

## Technical Description



# IP-50EX IP-50EX-P

February 2025 | Rev B

CeraOS: 12.9.5

© Copyright 2025 by Ceragon Networks Ltd. All rights reserved.

## Notice

This document contains information that is proprietary to Ceragon Networks Ltd. No part of this publication may be reproduced, modified, or distributed without prior written authorization of Ceragon Networks Ltd. This document is provided as is, without warranty of any kind.

## Trademarks

Ceragon® is a trademark of Ceragon Networks Ltd., registered in various countries.

Other names mentioned in this publication may be owned by their respective holders.

## Statement of Conditions

The information contained in this document is subject to change without notice. Ceragon Networks Ltd. shall not be liable for errors contained herein or for damage in connection with the furnishing, performance, or use of this document or equipment supplied with it.

Features and functionalities described in this document may change depending on future hardware and software releases without further notice.

## Open Source Statement

The Product may use open source software, among them O/S software released under the GPL or GPL alike license ("Open Source License"). Inasmuch that such software is being used, it is released under the Open Source License, accordingly. The complete list of the software being used in this product including their respective license and the aforementioned public available changes is accessible at:

Network element site: <ftp://ne-open-source.license-system.com>

NMS site: <ftp://nms-open-source.license-system.com/>

## Information to User

Any changes or modifications of equipment not expressly approved by the manufacturer could void the user's authority to operate the equipment and the warranty for such equipment.

## Intended Use/Limitation

Fixed point-to-point radio links for private networks.

## Authorized to Use

Only entities with individual authorization from the National Regulator to operate the mentioned radio equipment.

The equipment can be used in the following EU countries:

Austria (AT) - Belgium (BE) - Bulgaria (BG) - Switzerland/Liechtenstein (CH) - Cyprus (CY) - Czech Republic (CZ) - Germany (DE) - Denmark (DK) - Estonia (EE) - Finland (FI) - France (FR) - Greece (GR) - Hungary (HU) - Ireland (IE) - Iceland (IS) - Italy (IT) - Lithuania (LT) - Luxembourg (LU) - Latvia (LV) - Malta (MT) - Netherlands (NL) - Norway (NO) - Portugal (PT) - Romania (RO) - Sweden (SE) - Slovenia (SI) - Slovak Republic (SK) - United Kingdom (UK) - Spain (SP) - Poland (PL)

## Table of Contents

<b>1. Introduction.....</b>	<b>11</b>
1.1 Product Overview .....	12
1.2 System Configurations .....	14
1.2.1 1+0 – Direct Mount .....	14
1.2.2 1+0 – Low Visual Impact .....	15
1.2.3 2+0 XPIC – Direct Mount .....	16
1.2.4 2+0 XPIC – Low Visual Impact .....	17
<b>2. IP-50EX Hardware Description .....</b>	<b>18</b>
2.1 IP-50EX Unit Description .....	19
2.2 IP-50EX Interfaces .....	20
2.3 Hardware Architecture .....	21
2.4 PoE Injector .....	22
2.4.1 PoE Injector Interfaces .....	23
2.5 Voltage Alarm Thresholds and PMs .....	23
<b>3. Activation Keys .....</b>	<b>24</b>
3.1 Working with Activation Keys .....	25
3.2 Demo Mode .....	25
3.3 Activation Key Reclaim .....	25
3.4 Activation Key-Enabled Features .....	26
<b>4. Feature Description.....</b>	<b>31</b>
4.1 Innovative Techniques to Boost Capacity and Reduce Latency .....	32
4.1.1 Capacity Summary .....	33
4.1.2 Adaptive Coding Modulation and Bandwidth (ACM and ACMB) .....	34
4.1.3 Multiband.....	39
4.1.3.1 Multiband Antenna .....	40
4.1.4 Cross Polarization Interference Canceller (XPIC) .....	41
4.1.5 1+1 HSB and Unit Redundancy .....	46
4.1.6 ATPC.....	47
4.1.7 Radio Signal Quality PMs .....	48
4.1.8 Radio Utilization PMs .....	49
4.2 Ethernet Features .....	50
4.2.1 IP-50EX's Ethernet Capabilities .....	51
4.2.2 Ethernet Service Model .....	52
4.2.3 Ethernet Interfaces .....	68
4.2.4 Quality of Service (QoS) .....	77
4.2.5 Global Switch Configuration .....	94
4.2.6 Automatic State Propagation and Link Loss Forwarding .....	95
4.2.7 Network Resiliency .....	97
4.2.8 OAM .....	103
4.3 E-Stabilizer .....	107

4.4	Frequency Scanner .....	108
4.5	Synchronization .....	109
4.5.1	IP-50EX Synchronization Solution .....	109
4.5.2	Available Synchronization Interfaces .....	110
4.5.3	Synchronous Ethernet (SyncE) .....	111
4.5.4	IEEE-1588v2 PTP Optimized Transport .....	111
4.5.5	SSM Support and Loop Prevention .....	117
4.6	AES-GCM-256 Payload Encryption .....	120
4.6.1	AES Benefits .....	121
4.6.1.1	IP-50EX AES Implementation .....	121
<b>5.</b>	<b>IP-50EX Management.....</b>	<b>122</b>
5.1	Management Overview .....	123
5.2	Automatic Network Topology Discovery with LLDP Protocol .....	124
5.3	Management Communication Channels and Protocols .....	125
5.4	Web-Based Element Management System (Web EMS) .....	127
5.5	SDN Support.....	129
5.6	Command Line Interface (CLI).....	131
5.7	Configuration Management.....	131
5.8	Software Management .....	132
5.9	Using Pre-Defined Configuration Files .....	133
5.10	IPv6 Support.....	134
5.11	In-Band Management .....	134
5.12	Local Management .....	134
5.13	Alarms .....	135
5.13.1	Configurable BER Threshold for Alarms and Traps .....	135
5.13.2	RSL Threshold Alarm .....	135
5.13.3	Editing and Disabling Alarms and Events .....	135
5.13.4	Timeout for Trap Generation .....	135
5.14	NTP Support.....	136
5.15	UTC Support.....	136
5.16	Syslog Support .....	137
5.17	System Security Features .....	138
5.17.1	Ceragon's Layered Security Concept.....	138
5.17.2	Defenses in Management Communication Channels .....	139
5.17.3	Defenses in User and System Authentication Procedures.....	140
5.17.4	Secure Communication Channels .....	144
5.17.5	Security Log.....	147
5.17.6	Access Control Lists.....	148
<b>6.</b>	<b>Standards and Certifications.....</b>	<b>149</b>
6.1	Supported Ethernet Standards .....	150

6.2	MEF Specifications for Ethernet Services.....	151
<b>7.</b>	<b>Specifications.....</b>	<b>152</b>
7.1	PoE Port Specifications (IP-50EX-P only).....	152
7.2	General Radio Specifications .....	153
7.3	Radio Scripts .....	154
7.4	Radio Capacity Specifications .....	155
7.5	Transmit Power Specifications.....	162
7.6	Receiver Threshold Specifications (dBm@ 10E <sup>-6</sup> ) .....	163
7.7	Mediation Device Losses.....	164
7.8	Ethernet Latency Specifications.....	165
7.9	Interface Specifications.....	173
7.9.1	Ethernet Interface Specifications.....	173
7.10	Carrier Ethernet Functionality .....	175
7.11	Synchronization Protocols .....	176
7.12	Network Management, Diagnostics, Status, and Alarms.....	176
7.13	Mechanical Specifications.....	177
7.14	Standards Compliance .....	178
7.15	Environmental Specifications.....	179
7.16	Antenna Interface Specifications .....	180
7.17	Integrated Antenna.....	181
7.18	Power Input Specifications .....	181
7.19	PoE Port Specifications (IP-50EX-P only).....	181
7.20	Power Consumption Specifications .....	182
7.21	Cable Specifications .....	183
7.21.1	Outdoor Ethernet Cable Specifications.....	183
7.21.2	Outdoor DC Cable Specifications .....	184
<b>8.</b>	<b>Appendix A – Marketing Models.....</b>	<b>185</b>
<b>9.</b>	<b>Appendix B - Synonyms and Acronyms .....</b>	<b>186</b>

## List of Figures

Figure 1: IP-50EX 1+0 Direct Mount .....	14
Figure 2: Integrated 43dBi Antenna .....	15
Figure 3: IP-50EX 2+0 XPIC Direct Mount .....	16
Figure 4: IP-50EX 2+0 DP Low Visual Impact .....	17
Figure 5: IP-50EX Direct Mount HW Ready – Rear View (Left) and Front View (Right) .....	19
Figure 6: Cable Gland Construction .....	19
Figure 7: IP-50EX Interfaces .....	20
Figure 8: IP-50EX Block Diagram .....	21
Figure 9: PoE Injector .....	22
Figure 10: PoE Injector Ports .....	23
Figure 11: Adaptive Coding and Modulation with Eleven Working Points .....	35
Figure 12: Dual Polarization .....	41
Figure 13: XPIC Implementation – Direct Mount .....	42
Figure 14: XPIC Implementation – Integrated Antenna .....	42
Figure 15: XPIC – Impact of Misalignments and Channel Degradation .....	43
Figure 16: 2+0 XPIC Configuration – Direct Mount .....	44
Figure 17: 2+0 XPIC Configuration – Integrated Antenna .....	44
Figure 18: IP-50EX Services Model .....	52
Figure 19: IP-50EX Services Core .....	53
Service Types Figure 20: IP-50EX Services Flow .....	54
Figure 21: Point-to-Point Service .....	55
Figure 22: Multipoint Service .....	56
Figure 23: Management Service .....	58
Figure 24: Management Service and its Service Points .....	60
Figure 25: SAPs and SNPs .....	61
Figure 26: Pipe Service Points .....	62
Figure 27: SAP, SNP and Pipe Service Points in a Microwave Network .....	62
Figure 28: Service Path Relationship on Point-to-Point Service Path .....	66
Figure 29: Physical and Logical Interfaces .....	68
Figure 30: Grouped Interfaces as a Single Logical Interface on Ingress Side .....	69
Figure 31: Grouped Interfaces as a Single Logical Interface on Egress Side .....	69
Figure 32: Relationship of Logical Interfaces to the Switching Fabric .....	72
Figure 33: QoS Block Diagram .....	77
Figure 34: Hierarchical Classification .....	79
Figure 35: Classification Method Priorities .....	80

Figure 36: Synchronized Packet Loss.....	86
Figure 37: Random Packet Loss with Increased Capacity Utilization Using WRED .....	86
Figure 38: WRED Profile Curve .....	87
Figure 39: Scheduling Mechanism .....	89
Figure 40: G.8032 Ring in Idle (Normal) State.....	98
Figure 41: G.8032 Ring in Protecting State .....	99
Figure 42: Load Balancing Example in G.8032 Ring.....	99
Figure 43: IP-50EX End-to-End Service Management .....	103
Figure 44: SOAM Maintenance Entities (Example) .....	104
Figure 45: IEEE-1588v2 PTP Optimized Transport – General Architecture .....	111
Figure 46: Calculating the Propagation Delay for PTP Packets .....	112
Figure 47: Transparent Clock – General Architecture .....	115
Figure 48: Transparent Clock Delay Compensation .....	116
Figure 49: Boundary Clock – General Architecture .....	117
Figure 50 AES-GCM-256 Encrypted Link .....	120
Figure 51: Integrated Management Tools.....	123
Figure 52: Security Solution Architecture Concept .....	138

## List of Tables

Table 1: IP-50EX Antenna Mounting Kit .....	15
Table 2: Activation Key Types.....	26
Table 3: Capacity Activation Keys.....	28
Table 4: Edge CET Node Activation Keys .....	29
Table 5: Edge CET Node Upgrade Activation Keys .....	30
Table 6: ACM Working Points (Profiles) .....	35
Table 7: Ethernet Services Learning and Forwarding.....	56
Table 8: Service Point Types per Service Type .....	63
Table 9: Service Point Types that can Co-Exist on the Same Interface .....	64
Table 10: Service Point Type-Attached Interface Type Combinations that can Co-Exist on the Same Interface .....	65
Table 11: MPLS EXP Default Mapping to CoS and Color .....	80
Table 12: DSCP Default Mapping to CoS and Color.....	80
Table 13: C-VLAN 802.1 UP and CFI Default Mapping to CoS and Color .....	81
Table 14: S-VLAN 802.1 UP and DEI Default Mapping to CoS and Color.....	82
Table 15: QoS Priority Profile Example .....	89
Table 16: Marking Table for 802.1Q and 802.1AD UP Bits.....	91
Table 17: Summary of IP-50EX QoS Mechanism .....	93
Table 18: Synchronization Interface Options .....	110
Table 19: Boundary Clock Input Options.....	117
Table 20: Boundary Clock Output Options.....	117
Table 21: Dedicated Management Ports.....	125
Table 22: Supported Ethernet Standards.....	150
Table 23: Supported MEF Specifications .....	151
Table 24: Frequency Tuning Range: .....	153
Table 25: Radio Scripts .....	154
Table 26: Radio Capacity – 250 MHz Channel Bandwidth (Script 5803) .....	155
Table 27: Radio Capacity – 250 MHz Channel Bandwidth (Script 5853) .....	156
Table 28: Radio Capacity – 500 MHz Channel Bandwidth (Script 5804) .....	157
Table 29: Radio Capacity – 500 MHz Channel Bandwidth (Script 5854) .....	158
Table 30: Radio Capacity – 1000 MHz Channel Bandwidth (Script 5806) .....	159
Table 31: Radio Capacity – 1000 MHz Channel Bandwidth (Script 5856) .....	160
Table 32: Radio Capacity – 2000 MHz Channel Bandwidth (Script 5810) .....	160
Table 33: Radio Capacity – 2000 MHz Channel Bandwidth (Script 5860) .....	161
Table 34: Transmit Power – Standard IP-50EX Devices.....	162



Table 35: Transmit Power – IP-50EX-P Devices.....	162
Table 36: Receiver Threshold Specifications .....	163
Table 37: Ethernet Latency – 250 MHz Channel Bandwidth (Script 5803) .....	165
Table 38: Ethernet Latency – 250 MHz Channel Bandwidth (Script 5853) .....	166
Table 39: Ethernet Latency – 500 MHz Channel Bandwidth (Script 5804) .....	167
Table 40: Ethernet Latency – 500 MHz Channel Bandwidth (Script 5854) .....	168
Table 41: Ethernet Latency – 1000 MHz Channel Bandwidth (Script 5806) .....	169
Table 42: Ethernet Latency – 1000 MHz Channel Bandwidth (Script 5856) .....	170
Table 43: Ethernet Latency – 2000 MHz Channel Bandwidth (Script 5810) .....	171
Table 44: Ethernet Latency – 2000 MHz Channel Bandwidth (Script 5860) .....	172
Table 45: Approved SFP Modules .....	173
Table 46: Approved 10 GbE SFP+ Modules .....	173
Table 47: Approved SFP28 Modules .....	173
Table 48: QSFP Accessories .....	174
Table 49: Power Consumption – Standard IP-50EX Devices .....	182
Table 50: Power Consumption –IP-50EX-P Devices .....	182
Table 51: IP-50EX Marketing Models (Available) .....	185
Table 52: IP-50EX Marketing Models (Planned for Future Release) .....	185
Table 53: IP-50EX-P Marketing Models (Available) .....	185
Table 54: IP-50EX-P Marketing Models (Planned for Future Release) .....	185

## About This Guide

This document describes the main features, components, and specifications of the IP-50EX and IP-50EX-P.

## Target Audience

This manual is intended for use by Ceragon customers, potential customers, and business partners. The purpose of this manual is to provide basic information about the IP-50EX for use in system planning, and determining which IP-50EX configuration is best suited for a specific network.

## Related Documents

- Release Notes CeraOS 12.9.5, IP-50 Products
- User Guide for IP-50CX, IP-50EX, and IP-50EX-P, CeraOS 12.9.5
- MIB Reference for IP-50 Products, CeraOS 12.9.5
- Installation Guide for IP-50EX and IP-50EX-P

## 1. Introduction

IP-50EX is a compact, high-capacity, all-outdoor Ethernet backhaul system designed to operate in the E-Band frequency range. IP-50EX provides up to 10 Gbps capacity in 1+0 configurations. IP-50EX can operate over 250, 500, 1000, and 2000 MHz channels, with modulations of BPSK to 512 QAM and a rich feature set.

IP-50EX-P is a hardware variant of IP-50EX, with high TX power and support for PoE and AES-256 encryption. High TX power means higher signal range and quality, while PoE enables quicker installation and OPEX savings. These features, combined with the enhanced security offered by AES-256 encryption, make IP-50EX-P a robust and cost-effective solution for carrier-grade networks.

**Note:** In this document, IP-50EX also refers to IP-50EX-P, unless otherwise stated.

2+0 configurations are planned for future release.

### This chapter includes:

- Product Overview
- System Configurations

## 1.1 Product Overview

IP-50EX is a compact and versatile high capacity backhaul Ethernet system which operates in the E-band (71-76 GHz, 81-86 GHz). It's very light weight and small footprint make it versatile for many different applications. Thanks to its small footprint, low power consumption, and simple installation, IP-50EX can be installed in many different types of remote outdoor locations.

IP-50EX operates over 250, 500, 1000, and 2000 MHz channels to deliver up to 20 Gbps of Ethernet throughput in several system configurations.

Two IP-50EX units can be configured in 2+0 XPIC links, providing up to 20 Gbps capacity with load balancing to provide efficient traffic distribution between the two units.<sup>1</sup>

IP-50EX can also be used in Layer 1 Link Bonding configurations with IP-20N and IP-20A.

For mobile and other wireless carriers, IP-50EX supports a diverse set of features that are optimally suited for a variety of deployment scenarios, including:

- Macro site backhaul
- Macro site aggregation
- Building-to-building connectivity
- Private wireless networks
- Small cell backhaul

IP-50EX is equipped with a feature set which has become standard practice in deployment of carrier grade networks, including:

- Integrated Carrier Ethernet services switch, MEF CE 2.0 compliant
  - Rich packet processing feature set for support of engineered end-to-end Carrier Ethernet services with strict SLA.
  - High precision, flexible packet synchronization solution combining SyncE and 1588v2.
- ACMB – Adaptive Coding Modulation and Bandwidth: Hitless transmission between modulation steps (BPSK to 512 QAM<sup>2</sup>) and, at BPSK, hitless modification of the channel spacing when necessary by reducing the channel spacing to one half or one quarter, to increase link survivability.

---

<sup>1</sup> XPIC with IP-50EX-P is planned for future release.

<sup>2</sup> Supported maximum modulation may depend on the configured channel spacing. For details, see *Radio Capacity Specifications* on page 170.

- In-band and out-of-band management options.
- Network Management – Full suite of secured network management capabilities within IP-50EX and seamless connection to Ceragon's Network Management System (NMS) applications for secure remote management.
- Three high-capacity traffic interfaces (2 x SFP28 supporting up to 25 Gbps and 1 X QSFP using a QSFP to SFP+ adaptor supporting up to 10 Gbps).

The IP-50EX-P will have the following additional features:

- Higher Tx Power
- PoE-In support
- User data encryption (AES-GCM-256)

## 1.2 System Configurations

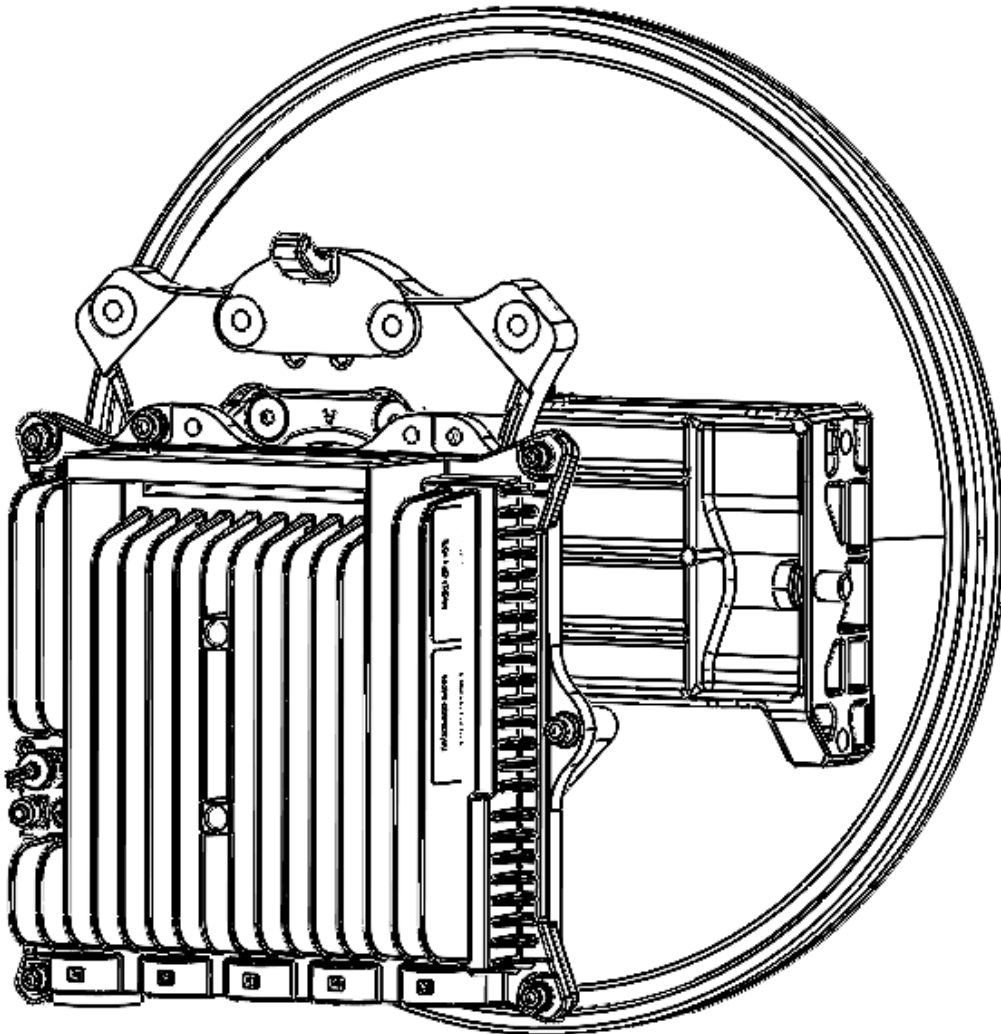
IP-50EX is designed to support the following site configurations:

- 1+0 – Direct Mount
- 1+0 – Low Visual Impact
- 2+0 XPIC (Direct Mount or Low Visual Impact)

**Note:** The Low Visual Impact configurations with integrated antenna are planned for future release.

### 1.2.1 1+0 – Direct Mount

The following figure illustrates a 1+0 direct mount configuration. In a direct mount installation, the IP-50EX is directly mounted on the antenna, without the use of flexible waveguides.



*Figure 1: IP-50EX 1+0 Direct Mount*

1.2.2 1+0 – Low Visual Impact

The following figure illustrates a 1+0 Low Visual Impact configuration. In this configuration, the IP-50EX is equipped with a 43dBi integrated antenna to minimize its installation form-fit and enable it to blend into an urban environment.

**Notes:** The Low Visual Impact variant is planned for future release.  
For this configuration, IP-50EX must be ordered together with the antenna mounting kit. See *Table 1*.

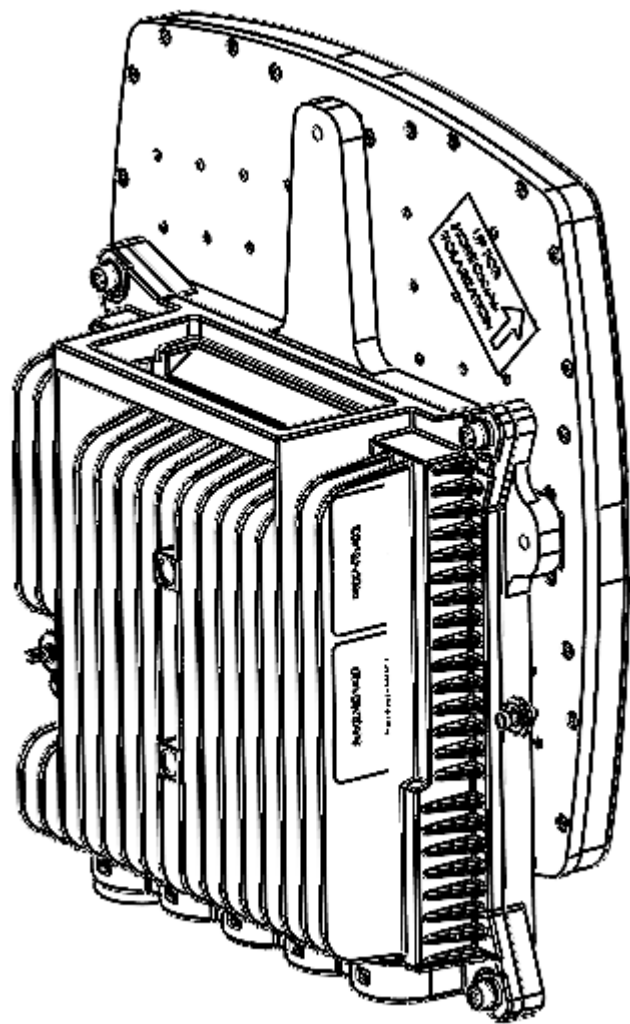


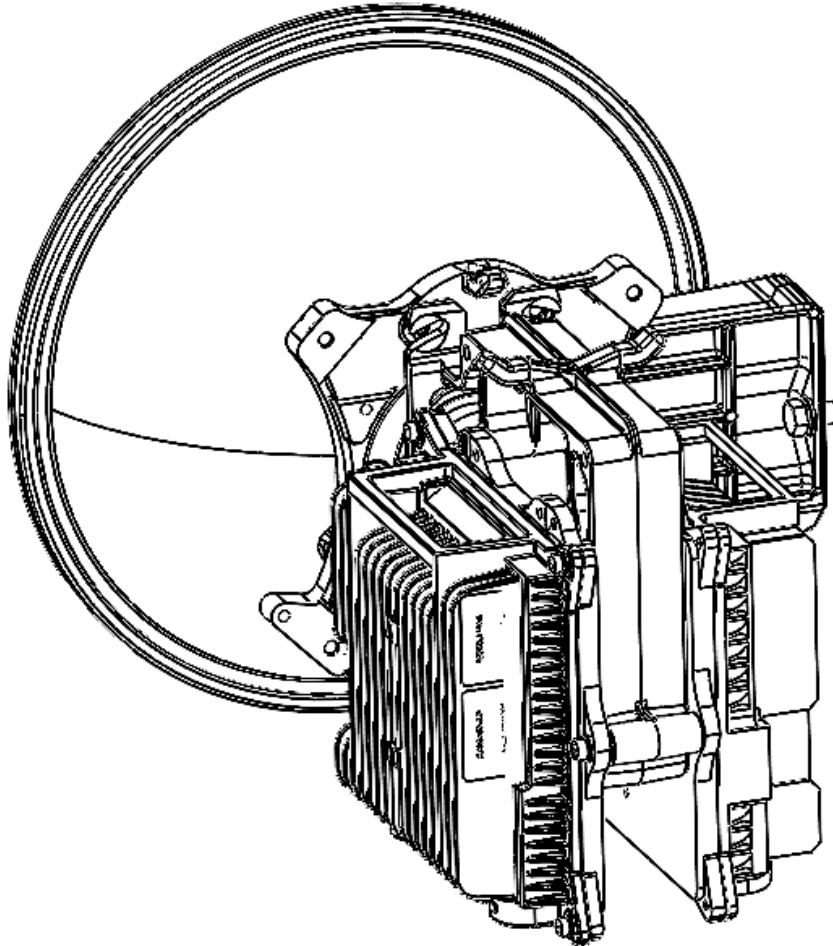
Figure 2: Integrated 43dBi Antenna

Table 1: IP-50EX Antenna Mounting Kit

Marketing Model	Description
Integrated_Ant_Mounting_Kit	Integrated Antenna Mounting Kit

### 1.2.3 2+0 XPIC – Direct Mount

The following figure illustrates a 2+0 direct mount XPIC configuration. This configuration requires an OMT mediation device.



*Figure 3: IP-50EX 2+0 XPIC Direct Mount*



#### 1.2.4 2+0 XPIC – Low Visual Impact

The following figure illustrates a 2+0 low visual impact XPIC configuration, with integrated antennas. No mediation device is required for this configuration.

**Notes:** The Low Visual Impact variant is planned for future release.  
For this configuration, IP-50EX must be ordered together with the antenna mounting kit. See *Table 1*.

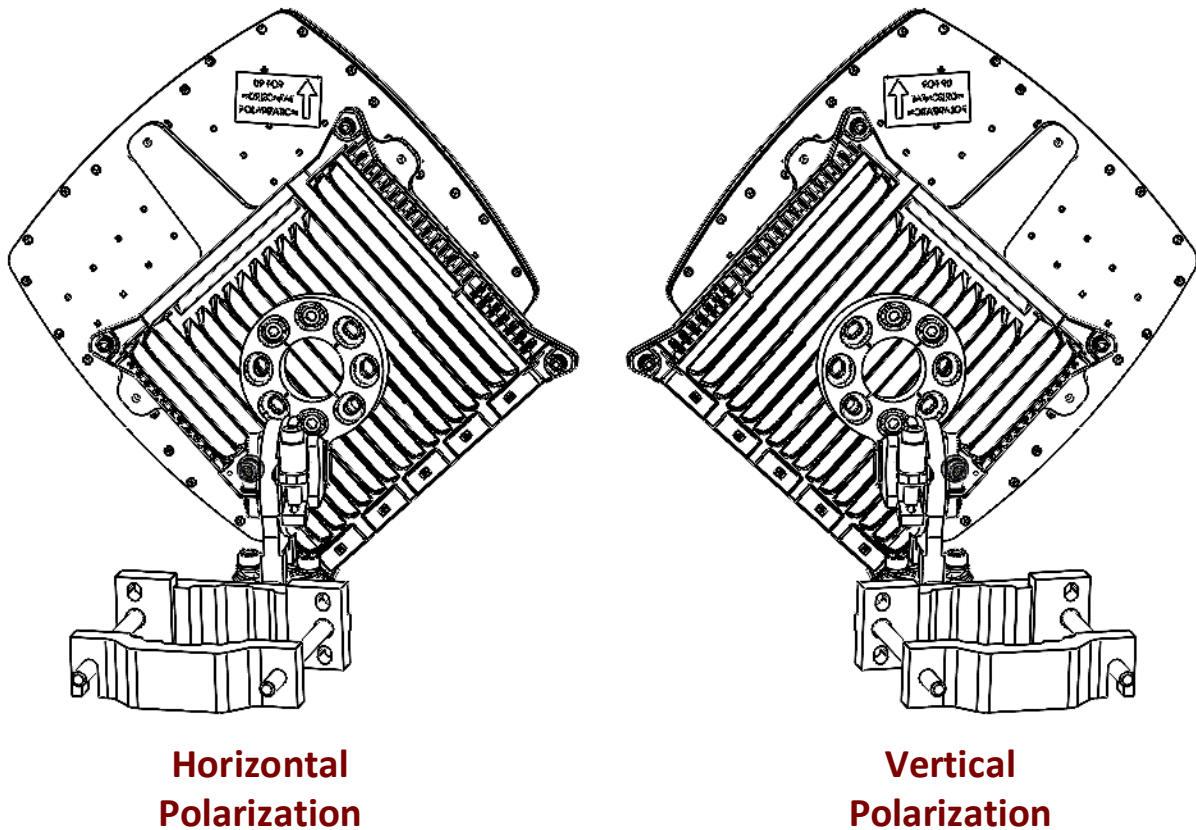


Figure 4: IP-50EX 2+0 DP Low Visual Impact

## 2. IP-50EX Hardware Description

This chapter describes the IP-50EX and its components and interfaces.

**This chapter includes:**

- IP-50EX Unit Description
- IP-50EX Interfaces
- Hardware Architecture
- PoE Injector
- Voltage Alarm Thresholds and PMs

## 2.1 IP-50EX Unit Description

IP-50EX features an all-outdoor architecture consisting of a single unit, which can be either directly mounted on the antenna or supplied with an integrated antenna.

**Note:** The equipment is type approved and labeled according to Radio Equipment Directive – RED (2014/53/EU).

Models with an integrated antenna are planned for future release.

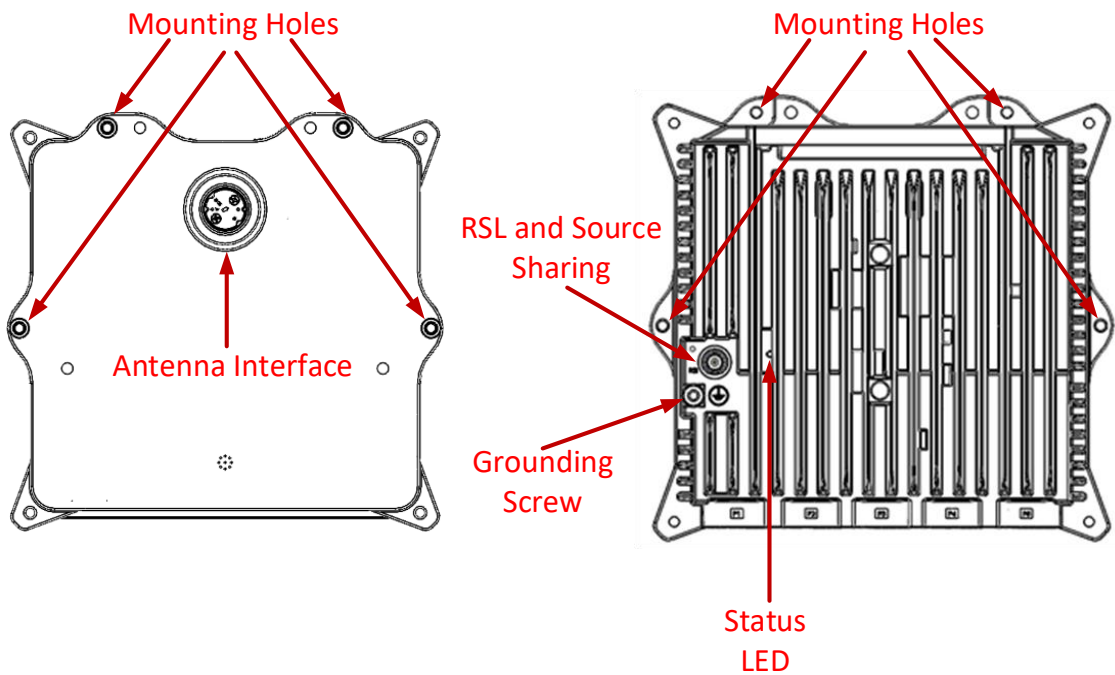


Figure 5: IP-50EX Direct Mount HW Ready – Rear View (Left) and Front View (Right)

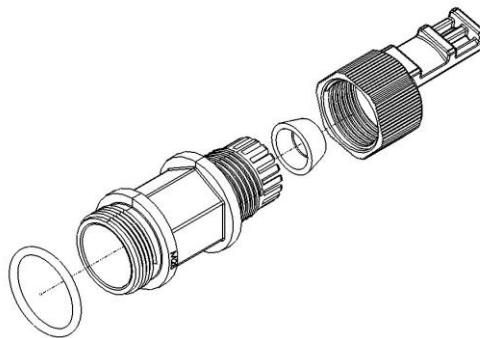


Figure 6: Cable Gland Construction

## 2.2 IP-50EX Interfaces

IP-50EX has two optical SFP28 cages for traffic. It also has one QSPF port which can be used as an XPIC/protection port or a 1 x 1GbE or 10GbE traffic port.

IP-50EX also has an RJ-45 management port.

For power, the IP-50EX has a DC power interface (-48V) (Port 1). IP-50EX-P also has an option to receive PoE power from a Ceragon-approved PoE injector via the management port, P2.

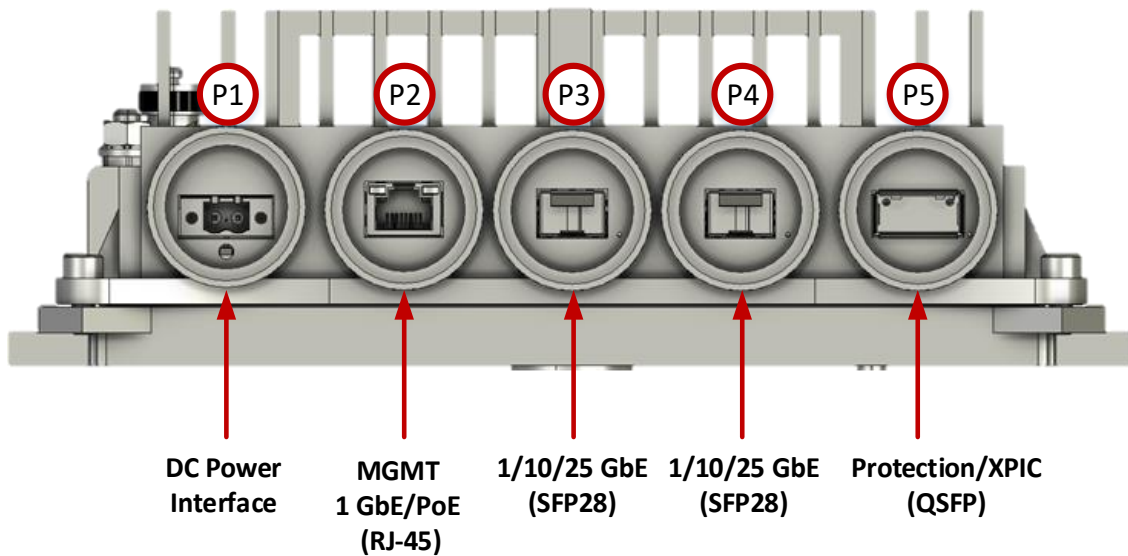


Figure 7: IP-50EX Interfaces

- P1 – Power Interface (-48V)
- P2 (MNG 1/Eth 1):
  - Electric: 100/1000Base-T RJ-45
  - Management port<sup>3</sup>
  - PoE-In (for IP-50EX-P)

**Note:** PoE requires IP-50EX-P.

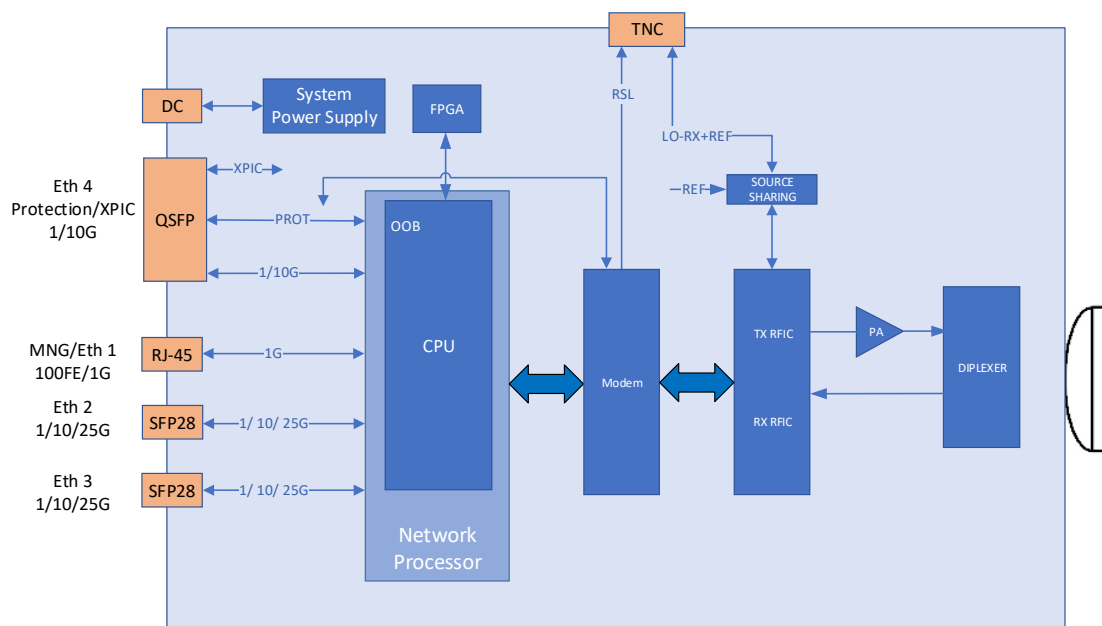
- P3 (Eth 2):
  - SFP cage which supports SFP28 standard
  - 1/10/25 GbE Eth traffic (user configurable)
- P4 (Eth 3):
  - SFP cage which supports SFP28 standard
  - 1/10/25 GbE Eth traffic (user configurable)

<sup>3</sup> In CeraOS 12.9.5, traffic over the Management port requires IP-50EX-P.

