Technical Description

IP-50CX

November 2025 | Rev A.01

CeraOS 13.1

Notice

Trademarks

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

List of Figures

List of Tables

About This Guide

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

Note that some features described in this document may not be supported in every CeraOS release. For a description of feature support per release, refer to the Release Notes for the CeraOS version you are using.

What You Should Know

This document describes both ETSI and ANSI (FCC) standards and specifications.

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-50CX for use in system planning, and determining which IP-50CX configuration is best suited for a specific network.

Related Documents

- Datasheet for IP-50CX

1. Synonyms and Acronyms

Acronym	Equivalent Term
ACAP	Adjacent Channel Alternate Polarization
ACCP	Adjacent Channel Co-Polarization
ACM	Adaptive Coding Modulation
AES	Advanced Encryption Standard
AIS	Alarm Indication Signal
ATPC	Automatic Tx Power Control
BER	Bit Error Ratio
BPDU	Bridge Protocol Data Units
CBS	Committed Burst Size
CE	Customer Equipment
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
EFM	Ethernet in the First Mile
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

Acronym	Equivalent Term
LOS	Loss of Signal
LTE	Long-Term Evolution
MEN	Metro Ethernet Network
MFA	Multi-Factor Authentication
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
PIR	Peak Information Rate
PM	Performance Monitoring
PTP	Precision Timing-Protocol
QoE	Quality of-Experience
QoS	Quality of Service
RBAC	Role-Based Access Control
RDI	Remote Defect Indication
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
SSO	Single Sign-On

Acronym	Equivalent Term
STP	Spanning Tree Protocol
SSH	Secured Shell (Protocol)
SSM	Synchronization Status Messages
SyncE	Synchronous Ethernet
TACACS+	Terminal Access Controller Access-Control System Plus
TLS	Transport Layer Security
TOS	Type of Service
UNI	User Network Interface
UTC	Coordinated Universal Time
VCC	Common Collector Voltage
Web EMS	Web-Based Element Management System
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection

2. Introduction

IP-50CX is a MultiCore microwave radio suitable for all deployment scenarios. IP-50CX provides cutting-edge capabilities that enable operators to base entire networks, from small cells to massive aggregation sites, on this single product.

IP-50CX supports cutting edge capacity-boosting techniques and a wide range of modulations from BPSK to 4096 QAM with ACM, along with a large range of channel bandwidth from 14 to 224 MHz, to offer a high capacity solution for every network topology and every site configuration.

This chapter includes:

- Product Overview
- Unique IP-50CX Feature Set
- System Configurations

2.1 Product Overview

Ceragon's IP-50CX sets a new standard for microwave transmission, offering 193 Gbps switching capacity, channel spacing of up to 224 MHz, and a wide range of modulations, from BPSK to 4096 QAM with ACM. These and other advanced capabilities are combined in IP-50CX with the full range of Ceragon's MultiCore technologies to produce an all-outdoor product that can be used throughout the microwave network, from small cells to massive aggregation sites.

The ability to use IP-50CX throughout the network offers the possibility of simplifying network deployment and maintenance by reducing complexity, costs, and time-to-revenue.

IP-50CX is easily and quickly deployable compared with fiber, enabling operators to achieve faster time to new revenue streams, lower total cost of ownership, and long-term peace of mind.

IP-50CX can deliver multi-Gbps capacity on a single frequency channel, setting a new standard for efficient spectrum use. IP-50CX's unique MultiCore radio architecture is based on an advanced parallel radio processing engine, built around Ceragon's in-house chipsets. The result is superior radio performance with reduced power consumption and form-factor.

Additionally, IP-50CX's MultiCore architecture enables operators to start with a single core with the option of enabling the second core remotely when network capacity requirements increase.

IP-50CX can be deployed as a stand-alone all-outdoor radio. In can also be used as an upgrade path to achieve the highest possible capacity of any existing link by utilizing Ceragon's unique Layer 1 Link Aggregation technique for single and dual-frequency configurations.

In a 4+0 Layer 1 Link Aggregation configuration, two IP-50CX units operate together to form a multi-carrier node operating over one or two microwave channels and connected to the switch via a single cable. This configuration can provide total capacity of up to 6 Gbps when wide channels are used.

Layer 1 Link Aggregation can also be used to pair an IP-50CX with an IP-20C. This enables operators to add an IP-50CX to existing IP-20C deployments in order to add significantly to node capacity utilizing the same physical footprint, adding to rather than replacing the existing IP-20C and its capacity.

As an upgrade path for existing IP-20C nodes, Layer 1 Aggregation enables operators to significantly increase the link's capacity while retaining the same network configuration, antennas, mediation devices, and cabling. This can facilitate quick and efficient network growth, minimizing the cost of upgrade and lowering the total cost of ownership.

Layer 1 Link Aggregation can also be used with an IP-50CX and a third-party device.

Along with its other configuration options, IP-50CX can be used in Multiband configurations with IP-50E. This configuration utilizes Layer 1 Link Bonding to provide robust links that combine microwave with E-band transmissions, for capacity of up to 14 Gbps. Multiband bundles E-Band and microwave radios in a single group that is shared with an Ethernet interface.

The following are some of the highlights of IP-50CX:

- **MultiCore Radio Technology** – Parallel radio processing engine that boosts capacity, distance and availability.
- **High Capacity and Spectral Efficiency** – 4096 QAM modulation, Layer 1 Link Aggregation
- **Simple Operation** – Software-defined radio, rapid deployment, and minimal truck rolls.
- **Environment-Friendly** – Compact, all-outdoor unit with low power consumption.

2.2 Unique IP-50CX Feature Set

The following table summarizes the basic IP-50CX feature set.

