SEL-2730M

Managed Ethernet Switch

Instruction Manual

20130429

SEL SCHWEITZER ENGINEERING LABORATORIES, INC.

PM2730M-01

⚠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

In order to avoid losing system logs on a factory default reset, configure the SEL-2730M to forward Syslog messages.

⚠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

Contact with instrument terminals can cause electrical shock that can result in injury or death.

⚠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

Use of this equipment in a manner other than specified in this manual can impair operator safety safeguards provided by this equipment.

⚠ATTENTION

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.

⚠ATTENTION

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”).

⚠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

Tout contact avec les bornes de l'appareil peut causer un choc électrique pouvant entraîner des blessuers ou la mort.

⚠AVERTISSEMENT

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.

⚠AVERTISSEMENT

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.

PM2730M-01

Table of Contents

List of Tables iii

List of Figures v

Preface vii

Section 1: Introduction and Specifications

Introduction 1.1
Product Overview 1.1
Product Features 1.1
Connections, Reset Button, and LED Indicators 1.3
Software System Requirements 1.6
General Safety and Care Information 1.6
Front- and Rear-Panel Diagrams 1.7
Dimension Drawing 1.8
Warranty 1.8
Specifications 1.9

Section 2: Installation

Introduction 2.1
Connecting to the Device 2.1
Commissioning the Device 2.4
Navigating the User Interface 2.4
Device Dashboard 2.6

Section 3: Managing Users

Introduction 3.1
User-Based Accounts 3.1

Section 4: Job Done Examples

Introduction 4.1
Job Done Example 1 ..... 4.1
Job Done Example 2 ..... 4.6
Job Done Example 3 ..... 4.8

Section 5: Settings and Commands

Introduction 5.1
Reports 5.1
Switch Management 5.3
Network Settings 5.10
Accounts 5.18
Security 5.19
System 5.21

Section 6: Testing and Troubleshooting

Introduction 6.1
Testing Philosophy 6.1
LED Indicators 6.2
Device Dashboard 6.3
Troubleshooting 6.5
Factory Assistance 6.7

Appendix A: Firmware and Manual Versions

Firmware A.1
Instruction Manual A.1

Appendix B: Firmware Upgrade Instructions

Introduction B.1
Firmware Upgrade Procedure B.1
Factory Assistance B.2

Appendix C: User-Based Accounts

Introduction C.1
Benefits of User-Based Accounts C.1
Administration of User-Based Accounts C.2
Acceptable Use Banner C.2
Logging on With SEL User-Based Accounts C.2
Passphrases C.3

Appendix D: Syslog

Introduction D.1
Remote Syslog Servers D.3
Open Source Syslog Servers D.3
SEL-2730M Event Logs D.4

Appendix E: Networking Fundamentals

Introduction E.1
OSI Model E.1

Appendix F: Virtual Local Area Networks

Appendix G: Classless Inter-Domain Routing (CIDR)

Appendix H: X.509

Introduction H.1
Public Key Cryptography H.1
X.509 Certificates H.2
Digital Signatures H.3
Public Key Infrastructure H.3
Web of Trust H.4
Simple Public Key Infrastructure H.4
Online Certificate Status Protocol (OCSP) H.5
Sample X.509 Certificate H.5

List of Tables

Table 1.1 Ethernet Status Indicators 1.4
Table 1.2 Gigabit Ethernet Port Pinout 1.5
Table 1.3 10/100 Mbps Ethernet Port Pinout 1.5
Table 1.4 High-Voltage Power Supply Connections 1.5
Table 1.5 Low-Voltage Power Supply Connections 1.6
Table 1.6 Alarm Contact Pinout 1.6
Table 1.7 Alarm Contact Ratings 1.6
Table 2.1 Network Interface Icon Colors 2.8
Table 2.2 System Statistics 2.8
Table 4.1 VLANs for Job Done Example 1 ..... 4.2
Table 4.2 VLAN 10 Configuration 4.3
Table 4.3 VLAN 20 Configuration 4.3
Table 4.4 VLAN 30 Configuration 4.3
Table 4.5 VLAN 100 Configuration 4.3
Table 4.6 VLAN 101 Configuration 4.4
Table 4.7 VLAN 102 Configuration 4.4
Table 4.8 VLAN 103 Configuration 4.4
Table 4.9 VLAN 104 Configuration 4.4
Table 4.10 VLAN 10 Configuration 4.5
Table 4.11 VLAN 20 Configuration 4.5
Table 4.12 VLAN 30 Configuration 4.5
Table 4.13 VLAN 100 Configuration 4.5
Table 4.14 VLAN 101 Configuration 4.5
Table 4.15 VLAN 102 Configuration 4.5
Table 4.16 VLAN 103 Configuration 4.6
Table 4.17 VLAN 104 Configuration 4.6
Table 5.1 VLAN Settings 5.3
Table 5.2 RSTP Settings 5.8
Table 5.3 Port Settings 5.9
Table 5.4 Global IP Settings 5.11
Table 5.5 ETH F Network Interface Settings 5.11
Table 5.6 Mgmt Network Interface Settings 5.12
Table 5.7 Edit Hosts Settings 5.14
Table 5.8 SNMP Profile Settings 5.15
Table 5.9 SNMP Trap Server Settings 5.17
Table 5.10 SNMP Trap Categories 5.17
Table 5.11 Syslog Threshold Values 5.18
Table 5.12 Syslog Destination Settings 5.18
Table 5.13 MAC Security Fields 5.21
Table 5.14 Web Settings 5.21
Table 5.15 System Contact Information Settings 5.22
Table 5.16 Features 5.22
Table 5.17 Alarm Contact Output Trigger Categories 5.23
Table 6.1 System Status Indicators 6.2
Table 6.2 Communications Interface Indicators 6.3
Table 6.3 Network Interface Icon Colors 6.4
Table 6.4 System Statistics 6.5
Table 6.5 Troubleshooting Procedure 6.6
Table A.1 Firmware Revision History A.1
Table A.2 Instruction Manual Revision History A.1
Table D.1 Syslog Message Severities D.1
Table D.2 Syslog Message Facilities D.2

Table D.3 Event Logs D.4
Table E.1 Sample IP Address E.4
Table G.1 CIDR to Dotted Decimal Mapping G.3

List of Figures

Figure 1.1 Front-Panel View 1.3
Figure 1.2 Close-Up of Front-Panel Status Indicators 1.3
Figure 1.3 Rear-Panel View 1.4
Figure 2.1 Commissioning Network 2.1
Figure 2.2 Open Network Connections With Run Command 2.2
Figure 2.3 Open Connection Properties 2.2
Figure 2.4 Local Area Connection Properties 2.3
Figure 2.5 Configuring Automatic Network Configuration 2.3
Figure 2.6 Device Commissioning Page 2.4
Figure 2.7 Device Dashboard 2.5
Figure 2.8 Local Users 2.5
Figure 2.9 Adding a New User 2.6
Figure 2.10 Device Dashboard 2.7
Figure 2.11 Network Interfaces 2.7
Figure 2.12 Version Information 2.8
Figure 2.13 System Statistics 2.8
Figure 2.14 Diagnostics 2.9
Figure 2.15 Open Terminal With Run Command 2.9
Figure 2.16 Open Network Connections With Run Command 2.10
Figure 2.17 Open Connection Properties 2.10
Figure 2.18 Local Area Connection Properties 2.11
Figure 2.19 Internet Protocol (TCP/IP) Properties 2.11
Figure 3.1 Add New User Form 3.2
Figure 4.1 Network Diagram 4.2
Figure 4.2 SEL-2730M–1 VLAN Configuration 4.4
Figure 4.3 SEL-2730M–2 VLAN Configuration 4.6
Figure 4.4 RSTP Network Topology 4.7
Figure 4.5 RSTP Root Bridge Notification 4.7
Figure 4.6 SNMP Network Diagram 4.8
Figure 4.7 Edit Hosts Configuration 4.8
Figure 4.8 SNMP v3 Profile 4.9
Figure 4.9 Add Trap Server 4.9
Figure 5.1 Sample Syslog Report 5.2
Figure 5.2 VLAN View 5.3
Figure 5.3 Edit VLAN 1 ..... 5.4
Figure 5.4 Switch Trunk Link 5.4
Figure 5.5 GOOSE Message 5.5
Figure 5.6 Untagged Ports 5.5
Figure 5.7 Port View 5.6
Figure 5.8 Add New VLAN 5.6
Figure 5.9 RSTP Disabled 5.7
Figure 5.10 RSTP Configuration Page 5.7
Figure 5.11 Root Bridge Notification 5.8
Figure 5.12 Add New Filter 5.9
Figure 5.13 Port Mirroring 5.10
Figure 5.14 IP Configuration 5.11
Figure 5.15 SNMP Settings Page 5.12
Figure 5.16 Edit Hosts 5.13
Figure 5.17 Add v2c Profile 5.14
Figure 5.18 Add v3 Profile 5.15
Figure 5.19 SNMP Trap Permissions Are Required 5.16
Figure 5.20 Add Trap Server 5.16
Figure 5.21 Syslog Settings 5.18
Figure 5.22 Renaming Certificates 5.19

Figure 5.23 MAC-Based Port Security 5.20
Figure 5.24 Date/Time Settings 5.23
Figure 5.25 Export Settings Page 5.25
Figure 5.26 Import Settings Page 5.25
Figure 6.1 Close-Up of Front-Panel Status Indicators 6.2
Figure 6.2 Device Dashboard 6.4
Figure B.1 File Management B.2
Figure D.1 Central Syslog Server D.3
Figure E.1 OSI Model E.2
Figure E.2 Ethernet Segment E.3
Figure E.3 Ethernet Frame E.3
Figure E.4 Layer 3 IP Network E.4
Figure E.5 TCP Three-Way Handshake E.5
Figure F.1 Network Illustration Not Utilizing VLANs F.1
Figure F.2 Network Illustration Utilizing VLANs F.2
Figure G.1 Classful Route Advertisements G.1
Figure G.2 CIDR Route Advertisements G.2
Figure H.1 Asymmetric Keys H.1
Figure H.2 Confidentiality With Asymmetric Keys H.2
Figure H.3 Authentication With Asymmetric Keys H.2
Figure H.4 Digital Signatures H.3
Figure H.5 Web of Trust H.4

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.

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. Provides an introduction to user-based accounts and the benefits associated with using user-based accounts.

Appendix D: Syslog. Provides an introduction to the Syslog protocol and its uses in SEL products.

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

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

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

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

Examples

This instruction manual uses several example illustrations and instructions to explain how to effectively operate the SEL-2730M 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.

Safety Information

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

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

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

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

The following hazard statements apply to this device. See the following table for the English statements and corresponding French translations.

English	French
⚠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.	**⚠ATTENTION** 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.	**⚠ATTENTION** 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”).
⚠WARNING Use of this equipment in a manner other than specified in this manual can impair operator safety safeguards provided by this equipment.	**⚠AVERTISSEMENT** 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.
⚠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.

Technical Assistance

Obtain technical assistance from the following:

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
Internet: www.selinc.com
E-mail: 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 on page 1.1*
- *Product Features on page 1.1*
- *Connections, Reset Button, and LED Indicators on page 1.3*
- *Software System Requirements on page 1.6*
- *General Safety and Care Information on page 1.6*
- *Front- and Rear-Panel Diagrams on page 1.7*
- *Dimension Drawing on page 1.8*
- *Specifications on page 1.9*

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 using ACSELERATOR QuickSet® SEL-5030 Software or through an exported settings file that can be imported later on the switch.
- **Virtual Local Area Networks (VLANs).** Segregate traffic and improve network organization and performance. Take advantage of 802.1Q VLANs to separate IEC 61850 GOOSE messages from other traffic.
- **Traffic Prioritization.** Support critical substation messaging using IEEE 802.1p Class of Service (CoS) traffic prioritization with four service levels and VLAN-based classification.
- **Rapid Spanning Tree Protocol (RSTP).** Use IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) to speed network recovery and convergence after a topology change caused by a link or device failure.
- **Multicast MAC Filtering.** Filter multicast traffic to reduce network load on end devices.
- **Port-Based MAC Security.** Use IEEE 802.1x port-based MAC security to limit network access to authorized devices.
- **Time Synchronization.** Synchronize time 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.
- **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 configurable system and security events to the alarm contact 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.
- **User-Based Accounts.** Provide user accountability and separate authorization levels for configuration and maintenance.

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 device's activity and status light-emitting diode (LED) indicators. 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.

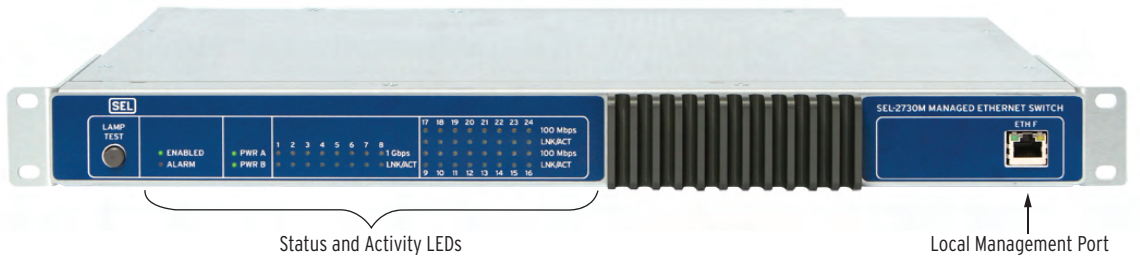


Figure 1.1 Front-Panel View

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 unlit during startup and if the unit fails self-test.

The **ALARM** indicator is unlit 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 be unlit.

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 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

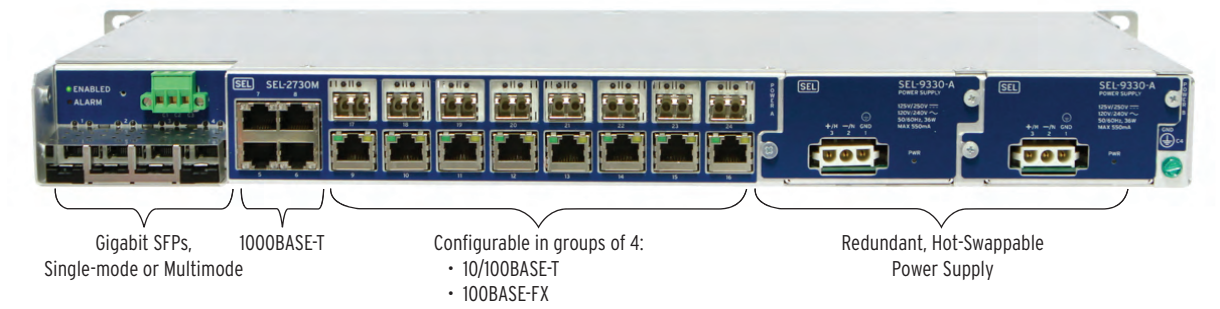


Figure 1.3 Rear-Panel View

The base-model SEL-2730M has 4 Gigabit Ethernet copper ports and 16 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 your network's unique requirements. You can also add as many as four fiber-optic Gigabit Ethernet ports via small form-factor pluggable (SFP) transceivers, for a total of 24 ports.

Ethernet copper ports support Auto MDI/MDX and autonegotiation for speed and duplex values.

Four Small Form-Factor Pluggable (SFP) Ports

Ports 1–4 support single- or multimode fiber SFP transceivers.

Four Gigabit Ethernet Ports

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

High-Voltage Power Supply (110/125/220/230 Vac, 110/125/220/250 Vdc)

Table 1.4 High-Voltage Power Supply Connections

Pin	Description
1	GND
2	–/N
3	+/H

Low-Voltage Power Supply (24/48 Vdc)

Table 1.5 Low-Voltage Power Supply Connections

Pin	Description
1	GND
2	–
3	+

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 source of failure.

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, 75 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 browser is Microsoft® Internet Explorer® 8.

General Safety and Care Information

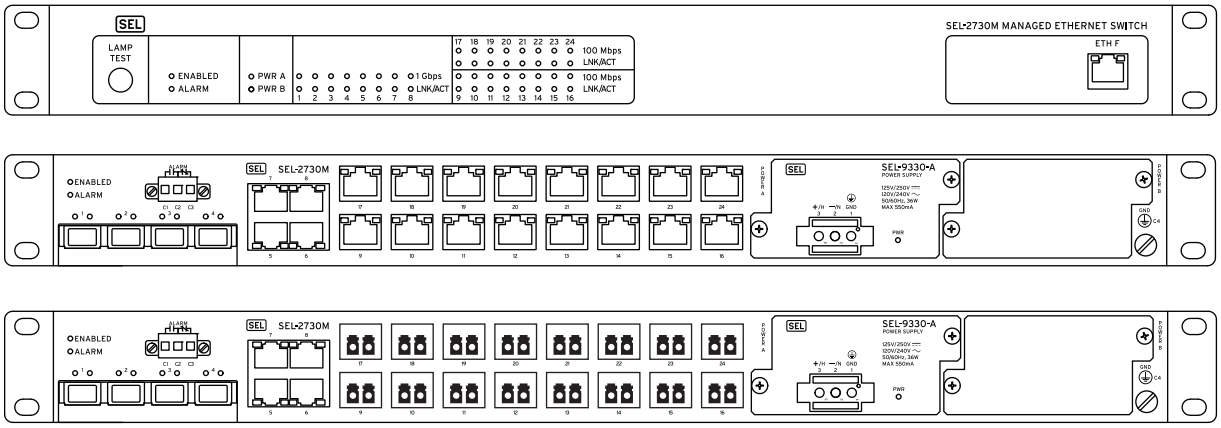
General Safety Notes

- 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.