- P5 (Eth 4):
  - QSFP (internal) for Protection/XPIC
  - QSFP cage which supports QSFP standard
  - Option for SFP or SFP+ (1 x 1 or 10GbE) with adaptor (1+0 configurations only)
- RSL/Source Sharing interface – TNC connector
- Antenna Port – Ceragon proprietary flange (flange compliant with UG385/U)
- Grounding screw

## 2.3 Hardware Architecture

The following diagram presents a detailed block diagram of the IP-50EX.



*Figure 8: IP-50EX Block Diagram*

For a detailed description of the IP-50EXs interfaces, refer to *IP-50EX Interfaces* on page 20.

## 2.4 PoE Injector

**Note:** PoE-In support requires IP-50EX-P.

IP-50EX-P will offer a single-cable solution for connecting both data and the DC power supply to the IP-50EX. The following Ceragon-approved PoE Injector is required:

- **PoE\_Inj\_AO\_2DC\_24V\_48V** – Includes two DC power ports with power input ranges of -(18-60)V each.

The PoE injector combines 48VDC input and GbE signals via a standard CAT5E cable using a proprietary Ceragon design.

The PoE injector can be ordered with a DC feed protection, as well as EMC surge protection for both indoor and outdoor installation options. It can be mounted on poles, walls, or inside racks.

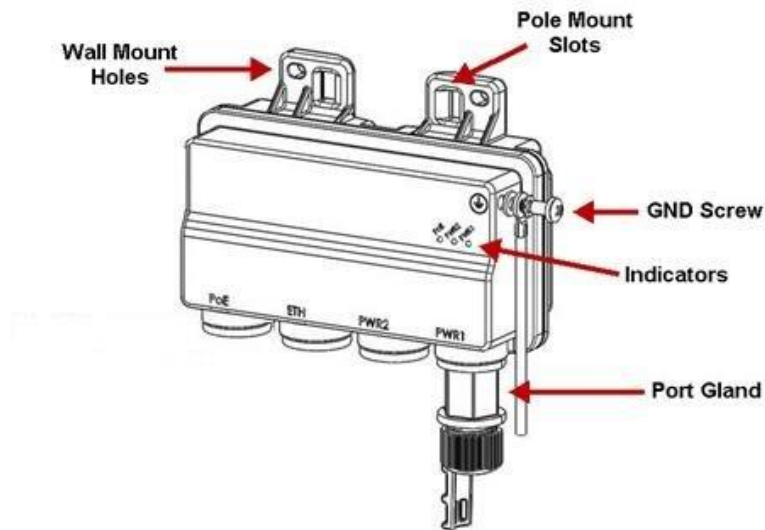


Figure 9: PoE Injector

### 2.4.1 PoE Injector Interfaces

- DC Power Port 1 -(18-60)V or -(40-60)V
- DC Power Port 2 -(18-60)V
- GbE Data Port supporting 10/100/1000Base-T
- Power-Over-Ethernet (PoE) Port
- Grounding screw

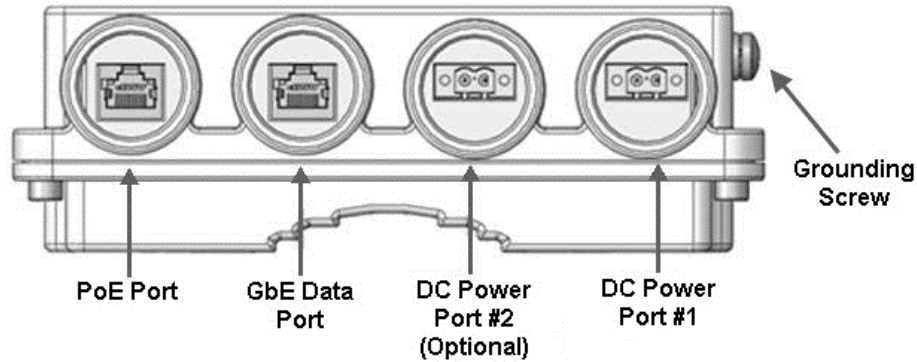


Figure 10: PoE Injector Ports

## 2.5 Voltage Alarm Thresholds and PMs

The allowed power input range for the IP-50EX is -40.5V to -60V. An undervoltage alarm is triggered if the power goes below a defined threshold, and an overvoltage alarm is triggered if the power goes above a defined threshold. The default thresholds are:

- Undervoltage Raise Threshold: 36V
- Undervoltage Clear Threshold: 38V
- Overvoltage Raise Threshold: 60V
- Overvoltage Clear Threshold: 58V

These thresholds are configurable.

IP-50EX also provides PMs that indicate, per 15-minute and 24-hour periods:

- The number of seconds the unit was in an undervoltage state during the measured period.
- The number of seconds the unit was in an overvoltage state during the measured period.
- The lowest voltage during the measured period.
- The highest voltage during the measured period.

### 3. Activation Keys

This chapter describes IP-50EX's activation key model. IP-50EX offers a pay as-you-grow concept in which future capacity growth and additional functionality can be enabled with activation keys. For purposes of the activation keys, each IP-50EX unit is considered a distinct device. Each device contains a single activation key.

**Note:** Alternatively, a Smart Activation Key is available for simplified and centralized activation key management, using a Smart Activation Key server to manage licensing for multiple devices. For further information about Smart Activation Key management, refer to the *Smart Activation Key User Guide*.

**This chapter includes:**

- Working with Activation Keys
- Demo Mode
- Activation Key Reclaim
- Activation Key-Enabled Features



### 3.1 Working with Activation Keys

Ceragon provides a web-based system for managing activation keys. This system enables authorized users to generate activation keys, which are generated per device serial number.

In order to upgrade an activation key, the activation key must be entered into the IP-50EX. The system checks and implements the new activation key, enabling access to new capacities and/or features.

In the event that the activated-key-enabled capacity and feature set is exceeded, an Activation Key Violation alarm occurs and the Web EMS displays a yellow background and an activation key violation warning. After a 48-hour grace period, all other alarms are hidden until the capacity and features in use are brought within the activation key's capacity and feature set.

### 3.2 Demo Mode

The system can be used in demo mode, which enables all features for 60 days. Demo mode expires 60 days from the time it was activated, at which time the most recent valid activation key cipher goes into effect. The 60-day period is only counted when the system is powered up. 10 days before demo mode expires, an alarm is raised indicating to the user that demo mode is about to expire.

<b>Note:</b>	Demo mode does not include AES radio encryption functionality unless a valid AES activation key has been applied for at least one carrier when demo mode is activated.
--------------	--

### 3.3 Activation Key Reclaim

If a customer needs to deactivate an IP-50EX device, whether to return it for repairs or for any other reason, the customer can reclaim the device's activation key and obtain a credit that can be applied to activation keys for other devices.

Where the customer has purchased upgrade activation keys, credit is given for the full feature or capacity, not for each individual upgrade. For example, if the customer purchased five capacity activation keys for 1G and later purchased two upgrade activation keys to 2.5G, credit is given as if the customer had purchased three activation keys for 1G and two activation keys for 2.5G.

### 3.4 Activation Key-Enabled Features

The default (base) activation key provides each carrier with a capacity of 10 Mbps. In addition, the default activation key provides:

- A single management service.
- A point-to-point (L1) service per each GbE port covered by the activation key.
  - 1 x GbE port for traffic.
- Full QoS.
- LAG
- No synchronization

**Note:** As described in more detail below, a CET Node activation key allows all CET service/EVC types including Point-to-Point, Multipoint, and MSTP for all services, as well as an additional GbE traffic port for a total of 2 x GbE traffic ports.

As your network expands and additional functionality is desired, activation keys can be purchased for the features described in the following table.

*Table 2: Activation Key Types*

Name	Marketing Model	Description	For Addition Information
ACM	SL-ACM	Adaptive Coding Modulation. A separate activation key is required per radio.	Adaptive Coding Modulation and Bandwidth (ACM and ACMB)
ACMB	SL-ACMB	Enables the use of ACMB. This activation key is required in order to use Profiles 0 and 1 with ACM scripts. A separate activation key is required per radio.	Adaptive Coding Modulation and Bandwidth (ACM and ACMB)
Advanced Security	SL-ADV-SEC	Enables Syslog Encryption and NTP Authentication. One activation key is required per device.	<ul style="list-style-type: none"> <li>• NTP Support</li> <li>• Syslog Support</li> </ul>
AES Encryption	SL-Encryption-AES256	<p>Enables the use of AES-GCM-256 encryption for full radio payload encryption. A separate activation key is required per carrier. Note that:</p> <ul style="list-style-type: none"> <li>• If no AES activation key is configured for the unit and the user attempts to enable AES on a radio carrier, in addition to an Activation Key Violation alarm the feature will remain inactive and no encryption will be performed.</li> <li>• After entering an AES activation key, the user must reset the unit before AES can be activated. Unit reset is only necessary for the first AES activation key. If AES activation keys are acquired later for additional radio carriers, unit reset is not necessary.</li> <li>• AES-GCM-256 requires IP-50EX-P.</li> </ul>	AES-GCM-256 Payload Encryption

Name	Marketing Model	Description	For Addition Information
ASP and LLF	SL-LLF	Enables the use of Link Loss Forwarding (LLF) with Automatic State Propagation (ASP). Without the activation key, only one LLF ID can be configured. This means that only one ASP pair can be configured per radio interface or radio group. One activation key is required per device.	Automatic State Propagation and Link Loss Forwarding
Carrier Ethernet Transport (CET)	Refer to <i>Edge CET Node Activation Keys</i> on page 29.	<p>Enables Carrier Ethernet Transport (CET) and a number of Ethernet services (EVCs), depending on the type of CET Node activation key:</p> <ul style="list-style-type: none"> <li>• Edge CET Node – Up to 8 EVCs.</li> <li>• Aggregation Level 1 CET Node – Up to 64 EVCs.</li> <li>• Aggregation Level 2 CET Node – Up to 1024 EVCs.</li> </ul> <p>A CET Node activation key also enables the following:</p> <ul style="list-style-type: none"> <li>• A GbE traffic port in addition to the port provided by the default activation key, for a total of 2 GbE traffic ports.</li> <li>• Network resiliency (MSTP/RSTP) for all services.</li> <li>• Full QoS for all services including basic queue buffer management (fixed queues buffer size limit, tail-drop only) and eight queues per port.</li> </ul>	<ul style="list-style-type: none"> <li>• Ethernet Service Model</li> <li>• Quality of Service (QoS)</li> </ul>
E-Stabilizer Advanced Features	SL-E-Stabilizer	Enables activation of automatic tracking mode and performance monitoring with E-Stabilizer.	E-Stabilizer
Eth. OAM - Fault Management	SL-Eth-OAM-FM	Enables Connectivity Fault Management (FM) per Y.1731. One activation key is required per device.	Connectivity Fault Management (FM)
Eth. OAM - Perf. Monitoring	SL-Eth-OAM-PM	Enables performance monitoring pursuant to Y.1731 (CET mode only). One activation key is required per device. <sup>4</sup>	
Ethernet traffic ports - 1GbE/2.5GbE	SL-GE-Port	Enables the use of 1GbE/2.5GbE ports. One GbE port is enabled by default without requiring any activation key. A separate activation key is required per port.	IP-50EX Interfaces
Ethernet traffic ports - 10GbE	SL-10GE-Port	Enables the use of 10GbE ports. A separate activation key is required per port.	IP-50EX Interfaces
Ethernet traffic ports – 25GbE	SL-25GE-Port	Enables the use of 25GbE ports. A separate activation key is required per port.	IP-50EX Interfaces

<sup>4</sup> Performance Monitoring (PM) is planned for future release.

Name	Marketing Model	Description	For Addition Information
IEEE 1588v2 Boundary Clock	SL-IEEE-1588-BC	Enables IEEE-1588 Boundary Clock. One activation key is required per device.	IEEE-1588v2 PTP Optimized Transport
IEEE 1588v2 Transparent Clock	SL-IEEE-1588-TC	Enables IEEE-1588 transparent clock. One activation key is required per device.	IEEE-1588v2 PTP Optimized Transport
LACP	SL-LACP	Enables Link Aggregation Control Protocol (LACP). One activation key is required per device. <sup>5</sup>	Link Aggregation Groups (LAG) and LACP
Netconf/YANG	SL-NETCONF/YANG	Enables management protocol Netconf on the device. One activation key is required per device.	SDN Support
Network Resiliency	SL-Network-Resiliency	Enables the following protocol for improving network resiliency: <ul style="list-style-type: none"> <li>• G.8032</li> </ul> One activation key is required per device.	Network Resiliency
Radio Capacity	Refer to <i>Capacity Activation Keys</i> on page 28	Enables you to increase your system's radio capacity in gradual steps by upgrading your capacity activation key. Without a capacity activation key, each IP-50EX unit has a capacity of 10 Mbps.	Radio Capacity Specifications
Secured Management	SL-Secure-Management	Enables secure management protocols (SSH, HTTPS, SFTP, SNMPv3, TACACS+, and RADIUS)	Secure Communication Channels
Synchronous Ethernet	SL-Sync-Unit	Enables the ITU-T G.8262 SyncE and ITU-T G.8264 ESMC synchronization unit. This activation key is required in order to provide end-to-end synchronization distribution on the physical layer. This activation key is also required to use Synchronous Ethernet (SyncE). One activation key is required per device.	Synchronization
XPIC	SL-mmW-XPIC	Enables the use of Cross Polarization Interference Canceller (XPIC). A separate activation key is required per radio member. <sup>6</sup>	Cross Polarization Interference Canceller (XPIC)

Table 3: Capacity Activation Keys

Marketing Model	Marketing Description	Notes
SL-mmW-Capacity-1G	Act.Key - Capacity 1G	
SL-mmW-Capacity-2.5G	SL - Capacity 2.5G	
SL-mmW-Capacity-3G	Act.Key - Capacity 3G	

<sup>5</sup> LACP is planned for future release.

<sup>6</sup> XPIC with IP-50EX-P is planned for future release.

Marketing Model	Marketing Description	Notes
SL-mmW-Capacity-4G	Act.Key - Capacity 4G	
SL-mmW-Capacity-5G	Act.Key - Capacity 5G	
SL-mmW-Capacity-6G	Act.Key - Capacity 6G	
SL-mmW-Capacity-7G	Act.Key - Capacity 7G	
SL-mmW-Capacity-8G	Act.Key - Capacity 8G	
SL-mmW-Capacity-9G	Act.Key - Capacity 9G	
SL-mmW-Capacity-10G	Act.Key - Capacity 10G	
SL-mmW-Upg-1G-2.5G	Act.Key - Upg 1G - 2.5G	
SL-mmW-Upg-1G-5G	Act.Key - Upg 1G - 5G	
SL-mmW-Upg-1G-10G	Act.Key - Upg 1G - 10G	
SL-mmW-Upg-2.5G - 5G	Act.Key - Upg 2.5G - 5G	
SL-mmW-Upg-2.5G - 7G	Act.Key - Upg 2.5G - 7G	
SL-mmW-Upg 2.5G--10G	Act.Key - Upg 2.5G - 10G	
SL-mmW-Upg-5G - 10G	Act.Key - Upg 5G - 10G	
SL-mmW-Upg-7G - 10G	Act.Key - Upg 7G - 10G	

Table 4: Edge CET Node Activation Keys

Marketing Model	# of Bundled GbE Ports for User Traffic	Management Service	# of Point-to-Point (L1) Ethernet Services	# of CET (L2) Ethernet Services
Default (No Activation Key)	1	Yes	Unlimited	-
SL-Edge-CET-Node	2	Yes	Unlimited	8
SL-Agg-Lvl-1-CET-Node	2	Yes	Unlimited	64
SL-Agg-Lvl-2-CET-Node	2	Yes	Unlimited	1024

If a CET activation key is not generated on the IP-50EX device upon initial configuration, the device uses by default a base smart pipe activation key (SL-0311-0). If the operator later wants to upgrade from the base smart pipe activation key to a CET activation key, the customer must use a CET upgrade activation key. The following table lists the CET upgrade activation keys:

*Table 5: Edge CET Node Upgrade Activation Keys*

Marketing Model	Upgrade From	Upgrade To
SL-Upg Smart-Pipe/Edge-CET nod	SL-Smart-Pipe (SL-0311-0)	SL-Edge-CET-Node (SL-0312-0)
SL - Upg Edge/Agg-Lvl-1-CET no	SL-Edge-CET-Node (SL-0312-0)	SL-Agg-Lvl-1-CET-Node (SL-0313-0)
SL - Upg Agg-Lvl-1/Lvl-2-CET n	SL-Agg-Lvl-1-CET-Node (SL-0313-0)	SL-Agg-Lvl-2-CET-Node (SL-0314-0)

## 4. Feature Description

This chapter describes the main IP-50EX features. The feature descriptions are divided into the categories listed below.

**Note:** For information on the availability of specific features, refer to the IP-50EX rollout plan or consult your Ceragon representative.

### This chapter includes:

- Capacity Summary
- Ethernet Features
- E-Stabilizer
- Frequency Scanner
- Synchronization
- AES-GCM-256 Payload Encryption (IP-50EX-P only)

## 4.1 Innovative Techniques to Boost Capacity and Reduce Latency

IP-50EX utilizes Ceragon's innovative technology to provide a high-capacity low-latency solution.

Ceragon was the first to introduce hitless and errorless Adaptive Coding and Modulation (ACM) to provide dynamic adjustment of the radio's modulation to account for up-to-the-minute changes in fading conditions.

IP-50EX employs full-range dynamic ACM, with modulations in the range of BPSK to 512 QAM.<sup>7</sup> IP-50EX takes ACM a step further by introducing Adaptive Coding Modulation and Bandwidth (ACMB). ACMB enhances standard ACM by decreasing channel spacing at BPSK when necessary to mitigate against fading.

IP-50EX also supports Cross Polarization Interference Canceller (XPIC). XPIC enables operators to achieve capacity of up to 20 Gbps in a single node with either two IP-50EX units directly mounted to an antenna via an OMT or two IP-50EX units each with a 43dBi integrated antenna. The two units utilize dual-polarization radio over a single-frequency channel, thereby transmitting two separate carrier waves over the same frequency, but with alternating polarities.<sup>8</sup>

### This section includes:

- Capacity Summary
- Adaptive Coding Modulation and Bandwidth (ACM and ACMB)
- Multiband
- Cross Polarization Interference Canceller (XPIC)
- 1+1
- ATPC
- Radio Signal Quality PMs

---

<sup>7</sup> Certain modulations are only supported with specific channels. For details, see *Radio Capacity Specifications* on page 170.

<sup>8</sup> The integrated antenna option is planned for future release. XPIC with IP-50EX-P is planned for future release.



#### 4.1.1 Capacity Summary

An IP-50EX unit can provide the following radio capacity:

- **Supported Channel Bandwidths** – 250/500/1000/2000 MHz channels
- **E-Band Frequency Bands** – 71-76 GHz, 81-86 GHz
- **Supported Modulation Range** – BPSK to 512 QAM<sup>9</sup> with ACMB

**For additional information:**

- Radio Capacity Specifications

---

<sup>9</sup> Certain modulations are only supported with specific channels. For details, see *Radio Capacity Specifications* on page 170.

#### 4.1.2 Adaptive Coding Modulation and Bandwidth (ACM and ACMB)

##### Related topics:

- Quality of Service (QoS)

---

ACM dynamically adjusts the radio's modulation to account for up-to-the-minute changes in fading conditions. ACMB is an enhancement of ACM that provides further flexibility to mitigate fading at BPSK by reducing the channel spacing to one half or one quarter of the original channel bandwidth when fading conditions make this appropriate.

IP-50EX employs full-range dynamic ACMB. IP-50EX's ACMB mechanism copes with 100 dB per second fading in order to ensure high transmission quality. IP-50EX's ACM mechanism is designed to work with IP-50EX's QoS mechanism to ensure that high priority voice and data frames are never dropped, thus maintaining even the most stringent service level agreements (SLAs).

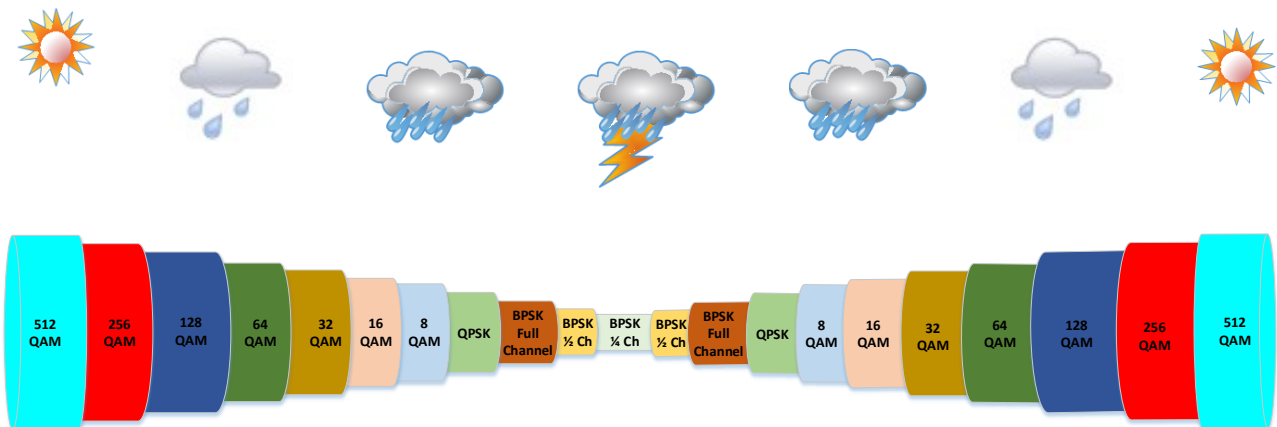
The hitless and errorless functionality of IP-50EX's ACM has another major advantage in that it ensures that TCP/IP sessions do not time-out. Without ACM, even interruptions as short as 50 milliseconds can lead to timeout of TCP/IP sessions, which are followed by a drastic throughput decrease while these sessions recover.

#### 4.1.2.1 Eleven Working Points

IP-50EX implements ACMB with eleven available working points, as shown in the following table:

*Table 6: ACM Working Points (Profiles)*

Profile 0	BPSK – $\frac{1}{4}$ channel spacing
Profile 1	BPSK – $\frac{1}{2}$ channel spacing
Profile 2	BPSK – full channel spacing
Profile 3	QPSK
Profile 4	8 PSK
Profile 5	16 QAM
Profile 6	32 QAM
Profile 7	64 QAM
Profile 8	128 QAM
Profile 9	256 QAM
Profile 10	512 QAM



*Figure 11: Adaptive Coding and Modulation with Eleven Working Points*

#### 4.1.2.2 Hitless and Errorless Step-by Step Adjustments

ACMB works as follows. Assuming a system configured for 128 QAM over a 250 MHz channel, when the receive signal Bit Error Ratio (BER) level reaches a predetermined threshold, the system preemptively switches to 64 QAM and the throughput is stepped down accordingly. This is an errorless, virtually instantaneous switch. The system continues to operate at 64 QAM until the fading condition either intensifies or disappears. If the fade intensifies, another switch takes the system down to 32 QAM. If, on the other hand, the weather condition improves, the modulation is switched back to the next higher step (e.g., 128 QAM) and so on, step by step. The switching continues automatically and as quickly as needed, and can reach all the way down to QPSK during extreme conditions.

At BSPK, the channel spacing comes into play. At BSPK, frequency selective fading can become problematic. To mitigate against fading, the ACMB mechanism can automatically reduce the channel bandwidth to half or a quarter of the ordinary channel bandwidth configured for the radio. Once the fading condition has been reduced or eliminated, the mechanism restores half or full channel bandwidth.

#### 4.1.2.3 ACM Radio Scripts

An ACM radio script is constructed of a set of profiles. Each profile is defined by a modulation order (QAM) and coding rate, and defines the profile's capacity (bps). When an ACM script is activated, the system automatically chooses which profile to use according to the channel fading conditions.

The ACM TX profile can be different from the ACM RX profile.

The ACM TX profile is determined by remote RX MSE performance. The RX end is the one that initiates an ACM profile upgrade or downgrade. When MSE improves above a predefined threshold, RX generates a request to the remote TX to upgrade its profile. If MSE degrades below a predefined threshold, RX generates a request to the remote TX to downgrade its profile.

ACM profiles are decreased or increased in an errorless operation, without affecting traffic.

ACM scripts can be activated in one of two modes:

- **Fixed Mode.** In this mode, the user can select the specific profile from all available profiles in the script. The selected profile is the only profile that will be valid, and the ACM engine will be forced to be OFF. This mode can be chosen without an ACM activation key.
- **Adaptive Mode.** In this mode, the ACM engine is running, which means that the radio adapts its profile according to the channel fading conditions. Adaptive mode requires an ACM activation key.

The user can define a minimum and maximum profile. For example, if the user selects a maximum profile of 5, the system will not climb above the profile 5, even if channel fading conditions allow it.

For all scripts, Profile 2 has a modulation of BPSK using the full channel bandwidth defined for the script. Profile 1 has a modulation of BPSK with half of the defined channel bandwidth, and Profile 0 has a modulation of BPSK with a quarter of the defined channel bandwidth. Profiles 0 and 1 come into play when ACMB reduces the channel bandwidth at BSPK to cope with fading conditions.

**Note:** The default minimum profile is Profile 2.

#### 4.1.2.4 Hysteresis Value

When stepping down to a lower profile, the switch is initiated when the RSL is approximately 3.5 dB higher than the threshold for the current profile. When stepping up to a higher profile, the switch is initiated when the RSL is approximately 5 dB higher than the threshold for the higher profile.

#### 4.1.2.5 ACM PMs

Users can configure two thresholds, per radio carrier, for the ACM profile. These thresholds enable users to monitor ACM profile fluctuations by displaying the number of seconds, per 15-minute or 24-hour interval, that the ACM profile drops beneath each profile threshold.

In addition, these thresholds trigger the following alarms:

- **Threshold 1** – When the ACM profile goes beneath this threshold, Alarm ID 1313 (Major) is raised. The alarm is cleared when the ACM profile is at or above this threshold.
- **Threshold 2** – When the ACM profile goes beneath this threshold, Alarm ID 1314 (Critical) is raised. The alarm is cleared when the ACM profile is at or above this threshold.

#### 4.1.2.6 ACMB Benefits

The advantages of IP-50EX's dynamic ACMB include:

- Maximized spectrum usage
- Increased capacity over a given bandwidth
- Up to eleven modulation/coding work points (~3 db system gain for each point change)
- Hitless and errorless modulation/coding changes, based on signal quality
- Adaptive Radio Transmit Power per modulation for maximal system gain per working point
- An integrated QoS mechanism that enables intelligent congestion management to ensure that high priority traffic is not affected during link fading

#### 4.1.2.7 ACM and Built-In QoS

IP-50EX's ACMB mechanism is designed to work with IP-50EX's QoS mechanism to ensure that high priority voice and data frames are never dropped, thus maintaining even the most stringent SLAs. Since QoS provides priority support for different classes of service, according to a wide range of criteria, you can configure IP-50EX to discard only low priority frames as conditions deteriorate.

If you want to rely on an external switch's QoS, ACMB can work with the switch via the flow control mechanism supported in the radio.

#### 4.1.2.8 ACM with Adaptive Transmit Power

##### **This feature requires:**

- ACM script

---

In ACM Adaptive Mode, Adaptive Transmit Power enables operators to dynamically apply the lowest transmit power that will perform satisfactorily at every modulation level.

When Adaptive Transmit Power is enabled, the radio adjusts its TX power dynamically based on the current modulation. When the modulation is at a high level, the TX power is adjusted to the level required with the high modulation. If the modulation goes down to a lower level, the TX power increases to compensate for the lower modulation. This ensures that the radio does not use more power than is necessary in order to optimize capacity at every modulation point. The user-configured TX power defines the maximum TX power, but when the link is functioning in optimal conditions, at high modulation, the actual TX power will typically be lower than the defined level, thereby minimizing the power required to operate the radio.

### 4.1.3 Multiband

IP-50EX can be used in Multiband configurations with IP-20N and IP-20A in which the IP-50EX is paired with an IP-50C, IP-20C, IP-20C-HP, RFU-D, RFU-D-HP, or RFU-C microwave radio.

IP-20C, IP-20C-HP, RFU-D, and RFU-D-HP can be used in 1+0 or 2+0 configurations.

Multiband bundles E-Band and microwave radios in a single group that is shared with an Ethernet interface. This provides an Ethernet link over the radio with capacity of up to 10 Gbps. A Multiband link is highly resilient because the microwave link acts, in effect, as a backup for the E-Band link.

In the event of radio failure in one device, the other device continues to operate to the extent of its available capacity. Thus, operators benefit from both the high capacity of E-Band and the high reliability of microwave.

#### 4.1.3.1 Multiband Antenna

For configurations with IP-50EX and IP-20C, RFU-D, or RFU-C, a special Multiband antenna can be used. This antenna transmits and receives both E-band and microwave signals. Both the E-band and the microwave units are connected to this antenna via direct mount.

The marketing model for Multiband antennas uses the following syntax:

*Am-sm-d-ff/80-pl/ph-vn*

Where:

- s – Standard compliance
  - E – ETSI only
  - F – FCC only
  - B – ETSI and FCC
 E and B includes a number (1-4) to designate ETSI Antenna Class (e.g., B3)
- m – ETSI class (1-4 – only applicable for “E” and “B”)

**Note:** Some older models do not include the *sm* designation in their marketing models.

- d – Size of the antenna (1 or 2 ft)
- ff – The microwave band (11, 13, 15, 18, 23, 28, etc.)
- pl – Interface of the microwave antenna
  - SP – single polarization (rectangular interface)
  - DP – dual polarization (circular interface)
- ph – Interface of the E-Band antenna:
  - SP – single polarization (rectangular interface)
  - DP – dual polarization (circular interface)
- vn – Antenna Vendor (MT: MTI, A: CommScope, RS: Prose, etc.)

For example, the following marketing model applies to a 2-foot antenna for an 18 GHz Microwave radio together with an E-band device, where the Microwave radio is operating with Dual Polarization and the E-band radio is operating with Single Polarization. The manufacturer is CommScope.

*Am-B3-2-18/80-DP/SP-A*

For a full list of available Multiband antennas, refer to the Price List or check with your Ceragon representative.

**Note:** The Multiband Antenna cannot be used with IP-20C-HP or RFU-D-HP.

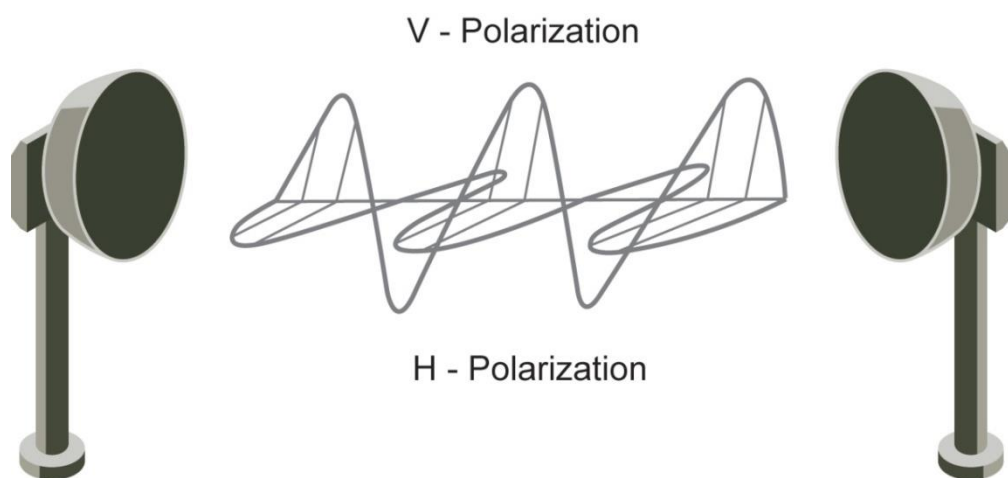


#### 4.1.4 Cross Polarization Interference Cancellation (XPIC)

**Note:** XPIC with IP-50EX-P is planned for future release.

XPIC is one of the best ways to break the barriers of spectral efficiency. Using dual-polarization radio over a single-frequency channel, two IP-50EX units connected to a single antenna via an OMT transmit two separate carrier waves over the same frequency, but using alternating polarities. XPIC enables IP-50EX links of up to 20 Gbps, consisting of 10 Gbps per each IP-50EX unit.

Despite the obvious advantages of dual-polarization, one must also keep in mind that typical antennas cannot completely isolate the two polarizations. In addition, propagation effects such as rain can cause polarization rotation, making cross-polarization interference unavoidable.



*Figure 12: Dual Polarization*

The relative level of interference is referred to as cross-polarization discrimination (XPD). While lower spectral efficiency systems (with low SNR requirements such as QPSK) can easily tolerate such interference, higher modulation schemes cannot and require XPIC. IP-50EX's XPIC algorithm enables detection of both streams even under the worst levels of XPD such as 10 dB. IP-50EX accomplishes this by adaptively subtracting from each carrier the interfering cross carrier, at the right phase and level.

#### 4.1.4.1 XPIC Implementation

The XPIC mechanism utilizes the received signals from the V and H modems to extract the V and H signals and cancel the cross polarization interference due to physical signal leakage between V and H polarizations.

The following figure is a basic graphic representation of the signals involved in this process.

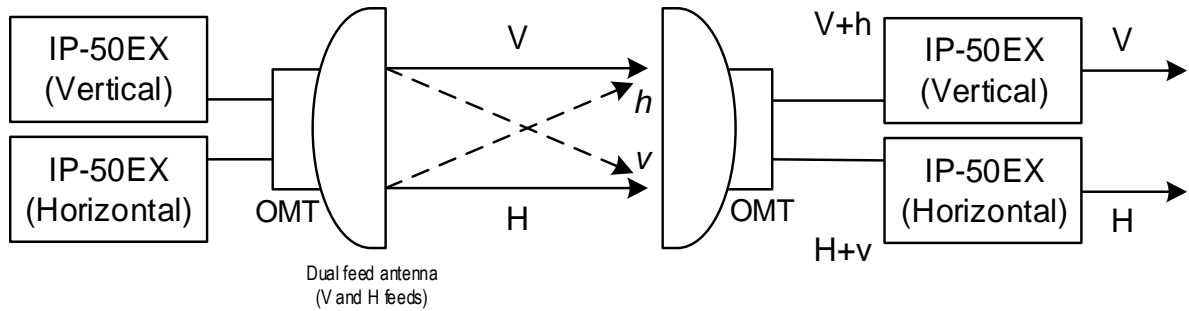


Figure 13: XPIC Implementation – Direct Mount

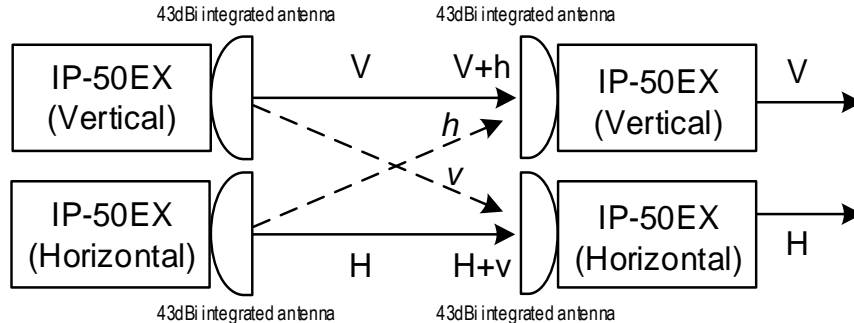
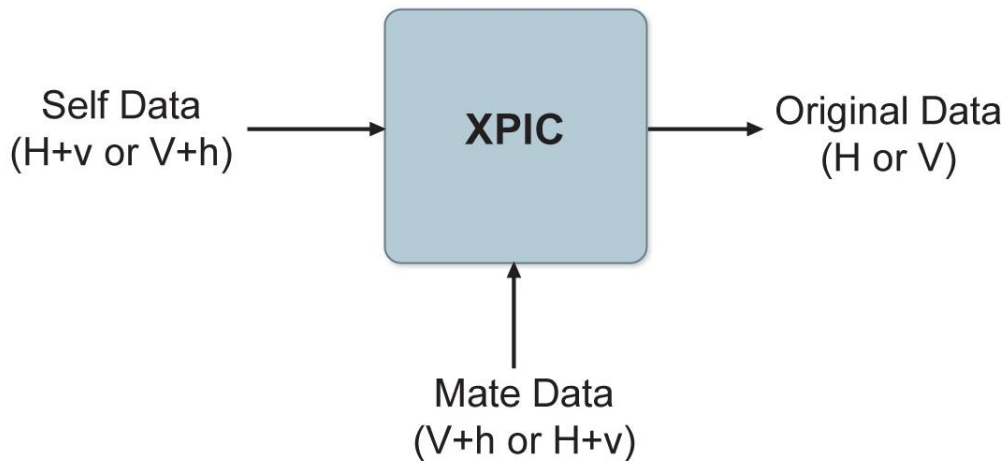


Figure 14: XPIC Implementation – Integrated Antenna

The H+v signal is the combination of the desired signal H (horizontal) and the interfering signal V (in lower case, to denote that it is the interfering signal). The same happens with the vertical (V) signal reception= V+h. The XPIC mechanism uses the received signals from both feeds and, manipulates them to produce the desired data.