Table 1: IP-50CX Feature Set

Extended Modulation Range	ACM BPSK – 4096 QAM
Frequency Bands	6L to 42 GHz
Wide Range of Channels	14 to 224 MHz
Power over Ethernet (PoE)	Proprietary
Compact Size and Weight	270mm(H), 233mm(W), 98mm(D), 6 kg
Antennas	Ceragon proprietary RFU-C interface Direct and remote mount – standard flange
Durable All-Outdoor System	IP67-compliant

2.3 System Configurations

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

- 2+0 Single/Dual Polarization
- 1+0 (Horizontal or Vertical Polarization)
- 4+0 Layer 1 Link Aggregation
- Layer 1 Link Aggregation with IP-20C
- Layer 1 Link Aggregation with Third-Party Devices
- 1+1 HSB (two units)
- 1+1 HSB-SD (two units)[1]
- 2+2 Single/Dual Polarization HSB
- 2+2 HSB-SD[1]
- Multiband (with IP-50E)

3. IP-50CX Hardware Description

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

This chapter includes:

- IP-50CX Unit Description
- Field-Replaceable Diplexer Units
- PoE Injector
- Voltage Alarm Thresholds and PMs

3.1 IP-50CX Unit Description and Interfaces

IP-50CX features an all-outdoor MultiCore architecture consisting of a single unit directly mounted on the antenna. The IP-50CX combines full system capabilities with a very compact form-fit. The all outdoor system architecture is designed around Ceragon's IP core components, enabling a true MultiCore design.

Note:	The equipment is type approved and labeled according to RED (2014/53/EU). Note that in IP-50CX, Port 2 is the upper port, located closest to the handle, and Port 1 is the lower port, located closest to the Ethernet ports.

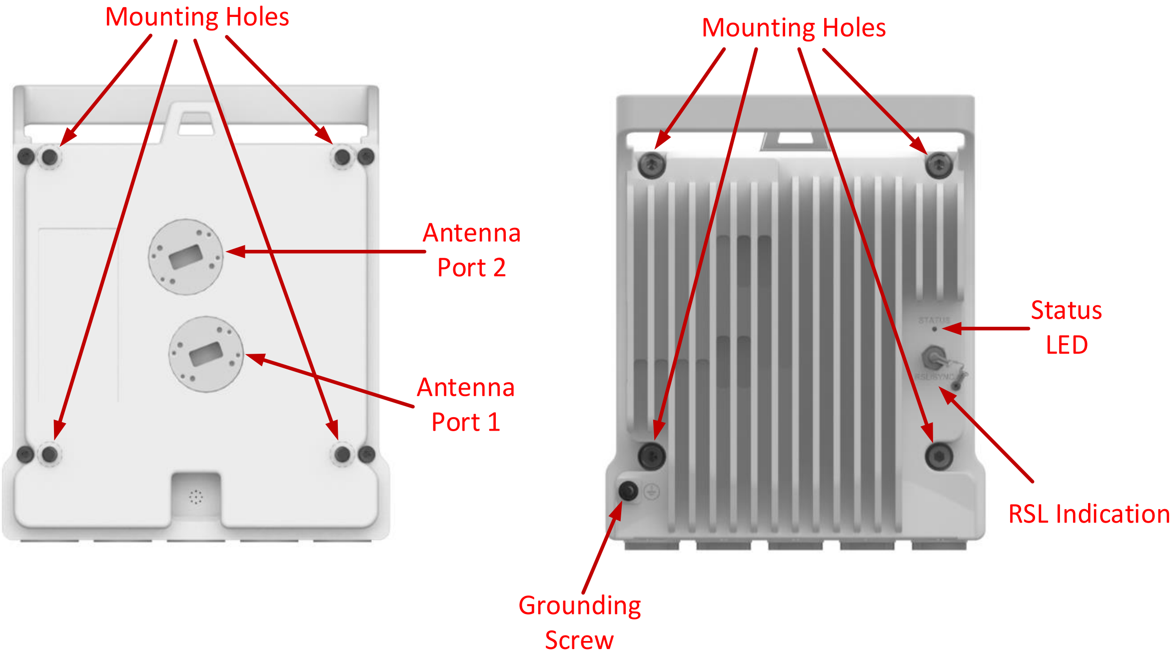


Figure 1: IP-50CX Rear View (Left) and Front View (Right)

For traffic, the IP-50CX has an RJ-45 interface (P2), an SFP+ cage (P3), and an SFP28 cage (P4). The IP-50CX also has an RJ-45 management port (P5) which can also be used for traffic.

Note:	Support for traffic via the management port is planned for future release.

For power, the IP-50CX has a DC power interface (-48V) (P1).