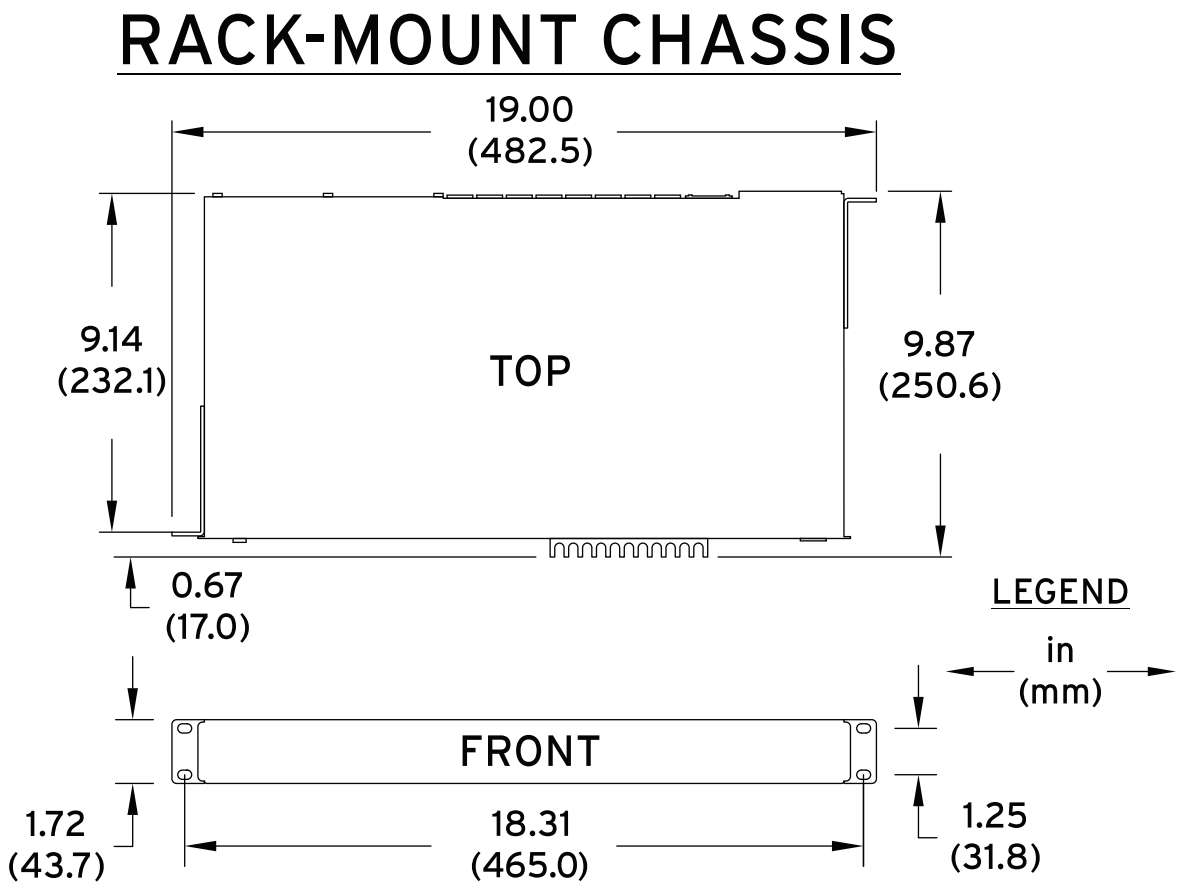
Cleaning Instructions

- 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



Mounting Options

The SEL-2730M comes with reversible mounting ears to support both front- and rear-panel installations.

Warranty

The SEL-2730M meets or exceeds the IEEE 1613 Class 2, 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 use of the same high standards as those for SEL protective relays and backs it with the same 10-year worldwide warranty.

Specifications

General

Operating Environment

Pollution Degree:	2
Overvoltage Category:	II

Dimensions

1U Rack Mount

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

Weight

1.96 kg (4.3 lbs)

Switching Properties

Switching Method:	Store and Forward
Switching Latency:	< 7 µs
Switch Fabric Throughput:	19.2 Gbps
Priority Queues:	4
Maximum VLANs:	256
VLAN ID Range:	1–4094
MAC Address Table Size:	8192 Addresses

Warranty

10 Years

Network Management

HTTPS Web User Interface

SNMP v2c/v3

ACSELERATOR QuickSet® Software

Settings Import/Export

Interoperable With SEL-5051 Network Management Software and 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

Digital Output

Rated Operational Voltage:	24–250 Vdc
Continuous Carry:	6 A

Environmental

Operating Temperature

–40° to +85°C (–40° to +185°F)

Relative Humidity

0 to 95% non-condensing

Altitude

2000 m

Power Supply

125/250 Volt Power Supply

Rated Supply Voltage:	125–250 Vdc; 110–240 Vac, 50/60 Hz
Input Voltage Range:	88–300 Vdc or 85–264 Vac
Power Consumption:	AC: < 60 VA DC: < 45 W
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 Vdc to 57.6 Vdc
Power Consumption:	< 45 W
Input Voltage Interruptions:	50 ms @ 48 Vdc

Type Tests

Communication Product Testing

IEC 61850-3:2002
IEEE 1613, Class 2

Electromagnetic Compatibility Emissions

IEC 60255-25:2000

Generic Emissions:	CFR 47 Part 15 Severity Level: Class A

Electromagnetic Compatibility Immunity

Conducted RF Immunity:	IEC 60255-22-6:2001 Severity Level: 10 Vrms IEC 6100-4-6:2008 Severity Level: 10 Vrms

Electrostatic Discharge Immunity:	IEC 60255-22-2:2008 Severity Level: 2, 4, 6, 8 kV contact; 2, 4, 8, 15 kV air IEC 61000-4-2:2008 Severity Level: 2, 4, 6, 8 kV contact; 2, 4, 8, 15 kV air IEEE C37.90.3:2001 Severity Level: 2, 4, and 8 kV contact; 4, 8, and 15 kV air
Fast Transient/Burst Immunity:	IEC 60255-22-4:2008 Severity Level: Class A - 4 kV, 5 kHz; 2 kV, 5 kHz on communications ports IEC 61000-4-4:2011 Severity Level: 4 kV, 5 kHz
Magnetic Field Immunity:	IEC 61000-4-10:2001 Severity Level: 100 A/m 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
Power Supply Immunity:	IEC 60255-11:2008 IEC 61000-4-11:2004 IEC 6100-4-29:2000
Radiated Digital Radio Telephone RF Immunity:	ENV 50204:1995 Severity Level: 10 V/m at 900 MHz and 1.89 GHz
Radiated Radio Frequency Immunity:	IEC 60255-22-3:2007 Severity Level: 10 V/m IEC 61000-4-3:2010 Severity Level: 10 V/m IEEE C37.90.2:2004 Severity Level: 35 V/m
Surge Immunity:	IEC 60255-22-5:2008 Severity Level: 1 kV line-to-line, 2 kV line-to-earth IEC 61000-4-5:2005 Severity Level: 1 kV line-to-line, 2 kV line-to-earth
Surge Withstand Capability Immunity:	IEC 60255-22-1:2007 Severity Level: 2.5 kV peak common mode, 1.0 kV peak differential mode IEEE C37.90.1:2002 Severity Level: 2.5 kV oscillatory, 4 kV fast transient waveform

Environmental

Cold:	IEC 60068-2-1:2007 Severity Level: 16 hours at –40°C
Damp Heat, Cyclic:	IEC 60068-2-30:2005 Severity Level: 25°C Relative Humidity: 93% Duration: 4 days
Dry Heat:	IEC 60068-2-2:2007 Severity Level: 16 hours at +85°C
Vibration (Front-Panel Mount Only):	IEC 60255-21-1:1988 Severity Level: Class 2 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 60255-5:2000 3100 Vdc on power supply. Type tested for 1 minute. IEEE C37.90:2005 3100 Vdc on power supply. Type tested for 1 minute.
Impulse:	IEC 60255-5:2000 Severity Level: 0.5 Joule, 5 kV IEEE C37.90:2005 Severity Level: 0.5 Joule, 5 kV

Certifications

ISO 9001:	This product was designed and manufactured under an ISO 9001 certified quality management system.
CE:	EMC Directive, Low Voltage Directive
EMC:	FCC Class A

Section 2
Installation

Introduction

This section includes the following information:

- *Connecting to the Device on page 2.1*
- *Commissioning the Device on page 2.4*
- *Navigating the User Interface on page 2.4*
- *Device Dashboard on page 2.6*

Connecting to the Device

The device includes an HTTPS web server for most configuration and management functions for use with Microsoft® Internet Explorer® 8.

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

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 5.10* for information on enabling an additional IP interface.

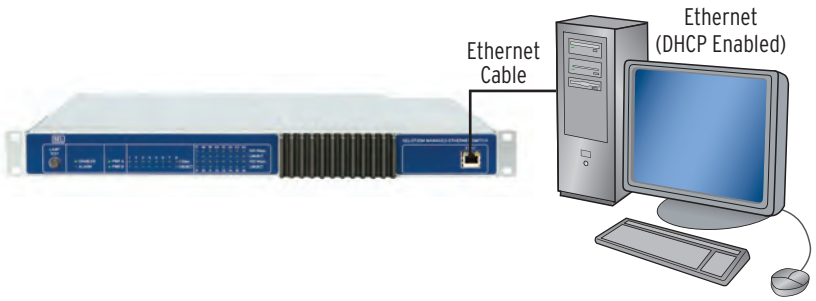


Figure 2.1 Commissioning Network

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 5.10*. 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 2.9*.

To set your computer's network connection 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*. Clicking **OK** will open the **Network Connections** window, which contains a list of the network devices available on your computer.

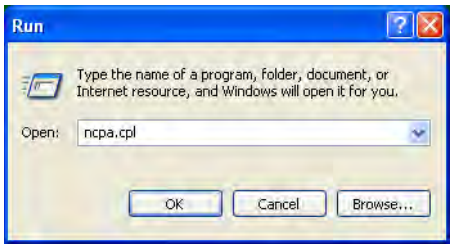


Figure 2.2 Open Network Connections With Run Command

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 **Local Area Connection**.

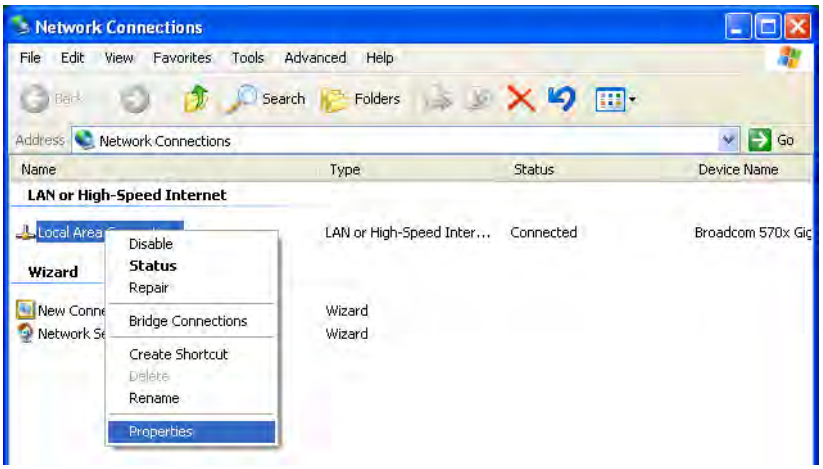


Figure 2.3 Open Connection Properties

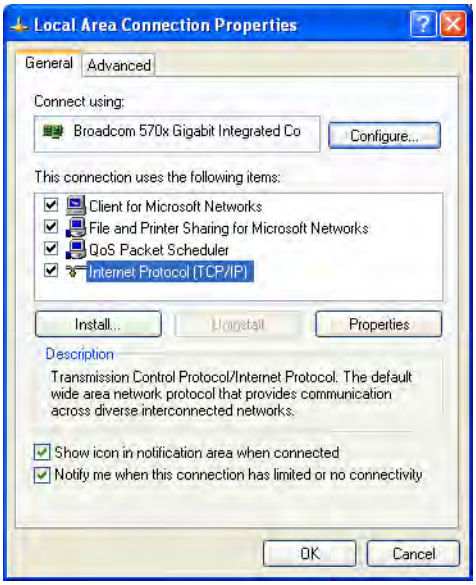


Figure 2.4 Local Area Connection Properties

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). Click the **Properties** button to show the **Internet Protocol (TCP/IP) Properties** window (see *Figure 2.5*).

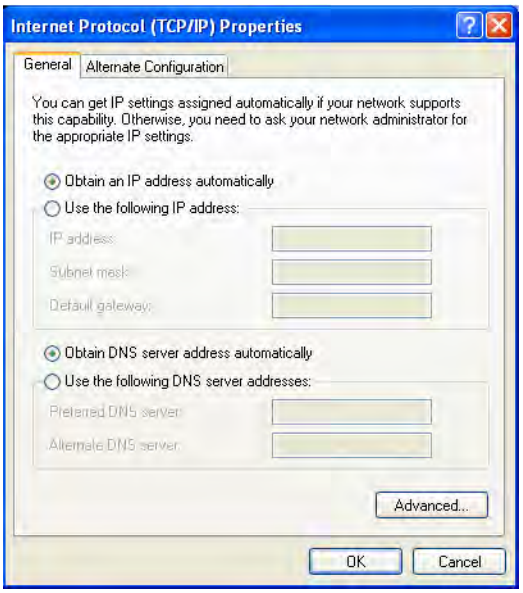


Figure 2.5 Configuring Automatic Network Configuration

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. Click the **OK** button.

Commissioning the Device

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 logon page. Your browser will provide instructions for doing this. For information on creating an X.509 certificate to eliminate this error, please see Section 5: Settings and Commands.

Configure your computer's network connection as described in *Physical Network on page 2.1*. 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., www.selinc.com)—the SEL-2730M will handle resolving the URL and connecting you to its web management interface.

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

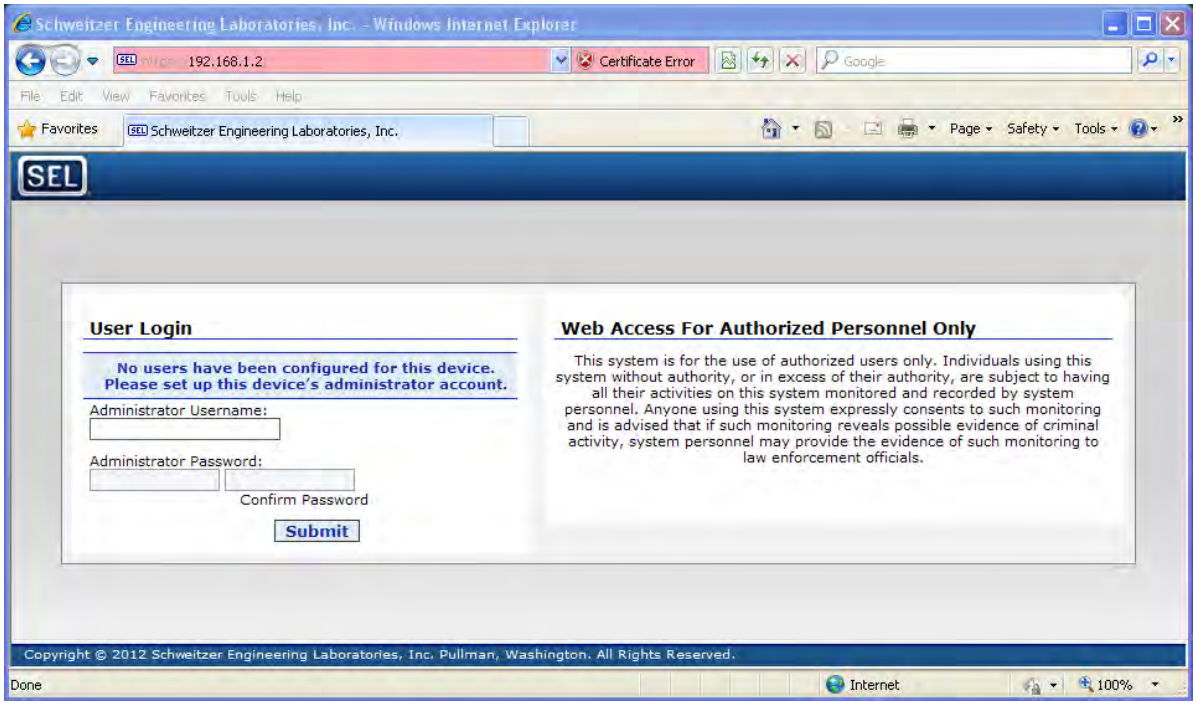


Figure 2.6 Device Commissioning Page

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, since the password characters are hidden.

Step 3. Click the **Submit** button to complete commissioning. When the page reloads, you will be able to log on as the administrative user to set up accounts and configure the system. *Navigating the User Interface on page 2.4* 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 on 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.

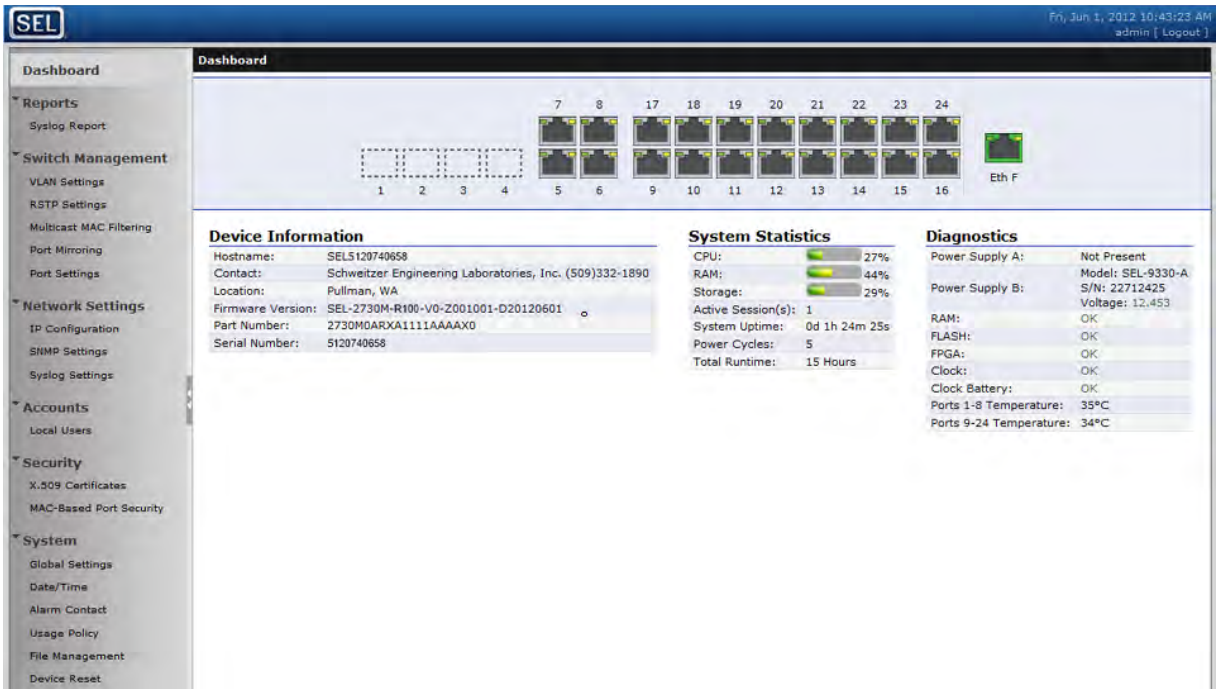


Figure 2.7 Device Dashboard

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 of 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. Clicking on 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.