*Figure 15: XPIC – Impact of Misalignments and Channel Degradation*

#### 4.1.4.2 XPIC Configuration

An IP-50EX 2+0 XPIC configuration requires two IP-50EX units on each side of the link. Two options are available:

- **Direct Mount** – The IP-50EX units are connected to the antenna via an OMT. One unit must be installed with horizontal polarization and the other must be installed with vertical polarization.
- **Integrated Antenna** – One IP-50EX unit and integrated antenna is assembled with a vertical polarization and the other IP-50EX unit and integrated antenna is assembled with a horizontal polarization.

For both options, the following cables must be used to connect the two units:

- An XPIC cable must be connected between the Protection/XPIC ports (P5) of each unit. This cable carries the data necessary for each unit to perform interference cancellation.
- A Clock Sharing cable must be connected between the TNC ports of each unit. This cable transmits clock frequency information between the two units, enabling synchronization.

On each side of the link, the unit with the higher MAC address is automatically assigned the role of clock master unit.

The main unit can be either vertical or horizontal. Just make sure that the main units on both side of the link have the same polarization (vertical or horizontal), and that the paired units on both side of the link have the same polarization, which should be the opposite polarization of the main units.

Each IP-50EX unit receives traffic from the external switch independently of the other unit. The traffic flows are completely independent, with no traffic sharing or load balancing between the units.

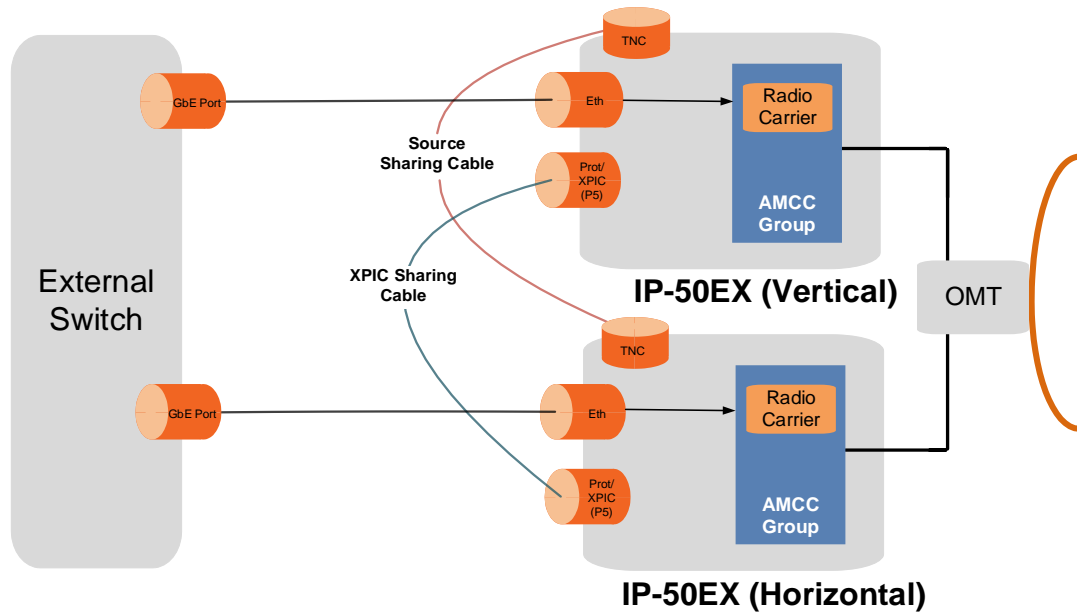


Figure 16: 2+0 XPIC Configuration – Direct Mount

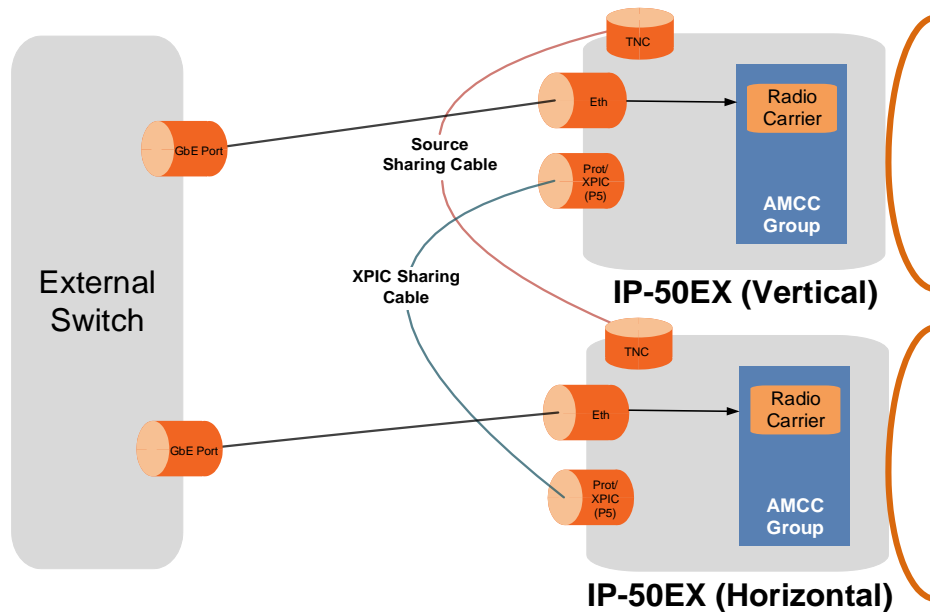


Figure 17: 2+0 XPIC Configuration – Integrated Antenna

Management data is not shared between the two IP-50EX units. Therefore, management must be configured independently for each IP-50EX unit. In-band management can be used as long as LAG is not configured on the external switch. However, if LAG is configured on the external switch, in-band management cannot be used, since there is no mechanism for sharing management traffic between the IP-50EX units.

In order for XPIC to be operational, all the following conditions must be met:

- The frequency of both carriers should be equal.
- The same script must be loaded in both carriers.

#### 4.1.5 1+1 HSB and Unit Redundancy

<b>Note:</b>	1+1 HSB protection and Unit Redundancy are planned for future release.
--------------	--

1+1 HSB protection with Unit Redundancy utilizes two IP-50EX units connected to a single antenna via a coupler to provide hardware redundancy for the radio link and Ethernet traffic.

One IP-50EX operates in active mode and the other operates in standby mode. Each IP-50EX monitors its own radio. If a protection switchover occurs, the roles are switched. The active unit goes into standby mode and the standby unit goes into active mode.

The standby unit is managed by the active unit. The standby unit's transmitter is muted, but the standby unit's receiver is kept on in order to monitor the link. However, the received signal is terminated at the switch level.

#### 4.1.6 ATPC

ATPC is a closed-loop mechanism by which each carrier changes the TX power according to the indication received across the link, in order to achieve a desired RSL on the other side of the link.

ATPC enables the transmitter to operate at less than maximum power for most of the time. When fading conditions occur, TX power is increased as needed until the maximum is reached.

The ATPC mechanism has several potential advantages, including less power consumption and longer amplifier component life, thereby reducing overall system cost.

ATPC is frequently used as a means to mitigate frequency interference issues with the environment, thus allowing new radio links to be easily coordinated in frequency congested areas.

##### 4.1.6.1 ATPC Override Timer

This feature complies with NSMA Recommendation WG 18.91.032. With ATPC enabled, if the radio automatically increases its TX power up to the configured maximum it can lead to a period of sustained transmission at maximum power, resulting in unacceptable interference with other systems.

To minimize interference, IP-50EX provides an ATPC override mechanism. When ATPC override is enabled, a timer begins when ATPC raises the TX power to its maximum. When the timer expires, the ATPC maximum TX power is overridden by the user-configured ATPC override TX power level until the user manually cancels the ATPC override. The unit then returns to normal ATPC operation.

The following parameters can be configured:

- **ATPC Override Admin** – Determines whether the ATPC override mechanism is enabled.
- **Override TX Level** – The TX power, in dBm, used when the unit is in an ATPC override state.
- **Override Timeout** – The amount of time, in seconds, the timer counts from the moment the radio reaches its maximum configured TX power until ATPC override goes into effect.

When the radio enters ATPC override state, the radio transmits no higher than the pre-determined ATPC override TX level, and an ATPC override alarm is raised. The radio remains in ATPC override state until the ATPC override state is manually cancelled by the user (or the unit is reset).

**Note:** When canceling an ATPC override state, the user should ensure that the underlying problem has been corrected. Otherwise, ATPC may be overridden again.

#### 4.1.7 Radio Signal Quality PMs

IP-50EX supports the following radio signal quality PMs. For each of these PM types, users can display the minimum and maximum values, per radio, for every 15-minute interval. Users can also define thresholds and display the number of seconds during which the radio was not within the defined threshold.

- RSL (users can define two RSL thresholds)
- TSL
- MSE
- XPI

Users can display BER PMs, including the current BER per radio, and define thresholds for Excessive BER and Signal Degrade BER. Alarms are issued if these thresholds are exceeded. See *Configurable BER Threshold for Alarms and Traps* on page 135. Users can also configure an alarm that is raised if the RSL falls beneath a user-defined threshold. See *RSL Threshold Alarm* on page 135.



#### 4.1.8 Radio Utilization PMs

IP-50EX supports the following counters, as well as additional PMs based on these counters:

- Radio Traffic Utilization – Measures the percentage of radio capacity utilization, and used to generate the following PMs for every 15-minute interval:
  - Peak Utilization (%)
  - Average Utilization (%)
  - Over-Threshold Utilization (seconds). Up to three utilization thresholds can be defined by users (0-100%).
- Radio Traffic Throughput – Measures the total effective Layer 2 traffic sent through the radio (Mbps), and used to generate the following PMs for every 15-minute interval:
  - Peak Throughput
  - Average Throughput
  - Over-Threshold Utilization (seconds). The default threshold is 100.
- Radio Traffic Capacity – Measures the total L1 bandwidth (payload plus overheads) sent through the radio (Mbps), and used to generate the following PMs for every 15-minute interval:
  - Peak Capacity
  - Average Capacity
  - Over-Threshold Utilization (seconds). The default threshold is 100.

## 4.2 Ethernet Features

IP-50EX's service-oriented Ethernet paradigm enables operators to configure VLAN definition and translation, CoS, and security on a service, service-point, and interface level.

IP-50EX provides personalized and granular QoS that enables operators to customize traffic management parameters per customer, application, service type, or in any other way that reflects the operator's business and network requirements.

### **This section includes:**

- IP-50EX's Ethernet Capabilities
- Ethernet Service Model
- Ethernet Interfaces
- Quality of Service (QoS)
- Global Switch Configuration
- Automatic State Propagation and Link Loss Forwarding
- Network Resiliency
- OAM

#### 4.2.1 IP-50EX's Ethernet Capabilities

IP-50EX is built upon a service-based paradigm that provides rich and secure frame backhaul services over any type of transport, with unified, simple, and error-free operation. IP-50EX's services core includes a rich set of tools that includes:

- Service-based Quality of Service (QoS).
- Service OAM.
- Carrier-grade service resiliency using G.8032

The following are IP-50EX's main Carrier Ethernet transport features. This rich feature set provides a future-proof architecture to support backhaul evolution for emerging services.

- Up to 1024 services
- Up to 32 service points per service
- Up to 4538 service points per device
- All service types:
  - Multipoint (E-LAN)
  - Point-to-Point (E-Line)
  - Management
- 32K MAC learning table (per device)
- Flexible transport and encapsulation via 802.1q and 802.1ad, with tag manipulation possible at ingress and egress
- High precision, flexible frame synchronization solution combining SyncE and IEEE-1588v2
- Hierarchical single-rate three-Color policers
  - Port-based – Unicast, Multicast, Broadcast. One policer per port.
  - Service point-based. One policer per service point.
- Up to four link aggregation groups (LAG)
  - Hashing based on L2, L3, and MPLS
- Enhanced <50msec network level resiliency (G.8032) for ring support

#### 4.2.2 Ethernet Service Model

IP-50EX's service-oriented Ethernet paradigm is based on Carrier-Ethernet Transport (CET), and provides a highly flexible and granular switching fabric for Ethernet services.

IP-50EX's virtual switching/forwarding engine is based on a clear distinction between user-facing service interfaces and intra-network service interfaces. User-facing interfaces (UNIs) are configured as Service Access Points (SAPs), while intra-network interfaces (E-NNIs or NNIs) are configured as Service Network Points (SNPs).

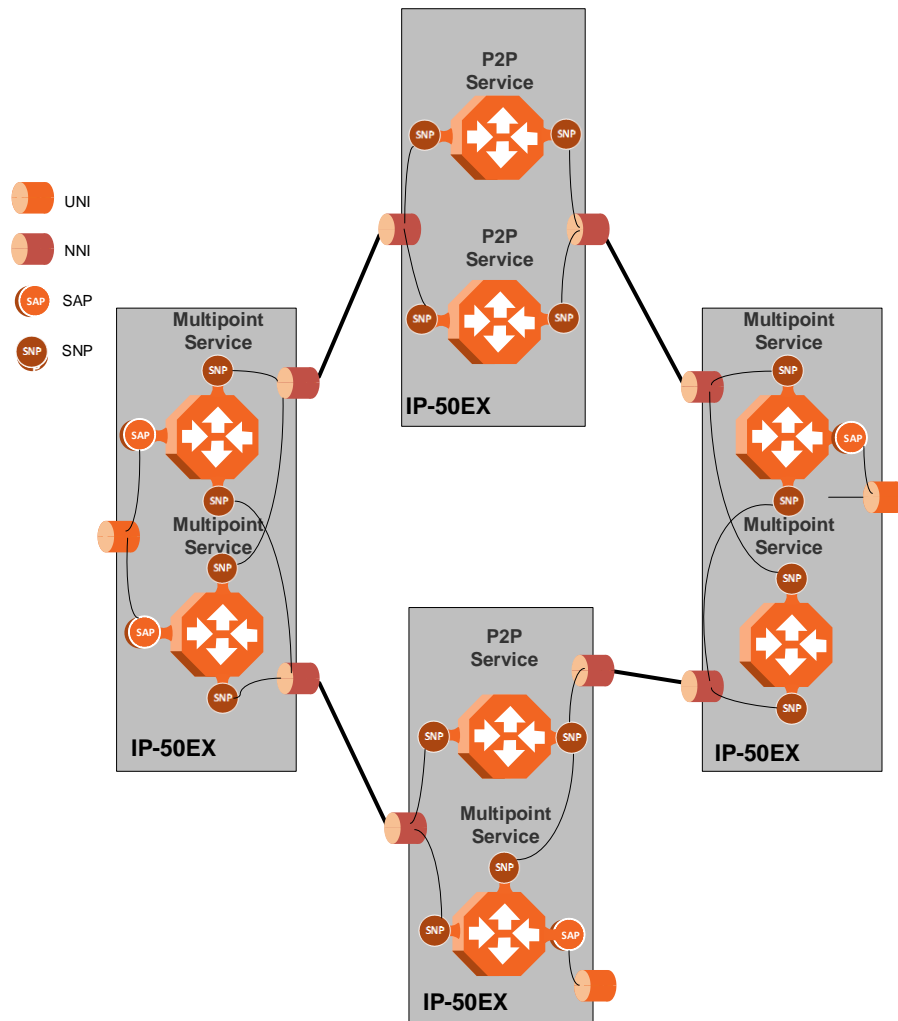


Figure 18: IP-50EX Services Model

The IP-50EX services core provides for fully flexible C-VLAN and S-VLAN encapsulation, with a full range of classification, preservation, and translation options available. Service security and isolation is provided without limiting the C-VLAN reuse capabilities of different customers.

**Note:** A single device supports up to a maximum of 9216 VLANs (9204 VLANs in Bundle-C and 8436 VLANs in Bundle-S).

Users can define up to 1024 services on a single IP-50EX. Each service constitutes a virtual bridge that defines the connectivity and behavior among the network element interfaces for the specific virtual bridge. In addition to user-defined services, IP-50EX contains a pre-defined management service (Service ID 1025). If needed, users can activate the management service and use it for in-band management.

To define a service, the user must configure virtual connections among the interfaces that belong to the service. This is done by configuring service points (SPs) on these interfaces.

A service can hold up to 32 service points. A service point is a logical entity attached to a physical or logical interface. Service points define the movement of frames through the service. Each service point includes both ingress and egress attributes.

**Note:** Management services can hold up to 30 SPs.

The following figure illustrates the IP-50EX services model, with traffic entering and leaving the network element. IP-50EX's switching fabric is designed to provide a high degree of flexibility in the definition of services and the treatment of data flows as they pass through the switching fabric.

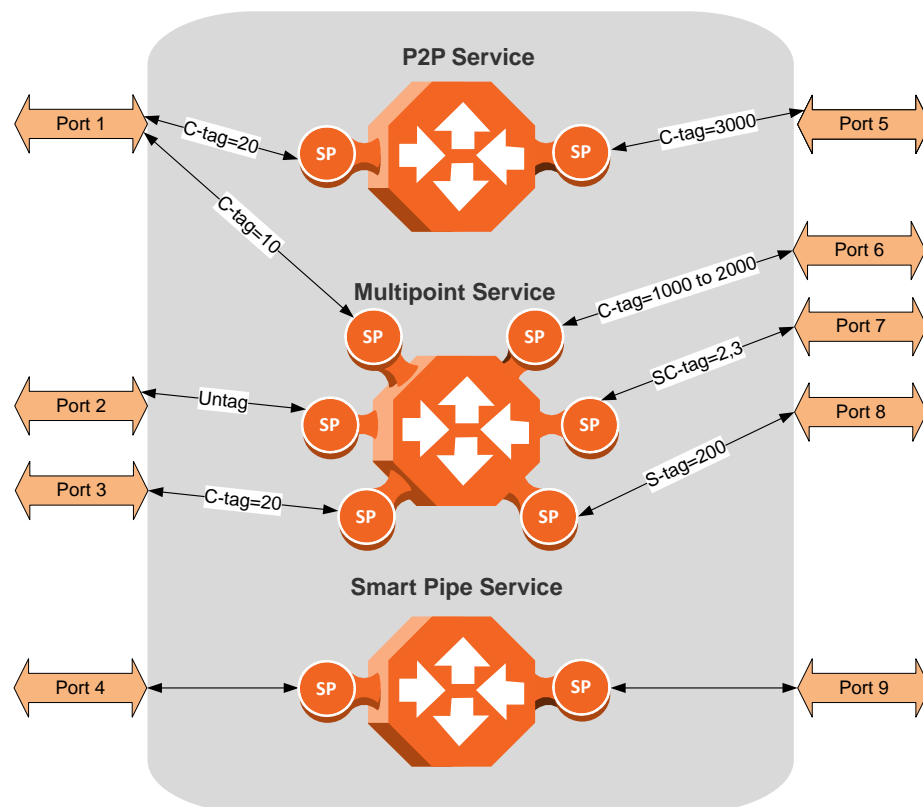


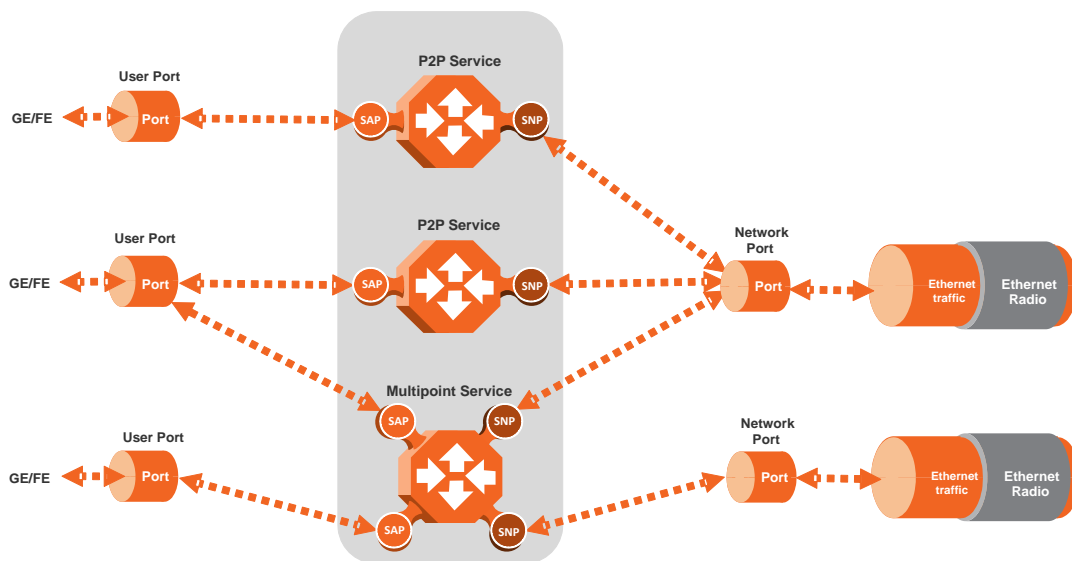
Figure 19: IP-50EX Services Core

#### 4.2.2.1 Frame Classification to Service Points and Services

Each arriving frame is classified to a specific service point, based on a key that consists of:

- The Interface ID of the interface through which the frame entered the IP-50EX.
- The frame's C-VLAN and/or S-VLAN tags.

If the classification mechanism finds a match between the key of the arriving frame and a specific service point, the frame is associated to the specific service to which the service point belongs. That service point is called the ingress service point for the frame, and the other service points in the service are optional egress service points for the frame. The frame is then forwarded from the ingress service point to an egress service point by means of flooding or dynamic address learning in the specific service.



Service Types Figure 20: IP-50EX Services Flow

IP-50EX supports the following service types:

- Point-to-Point Service (P2P)
- MultiPoint Service (MP)
- Management Service

### Point to Point Service (P2P)

Point-to-point services are used to provide connectivity between two interfaces of the network element. When traffic ingresses via one side of the service, it is immediately directed to the other side according to ingress and egress tunneling rules. This type of service contains exactly two service points and does not require MAC address-based learning or forwarding. Since the route is clear, the traffic is tunneled from one side of the service to the other and vice versa.

The following figure illustrates a P2P service.

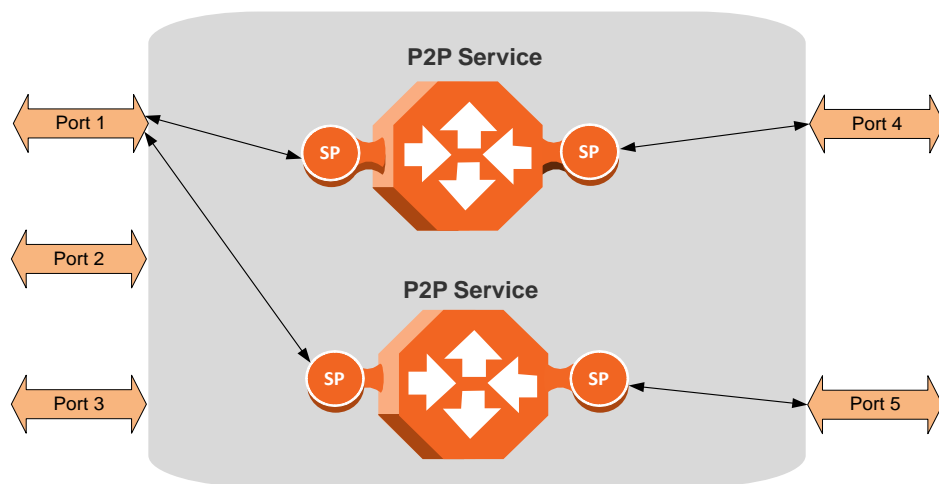


Figure 21: Point-to-Point Service

P2P services provide the building blocks for network services such as E-Line EVC (EPL and EVPL EVCs) and port-based services.

### Multipoint Service (MP)

Multipoint services are used to provide connectivity between two or more service points. When traffic ingresses via one service point, it is directed to one of the service points in the service, other than the ingress service point, according to ingress and egress tunneling rules, and based on the learning and forwarding mechanism. If the destination MAC address is not known by the learning and forwarding mechanism, the arriving frame is flooded to all the other service points in the service except the ingress service point.

The following figure illustrates a Multipoint service.

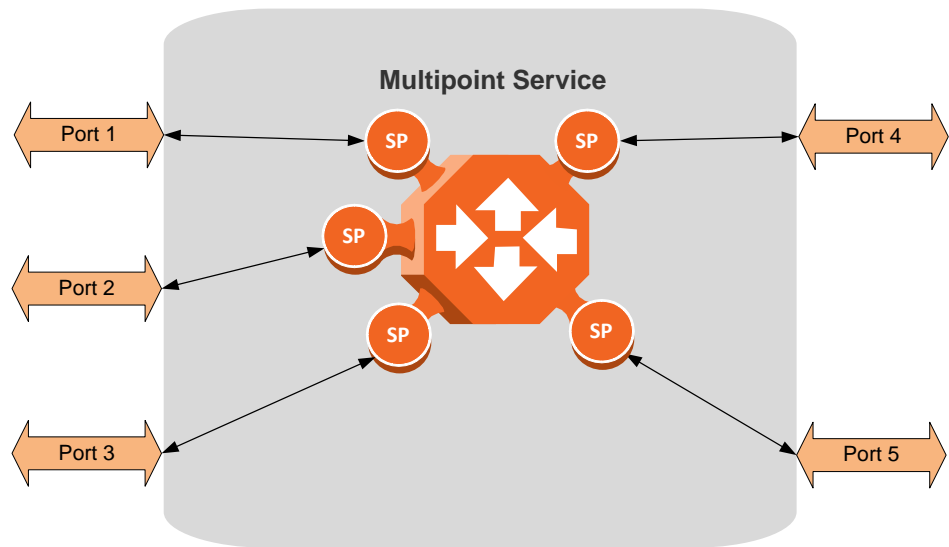


Figure 22: Multipoint Service

Multipoint services provide the building blocks for network services such as E-LAN EVCs (EP-LAN and EVP-LAN EVCs), and for E-Line EVCs (EPL and EVPL EVCs) in which only two service points are active. In such a case, the user can disable MAC address learning in the service points to conserve system resources.

Learning and Forwarding Mechanism

IP-50EX can learn up to 32K Ethernet source MAC addresses. The size of the MAC address table is for the device as a whole, and is not configurable.

When a frame arrives via a specific service point, the learning mechanism checks the MAC forwarding table to determine whether that frame’s source MAC address is known to the service. If the MAC address is not found, the learning mechanism adds it to the table under the specific service point.

In parallel with the learning process, the forwarding mechanism searches the service’s MAC forwarding table for the frame’s destination MAC address. If a match is found, the frame is forwarded to the service point associated with the MAC address. If not, the frame is flooded to all service points in the service.

The following table illustrates the operation of the learning and forwarding mechanism.

Table 7: Ethernet Services Learning and Forwarding

MAC Forwarding Table			
Input Key for learning / forwarding (search) operation		Result	Entry type
Service ID	MAC address	Service Point	
13	00:34:67:3a:aa:10	15	dynamic



MAC Forwarding Table

Input Key for learning / forwarding (search) operation		Result	Entry type
Service ID	MAC address	Service Point	
13	00:0a:25:33:22:12	31	dynamic
28	00:0a:25:11:12:55	31	static
55	00:0a:25:33:22:12	15	dynamic
55	00:c3:20:57:14:89	31	dynamic
55	00:0a:25:11:12:55	31	dynamic

In addition to the dynamic learning mechanism, users can add static MAC addresses for static routing in each service.

Users can manually clear all the dynamic entries from the MAC forwarding table. Users can also delete static entries per service.

The system also provides an automatic flush process. An entry is erased from the table as a result of:

- The global aging time expires for the entry.
- Loss of carrier occurs on the interface with which the entry is associated.
- Resiliency protocols, such as MSTP or G.8032.

### Management Service (MNG)

The management service connects the local management port, the network element host CPU, and the traffic ports into a single service. The management service is pre-defined in the system, with Service ID 1025. The pre-defined management service has a single service point that connects the service to the network element host CPU and the management port. To configure in-band management over multiple network elements, the user must connect the management service to the network by adding a service point on an interface that provides the required network connectivity.

Users can modify the attributes of the management service, but cannot delete it. The CPU service point is read-only and cannot be modified. The local management port is also connected to the service, but its service point is not visible to users. The management port is enabled by default and cannot be disabled.

The following figure illustrates a management service.

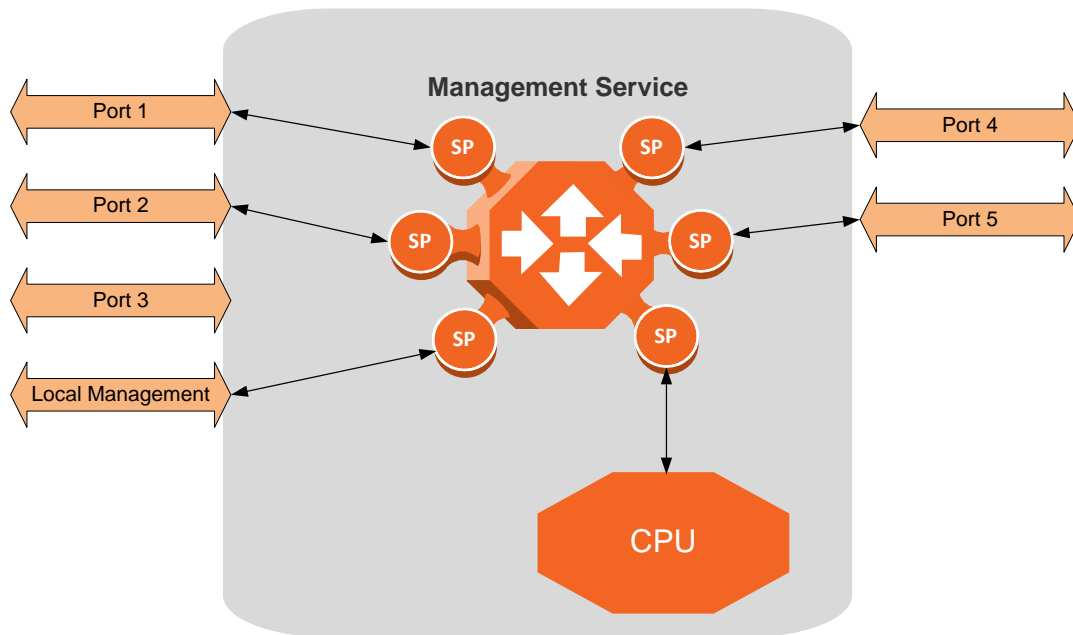


Figure 23: Management Service

Management services can provide building blocks for network services such as E-LAN EVCs (EP-LAN and EVP-LAN), as well as E-Line EVCs (EPL and EVPL EVCs) in which only two service points are active.

### Service Attributes

IP-50EX services have the following attributes:

- **Service ID** – A unique ID that identifies the service. The user must select the Service ID upon creating the service. The Service ID cannot be edited after the service has been created. Service ID 1025 is reserved for the pre-defined Management service.
- **Service Type** – Determines the specific functionality that will be provided for Ethernet traffic using the service. For example, a Point-to-Point service provides traffic forwarding between two service points, with no need to learn a service topology based on source and destination MAC addresses. A Multipoint service enables operators to create an E-LAN service that includes several service points.
- **Service Admin Mode** – Defines whether or not the service is functional, i.e., able to receive and transmit traffic. When the Service Admin Mode is set to Operational, the service is fully functional. When the Service Admin Mode is set to Reserved, the service occupies system resources but is unable to transmit and receive data.
- **EVC-ID** – The Ethernet Virtual Connection ID (end-to-end). This parameter does not affect the network element's behavior, but is used by the NMS for topology management.

- **EVC Description** – The Ethernet Virtual Connection description. This parameter does not affect the network element's behavior, but is used by the NMS for topology management.
- **Static MAC Address Configuration** – Users can add static entries to the MAC forwarding table. The global aging time does not apply to static entries, and they are not counted with respect to the Maximum Dynamic MAC Address Learning. It is the responsibility of the user not to use all the 32K entries in the table if the user also wants to utilize dynamic MAC address learning.
- **CoS Mode** – Defines whether the service inherits ingress classification decisions made at previous stages or overwrites previous decisions and uses the default CoS defined for the service. For more details on IP-50EX's hierarchical classification mechanism, refer to *Classification* on page 78.
- **Default CoS** – The default CoS value at the service level. If the CoS Mode is set to overwrite previous classification decisions, this is the CoS value used for frames entering the service.
- **xSTP Instance (0-46, 4095)** – The spanning tree instance ID to which the service belongs. The service can be a traffic engineering service (instance ID 4095) or can be managed by the xSTP engines of the network element.

#### 4.2.2.2 Service Points

Service points are logical entities attached to the interfaces that make up the service. Service points define the movement of frames through the service. Without service points, a service is simply a virtual bridge with no ingress or egress interfaces.

IP-50EX supports several types of service points:

- **Management (MNG) Service Point** – Only used for management services. The following figure shows a management service used for in-band management among four network elements in a ring. In this example, each service contains three MNG service points, two for East-West management connectivity in the ring, and one serving as the network gateway.

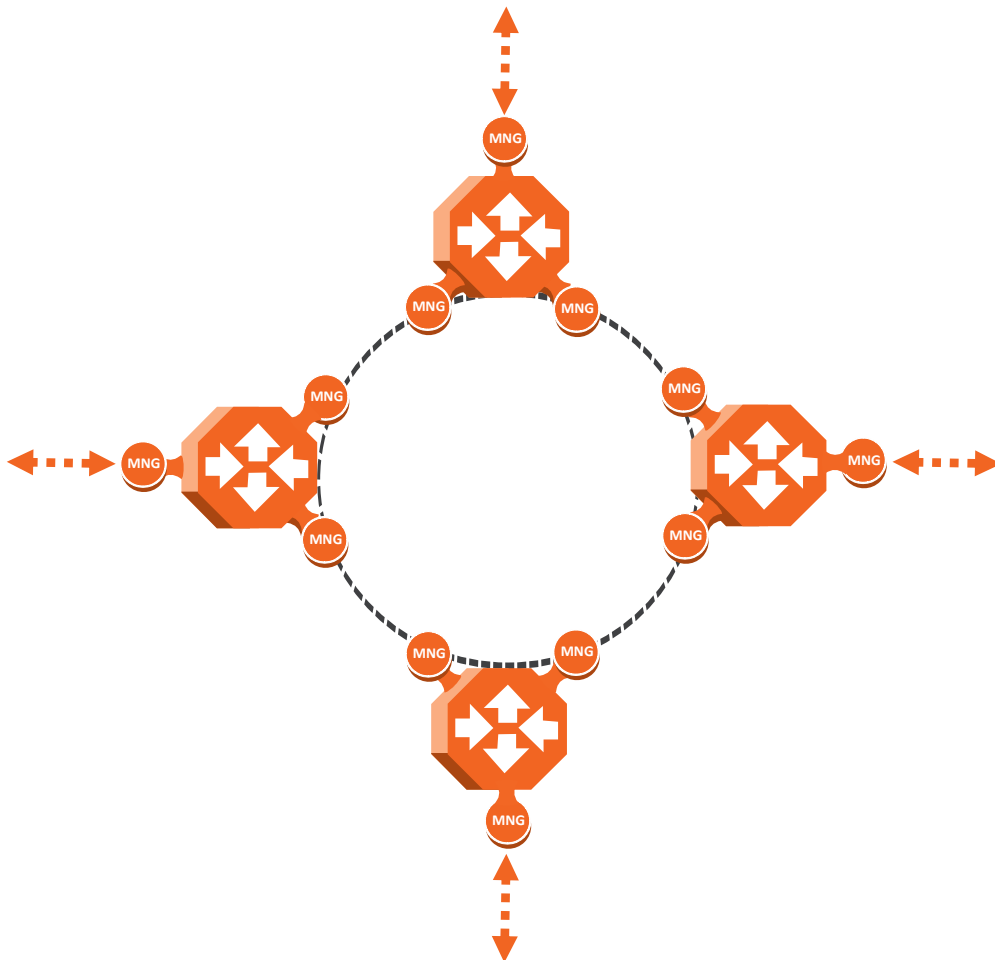


Figure 24: Management Service and its Service Points

- **Service Access Point (SAP) Service Point** – An SAP is equivalent to a UNI in MEF terminology and defines the connection of the user network with its access points. SAPs are used for Point-to-Point and Multipoint traffic services.

- **Service Network Point (SNP) Service Point** – An SNP is equivalent to an NNI or E-NNI in MEF terminology and defines the connection between the network elements in the user network. SNPs are used for Point-to-Point and Multipoint traffic services.

The following figure shows four network elements in ring. An MP Service with three service points provides the connectivity over the network. The SNPs provide the connectivity among the network elements in the user network while the SAPs provide the access points for the network.

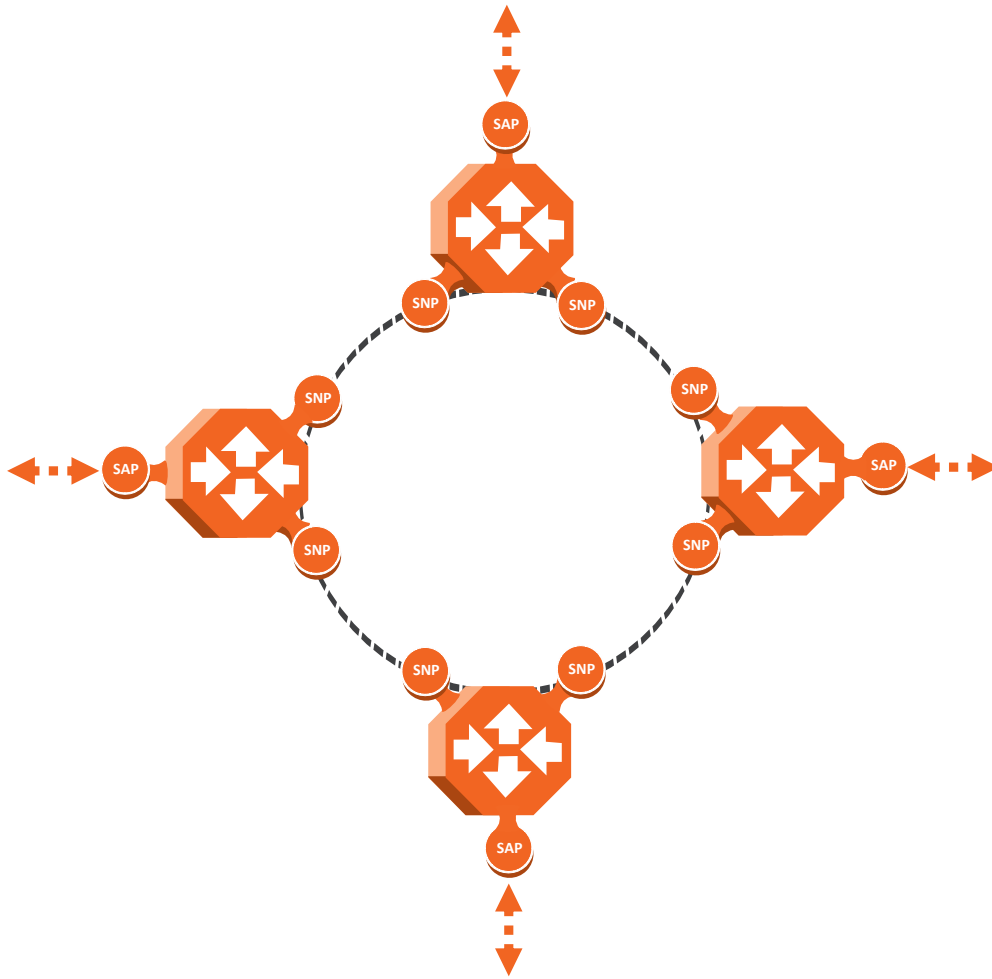


Figure 25: SAPs and SNPs

- **Pipe Service Point** – Used to create traffic connectivity between two points in a port-based manner. In other words, all the traffic from one port passes to the other port. Pipe service points are used in Point-to-Point services.