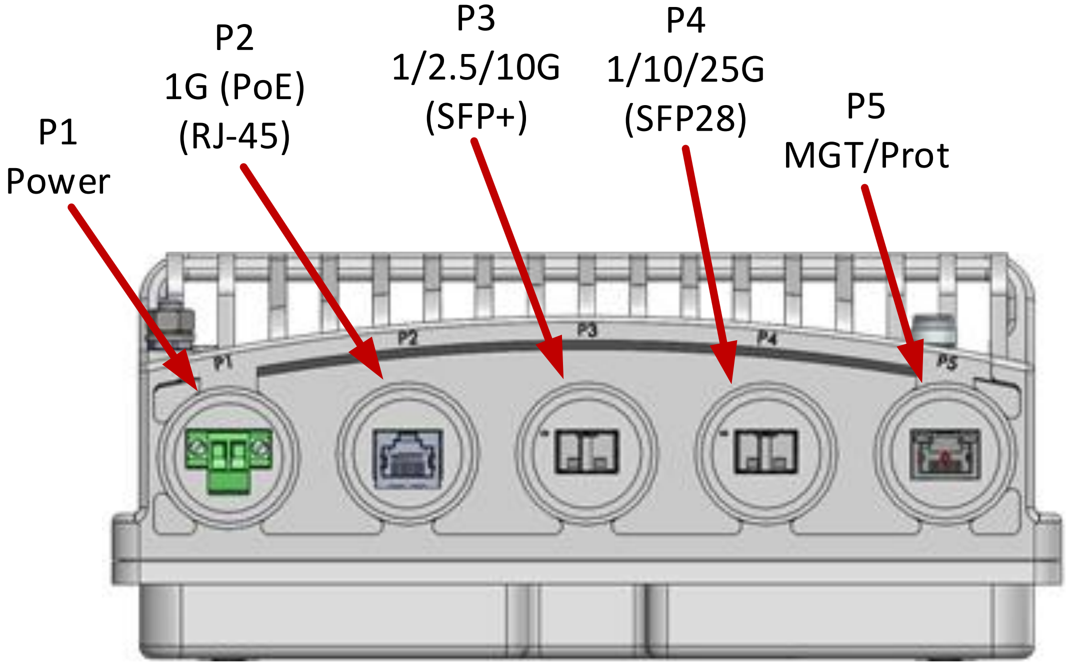


Figure 2: IP-50CX Interfaces

- Port 1 – Power Interface (-48V)
- Port 2 (Eth 1):
  - RJ-45: 100/1000BASE-T
  - PoE
- Port 3 (Eth 2):
  - SFP cage which supports SFP+ standard
  - Electric: 1000BASE-T
  - Optical: 1000BASE-X, 10GBASE-X
- Port 4 (Eth 3):
  - SFP cage which supports SFP28 standard
  - Electric: 1000BASE-T
  - Optical: 1000BASE-X, 10GBASE-X, 25GBASE-X
- Port 5:
  - RJ-45: 100BASE-T
  - Management and Protection port
- 2 RF Interfaces: Standard interface per frequency band
- RSL interface: BNC connector
- Grounding screw

3.2 Field-Replaceable Diplexer Units

Using Ceragon's Easy Set technology, an IP-50CX consists of a generic radio unit and a diplexer unit. For 6 to 11 GHz, the diplexer unit is field-replaceable, which means it can be replaced without replacing the radio unit. The generic radio unit covers an entire frequency band. It is the diplexer unit, which is passive, that determines the sub-band coverage for the entire integrated IP-50CX unit. This provides operators with major benefits in terms of both deployment time and maintenance.

For maintenance, the operator can reduce the number of spare radio units in its inventory because a single generic radio unit can be used for any sub-band. This means that for a site covering four channel ranges within a single frequency band, a single spare radio unit can be kept on hand, because that unit can be used as a spare for any of the IP-50CX units in the site. The diplexer units, because they are passive, are much less likely to require replacement, so the maintenance of spare parts for the diplexer units is much less of a concern for the operator.

The use of separate generic radio units and diplexer units also enables operators to achieve a quicker system deployment time. In the planning stage, when the frequency bands have been determined but the exact sub-band layout is still under consideration, operators can already order all the radio units required for the frequency bands that have been determined, and can begin ordering diplexer units for the approximate sub-bands that are anticipated, while still determining the exact network parameters. This enables faster delivery and deployment of the network.

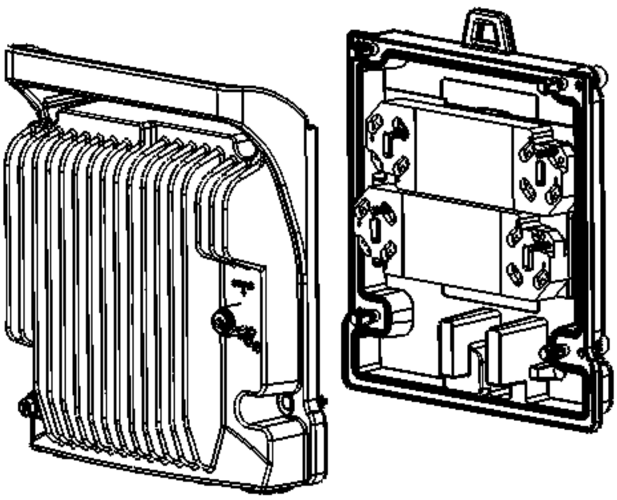


Figure 3: IP-50CX Radio Unit (Left) and Diplexers Unit (Right)

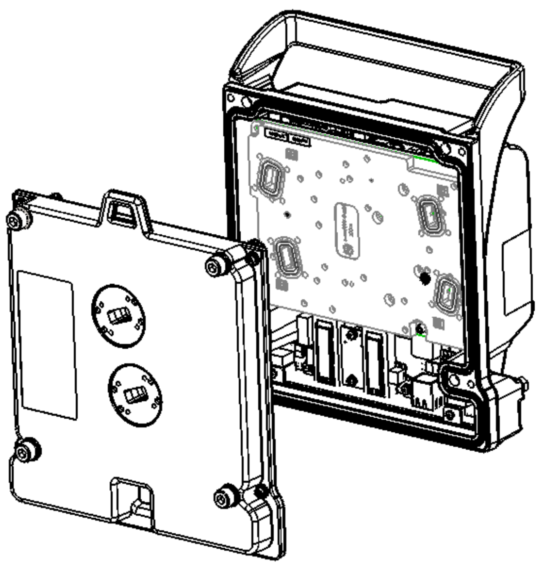


Figure 4: IP-50CX Radio Unit (Right) and Diplexers Unit (Left)

3.3 PoE Injector

The PoE injector box is designed to offer a single cable solution for connecting both data and the DC power supply to the IP-50CX.

To do so, 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.