Clicking 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. Clicking the **Edit** button will show the same form, without the username box.

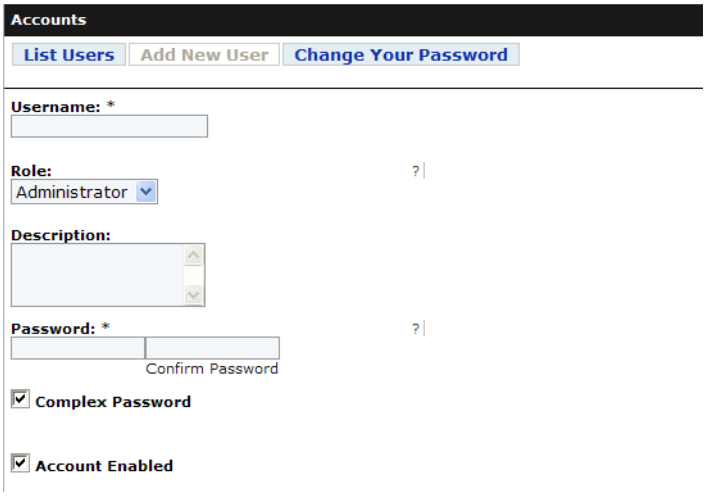


Figure 2.9 Adding a New User

Device Dashboard

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

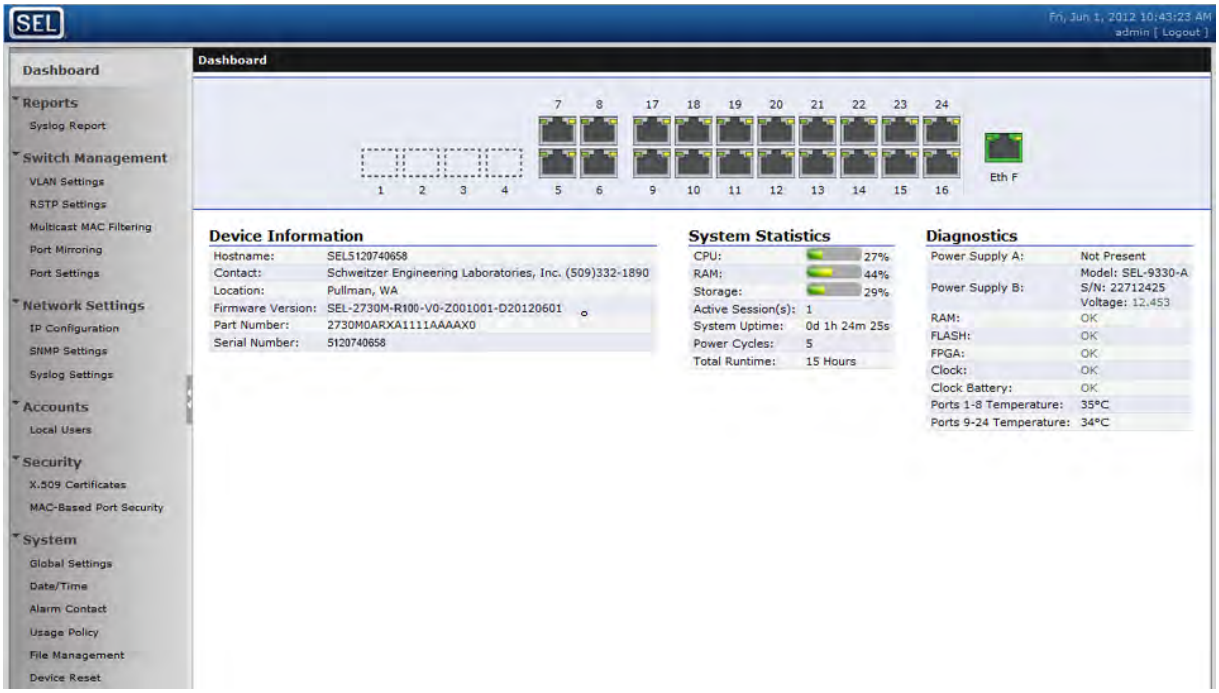


Figure 2.10 Device Dashboard

The device 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 may mouse over any of the network interface port icons to see the current status information of the port. Clicking 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 2.11 Network Interfaces

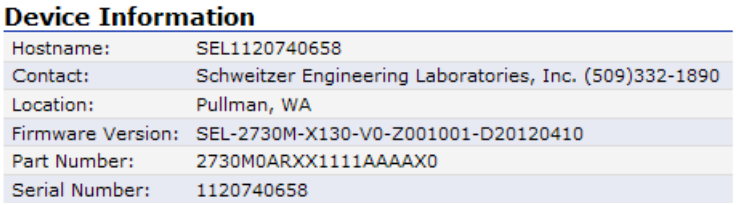
The network interface icons are color coded to indicate the configuration state of that interface. The interface icon colors and their meanings can be found in *Table 2.1*.

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 factory support or firmware upgrades are necessary.



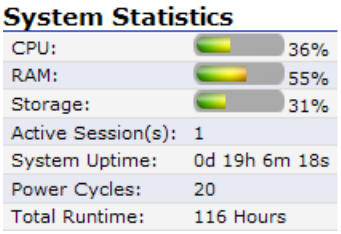
Device Information

Hostname:	SEL1120740658
Contact:	Schweitzer Engineering Laboratories, Inc. (509)332-1890
Location:	Pullman, WA
Firmware Version:	SEL-2730M-X130-V0-Z001001-D20120410
Part Number:	2730M0ARXX1111AAAAX0
Serial Number:	1120740658

Figure 2.12 Version Information

System Statistics

The System Statistics area (see *Figure 2.13*) of the Dashboard provides some basic statistics of device operations. This information can quickly help determine whether the device firmware is operating properly.



System Statistics

CPU:	36%
RAM:	55%
Storage:	31%
Active Session(s):	1
System Uptime:	0d 19h 6m 18s
Power Cycles:	20
Total Runtime:	116 Hours

Figure 2.13 System Statistics

Table 2.2 explains the meaning of each of these statistics. The CPU, RAM, and Storage statistics provide a visual indication of reserve processing or storage capacity in the unit. Any potential problems related to system resource utilization would be noticeable through these statistics on the Dashboard.

Table 2.2 System Statistics (Sheet 1 of 2)

Statistic	Meaning
CPU	Percentage loading of the processor of the SEL-2730M
RAM	Percentage usage of the on-board memory used by the CPU
Storage	Percentage of the nonvolatile storage used by the SEL-2730M to store account information, logs, and other information that is maintained when power is off

Table 2.2 System Statistics (Sheet 2 of 2)

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 the last powerup or reboot
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 2.14*) 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.

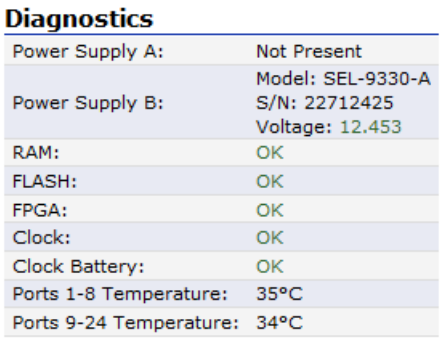


Figure 2.14 Diagnostics

Configuring a Static IP Address in Microsoft Windows Networking

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.

To configure the SEL-2730M 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, please see *Appendix G: Classless Inter-Domain Routing (CIDR)*.

Step 1. Start the Microsoft® Windows® Command Terminal.

a. Open the **Run** command (from the Start menu).

b. Type **cmd** in the text box.

c. Click **OK**.

Figure 2.15 Open Terminal With Run Command

Step 2. In the command window, type **ipconfig <Enter>**. This will show you 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.

a. Type **ncpa.cpl** in the **Run** command.

b. Click **OK**.

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

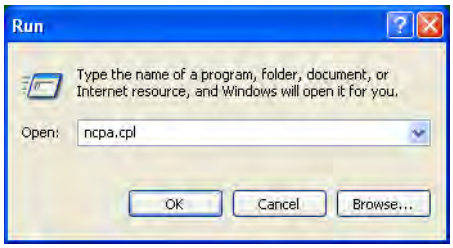


Figure 2.16 Open Network Connections With Run Command

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

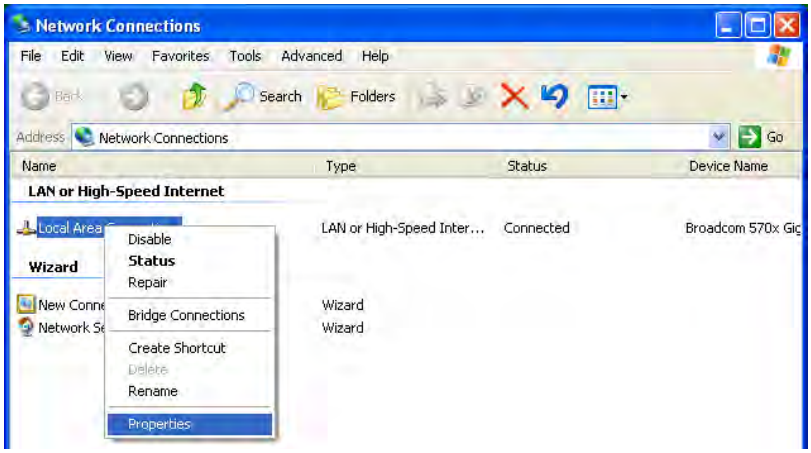


Figure 2.17 Open Connection Properties

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

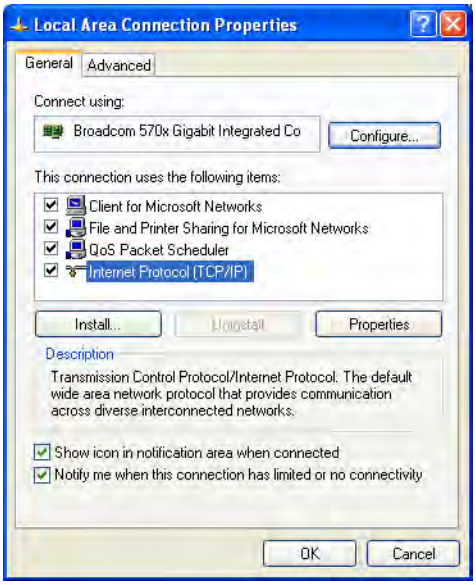


Figure 2.18 Local Area Connection Properties

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 2.19*. Click the **OK** button.

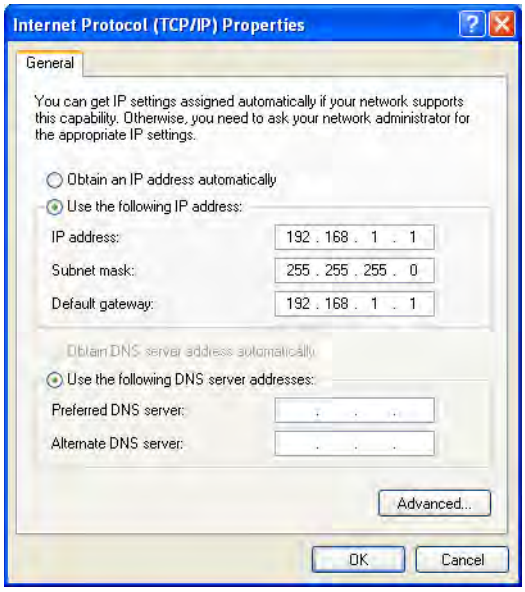


Figure 2.19 Internet Protocol (TCP/IP) Properties

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

This page intentionally left blank

Section 3
Managing Users

Introduction

This section includes the following:

- *User-Based Accounts on page 3.1*
- *Adding a User on page 3.2*
- *Editing a User and Resetting a Password on page 3.2*
- *Removing a User on page 3.3*
- *Enabling or Disabling a User on page 3.3*
- *Changing a User Password on page 3.4*

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 User

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

Step 1. Log on 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. From this page, a user with the Administrator or the User Manager role can view, add, enable, disable, or delete other users.

Step 3. Click **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.

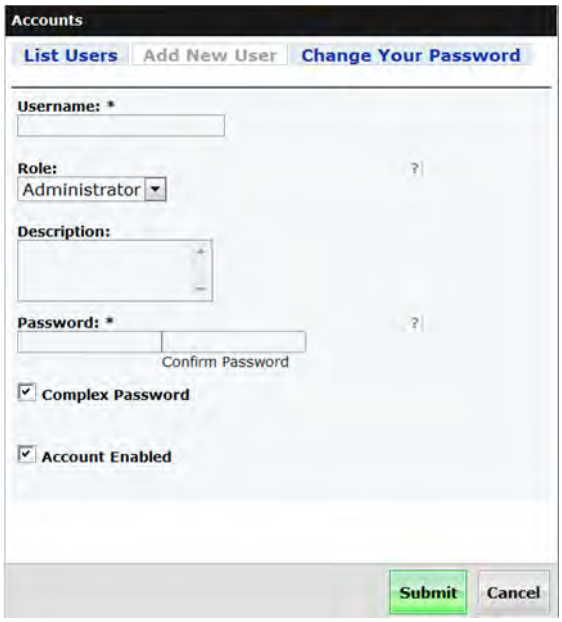


Figure 3.1 Add New User Form

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

Editing a 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. Please perform the following steps to reset an account's password.

Step 1. Log on 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. From this page, a user with the Administrator or the User Manager role can view, add, edit, enable, disable, or delete other users.

Step 3. Click 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 click the **Submit** button.

Removing a 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. Please follow these steps to remove an account.

Step 1. Log on 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. From here, an Administrator or User Manager can view, add, edit, enable, disable, or delete other users.

Step 3. Click 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, click **Delete**. If this person is not the correct user, click **No** to go back to the User Accounts page.

Enabling or Disabling a 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. Please use the following steps to enable or disable a user's account.

Step 1. Log on 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.

Step 3. This link will open the User Accounts page. From here, an Administrator or User Manager can view, add, edit, enable, disable, or delete other users.

Step 4. Click the **Edit** button associated with the account that you want to edit. This step will open the Edit User form.

Step 5. 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. Please use the following steps to change your password.

Step 1. Log on 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 click the **Submit** button to change your password.

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 4.1*
- Example 2: *Configure RSTP Network Topology on page 4.6*
- Example 3: *SNMP Monitoring From a Central Location on page 4.8*

Job Done Example 1

Create VLANs to Effectively Manage Network Traffic

Virtual Local Area Networks (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.

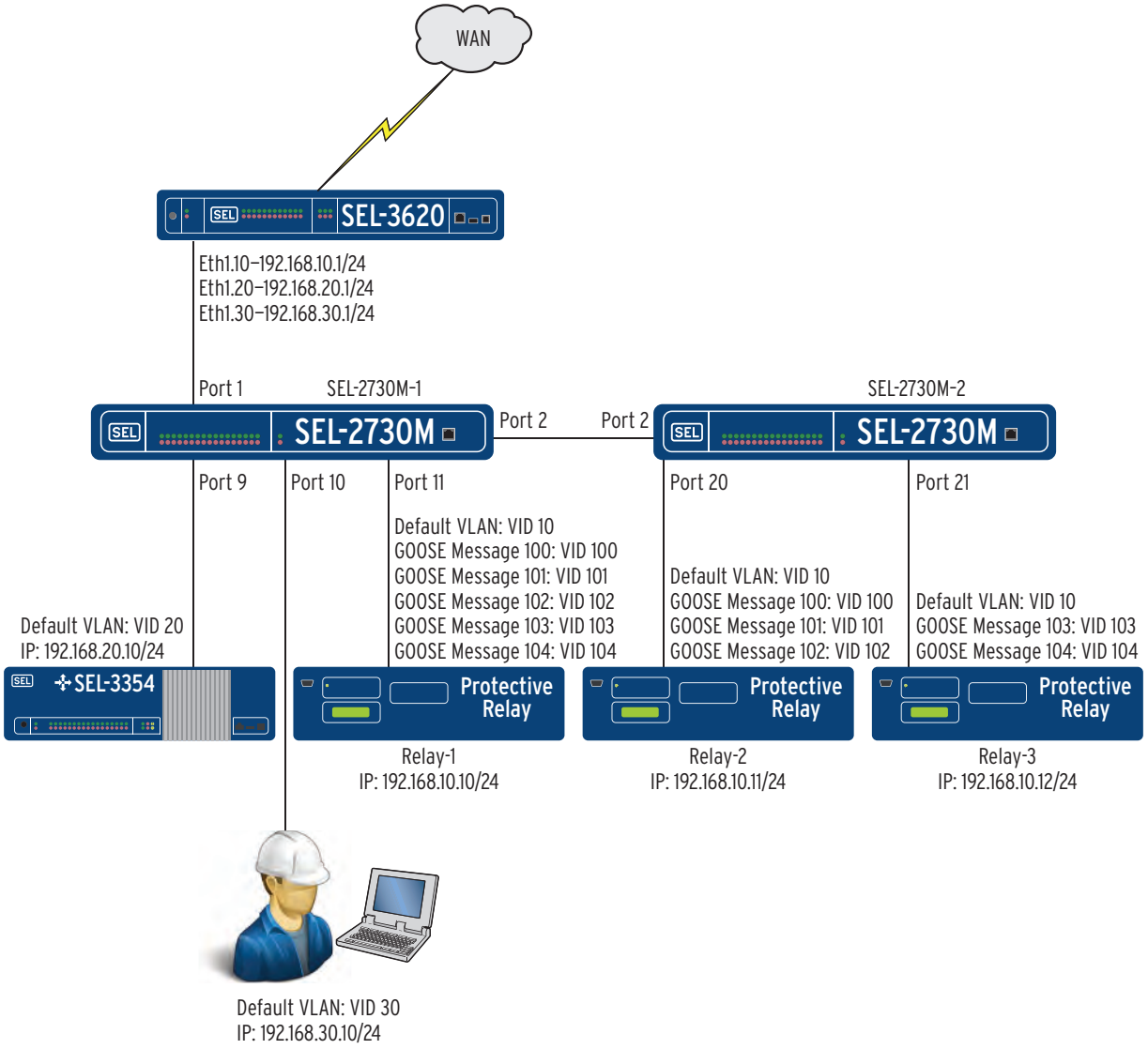


Figure 4.1 Network Diagram

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

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

Step 3. Navigate to VLAN Settings and select **Add New VLAN**.