**Note:** Pipe service points can only be used in a service with other Pipe service points.

The following figure shows a Point-to-Point service with Pipe service points that create a service between Port 1 of the network element on the left and Port 2 of the network element on the right.



Figure 26: Pipe Service Points

The following figure shows the usage of SAP, SNP and Pipe service points in a microwave network. The SNPs are used for interconnection between the network elements while the SAPs provide the access points for the network. Pipe service points are also used, to provide connectivity between elements that require port-based connectivity.

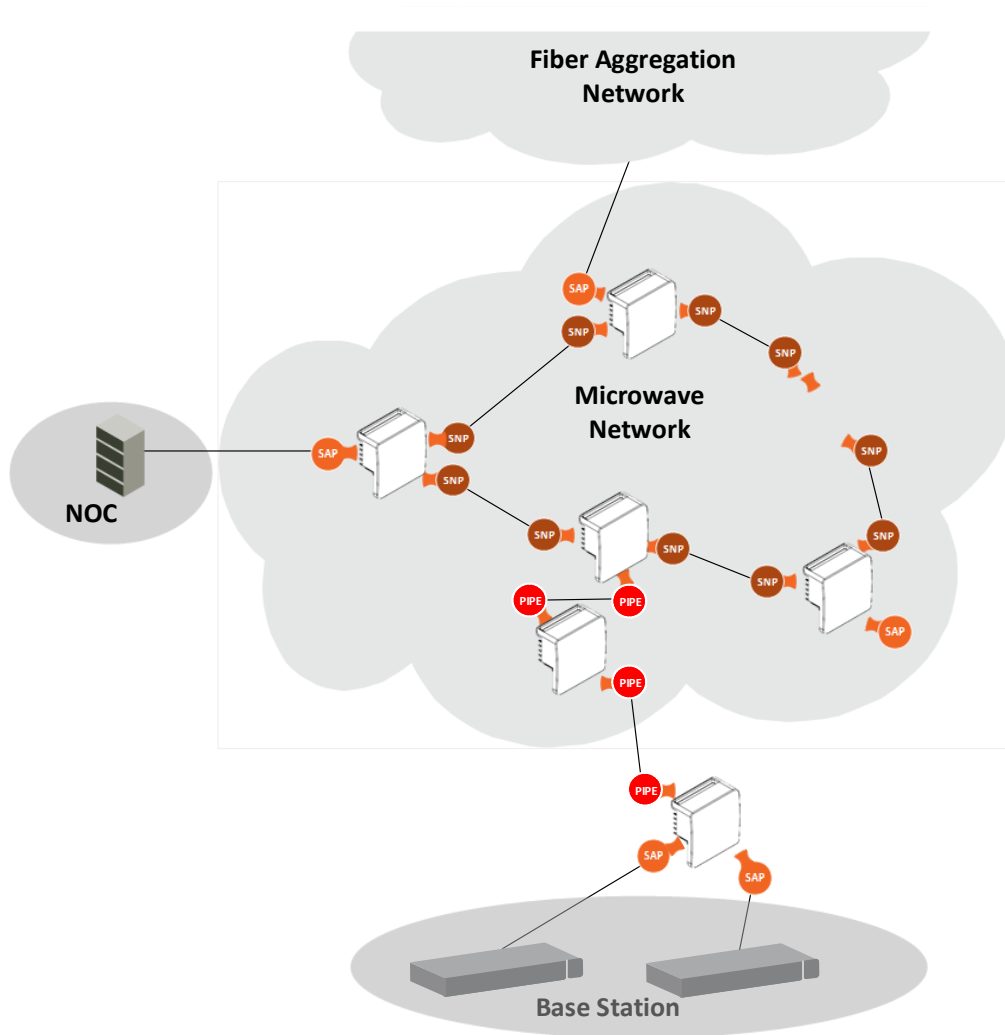


Figure 27: SAP, SNP and Pipe Service Points in a Microwave Network

The following table summarizes the service point types available per service type.

*Table 8: Service Point Types per Service Type*

		Service point type			
		MNG	SAP	SNP	Pipe
Service Type	Management	Yes	No	No	No
	Point-to-Point	No	Yes	Yes	Yes
	Multipoint	No	Yes	Yes	No

### Service Point Classification

As explained above, service points connect the service to the network element interfaces. It is crucial that the network element have a means to classify incoming frames to the proper service point. This classification process is implemented by means of a parsing encapsulation rule for the interface associated with the service point. This rule is called the Attached Interface Type, and is based on a three-part key consisting of:

- The Interface ID of the interface through which the frame entered.
- The frame's C-VLAN and/or S-VLAN tags.

The Attached Interface Type provides a definitive mapping of each arriving frame to a specific service point in a specific service. Since more than one service point may be associated with a single interface, frames are assigned to the earliest defined service point in case of conflict.

### SAP Classification

SAPs can be used with the following Attached Interface Types:

- **All to one** – All C-VLANs and untagged frames that enter the interface are classified to the same service point.
- **Dot1q** – A single C-VLAN is classified to the service point.
- **QinQ** – A single S-VLAN and C-VLAN combination is classified to the service point.
- **Bundle C-Tag** – A set of multiple C-VLANs are classified to the service point.
- **Bundle S-Tag** – A single S-VLAN and a set of multiple C-VLANs are classified to the service point.

### SNP Classification

SNPs can be used with the following Attached Interface Types:

- **Dot1q** – A single C VLAN is classified to the service point.
- **S-Tag** – A single S- VLAN is classified to the service point.

### PIPE Classification

Pipe service points can be used with the following Attached Interface Types:

- **Dot1q** – All C-VLANs and untagged frames that enter the interface are classified to the same service point.
- **S-Tag** – All S-VLANs and untagged frames that enter the interface are classified to the same service point.

### MNG classification

Management service points can be used with the following Attached Interface Types:

- **Dot1q** – A single C-VLAN is classified to the service point.
- **S-Tag** – A single S-VLAN is classified to the service point.
- **QinQ** – A single S-VLAN and C-VLAN combination is classified into the service point.

The following table shows which service point types can co-exist on the same interface.

*Table 9: Service Point Types that can Co-Exist on the Same Interface*

	MNG SP	SAP SP	SNP SP	Pipe SP
MNG SP	Only one MNG SP is allowed per interface.	Yes	Yes	Yes
SAP SP	Yes	Yes	No	No
SNP SP	Yes	No	Yes	No
PIPE SP	Yes	No	No	Only one Pipe SP is allowed per interface.

The following table shows in more detail which service point – Attached Interface Type combinations can co-exist on the same interface.

.



Table 10: Service Point Type-Attached Interface Type Combinations that can Co-Exist on the Same Interface

	SP Type	SAP				SNP			Pipe		MNG		
SP Type	Attached Interface Type	802.1q	Bundle C-Tag	Bundle S-Tag	All to One	QinQ	802.1q	S-Tag	802.1q	S-Tag	802.1q	QinQ	S-Tag
SAP	802.1q	Yes	Yes	No	No	No	No	No	Only for P2P Service	No	Yes	No	No
	Bundle C-Tag	Yes	Yes	No	No	No	No	No	Only for P2P Service	No	Yes	No	No
	Bundle S-Tag	No	No	Yes	No	Yes	No	No	No	No	No	Yes	No
	All to One	No	No	No	Only 1 All to One SP Per Interface	No	No	No	No	No	No	No	No
	QinQ	No	No	Yes	No	Yes	No	No	No	No	No	Yes	No
SNP	802.1q	No	No	No	No	No	Yes	No	Only for P2P Service	No	Yes	No	No
	S-Tag	No	No	No	No	No	No	Yes	No	Only for P2P Service	No	No	Yes
Pipe	802.1q	Only for P2P Service	Only for P2P Service	No	No	No	Only for P2P Service	No	Only one Pipe SP Per Interface	No	Yes	No	No
	S-Tag	No	No	No	No	No	No	Only for P2P Service	No	Only one Pipe SP Per Interface	No	No	Yes
MNG	802.1q	Yes	Yes	No	No	No	Yes	No	Yes	No	No	No	No
	QinQ	No	No	Yes	No	Yes	No	No	No	No	No	No	No
	S-Tag	No	No	No	No	No	No	Yes	No	Yes	No	No	No

### Service Point Attributes

As described above, traffic ingresses and egresses the service via service points. The service point attributes are divided into two types:

- **Ingress Attributes** – Define how frames are handled upon ingress, e.g., policing.
- **Egress Attributes** – Define how frames are handled upon egress, e.g., preservation of the ingress CoS value upon egress, VLAN swapping.

The following figure shows the ingress and egress path relationship on a point-to-point service path. When traffic arrives via port 1, the system handles it using service point 1 ingress attributes then forwards it to service point 2 and handles it using the SP2 egress attributes:

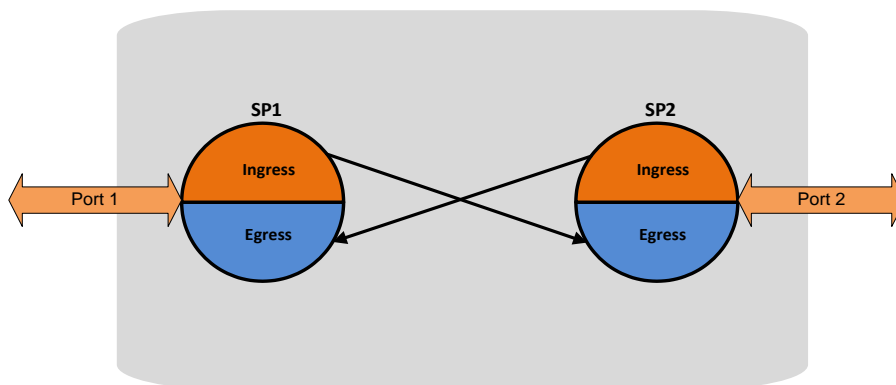


Figure 28: Service Path Relationship on Point-to-Point Service Path

Service points have the following attributes:

### General Service Point Attributes

- **Service Point ID** – Users can define up to 32 service points per service, except for management services which are limited to 30 service points in addition to the pre-defined management system service point.
- **Service Point Name** – A descriptive name, which can be up to 20 characters.
- **Service Point Type** – The type of service point, as described above.
- **S-VLAN Encapsulation** – The S-VLAN ID associated with the service point.
- **C-VLAN Encapsulation** – The C-VLAN ID associated with the service point.
- **Attached C VLAN** – For service points with an Attached Interface Type of Bundle C-Tag, this attribute is used to create a list of C-VLANs associated with the service point.
- **Attached S-VLAN** – For service points with an Attached Interface Type of Bundle S-Tag, this attribute is used to create a list of S-VLANs associated with the service point.

### Ingress Service Point Attributes

The ingress attributes are attributes that operate upon frames when they ingress via the service point.

- **Attached Interface Type** – The interface type to which the service point is attached, as described above. Permitted values depend on the service point type.
- **Learning Administration** – Enables or disables MAC address learning for traffic that ingresses via the service point. This option enables users to enable or disable MAC address learning for specific service points.
- **Allow Broadcast** – Determines whether to allow frames to ingress the service via the service point when the frame has a broadcast destination MAC address.
- **Allow Flooding** – Determines whether incoming frames with unknown MAC addresses are forwarded to other service points via flooding.
- **CoS Mode** – Determines whether the service point preserves the CoS decision made at the interface level, overwrites the CoS with the default CoS for the service point.
- **Default CoS** – The service point CoS. If the CoS Mode is set to overwrite the CoS decision made at the interface level, this is the CoS value assigned to frames that ingress the service point.

### Egress Service Point Attributes

The egress attributes are attributes that operate upon frames egressing via the service point.

- **C-VLAN ID Egress Preservation** – If enabled, C-VLAN frames egressing the service point retain the same C-VLAN ID they had when they entered the service.
- **C-VLAN CoS Egress Preservation** – If enabled, the C-VLAN CoS value of frames egressing the service point is the same as the value when the frame entered the service.
- **S-VLAN CoS Egress Preservation** – If enabled, the S-VLAN CoS value of frames egressing the service point is the same as the value when the frame entered the service.
- **Marking** – Marking refers to the ability to overwrite the outgoing priority bits and Color of the outer VLAN of the egress frame, either the C-VLAN or the S-VLAN. If marking is enabled, the service point overwrites the outgoing priority bits and Color of the outer VLAN of the egress frame. Marking mode is only relevant if either the outer frame is S-VLAN and S-VLAN CoS preservation is disabled, or the outer frame is C-VLAN and C-VLAN CoS preservation is disabled. When marking is enabled and active, marking is performed according to global mapping tables that map the 802.1p-UP bits to a defined CoS and Color value and maps Color values to the DEI or CFI bits.

### 4.2.3 Ethernet Interfaces

The IP-50EX switching fabric distinguishes between physical interfaces and logical interfaces. Physical and logical interfaces serve different purposes in the switching fabric.

The concept of a physical interface refers to the physical characteristics of the interface, such as speed, duplex, auto-negotiation, master/slave, and standard RMON statistics.

A logical interface can consist of a single physical interface or a group of physical interfaces that share the same function. Examples of the latter are protection groups and link aggregation groups. Switching and QoS functionality are implemented on the logical interface level.

It is important to understand that the IP-50EX switching fabric regards all traffic interfaces as regular physical interfaces, distinguished only by the media type the interface uses, e.g., RJ-45, SFP, or Radio.

From the user's point of view, the creation of the logical interface is simultaneous with the creation of the physical interface. For example, when the user enables a radio interface, both the physical and the logical radio interface come into being at the same time.

Once the interface is created, the user configures both the physical and the logical interface. In other words, the user configures the same interface on two levels, the physical level and the logical level.

The following figure shows physical and logical interfaces in a one-to-one relationship in which each physical interface is connected to a single logical interface, without grouping.

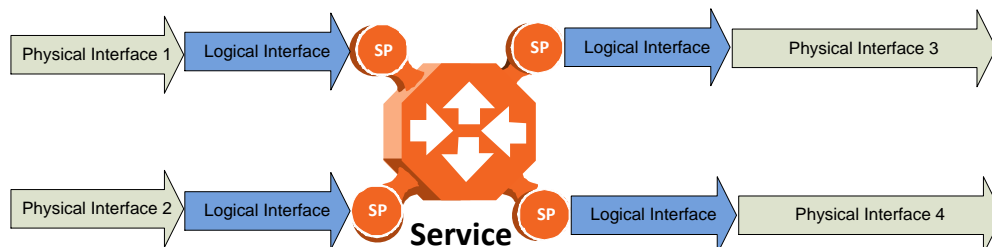


Figure 29: Physical and Logical Interfaces

**Note:** For simplicity only, this figure represents a uni-directional rather than a bi-directional traffic flow.

The next figure illustrates the grouping of two or more physical interfaces into a logical interface, a link aggregation group (LAG) in this example. The two physical interfaces on the ingress side send traffic into a single logical interface. The user configures each physical interface separately, and configures the logical interface as a single logical entity. For example, the user might configure each physical interface to 100 Mbps, full duplex, with auto-negotiation off. On the group level, the user might limit the group to a rate of 200 Mbps by configuring the rate meter on the logical interface level.

When physical interfaces are grouped into a logical interface, IP-50EX also shows standard RMON statistics for the logical interface, i.e., for the group. This information enables users to determine the cumulative statistics for the group, rather than having to examine the statistics for each interface individually.

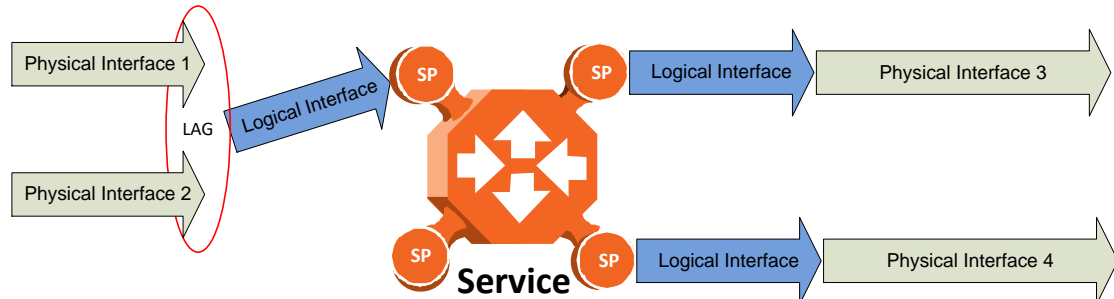


Figure 30: Grouped Interfaces as a Single Logical Interface on Ingress Side

**Note:** For simplicity only, this figure represents a uni-directional rather than a bi-directional traffic flow.

The following figure shows the logical interface at the egress side. In this case, the user can configure the egress traffic characteristics, such as scheduling, for the group as a whole as part of the logical interface attributes.



Figure 31: Grouped Interfaces as a Single Logical Interface on Egress Side

**Note:** For simplicity only, this figure represents a uni-directional rather than a bi-directional traffic flow.

#### 4.2.3.1 Physical Interfaces

The physical interfaces refer to the real traffic ports (Layer 1) that are connected to the network. The Media Type attribute defines the Layer 1 physical traffic interface type, which can be:

- Radio interface
- RJ-45 or SFP Ethernet interface.

#### Physical Interface Attributes

The following physical interface parameters can be configured by users:

- **Admin** – Enables or disables the physical interface. This attribute is set via the Interface Manager section of the Web EMS.
- **Auto Negotiation** – Enables or disables auto-negotiation on the physical interface. Auto Negotiation is always off for radio and SFP interfaces.
- **Speed and Duplex** – The physical interface speed and duplex mode. Permitted values are:
  - **Ethernet RJ-45 Management interface:** 100Mbps and 1000Mbps FD.
  - **Ethernet SFP28 interfaces:** 1G, 10G and 25G
  - **Ethernet QSFP interface:** 1G and 10G
  - **Radio interfaces:** The parameter is read-only and set by the system to 10G FD.
- **Flow Control** – The physical port flow control capability. Permitted values are: Symmetrical Pause and/or Asymmetrical Pause. This parameter is only relevant in Full Duplex mode.
- **IFG** – The physical port Inter-frame gap. Although users can modify the IFG field length, it is strongly recommended not to modify the default value of 12 bytes without a thorough understanding of how the modification will impact traffic. Permitted values are 6 to 15 bytes.
- **Preamble** – The physical port preamble value. Although users can modify the preamble field length, it is strongly recommended not to modify the default values of 8 bytes without a thorough understanding of how the modification will impact traffic. Permitted values are 6 to 15 bytes.
- **Interface description** – A text description of the interface, up to 40 characters.

The following read-only physical interface status parameters can be viewed by users:

- **Operational State** – The operational state of the physical interface (Up or Down).
- **Actual Speed and Duplex** – The actual speed and duplex value for the Ethernet link as agreed by the two sides of the link after the auto negotiation process.
- **Actual Flow Control State** – The actual flow control state values for the Ethernet link as agreed by the two sides after the auto negotiation process.
- **Actual Physical Mode** (only relevant for RJ-45 interfaces) – The actual physical mode (master or slave) for the Ethernet link, as agreed by the two sides after the auto negotiation process.

### Ethernet Statistics

The IP-50EX platform stores and displays statistics in accordance with RMON and RMON2 standards.

Users can display various peak TX and RX rates (in seconds) and average TX and RX rates (in seconds), both in bytes and in packets, for each measured time interval. Users can also display the number of seconds in the interval during which TX and RX rates exceeded the configured threshold.

The following transmit statistic counters are available:

- Transmitted bytes (not including preamble) in good or bad frames. Low 32 bits.
- Transmitted bytes (not including preamble) in good or bad frames. High 32 bits.
- Transmitted frames (good or bad)
- Multicast frames (good only)
- Broadcast frames (good only)
- Pause control and PFC frames transmitted
- Oversized frames – frames with length from 1518 bytes (1522 bytes for VLAN-tagged frames) up to the maximum configured frame size, without errors
- Frames with length 64 bytes, good or bad
- Frames with length 65-127 bytes, good or bad
- Frames with length 128-255 bytes, good or bad
- Frames with length 256-511 bytes, good or bad
- Frames with length 512-1023 bytes, good or bad.
- Frames with length 1024-1518 bytes, good or bad

The following receive statistic counters are available:

- Received bytes (not including preamble) in good or bad frames. Low 32 bits.
- Received bytes (not including preamble) in good or bad frames. High 32 bits.
- Received frames (good or bad)
- Multicast frames (good only)
- Broadcast frames (good only)
- Pause control and PFC frames received
- FCS error frames
- Oversized frames – frames with length up to the maximum configured frame size, without errors
- Undersized frames (good only)
- Fragments frames (undersized bad)
- Frames with length 64 bytes, good or bad
- Frames with length 65-127 bytes, good or bad
- Frames with length 128-255 bytes, good or bad
- Frames with length 256-511 bytes, good or bad
- Frames with length 512-1023 bytes, good or bad

- Frames with length 1024-1518 bytes, good or bad

#### 4.2.3.2 Logical Interfaces

A logical interface consists of one or more physical interfaces that share the same traffic ingress and egress characteristics. From the user's point of view, it is more convenient to define interface behavior for the group as a whole than for each individual physical interface that makes up the group. Therefore, classification, QoS, and resiliency attributes are configured and implemented on the logical interface level, in contrast to attributes such as interface speed and duplex mode, which are configured on the physical interface level.

It is important to understand that the user relates to logical interfaces in the same way in both a one-to-one scenario in which a single physical interface corresponds to a single logical interface, and a grouping scenario such as a link aggregation group or a protection group, in which several physical interfaces correspond to a single logical interface.

The following figure illustrates the relationship of a LAG group to the switching fabric. From the point of view of the user configuring the logical interface attributes, the fact that there are two Ethernet interfaces is not relevant. The user configures and manages the logical interface just as if it represented a single Ethernet interface.

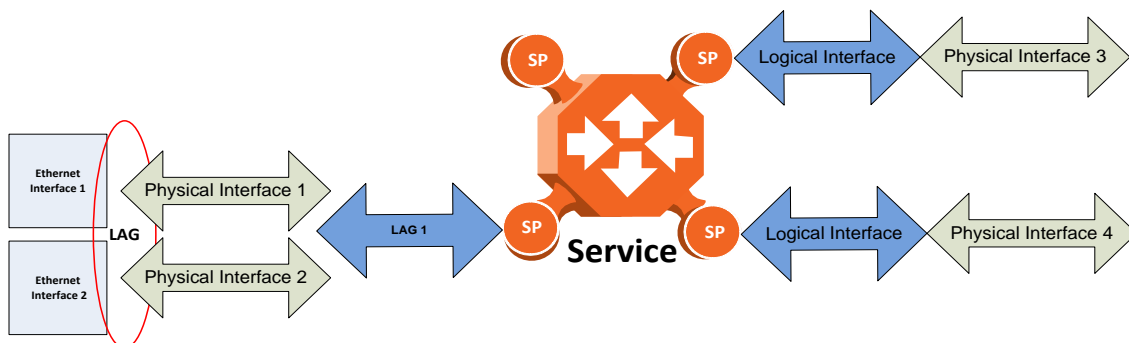


Figure 32: Relationship of Logical Interfaces to the Switching Fabric

#### Logical Interface Attributes

The following logical interface attributes can be configured by users:

##### General Attributes

- **Traffic Flow Administration** – Enables traffic via the logical interface. This attribute is useful when the user groups several physical interfaces into a single logical interface. The user can enable or disable traffic to the group using this parameter.

##### Ingress Path Classification at Logical Interface Level

These attributes represent part of the hierarchical classification mechanism, in which the logical interface is the lowest point in the hierarchy.



- **MPLS Trust Mode** – When this attribute is set to Trust mode and the arriving packet has MPLS EXP priority bits, the interface performs QoS and Color classification according to a user-configurable MPLS EXP bit to CoS and Color classification table.
- **DSCP Trust Mode** – When this attribute is set to Trust mode and the arriving packet has DSCP priority bits, the interface performs QoS and Color classification according to a user-configurable DSCP bit to CoS and Color classification table. If MPLS EXP priority bits are present, DSCP is not considered regardless of the Trust mode setting and regardless of whether an MPLS match was found.
- **802.1p Trust Mode** – When this attribute is set to Trust mode and the arriving packet is 802.1Q or 802.1AD, the interface performs QoS and Color classification according to user-configurable tables for 802.1q UP bit (C-VLAN frames) or 802.1AD UP bit (S-VLAN frames) to CoS and Color classification. MPLS and DSCP classification have priority over 802.1p Trust Mode, so that if a match is found on the MPLS or DSCP level, 802.1p bits are not considered.
- **Default CoS** – The default CoS value for frames passing through the interface. This value can be overwritten on the service point and service level. The Color is assumed to be Green.

For more information about classification at the logical interface level, refer to *Logical Interface-Level Classification* on page 79.

#### Ingress Path Rate Meters at Logical Interface Level

- **Unicast Traffic Rate Meter Admin** – Enables or disables the unicast rate meter (policer) on the logical interface.
- **Unicast Traffic Rate Meter Profile** – Associates the rate meter (policer) with a specific rate meter (policer) profile.
- **Multicast Traffic Rate Meter Admin** – Enables or disables the multicast rate meter (policer) on the logical interface.
- **Multicast Traffic Rate Meter Profile** – Associates the rate meter (policer) with a specific rate meter (policer) profile.
- **Broadcast Traffic Rate Meter Admin** – Enables or disables the broadcast rate meter (policer) on the logical interface.
- **Broadcast Traffic Rate Meter Profile** – Associates the rate meter (policer)

The following read-only logical interface status parameters can be viewed by users:

- **Traffic Flow Operational Status** – Indicates whether or not the logical interface is currently functional.

#### Logical Interface Statistics

##### RMON Statistics at Logical Interface Level

As discussed in *Ethernet Statistics* on page 71, if the logical interface represents a group, such as a LAG, the IP-50EX platform stores and displays RMON and RMON2 statistics for the logical interface.

### Ingress Frame and Byte per Color Statistics at Logical Interface Level

Users can display the number of frames and bytes ingressing the logical interface per color, in granularity of 64 bits:

- Green Frames
- Green Bytes
- Yellow Frames
- Yellow Bytes
- Red Frames
- Red Bytes

### Link Aggregation Groups (LAG) and LACP

**Note:** LACP is planned for future release.

Link aggregation (LAG) enables users to group several physical interfaces into a single logical interface bound to a single MAC address. This logical interface is known as a LAG group. Traffic sent to the interfaces in a LAG group is distributed by means of a load balancing function.

IP-50EX uses an automated distribution function to generate the most efficient distribution among the LAG physical ports. The LAG distribution function uses the following parameters:

- Ethernet
  - MAC – DA and SA. Not taken into account if at least one MPLS label is present
- MPLS
  - For multiple MPLS labels, only the first three labels are considered
  - Not all bits of the MPLS label trigger the distribution function. Bits 5, 6, 7, and 17-20 do not trigger the distribution function.
- IPv4
  - DA and SA, if up to three MPLS labels are defined
- IPv6
  - DA bytes 1-5 and 7-16 and SA bytes 1-16 if up to three MLPS labels are defined
  - Flow label triggers the distribution function
- UDP and TCP
  - Destination Port and Source Port if up to three MLPS labels are defined

LAG can be used to provide redundancy for Ethernet interfaces, both on the same IP-50EX unit (line protection) and on separate units (line protection and equipment protection).

LAG can also be used to aggregate several interfaces in order to create a wider (aggregate) Ethernet link. For example, LAG can be used to create a 3 Gbps channel by grouping the three Ethernet interfaces to a single LAG.

A LAG group can be configured to be automatically closed in the event of LAG degradation. This option is used if the customer wants traffic from the switch to be re-routed during such time as the link is providing less than a certain capacity. When enabled, the LAG is automatically closed in the event that any one or more ports in the LAG fail. When all ports in the LAG are again operational, the LAG is automatically re-opened.

Up to four LAG groups can be created.

Link Aggregation Control Protocol (LACP) expands the capabilities of static LAG, and provides interoperability with third-party equipment that uses LACP. LACP improves the communication between LAG members. This improves error detection capabilities in situations such as improper LAG configuration or improper cabling. It also enables the LAG to detect uni-directional failure and remove the link from the LAG, preventing packet loss.

IP-50EX's LACP implementation does not include write parameters or churn detection.

<b>Note:</b>	LACP can only be used with Ethernet interfaces. LACP cannot be used with the LAG Group Shutdown in Case of Degradation Event feature.
--------------	--

Optionally, Multi-Homing can be enabled on a LAG group. When Multi-Homing is enabled:

- If ETH-BN (Ethernet Bandwidth Notification) is enabled on one of the interfaces in the LAG, BNM messages with current radio bandwidth are sent simultaneously on all of the LAG members.
- If ASP Management Safe Mode is enabled on one of the interfaces in the LAG, CSF messages are sent simultaneously on all of the LAG members.

An additional option to support Multi-Homing is Multi-Active. This option is only available when Multi-Homing is configured, and is primarily used when the LAG is a Control interface for ETH-BN in configurations where the device is receiving traffic from devices in a static MLAG active-active multi-homing configuration. Multi-Active enables the device to support load balancing when the LAG is receiving traffic from two active routers.

When Multi-Active is enabled, the radio bandwidth reported in the BNM packets is divided by the number of active LAG members.

LAG groups can include interfaces with the following constraints:

- Only physical interfaces, not logical interfaces, can belong to a LAG group.
- It is recommended not to include radio interfaces in a LAG group.
- Interfaces can only be added to the LAG group if no services or service points are attached to the interface.
- Any classification rules defined for the interface are overridden by the classification rules defined for the LAG group.
- When removing an interface from a LAG group, the removed interface is assigned the default interface values.

IP-50EX enables users to select the LAG members without limitations, such as interface speed and interface type. Proper configuration of a LAG group is the responsibility of the user.

#### 4.2.4 Quality of Service (QoS)

##### Related topics:

- Ethernet Service Model
- In-Band Management

Quality of Service (QoS) deals with the way frames are handled within the switching fabric. QoS is required in order to deal with many different network scenarios, such as traffic congestion, packet availability, and delay restrictions.

IP-50EX's personalized QoS enables operators to handle a wide and diverse range of scenarios. IP-50EX's smart QoS mechanism operates from the frame's ingress into the switching fabric until the moment the frame egresses via the destination port.

QoS capability is very important due to the diverse topologies that exist in today's network scenarios. These can include, for example, streams from two different ports that egress via single port, or a port-to-port connection that holds hundreds of services. In each topology, a customized approach to handling QoS will provide the best results.

The figure below shows the basic flow of IP-50EX's QoS mechanism. Traffic ingresses (left to right) via the Ethernet or radio interfaces, on the "ingress path." Based on the services model, the system determines how to route the traffic. Traffic is then directed to the most appropriate output queue via the "egress path."

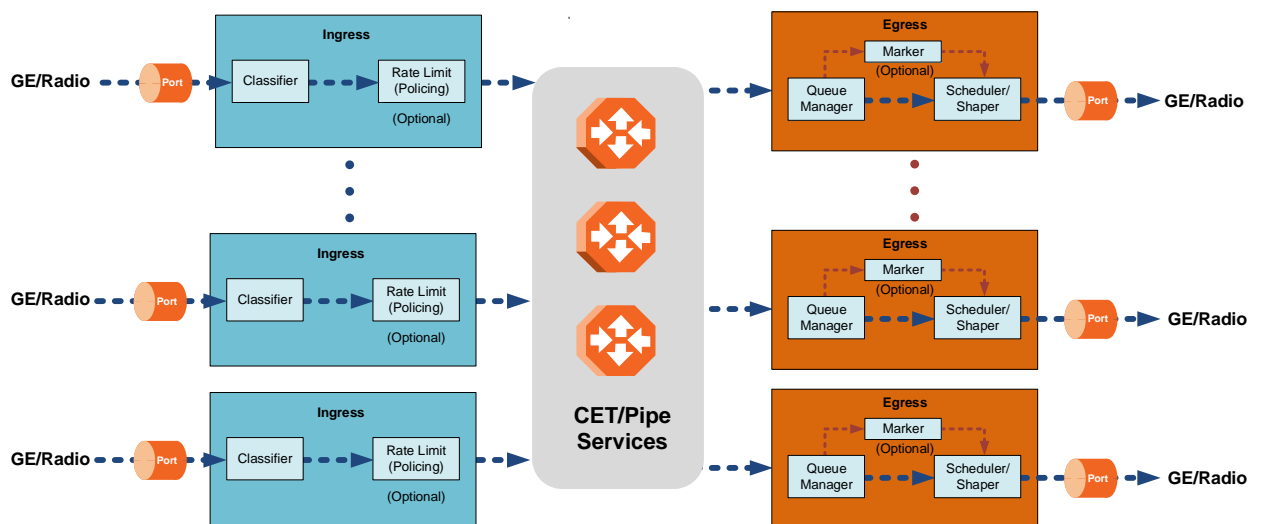


Figure 33: QoS Block Diagram

The ingress path consists of the following QoS building blocks:

- **Ingress Classifier** – A hierarchical mechanism that deals with ingress traffic on three different levels: interface, service point, and service. The classifier determines the exact traffic stream and associates it with the appropriate service. It also calculates an ingress frame CoS and Color. CoS and Color classification can be performed on three levels, according to the user's configuration.
- **Ingress Rate Metering** – A hierarchical mechanism that deals with ingress traffic on the interface and service point levels. The rate metering mechanism enables the system to measure the incoming frame rate on different levels using a TrTCM standard MEF rate meter, and to determine whether to modify the color calculated during the classification stage.

The egress path consists of the following QoS building blocks:

- **Queue Manager** – This is the mechanism responsible for managing the transmission queues, utilizing smart WRED per queue and per packet color (Green or Yellow).
- **Scheduling and Shaping** – A hierarchical mechanism that is responsible for scheduling the transmission of frames from the transmission queues, based on priority among queues, Weighted Fair Queuing (WFQ) in bytes per each transmission queue, and eligibility to transmit based on required shaping on several different levels (per queue and per port).
- **Marker** – This mechanism provides the ability to modify priority bits in frames based on the calculated CoS and Color.

Eight transmission queues are provided per port.

#### 4.2.4.1 QoS on the Ingress Path

##### Classification

IP-50EX supports a hierarchical classification mechanism. The classification mechanism examines incoming frames and determines their CoS and Color. The benefit of hierarchical classification is that it provides the ability to “zoom in” or “zoom out”, enabling classification at higher or lower levels of the hierarchy. The nature of each traffic stream defines which level of the hierarchical classifier to apply, or whether to use several levels of the classification hierarchy in parallel.

The hierarchical classifier consists of the following levels:

- Logical interface-level classification
- Service point-level classification
- Service level classification

The following figure illustrates the hierarchical classification model. In this figure, traffic enters the system via the port depicted on the left and enters the service via the SAP depicted on the upper left of the service. The classification can take place at the logical interface level, the service point level, and/or the service level.

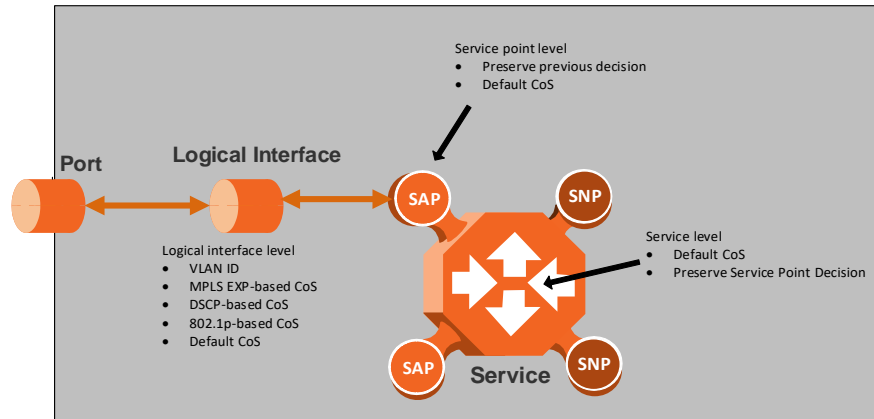


Figure 34: Hierarchical Classification

#### Logical Interface-Level Classification

Logical interface-level classification enables users to configure classification on a single interface or on a number of interfaces grouped together, such as a LAG group.

The classifier at the logical interface level supports the following classification methods, listed from highest to lowest priority. A higher level classification method supersedes a lower level classification method:

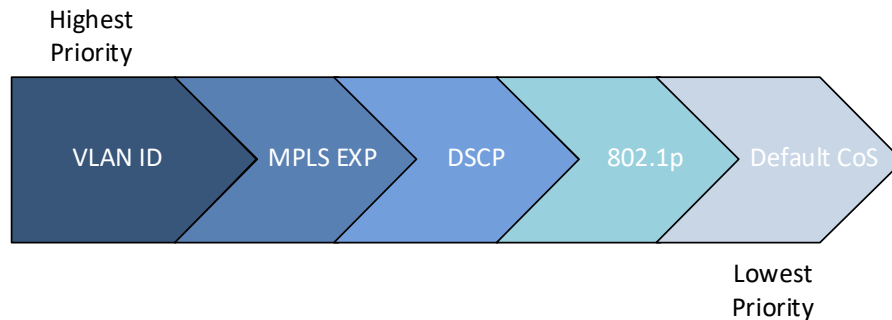
- Service
- Service Point
- VLAN ID
- 802.1p bits
- MPLS EXP field.
- DSCP bits (only considered if MPLS is not present, regardless of trust setting)
- Default CoS

IP-50EX performs the classification on each frame ingressing the system via the logical interface. Classification is performed step by step from the highest priority to the lowest priority classification method. Once a match is found, the classifier determines the CoS and Color decision for the frame for the logical interface-level.

Users can disable some of these classification methods by configuring them as un-trusted. For example, if MPLS classification is configured as un-trusted for a specific interface, the classification mechanism does not perform classification according to the MPLS EXP bits. This is useful, for example, if the required classification is based on 802.1p bits.

If no match is found at the logical interface level, the default CoS is applied to incoming frames at this level. In this case, the Color of the frame is assumed to be Green.

The following figure illustrates the hierarchy of priorities among classification methods, from highest (on the left) to lowest (on the right) priority.