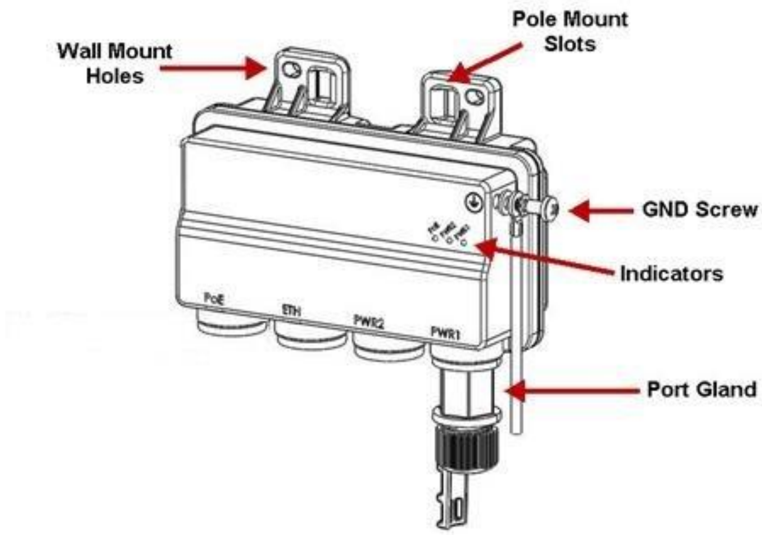


Figure 5: PoE Injector

The following PoE Injector is available:

- **PoE_Inj_AO_2DC_24V_48V** – Includes two DC power ports with power input ranges of -(18-60)V each.

3.3.1 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

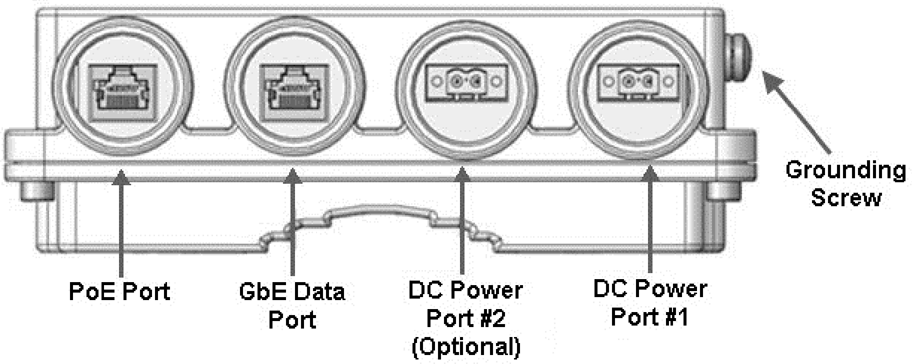


Figure 6: PoE Injector Ports

3.4 Voltage Alarm Thresholds and PMs

The allowed power input range for the IP-50CX 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-50CX 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.

4. Activation Keys

This chapter describes IP-50CX's activation key model. IP-50CX 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-50CX 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

4.1 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-50CX. 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.

4.2 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.

Note:	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.

4.3 Activation Key Reclaim

If a customer needs to deactivate an IP-50CX 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 300M and later purchased three upgrade activation keys to 350M, credit is given as if the customer had purchased three activation keys for 350M and two activation keys for 300M.

4.4 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	Addition Information
2nd Core Activation	SL-2nd-Core-Act.	Enables the second carrier of an IP-50CX. A separate activation key is required per radio.	Unique MultiCore Architecture
Advanced Security	SL-ADV-SEC	Enables Syslog Encryption and NTP Authentication. One activation key is required per device.	• NTP Support • Syslog Support
AES Encryption	SL-Encryption-AES256	Enables the use of AES-256 encryption for full radio payload encryption. A separate activation key is required per carrier. Note that: • 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. • 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.	• AES-256 Payload Encryption
ACM	SL-ACM	Adaptive Coding Modulation. A separate activation key is required per radio.	Adaptive Coding Modulation (ACM)
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

Name	Marketing Model	Description	Addition Information
Carrier Ethernet Transport (CET)	Refer to *Edge CET Node Activation Keys* on page 31.	Enables Carrier Ethernet Transport (CET) and a number of Ethernet services (EVCs), depending on the type of CET Node activation key: • Edge CET Node – Up to 8 EVCs. • Aggregation Level 1 CET Node – Up to 64 EVCs. • Aggregation Level 2 CET Node – Up to 1024 EVCs. A CET Node activation key also enables the following: • A GbE traffic port in addition to the port provided by the default activation key, for a total of 2 GbE traffic ports. • Network resiliency (MSTP/RSTP) for all services. • Full QoS for all services including basic queue buffer management (fixed queues buffer size limit, tail-drop only) and eight queues per port.	• Ethernet Service Model • Quality of Service (QoS) • Network Resiliency
Eth. OAM - Fault Management	SL-Eth-OAM-FM	Enables Connectivity Fault Management (FM) per Y.1731 (CET mode only). 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.[2]	
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-50CX Unit Description and Interfaces
Ethernet traffic ports - 10GbE	SL-10GE-Port	Enables the use of 10GbE ports. A separate activation key is required per port.	IP-50CX Unit Description and Interfaces
Ethernet traffic ports – 25GbE	SL-25GE-Port	Enables the use of 25GbE ports. A separate activation key is required per port.	IP-50CX Unit Description and Interfaces
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.	Link Aggregation Groups (LAG) and LACP
Multi Carrier ABC	SL-MC-ABC	Multi-Carrier ABC. A separate activation key is required per radio member.	Enhanced Multi-Carrier ABC

[2] Performance monitoring pursuant to Y.1731 is planned for future release.