Step 4. Enter the configuration in *Table 4.2* and click **Submit** to create VLAN 10 on SEL-2730M–1.

Table 4.2 VLAN 10 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
10	Relay LAN	1, 2	11

Step 5. Select **Add New VLAN**.

Step 6. Enter the configuration in *Table 4.3* and click **Submit** to create VLAN 20 on SEL-2730M–1.

Table 4.3 VLAN 20 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
20	SCADA LAN	1, 2	9

Step 7. Select **Add New VLAN**.

Step 8. Enter the configuration in *Table 4.4* and click **Submit** to create VLAN 30 on SEL-2730M–1.

Table 4.4 VLAN 30 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
30	Engineering Access LAN	1, 2	10

Step 9. Select **Add New VLAN**.

Step 10. Enter the configuration in *Table 4.5* and click **Submit** to create VLAN 100 on SEL-2730M–1.

Table 4.5 VLAN 100 Configuration

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

Step 11. Select **Add New VLAN**.

Step 12. Enter the configuration in *Table 4.6* and click **Submit** to create VLAN 101 on SEL-2730M–1.

Table 4.6 VLAN 101 Configuration

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

Step 13. Select **Add New VLAN**.

Step 14. Enter the configuration in *Table 4.7* and click **Submit** to create VLAN 102 on SEL-2730M–1.

Table 4.7 VLAN 102 Configuration

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

Step 15. Select **Add New VLAN**.

Step 16. Enter the configuration in *Table 4.8* and click **Submit** to create VLAN 103 on SEL-2730M–1.

Table 4.8 VLAN 103 Configuration

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

Step 17. Select **Add New VLAN**.

Step 18. Enter the configuration in *Table 4.9* and click **Submit** to create VLAN 104 on SEL-2730M–1.

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*.

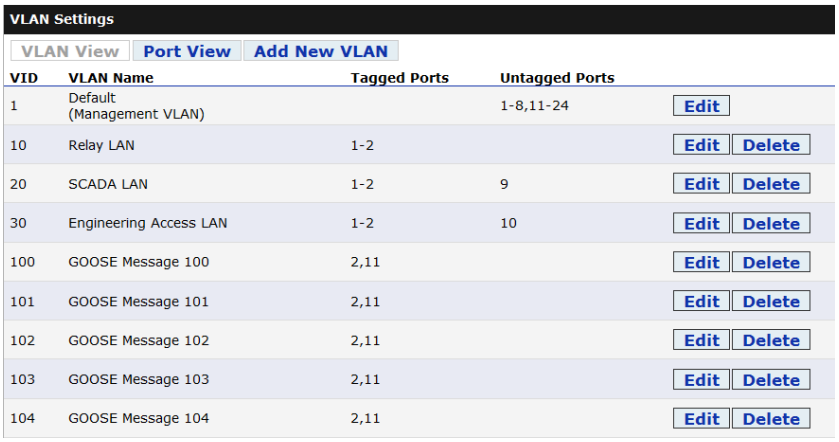


Figure 4.2 SEL-2730M-1 VLAN Configuration

Configure VLANs on SEL-2730M–2

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

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

Step 3. Navigate to VLAN Settings and select **Add New VLAN**.

Step 4. Enter the configuration in *Table 4.10* and click **Submit** to create VLAN 10 on SEL-2730M–2.

Table 4.10 VLAN 10 Configuration

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

Step 5. Select **Add New VLAN**.

Step 6. Enter the configuration in *Table 4.11* and click **Submit** to create VLAN 20 on SEL-2730M–2.

Table 4.11 VLAN 20 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
20	SCADA LAN	2	None

Step 7. Select **Add New VLAN**.

Step 8. Enter the configuration in *Table 4.12* and click **Submit** to create VLAN 30 on SEL-2730M–2.

Table 4.12 VLAN 30 Configuration

VID	VLAN Name	Tagged Ports	Untagged Ports
30	Engineering Access LAN	2	None

Step 9. Select **Add New VLAN**.

Step 10. Enter the configuration in *Table 4.13* and click **Submit** to create VLAN 100 on SEL-2730M–2.

Table 4.13 VLAN 100 Configuration

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

Step 11. Select **Add New VLAN**.

Step 12. Enter the configuration in *Table 4.14* and click **Submit** to create VLAN 101 on SEL-2730M–2.

Table 4.14 VLAN 101 Configuration

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

Step 13. Select **Add New VLAN**.

Step 14. Enter the configuration in *Table 4.15* and click **Submit** to create VLAN 102 on SEL-2730M–2.

Table 4.15 VLAN 102 Configuration

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

Step 15. Select **Add New VLAN**.

Step 16. Enter the configuration in *Table 4.16* and click **Submit** to create VLAN 103 on SEL-2730M–2.

Table 4.16 VLAN 103 Configuration

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

Step 17. Select **Add New VLAN**.

Step 18. Enter the configuration in *Table 4.17* and click **Submit** to create VLAN 104 on SEL-2730M–2.

Table 4.17 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*.

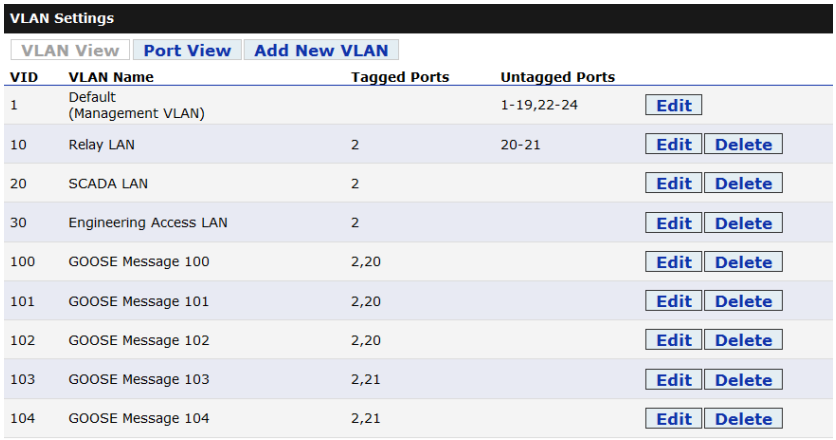


Figure 4.3 SEL-2730M-2 VLAN Configuration

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 Link will be the path communications will take unless there is a link or device failure impacting that communications path. In the event of such a failure, the Blocking RSTP Link will become the active communications path. Without RSTP, the network topology depicted in the figure below would have a loop, which would be detrimental to the network.

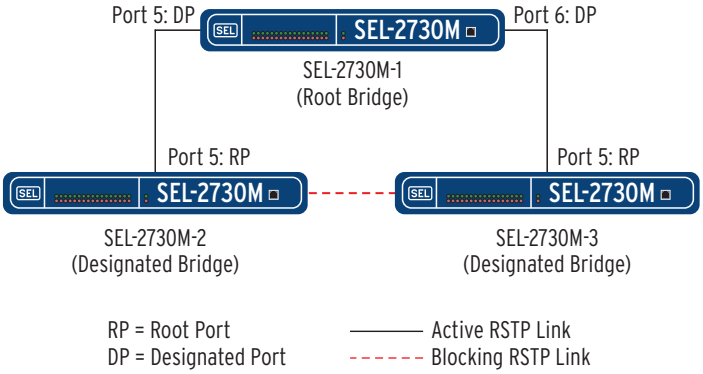


Figure 4.4 RSTP Network Topology

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 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 into 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 will be 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.

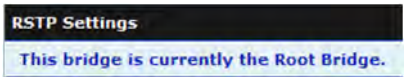


Figure 4.5 RSTP Root Bridge Notification

Job Done Example 3

SNMP Monitoring From a Central Location

Simple Network Monitoring 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. SNMP v3 is used in this example, but the steps to configure SNMP v2c are very similar.

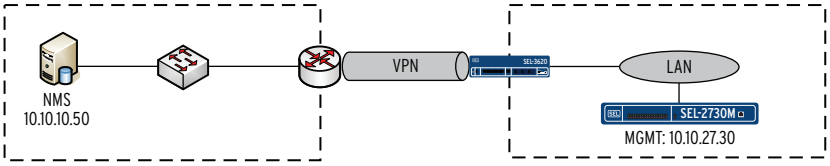


Figure 4.6 SNMP Network Diagram

Configure SNMP on the SEL-2730M

Step 1. Log into 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 click **Submit**.

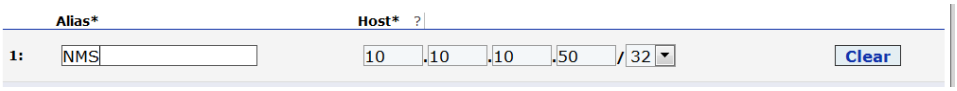


Figure 4.7 Edit Hosts Configuration

Step 3. Select the **Add v3 Profile** tab at the top of the SNMP Settings page. Configure the SNMP v3 settings as shown below and click **Submit**. These settings must match the SNMP v3 configuration on the NMS.

Figure 4.8 SNMP v3 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.

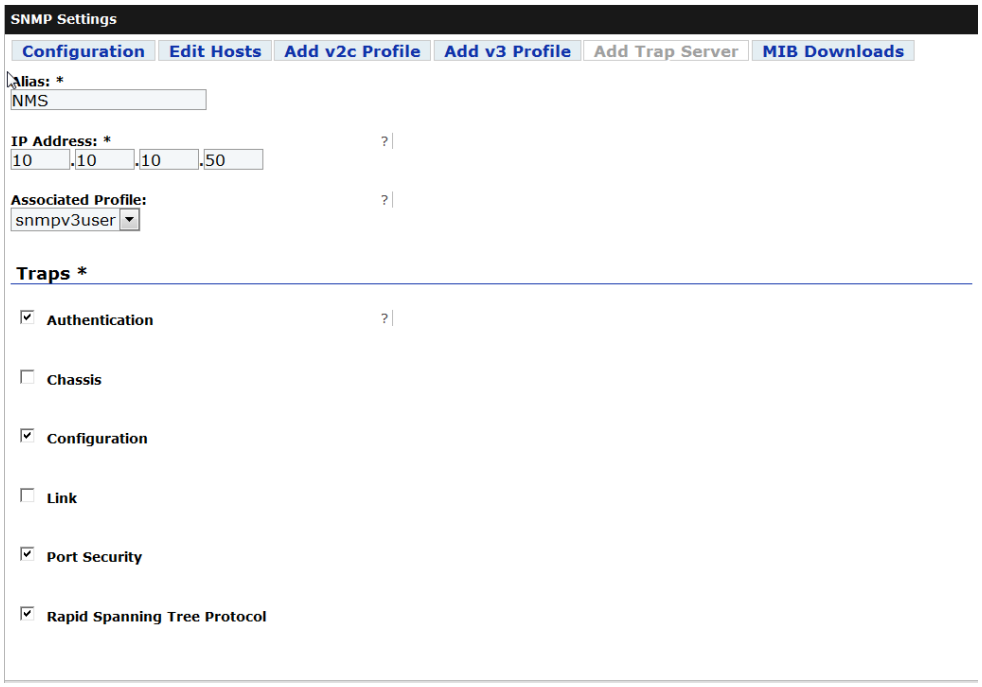


Figure 4.9 Add Trap Server

This page intentionally left blank

Section 5
Settings and Commands

Introduction

This section explains the settings and commands of the device.

- *Reports on page 5.1*
  - Syslog Report
- *Switch Management on page 5.3*
  - VLAN Settings
  - RSTP Settings
  - Multicast MAC Filtering
  - Port Mirroring
  - Port Settings
- *Network Settings on page 5.10*
  - IP Configuration
  - SNMP Settings
  - Syslog Settings
- *Accounts on page 5.19*
  - Local Users
- *Security on page 5.19*
  - X.509 Certificates
  - MAC-Based Port Security
- *System on page 5.22*
  - Global Settings
  - Date/Time
  - Alarm Contact
  - Usage Policy
  - File Management
  - Device Reset

Reports

Syslog Report

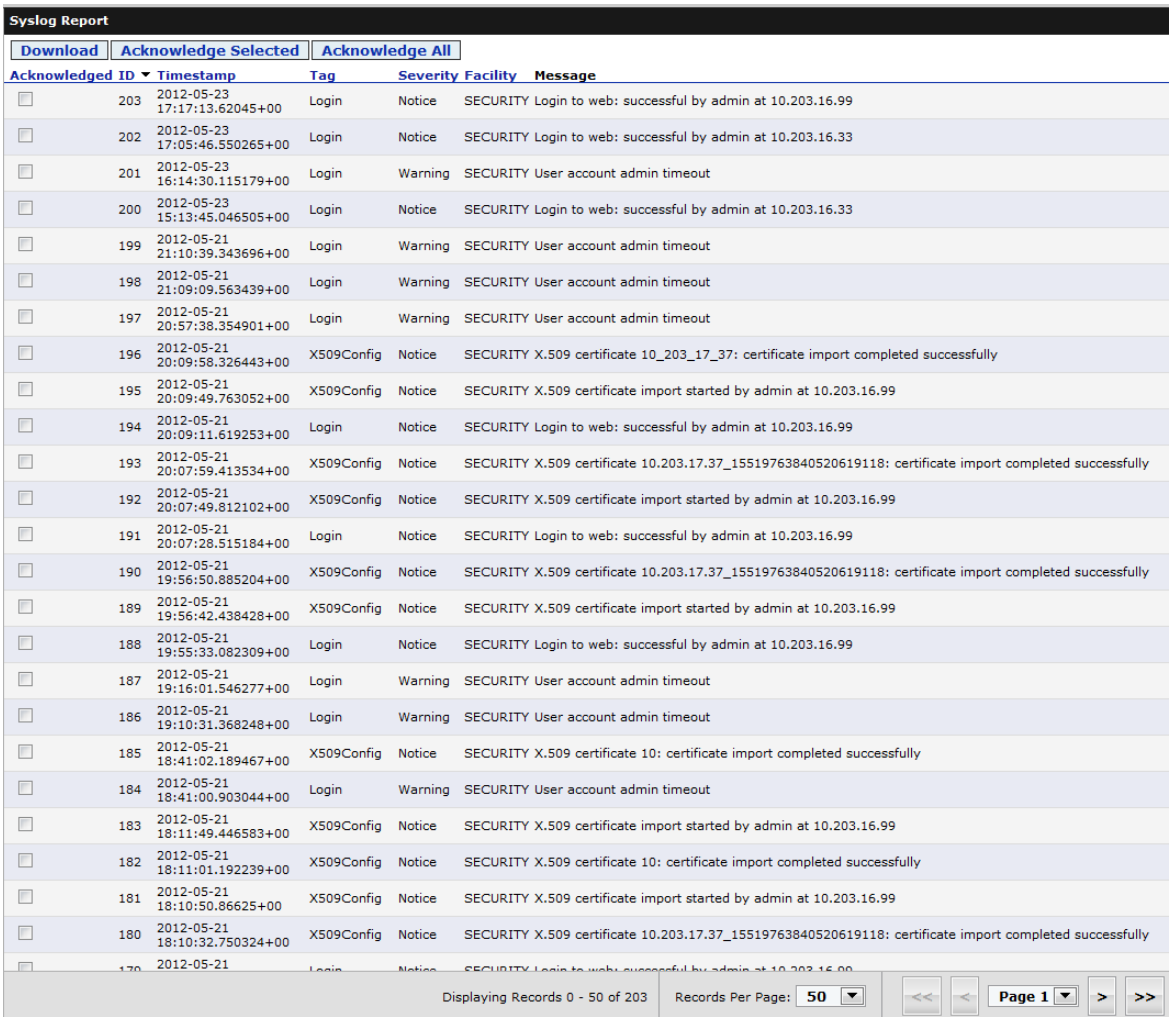
The SEL-2730M uses the Syslog message format to record event data. The device has storage for 60,000 of these messages. The device can also forward Syslog messages to three destinations.

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 D: 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 will limit the logs of concern to only those logs the device has generated since the last examination.

Click 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.

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 5.22* for information on enabling VLAN-aware mode.

Table 5.1 VLAN Settings

Field Name	Values	Default	Description
VID	1 to 4094	N/A	The VLAN Identifier (VID) identifies the VLAN in 802.1Q 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 are allowed to ingress and egress frames for the VLAN.
Untagged Ports	Available ports	N/A	Untagged Ports tag all untagged frames with the VID of the VLAN they are associated with.

VLAN View

The VLAN View page (*Figure 5.2*) provides a VLAN-centric view of the configuration of VLANs and the member ports. The Edit button is available for each VLAN when the device is in VLAN-aware mode.

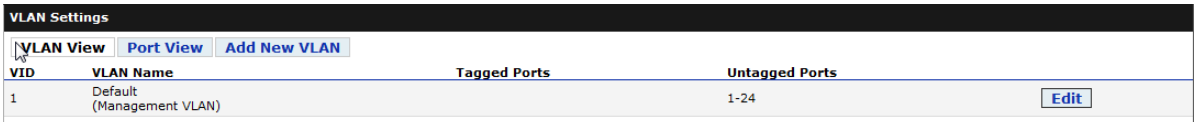


Figure 5.2 VLAN View

To edit an existing VLAN, click the **Edit** button for the VLAN that you would like to update. You will be presented with a configuration page similar to the one shown in *Figure 5.3*.