*Figure 35: Classification Method Priorities*

Interface-level classification is configured as part of the logical interface configuration. For details, refer to *Ingress Path Classification at Logical Interface Level* on page 72.

The following tables show the default values for logical interface-level classification. The key values for these tables are the priority bits of the respective frame encapsulation layers (VLAN, IP, and MPLS), while the key results are the CoS and Colors calculated for incoming frames. These results are user-configurable, but it is recommended that only advanced users should modify the default values.

*Table 11: MPLS EXP Default Mapping to CoS and Color*

MPLS EXP bits	CoS (configurable)	Color (configurable)
0	0	Yellow
1	1	Green
2	2	Yellow
3	3	Green
4	4	Yellow
5	5	Green
6	6	Green
7	7	Green

*Table 12: DSCP Default Mapping to CoS and Color*

DSCP	DSCP (bin)	Description	CoS (Configurable)	Color (Configurable)
0 (default)	000000	BE (CS0)	0	Green
10	001010	AF11	1	Green
12	001100	AF12	1	Yellow



DSCP	DSCP (bin)	Description	CoS (Configurable)	Color (Configurable)
14	001110	AF13	1	Yellow
18	010010	AF21	2	Green
20	010100	AF22	2	Yellow
22	010110	AF23	2	Yellow
26	011010	AF31	3	Green
28	011100	AF32	3	Yellow
30	011110	AF33	3	Yellow
34	100010	AF41	4	Green
36	100100	AF42	4	Yellow
38	100110	AF43	4	Yellow
46	101110	EF	7	Green
8	001000	CS1	1	Green
16	010000	CS2	2	Green
24	011000	CS3	3	Green
32	100000	CS4	4	Green
40	101000	CS5	5	Green
48	110000	CS6	6	Green
51	110011	DSCP_51	6	Green
52	110100	DSCP_52	6	Green
54	110110	DSCP_54	6	Green
56	111000	CS7	7	Green

Default value is CoS equal best effort and Color equal Green.

For the DSCP mapping table, users can modify not only the CoS and Color per entry, but also the Description. In addition, users can delete and add entries to the table, up to a maximum of 64 entries.

*Table 13: C-VLAN 802.1 UP and CFI Default Mapping to CoS and Color*

802.1 UP	CFI	CoS (configurable)	Color (configurable)
0	0	0	Green
0	1	0	Yellow
1	0	1	Green
1	1	1	Yellow
2	0	2	Green

802.1 UP	CFI	CoS (configurable)	Color (configurable)
2	1	2	Yellow
3	0	3	Green
3	1	3	Yellow
4	0	4	Green
4	1	4	Yellow
5	0	5	Green
5	1	5	Yellow
6	0	6	Green
6	1	6	Yellow
7	0	7	Green
7	1	7	Yellow

*Table 14: S-VLAN 802.1 UP and DEI Default Mapping to CoS and Color*

802.1 UP	DEI	CoS (Configurable)	Color (Configurable)
0	0	0	Green
0	1	0	Yellow
1	0	1	Green
1	1	1	Yellow
2	0	2	Green
2	1	2	Yellow
3	0	3	Green
3	1	3	Yellow
4	0	4	Green
4	1	4	Yellow
5	0	5	Green
5	1	5	Yellow
6	0	6	Green
6	1	6	Yellow
7	0	7	Green
7	1	7	Yellow

### Service Point-Level Classification

Classification at the service point level enables users to give special treatment, in higher resolution, to specific traffic flows using a single interface to which the service point is attached. The following classification modes are supported at the service point level. Users can configure these modes by means of the service point CoS mode.

- Preserve previous CoS decision (logical interface level)
- Default service point CoS

If the service point CoS mode is configured to preserve previous CoS decision, the CoS and Color are taken from the classification decision at the logical interface level. If the service point CoS mode is configured to default service point CoS mode, the CoS is taken from the service point's default CoS, and the Color is Green.

### Service-Level Classification

Classification at the service level enables users to provide special treatment to an entire service. For example, the user might decide that all frames in a management service should be assigned a specific CoS regardless of the ingress port. The following classification modes are supported at the service level:

- Preserve previous CoS decision (service point level)
- Default CoS

If the service CoS mode is configured to preserve previous CoS decision, frames passing through the service are given the CoS and Color that was assigned at the service point level. If the service CoS mode is configured to default CoS mode, the CoS is taken from the service's default CoS, and the Color is Green.

### Rate Meter (Policing)

IP-50EX's TrTCM rate meter mechanism complies with MEF 10.2, and is based on a dual leaky bucket mechanism. The TrTCM rate meter can change a frame's CoS settings based on CIR/EIR+CBS/EBS, which makes the rate meter mechanism a key tool for implementing bandwidth profiles and enabling operators to meet strict SLA requirements.

The IP-50EX hierarchical rate metering mechanism is part of the QoS performed on the ingress path, and consists of the following levels:

- Logical interface-level rate meter
- Service point-level rate meter

MEF 10.2 is the de-facto standard for SLA definitions, and IP-50EX's QoS implementation provides the granularity necessary to implement service-oriented solutions.

Hierarchical rate metering enables users to define rate meter policing for incoming traffic at any resolution point, from the interface level to the service point level.

Another important function of rate metering is to protect resources in the network element from malicious users sending traffic at an unexpectedly high rate. To prevent this, the rate meter can cut off traffic from a user that passes the expected ingress rate.

TrTCM rate meters use a leaky bucket mechanism to determine whether frames are marked Green, Yellow, or Red. Frames within the Committed Information Rate (CIR) or Committed Burst Size (CBS) are marked Green. Frames within the Excess Information Rate (EIR) or Excess Burst Size (EBS) are marked Yellow. Frames that do not fall within the CIR/CBS+EIR/EBS are marked Red and dropped, without being sent any further.

IP-50EX provides up to 1024 user-defined TrTCM rate meters. The rate meters implement a bandwidth profile, based on CIR/EIR, CBS/EBS, Color Mode (CM), and Coupling flag (CF). Up to 250 different profiles can be configured.

Ingress rate meters operate at the following levels:

- Logical Interface – Per Frame Type (unicast, multicast, and broadcast)
- Per Service Point

Users can attach and activate a rate meter profile at the logical interface level and on a service point level. Users must create the profile first, then attach it to the interface or service point.

#### Global Rate Meter Profiles

Users can define up to 250 rate meter user profiles. The following parameters can be defined for each profile:

- **Committed Information Rate (CIR)** – Frames within the defined CIR are marked Green and passed through the QoS module. Frames that exceed the CIR rate are marked Yellow. The CIR defines the average rate in bits/s of Service Frames up to which the network delivers service frames and meets the performance objectives. Permitted values are 0 to 25 Gbps.
- **Committed Burst Size (CBS)** – Frames within the defined CBS are marked Green and passed through the QoS module. This limits the maximum number of bytes available for a burst of service frames in order to ensure that traffic conforms to the CIR. Permitted values are 0 to 8192 Kbytes.
- **Excess Information Rate (EIR)** – Frames within the defined EIR are marked Yellow and processed according to network availability. Frames beyond the combined CIR and EIR are marked Red and dropped by the policer. Permitted values are 0 to 25 Gbps.
- **Excess Burst Size (EBS)** – Frames within the defined EBS are marked Yellow and processed according to network availability. Frames beyond the combined CBS and EBS are marked Red and dropped by the policer. Permitted values are 0 to 8192 Kbytes.

- **Color Mode** – Color mode can be enabled (Color aware) or disabled (Color blind). In Color aware mode, all frames that ingress with a CFI/DEI field set to 1 (Yellow) are treated as EIR frames, even if credits remain in the CIR bucket. In Color blind mode, all ingress frames are treated first as Green frames regardless of CFI/DEI value, then as Yellow frames (when there is no credit in the Green bucket). A Color-blind policer discards any previous Color decisions.
- **Coupling Flag** – If the coupling flag between the Green and Yellow buckets is enabled, then if the Green bucket reaches the maximum CBS value the remaining credits are sent to the Yellow bucket up to the maximum value of the Yellow bucket.

### Ingress Statistics

Users can display the following statistics counters for ingress frames and bytes per interface and per service point:

- Green Frames (64 bits)
- Green Bytes (64 bits)
- Yellow Frames (64 bits)
- Yellow Bytes (64 bits)
- Red Frames (64 bits)
- Red Bytes (64 bits)

Service point statistics can be displayed for the service point in general or for specific CoS queues on the service point.

#### 4.2.4.2 QoS on the Egress Path

##### Queue Manager

The queue manager (QM) is responsible for managing the output transmission queues. IP-50EX supports eight transmission queues per interface.

Users can configure burst size as a tradeoff between latency and immunity to bursts, according the application requirements.

The queues are ordered in groups of eight queues. These eight queues correspond to CoS values, from 0 to 7; in other words, eight priority queues.

Before assigning traffic to the appropriate queue, the system makes a determination whether to forward or drop the traffic using a WRED algorithm with a predefined green and yellow curve for the desired queue. This operation is integrated with the queue occupancy level.

The queue size is defined by the WRED profile that is associated with the queue. For more details, refer to *WRED* on page 85.

##### WRED

The Weighted Random Early Detection (WRED) mechanism can increase capacity utilization of TCP traffic by eliminating the phenomenon of global synchronization. Global synchronization occurs when TCP flows sharing bottleneck conditions

receive loss indications at around the same time. This can result in periods during which link bandwidth utilization drops significantly as a consequence of simultaneous falling to a “slow start” of all the TCP flows. The following figure demonstrates the behavior of two TCP flows over time without WRED.

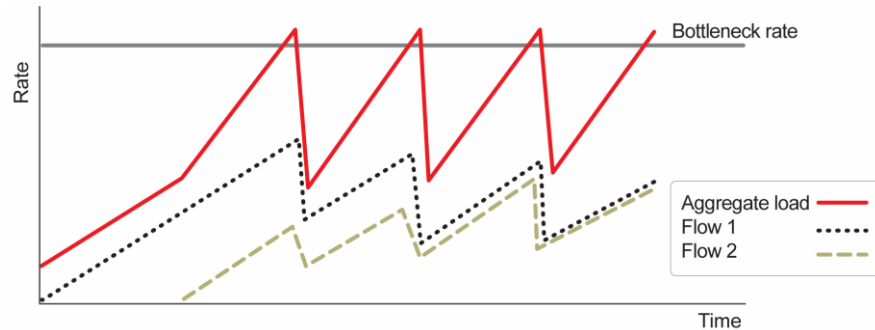


Figure 36: Synchronized Packet Loss

WRED eliminates the occurrence of traffic congestion peaks by restraining the transmission rate of the TCP flows. Each queue occupancy level is monitored by the WRED mechanism and randomly selected frames are dropped before the queue becomes overcrowded. Each TCP flow recognizes a frame loss and restrains its transmission rate (basically by reducing the window size). Since the frames are dropped randomly, statistically each time another flow has to restrain its transmission rate as a result of frame loss (before the real congestion occurs). In this way, the overall aggregated load on the radio link remains stable while the transmission rate of each individual flow continues to fluctuate similarly. The following figure demonstrates the transmission rate of two TCP flows and the aggregated load over time when WRED is enabled.

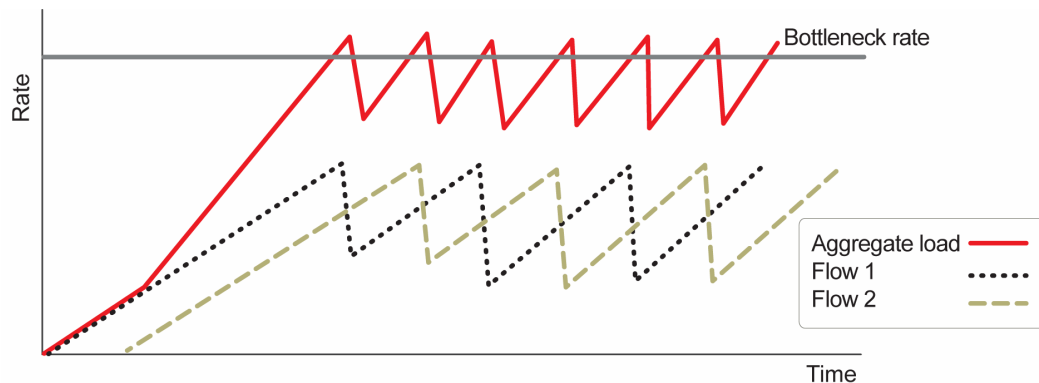


Figure 37: Random Packet Loss with Increased Capacity Utilization Using WRED

When queue occupancy goes up, this means that the ingress path rate (the TCP stream that is ingressing the switch) is higher than the egress path rate. This difference in rates should be fixed in order to reduce packet drops and to reach the maximal media utilization, since IP-50EX will not egress packets to the media at a rate which is higher than the media is able to transmit.

To deal with this, IP-50EX enables users to define up to 14 WRED profiles. Each profile contains a Green traffic curve and a Yellow traffic curve. These curves

describe the probability of randomly dropping frames as a function of queue occupancy. In addition, using different curves for Yellow packets and Green packets enables users to enforce the rule that Yellow packets be dropped before Green packets when there is congestion.

IP-50EX also includes two pre-defined read-only WRED profiles:

- Profile number 31 defines a tail-drop curve and is configured with the following values:
  - 100% Yellow traffic drop after 64kbytes occupancy.
  - 100% Green traffic drop after 128kbytes occupancy.
- Profile number 32 defines a profile in which all will be dropped. It is for internal use and should not be applied to traffic.

A WRED profile can be assigned to each queue. The WRED profile assigned to the queue determines whether or not to drop incoming packets according to the occupancy of the queue. Basically, as queue occupancy grows, the probability of dropping each incoming frame increases as well. As a consequence, statistically more TCP flows will be restrained before traffic congestion occurs.

The following figure provides an example of a WRED profile.

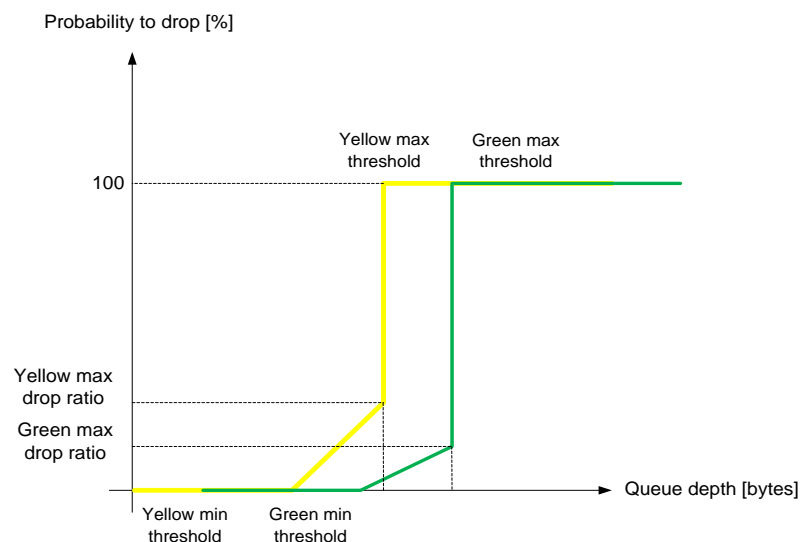


Figure 38: WRED Profile Curve

**Note:** The tail-drop profile, Profile 31, is the default profile for each queue. A tail drop curve is useful for reducing the effective queue size, such as when low latency must be guaranteed.

With respect to queue size, note the following:

- All memory is shared among all the queues
- There is no guaranteed minimum queue size
- The default maximum queue size is 128 KB (set by the default WRED profile)
- The maximum queue size can be 1.25 MB (regardless of the WRED setting)
- The maximum queue size is not guaranteed and depends on the traffic load

## Shaping on the Egress Path

Egress shaping determines the traffic profile for each queue. IP-50EX performs single leaky bucket egress shaping on the queue level.

### Queue Shapers

Users can configure up to 31 single leaky bucket shaper profiles. Frames within the Committed Information Rate (CIR) or Committed Burst Size (CBS) are marked Green. Frames within the Excess Information Rate (EIR) or Excess Burst Size (EBS) are marked Yellow. Frames that do not fall within the CIR/CBS+EIR/EBS are marked Red and dropped, without being sent any further.

The CIR value can be set to the following values:

- 0 - 25 Gbps

The CBS value can be set to the following values:

- 1-63 KB. The default value is 16 KB.

<b>Note:</b>	Users can enter any values within the permitted range. Based on the value entered by the user, the software automatically rounds off the setting according to the granularity. If the user enters a value below the lowest granular value (except 0), the software adjusts the setting to the minimum.
--------------	--

Users can attach one of the configured queue shaper profiles to each priority queue. If no profile is attached to the queue, no egress shaping is performed on that queue.

### Line Compensation for Shaping

Users can configure a line compensation value for all the shapers under a specific logical interface. For more information, refer to *Global Rate Meter Profiles* on page 84.

## Egress Scheduling

Egress scheduling is responsible for transmission from the priority queues. IP-50EX uses a unique algorithm with a hierarchical scheduling model over the three levels of the egress path that enables compliance with SLA requirements.

The scheduler scans all the queues, per interface, and determines which queue is ready to transmit. If more than one queue is ready to transmit, the scheduler determines which queue transmits first based on:

- **Queue Priority** – A queue with higher priority is served before lower-priority queues.
- **Weighted Fair Queuing (WFQ)** – If two or more queues have the same priority and are ready to transmit, the scheduler transmits frames from the queues based on a WFQ algorithm that determines the ratio of frames per queue based on a predefined weight assigned to each queue.

The following figure shows the scheduling mechanism.



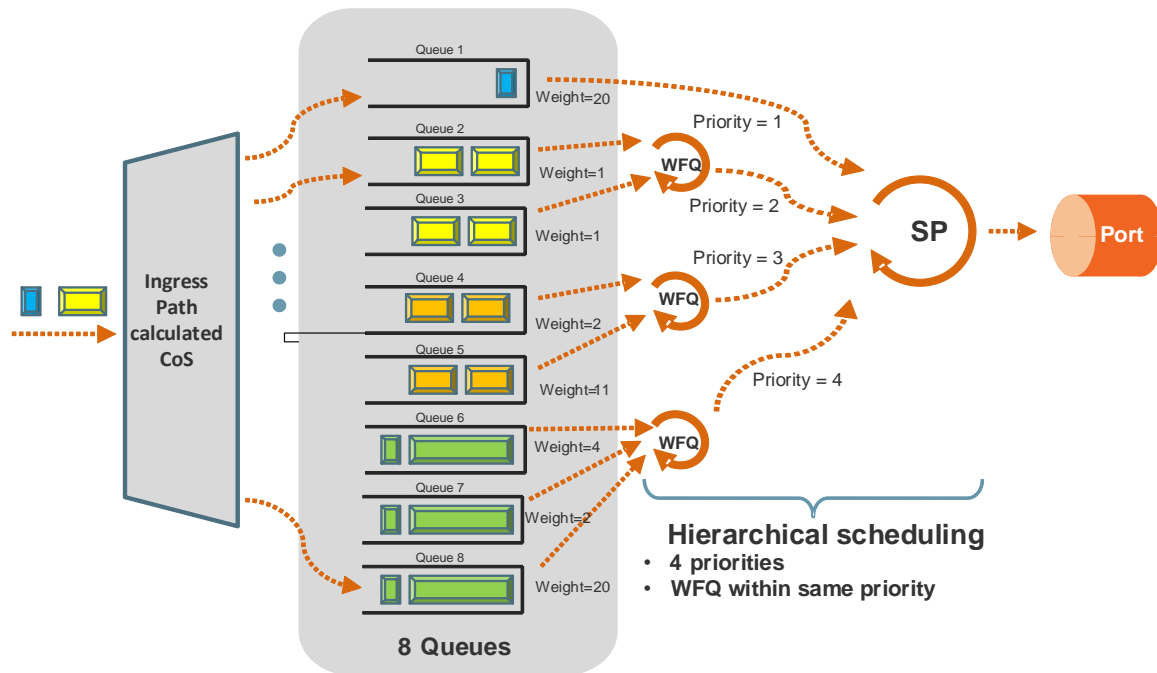


Figure 39: Scheduling Mechanism

### Interface Priority

The profile defines the exact order for serving the eight priority queues. Users can define up to four priority profiles, from 4 (highest) to 1 (lowest).

The following table provides a sample of an interface priority profile. This profile is also used as the default interface priority profile.

Table 15: QoS Priority Profile Example

Profile ID (1-9)		
CoS	Priority (user defined)	Description
0	1	Best Effort
1	2	Data Service 4
2	2	Data Service 3
3	2	Data Service 2
4	2	Data Service 1
5	3	Real Time 2 (Video with large buffer)
6	3	Real Time 1 (Video with small buffer)
7	4	Management (Sync, PDUs, etc.)

**Note:** CoS 7 is always marked with the highest priority, no matter what the state is, since it is assumed that only high priority traffic will be tunneled via CoS 7.

The system supports up to nine interface priority profiles. Profiles 1 to 8 are defined by the user, while profile 9 is the pre-defined read-only default interface priority profile.

The following interface priority profile parameters can be configured by users:

- **Profile ID** – Profile ID number. Permitted values are 1 to 8.
- **CoS 0 Priority** – CoS 0 queue priority, from 4 (highest) to 1 (lowest).
- **CoS 0 Description** – CoS 0 user description field, up to 20 characters.
- **CoS 1 Priority** – CoS 1 queue priority, from 4 (highest) to 1 (lowest).
- **CoS 1 Description** – CoS 1 user description field, up to 20 characters.
- **CoS 2 Priority** – CoS 2 queue priority, from 4 (highest) to 1 (lowest).
- **CoS 2 Description** – CoS 2 user description field, up to 20 characters.
- **CoS 3 Priority** – CoS 3 queue priority, from 4 (highest) to 1 (lowest).
- **CoS 3 Description** – CoS 3 user description field, up to 20 characters.
- **CoS 4 Priority** – CoS 4 queue priority, from 4 (highest) to 1 (lowest).
- **CoS 4 Description** – CoS 4 user description field, up to 20 characters.
- **CoS 5 Priority** – CoS 5 queue priority, from 4 (highest) to 1 (lowest).
- **CoS 5 Description** – CoS 5 user description field, up to 20 characters.
- **CoS 6 Priority** – CoS 6 queue priority, from 4 (highest) to 1 (lowest).
- **CoS 6 Description** – CoS 6 user description field, up to 20 characters.
- **CoS 7 Priority** – CoS 7 queue priority, from 4 (highest) to 1 (lowest).
- **CoS 7 Description** – CoS 7 user description field, up to 20 characters.

Users can attach one of the configured interface priority profiles to each interface. By default, the interface is assigned Profile ID 9, the pre-defined system profile.

#### Weighted Fair Queuing (WFQ)

As described above, the scheduler serves the queues based on their priority, but when two or more queues have data to transmit and their priority is the same, the scheduler uses WFQ to determine the weight within each priority. WFQ defines the transmission ratio between the queues.

The system supports up to six WFQ profiles. Profile ID 1 is a pre-defined read-only profile, and is used as the default profile. Profiles 2 to 6 are user-defined profiles.

## Egress PMs and Statistics

### Queue-Level Statistics

IP-50EX supports the following counters per queue at the queue level:

- Transmitted Green Packet (64 bits counter)
- Transmitted Green Bytes (64 bits counter)
- Transmitted Green Bits per Second (32 bits counter)
- Dropped Green Packets (64 bits counter)
- Dropped Green Bytes (64 bits counter)
- Transmitted Yellow Packets (64 bits counter)
- Transmitted Yellow Bytes (64 bits counter)
- Transmitted Yellow Bits per Second (32 bits counter)
- Dropped Yellow Packets (64 bits counter)
- Dropped Yellow Bytes (64 bits counter)

### Interface-Level Statistics

For information on statistics at the interface level, refer to *Ethernet Statistics* on page 71.

### Marker

Marking refers to the ability to overwrite the outgoing priority bits and Color of the outer VLAN of the egress frame. Marking mode is only applied if the outer frame is S-VLAN and S-VLAN CoS preservation is disabled, or if the outer frame is C-VLAN and C-VLAN CoS preservation is disabled. If outer VLAN preservation is enabled for the relevant outer VLAN, the egress CoS and Color are the same as the CoS and Color of the frame when it ingressed into the switching fabric.

Marking is performed according to a global table that maps CoS and Color values to the 802.1p-UP bits and maps Color values to the DEI or CFI bits. If Marking is enabled on a service point, the CoS and Color of frames egressing the service via that service point are overwritten according to this global mapping table.

If marking and CoS preservation for the relevant outer VLAN are both disabled, marking is applied according to the Green frame values in the global marking table.

If CoS preservation is enabled, an added VLAN always has UP and DEI set to 0.

When marking is performed, the following global tables are used by the marker to decide which CoS and Color to use as the egress CoS and Color bits.

*Table 16: Marking Table for 802.1Q and 802.1AD UP Bits*

CoS	Color	802.1Q UP (Configurable)	802.1AD UP (Configurable)
0	Green	0	0
0	Yellow	0	0

CoS	Color	802.1Q UP (Configurable)	802.1AD UP (Configurable)
1	Green	1	1
1	Yellow	1	1
2	Green	2	2
2	Yellow	2	2
3	Green	3	3
3	Yellow	3	3
4	Green	4	4
4	Yellow	4	4
5	Green	5	5
5	Yellow	5	5
6	Green	6	6
6	Yellow	6	6
7	Green	7	7
7	Yellow	7	7

The keys for these tables are the CoS and Color. The results are the 802.1q/802.1AD UP and bits, which are user-configurable. It is strongly recommended that the default values not be changed except by advanced users.

The following are the default values for marking CFI/DEI bits:

- Green: 0
- Yellow: 1

## QoS Summary

The following table summarizes the capabilities of the IP-50EX QoS mechanism.

*Table 17: Summary of IP-50EX QoS Mechanism*

Number of transmission queues per port	8
Number of service bundles	1 (service bundle ID is always 1)
WRED	Per queue (two curves – for green traffic and for yellow traffic via the queue)
Shaping at queue level	Single leaky bucket
Shaping at service bundle level	None
Shaping at port level	Single leaky bucket
Transmission queues priority	Per queue priority (4 priorities).
Weighted Fair Queuing (WFQ)	Queue level (between queues)
Marker	Supported
Statistics	Queue level (8 queues) Service bundle level (1 service bundle) Port level

#### 4.2.5 Global Switch Configuration

The following parameters are configured globally for the IP-50EX switch:

- **S- VLAN Ethertype** – Defines the ethertype recognized by the system as the S-VLAN ethertype. IP-50EX supports the following S-VLAN ethertypes:
  - 0x8100
  - 0x88A8 (default)
  - 0x9100
  - 0x9200
- **C-VLAN Ethertype** – Defines the ethertype recognized by the system as the C-VLAN ethertype. IP-50EX supports 0x8100 as the C-VLAN ethertype.
- **MRU** – The maximum segment size defines the maximum receive unit (MRU) capability and the maximum transmit capability (MTU) of the system. Users can configure a global MRU for the system. Permitted values are 64 bytes to 9612 bytes.

## 4.2.6 Automatic State Propagation and Link Loss Forwarding

### Related topics:

- Network Resiliency
- Link Aggregation Groups (LAG)

---

Automatic State Propagation (ASP) enables propagation of radio failures back to the Ethernet port. You can also configure ASP to close the Ethernet port based on a radio failure at the remote carrier. ASP improves the recovery performance of resiliency protocols.

**Note:** It is recommended to configure both ends of the link to the same ASP configuration.

### 4.2.6.1 Automatic State Propagation Operation

Automatic state propagation is configured as pairs of interfaces. Each interface pair includes one Monitored Interface and one Controlled Interface. Multiple pairs can be configured using the same Monitored Interface and multiple Controlled Interfaces.

The Monitored Interface is a radio interface. The Controlled Interface is an Ethernet interface or LAG. An Ethernet interface can only be assigned to one Monitored interface.

Each Controlled Interface is assigned an LLF ID. If **ASP trigger by remote fault** is enabled on the remote side of the link, the ASP state of the Controlled Interface is propagated to the Controlled Interface with the same LLF ID at the remote side of the link. This means if ASP is triggered locally, it is propagated to the remote side of the link, but only to Controlled Interfaces with LLF IDs that match the LLF IDs of the affected Controlled Interfaces on the local side of the link.

The following events in the Monitored Interface trigger ASP:

- Radio LOF
- Radio Excessive BER
- Remote Radio LOF
- Remote Excessive BER
- Remote LOC

The user can also configure the ASP pair so that Radio LOF, Radio Excessive BER, or loss of the Ethernet connection at the remote side of the link will also trigger ASP.

When a triggering event takes place:

- If the Controlled Interface is an electrical GbE port, the port is closed.
- If the Controlled Interface is an optical GbE port, the port is muted.

The Controlled Interface remains closed or muted until all triggering events are cleared.

In addition, when a local triggering event takes place, the ASP mechanism sends an indication to the remote side of the link. Even when no triggering event has taken place, the ASP mechanism sends periodic update messages indicating that no triggering event has taken place.

Users can configure a trigger delay time, so that when a triggering event takes place, the ASP mechanism does not propagate the event until this delay time has elapsed.

#### **4.2.6.2 Automatic State Propagation and Protection**

When the Controlled Interface is part of a 1+1 protection pair, such as a 1+1 HSB protection configuration, a port shutdown message is only sent to the remote side of the link if both of the protected interfaces are shut down.

In a 1+1 HSB configuration using Multi-Unit LAG mode, in which two Ethernet interfaces on each unit belong to a static LAG, an ASP triggering event only shuts down the external user port.

When the Monitored interface is part of a 1+1 HSB configuration, ASP is only triggered if both interfaces fail.

Closing an Ethernet port because of ASP does not trigger a protection switchover.

#### **4.2.6.3 Preventing Loss of In-Band Management**

If the link uses in-band management, shutting down the Ethernet port can cause loss of management access to the unit. To prevent this, users can configure ASP to operate in Client Signal Failure (CSF) mode. In CSF mode, the ASP mechanism does not physically shut down the Controlled Interface when ASP is triggered. Instead, the ASP mechanism sends a failure indication message (a CSF message). The CSF message is used to propagate the failure indication to external equipment.

CSF mode is particularly useful when the IP-50EX unit is an element in the following network topologies:

- Ring or mesh network topology.
- An IP-20N connected to an IP-50EX unit being utilized as a pipe via an Ethernet interface (back-to-back on the same site).
- Payload traffic is spanned by G.8032 in the network.
- In-band management is spanned by MSTP in the network.
- An IP-50EX unit being utilized as a pipe is running one MSTP instance for spanning in-band management.



#### 4.2.7 Network Resiliency

IP-50EX provides carrier-grade service resiliency using the following protocols:

- G.8032 Ethernet Ring Protection Switching (ERPS)
- Multiple Spanning Tree Protocol (MSTP)

These protocols are designed to prevent loops in ring/mesh topologies.

##### 4.2.7.1 G.8032 Ethernet Ring Protection Switching (ERPS)

ERPS, as defined in the G.8032 ITU standard, is currently the most advanced ring protection protocol, providing convergence times of sub-50ms. ERPS prevents loops in an Ethernet ring by guaranteeing that at any time, traffic can flow on all except one link in the ring. This link is called the Ring Protection Link (RPL). Under normal conditions, the RPL is blocked, i.e., not used for traffic. One designated Ethernet Ring Node, the RPL Owner Node, is responsible for blocking traffic at one end of the RPL. When an Ethernet ring failure occurs, the RPL Owner unblocks its end of the RPL, allowing the RPL to be used for traffic. The other Ethernet Ring Node adjacent to the RPL, the RPL Neighbor Node, may also participate in blocking or unblocking its end of the RPL. A number of ERP instances (ERPis) can be created on the same ring.

##### G.8032 ERPS Benefits

ERPS, as the most advanced ring protection protocol, provides the following benefits:

- Provides sub-50ms convergence times.
- Provides service-based granularity for load balancing, based on the ability to configure multiple ERPis on a single physical ring.
- Provides configurable timers to control switching and convergence parameters per ERPi.

##### G.8032 ERPS Operation

The ring protection mechanism utilizes an APS protocol to implement the protection switching actions. Forced and manual protection switches can also be initiated by the user, provided the user-initiated switch has a higher priority than any other local or far-end request.

Ring protection switching is based on the detection of defects in the transport entity of each link in the ring. For purposes of the protection switching process, each transport entity within the protected domain has a state of either Signal Fail (SF) or Non-Failed (OK). R-APS control messages are forwarded by each node in the ring to update the other nodes about the status of the links.

**Note:** An additional state, Signal Degrade (SD), is planned for future release. The SD state is similar to SF, but with lower priority.

Users can configure up to 16 ERPIs. Each ERPI is associated with an Ethernet service defined in the system. This enables operators to define a specific set of G.8032 characteristics for individual services or groups of services within the same physical ring. This includes a set of timers that enables operators to optimize protection switching behavior per ERPI:

- **Wait to Restore (WTR) Timer** – Defines a minimum time the system waits after signal failure is recovered before reverting to idle state.
- **Guard Time** – Prevents unnecessary state changes and loops.
- **Hold-off Time** – Determines the time period from failure detection to response.

Each ERPI maintains a state machine that defines the node's state for purposes of switching and convergence. The state is determined according to events that occur in the ring, such as signal failure and forced or manual switch requests, and their priority. Possible states are:

- Idle
- Protecting
- Forced Switch (FS)
- Manual Switch (MS)
- Pending

As shown in the following figure, in idle (normal) state, R-APS messages pass through all links in the ring, while the RPL is blocked for traffic. The RPL can be on either edge of the ring. R-APS messages are sent every five seconds.

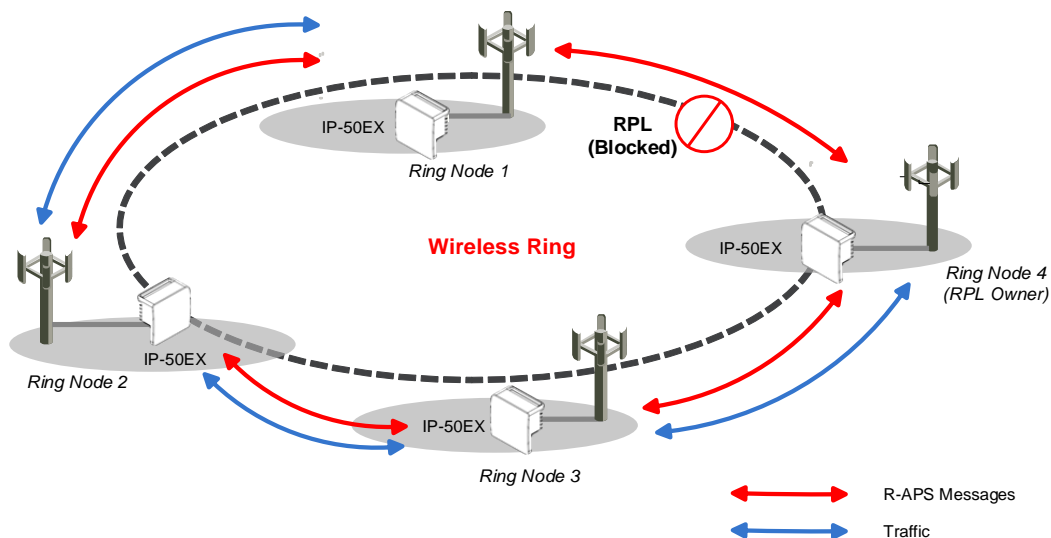


Figure 40: G.8032 Ring in Idle (Normal) State

Once a signal failure is detected, the RPL is unblocked for each ERPI. As shown in the following figure, the ring switches to protecting state. The nodes that detect the failure send periodic SF messages to alert the other nodes in the link of the failure and initiate the protecting state.

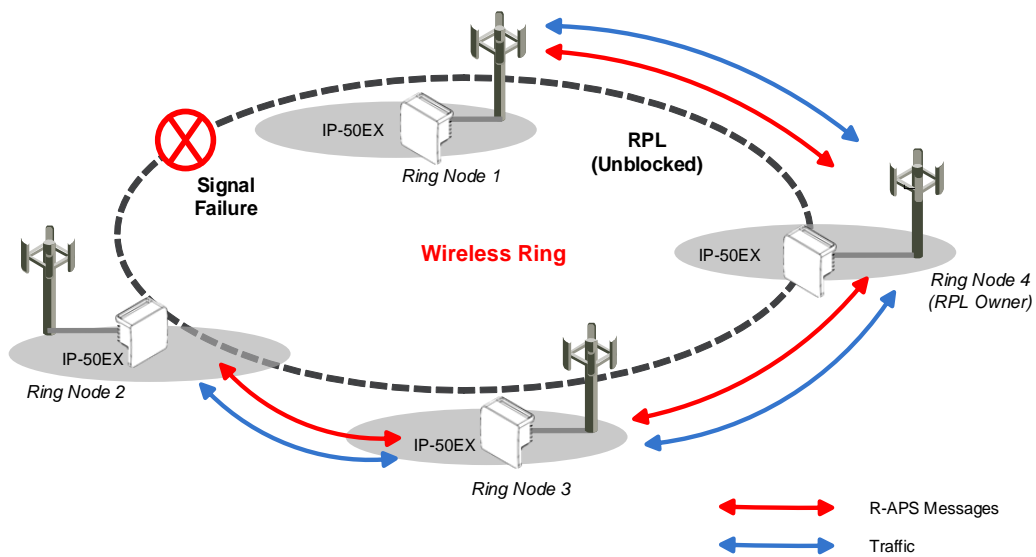


Figure 41: G.8032 Ring in Protecting State

The ability to define multiple ERPIs and assign them to different Ethernet services or groups of services enables operators to perform load balancing by configuring a different RPL for each ERPI. The following figure illustrates a ring in which four ERPIs each carry services with 33% capacity in idle state, since each link is designated the RPL, and is therefore idle, for a different ERPI.