Name	Marketing Model	Description	Addition Information
Multiband	SL-Enh-MC-ABC	For IP-50CX, this activation key is required for the main unit in a Layer 1 Link Aggregation configuration in order to add the Ethernet interface connected to the attached unit to the Multi-Carrier ABC group on the main unit.	Layer 1 Link Aggregation
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: • G.8032 One activation key is required per device.	Network Resiliency
Radio Capacity	Refer to *Capacity Activation* Keys on page 30.	Enables you to increase your system's radio capacity in gradual steps by upgrading your capacity activation key. Without a capacity activation key, each core has a capacity of 10 Mbps. A separate activation key is required per radio.	Capacity Summary
SD	SL-SD	Space Diversity. A separate activation key is required per radio member.[3]	Space Diversity
Secured Management	SL-Secure-Management	Enables secure management protocols (SSH, HTTPS, SFTP, SNMPv3, TACACS+, and RADIUS).	Secure Communication Channels
Single Sign-On (SSO)	SL-SSO	Enables single sign-on (SSO).	SSO Web Login with Microsoft Entra ID
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-XPIC	Enables the use of Cross Polarization Interference Canceller (XPIC). A separate activation key is required per radio member.	Cross Polarization Interference Canceller (XPIC)

Table 3: Capacity Activation Keys

Marketing Model	Marketing Description	Notes
SL-Capacity-50M	IP-20 SL - Capacity 50M	
SL-Capacity-100M	IP-20 SL - Capacity 100M	
SL-Capacity-150M	IP-20 SL - Capacity 150M	
SL-Capacity-200M	IP-20 SL - Capacity 200M	
SL-Capacity-225M	IP-20 SL - Capacity 225M	

[3] Space Diversity is planned for future release.

Marketing Model	Marketing Description	Notes
SL-Capacity-250M	IP-20 SL - Capacity 250M	
SL-Capacity-300M	IP-20 SL - Capacity 300M	
SL-Capacity-350M	IP-20 SL - Capacity 350M	
SL-Capacity-400M	IP-20 SL - Capacity 400M	
SL-Capacity-450M	IP-20 SL - Capacity 450M	
SL-Capacity-500M	IP-20 SL - Capacity 500M	
SL-Capacity-650M	IP-20 SL - Capacity 650M	
SL-Capacity-1G	IP-20 SL - Capacity 1G	
SL-Capacity-1.6G	IP-20 SL - Capacity 1.6G	
SL-Capacity-2G	IP-20 SL - Capacity 2G	
SL-Upg-50M-100M	IP-20 SL - Upg 50M - 100M	
SL-Upg-100M-150M	IP-20 SL - Upg 100M - 150M	
SL-Upg-150M-200M	IP-20 SL - Upg 150M - 200M	
SL-Upg-200M-225M	IP-20 SL - Upg 200M - 225M	
SL-Upg-225M-250M	IP-20 SL - Upg 225M - 250M	
SL-Upg-250M-300M	IP-20 SL - Upg 250M - 300M	
SL-Upg-300M-350M	IP-20 SL - Upg 300M - 350M	
SL-Upg-350M-400M	IP-20 SL - Upg 350M - 400M	
SL-Upg-400M-450M	IP-20 SL - Upg 400M - 450M	
SL-Upg-450M-500M	IP-20 SL - Upg 450M - 500M	
SL-Upg-500M-650M	IP-20 SL - Upg 500M - 650M	
SL-Upg-500M-2.5G	IP-20 Act.Key - Upg 500M -2.5G	
SL-Upg-650M-1G	IP-20 SL - Upg 650M - 1G	
SL-Upg-1G-1.6G	IP-20 SL - Upg 1G - 1.6G	
SL-Upg-1.6G-2G	IP-20 SL - Upg 1.6G - 2G	

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

Marketing Model	# of Bundled GbE Ports for User Traffic	Management Service	# of Point-to-Point (L1) Ethernet Services	# of CET (L2) Ethernet Services
SL-Agg-Lvl-2-CET-Node	2	Yes	Unlimited	1024

If a CET activation key is not generated on the IP-50CX 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)

5. Feature Description

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

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

This chapter includes:

- Unique MultiCore Architecture
- Innovative Techniques to Boost Capacity and Reduce Latency
- Ethernet Features
- Synchronization
- AES-256 Payload Encryption

5.1 Unique MultiCore Architecture

IP-50CX's MultiCore radio architecture is based on an advanced parallel radio processing engine built around Ceragon's proprietary baseband modem and RFIC chipsets. This architecture is optimized for parallel processing of multiple radio signal flows, and enables IP-50CX to multiply capacity and increase system gain in comparison with current technology.

Utilizing common processing resources at the kernel of the radio terminal, the MultiCore system reduces power consumption and maintains a small form-factor. This makes IP-50CX an advantageous choice for deployment in numerous heterogeneous network scenarios, such as small cells and fronthaul.

IP-50CX's parallel radio processing engine is what differentiates IP-50CX from other multiple-core solutions, which are really nothing more than multiple radio systems compacted into a single box. IP-50CX's MultiCore architecture enables IP-50CX to provide significant improvements in capacity and link distance, as well as low power consumption, smaller antennas, more efficient frequency utilization, less expensive frequency use, and a small form factor.

5.1.1 Flexible Operating Modes with MultiCore Architecture

IP-50CX's MultiCore architecture is inherently versatile and suitable for many different network deployment scenarios. IP-50CX can operate as a high-capacity, single-core solution. At any time in the network's growth cycle, the second core can be activated remotely for optimized performance.

To illustrate the many advantages of IP-50CX's MultiCore architecture, consider a generic, 1+0 single-core radio with high performance in terms of capacity, link distance, and antenna size.

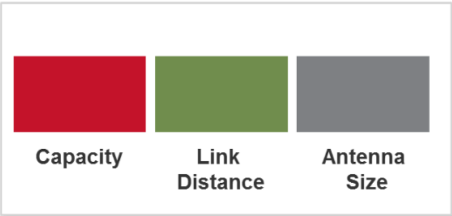


Figure 7: Performance Characteristics of Generic, 1+0 Single-Core Radio

IP-50CX can operate in single-core mode, with similar parameters to a standard radio, but with additional capacity due to its ability to operate at 4096 QAM modulation.