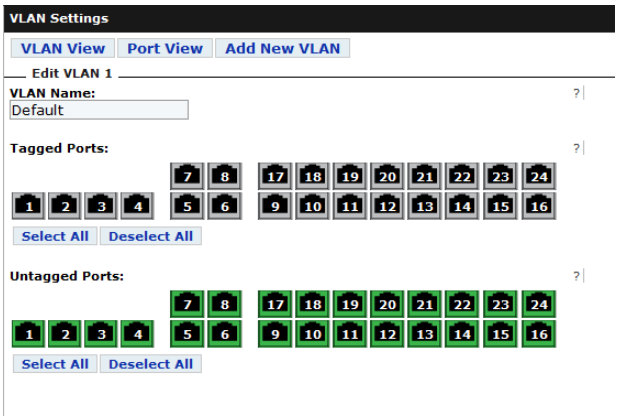


Figure 5.3 Edit VLAN 1

Tagged Ports

Tagged Ports are used to determine which ports are allowed to ingress and egress frames for a given VLAN. Devices capable of 802.1Q 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 the frame to ingress or egress, the port the frame is ingressing or egressing must be configured as a Tagged Port for the VLAN.

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 is capable of passing traffic among multiple VLANs. *Figure 5.4* shows an example of two switches with a trunk link carrying VLANs 100, 101, and 102. To configure a trunk port, each switch would need to add Port 1 as a Tagged Port for VLANs 100, 101, and 102.

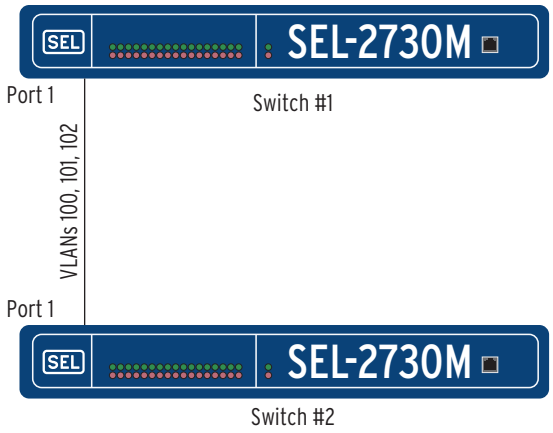


Figure 5.4 Switch Trunk Link

Another example of using VLAN tagging is with the IEC 61850 GOOSE protocol. The IEDs tag GOOSE messages with a VID. For this message to ingress or egress the switch, you must configure the port the GOOSE message is ingressing or egressing as a Tagged Port for the VID tag of the GOOSE frame. In the example shown in *Figure 5.5*, two IEDs must use GOOSE messages tagged with VIDs 200, 201, and 202 to communicate through the switch. 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 ingress and egress the switch.

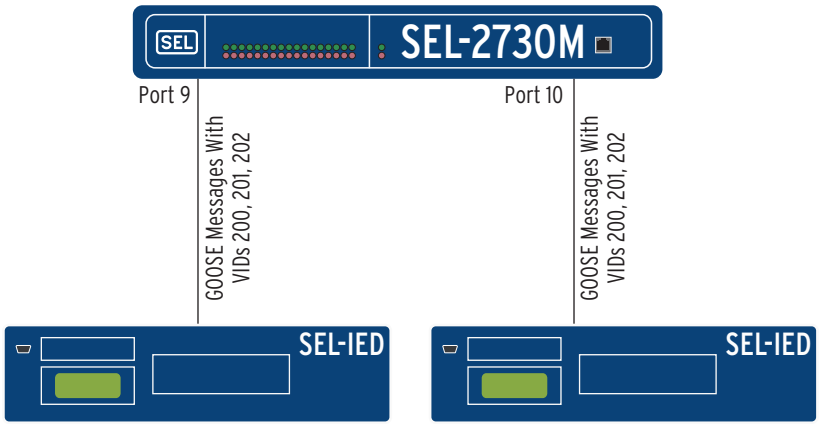


Figure 5.5 GOOSE Message

Untagged Ports

Some frames ingress the device untagged and will need to be assigned a VID to be forwarded to other devices within the same VLAN. Untagged Ports receive untagged frames from devices connected to the port and apply the VID of the VLAN to which the port is assigned. Each port must be assigned as an untagged port in one VLAN. Ports cannot be assigned as an untagged port in multiple VLANs.

In the example shown in *Figure 5.6*, an engineer must log on to the SEL IED to perform maintenance. Communications from the SEL-3354 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.

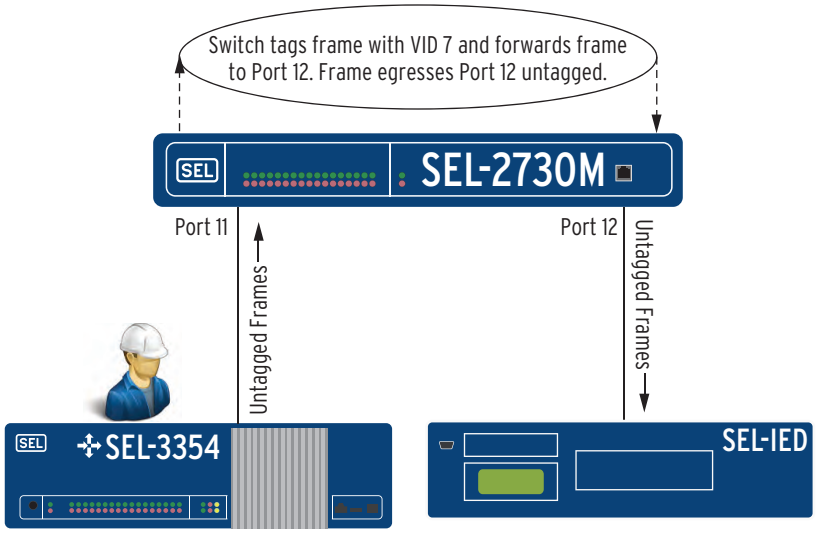


Figure 5.6 Untagged Ports

Port View

The Port View page (see *Figure 5.7*) 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.

Figure 5.7 Port View

Add New VLAN

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

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

Step 2. Navigate to the **VLAN Settings** page and select **Add New VLAN**. You will be presented with the following page.

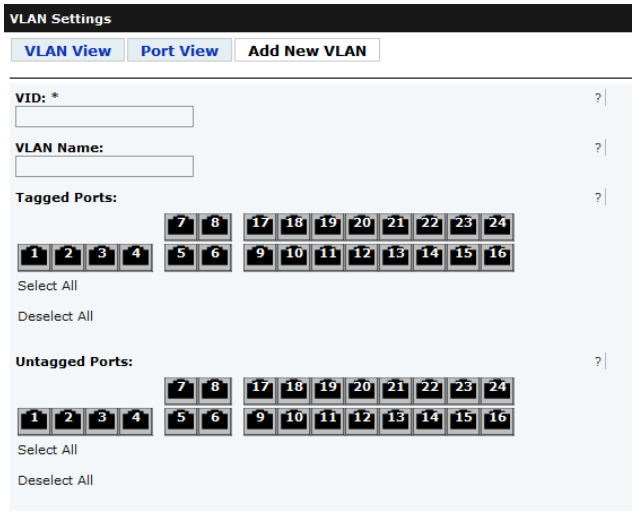


Figure 5.8 Add New VLAN

Step 3. Assign a **VID**, optionally enter a **VLAN Name**, and assign the port(s) based on your required configuration. *VLAN Settings on page 5.3* 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.

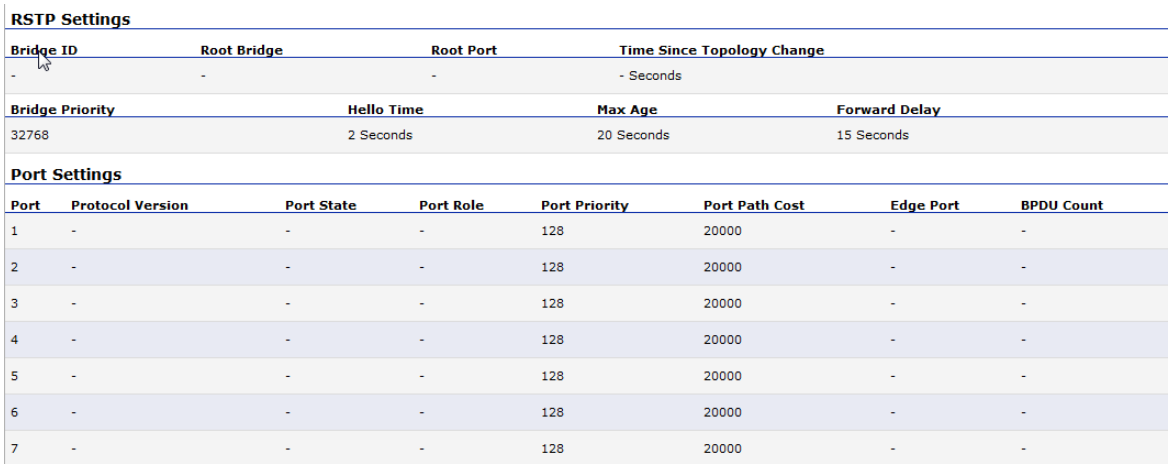
If RSTP is disabled, the following message displays at the top of the RSTP Settings page.

Figure 5.9 RSTP Disabled

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

Configuration

Figure 5.10 shows the RSTP configuration of the device. The following text describes each item on the page.



RSTP Settings

Bridge ID	Root Bridge	Root Port	Time Since Topology Change
-	-	-	- Seconds

Bridge Priority	Hello Time	Max Age	Forward Delay
32768	2 Seconds	20 Seconds	15 Seconds

Port Settings

Port	Protocol Version	Port State	Port Role	Port Priority	Port Path Cost	Edge Port	BPDU Count
1	-	-	-	128	20000	-	-
2	-	-	-	128	20000	-	-
3	-	-	-	128	20000	-	-
4	-	-	-	128	20000	-	-
5	-	-	-	128	20000	-	-
6	-	-	-	128	20000	-	-
7	-	-	-	128	20000	-	-

Figure 5.10 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.

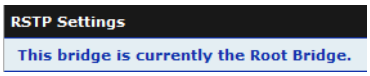


Figure 5.11 Root Bridge Notification

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.

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 seconds during which the information in a BPDU is valid.

Forward Delay

The forward delay is the time 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.

RSTP Settings

Table 5.2 RSTP Settings (Sheet 1 of 2)

Field Name	Values	Default	Description
Bridge Priority	0–61440 in increments of 4096	32768	Bridge priority helps determine the root bridge. The lower the value, the more likely the device will be the root bridge.
Hello Time	1–10 s	2 s	Interval in which device sends BPDUs.

Table 5.2 RSTP Settings (Sheet 2 of 2)

Field Name	Values	Default	Description
Max Age	6–40 s	20 s	Maximum number of seconds during which the information in a BPDU is valid.
Forward Delay	4–30 s	15 s	The time 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.

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 VLAN. If a match does occur, the device sends the frame to only the member ports the device configuration specifies.

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

Step 1. Log on 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.

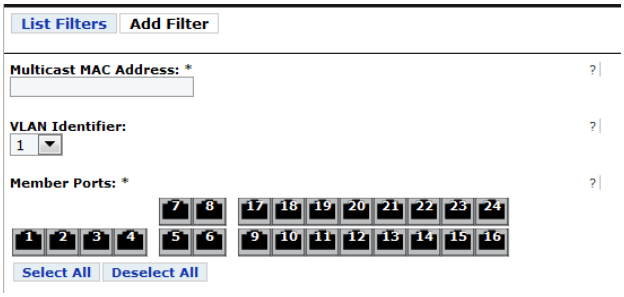


Figure 5.12 Add New Filter

Step 3. Enter the multicast MAC address on which you would like to filter the VLAN identifier of the VLAN on which the multicast traffic is located, and the member ports.

NOTE: This VLAN Identifier field displays only when the device is in VLAN-aware mode.

NOTE: The device automatically updates the member ports with the ports that are members of the VLAN you selected.

Step 4. Click **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 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 use of a non-intrusive troubleshooting technique for gathering network traffic information for a connected port.

The device can mirror network traffic from one source port to one target port. The source port may be any physical port on the device except the target port 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 5.13*, 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.

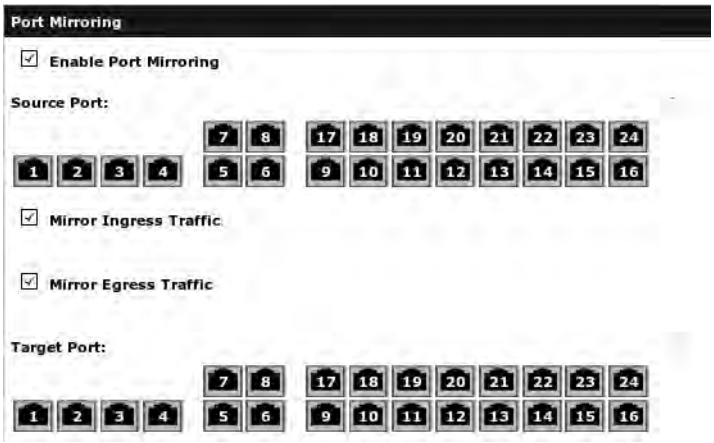


Figure 5.13 Port Mirroring

Port Settings

The Port Settings page provides you the ability to enable and disable ports, set an alias for a port, and configure port speed and duplex mode. 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.

Network Settings

IP Configuration

The IP Configuration page provides the configuration options for the Internet Protocol (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 5.14*.

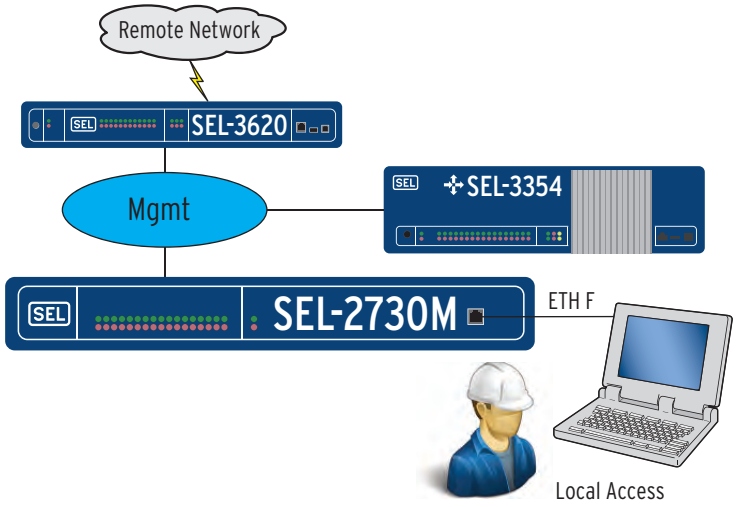


Figure 5.14 IP Configuration

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 only for local access and is not considered a switch fabric 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 5.4 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 5.5 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.
HTTPS	Enabled, Disabled	Enabled	Enables or disables HTTPS on the interface.
Captive Port	Enabled, Disabled	Enabled	Enables or disables captive port on the interface.

When captive port is enabled on **ETH F**, the device issues 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 use of this feature. Simply open your web browser and navigate to any site (e.g., www.selinc.com); the device resolves this query to the ETH F IP address and redirects you to the web management interface of the device.

Table 5.6 Mgmt Network Interface Settings

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.

SNMP Settings

The device supports SNMP v2c and v3 read-only operations. Use SNMP to monitor device health, status, and to gather data. *Figure 5.15* shows the SNMP Settings page.

Figure 5.15 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* 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 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, click **Edit Hosts**. This will take you to the page shown in *Figure 5.16*.

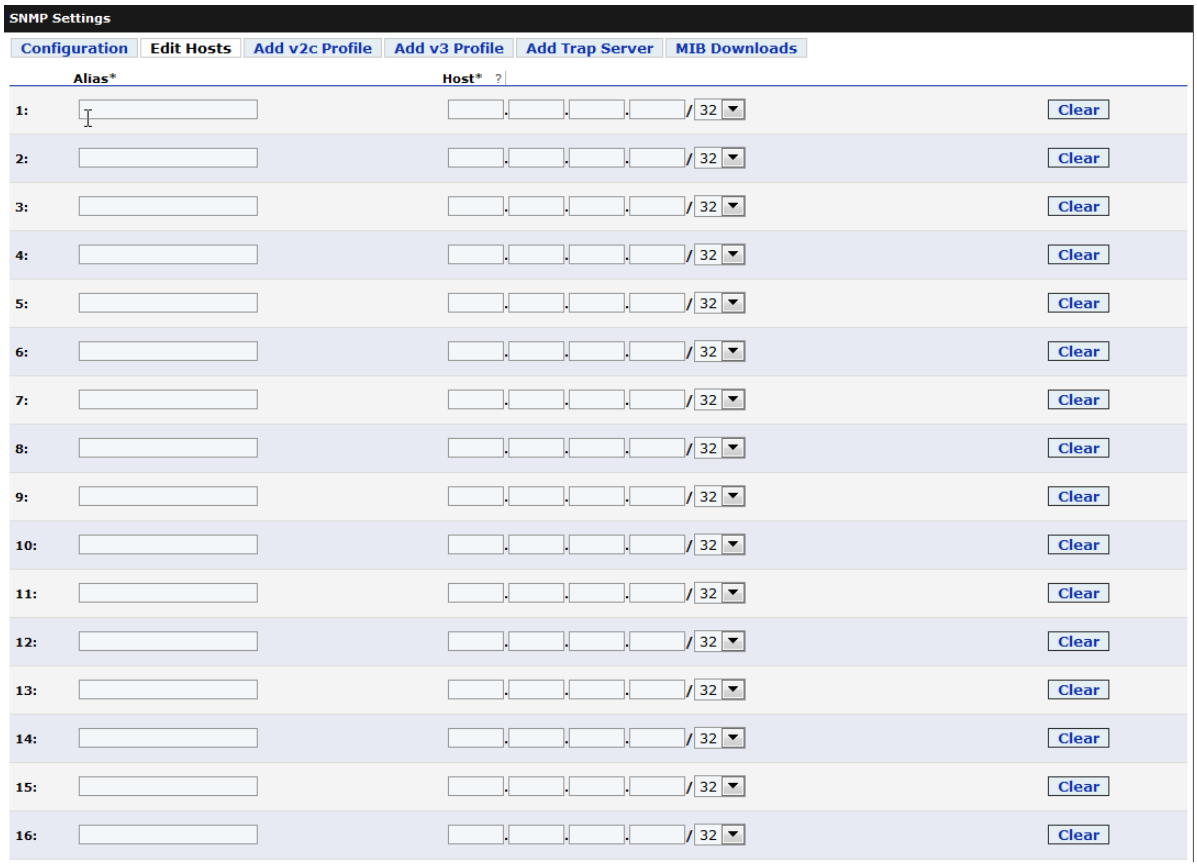


Figure 5.16 Edit Hosts

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 Edits Hosts page allows you to enter as many as 16 entries on this page.