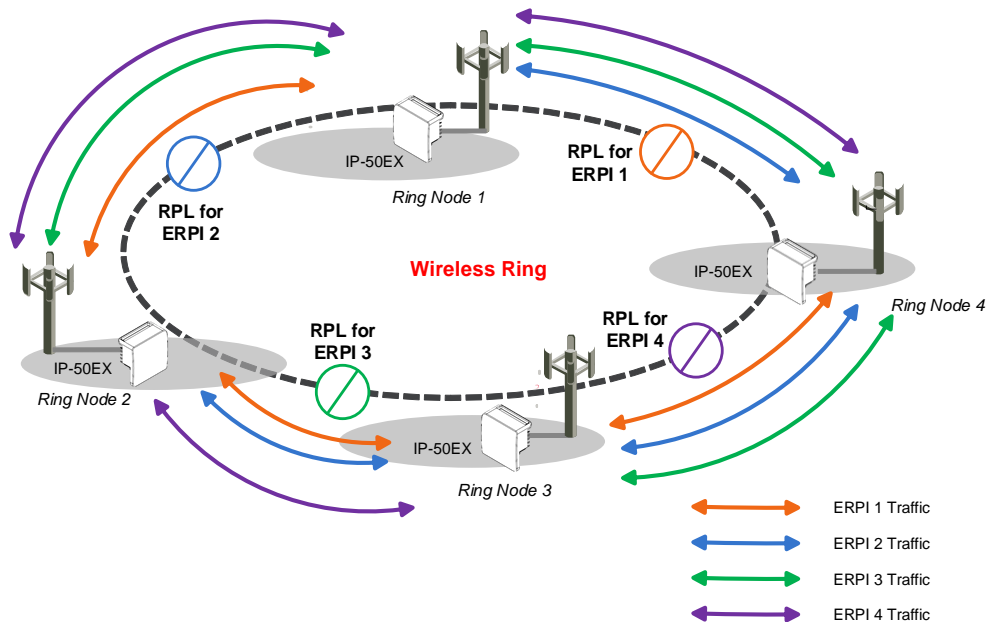


Figure 42: Load Balancing Example in G.8032 Ring

#### 4.2.7.2 Multiple Spanning Tree Protocol (MSTP)

MSTP, as defined in IEEE 802.1q, provides full connectivity for frames assigned to any given VLAN throughout a bridged LAN consisting of arbitrarily interconnected bridges.

With MSTP, an independent multiple spanning tree instance (MSTI) is configured for each group of services, and only one path is made available (unblocked) per spanning tree instance. This prevents network loops and provides load balancing capability. It also enables operators to differentiate among Ethernet services by mapping them to different, specific MSTIs. The maximum number of MSTIs is configurable, from 2 to 16.

MSTP is an extension of, and is backwards compatible with, Rapid Spanning Tree Protocol (RSTP).

IP-50EX supports MSTP according to the following IEEE standards:

- 802.1q
- 802.1ad amendment
- 802.1ah (TE instance)

##### MSTP Benefits

MSTP significantly improves network resiliency in the following ways:

- Prevents data loops by configuring the active topology for each MSTI such that there is never more than a single route between any two points in the network.
- Provides for fault tolerance by automatically reconfiguring the spanning tree topology whenever there is a bridge failure or breakdown in a data path.
- Automatically reconfigures the spanning tree to accommodate addition of bridges and bridge ports to the network, without the formation of transient data loops.
- Enables frames assigned to different services or service groups to follow different data routes within administratively established regions of the network.
- Provides for predictable and reproducible active topology based on management of the MSTP parameters.
- Operates transparently to the end stations.
- Consumes very little bandwidth to establish and maintain MSTIs, constituting a small percentage of the total available bandwidth which is independent of both the total traffic supported by the network and the total number of bridges or LANs in the network.
- Does not require bridges to be individually configured before being added to the network.

## MSTP Operation

MSTP includes the following elements:

- **MST Region** – A set of physically connected bridges that can be portioned into a set of logical topologies.
- **Internal Spanning Tree (IST)** – Every MST Region runs an IST, which is a special spanning tree instance that disseminates STP topology information for all other MSTIs.
- **CIST Root** – The bridge that has the lowest Bridge ID among all the MST Regions.
- **Common Spanning Tree (CST)** – The single spanning tree calculated by STP, RSTP, and MSTP to connect MST Regions. All bridges and LANs are connected into a single CST.
- **Common Internal Spanning Tree (CIST)** – A collection of the ISTs in each MST Region, and the CST that interconnects the MST regions and individual spanning trees. MSTP connects all bridges and LANs with a single CIST.

MSTP specifies:

- An MST Configuration Identifier that enables each bridge to advertise its configuration for allocating frames with given VIDs to any of a number of MSTIs.
- A priority vector that consists of a bridge identifier and path cost information for the CIST.
- An MSTI priority vector for any given MSTI within each MST Region.

Each bridge selects a CIST priority vector for each port based on the priority vectors and MST Configuration Identifiers received from the other bridges and on an incremental path cost associated with each receiving port. The resulting priority vectors are such that in a stable network:

- One bridge is selected to be the CIST Root.
- A minimum cost path to the CIST Root is selected for each bridge.
- The CIST Regional Root is identified as the one root per MST Region whose minimum cost path to the root is not through another bridge using the same MST Configuration Identifier.

Based on priority vector comparisons and calculations performed by each bridge for each MSTI, one bridge is independently selected for each MSTI to be the MSTI Regional Root, and a minimum cost path is defined from each bridge or LAN in each MST Region to the MSTI Regional Root.

The following events trigger MSTP re-convergence:

- Addition or removal of a bridge or port.
- A change in the operational state of a port or group (LAG or protection).
- A change in the service to instance mapping.
- A change in the maximum number of MSTIs.
- A change in an MSTI bridge priority, port priority, or port cost.

**Note:** All except the last of these triggers can cause the entire MSTP to re-converge. The last trigger only affects the modified MSTI.

### **MSTP Interoperability**

MSTP in IP-50EX units is interoperable with:

- Third-party bridges running MSTP.
- Third-party bridges running RSTP

#### 4.2.8 OAM

IP-50EX provides complete Service Operations Administration and Maintenance (SOAM) functionality at multiple layers, including:

- Fault management status and alarms.
- Loopback
- Ethernet Bandwidth Notification (ETH-BN)

IP-50EX is fully compliant with 802.1ag, G.8013/Y.1731, MEF-17, MEF-20, MEF-30, and MEF-31.

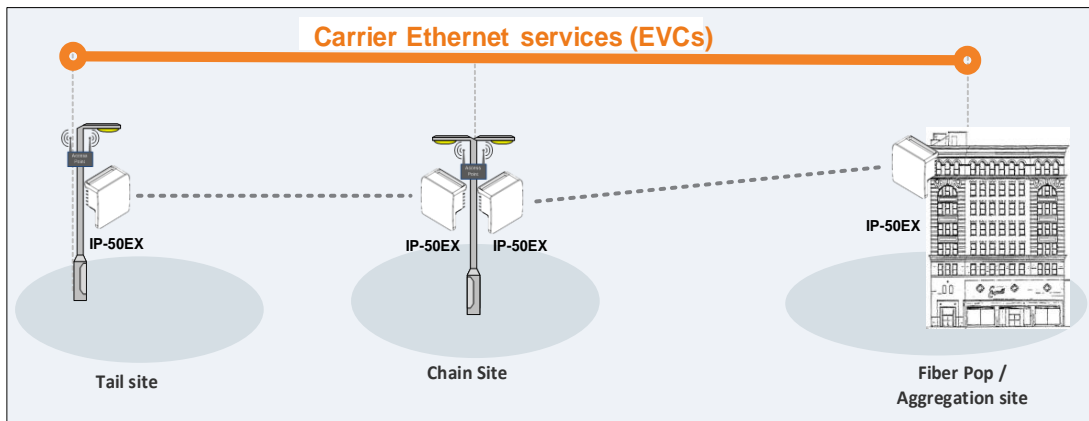


Figure 43: IP-50EX End-to-End Service Management

##### 4.2.8.1 Connectivity Fault Management (FM)

The IEEE 802.1ag and G.8013/Y.1731 standards and the MEF-17, MEF-20, MEF-30, and MEF-31 specifications define SOAM. SOAM is concerned with detecting, isolating, and reporting connectivity faults spanning networks comprising multiple LANs, including LANs other than IEEE 802.3 media.

IEEE 802.1ag Ethernet FM (Connectivity Fault Management) consists of three protocols that operate together to aid in fault management:

- Continuity check
- Loopback

IP-50EX utilizes these protocols to maintain smooth system operation and non-stop data flow.

The following are the basic building blocks of FM:

- Maintenance domains, their constituent maintenance points, and the managed objects required to create and administer them.

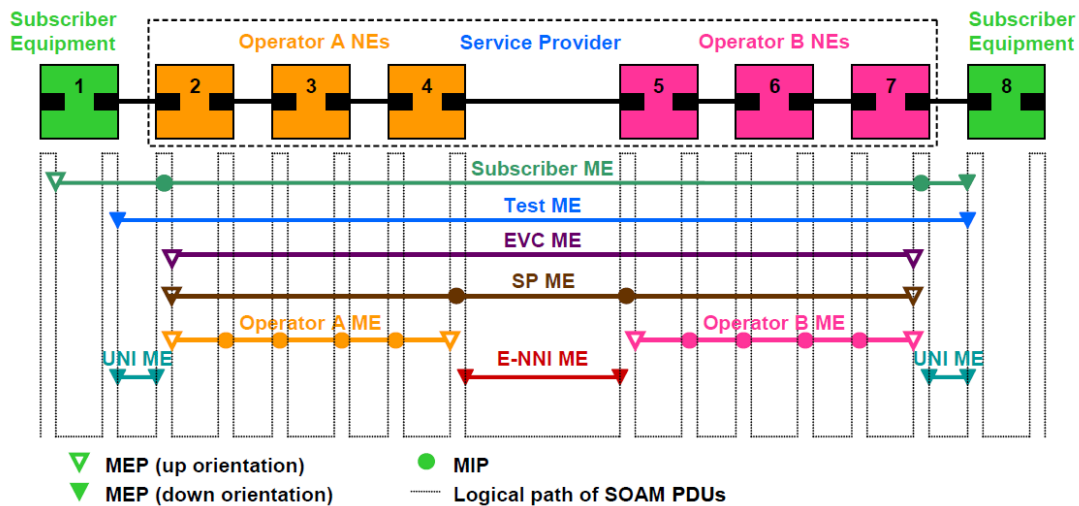


Figure 44: SOAM Maintenance Entities (Example)

- Protocols and procedures used by maintenance points to maintain and diagnose connectivity faults within a maintenance domain.
  - CCM (Continuity Check Message): CCM can detect Connectivity Faults (loss of connectivity or failure in the remote MEP).
  - Loopback: LBM/LBR mechanism is an on-demand mechanism. It is used to verify connectivity from any MEP to any certain Maintenance Point in the MA/MEG. A session of loopback messages can include up to 1024 messages with varying intervals ranging from 1 to 60 seconds. Message size can reach jumbo frame size.<sup>10</sup>

#### 4.2.8.2 SFP DDM and Inventory Monitoring

IP-50EX supports static and dynamic monitoring for all SFP modules, including all SFP, SFP+, and QSFP modules used in Ethernet ports. Dynamic monitoring PMs are also available.

DDM (Digital Diagnostic Monitoring) enables users to display dynamic information about the SFP state, including:

- RX Power (in dBm)
- TX Power (in dBm)
- Bias current (mA)
- Temperature (both Celsius and Fahrenheit)

**Note:** Tx Power level DDM is not supported for QSFP (P5) – not part of the standard.

<sup>10</sup> Support for Loopback is planned for future release.



Inventory monitoring enables users to display the following information about each SFP module installed in the IP-50EX unit:

- Connector Type
- Transceiver Type (e.g., 10G BASE-LR)
- Vendor Name
- Vendor Part Number
- Vendor Serial Number
- Vendor Revision
- Wavelength
- Maximum length of link per fiber optic cable type

DDM PMs can be displayed for 15-minute and 24-hour intervals. For each interval, the following PMs are displayed:

- Minimum RX power during the interval (dBm)
- Average RX power during the interval (dBm)
- Maximum RX power during the interval (dBm)
- Minimum TX power during the interval (dBm)
- Average TX power during the interval (dBm)
- Maximum TX power during the interval (dBm)

**Note:** DDM parameters are not relevant for electrical SFPs.

Thresholds for these alarms are programmed into the SFP modules by the manufacturer.

#### 4.2.8.3 Ethernet Bandwidth Notification (ETH-BN)

Ethernet Bandwidth Notification (ETH-BN) is defined by the Y.1731 OAM standard. The purpose of ETH-BN is to inform the L2 or L3 customer switch of the capacity of the radio link in transmit direction. This enables the switch to respond to fluctuations in the radio link by, for example, reconfiguring the shaper on the egress port facing the radio link or rerouting traffic to other egress ports.

Once ETH-BN is enabled, the radio unit reports bandwidth information to upstream third-party switches. The ETH-BN entity creates a logical relationship between a radio interface, called the Monitored Interface, and an Ethernet interface, called the Control Interface. When bandwidth degrades from the nominal value in the Monitored Interface, messages relaying the actual bandwidth values (BNM frames) are periodically sent over the Control Interface. Once the bandwidth returns to its nominal level, BNM messages are no longer sent. Optionally, the device can be configured to send BNM frames even when bandwidth is at its nominal level.

The Monitored Interface can be a single radio interface, a Multiband group, or a radio LAG. To be used as a Monitored Interface, the LAG must consist of radio interfaces only.

The same radio interface can be configured as a Monitored Interface for multiple EBN instances. However, an Ethernet interface can only be configured as a Control Interface for a single EBN instance.

Note the following limitations:

- If CFM MEPs are being used, the MEL for ETH-BN must be set to a value greater than the MEG level of the CFM MEP. Otherwise, the BNM frames will be dropped. – this is a correct behavior.
- If CFM MEPs are not being used, the MEL for ETH-BN must be set to a value greater than 0. Otherwise, the BNM frames will be dropped.

### 4.3 E-Stabilizer

IP-50EX can be used with the E-Stabilizer antenna. E-Stabilizer is a 3-foot (90 cm) E-Band antenna that features a beam-stabilizing mechanism. This is an important advancement that can increase the IP-50EX's radio coverage by up to 50% by enabling the use of a higher-gain 3-foot antenna with IP-50EX. Without the beam-stabilizing mechanism, the use of 3-foot antennas with E-Band radios is generally impractical due to the antenna's very narrow beamwidth, which prevents the common commercial use of 3-foot antennas with E-Band radios.

E-Stabilizer also shortens installation time. E-Stabilizer's built-in manual antenna alignment makes it easy to align the antenna, despite the narrow beamwidth. E-Stabilizer provides easy-to-read indications as to which direction and at what angle the antenna should be moved to achieve perfect alignment.

An important feature of E-Stabilizer is its automatic beam alignment ability. E-Stabilizer can automatically stabilize the beam of the antenna to compensate for movements, such as slow pole deflection or fast vibrations due to heavy winds. E-Stabilizer can keep the beam stabilized whether the movements are vertical, horizontal, or in any direction. E-Stabilizer can also compensate for thermal expansion and contraction of the tower during the day and night. Triggered from the radio RSS readout, E-Stabilizer keeps the link well-aligned in windy conditions.

In addition to the consistency of alignment provided by the automatic beam alignment ability, this feature enables the use of less rigid poles, lowering installation costs. No moving parts are involved, providing greater reliability and lower maintenance costs.

E-Stabilizer also provides detailed performance monitoring counters and statistics. These counters and statistics provide detailed information about beam correction, facilitating preventive maintenance when needed. E-Stabilizer raises an SNMP alarm any time the mechanism fails to compensate for beam movements.

## 4.4 Frequency Scanner

**Note:** The frequency scanner is planned for future release.

Operating in the E-band poses both challenges and advantages with respect to interference and interference mitigation. On one hand, since the E-band is an unlicensed band in many countries, systems operating in the E-band must be able to handle interference scenarios. On the other hand, the nature of the E-band spectrum provides a degree of built-in interference mitigation through an unusually high degree of oxygen and rain attenuation and a wide range of available channels. Ceragon's use of narrow-beamed antennas with the IP-50EX further minimizes the occurrence of interference.

To further facilitate optimal IP-50EX operation in frequency scenarios, IP-50EX includes a frequency scanner that enables users to scan a defined frequency range and determine the current interference level for each channel.

The frequency scanner can be used both in the initial provisioning of the link and at any time after the link has been provisioned. The scanner is run at both sides of the link to determine the interference level for each RX channel. Using this information, the user can select the channels with the least interference, and configure IP-50EX's frequency accordingly.

The frequency scanner can be run in either of two modes, over a user-defined frequency range:

- **Continuous Mode** – The frequency scanner scans each channel in the script, and repeats the scan continuously until the user manually stops the scan. For each channel, the Web EMS displays the minimum, maximum, and most recently measured interference levels, in table and graph formats.
- **Single Mode** – The frequency scanner scans each channel in the script once. For each channel, the Web EMS displays the measured interference level, in table and graph formats.

## 4.5 Synchronization

This section describes IP-50EXmos's flexible synchronization solution that enables operators to configure a combination of synchronization techniques, based on the operator's network and migration strategy, including:

- PTP optimized transport, supporting IEEE 1588 and NTP, with guaranteed ultra-low PDV and support for ACMB and narrow channels.
- Native Sync Distribution, for end-to-end distribution using GbE.

### **This section includes:**

- IP-50EX Synchronization Solution
- Available Synchronization Interfaces
- Synchronous Ethernet (SyncE)
- IEEE-1588v2 PTP Optimized Transport
- SSM Support and Loop Prevention

### **Related topics:**

- NTP Support

### 4.5.1 IP-50EX Synchronization Solution

Ceragon's synchronization solution ensures maximum flexibility by enabling the operator to select any combination of techniques suitable for the operator's network and migration strategy.

- PTP optimized transport
  - Supports a variety of protocols, such as IEEE-1588 and NTP
  - Supports IEEE-1588 Transparent Clock
  - Guaranteed ultra-low PDV (<0.015 ms per hop)
  - Unique support for ACMB and narrow channels
- SyncE node
- IEEE-1588v2 PTP Optimized Transport
  - Transparent Clock – Resides between master and slave nodes, and measurers and adjusts for delay variation to guarantee ultra-low PDV.
  - Boundary Clock – Regenerates frequency and phase synchronization, providing, increasing the scalability of the synchronization network while rigorously maintaining timing accuracy.

#### 4.5.2 Available Synchronization Interfaces

Frequency signals can be taken by the system from a number of different interfaces (one reference at a time). The reference frequency may also be conveyed to external equipment through different interfaces.

*Table 18: Synchronization Interface Options*

Available interfaces as frequency input (reference sync source)	Available interfaces as frequency output
<ul style="list-style-type: none"><li>• Radio carrier</li><li>• GbE Ethernet interfaces</li></ul>	<ul style="list-style-type: none"><li>• Radio carrier</li><li>• GbE Ethernet interfaces</li></ul>

It is possible to configure up to five synchronization sources in the system. At any given moment, only one of these sources is active; the clock is taken from the active source onto all other appropriately configured interfaces.

Users can configure a revertive timer for the IP-50 unit. When the revertive timer is configured, the unit will not switch to another synchronization source unless that source has been stable for at least the number of seconds defined in the revertive timer. This helps to prevent a situation in which numerous switchovers occur when a synchronization source reports a higher quality for a brief time interval, followed by a degradation of the source's quality. By default, the revertive timer is set to 0, which means that it is disabled.

### 4.5.3 Synchronous Ethernet (SyncE)

SyncE is standardized in ITU-T G.8261 and G.8262, and refers to a method whereby the frequency is delivered on the physical layer.

**Note:** SyncE is not supported with electrical SFP modules.

### 4.5.4 IEEE-1588v2 PTP Optimized Transport

Precision Timing Protocol (PTP) refers to the distribution of frequency and phase, information across a packet-switched network.

IP-50EX supports PTP optimized transport, a message-based protocol that can be implemented across packet-based networks. To ensure minimal packet delay variation (PDV), IP-50EX's synchronization solution includes 1588v2-compliant Transparent Clock. Transparent Clock provides the means to measure and adjust for delay variation, thereby ensuring low PDV.

IEEE-1588v2 PTP synchronization is based on a master-slave architecture in which the master and slave exchange PTP packets carrying clock information. The master is connected to a reference clock, and the slave synchronizes itself to the master.

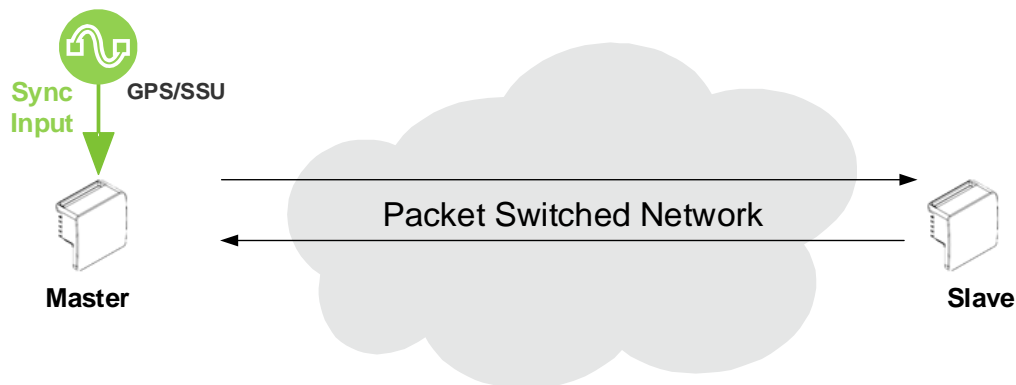


Figure 45: IEEE-1588v2 PTP Optimized Transport – General Architecture

Accurate synchronization requires a determination of the propagation delay for PTP packets. Propagation delay is determined by a series of messages between the master and slave.

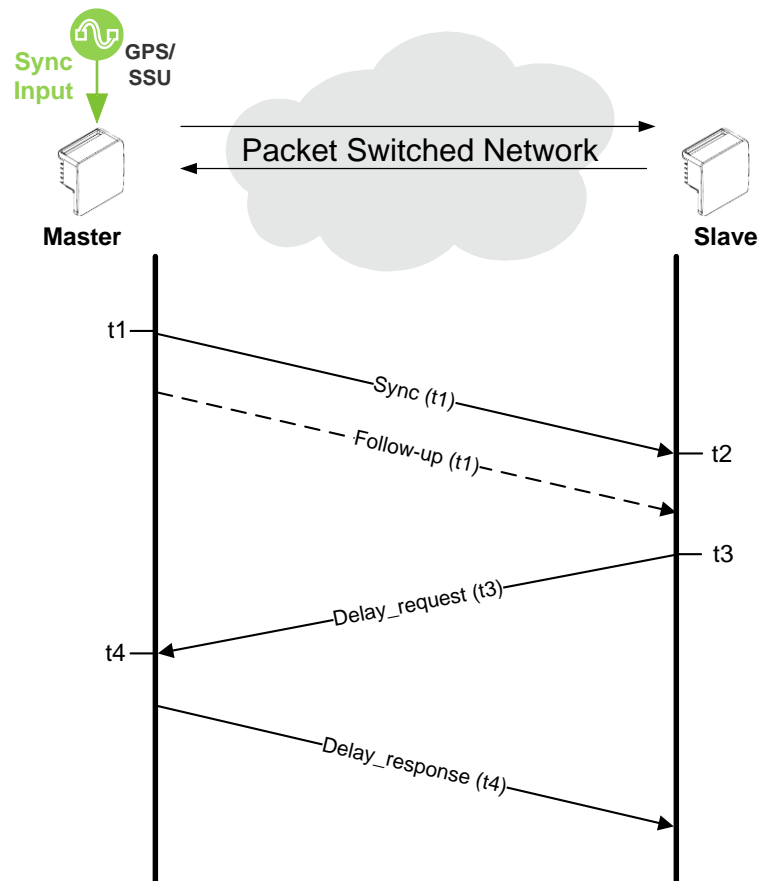


Figure 46: Calculating the Propagation Delay for PTP Packets

In this information exchange:

- 1 The master sends a Sync message to the slave and notes the time (t1) the message was sent.
- 2 The slave receives the Sync message and notes the time the message was received (t2).
- 3 The master conveys the t1 timestamp to the slave, in one of the following ways:
  - One-Step – Embedding the t1 timestamp in the Sync message.
  - Two-Step – Embedding the t1 timestamp in a Follow-up message.
- 4 The slave sends a Delay\_request message to the master and notes the time the message was sent (t3).
- 5 The master receives the Delay\_request message and notes the time the message was received (t4).
- 6 The master conveys the t4 timestamp to the slave by embedding the t4 timestamp in a Delay\_response message.

Based on this message exchange, the protocol calculates both the clock offset between the master and slave and the propagation delay, based on the following formulas:

$$\text{Offset} = [(t2 - t1) - (t4 - t3)]/2$$



$$\text{Propagation Delay} = [(t_2 - t_1) + (t_4 - t_3)]/2$$

The calculation is based on the assumption that packet delay is constant and that delays are the same in each direction. For information on the factors that may undermine these assumptions and how IP-50EX's IEEE-1588v2 implementations mitigate these factors, see *Mitigating PDV* on page 114.

#### 4.5.4.1 IEEE-1588v2 Characteristics

IEEE-1588v2 provides packet-based synchronization that can transmit both frequency accuracy and phase information. This is essential for LTE and 5G applications, and adds the ability to transmit phase information in addition to the frequency distributed by SyncE.

Other IEEE-1588v2 benefits include:

- Nanosecond precession.
- Meets strict 5G requirements for rigorous frequency and phase timing.
- Hardware time stamping of PTP packets.
- Standard protocol compatible with third-party equipment.
- Short frame and higher message rates.
- Supports unicast as well as multicast.
- Enables smooth transition from unsupported networks.
- Mitigates PDV issues by using Transparent Clock and Boundary Clock (see *Mitigating PDV* on page 114).
- Minimal consumption of bandwidth and processing power.
- Simple configuration.

The following modes of PTP operation are supported:

- Boundary Clock:
  - PTP over IEEE 802.3 Ethernet, per IEEE 1588 Annex F
  - ITU-T G.8275.1
  - Multicast mode
  - Untagged PTP packets
- Transparent Clock:
  - PTP over IEEE 802.3 Ethernet, per IEEE 1588 Annex F
  - PTP over UDP/IPv4, per IEEE 1588 Annex D
  - ITU-T G.8275.1
  - ITU-T G.8275.2
  - Unicast or multicast mode
  - Untagged or tagged PTP packets

#### 4.5.4.2 Mitigating PDV

To get the most out of PTP and minimize PDV, IP-50EX supports Transparent Clock and Boundary Clock.

PTP calculates path delay based on the assumption that packet delay is constant and that delays are the same in each direction. Delay variation invalidates this assumption. High PDV in wireless transport for synchronization over packet protocols, such as IEEE-1588, can dramatically affect the quality of the recovered clock. Slow variations are the most harmful, since in most cases it is more difficult for the receiver to average out such variations.

PDV can arise from both packet processing delay variation and radio link delay variation.

Packet processing delay variation can be caused by:

- **Queuing Delay** – Delay associated with incoming and outgoing packet buffer queuing.
- **Head of Line Blocking** – Occurs when a high priority frame, such as a frame that contains IEEE-1588 information, is forced to wait until a lower-priority frame that has already started to be transmitted completes its transmission.
- **Store and Forward** – Used to determine where to send individual packets. Incoming packets are stored in local memory while the MAC address table is searched and the packet's cyclic redundancy field is checked before the packet is sent out on the appropriate port. This process introduces variations in the time latency of packet forwarding due to packet size, flow control, MAC address table searches, and CRC calculations.

Radio link delay variation is caused by the effect of ACMB, which enables dynamic modulation changes to accommodate radio path fading, typically due to weather changes. Lowering modulation reduces link capacity, causing traffic to accumulate in the buffers and producing transmission delay.

<b>Note:</b>	When bandwidth is reduced due to lowering of the ACMB modulation point, it is essential that high priority traffic carrying IEEE-1588 packets be given the highest priority using IP-50EX's enhanced QoS mechanism, so that this traffic will not be subject to delays or discards.
--------------	---

These factors can combine to produce a minimum and maximum delay, as follows:

- **Minimum frame delay** can occur when the link operates at a high modulation and no other frame has started transmission when the IEEE-1588 frame is ready for transmission.
- **Maximum frame delay** can occur when the link is operating at QPSK modulation and a large (e.g., 1518 bytes) frame has just started transmission when the IEEE-1588 frame is ready for transmission.

The worst case PDV is defined as the greatest difference between the minimum and maximum frame delays. The worst case can occur not just in the radio equipment itself but in every switch across the network.

To ensure minimal packet delay variation (PDV), IP-50EX's synchronization solution includes 1588v2-compliant Transparent Clock and Boundary Clock synchronization protocols. The following section describes Transparent Clock and how it counters PDV.

#### 4.5.4.3 Transparent Clock

IP-50EX supports End-to-End Transparent Clock, which updates the correction field for the delay associated with individual packet transfers. End-to-End Transparent Clock is the most appropriate option for microwave radio links.

A Transparent Clock node resides between a master and a slave node, and updates the packets passing between the master and slave to compensate for delay, enabling the terminating clock in the slave node to remove the delay accrued in the Transparent Clock node. The Transparent Clock node is itself neither a master nor a slave node, but rather, serves as a bridge between master and slave nodes.

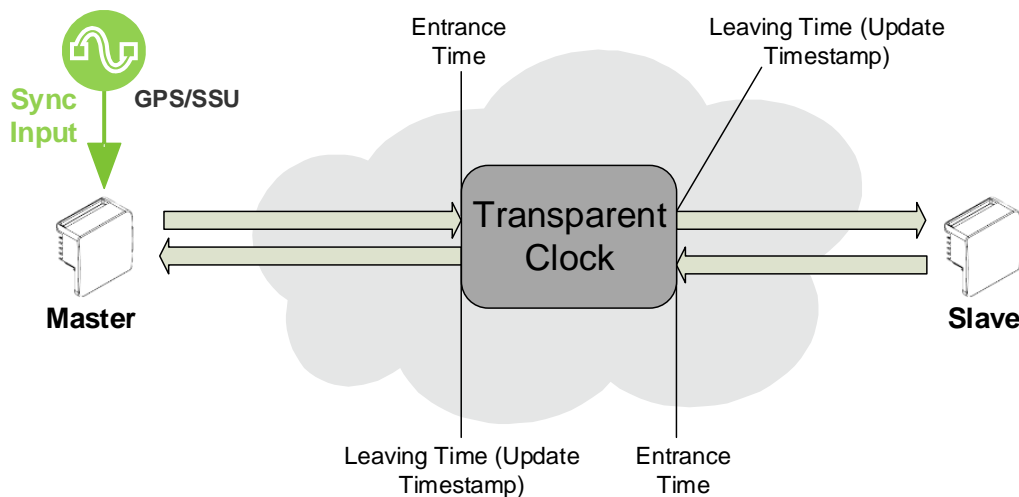


Figure 47: Transparent Clock – General Architecture

IP-50EX uses 1588v2-compliant Transparent Clock to counter the effects of asymmetrical delay and delay variation. Transparent Clock measures and adjusts for delay variation, enabling the IP-50EX to guarantee ultra-low PDV.

The Transparent Clock algorithm forwards and adjusts the messages to reflect the residency time associated with the Sync and Delay\_Request messages as they pass through the device. The delays are inserted in the 64-bit time-interval correction field.

As shown in the figure below, IP-50EX measures and updates PTP messages based on both the radio link delay, and the packet processing delay that results from the network processor (switch operation).

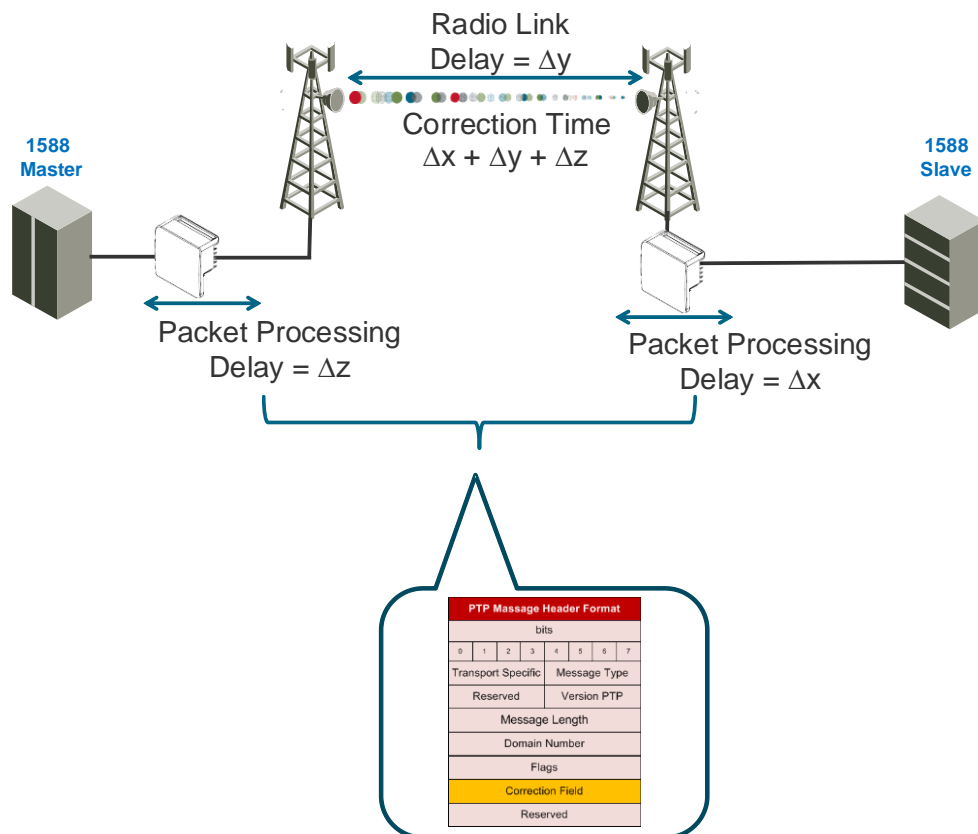


Figure 48: Transparent Clock Delay Compensation

#### 4.5.4.4 Boundary Clock

Boundary Clock provides better performance than other synchronization methods, enabling compliance with ITU-T Telecom Profile G.8275.1. This enables IP-50EX, with Boundary Clock, to meet the rigorous synchronization requirements of 5G networks.

In Boundary Clock, a single node can serve in both master and slave roles. The Boundary Clock node terminates the PTP flow, recovers the clock and timestamp, and regenerates the PTP flow. The Boundary Clock node selects the best synchronization source from a higher domain and regenerates PTP towards lower domains. This reduces the processing load from master clocks and increases the scalability of the synchronization network, while rigorously maintaining timing accuracy.

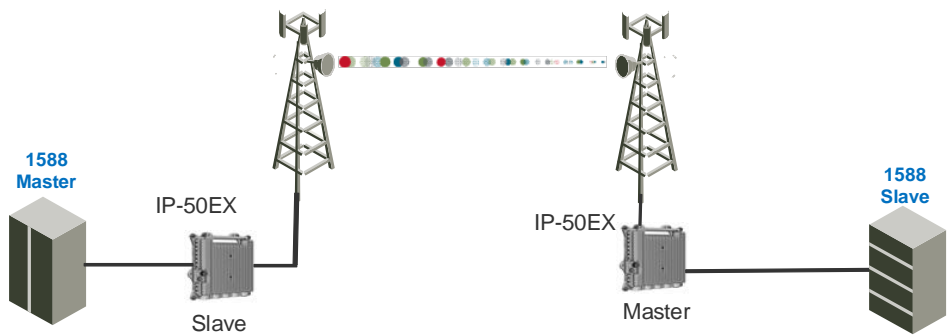


Figure 49: Boundary Clock – General Architecture

Boundary Clock uses the Best Master Clock (BMC) algorithm to determine which of the clocks in the network has the highest quality. This clock is designated the Grand Master clock, and it synchronizes all other clocks (slave clocks) in the network. If the Grand Master clock is removed from the network, or the BMC algorithm determines that another clock has superior quality, the BMC algorithm defines a new Grand Master clock and adjusts all other clocks accordingly. This process is fault tolerant, and no user input is required.

A node running as master clock can use the following inputs and outputs.

Table 19: Boundary Clock Input Options

Synchronization Input	Frequency/Phase
Ethernet packets from PTP 1588 Remote Master via radio or Ethernet interface	Phase
SyncE (including ESMC) via radio or Ethernet interface	Frequency

Table 20: Boundary Clock Output Options

Synchronization Input	Frequency/Phase
Ethernet packets from PTP 1588 master via radio or Ethernet interface	Phase
SyncE (including ESMC) via radio or Ethernet interface	Frequency

• .

4.5.5 SSM Support and Loop Prevention

In order to provide topological resiliency for synchronization transfer, IP-50EX implements the passing of SSM messages over the radio interfaces. SSM timing in IP-50EX complies with ITU-T G.781.

In addition, the SSM mechanism provides reference source resiliency, since a network may have more than one source clock.

The following are the principles of operation:

- At all times, each source interface has a “quality status” which is determined as follows:
  - If quality is configured as fixed, then the quality status becomes “failure” upon interface failure (such as LOS, LOC, LOF, etc.).
  - If quality is automatic, then the quality is determined by the received SSMs or becomes “failure” upon interface failure (such as LOS, LOC, LOF, etc.).
- Each unit holds a parameter which indicates the quality of its reference clock. This is the quality of the current synchronization source interface.
- The reference source quality is transmitted through SSM messages to all relevant radio interfaces.
- Each unit determines the current active clock reference source interface:
  - The interface with the highest available quality is selected.
  - From among interfaces with identical quality, the interface with the highest priority is selected.
- In order to prevent loops, an SSM with quality “Do Not Use” is sent towards the active source interface

At any given moment, the system enables users to display:

- The current source interface quality.
- The current received SSM status for every source interface.
- The current node reference source quality.

As a reference, the following are the possible quality values (from highest to lowest):

- AUTOMATIC (available only in interfaces for which SSM support is implemented)
- G.811 (ETSI systems)
- SSU-A (ETSI systems)
- SSU-B (ETSI systems)
- G.813/8262 – default
- PRS (ANSI systems)
- Stratum 2 (ANSI systems)
- Transit Node (ANSI systems)
- Stratum 3E (ANSI systems)
- Stratum 3 (ANSI systems)
- SMC (ANSI systems)
- Unknown (ANSI systems)
- DO NOT USE
- Failure (cannot be configured by user)

**Note:** Normally, when an interface is in holdover state, it uses stored data to determine its outgoing clock. However, customers can set the unit to apply a default quality of DNU (Do Not Use) to any interface in holdover state.

## 4.6 AES-GCM-256 Payload Encryption

**Note:** AES-GCM-256 requires IP-50EX-P.

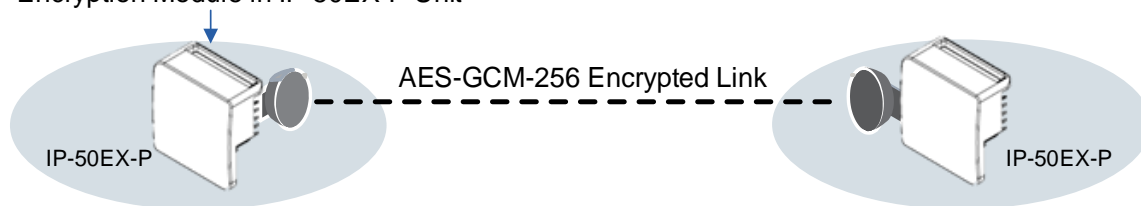
IP-50EX supports AES-GCM-256 payload encryption based on MACsec technology. MACsec (Media Access Control Security) is a Layer 2 security protocol that operates on Ethernet frames. MACsec is designed to provide authentication, confidentiality and integrity for data transported on point-to-point links in the enterprise Local Area Network (LAN) using the Advanced Encryption Standard with Galois/Counter Mode (AES-GCM) data cryptography algorithm.

