)

See *Appendix C: User-Based Accounts* for more information.

Passwords

See *Appendix C: User-Based Accounts* for more information.

X.509 Certificates

See *Appendix I: X.509* for more information.

Physical Access Controls

The SEL-2730M does not have any tamper evident protections but is designed to be difficult to open without disconnecting communications cables so that loss of communication is an event-triggering an incident response.

Logging Features

Security Events

See *Appendix J: Accessing Port Information Through SNMP* and *Appendix E: Syslog* for more information.

Internal Log Storage

See *Appendix E: Syslog* for more information.

Alarm Contact

See *Alarm Contact on page 93* for more information.

Backup and Restore

See *File Management on page 96* for more information.

Malware Protection Features

The SEL-2730M is an embedded device that does not allow the installation of additional software and only accepts digitally signed firmware upgrades. The SEL-2730M includes a self-test that continually checks running code against the known good baseline version of code in nonvolatile memory. See "The SEL Process for Mitigating Malware Risk to Embedded Devices" at selinc.com/malware_protection for more details.

Product Updates

Table A.1 contains a description of each firmware update. The product page selinc.com/SEL-2730M shows the latest firmware version available. To obtain product updates, contact any sales or technical support contact. For the SEL disclosure process and details on vulnerability disclosures, see "The SEL Process for Disclosing Security Vulnerabilities" at selinc.com/security_vulnerabilities.

Update Verification

The SEL-2730M automatically checks firmware authenticity and integrity and only loads firmware files that have been signed by SEL. The authenticity and integrity of firmware updates can be verified by checking the firmware hash. For instructions and firmware hash values, see selinc.com/products/firmware.

Contact SEL

For further questions or concerns about product security, contact SEL at security@selinc.com or +1.509.332.1890.

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 U.S.A.
Phone: +1.509.332.1890 • Fax: +1.509.332.7990
selinc.com • info@selinc.com