Step 5. Click **Submit** to complete.

Table 5.7 Edit Hosts Settings

Field Name	Values	Default	Description
Alias	1 to 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 v2c Profile

The Add v2c Profile page allows you to add an SNMP v2c profile. Perform the following steps to add an SNMP v2c profile:

Step 1. From the SNMP Settings page, click **Add v2c Profile**. This will take you to the page shown in *Figure 5.17*.

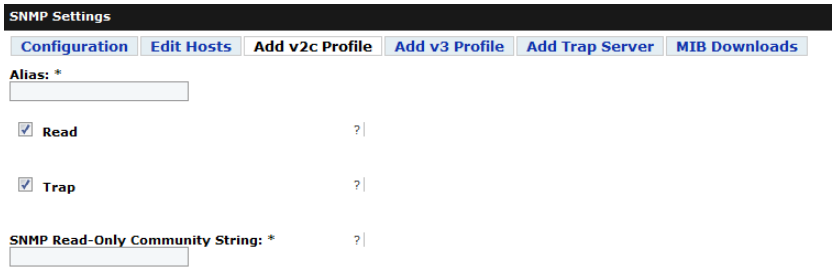


Figure 5.17 Add v2c Profile

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. Click **Submit** to add the SNMP profile.

Add v3 Profile

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

Step 1. From the SNMP Settings page, click **Add v3 Profile**. This will take you to the page shown in *Figure 5.18*.

Figure 5.18 Add v3 Profile

Step 2. Enter the **Username** you would like to use for the SNMP v3 user.

NOTE: SNMP v3 provides authentication and encryption to ensure a secure SNMP communications channel. SNMP v2c provides mutual authentication through use of a pre-shared key and the SNMP Read Only Community String, but SNMP communication is in plaintext.

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. Click **Submit** to add the SNMP profile.

Table 5.8 SNMP Profile Settings

Field Name	Values	Default	Description
Username	1–64 characters	N/A	SNMP v3 username
Alias	1–64 characters	N/A	SNMP v2c 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 (SNMP v2c only)
Authentication Protocol	None, MD5, SHA-1	SHA-1	Authentication protocol to use for authenticating SNMP messages between this SNMP user and SNMP manager (SNMP v3 only)
Authentication Password	8–128 characters	N/A	Cannot be the same as the Encryption Password (SNMP v3 only)
Encryption Protocol	None, DES, AES-128	AES-128	Encryption protocol to use for encrypting SNMP messages between this SNMP user and SNMP manager (SNMP v3 only)
Encryption Password	8–128 characters	N/A	Cannot be the same as the Authentication Password (SNMP v3 only)

Add Trap Server

The Add Trap Server page allows you to add SNMP trap servers to which the device will send SNMP traps. At least one SNMP profile with trap permission is necessary. The following message displays on the Add Trap Server page if no SNMP profiles are configured with trap permission.

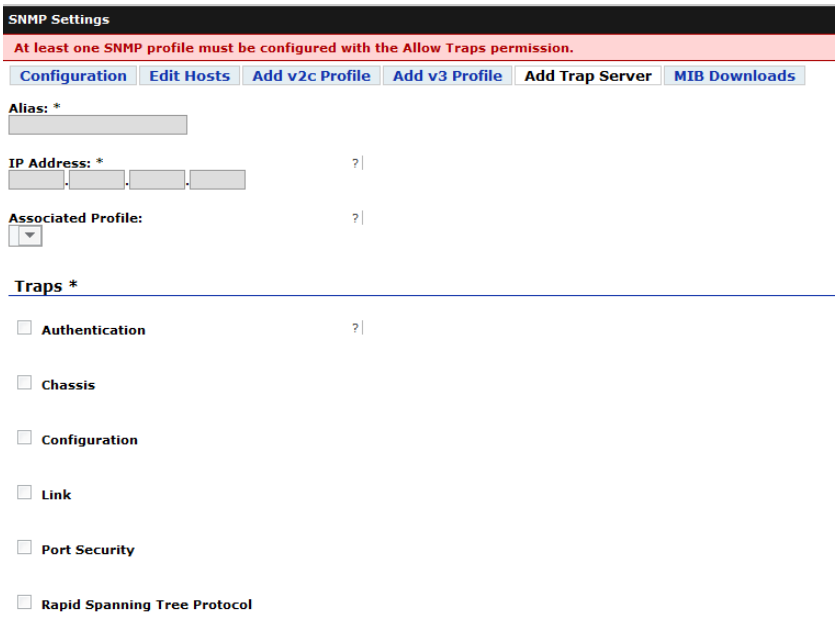


Figure 5.19 SNMP Trap Permissions Are Required

The device will send traps to the configured trap server through 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, click **Add Trap Server**. This will take you to the page shown in *Figure 5.20*.

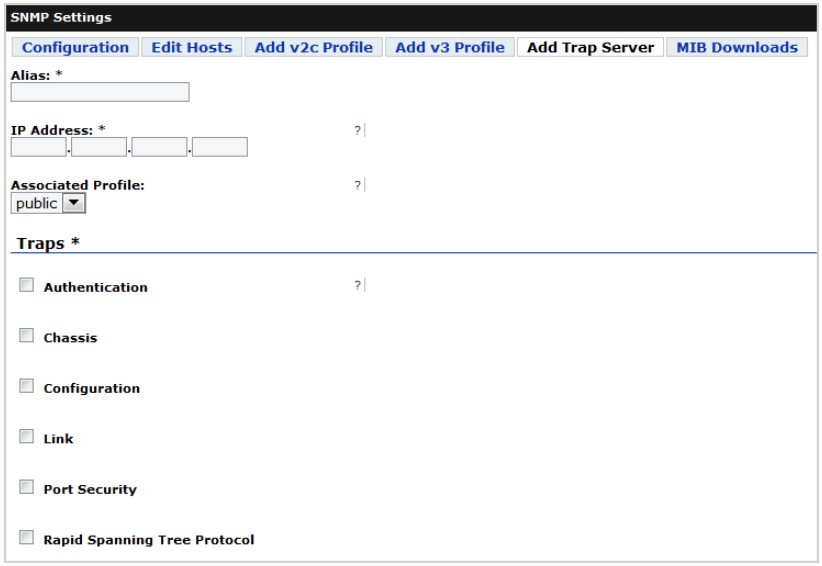


Figure 5.20 Add Trap Server

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. Click **Submit** to add the SNMP trap server.

Table 5.9 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	SNMP profile whose identity you will use to send traps.
Traps	See *Table 5.10*.	N/A	The device will send SNMP traps to the configured trap server when an event occurs within the selected trap category.

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 5.10 SNMP Trap Categories

Category	Description
Authentication	Authentication-related events
Chassis	Physical hardware-related events
Configuration	Configuration events related to settings changes
Link	Interface 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 Managment 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 clicking 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 on attempts, and configuration changes. The device can send its log information to three 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, please refer to *Appendix D: Syslog*.

Select the **Syslog Settings** link from the navigation menu to configure the Syslog settings for the device. The Syslog Settings page (see *Figure 5.21*) allows you to configure the local logging threshold, as well as remote Syslog destinations. The Local Logging Threshold setting indicates the minimum severity that a Syslog message must have for the device to store that message locally. Similarly, the logging threshold under Syslog Destinations determines

the minimum severity that a Syslog message must have for that message to be sent to the configured Syslog server. For a description of these severity levels, please refer to *Appendix D: Syslog*.

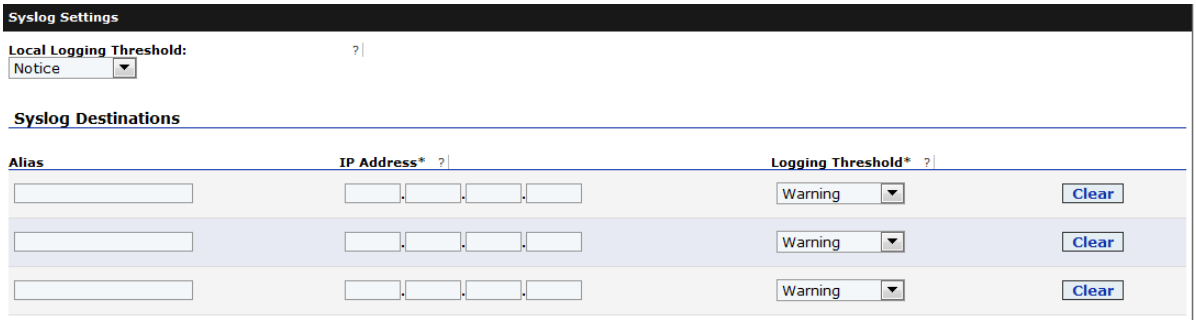


Figure 5.21 Syslog Settings

Table 5.11 Syslog Threshold Values

Field Name	Values	Default	Description
Local Logging Threshold	Error Warning Notice Informational	Notice	The minimum severity level that an event must have to be stored locally on the device.

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

The settings under Syslog Destinations are to configure remote Syslog destinations. These destinations are the Syslog servers that will store the Syslog events remotely. 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 specify the logging threshold of the Syslog events to be sent to the remote Syslog server.

Table 5.12 Syslog Destination Settings

Field Name	Values	Default	Description
Alias	1–32 characters	N/A	A name that is associated with the Syslog destination.
IP Address	Unicast IP Address	N/A	The IP address of the Syslog destination.
Logging Threshold	Alert Critical Error Warning Notice Informational	Warning	The minimum severity level that an event must have to be forwarded to this destination.

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 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.

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 5.22 Renaming Certificates

Export

This option provides a form for exporting the installed certificate. Descriptions follow for the two available export options.

Certificate Text

Export the certificate by copying and pasting the certificate text into a text file.

CSR Text

The certificate signing request (CSR) text will be empty unless the X.509 certificate has been generated on the device through use of the Regenerate option from the X.509 Certificates page. If the certificate has been regenerated on the device, it is still considered a self-signed certificate and will cause a security alert in web browsers accessing the device. To sign the certificate

using a trusted certificate authority (CA), export the CSR Text and send the certificate signing request to the CA administrator. Once the CA administrator signs the request, the CA administrator will provide a file that you can import through use of the Import option on the X.509 Certificates page.

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.

Regenerate

Use the Regenerate option to create a new self-signed X.509 certificate for the device. Once generated, the certificate signing request (CSR) can be exported and signed by a CA and then imported back into the device as a signed X.509 certificate.

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

MAC-Based Port Security

MAC-based port security provides the ability to create MAC address filters that only allow traffic on a port from specific MAC addresses. 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

Click 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.

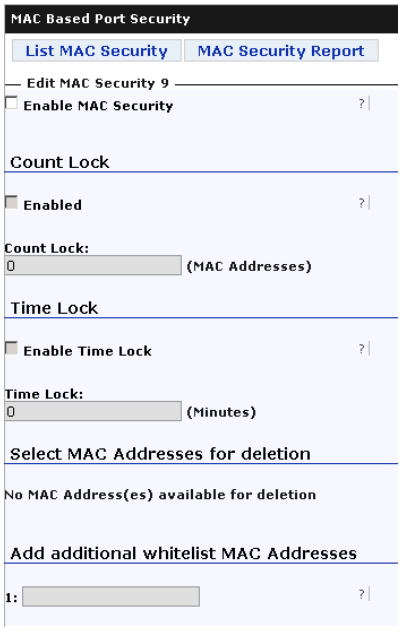


Figure 5.23 MAC-Based Port Security

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 5.13*.

Table 5.13 MAC Security Fields

Field Name	Values	Description
Count Lock	1–1000 MAC Addresses	The number of MAC addresses that will be added to the filter.
Time Lock	1–1440 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.

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 5.14 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 will default to the highest priority accepted language the requesting client web browser specifies that is a supported language for the web management interface of the device. In the event of a tie in priorities of supported languages, the device selects the language based on the Language setting configured in the Global Settings. If none of the requested languages are supported, the language defaults to the Language setting configured in the Global Settings. The device always 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 5.15 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 5.16 Features

Field Name	Values	Default	Description
VLAN-aware	Enabled, Disabled	Disabled	Determines the operational mode of the device with respect to VLANs.
CoS Mode	Weighted Round Robin, Strict	Weighted Round Robin	Sets the device's queue scheduling scheme for egressing frames. Weighted Round Robin will cycle through each egress priority queue, using an 8:4:2:1 ratio to transmit Critical, High, Medium, and Low traffic frames, respectively. Strict priority will always egress traffic from a higher priority queue before a lower priority queue.
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 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 device determines daylight-saving adjustments. To select a time zone, find the appropriate time zone entry in the **Time Zone** drop-down list, and click 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 click 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.

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 5.24*. Replace 192.168.100.1 with the IP address of your NTP server, and click the **Submit** button.

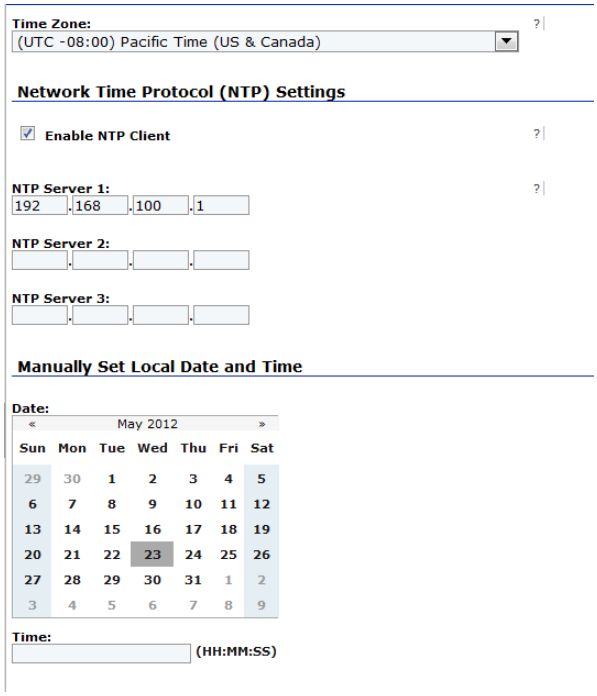


Figure 5.24 Date/Time Settings

Alarm Contact

The alarm contact is used as a means of alerting system personnel to system and security-related events that have occurred on the device. The alarm contact pulses for 1 second if any of the selected Alarm Contact Output Trigger categories are selected and an event that falls within the category occurs. Each category is listed in *Table 5.17* with an explanation of the event types that fall within each category.

Table 5.17 Alarm Contact Output Trigger Categories

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

Usage Policy

The device presents a usage policy to all users accessing the logon page. This policy notifies users of what constitutes 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 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. 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, with the exception of 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 on to the device and browse to the File Management page.

Step 2. You should be on the Export Settings page shown in *Figure 5.25*.

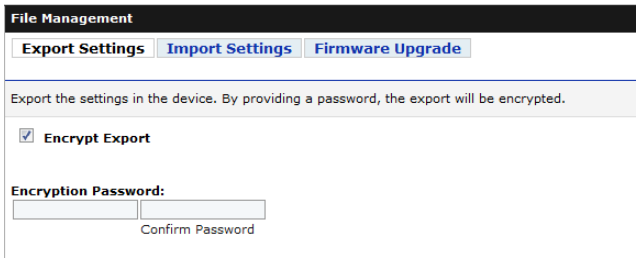


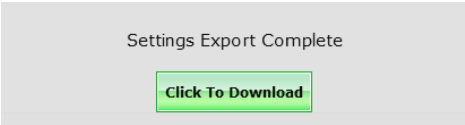
Figure 5.25 Export Settings Page

Step 3. Skip this step if you would like to export settings in an unencrypted format for offline viewing or editing.

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.

Step 4. Click the **Export** button.

Step 5. 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 6. Click the **Click to Download** button. The device will download the settings to your local computer.

Import Settings

Figure 5.26 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 on to the device and browse to the File Management page.

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

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

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

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. Click 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 will turn the device off and back on. All communication through the device will be lost while the device reboots.

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 on page 6.1*

➤ *LED Indicators on page 6.2*

➤ *Device Dashboard on page 6.3*

➤ *Troubleshooting on page 6.5*

➤ *Factory Assistance on page 6.7*

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 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 (Sheet 1 of 2)

Indicator	Green Condition	Red Condition
ENABLED	Normal operation	System is halted, system is booting, or an error condition has occurred.
ALARM	N/A	When the alarm contact operates or watchdog timer expires.

Table 6.1 System Status Indicators (Sheet 2 of 2)

Indicator	Green Condition	Red Condition
PWR A	Power supply installed and working properly	Power supply is installed and failed.
PWR B	Power supply installed and working properly	Power supply is installed and failed.

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 lit when the port is operating at full speed. When the port is operating at a reduced speed the indicator is unlit. Ports 9–24 are 100 Mbps ports. The yellow **100 Mbps** speed indicator is lit when these ports are operating at 100 Mbps, and unlit 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	Unlit Condition	Lit 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. *Figure 6.2* shows the Dashboard page. The system status and statistics information on the Dashboard page is updated periodically.