The MACsec key agreement is a companion protocol that provides multiple authentications between hosts in a network. It creates a connectivity Association and generates session keys. MACsec adds a security tag and an integrity check value to each Ethernet frame, providing integrity to all the frames and, optionally, confidentiality to the user data.

MACsec is defined in IEEE 802.1AE-2018.

The Advanced Encryption Standard (AES) is defined in Federal Information Processing Standard Publication 197 (FIPS 197) for symmetric encryption. AES-GCM-256 is widely considered to be secure and efficient and is therefore broadly accepted as the standard for both government and industry applications.

Encryption Module in IP-50EX-P Unit



*Figure 50 AES-GCM-256 Encrypted Link*

**Notes:** The AES-GCM-256 payload encryption feature is a controlled item under applicable Export Laws. Please contact your Ceragon representative to confirm that the encryption feature can be delivered.

AES encryption is not supported with Multiband links.



#### 4.6.1 AES Benefits

- Provides protection against eavesdropping and man-in-the-middle attacks on the radio
- Full encryption for all radio traffic
- Wire-speed, lowest latency encryption
- Eliminates the need for external encryption devices:
  - Cost effective encryption solution
  - Low Capex and operational costs; fast and simple deployment

##### 4.6.1.1 IP-50EX AES Implementation

In IP-50EX-P, AES provides full payload encryption for all L1 radio traffic. AES encryption operates on a point-to-point radio link level. It also encrypts control data passing through the radio link, such as the Link ID, ATPC data, and SSM messages. AES encryption operates on a point-to-point radio link level. AES is enabled and configured separately for each radio carrier.

IP-50EX-P uses a dual-key encryption mechanism for AES.

- The user provides a master key. The master key can also be generated by the system upon user command. The master key is a 32-byte symmetric encryption key. The same master key must be manually configured on both ends of the encrypted link.
- The session key is a 32-byte symmetric encryption key used to encrypt the actual data. Each link uses two session keys, one for each direction. For each direction, the session key is generated by the transmit side unit and propagated automatically to the other side of the link via a Key Exchange Protocol. The Key Exchange Protocol exchanges session keys by encrypting them with the master key, using the AES-GCM-256 encryption algorithm. Session keys are regenerated at user-configured intervals.

The first KEP exchange that takes place after a new master key is configured causes traffic to be blocked for up to one minute, until the Crypto Validation State becomes Valid. Subsequent KEP exchanges that take place when a session key expires do not affect traffic. KEP exchanges have no effect upon ACM, RSL, and MSE.

Once AES encryption has been enabled on both sides of the link, the Key Exchange Protocol periodically verifies that both ends of the link have the same master key. If a mismatch is detected, an alarm is raised and traffic transmission is stopped for the mismatched carrier at both sides of the link. The link becomes non-valid and traffic stops being forwarded.

## 5. IP-50EX Management

**This chapter includes:**

- Management Overview
- Automatic Network Topology Discovery with LLDP Protocol
- Management Communication Channels and Protocols
- Web-Based Element Management System (Web EMS)
- SDN Support
- Command Line Interface (CLI)
- Configuration Management
- Software Management
- Using Pre-Defined Configuration Files
- IPv6 Support
- In-Band Management
- Local Management
- Alarms
- NTP Support
- UTC Support
- Syslog Support
- System Security Features

## 5.1 Management Overview

The Ceragon management solution is built on several layers of management:

- Web-based EMS – HTTP web-based Element Management System (EMS)
- CLI – Command Line Interface
  - SDN – Software-Defined Networking with NETCONF/YANG capabilities
- NMS – NetMaster Network Management System

Every IP-50EX includes an HTTP web-based EMS that enables the operator to perform device configuration, performance monitoring, remote diagnostics, alarm reports, and more. These same tasks can also be performed using the CLI.

IP-50EX supports NETCONF/YANG, enabling customers to manage, configure, and monitor network elements within the paradigm of SDN network architecture.

In addition, IP-50EX devices provide an SNMP v1/v2c/v3 northbound interface on the IDU for centralized network management. Ceragon offers the NetMaster network management system (NMS), which provides centralized operation and maintenance capability for the complete range of IP-50 devices. To facilitate automated network topology discovery via NMS, IP-50EX supports the Link Layer Discovery Protocol (LLDP).

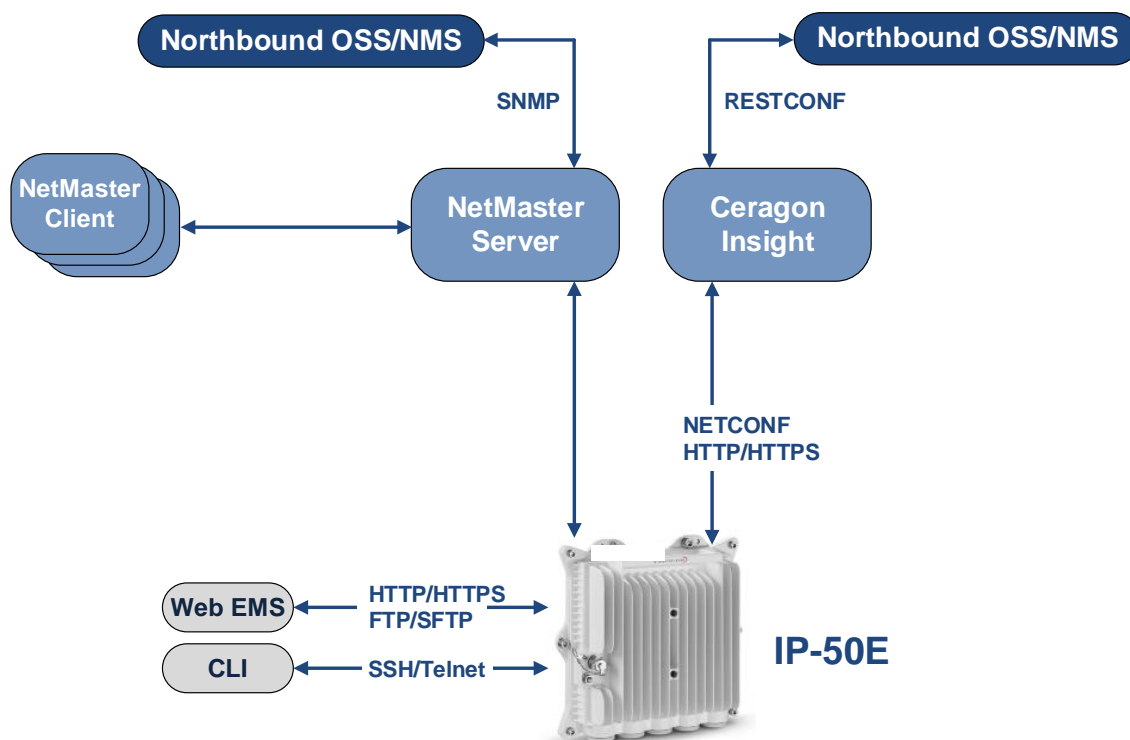


Figure 51: Integrated Management Tools

## 5.2 Automatic Network Topology Discovery with LLDP Protocol

IP-50E supports the Link Layer Discovery Protocol (LLDP), a vendor-neutral layer 2 protocol that can be used by a station attached to a specific LAN segment to advertise its identity and capabilities and to receive identity and capacity information from physically adjacent layer 2 peers. IP-50E's LLDP implementation is based on the IEEE 802.1AB – 2009 standard.

LLDP provides automatic network connectivity discovery by means of a port identity information exchange between each port and its peer. The port exchanges information with its peer and advertises this information to the NMS managing the unit. This enables the NMS to quickly identify changes to the network topology.

Enabling LLDP on IP-50EX units enables the NMS to:

- Automatically detect the IP-50EX unit neighboring the managed IP-50EX unit, and determine the connectivity state between the two units.
- Automatically detect a third-party switch or router neighboring the managed IP-50EX unit, and determine the connectivity state between the IP-50EX unit and the switch or router.

### 5.3 Management Communication Channels and Protocols

#### Related Topics:

- Secure Communication Channels

Network Elements can be accessed locally via serial or Ethernet management interfaces, or remotely through the standard Ethernet LAN. The application layer is indifferent to the access channel used.

The NMS can be accessed through its GUI interface application, which may run locally or in a separate platform; it also has an SNMP-based northbound interface to communicate with other management systems.

*Table 21: Dedicated Management Ports*

Port number	Protocol	Frame structure	Details
161	SNMP	UDP	Sends SNMP Requests to the network elements
162 Configurable	SNMP (traps)	UDP	Sends SNMP traps forwarding (optional)
514	Syslog	UDP	Sends Syslog messages (optional)
80	HTTP	TCP	Manages devices <b>Note:</b> When HTTPS is used, users can configure Port 80 to be closed and traffic redirected to Port 443.
443	HTTPS	TCP	Manages devices (optional)
From port 21 (default) to any remote port (>1023). Initial port (21) is configurable.	FTP Control Port	TCP	Downloads software and configuration files, uploads security and configuration logs, and unit info files. (FTP Server responds to client's control port) (optional)
From Any port (>1023) to any remote port (>1023)	FTP Data Port	TCP	Downloads software and configuration files, uploads security and configuration logs, and unit info files. The FTP server sends ACKs (and data) to client's data port.
From port 22 (default) to any remote port (>1023). Initial port (22) is configurable.	SFTP Control Port	TCP	Downloads software and configuration files, and CSR certificates, uploads security and configuration logs, and unit info files. (SFTP Server responds to client's control port) (optional)
From Any port (>1023) to any remote port (>1023)	SFTP Data Port	TCP	Downloads software and configuration files, and CSR certificates, uploads security and configuration logs, and unit info files. The SFTP server sends ACKs (and data) to client's data port.

Port number	Protocol	Frame structure	Details
23	telnet	TCP	Remote CLI access (optional)
22	SSH	TCP	Secure remote CLI access (optional)

All remote system management is carried out through standard IP communications. Each NE behaves as a host with a single IP address.

The communications protocol used depends on the management channel being accessed.

As a baseline, these are the protocols in use:

- Standard HTTP for web-based management
- Standard telnet for CLI-based management

## 5.4 Web-Based Element Management System (Web EMS)

The CeraWeb Element Management System (Web EMS) is an HTTP web-based element manager that enables the operator to perform configuration operations and obtain statistical and performance information related to the system, including:

- **Configuration Management** – Enables you to view and define configuration data for the IP-50EX system.
- **Fault Monitoring** – Enables you to view active alarms.
- **Performance Monitoring** – Enables you to view and clear performance monitoring values and counters.
- **Diagnostics and Maintenance** – Enables you to define and perform loopback tests, and software updates.
- **Security Configuration** – Enables you to configure IP-50EX security features.
- **User Management** – Enables you to define users and user profiles.

A Web-Based EMS connection to the IP-50EX can be opened using an HTTP Browser (Explorer or Mozilla Firefox). The Web EMS uses a graphical interface. Most system configurations and statuses are available via the Web EMS. However, some advanced configuration options are only available via CLI.

The Web EMS shows the actual unit configuration and provides easy access to any interface on the unit. The Web EMS opens to a Unit Summary page that displays the key unit parameters on a single page for quick viewing. The next page in the Web EMS, easily accessible from the root directory, is the Link Summary page, which provides a graphical representation of the link and enables to easily display and configure the radio parameters on both the local and the remote device.

<b>Note:</b>	For optimal Web EMS performance, it is recommended to ensure that the network speed is at least 100 Kbps for most operations, and at least 5 Mbps for software download operations.
--------------	---

The Web EMS includes a Quick Platform Setup page designed to simplify initial configuration and minimize the time it takes to configure a working link.

The Web EMS also includes quick link configuration wizards that guide the user, step-by-step, through the creation of 1+0 links with point-to-point services.

With respect to system security, the Web EMS includes two features to facilitate monitoring and configuring security-related parameters.

To configure security-related features, the Web EMS gathers several pages under the Quick Configuration portion of the Web EMS main menu. Users can configure the following parameters from these pages:

- Import and export security settings
- Session timeout
- Login banner

- AES-GCM-256 payload encryption<sup>11</sup>
- HTTP or HTTPS
- Telnet access
- SNMP parameters
- Users and user profiles
- Login and password parameters
- RSA public key configuration
- Certificate Signing Request (CSR) file download and install

The Web EMS also includes a Security Summary page that gathers a number of important security-related parameters in a single page for quick viewing. The Security Summary page can be displayed from the root of the Web EMS main menu.

The Security Summary page includes:

- FIPS Admin status
- Session Timeout
- Login Banner
- AES-GCM-256 payload encryption status<sup>11</sup>
- HTTP/HTTPS configuration
- Telnet access status (enabled/disabled)
- SNMP parameters
- Login and password security parameters
- Users and their parameters
- Public RSA key currently configured on the device

Users can toggle between the following menu structure options:

- **Advanced** – Advanced mode includes all available Web EMS options, including both basic link and configuration and advanced configuration such as QoS and Ethernet protocols.
- **Basic** – Basic mode provides a condensed set of menu options that cover most or all of the configurations necessary to set up and maintain an IP-50 unit, including link configuration wizards for most link types. The purpose of Basic mode is to provide the average user with a menu tree that is simple to navigate yet includes most or all options that most users need.

Users can toggle between Advanced or Basic mode by clicking **Advanced** and **Basic** in the upper left corner or any page in the Web EMS. The default mode is **Advanced** mode.

---

<sup>11</sup> Requires IP-50EX-P.



## 5.5 SDN Support

IP-50EX supports SDN, with NETCONF/YANG capabilities.

SDN (Software-Defined Networking) is a comprehensive, software-centric approach to networking that makes network planning and management more flexible, efficient, and effective in many ways

IP-50EX's SDN implementation is a key part of Ceragon's vision for evolving wireless backhaul towards SDN via open architecture based on standard Northbound and Southbound interfaces. This vision includes innovative SDN solutions for dynamic network performance and resource optimization, and SDN-based backhaul network provisioning, monitoring, and self-healing.

SDN provides a full portfolio of network and network element management capabilities, including

- Topology auto discovery
- Performance monitoring
- Fault Management
- Alarms and events

IP-50EX's NETCONF and YANG implementation includes the following main standard interfaces, protocols, and data models:

- NETCONF RFC 6241
- Support for get/get-config/edit/copy/delete
- YANG RFC 6020
- YANG data models:
  - ONF Core Model v1.4
  - AirInterface v2.0 – openBackhaul.com proposal to Open Networking Foundation (ONF)
  - WireInterface v2.0 – openBackhaul.com proposal to Open Networking Foundation (ONF)
  - PureEthernetStructure v2.0 – openBackhaul.com proposal to Open Networking Foundation (ONF)
  - EthernetContainer v2.0 – openBackhaul.com proposal to Open Networking Foundation (ONF)
  - Adds support for alarms v1.0 – openBackhaul.com proposal to Open Networking Foundation (ONF)
  - Adds support for firmware v1.0 – openBackhaul.com proposal to Open Networking Foundation (ONF)

SDN provides significant benefits to network operators, including:

- Improving time-to-market and increasing network planning flexibility by enabling easy connection and integration with legacy devices from multiple vendors.
- High performance and resiliency due to the availability of plug-in applications and SDN's intrinsic design for resiliency and availability.
- Lower CAPEX and OPEX resulting from self-defined scripts, quicker introduction of new services, and fast troubleshooting.

For additional information, refer to the *NETCONF Reference Guide for IP-20 and IP-50 Products*.

## 5.6 Command Line Interface (CLI)

A CLI connection to the IP-50EX can be opened via SSH or telnet. All parameter configurations can be performed via CLI.

**Note:** Telnet is disabled by default and must be enabled by user configuration. Therefore, if initial access to the device is via CLI, the user must use a terminal connection or SSH.

## 5.7 Configuration Management

The system configuration file consists of a set of all the configurable system parameters and their current values.

IP-50EX configuration files can be imported and exported. This enables you to copy the system configuration to multiple IP-50EX units.

System configuration files consist of a zip file that contains three components:

- A binary configuration file which is used by the system to restore the configuration.
- A text file which enables users to examine the system configuration in a readable format. The file includes the value of all system parameters at the time of creation of the backup file.
- An additional text file which enables users to write CLI scripts in order to make desired changes in the backed-up configuration. This file is executed by the system after restoring the configuration.

The system provides three restore points to manage different configuration files. Each restore point contains a single configuration file. Files can be added to restore points by creating backups of the current system state or by importing them from an external server.

**Note:** In the Web EMS, these restore points are referred to as “file numbers.”

For example, a user may want to use one restore point to keep a last good configuration, another to import changes from an external server, and the third to store the current configuration.

Any of the restore points can be used to apply a configuration file to the system.

The user can determine whether or not to include security-related settings, such as users and user profiles, in the exported configuration file. By default, security settings are included.

## 5.8 Software Management

The IP-50EX software installation and upgrade process includes the following steps:

- **Download** – The files required for the installation or upgrade are downloaded from a remote server.
- **Installation** – The files are installed in the appropriate modules and components of the IP-50EX.
- **Reset** – The IP-50EX is restarted in order to boot the new software and firmware versions.

IP-50EX software and firmware releases are provided in a single bundle that includes software and firmware for all components supported by the system. When the user downloads a software bundle, the system verifies the validity of the bundle. The system also compares the files in the bundle to the files currently installed in the IP-50EX and its components, so that only files that differ between the new version bundle and the current version in the system are actually downloaded. A message is displayed to the user for each file that is actually downloaded.

**Note:** When downloading an older version, all files in the bundle may be downloaded, including files that are already installed.

Software bundles can be downloaded via FTP, SFTP, HTTP, or HTTPS. When downloading software via HTTP or HTTPS, the IP-50EX unit acts as an HTTP server, and the software can be downloaded directly to the unit. When downloading software via FTP or SFTP, the IP-50EX functions as an FTP or SFTP client, and FTP or SFTP server software must be installed on the PC or laptop being using to perform the upgrade.

After the software download is complete, the user initiates the installation. A timer can be used to perform the installation after a defined time interval. The system performs an automatic reset after the installation.

## 5.9 Using Pre-Defined Configuration Files

**Note:** Pre-defined configuration files are planned for future release.

IP-50EX units can be configured from the Web EMS in a single step by applying a pre-defined configuration file. This drastically reduces the initial installation and setup time in the field.

Using pre-defined configuration files also reduces the risk of configuration errors and enables operators to invest less time and money training installation personnel. Installers can focus on hardware configuration, relying on the pre-defined configuration file to implement the proper software configuration on each device.

***The pre-defined configuration file can be generated by Ceragon Professional Services and provided as a service.***

A pre-defined configuration file can be prepared for multiple IP-50EX units, with the relevant configuration details specified and differentiated per-unit. This simplifies administration, since a single file can be used with multiple devices.

Pre-defined configuration files can include all the parameters necessary to configure basic links, including:

- Activation Key (or Demo mode) configuration
- Radio Parameters
- Interface Groups (e.g., LAG)
- Management Service

All configurations that can be implemented via the Web EMS Quick Configuration wizards can also be configured using pre-defined configuration files.

Pre-defined configuration files can be created by Ceragon Professional Services, according to customer specifications. For further information, consult your Ceragon representative.

## 5.10 IPv6 Support

IP-50E management communications can use both IPv4 and IPv6. The unit IP address for management can be configured in either or both formats.

Additionally, other management communications can utilize either IPv4 or IPv6. This includes:

- Software file downloads
- Configuration file import and export
- Trap forwarding
- Unit information file export (used primarily for maintenance and troubleshooting)

Dynamic IPv6 configuration is supported via DHCPv6. When enabled, devices can obtain their IPv6 address automatically via DHCPv6.

## 5.11 In-Band Management

IP-50EX can optionally be managed In-Band, via its radio and Ethernet interfaces. This method of management eliminates the need for a dedicated management interface. For more information, refer to *Management Service (MNG)* on page 57.

## 5.12 Local Management

IP-50EX includes an electrical GbE management port.

## 5.13 Alarms

### 5.13.1 Configurable BER Threshold for Alarms and Traps

Users can configure alarm and trap generation in the event of Excessive BER and Signal Degrade BER above user-defined thresholds. Users have the option to configure whether or not excessive BER is propagated as a fault and considered a system event.

### 5.13.2 RSL Threshold Alarm

Users can configure an alarm that is raised if the RSL falls beneath a user-defined threshold. This feature can be enabled or disabled per radio carrier. By default, it is disabled. The RSL threshold alarm provides a preventative maintenance tool for monitoring the health of the link and ensuring that problems can be identified and corrected quickly.

### 5.13.3 Editing and Disabling Alarms and Events

Users can change the description text (by appending extra text to the existing description) or the severity of any alarm in the system. Users can also choose to disable specific alarms and events. Any alarm or event can be disabled, so that no indication of the alarm or event is displayed, and no traps are sent for the alarm or event.

This is performed as follows:

- Each alarm and event in the system is identified by a unique name (see separate list of system alarms and events).
- The user can perform the following operations on any alarm:
  - View current description and severity
  - Define the text to be appended to the description and/or severity
  - Return the alarm to its default values
  - Disable or re-enable the alarm (or event)
- The user can also return all alarms and events to their default values.

### 5.13.4 Timeout for Trap Generation

Users can configure a wait time of 0 to 120 seconds after an alarm is cleared in the system before the alarm is actually reported as being cleared. This prevents traps flooding the NMS in the event that some external condition causes the alarm to be raised and cleared continuously.

This means that when the alarm is cleared, the alarm continues to be displayed and no *clear alarm* trap is sent until the timeout period is finished.

The timeout for trap generation can be configured via CLI. By default, the timeout is 10 seconds.

## 5.14 NTP Support

### Related topics:

- Synchronization

---

IP-50EX supports Network Time Protocol (NTP). NTP distributes Coordinated Universal Time (UTC) throughout the system, using a jitter buffer to neutralize the effects of variable latency.

Users can configure up to four NTP servers. Each server can be configured using IPv4 or IPv6. When multiple servers are configured, the unit chooses the best server according to the implementation of Version 4.2.6p1 of the NTPD (Network Time Protocol Daemon). The servers are continually polled. The polling interval is determined by the NTPD, to achieve maximum accuracy consistent with minimum network overhead.

IP-50EX supports NTPv3 and NTPv4. NTPv4 provides interoperability with NTPv3 and with SNTP.

Optionally, NTP authentication is available, as defined in the NTP specification (IETF RFC 5905). NTP authentication enables the client to verify the authenticity of the NTP server before synchronizing its clock with the server's time. This can help prevent man-in-the-middle attacks and other types of threats that could manipulate the client's clock by providing it with false time information.

## 5.15 UTC Support

IP-50EX uses the Coordinated Universal Time (UTC) standard for time and date configuration. UTC is a more updated and accurate method of date coordination than the earlier date standard, Greenwich Mean Time (GMT).

Every IP-50EX unit holds the UTC offset and daylight savings time information for the location of the unit. Each management unit presenting the information (CLI and Web EMS) uses its own UTC offset to present the information in the correct time.



## 5.16 Syslog Support

Syslog can be used to send Security Log, Event Log, and Configuration Log messages to up to two external Syslog servers. This can simplify network monitoring and maintenance for operators by enabling them to centralize troubleshooting and monitoring information for multiple network elements in a single location.

Syslog uses UDP protocol on port 514.

Optionally, for extra security you can enable TLS-based Secure Syslog. This enables server authentication, which means the client authenticates the Syslog server. This provides an extra layer of protection against various types of security threats, including masquerade, modification, and disclosure threats.

When Secure Syslog is enabled, the device uses the TCP port (6514) for Syslog messages.

**Note:** Secure Syslog requires that the server support TLS 1.2 or higher.

## 5.17 System Security Features

To guarantee proper performance and availability of a network as well as the data integrity of the traffic, it is imperative to protect it from all potential threats, both internal (misuse by operators and administrators) and external (attacks originating outside the network).

System security is based on making attacks difficult (in the sense that the effort required to carry them out is not worth the possible gain) by putting technical and operational barriers in every layer along the way, from the access outside the network, through the authentication process, up to every data link in the network.

### 5.17.1 Ceragon's Layered Security Concept

Each layer protects against one or more threats. However, it is the combination of them that provides adequate protection to the network. In most cases, no single layer protection provides a complete solution to threats.

The layered security concept is presented in the following figure. Each layer presents the security features and the threats addressed by it. Unless stated otherwise, requirements refer to both network elements and the NMS.

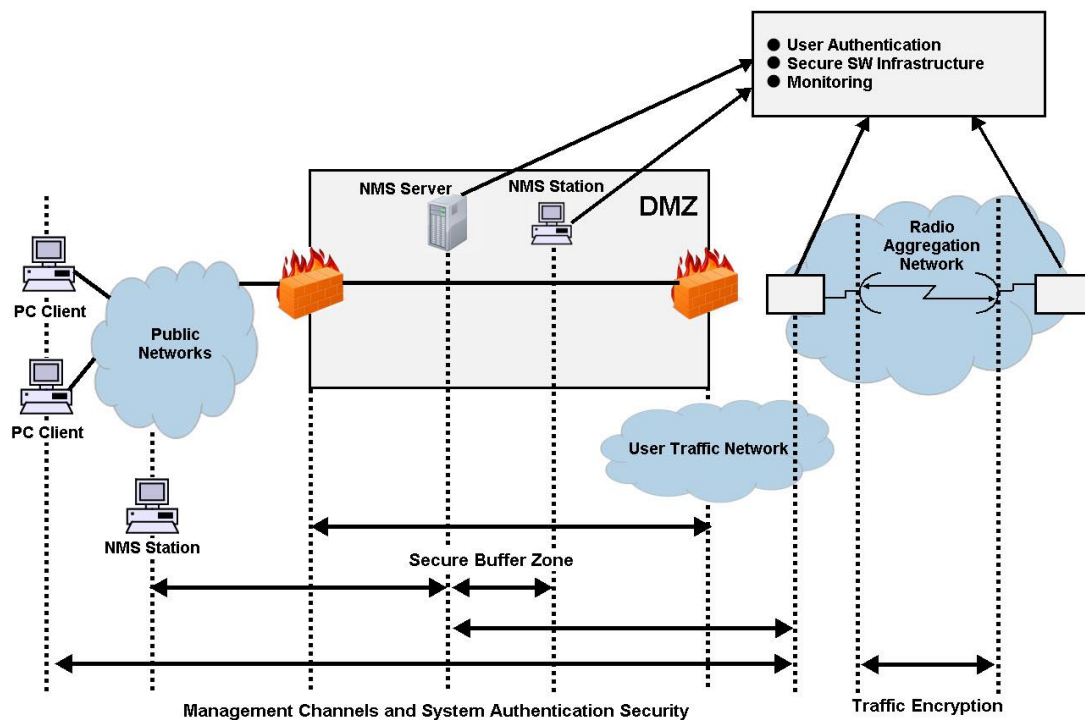


Figure 52: Security Solution Architecture Concept

### 5.17.2 Defenses in Management Communication Channels

Since network equipment can be managed from any location, it is necessary to protect the communication channels' contents end to end.

These defenses are based on existing and proven cryptographic techniques and libraries, thus providing standard secure means to manage the network, with minimal impact on usability.

They provide defense at any point (including public networks and radio aggregation networks) of communications.

While these features are implemented in Ceragon equipment, it is the responsibility of the operator to have the proper capabilities in any external devices used to manage the network.

In addition, inside Ceragon networking equipment it is possible to control physical channels used for management. This can greatly help deal with all sorts of DoS attacks.

Operators can use secure channels instead or in addition to the existing management channels:

- SNMPv3 for all SNMP-based protocols for both NEs and NMS
- HTTPS for access to the NE's web server
- SSH-2 for all CLI access SFTP for all software and configuration download between NMS and NEs

All protocols run with secure settings using strong encryption techniques. Unencrypted modes are not allowed, and algorithms used must meet modern and client standards.

Users are allowed to disable all insecure channels.

In the network elements, the bandwidth of physical channels transporting management communications is limited to the appropriate magnitude, in particular, channels carrying management frames to the CPU.

#### **Attack types addressed**

- Tempering with management flows
- Management traffic analysis
- Unauthorized software installation
- Attacks on protocols (by providing secrecy and integrity to messages)
- Traffic interfaces eavesdropping (by making it harder to change configuration)
- DoS through flooding

### 5.17.3 Defenses in User and System Authentication Procedures

#### 5.17.3.1 User Configuration and User Profiles

User configuration is based on the Role-Based Access Control (RBAC) model. According to the RBAC model, permissions to perform certain operations are assigned to specific roles. Users are assigned to particular roles, and through those role assignments acquire the permissions to perform particular system functions.

In the IP-50EX GUI, these roles are called user profiles. Up to 50 user profiles can be configured. Each profile contains a set of privilege levels per functionality group, and defines the management protocols (access channels) that can be used to access the system by users to whom the user profile is assigned.

The system parameters are divided into the following functional groups:

- Security
- Management
- Radio
- Ethernet
- Synchronization

A user profile defines the permitted access level per functionality group. For each functionality group, the access level is defined separately for read and write operations. The following access levels can be assigned:

- **None** – No access to this functional group.
- **Normal** – The user has access to parameters that require basic knowledge about the functional group.
- **Advance** – The user has access to parameters that require advanced knowledge about the functional group, as well as parameters that have a significant impact on the system as a whole, such as restoring the configuration to factory default settings.

### 5.17.3.2 User Identification

IP-50EX supports the following user identification features:

- Configurable inactivity time-out for automatically closing unused management channels
- Optional password strength enforcement. When password strength enforcement is enabled; passwords must comply with the following rules:
  - Password must be at least eight characters long.
  - Password must include characters of at least three of the following character types: lower case letters, upper case letters, digits, and special characters.
  - No character can be repeated three times, e.g., aaa, ###, 333.
  - No more than two consecutive characters can be used, e.g., ABC, DEF, 123.
  - The user name string cannot appear in the password, either in order or in reverse order. For example, if the user name is “admin”, neither of the following passwords are allowed: %Asreadmin!df23 and %Asrenimda!df23.
- Password reuse can be configured so that up to ten previous passwords cannot be reused.
- Users can be prompted to change passwords after a configurable amount of time (password aging).
- Users can be blocked for a configurable time period after a configurable number of unsuccessful login attempts.
- Users can be configured to expire at a certain date
- Mandatory change of password at first time login can be enabled and disabled upon user configuration. It is enabled by default.
- SHA-512 is used to encrypt user passwords.

### 5.17.3.3 Remote Authentication

Certificate-based strong standard encryption techniques are used for remote authentication. Users may choose to use this feature or not for all secure communication channels.

Since different operators may have different certificate-based authentication policies (for example, issuing its own certificates vs. using an external CA or allowing the NMS system to be a CA), NEs and NMS software provide the tools required for operators to enforce their policy and create certificates according to their established processes.

Server authentication capabilities are provided.

#### 5.17.3.4 RADIUS Support

The RADIUS protocol provides centralized user management services. IP-50EX supports RADIUS server and provides a RADIUS client for authentication and authorization.

RADIUS can be enabled or disabled. When RADIUS is enabled, a user attempting to log into the system from any access channel (CLI, WEB, NMS) is not authenticated locally. Instead, the user's credentials are sent to a centralized standard RADIUS server which indicates to the IP-50EX whether the user is known, and which privilege is to be given to the user. RADIUS uses the same user attributes and privileges defined for the user locally.

**Note:** When using RADIUS for user authentication and authorization, the access channels configured per IP-50EX user profile are not applicable. Instead, the access channels must be configured as part of the RADIUS server configuration.

RADIUS login works as follows:

- If the RADIUS server is reachable, the system expects authorization to be received from the server:
  - The server sends the appropriate user privilege to the IP-50EX, or notifies the IP-50EX that the user was rejected.
  - If rejected, the user will be unable to log in. Otherwise, the user will log in with the appropriate privilege and will continue to operate normally.
- If the RADIUS server is unavailable, the IP-50EX will attempt to authenticate the user locally, according to the existing list of defined users.

**Note:** Local login authentication is provided in order to enable users to manage the system in the event that RADIUS server is unavailable. This requires previous definition of users in the system. If the user is only defined in the RADIUS server, the user will be unable to login locally in case the RADIUS server is unavailable.

In order to support IP-50EX - specific privilege levels, the vendor-specific field is used. Ceragon's IANA number for this field is 2281.

The following RADIUS servers are supported:

- FreeRADIUS
- RADIUS on Windows Server (IAS)
  - Windows Server 2008
  - Windows Server 2003
- Cisco ACS

#### 5.17.3.5 TACACS+ Support

IP-50EX supports TACACS+ for remote access user authentication, authorization, and accounting. Using TACACS+, the IP-50 device acts as the client, working with a TACACS+ server to authenticate and authorize users.

The TACACS+ protocol provides centralized user management services. TACACS+ separates the functions of Authentication, Authorization, and Accounting (AAA). It

enables arbitrary length and content authentication exchanges, in order to support future authentication mechanisms. It is extensible to provide for site customization and future development features, and uses TCP to ensure reliable communication.

**Note:** IP-50 supports session-based TACACS+ authorization, but not command-based.

When TACACS+ is enabled, a user attempting to log into the system from any access channel (CLI, WEB, NMS) is not authenticated locally. Instead, the user's credentials are sent to a centralized standard TACACS+ server which indicates to the IP-50 device whether the user is known, and which privilege is to be given to the user.

When a user successfully logs in or logs out of an IP-50 device via TACACS+, the device sends an accounting packet to the TACACS+ server packet which contains the following information:

- User Name
- User IP Address
- Time and Date of Connection
- Connection port on the device

**Note:** This information is also written to the device's Security Log.

Ceragon's TACACS+ solution is compliant with any standard TACACS+ server. Testing has been performed, and interoperability confirmed, with the following TACACS+ servers:

- Cisco ISE - Version 2.6.0.156
- Tacacs.net - Version 1.2
- tac\_plus version F4.0.4.27a

Up to four TACACS+ servers can be defined to work with an IP-50 device. When a user attempts to log into the device, the device attempts to contact the first TACACS+ server to authenticate the user. If no response is received from the server within the user-defined timeout period, the device tries again to contact the server up to the user-configured number of retries. Then, if no response is received from the server, the device attempts to contact the second user-defined TACACS+ server. If no response is received from any of the servers, the device performs user authentication locally.

#### 5.17.4 Secure Communication Channels

IP-50EX supports a variety of standard encryption protocols and algorithms, as described in the following sections.

##### 5.17.4.1 SSH (Secured Shell)

SSH protocol can be used as a secured alternative to Telnet. In IP-50EX:

- SSHv2 is supported.
- SSH protocol will always be operational. Admin users can choose whether to enable Telnet protocol, which is disabled by default. Server authentication is based on IP-50EX's public key.
- RSA and DSA key types are supported.
- MAC (Message Authentication Code): SHA-1-96 (MAC length = 96 bits, key length = 160 bit). Supported MAC: hmac-md5, hmac-sha1, hmac-ripemd160, hmac-sha1-96, hmac-md5-96'
- The server authenticates the user based on user name and password. The number of failed authentication attempts is not limited.
- The server timeout for authentication is 10 minutes. This value cannot be changed.

##### 5.17.4.2 HTTPS (Hypertext Transfer Protocol Secure)

HTTPS combines the Hypertext Transfer protocol with the TLS (1.0, 1.1, 1.2, 1.3) protocol to provide encrypted communication and secure identification of a network web server. IP-50EX enables administrators to configure secure access via HTTPS protocol.

For a list of supported HTTPS ciphers, including an indication of which ciphers are supported in HTTPS strong mode, see *Annex A – Supported Ciphers for Secured Communication Protocols* in the Release Notes for the CeraOS version you are using. From CeraOS 12.0, all supported HTTPS ciphers are also supported in FIPS mode.

##### 5.17.4.3 SFTP (Secure FTP)

SFTP can be used for the following operations:

- Configuration upload and download,
- Uploading unit information
- Uploading a public key
- Downloading certificate files
- Downloading software



#### 5.17.4.4 Creation of Certificate Signing Request (CSR) File

In order to create a digital certificate for the NE, a Certificate Signing Request (CSR) file should be created by the NE. The CSR contains information that will be included in the NE's certificate such as the organization name, common name (domain name), locality, and country. It also contains the public key that will be included in the certificate. Certificate authority (CA) will use the CSR to create the desired certificate for the NE.

While creating the CSR file, the user will be asked to input the following parameters that should be known to the operator who applies the command:

- **Common name** – The identify name of the element in the network (e.g., the IP address). The common name can be a network IP or the FQDN of the element.
- **Organization** – The legal name of the organization.
- **Organizational Unit** - The division of the organization handling the certificate.
- **City/Locality** - The city where the organization is located.
- **State/County/Region** - The state/region where the organization is located.
- **Country** - The two-letter ISO code for the country where the organization is location.
- **Email address** - An email address used to contact the organization.

#### 5.17.4.5 RSA Keys

IP-50 devices support RSA keys for communication using HTTPS and SSH protocol. The IP-50 device comes with randomly generated private and public RSA keys. However, customers can replace the private/public key pair with customer-defined private key. The corresponding RSA public key will be generated based on this private keys. The file must be in PEM format. Supported RSA private key sizes are 2048, 4096, and 8192. The customer-defined private key can be downloaded to the device via HTTPS or SFTP. It is recommended to use HTTPS.

#### 5.17.4.6 SNMP

IP-50EX supports SNMP v1, V2c, and v3. The default community string in NMS and the SNMP agent in the embedded SW are disabled. Users are allowed to set community strings for access to network elements.

IP-50EX supports the following MIBs:

- RFC-1213 (MIB II)
- RMON MIB
- Ceragon (proprietary) MIB.

Access to all network elements in a node is provided by making use of the community and context fields in SNMPv1 and SNMPv2c/SNMPv3, respectively.

#### 5.17.4.7 Server Authentication (TLS 1.0, 1.1, 1.2, 1.3)

- All protocols making use of SSL (such as HTTPS) use TLS (1.0, 1.1, 1.2, 1.3) and support X.509 certificates-based server authentication.
- Users with type of “administrator” or above can perform the following server (network element) authentication operations for certificates handling:
  - Generate server key pairs (private + public)
  - Export public key (as a file to a user-specified address)
  - Install third-party certificates
    - The Admin user is responsible for obtaining a valid certificate.
  - Load a server RSA key pair that was generated externally for use by protocols making use of SSL.
- Non-SSL protocols using asymmetric encryption, such as SSH and SFTP, can make use of public-key based authentication.
  - Users can load trusted public keys for this purpose.

#### 5.17.4.8 Encryption

- Encryption algorithms for secure management protocols include:
  - Symmetric key algorithms: 128-bit AES
  - Asymmetric key algorithms: 1024-bit RSA

### 5.17.5 Security Log

The security log is an internal system file which records all changes performed to any security feature, as well as all security related events.