Activating the second core does not simply double the capacity of the IP-50CX, but rather, provides a package of options for improved performance that can be utilized in a number of ways, according to the requirements of the specific deployment scenario.

5.1.1.1 Doubling the Capacity

Turning on the IP-50CX's second core automatically doubles the IP-50CX's capacity. This doubling of capacity is achieved without affecting system gain or availability, since it results from the use of an additional core with the same modulation, Tx power, and Rx sensitivity. The IP-50CX also maintains the same small form-factor. Effectively, activating the second core provides a pure doubling of capacity without any tradeoffs.

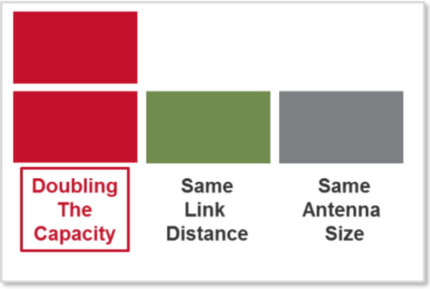


Figure 8: Doubling IP-50CX's Capacity by Activating Second Core

5.1.1.2 Doubling the Link Distance

The increased performance that IP-50CX's MultiCore architecture provides can be leveraged to increase link distance. IP-50CX splits the bitstream between its two cores using Enhanced Multi-Carrier Adaptive Bandwidth Control (ABC). This makes it possible to utilize a lower modulation scheme that significantly increases system gain for Tx power and Rx sensitivity. This enables IP-50CX to support longer signal spans, enabling operators to as much as double their link spans.

For example, consider an IP-50CX in a 1+0 configuration with only one core activated, transmitting 260 Mbps over a 28 MHz channel with 2048 QAM modulation. Activating the second core makes it possible to reduce the modulation to 64 QAM and still add capacity, from 260 Mbps to 280 Mbps, consisting of 2 x 140 Mbps over the 28 MHz channel. Reducing the modulation from 2048 QAM to 64 QAM delivers a 4dB improvement in Tx power and a 15dB improvement in Rx sensitivity, for a total increase of 19dB in system gain. This improved system gain enables the operator to double the link distance, while benefiting from a 20 Mbps increase in capacity.

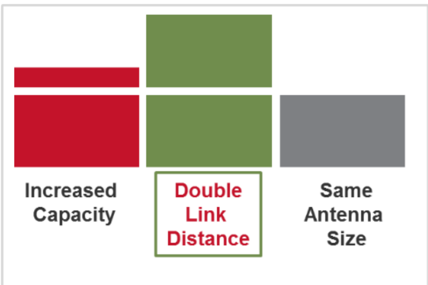


Figure 9: Doubling Link Span While Increasing Capacity by Activating Second Core

For additional information:

- Enhanced Multi-Carrier ABC

5.1.1.3 Reducing Antenna Size by Half

The increased system gain that IP-50CX's MultiCore architecture makes possible can be leveraged to scale down antenna size by as much as half. In general, each doubling of antenna size on one side of the link translates into 6dB in additional link budget. The 19dB increase in system gain that IP-50CX's MultiCore architecture can provide can be exploited to halve the antenna size. This uses 12dB of the 19dB system gain, leaving 7dB to further reduce antenna size on either side of the link. This enables the operator to realize CAPEX savings from the MultiCore deployment.

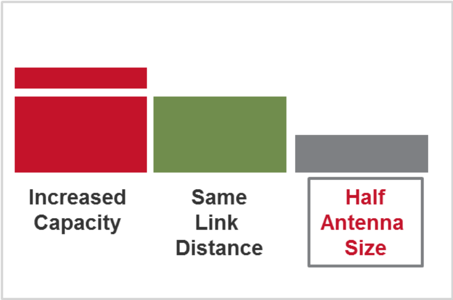


Figure 10: Utilizing Increased System Gain to Reduce Antenna Size

5.1.1.4 Frequency Decongestion and Lower License Fees

Another way in which the increased system gain that IP-50CX's MultiCore architecture makes possible can be leveraged is by taking advantage of the increased system gain to shift from congested and expensive frequency bands to uncongested and less costly higher frequency bands. The loss in link budget incurred by moving to higher frequencies is absorbed by the increased system gain provided by IP-50CX's MultiCore architecture. Relatively long-span links, which previously required operation in lower, more congested, and more expensive frequencies such as 6, 7, and 8 GHz, can be shifted to higher, less congested, and less expensive frequency bands such as 13 GHz with the help of IP-50CX's MultiCore architecture.

5.1.2 TCO Savings as a Result of MultiCore Architecture

The various ways described above in which IP-50CX MultiCore architecture can be leveraged to provide additional capacity, longer link distances, and smaller antenna side, all carry significant cost savings for operators.

Consider the common and practical scenario of a 1+0 link that must be upgraded to MultiCore 2+0 in order to accommodate growing demand for capacity. For a single-core system, the upgrade is a complicated process that requires:

- Purchasing a new radio unit.
- Sending an installation team to the site.
- Dismantling the existing radio unit.
- Replacing the single-mount radio-antenna interface with a coupler (for single polarization) or OMT (for dual polarization) to accommodate the two units.
- Re-installing the original radio unit along with the new radio unit.

- Connecting both radios to a switch in order to provide Layer 2 link aggregation (LAG), necessary to achieve a MultiCore 2+0 link.

These steps incur a high initial cost for re-installing and re-configuring the link, as well as high site leasing fees due to the additional equipment required, the larger footprint, and additional ongoing power consumption. The upgrade process involves hours of link down-time, incurring loss of revenue and impaired customer Quality of Experience (QoE) throughput the upgrade process. During its lifetime, the upgraded 2+0 single-core system will consume 100% more power than the 1+0 system and will be virtually twice as likely to require on-site maintenance.