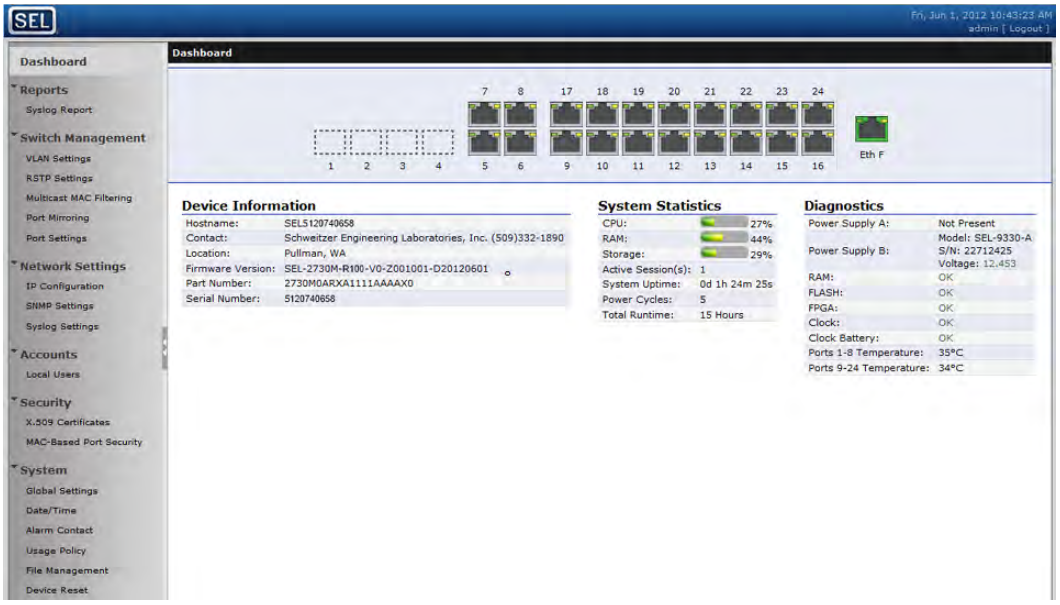


Figure 6.2 Device Dashboard

The Device 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 showing the current state of each physical Ethernet network interface on the device. You can mouse over any of the network interface port icons to see packet statistics for the port. Clicking one of these icons will add a status area to the Dashboard and adds 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*.

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 6.3*.

Table 6.3 Network Interface Icon Colors

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

Device Information

The Device Information section of the dashboard provides information about the SEL-2730M and its firmware, including part number, serial number, and the firmware identification string. This information can be useful when factory support or firmware upgrades are necessary.

System Statistics

The System Statistics area of the dashboard provides some basic statistics for device operations. This information can quickly help determine whether the device firmware is operating properly.

Table 6.4 explains the meaning of each of these statistics. The CPU, RAM, and storage statistics provide a visual indication of reserve processing or storage capacity in the unit. Any potential problems related to system resource utilization would be noticeable through these statistics on the dashboard.

Table 6.4 System Statistics

Statistic	Meaning
CPU	Percentage loading of the processor of the SEL-2730M.
RAM	Percentage usage of the on-board memory used by the SEL-2730M.
Storage	Percentage of the nonvolatile storage used by the SEL-2730M to store account information, logs, and other information that is maintained when power is off.
Active Session(s)	Number of users currently logged on to the management web interface.
System Uptime	How long the unit has been running since the last powerup or reboot.
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 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.

Troubleshooting

Inspection Procedure

Complete the following procedure before disturbing the device. After you finish the inspection, refer to *Table 6.5*.

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 6.5 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 logon 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 using DHCP as described in the Installation section.
	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 2 seconds. This will enable the interface and turn on the Captive Port feature to allow you to connect to the management interface 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 on	The user's account is missing.	Log on 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**, 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 www.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 two 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 www.selinc.com, or you can browse directly to the IP address for the unit at https://192.168.1.2.

Factory Assistance

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: +1.509.332.1890
Fax: +1.509.332.7990
Internet: www.selinc.com
Email: info@selinc.com

This page intentionally left blank

Appendix A
Firmware and Manual Versions

Firmware

This manual covers SEL-2730M devices containing firmware bearing the firmware version numbers listed in *Table A.1*. This table also lists a description of modifications and the instruction manual date code that corresponds to firmware versions. The most recent firmware version is listed first.

Table A.1 Firmware Revision History

Firmware Identification (FID) Number	Summary of Revisions	Manual Date Code
SEL-2730M-R101-V0-Z001001-D20121206	➤ Manual updates only (see *Table A.2*).	20130429
SEL-2730M-R101-V0-Z001001-D20121206	➤ Manual update only (see *Table A.2*).	20130416
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 release dates and a description of modifications. The most recent instruction manual revisions are listed at the top.

Table A.2 Instruction Manual Revision History

Revision Date	Summary of Revisions
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 revision R101.
20120611	➤ Initial version.

This page intentionally left blank

Appendix B
Firmware Upgrade Instructions

Introduction

SEL occasionally offers firmware upgrades to improve the performance of your device. The SEL-2730M stores firmware in nonvolatile memory. Opening the case or changing physical components is not necessary. These instructions give a step-by-step procedure to upgrade the device firmware by uploading a file from a personal computer to the device via the web interface. All firmware updates are logged.

Firmware releases are enhancements to improve functionality that change the way your device is configured or maintained, and can be installed in increasing or decreasing order. All existing settings will be transferred to newer firmware. Settings may not be transferred to older firmware. After a firmware update it is possible to revert to the previously installed firmware version.

To perform an upgrade you will need the appropriate firmware upgrade file and access to an administrative account on the device.

Firmware Files

SEL-2730M firmware upgrade files have a tar.gz file 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

Perform the following steps to upgrade the SEL-2730M firmware:

Step 1. Log on 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, click 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*).

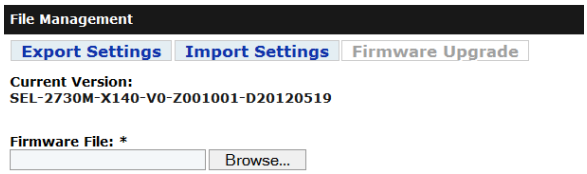


Figure B.1 File Management

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

Step 5. Click 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 shown progress of the upgrade operation as it proceeds. Firmware update takes about 10 minutes to complete.

Factory Assistance

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: +1.509.332.1890
Fax: +1.509.332.7990
Internet: www.selinc.com
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 logon 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 really 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 a large number of 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 are able to 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 on 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 on With SEL User-Based Accounts

Upon connection to this SEL product, a user will see a use banner and a logon prompt. The logon prompt includes fields for entering a username and the password associated with that username. To log on to this SEL product, 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 will have access to the device.

If the SEL-2730M determines a username or password to be invalid, then it rejects the access attempt and provides an alert to the user. This alert will inform the user that the logon credentials were incorrect. After three failed logon attempts within a one-minute period, this SEL product will disallow access attempts with the locked username for 30 seconds. Additionally, this device will pulse the alarm contact for one second to provide an alert to the control center that a failed logon attempt has occurred. These security features are designed to prevent and slow down password guessing attacks. Logon failure can happen for three reasons: the username was invalid, the password was incorrect, or the user's account is disabled. Please 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, please 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 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
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 angel brackets as <0> and <165> respectively.

The severity code (*Table D.1*) is a number indicative of how critical the message is.

Table D.1 Syslog Message Severities

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

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

Table D.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
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 utilize 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 utilize both Facilities 9 and 15 for clock (cron/at) messages.
Source: http://www.faqs.org/rfcs/rfc3164.html

2. **HEADER:** The header of a Syslog packet contains the timestamp and the source of the message. The IP address or the hostname defines the source of the message originator. Timestamps are based on the time of the originating host, so it is critical to have time synchronized across devices for the entire network in order 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 logon 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 D.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.

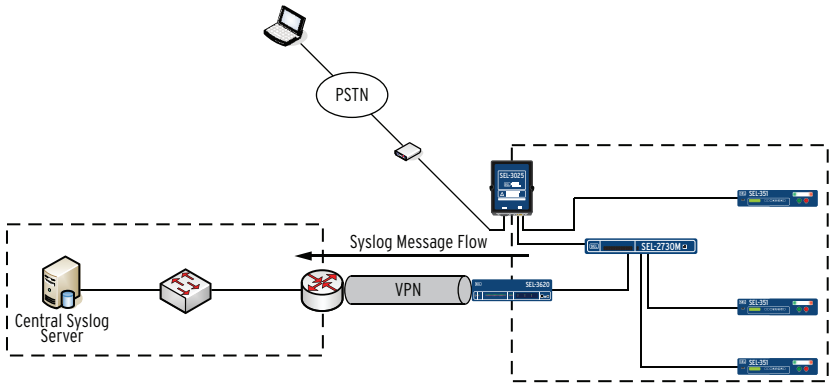


Figure D.1 Central Syslog Server

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 timestamps all events in the Syslog format consistent with the Syslog description from RFC 3164. *Table D.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 {0}. This notation indicates that this is a variable that will be replaced with the value being logged. For example, the {0} in Syslog message, `User account {0} locked out due to consecutive failed login attempts`, would be replaced with the actual username that was locked out.

Table D.3 Event Logs (Sheet 1 of 4)

Message	Tag Name	Severity	Facility
Commissioning			
Device commissioned by {0} at {user_ip}	Commissioning	Notice	SECURITY
User Configuration			
User {0}: created by {1} at {user_ip}	UserConfig	Warning	SECURITY
User {0}: deleted by {username} at {user_ip}	UserConfig	Warning	SECURITY
User {0}: enabled by {username} at {user_ip}	UserConfig	Notice	SECURITY
User {0}: disabled by {username} at {user_ip}	UserConfig	Notice	SECURITY
User {0}: password set by {username} at {user_ip}	UserConfig	Warning	SECURITY
User {0}: attributes changed by {username} at {user_ip}	UserConfig	Notice	SECURITY
Login			
Login to {interface}: successful by {username} at {user_ip}	Login	Notice	SECURITY
Login to {interface}: failed from {user_ip}	Login	Notice	SECURITY
Logout {interface}: {username} at {user_ip}	Login	Notice	SECURITY
User account {0} locked out due to consecutive failed login attempts	Login	Warning	SECURITY
User account {0} timeout	Login	Warning	SECURITY
Miscellaneous Configuration			
Usage Policy: changed by {username} at {user_ip}	Config	Notice	SECURITY
System Contact Information: changed by {username} at {user_ip}	Config	Notice	USER
Ports			
Port Settings: changed by {username} at {user_ip}	Config	Notice	SYSTEM
Port {0} changed link state to up	Link Up/Down	Notice	SYSTEM
Port {0} changed link state to down	Link Up/Down	Notice	SYSTEM
Firmware			
Firmware update from {0} to {1} 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 {user_ip}	Firmware	Warning	USER
The firmware update from {0} to new version failed with an error of {1}. Please contact Schweitzer Engineering Laboratories, Inc. for assistance.	Firmware	Critical	SYSTEM
Firmware: update to new version initiated by {username} at {user_ip}	Firmware	Notice	USER

Table D.3 Event Logs (Sheet 2 of 4)

Message	Tag Name	Severity	Facility
VLAN Configuration			
VLAN {0}: updated by {username} at {user_ip}	VLANConfig	Notice	USER
VLAN-aware mode disabled by {username} at {user_ip}	VLANConfig	Notice	USER
VLAN-aware mode enabled by {username} at {user_ip}	VLANConfig	Notice	USER
VLAN {0}: created by {username} at {user_ip}	VLANConfig	Notice	USER
VLAN {0}: deleted by {username} at {user_ip}	VLANConfig	Notice	USER
Multicast MAC Filtering			
Static Multicast MAC Group {0}: updated by {username} at {user_ip}	StaticMulticastMAC	Notice	USER
Static Multicast MAC Group {0}: deleted by {username} at {user_ip}	StaticMulticastMAC	Notice	USER
Static Multicast MAC Group {0}: created by {username} at {user_ip}	StaticMulticastMAC	Notice	USER
Port Mirroring			
Port Mirroring Settings: changed by {username} at {user_ip}	PortMirroringConfig	Notice	USER
Port Mirroring disabled on {0} by {username} at {user_ip}	PortMirroring	Notice	USER
Port Mirroring enabled on {0} by {username} at {user_ip}	PortMirroring	Notice	USER
Spanning Tree			
Spanning Tree: {hostname} has become the root bridge	SpanningTree	Notice	SYSTEM
Spanning Tree: Configuration changed by {username} at {user_ip}	SpanningTree	Notice	USER
Spanning Tree: Port {0} transitioned from {1} to {2}	SpanningTree	Informational	SYSTEM
Spanning Tree: Port {0} transitioned from {1} to {2}	SpanningTree	Notice	SYSTEM
Class of Service Configuration			
Class of Service queuing changed from {0} to {1} by {username} at {user_ip}	Config	Notice	USER
MAC-Based Port Security			
MAC-Based Port Security: configuration changed on port {0} by {username} at {user_ip}	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 {0} on port {1}	PortSecurity	Critical	SECURITY
Address table overflow resulting from hash collision when attempting to insert {0} on port {1}	PortSecurity	Error	SYSTEM
Alarm Contact			
Alarm Contact: configuration changed by {username} at {user_ip}	Alarm Contact	Notice	USER
X.509 Certificate			
X.509 certificate generation started by {username} at {user_ip}	X509Config	Notice	SECURITY
X.509 certificate {0} has expired; communications requiring X.509 based authentication may have stopped	X509Config	Alert	SYSTEM
X.509 certificate {0} Alias: certificate changed to {1} by {username} at {user_ip}	X509Config	Notice	USER
X.509 certificate {0} will expire in {1} days; communications requiring X.509 based authentication may be affected when it expires	X509Config	Critical	SYSTEM
X.509 certificate {0} will expire in {1} days; communications requiring X.509 based authentication may be affected when it expires	X509Config	Warning	SYSTEM

Table D.3 Event Logs (Sheet 3 of 4)

Message	Tag Name	Severity	Facility
X.509 certificate {0}: certificate generation completed successfully	X509Config	Notice	SECURITY
X.509 certificate {0} will expire in {1} days; communications requiring X.509 based authentication may be affected when it expires	X509Config	Notice	SYSTEM
X.509 certificate {0}: certificate import completed successfully	X509Config	Notice	SECURITY
X.509 certificate import failed	X509Config	Warning	SECURITY
X.509 certificate import started by {username} at {user_ip}	X509Config	Notice	SECURITY
X.509 certificate generation failed	X509Config	Warning	SECURITY
X.509 certificate {0}: certificate exported by {username} at {user_ip}	X509Config	Notice	USER
Networking Configuration			
Global Network Settings: changed by {username} at {user_ip}	NetworkConfig	Notice	USER
Network Interface {0}: changed by {username} at {user_ip}	NetworkConfig	Notice	USER
Captive Port			
Captive Port: disabled by {username} at {user_ip}	CaptivePortConfig	Notice	USER
Captive Port: enabled by {username} at {user_ip}	CaptivePortConfig	Notice	USER
SNMP			
SNMP Settings: changed by {username} at {user_ip}	SNMPConfig	Informational	USER
Syslog			
Syslog Settings: changed by {username} at {user_ip}	SyslogConfig	Notice	USER
Syslog Destination {0}: created by {username} at {user_ip}	SyslogConfig	Notice	USER
Syslog Destination {0}: deleted by {username} at {user_ip}	SyslogConfig	Warning	USER
Syslog Destination {0} Settings: modified by {username} at {user_ip}	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 {user_ip}	Syslog	Notice	USER
The {0} event queue overflowed	Syslog	Critical	SYSTEM
The {0} event queue left the overflow condition. Approximately {1} events were lost.	Syslog	Notice	SYSTEM
Date/Time			
Time Zone: changed from {0} to {1} by {username} at {user_ip}	DateTimeConfig	Notice	USER
System Time: changed from {0} to {1} by {username} at {user_ip}	DateTimeConfig	Notice	USER
Time Source: set to {0} by {username} at {user_ip}	DateTimeConfig	Notice	USER
NTP: server mode enabled by {username} at {user_ip}	DateTimeConfig	Notice	USER
NTP Server {0}: created by {username} at {user_ip}	DateTimeConfig	Notice	USER
NTP Server {0}: deleted by {username} at {user_ip}	DateTimeConfig	Notice	USER
NTP: server mode disabled by {username} at {user_ip}	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 {user_ip}	DateTime	Notice	USER

Table D.3 Event Logs (Sheet 4 of 4)

Message	Tag Name	Severity	Facility
Configuration File Import and Export			
Configuration file import started by {username} at {user_ip}	ImportExport	Notice	USER
Configuration file import successful	ImportExport	Notice	USER
Configuration file import failed	ImportExport	Warning	USER
Configuration file export started by {username} at {user_ip}	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 {user_ip}	Power	Error	USER
Device factory reset initiated by {username} at {user_ip}	Commissioning	Notice	SECURITY
Device factory reset initiated through pinhole button	PushbuttonReset	Notice	USER
Front management port reset initiated through pinhole button	PushbuttonReset	Alert	USER

This page intentionally left blank

Appendix E
Networking Fundamentals

Introduction

A telecommunications network can be as simple as two devices linked together for the purpose of 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 Standards Organization (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 provides an introduction to 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 E.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 an Ethernet, serial, or radio physical medium.

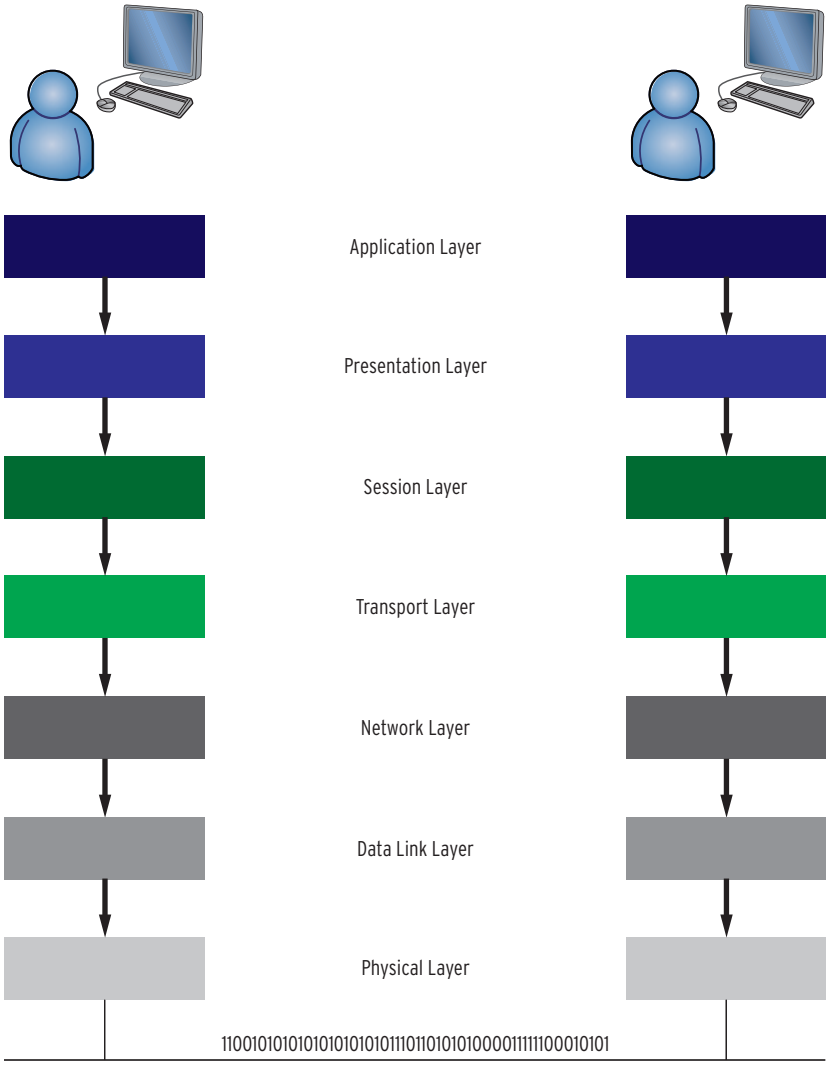


Figure E.1 OSI Model

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 Ethernet 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 reliable transit of data across physical mediums by controlling frame synchronization, flow control, error detection, and providing physical addressing. Directly connected devices (*Figure E.2*) communicate at this layer without the need for a Layer 3 device, such as a router.