**Note:** In order to read the security log, the user must upload the log to his or her server.

The security log file has the following attributes:

- The file is of a “cyclic” nature (fixed size, newest events overwrite oldest).
- The log can only be read by users with "admin" or above privilege.
- The contents of the log file are cryptographically protected and digitally signed.
  - In the event of an attempt to modify the file, an alarm will be raised.
- Users may not overwrite, delete, or modify the log file.

The security log records:

- Changes in security configuration
  - Carrying out “security configuration copy-to-mate”
  - Management channels time-out
  - Password aging time
  - Number of unsuccessful login attempts for user suspension
  - Warning banner change
  - Adding/deleting of users
  - Password changed
  - SNMP enable/disable
  - SNMP version used (v1/v3) change
  - SNMPv3 parameters change
    - ☐ Security mode
    - ☐ Authentication algorithm
    - ☐ User
    - ☐ Password
  - SNMPv1 parameters change
    - ☐ Read community
    - ☐ Write community
    - ☐ Trap community for any manager
  - HTTP/HTTPS change
  - FTP/SFTP change
  - Telnet and web interface enable/disable
  - FTP enable/disable
  - Loading certificates
  - RADIUS server
  - Radius enable/disable

- TACACS+ server
- TACACS+ enable/disable
- Remote logging enable/disable (for security and configuration logs)
- System clock change
- NTP enable/disable
- Security events
- Successful and unsuccessful login attempts
- N consecutive unsuccessful login attempts (blocking)
- Configuration change failure due to insufficient permissions
- SNMPv3/PV authentication failures
- User logout
- User account expired

For each recorded event the following information is available:

- User ID
- Communication channel (WEB, terminal, telnet/SSH, SNMP, NMS, etc.)
- IP address, if applicable
- Date and time

#### 5.17.6 Access Control Lists

Access control lists enable operators to define rules to limit management traffic, i.e., traffic destined to the logical management interface. This includes both in-band and out-of-band management traffic. These rules are added to an access control list. IP-50 devices maintain separate access control lists for IPv4 addresses and IPv6 addresses. Each list can include up to 40 rules.

Access control rules can be based on the following criteria:

- Source IP address
- Network subnet prefix length
- Protocol type
- Destination port

Each rule is either an “accept” rule or a “drop” rule. By using combinations of accept and drop rules, operators can ensure that only certain traffic is permitted to ingress the management interface. Traffic received by the logical management interface is checked against the rules in the access control list in the order of priority configured by the user, from highest priority to lowest priority. Once a matching rule is found, the rule is applied to accept or drop the packet, and the checking stops for that packet.

## 6. Standards and Certifications

**This chapter includes:**

- Supported Ethernet Standards
- MEF Specifications for Ethernet Services

## 6.1 Supported Ethernet Standards

*Table 22: Supported Ethernet Standards*

Standard	Description
802.3	10base-T, 100base-T, 1000base-T, 1000base-X, 10GBase-LR
802.3ac	Ethernet VLANs
802.1Q	Virtual LAN (VLAN)
802.1p	Class of service
802.1ad	Provider bridges (QinQ)
802.1AX	Link aggregation
Auto MDI/MDIX for 1000baseT	
RFC 1349	IPv4 TOS
RFC 2474	IPv4 DSCP
RFC 2460	IPv6 Traffic Classes

## 6.2 MEF Specifications for Ethernet Services

IP-50EX supports the specifications listed in the following table.

*Table 23: Supported MEF Specifications*

Specification	Description
MEF-2	Requirements and Framework for Ethernet Service Protection
MEF-6.1	Metro Ethernet Services Definitions Phase 2
MEF-10.3	Ethernet Services Attributes Phase 3
MEF 22.1	Mobile Backhaul Implementation Agreement Phase 2
MEF-30.1	Service OAM Fault Management Implementation Agreement Phase 2
MEF-35	Service OAM Performance Monitoring Implementation Agreement
CE 2.0	Second generation Carrier Ethernet certification
MEF-9	Abstract Test Suite for Ethernet Services at the UNI. Certified for all service types (EPL, EVPL & E-LAN).  This is a first generation certification. It is fully covered as part of CE2.0)
MEF-14	Abstract Test Suite for Traffic Management Phase 1. Certified for all service types (EPL, EVPL & E-LAN).  This is a first generation certification. It is fully covered as part of CE2.0)

## 7. Specifications

### This chapter includes:

- General Radio Specifications
- Radio Scripts
- Radio Capacity Specifications
- Transmit Power Specifications
- Receiver Threshold Specifications
- Mediation Device Losses
- Ethernet Latency Specifications
- Interface Specifications
- Carrier Ethernet Functionality
- Synchronization Protocols
- Network Management, Diagnostics, Status, and Alarms
- Mechanical Specifications
- Standards Compliance
- Environmental Specifications
- Antenna Interface Specifications
- Integrated Antenna
- Power Input Specifications

### 7.1 PoE Port Specifications (IP-50EX-P only)

The IP-50EX-P PoE port (P2) is compliant with IEEE802.3bt Class 8 Endpoint PSE.

The maximum supported cable length is 100m using Cat5e or Cat6 cables.

DC Input range	-40.5 to -60 VDC
----------------	------------------

- Power Consumption Specifications
- Cable Specifications

### Related Topics:

- Standards and Certifications

**Note:** All specifications are subject to change without prior notification.



## 7.2 General Radio Specifications

Specification	Description
Radio Standards	ETSI: EN 302 217 FCC: Part 101 (2004) ITU-R F.2006 (03/2012) CEPT ECC/REC/(05)07
Operating mode	FDD
System Configurations	1+0
Operating Frequency Range	71-76GHz, 81-86GHz
Channel Bandwidth	250, 500, 1000, 2000 MHz
Frequency Stability	±5ppm
Channel Allocation	According to Recommendation ITU-R F.2006 (03/2012), ECC RECOMMENDATION (05)07 or FCC CFR 47 Part 101

*Table 24: Frequency Tuning Range:*

Low Range [MHz]	High Range [MHz]	TX-RX Separation [MHz]	Low BW [MHz]	High BW [MHz]
71,000 - 76000	81,000 – 86,000	10,000	5000	5000

### 7.3 Radio Scripts

*Table 25: Radio Scripts*

Script ID	ETSI/FCC	Channel BW	Occupied BW	XPIC	Maximum Profile (ACM)	Maximum Profile (Fixed)
Script ID	ETSI/FCC	Channel BW	Occupied BW	XPIC	Maximum Profile (ACM)	Maximum Profile (Fixed)
5803	ETSI/FCC	250 MHz	230 MHz	No	512 QAM	512 QAM
5853	ETSI/FCC	250 MHz	230 MHz	Yes	512 QAM	512 QAM
5804	ETSI/FCC	500 MHz	460 MHz	No	512 QAM	32 QAM
5854	ETSI/FCC	500 MHz	460 MHz	Yes	512 QAM	32 QAM
5806	ETSI/FCC	1000 MHz	880 MHz	No	256 QAM	32 QAM
5856	ETSI/FCC	1000 MHz	880 MHz	Yes	256 QAM	32 QAM
5810	ETSI/FCC	2000 MHz	1599 MHz	No	128 QAM	32 QAM
5860	ETSI/FCC	2000 MHz	1599 MHz	Yes	128 QAM	32 QAM

## 7.4 Radio Capacity Specifications

**Note:** The figures in this section are indicative only. Exact results will depend on multiple factors, such as packet size, type of traffic, headers, etc.

The capacity figures for LTE scenario take into account packets encapsulated inside GTP tunnels with IPv4/UDP encapsulation and double VLAN tagging (QinQ).

The minimum and maximum capacity is based on Ethernet frame sizes between 64 and 1518 bytes.

When AES-GCM-256 Payload Encryption is enabled, throughput is reduced.

*Table 26: Radio Capacity – 250 MHz Channel Bandwidth (Script 5803)*

Profile	Modulation	Minimum Required Capacity Activation Key (Gbps)	Throughput (Mbps)
0	BPSK <sup>12</sup>	50	48-59
1	BPSK <sup>13</sup>	100	96-117
2	BPSK	200	192-235
3	QPSK	400	386-471
4	8 PSK	650	579-707
5	16 QAM	1000	772-944
6	32 QAM	1000	1159-1416
7	64 QAM	1600	1159-1416
8	128 QAM	1600	1352-1652
9	256 QAM	1600	1545-1889
10	512 QAM	2000	1738-2125

<sup>12</sup> Profile 0 is BPSK at  $\frac{1}{4}$  of the script's normal channel bandwidth.

<sup>13</sup> Profile 1 is BPSK at  $\frac{1}{2}$  of the script's normal channel bandwidth.

*Table 27: Radio Capacity – 250 MHz Channel Bandwidth (Script 5853)*

Profile	Modulation	Minimum Required Capacity Activation Key (Gbps)	Throughput (Mbps)
0	BPSK <sup>14</sup>	50	48-59
1	BPSK <sup>15</sup>	100	96-117
2	BPSK	200	192-235
3	QPSK	400	385-471
4	8 PSK	650	579-707
5	16 QAM	1000	772-944
6	32 QAM	1000	965-1180
7	64 QAM	1600	1158-1416
8	128 QAM	1600	1352-1652
9	256 QAM	1600	1545-1889
10	512 QAM	2000	1738-2125

---

<sup>14</sup> Profile 0 is BPSK at  $\frac{1}{4}$  of the script's normal channel bandwidth.

<sup>15</sup> Profile 1 is BPSK at  $\frac{1}{2}$  of the script's normal channel bandwidth.

*Table 28: Radio Capacity – 500 MHz Channel Bandwidth (Script 5804)*

Profile	Modulation	Minimum Required Capacity Activation Key (Gbps)	Throughput (Mbps)
0	BPSK <sup>16</sup>	100	99-121
1	BPSK <sup>17</sup>	200	199-243
2	BPSK	400	397-485
3	QPSK	1000	795-972
4	8 PSK	1600	1194-1459
5	16 QAM	1600	1592-1946
6	32 QAM	2000	1990-2433
7	64 QAM	2500	2388-2920
8	128 QAM	3000	2787-3406
9	256 QAM	4000	3185-3893
10	512 QAM	4000	3583-4380

---

<sup>16</sup> Profile 0 is BPSK at  $\frac{1}{4}$  of the script's normal channel bandwidth.

<sup>17</sup> Profile 1 is BPSK at  $\frac{1}{2}$  of the script's normal channel bandwidth.

*Table 29: Radio Capacity – 500 MHz Channel Bandwidth (Script 5854)*

Profile	Modulation	Minimum Required Capacity Activation Key (Gbps)	Throughput (Mbps)
0	BPSK <sup>18</sup>	100	99-121
1	BPSK <sup>19</sup>	200	199-243
2	BPSK	400	397-485
3	QPSK	1000	795-972
4	8 PSK	1600	1194-1459
5	16 QAM	1600	1592-1946
6	32 QAM	2000	1990-2433
7	64 QAM	2500	2388-2919
8	128 QAM	3000	2786-3406
9	256 QAM	4000	3185-3893
10	512 QAM	4000	3583-4380

---

<sup>18</sup> Profile 0 is BPSK at  $\frac{1}{4}$  of the script's normal channel bandwidth.

<sup>19</sup> Profile 1 is BPSK at  $\frac{1}{2}$  of the script's normal channel bandwidth.

*Table 30: Radio Capacity – 1000 MHz Channel Bandwidth (Script 5806)*

Profile	Modulation	Minimum Required Capacity Activation Key (Gbps)	Throughput (Mbps)
0	BPSK <sup>20</sup>	200	191-234
1	BPSK <sup>21</sup>	400	382-467
2	BPSK	1000	765-935
3	QPSK	1600	1531-1871
4	8 PSK	2500	2297-2807
5	16 QAM	3000	3063-3744
6	32 QAM	4000	3829-4680
7	64 QAM	5000	4594-5616
8	128 QAM	6000	5360-6553
9	256 QAM	6000	6126-7489

---

<sup>20</sup> Profile 0 is BPSK at  $\frac{1}{4}$  of the script's normal channel bandwidth.

<sup>21</sup> Profile 1 is BPSK at  $\frac{1}{2}$  of the script's normal channel bandwidth.

*Table 31: Radio Capacity – 1000 MHz Channel Bandwidth (Script 5856)*

Profile	Modulation	Minimum Required Capacity Activation Key (Gbps)	Throughput (Mbps)
0	BPSK <sup>22</sup>	200	191-234
1	BPSK <sup>23</sup>	400	382-467
2	BPSK	1000	765-935
3	QPSK	1600	1531-1871
4	8 PSK	2500	2296-2807
5	16 QAM	3000	3062-3744
6	32 QAM	4000	3828-4680
7	64 QAM	5000	4594-5616
8	128 QAM	6000	5360-6553
9	256 QAM	6000	6126-7489

*Table 32: Radio Capacity – 2000 MHz Channel Bandwidth (Script 5810)*

Profile	Modulation	Minimum Required Capacity Activation Key (Gbps)	Throughput (Mbps)
0	BPSK <sup>12</sup>	300	333-407
1	BPSK <sup>13</sup>	650	666-814
2	BPSK	1600	1331-1627
3	QPSK	3000	2664-3256
4	8 PSK	5000	4145-5067
5	16 QAM	6000	5527-6756
6	32 QAM	7000	6909-8446
7	64 QAM	9000	8291-10000
8	128 QAM	10000	10000-10000

---

<sup>22</sup> Profile 0 is BPSK at  $\frac{1}{4}$  of the script's normal channel bandwidth.

<sup>23</sup> Profile 1 is BPSK at  $\frac{1}{2}$  of the script's normal channel bandwidth.



*Table 33: Radio Capacity – 2000 MHz Channel Bandwidth (Script 5860)*

Profile	Modulation	Minimum Required Capacity Activation Key (Gbps)	Throughput (Mbps)
0	BPSK <sup>12</sup>	300	333-407
1	BPSK <sup>13</sup>	650	666-814
2	BPSK	1600	1331-1627
3	QPSK	3000	2664-3256
4	8 PSK	5000	4145-5066
5	16 QAM	6000	5527-6756
6	32 QAM	7000	6909-8445
7	64 QAM	9000	8291-10000
8	128 QAM	10000	10000-10000

## 7.5 Transmit Power Specifications

*Table 34: Transmit Power – Standard IP-50EX Devices*

Modulation	250 MHz	500 MHz	1000 MHz	2000 MHz
¼ BPSK	21	21	21	21
½ BPSK	21	21	21	21
BPSK	21	21	21	21
QPSK	21	21	21	21
8 QAM	20	20	20	20
16 QAM	19	19	19	19
32 QAM	18	18	18	18
64 QAM	17	17	17	17
128 QAM	16	16	16	16
256 QAM	15	15	15	–
512 QAM	15	15	–	–

**Note:** The accuracy of these values is up to +/-2dB.  
The Pmin for standard TX power is +10dBm for all supported frequencies and modulations.

*Table 35: Transmit Power – IP-50EX-P Devices*

Modulation	250 MHz	500 MHz	1000 MHz	2000 MHz
¼ BPSK	24	24	24	24
½ BPSK	24	24	24	24
BPSK	24	24	24	24
QPSK	24	24	24	24
8 QAM	23	23	23	23
16 QAM	22	22	22	22
32 QAM	21	21	21	21
64 QAM	20	20	20	20
128 QAM	19	19	19	19
256 QAM	18	18	18	–
512 QAM	18	18	–	–

**Note:** The accuracy of these values is up to +/-3dB.  
The Pmin for IP-50EX-P TX power is +10dBm for all supported frequencies and modulations.

## 7.6 Receiver Threshold Specifications (dBm@ 10E<sup>-6</sup>)

**Note:** The RSL values listed in this section refer to fixed profiles. When ACM is enabled, the RSL levels may be different when the radio switches to other profiles.

The values listed in this section are typical. Actual values may differ in either direction by up to 2dB.

*Table 36: Receiver Threshold Specifications*

Modulation	250 MHz	500 MHz	1000 MHz	2000 MHz
BPSK	-76.7	-73.7	-70.5	-68.4
QPSK	-74.4	-71.1	-68.0	-65.4
8 PSK	-69.3	-65.9	-62.8	-60.0
16 QAM	-67.9	-64.7	-61.4	-58.6
32 QAM	-63.8	-60.7	-57.6	-55.7
64 QAM	-62.0	-58.7	-55.5	-52.9
128 QAM	-59.1	-55.8	-52.5	-49.3
256 QAM	-56.2	-52.9	-49.6	—
512 QAM	-53.0	-49.8	—	—

The RSL overload is -10 dBm for all supported frequencies and modulations.

The maximum RSL before damage is +10 dBm.

## 7.7 Mediation Device Losses

Device Type	Maximum Insertion Loss (Main/Secondary)
OMT	2dB
Splitter 1:2	4.5dB
Coupler 1:4	2.2dB/ 6.5±1dB

## 7.8 Ethernet Latency Specifications

**Note:** When AES-GCM-256 Payload Encryption is enabled, latency is increased.

*Table 37: Ethernet Latency – 250 MHz Channel Bandwidth (Script 5803)*

ACMB Profile	Modulation	Latency (μsec) with 10 GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK <sup>24</sup>		348	361	380	425	511	587
1	BPSK <sup>25</sup>		180	186	197	219	263	300
2	BPSK		93	97	102	114	137	156
3	QPSK		53	54	58	64	76	86
4	8 QAM		39	40	43	47	55	62
5	16 QAM		32	33	35	38	45	51
6	32 QAM		28	29	31	33	39	44
7	64 QAM		25	26	28	30	35	39
8	128 QAM		23	24	25	28	32	36
9	256 QAM		22	22	24	26	30	33
10	512 QAM		21	22	23	24	28	31

<sup>24</sup> Profile 0 is BPSK at  $\frac{1}{4}$  of the script's normal channel bandwidth.

<sup>25</sup> Profile 1 is BPSK at  $\frac{1}{2}$  of the script's normal channel bandwidth.

*Table 38: Ethernet Latency – 250 MHz Channel Bandwidth (Script 5853)*

ACMB Profile	Modulation	Latency (μsec) with 10 GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK <sup>26</sup>		354	367	387	432	522	597
1	BPSK <sup>27</sup>		185	192	203	226	272	311
2	BPSK		101	105	111	123	148	168
3	QPSK		60	62	66	73	87	98
4	8 QAM		47	48	51	56	67	75
5	16 QAM		40	41	44	48	57	63
6	32 QAM		36	37	39	43	51	56
7	64 QAM		33	34	36	40	47	52
8	128 QAM		31	32	34	37	44	48
9	256 QAM		30	31	33	35	42	46
10	512 QAM		29	29	31	34	40	44

---

<sup>26</sup> Profile 0 is BPSK at  $\frac{1}{4}$  of the script's normal channel bandwidth.

<sup>27</sup> Profile 1 is BPSK at  $\frac{1}{2}$  of the script's normal channel bandwidth.

*Table 39: Ethernet Latency – 500 MHz Channel Bandwidth (Script 5804)*

ACMB Profile	Modulation	Latency (μsec) with 10 GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK <sup>28</sup>		173	179	189	211	254	291
1	BPSK <sup>29</sup>		91	94	99	110	132	151
2	BPSK		50	51	55	61	72	82
3	QPSK		30	31	33	36	42	48
4	8 QAM		23	24	25	28	32	36
5	16 QAM		20	20	21	23	28	31
6	32 QAM		17	18	19	21	25	27
7	64 QAM		16	17	18	20	23	25
8	128 QAM		15	16	17	18	21	24
9	256 QAM		15	15	16	18	20	22
10	512 QAM		14	14	16	17	19	21

---

<sup>28</sup> Profile 0 is BPSK at  $\frac{1}{4}$  of the script's normal channel bandwidth.

<sup>29</sup> Profile 1 is BPSK at  $\frac{1}{2}$  of the script's normal channel bandwidth.

*Table 40: Ethernet Latency – 500 MHz Channel Bandwidth (Script 5854)*

ACMB Profile	Modulation	Latency (μsec) with 10 GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK <sup>30</sup>		183	188	199	222	268	302
1	BPSK <sup>31</sup>		99	102	109	121	145	164
2	BPSK		58	59	63	70	84	94
3	QPSK		38	39	41	46	54	60
4	8 QAM		31	32	34	37	44	49
5	16 QAM		28	28	30	33	39	43
6	32 QAM		26	26	28	31	36	40
7	64 QAM		24	25	27	29	34	38
8	128 QAM		23	24	26	28	33	36
9	256 QAM		22	23	25	27	32	35
10	512 QAM		22	23	24	27	31	34

---

<sup>30</sup> Profile 0 is BPSK at  $\frac{1}{4}$  of the script's normal channel bandwidth.

<sup>31</sup> Profile 1 is BPSK at  $\frac{1}{2}$  of the script's normal channel bandwidth.



Table 41: Ethernet Latency – 1000 MHz Channel Bandwidth (Script 5806)

ACMB Profile	Modulation	Latency (μsec) with 10 GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK <sup>32</sup>		94	97	103	115	138	156
1	BPSK <sup>33</sup>		51	53	56	62	74	84
2	BPSK		29	30	32	36	42	48
3	QPSK		19	19	21	23	27	30
4	8 QAM		15	16	17	19	22	24
5	16 QAM		14	14	15	17	19	21
6	32 QAM		13	13	14	15	18	20
7	64 QAM		12	12	13	14	17	18
8	128 QAM		11	12	13	14	16	18
9	256 QAM		11	11	12	13	15	17

---

<sup>32</sup> Profile 0 is BPSK at  $\frac{1}{4}$  of the script's normal channel bandwidth.

<sup>33</sup> Profile 1 is BPSK at  $\frac{1}{2}$  of the script's normal channel bandwidth.

Table 42: Ethernet Latency – 1000 MHz Channel Bandwidth (Script 5856)

ACMB Profile	Modulation	Latency (μsec) with 10 GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK <sup>34</sup>		102	105	112	124	150	168
1	BPSK <sup>35</sup>		59	61	65	72	86	96
2	BPSK		37	38	41	45	54	60
3	QPSK		27	27	29	33	39	43
4	8 QAM		23	24	26	28	33	37
5	16 QAM		21	22	24	26	31	34
6	32 QAM		21	21	23	25	29	32
7	64 QAM		20	20	22	24	28	31
8	128 QAM		19	20	22	25	28	30
9	256 QAM		19	19	21	24	27	30

---

<sup>34</sup> Profile 0 is BPSK at  $\frac{1}{4}$  of the script's normal channel bandwidth.

<sup>35</sup> Profile 1 is BPSK at  $\frac{1}{2}$  of the script's normal channel bandwidth.

*Table 43: Ethernet Latency – 2000 MHz Channel Bandwidth (Script 5810)*

ACMB Profile	Modulation	Latency (μsec) with 10 GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK <sup>24</sup>		58	60	63	70	84	95
1	BPSK <sup>25</sup>		33	34	36	40	47	53
2	BPSK		20	21	22	25	29	33
3	QPSK		14	15	16	17	20	22
4	8 QAM		12	12	13	15	17	19
5	16 QAM		11	11	12	13	15	17
6	32 QAM		10	11	12	13	15	16
7	64 QAM		10	10	11	12	14	16
8	128 QAM		10	10	11	12	13	15

*Table 44: Ethernet Latency – 2000 MHz Channel Bandwidth (Script 5860)*

ACMB Profile	Modulation	Latency (μsec) with 10 GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK <sup>24</sup>		66	68	72	80	96	107
1	BPSK <sup>25</sup>		41	42	45	50	59	66
2	BPSK		28	29	31	34	41	45
3	QPSK		22	23	24	27	32	35
4	8 QAM		20	20	22	25	29	31
5	16 QAM		18	19	21	24	27	30
6	32 QAM		18	19	20	23	26	29
7	64 QAM		18	18	20	22	25	28
8	128 QAM		18	18	19	22	25	28

## 7.9 Interface Specifications

### 7.9.1 Ethernet Interface Specifications

Supported Ethernet Interfaces for Traffic	2x1000base-X (Optical SFP28) 1x1000base-X (Optical using QSFP-to-SFP+ adaptor)
Supported Ethernet Interfaces for Management	1x100/1000 Base-T (RJ-45)

*Table 45: Approved SFP Modules*

Marketing Model	Marketing Description	Item Description
SFP-GE-SX-EXT-TEMP	SFP optical interface 1000Base-SX,EXT-TE	XCVR,SFP,850nm,MM,1.0625 Gbit/s FC/ 1.25 GBE, INDUSTRIAL GRADE,SINGLE PACK KIT
SFP-GE-LX-EXT-TEMP	SFP OPTICAL 1000Base-LX,EXT TEMP	XCVR,SFP,1310nm,1.25Gb,SM,10km,W.DDM,INDUSTRIAL GRADE,SINGLE PACK KIT
SFP-GE-COPER-EXT-TMP-LOS-DIS	SFP ELECT INT 1000Base-T RX_LOS DIS, IND	XCVR,SFP,COPPER 1000BASE-T,RX_LOS DISABLE,INDUSTRIAL TEMP

*Table 46: Approved 10 GbE SFP+ Modules*

Marketing Model	Marketing Description	Item Description
SFP+10GBASE-LR10-EXT-TEMP	SFP+ 10GE OPT 10GBASELR, 10km,EXT-TEMP	XCVR,SFP+,1310nm,SM,10 Gbit/s,10km,INDUSTRIAL GRADE,SINGLE P
SFP+10GBASE-SR10-EXT-TEMP	XCVR,SFP+,850nm,MM,10 Gbit/s, INDUSTRIAL GRADE	SFP+10GBASE-SR10-EXT-TEMP

*Table 47: Approved SFP28 Modules*

Marketing Model	Marketing Description	Item Description
SFP28-25GbE-SM-LR10-EXT-TEMP	SFP28 25GE OPT 1310nm,SM,10km,EXT-TEMP	XCVR,SFP28,25GbE,1310nm DBF, Up to 25.78Gb/s ,SM, up to 10 km on 9/125um MF, Duplex LC, W.DDM,INDUSTRIAL
SFP28-25GbE-MM-SR-EXT-TEMP	SFP28 25GE OPT 850nm,MM,70m,EXT-TEMP	XCVR,SFP28,10GbE / 25GbE,850nm VCSEL, 10.3Gb/s & 25.78Gb/s ,MM, up to 70m OM3 MMF and 100M on OM4 MMF, Duplex LC, W.DDM,

Table 48: QSFP Accessories

Marketing Model		Item Description
QSFP to SFP Kit	Adapter QSFP to SFP For Outdoor kit	Converts the QSFP port to an SFP or SFP+ port. <b>Note:</b> This adaptor supports a temperature range of 0° to +70°C (32° to 158°F).
<b>Notes:</b>		Ceragon recommends the use of SFP, SFP+, and SFP28modules certified by Ceragon, as listed above.

## 7.10 Carrier Ethernet Functionality

"Jumbo" Frame Support	Up to 9600 Bytes
General	Enhanced link state propagation
Integrated Carrier Ethernet Switch	Maximum number of Ethernet services: 1024 plus one pre-defined management service MAC address learning with up to 32K MAC addresses 802.1ad provider bridges (QinQ) 802.3ad link aggregation
QoS	Advanced CoS classification and remarking Per interface CoS based packet queuing/buffering (8 queues) Per queue statistics Tail-drop and WRED with CIR/EIR support Flexible scheduling schemes (SP/WFQ) Per interface and per queue traffic shaping 2750 KB packet buffer
Network resiliency	MSTP ERP (G.8032)
OAM	CFM (802.1ag)
Performance Monitoring	Per port Ethernet counters (RMON/RMON2) Radio ACMB statistics
Supported Ethernet/IP Standards	100/1000base-T/X (IEEE 802.3) Optical 10Gbase-X (IEEE 802.3) Ethernet VLANs (IEEE 802.3ac) Virtual LAN (VLAN, IEEE 802.1Q) Class of service (IEEE 802.1p) Provider bridges (QinQ – IEEE 802.1ad) Link aggregation (IEEE 802.3ad) Auto MDI/MDIX for 1000baseT RFC 1349: IPv4 TOS RFC 2474: IPv4 DSCP RFC 2460: IPv6 Traffic Classes

## 7.11 Synchronization Protocols

- Enhanced Ethernet Equipment Clock (eEEC) Specification (G.8262.1)
- PTP Telecom Class C Boundary Clock (T-BC) and Time Slave Clock (T-TSC) Specification (G.8273.2)
- PTP Telecom Class C Transparent Clock (T-TC) Specification (G.8273.3)
- Enhanced SyncE Network Limits (G.8261, clause 9.2.1)
- Enhanced PTP Network Limits (G.8271.1)
- Ethernet Synchronization Messaging Channel (ESMC) (G.8264, clause 11)
- PTP Telecom Profile for Time (Full Timing Support) (G.8275.1)
- Precision Time Protocol (version 2, IEEE1588-2008)

## 7.12 Network Management, Diagnostics, Status, and Alarms

Network Management System	Ceragon NMS
NMS Interface protocol	SNMPv1/v2c/v3 XML over HTTP/HTTPS toward NMS
Element Management	Web based EMS, CLI
Management Channels & Protocols	HTTP/HTTPS Telnet/SSH-2 FTP/SFTP
Authentication, Authorization & Accounting	User access control X-509 Certificate
Management Interface	Dedicated Ethernet interfaces or in-band in traffic ports
In-Band Management	Support dedicated VLAN for management
TMN	Ceragon NMS functions are in accordance with ITU-T recommendations for TMN
RSL Indication	Accurate power reading (dBm) available at IP-50EX <sup>36</sup> , and NMS
Performance Monitoring	Integral with onboard memory per ITU-T G.826/G.828

<sup>36</sup> The voltage at the RSL port is 0.XX where XX is the RSL level. For example: 0.59V means an RSL of -59 dBm. Note that the voltage measured at the RSL port is not accurate and should be used only as an aid).





7.13 Mechanical Specifications

	Direct Mount HW (For parabolic antennas)	43dBi Integrated Antenna
Module Dimensions	228mm(H), 233mm(W), 76mm(D) 9"(H), 9.2"(W), 3"(D)	313mm(H), 276mm(W), 97mm(D) 12.3"(H), 10.9"(W), 3.8"(D)
Module Weight	2.77 kg/6.1 lbs.	4.5 kg/9.9 lbs.

## 7.14 Standards Compliance

Specification	Standard
Radio Spectral Efficiency	ETSI: EN 302 217-2 FCC Part 101
EMC	EN 301 489-1, EN 301 489-4 (Europe) FCC 47 CFR, part 15, subpart B (US) ICES-003 (Canada) TEC/SD/DD/EMC-221/05/OCT-16 (India) IEC 61000-4-29 (India)
Safety	EN 62368-1 (Europe) IEC 62368-1 (International) UL 62368-1 (US) CSA-C22.2 No.62368-1 (Canada)

## 7.15 Environmental Specifications

- Operating: ETSI EN 300 019-1-4 Class 4.1
  - Temperature range: **-40°C to +55°C/-40°F to +131°F**

Humidity: **5%RH to 100%RH**  
**IEC 60529 IP67**

- Storage: ETSI EN 300 019-1-1 Class 1.2
- Transportation: ETSI EN 300 019-1-2 Class 2.3

IP-50EX is exempt from the list of equipment subject to EU DIRECTIVE 2000/14/EC regarding noise emission in the environment by equipment for use outdoors.

IP-50EX complies with the 1972 Noise Control Act.

IP-50EX does not include any acoustic noise generating components.



**7.16    Antenna Interface Specifications**

Remote Mount Antenna Interface:

Waveguide Standard	Antenna Flange
WR12	UG387/U Ceragon Antenna Interface

## 7.17 Integrated Antenna

**Note:** IP-50EX and IP-50EX-P models with Integrated Antenna are planned for future release.

The following table describes the electrical parameters of the integrated antenna:

Frequency coverage	71-86 GHz
Gain	43dBi
VSWR	1.6
3dB beam width (azimuth and elevation)	1°
Polarization	Single Linear: 45° (diamond)
Co/cross-polar ratio	>35dB
Front to back ratio	>60dB
Side lobe suppression	ETSI EN 3020217-42 V1 5.1 CLASS 2 CLASS 3

## 7.18 Power Input Specifications

Standard Input	-48 VDC nominal
Standard Input	-48 VDC
DC Input range	-40.5 to -60 VDC

## 7.19 PoE Port Specifications (IP-50EX-P only)

The IP-50EX-P PoE port (P2) is compliant with IEEE802.3bt Class 8 Endpoint PSE.

The maximum supported cable length is 100m using Cat5e or Cat6 cables.

DC Input range	-40.5 to -60 VDC
----------------	------------------

## 7.20 Power Consumption Specifications

*Table 49: Power Consumption – Standard IP-50EX Devices*

Unit Configuration	Power Consumption
Typical Power	50W
Maximum Power	55W

*Table 50: Power Consumption –IP-50EX-P Devices*

Unit Configuration	Power Consumption
Typical Power	61W
Maximum Power	65W


## 7.21 Cable Specifications

### 7.21.1 Outdoor Ethernet Cable Specifications

#### Electrical Requirements

Cable type	CAT-5e SFUTP, 4 pairs, according to ANSI/TIA/EIA-568-B-2
Wire gage	24 AWG
Stranding	Solid
Voltage rating	70V
Shielding	Braid + Foil

#### RJ-45 Connector Pinout

Pin #	Wire Color Legend	Signal
1	 White/Orange	TX+
2	 Orange	TX-
3	 White/Green	RX+
4	 Blue	TRD2+
5	 White/Blue	TRD2
6	 Green	RX-
7	 White/Brown	TRS3+
8	 Brown	TRD3-

#### Mechanical/ Environmental Requirements

Jacket	PVC, double, UV resistant
Outer diameter	7-10 mm/0.28 – 0.39 inches
Operating and Storage temperature range	-40°C - 85°C/-40°F - 185°F
Flammability rating	According to UL-1581 VW1, IEC 60332-1
RoHS	According to Directive/2002/95/EC

### 7.21.2 Outdoor DC Cable Specifications

#### Electrical Requirements

Cable type	2 tinned copper wires
Wire gage	18 AWG (for $\leq 75\text{m}$ installations) 14 AWG (for $75\text{m} \div 200\text{m}$ installations)
Stranding	stranded
Voltage rating	600V
Spark test	4KV
Dielectric strength	2KV AC min

#### Mechanical/ Environmental Requirements

Jacket	PVC, double, UV resistant
Outer diameter	7-10 mm/0.28 – 0.39 inches
Operating & Storage temperature range	-40°C - 85°C/-40°F - 185°F
Flammability rating	According to UL-1581 VW1, IEC 60332-1
RoHS	According to Directive/2002/95/EC



## 8. Appendix A – Marketing Models

The following IP-50EX hardware models are available.

*Table 51: IP-50EX Marketing Models (Available)*

Marketing Model	Description	Notes
IP-50EX-L	IP-50EX AO TL (TX 71-76G/RX 81-86G)	TX Low, external antenna
IP-50EX-H	IP-50EX AO TH (TX 81-86G/RX 71-76G)	TX High, external antenna

The following IP-50EX hardware models are planned for future release:

*Table 52: IP-50EX Marketing Models (Planned for Future Release)*

Marketing Model	Description	Notes
IP-50EX-43IA-L	IP-50EX AO TL (TX 71-76G/RX 81-86G) 43dBIA	TX Low, 43 dBi integrated antenna
IP-50EX-43IA-H	IP-50EX AO TH (TX 81-86G/RX 71-76G) 43dBIA	TX High, 43 dBi integrated antenna

The following IP-50EX-P hardware models are available.

*Table 53: IP-50EX-P Marketing Models (Available)*

Marketing Model	Description	Notes
IP-50EX-P-TL	IP-50EX AO, HP, PoE, AES HW support TL (TX 71-76G/RX 81-86G)	TX Low, external antenna, PoE input
IP-50EX-P-H	IP-50EX AO, HP, PoE, AES HW support TH (TX 81-86G/RX 71-76G)	TX High, external antenna, PoE input

The following IP-50EX-P hardware models are planned for future release.

*Table 54: IP-50EX-P Marketing Models (Planned for Future Release)*

Marketing Model	Description	Notes
IP-50EX-P-43IA-L	IP-50EX AO Premium w/ 43 dBi Integrated Antenna TL (TX 71-76G/RX 81-86G)	TX Low, 43 dBi integrated antenna, PoE input
IP-50EX-P-43IA-H	IP-50EX AO Premium w/ 43 dBi Integrated Antenna TH (TX 81-86G/RX 71-76G)	TX High, 43 dBi integrated antenna, PoE input

## 9. Appendix B - Synonyms and Acronyms

Acronym	Equivalent Term
ACM	Adaptive Coding Modulation
ACMB	Adaptive Coding Modulation and Bandwidth
AES	Advanced Encryption Standard
AIS	Alarm Indication Signal
ATPC	Automatic Transmit Power Control
BER	Bit Error Ratio
CBS	Committed Burst Size
CET	Carrier-Ethernet Transport
CIR	Committed Information Rate
CLI	Command Line Interface
CoS	Class of Service
CSF	Client Signal Failure
DA	Destination Address
DSCP	Differentiated Service Code Point
EBS	Excess Burst Size
EIR	Excess Information Rate
EPL	Ethernet Private Line
ETH-BN	Ethernet Bandwidth Notification
EVPL	Ethernet Virtual Private Line
EVC	Ethernet Virtual Connection
FM	Fault Management
FTP (SFTP)	File Transfer Protocol (Secured File Transfer Protocol)
GbE	Gigabit Ethernet
HTTP (HTTPS)	Hypertext Transfer Protocol (Secured HTTP)
LAN	Local area network
LLF	Link Loss Forwarding
LOC	Loss of Carrier
LOF	Loss of Frame
LOS	Loss of Signal
LTE	Long-Term Evolution
MACsec	Media Access Control Security

Acronym	Equivalent Term
MPLS	Multiprotocol Label Switching
MRU	Maximum Receive Unit
MSE	Mean Square Error
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmit Capability
NMS	Network Management System
NSMA	National Spectrum Management Association
NTP	Network Time Protocol
OAM	Operation Administration & Maintenance (Protocols)
PDV	Packed Delay Variation
PFC	Priority-based Flow Control
PIR	Peak Information Rate
PM	Performance Monitoring
PTP	Precision Timing-Protocol
QoS	Quality of Service
RBAC	Role-Based Access Control
RDI	Remote Defect Indication
REC	Radio Equipment Control
RMON	Remote Network Monitoring
RSL	Received Signal Level
RSTP	Rapid Spanning Tree Protocol
SAP	Service Access Point
SDN	Software-Defined Networking
SFTP	Secure FTP
SLA	Service level agreements
SNMP	Simple Network Management Protocol
SNP	Service Network Point
SNTP	Simple Network Time Protocol
SP	Service Point
STP	Spanning Tree Protocol
SSH	Secured Shell (Protocol)
SSM	Synchronization Status Messages
SyncE	Synchronous Ethernet

Acronym	Equivalent Term
TACACS+	Terminal Access Controller Access-Control System Plus
TLS	Transport Layer Security
TOS	Type of Service
UNI	User Network Interface
UTC	Coordinated Universal Time
Web EMS	Web-Based Element Management System
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection
XPIC	Cross Polarization Interference Cancellation