With IP-50CX, network operators can initially install the MultiCore IP-50CX unit in single-core mode, with enough network capacity to meet current needs and the ability to expand capacity on the fly in the future. When an upgrade to MultiCore 2+0 becomes necessary, the operator merely needs to perform the following steps:

- Purchase an activation key for the second core.
- Remotely upload the activation key and activate the second core.

No site visits are required, and virtually no downtime is incurred, enabling customers to enjoy continuous, uninterrupted service. No additional switch is necessary, because IP-50CX can use Multi-Carrier ABC internally between the two cores to utilize the multi-channel capacity, in a much more efficient manner than with Layer 2 LAG. Network operators benefit from much lower power consumption than 2+0 systems made up of separate, single-core radio units, and site leasing fees do not increase since no additional hardware is required.

The following table summarizes the cost benefits of IP-50CX's MultiCore technology in terms of TCO.

Table 6: TCO Comparison Between Single-Core and MultiCore Systems

	Single-Core system	**MultiCore system**
Initial Installation	1+0 link with 1+0 antenna mediation device (remote or direct mount).	2+0 installation (remote or direct mount). Only one core has an activation key and is activated.
Upgrade to 2+0	• Obtain new radio equipment • Send technical team to both ends of the link (at least two site visits). • Dismantle existing radio and mediation device. • Install new mediation device (OMT or splitter). • Re-install old radio with new radio. • Obtain and install Ethernet switch for 2+0 L2 LAG.	• Obtain activation key for second core. • Activate second core remotely. • Remotely define the link as 2+0 with L1 Multi-Carrier ABC (more efficient than LAG).

	Single-Core system	MultiCore system
Downtime	Hours of downtime for complete reconfiguration of the link. Negative impact on end-user QoE.	Negligible downtime.
Power consumption	100% more than 1+0 link (even more with external switch).	Only 55% more power consumption than 1+0 configuration (single core).
Site leasing fees	Approximately double, since equipment is doubled.	No impact, MultiCore system within same small form factor unit
Warehouse management	Complicated, with different equipment for different deployment scenarios (standard/high power, low/high capacity).	Simple with single-spare, versatile radio for many deployment scenarios.

5.2 Innovative Techniques to Boost Capacity and Reduce Latency

IP-50CX utilizes Ceragon's innovative technology to provide a high-capacity low-latency solution. The total switching capacity of IP-50CX is 193 Gbps, with a system capacity of 6.5 Gbps in a 4+0 configuration. IP-50CX also utilizes established Ceragon technology to provide low latency, representing a 50% latency reduction for Ethernet services compared to the industry benchmark for wireless backhaul.

Ceragon was the first to introduce hitless and errorless Adaptive Coding Modulation (ACM) to provide dynamic adjustment of the radio's modulation. ACM shifts modulations instantaneously in response to changes in fading conditions. IP-50CX utilizes Ceragon's advanced ACM technology, and extends it to the range of BPSK to 4096 QAM.

In a 4+0 Layer 1 Link Aggregation configuration, two IP-50CX units operate together to form a single link connected to the switch via a single cable. Link Aggregation can also be used with an IP-50CX and a third-party device.

Layer 1 Aggregation can be used to add an IP-50CX to existing IP-20C deployments, thereby significantly increasing the capacity of existing IP-20 links.

IP-50CX can also be used in Multiband configurations with IP-50E to provide robust links that combine microwave with E-band transmissions.

IP-50CX supports Cross Polarization Interference Canceller (XPIC). XPIC enables operators to double their capacity with a single IP-50CX unit directly mounted to the antenna. The dual core IP-50CX utilizes dual-polarization radio over a single-frequency channel, thereby transmitting two separate carrier waves over the same frequency, but with alternating polarities. XPIC can be used in standard MultiCore 2+0 dual polarization configurations.

IP-50CX can be used in MultiCore 1+1 and 2+2 HSB configurations. A 1+1 configuration can easily be scaled up into a 2+2 configuration by activating the second core on each IP-50CX unit.

This section includes:

- Capacity Summary
- Space Diversity
- Enhanced Multi-Carrier ABC
- Layer 1 Link Aggregation
- Multiband with Layer 1
- Adaptive Coding Modulation (ACM)
- Cross Polarization Interference Canceller (XPIC)
- Unit Redundancy
- ATPC
- Radio Signal Quality PMs

5.2.1 Capacity Summary

Each of the two cores in an IP-50CX unit can provide the following radio capacity:

- **Supported Channels (ETSI)** –14/28/40/56/70/80/112/140/224 MHz channels
- **Supported Channels (FCC)** –20/25/30/40/60/80/160 MHz channels
- **All licensed bands** –L6, U6, 7, 8, 10, 11, 13, 15, 18, 23, 26, 28, 32, 38, 42 GHz
- **High Modulation** – BPSK to 4096 QAM

For additional information:

- Radio Capacity Specifications

5.2.2 Space Diversity

Note:	Space Diversity is planned for future release.

IP-50CX offers Baseband Combining (BBC) Space Diversity (SD), with antenna separation based on SD requirements.

In SD configurations, the carrier connected to the diversity antenna is muted to achieve a configuration that consists of a single transmitter and two receivers.

When IP-50CX is configured for SD operation, the signal is combined at the Baseband level to improve signal quality selective fading.

5.2.2.1 1+0 Space Diversity

A Space Diversity configuration utilizes a single IP-50CX on each side of the link, with both radio carriers activated. The second carrier is muted. On the receiving side, the signals are combined to produce a single, optimized signal.