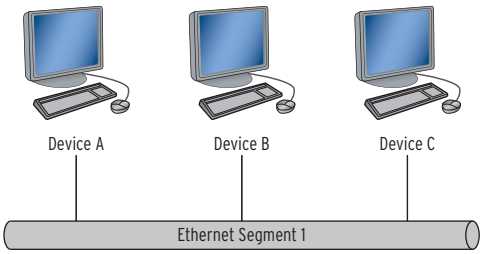


Figure E.2 Ethernet Segment

The Data Link Layer is subdivided into the Logical Link Control (LLC) and the Media Access Control (MAC) sub-layers. The LLC sub-layer manages communication among devices and handles the frame synchronization, flow control, and error checking introduced previously. The MAC sub-layer manages physical addressing at the Data Link layer. 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. The OSI model represents MAC addresses, also known as hardware addresses, in the form of *01-23-45-67-89-ab*.

At this layer, devices organize data they receive into frames, called headers, that encapsulate the data with descriptive information. *Figure E.3* depicts an example of an Ethernet frame.

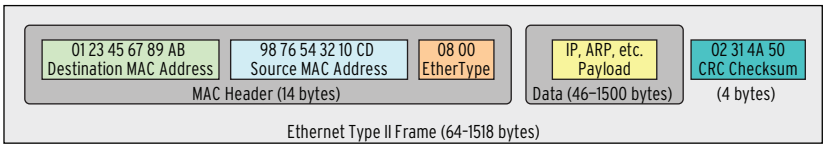


Figure E.3 Ethernet Frame

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

- MAC 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 are received exactly as sent.

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, error handling, and congestion control 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 IP networks.

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

Table E.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 E.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 E.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)*. The same is true for communication among Device D, Device E, and Device F.

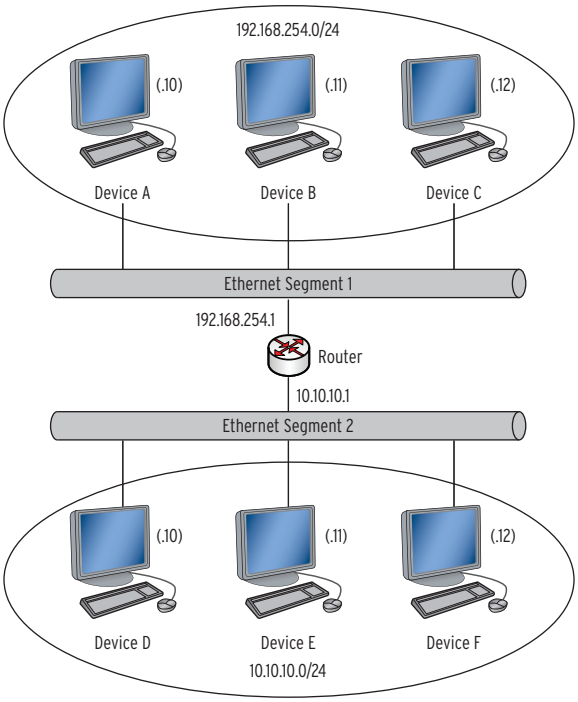


Figure E.4 Layer 3 IP Network

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 end-to-end control and ensures successful data transfer. The main Transport Layer functions are flow control and error recovery.

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 in the event that 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 connection between two devices through a three-way handshake (*Figure E.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.

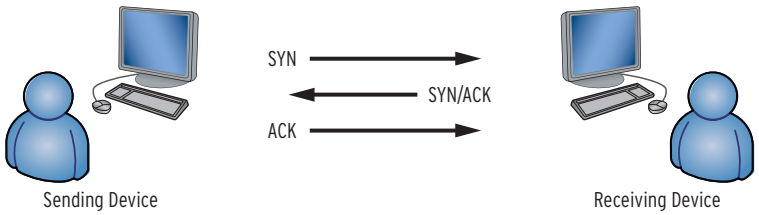


Figure E.5 TCP Three-Way Handshake

At 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 receiving device's application. 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 F

Virtual Local Area Networks

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 F.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. In order 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 utilizing VLANs provides the flexibility to assign a device to a broadcast domain regardless of the physical location.

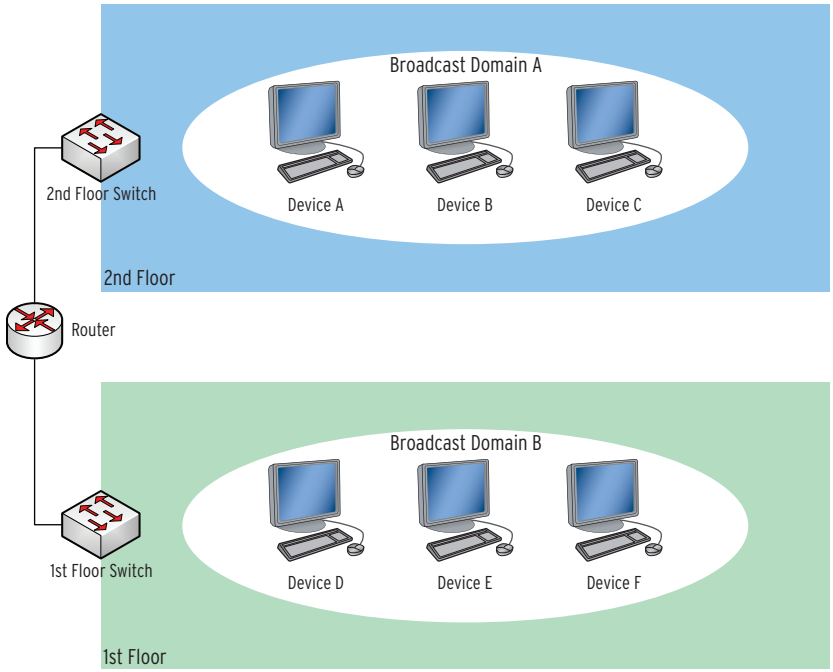


Figure F.1 Network Illustration Not Utilizing VLANs

Figure F.2 shows the same physical network utilizing 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 F.2*, VLAN membership is independent of physical location.

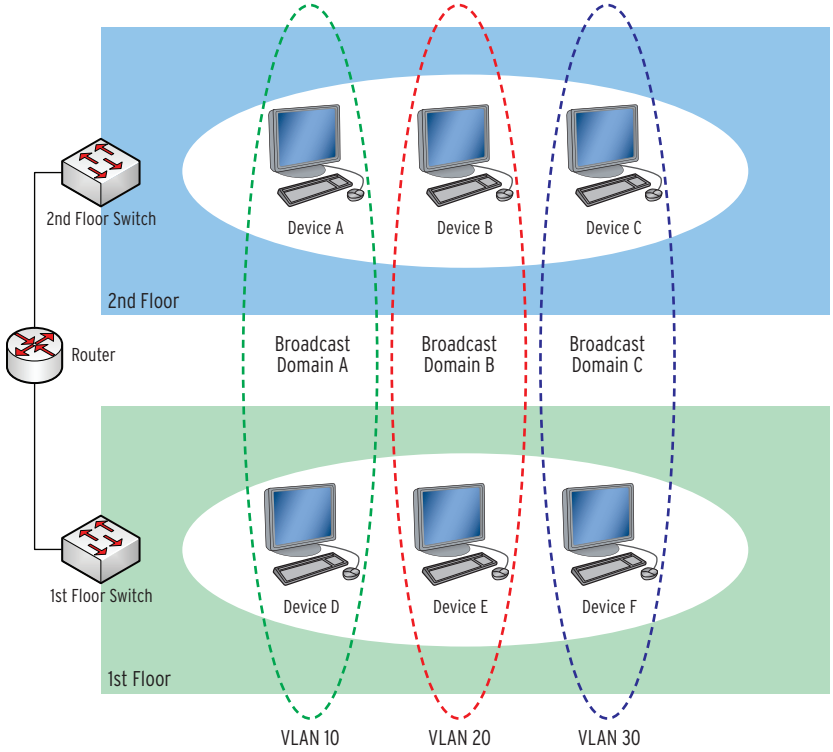


Figure F.2 Network Illustration Utilizing VLANs

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 utilize a switch independent of the switch utilized 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 local area network (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 G

Classless Inter-Domain Routing (CIDR)

CIDR was developed as a method to help alleviate the exhaustion of IPv4 addresses available on the Internet and also 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.

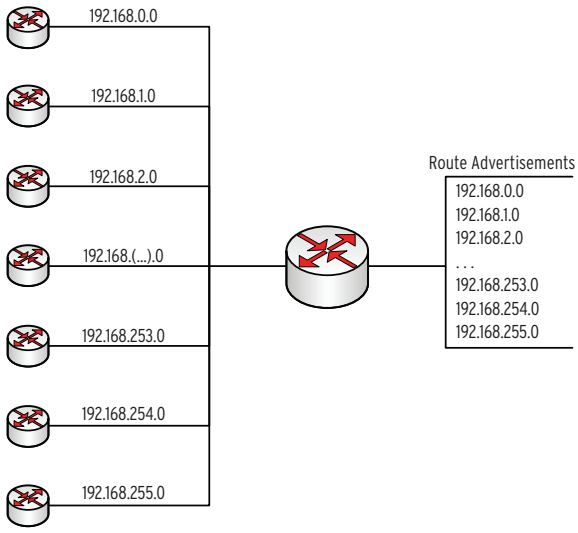


Figure G.1 Classful Route Advertisements

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.

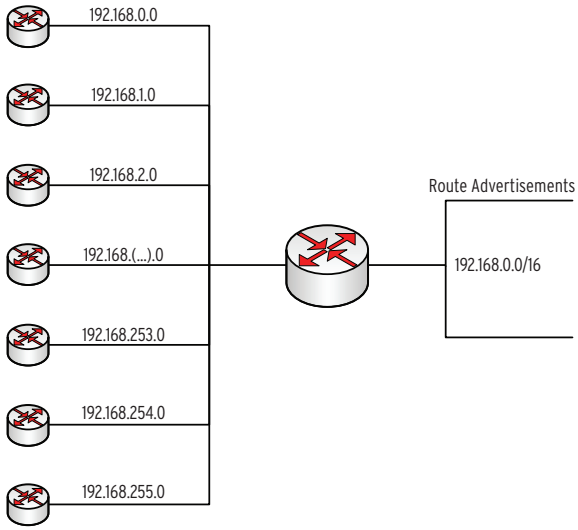


Figure G.2 CIDR Route Advertisements

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 G.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
/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 H
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.

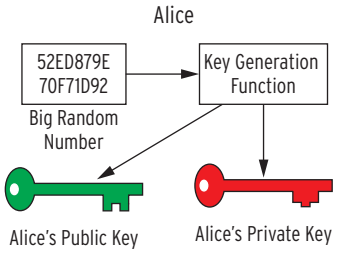


Figure H.1 Asymmetric Keys

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.

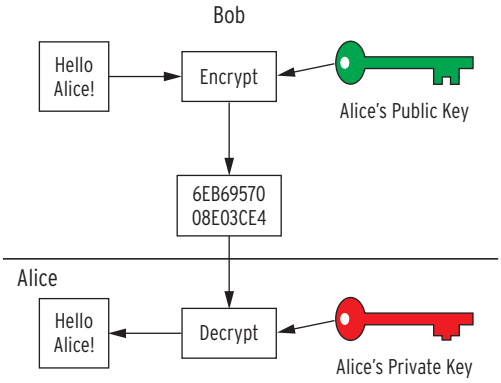


Figure H.2 Confidentiality With Asymmetric Keys

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.

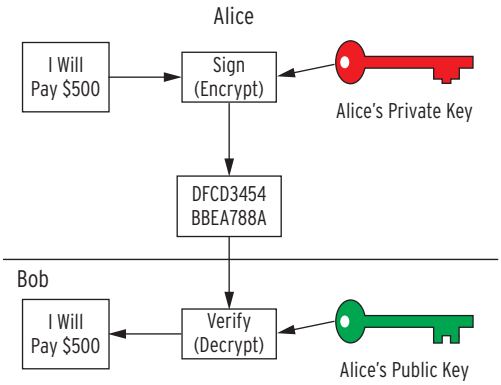


Figure H.3 Authentication With Asymmetric Keys

X.509 Certificates

Digital certificates, also known as public key certificates, provide a formal method for tracking pairs of asymmetric keys and their owners. You can use these electronic documents, through the use of digital signatures, to bind public keys to their owners. You would use digital certificates primarily in three different ways involving public key infrastructure, web of trust, and simple public key infrastructure. The certificate issuer distinguishes these three methods.

Digital Signatures

A digital signature is a more formal method of authentication 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, you would first compute a hash of the certificate and then encrypt that hash with the issuer's private key. You would then attach this signature to the certificate. To verify the authenticity of the certificate, the system first separates certificate and signature. The system computes a hash of the certificate and then uses the issuer's public key to decrypt the signature. We compare these two results and, if they match, we know the certificate is authentic.

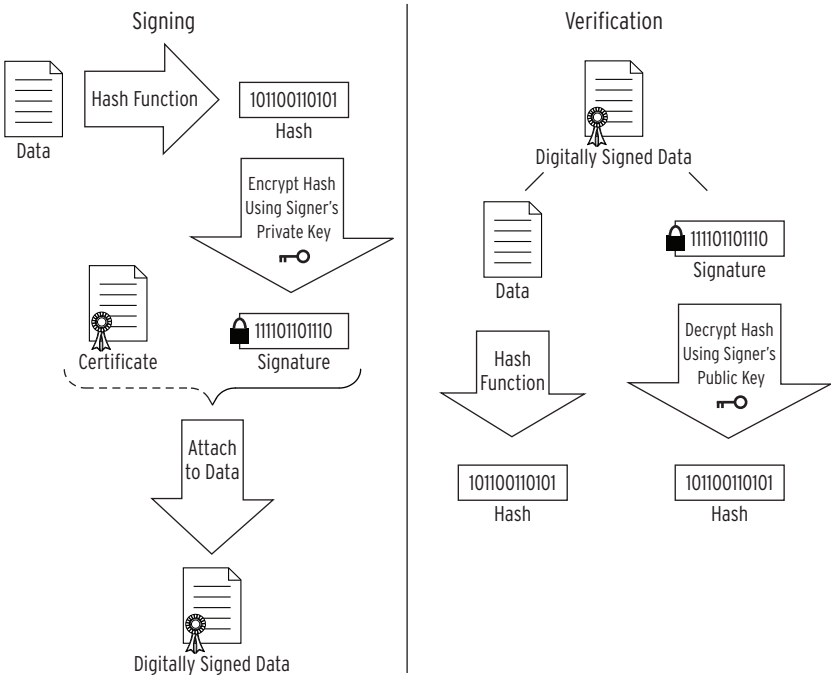


Figure H.4 Digital Signatures

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 contains the signature of a more trusted certificate. At the top of the PKI hierarchy is the most trusted certificate, the root certificate. This certificate is self-signed, highly protected, and should only be used to sign CA certificates. If the 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 will generate a key pair, and send the public key and credentials to a CA. The CA will verify the authenticity of the credentials and issue the certificate containing those credentials, the public key, and the CA's digital signature. A CA is responsible for saying "yes" these people are whom they claim to be. CAs are authenticated by other CAs or by the root certificate.

Be aware that an attacker can subvert this process. This happens when an attacker requests a certificate and provides valid credentials for the victim. The CA, thinking everything is good, issues a certificate in the victim's name to the attacker. Take care in communicating with the CA to ensure that this will not happen.

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 H.5* below illustrates a simple example of a web of trust. If Alice trusts Bob, and Bob trusts Charlie, then Alice implicitly trusts Charlie.

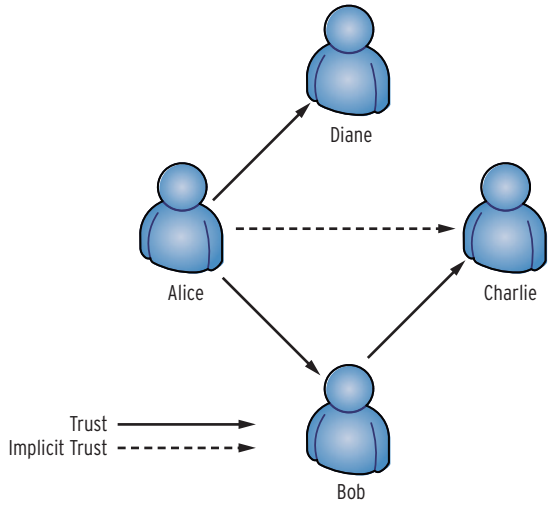


Figure H.5 Web of Trust

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 pre-shared 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 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
```

SCHWEITZER ENGINEERING LABORATORIES, INC.
2350 NE Hopkins Court • Pullman, WA 99163-5603 USA
Tel: +1.509.332.1890 • Fax: +1.509.332.7990
www.selinc.com • info@selinc.com