5.2.2.2 1+1 HSB with Space Diversity

A 1+1 HSB-SD configuration utilizes two IP-50CX units on each side of the link, with both radio carriers activated. On each unit, the carrier connected to the diversity antenna is muted. On the receiving side, the signals are combined in the active unit to produce a single, optimized signal. The link is protected via Unit Redundancy, so that if a switchover occurs, the standby unit becomes the activate unit, and the link continues to function with full space diversity.

5.2.3 Enhanced Multi-Carrier ABC

Multi-Carrier Adaptive Bandwidth Control (ABC) is an innovative technology that creates logical bundles of multiple radio links and optimizes them for wireless backhaul applications. Multi-Carrier ABC enables separate radio carriers to be shared by a single Ethernet port. This provides an Ethernet link over the radio with double capacity, while still behaving as a single Ethernet interface.

IP-50CX utilizes Enhanced Multi-Carrier ABC, which provides excellent traffic distribution among the carriers in the group. In Enhanced Multi-Carrier ABC mode, traffic is divided among the carriers optimally at the radio frame level without requiring Ethernet link aggregation (LAG). Load balancing is performed without regard to the number of MAC addresses or the number of traffic flows. During fading events which cause ACM modulation changes, each carrier fluctuates independently with hitless switchovers between modulations, increasing capacity over a given bandwidth and maximizing spectrum utilization. The result is close to 100% utilization of radio resources in which traffic load is balanced based on instantaneous radio capacity per carrier.

The following diagram illustrates the Enhanced Multi-Carrier ABC traffic flow.

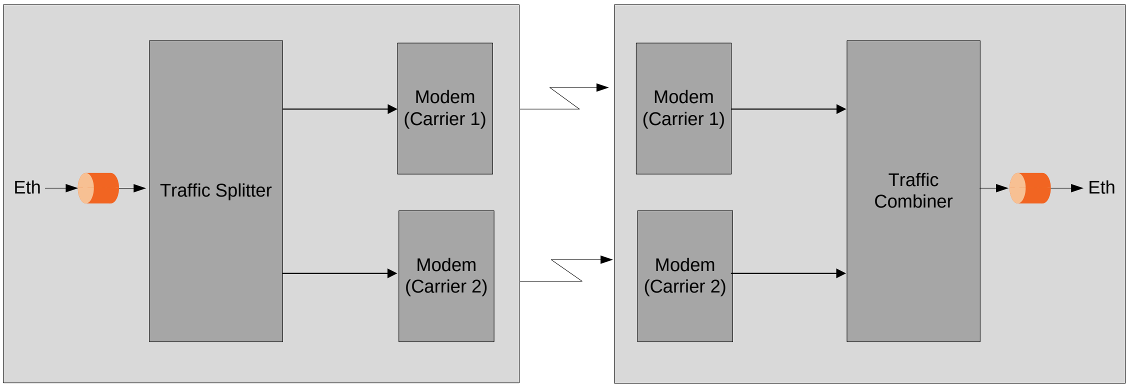


Figure 11: Enhanced Multi-Carrier ABC Traffic Flow

5.2.3.1 Enhanced Multi-Carrier ABC Operation

Multi-Carrier ABC is designed to achieve 100% utilization of available radio resources by optimizing the way traffic is distributed between the multiple wireless links. Traffic is forwarded over available radio carriers using proprietary Layer 1 distribution. This enhances load balancing.

Traffic distribution is proportional to the available bandwidth in every link:

- If both links have the same capacity, half the data is sent through each link.
- In ACM conditions, the links could be in different modulations; in this case, data is distributed proportionally in order to maximize the available bandwidth.

IP-50CX's proprietary Layer 1 distribution mechanism enables IP-50CX's Enhanced Multi-Carrier ABC implementation to maintain optimal load balancing that accounts for the condition of each radio link at any given moment. This means that if a link shifts to a lower ACM modulation point, the Enhanced Multi-Carrier ABC load balancing mechanism is notified immediately and adjusts the traffic distribution by sending less traffic over the link with the lower modulation and more traffic to links operating at a higher modulation. If there is a failure in one or more of the links, the load balancing mechanism implements graceful degradation by directing traffic to the operational links.

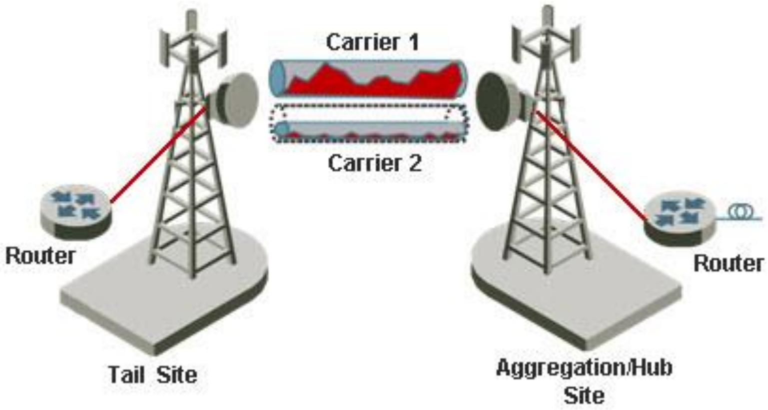


Figure 12: Enhanced Multi-Carrier ABC Load Balancing with Different ACM Points

5.2.3.2 Graceful Degradation of Service

Enhanced Multi-Carrier ABC provides for protection and graceful degradation of service in the event that one of the links fails. This ensures that if one link is lost, not all data is lost. Instead, bandwidth is simply reduced until the link returns to service.

Graceful degradation in Enhanced Multi-Carrier ABC is achieved by blocking one of the radio links from Enhanced Multi-Carrier ABC data. When a link is blocked, the transmitter does not distribute data to this link and the receiver ignores it when combining.

The minimum profile of the two radio carriers in the Enhanced Multi-Carrier ABC group can be set to any value, as long as they are set to the same value. This enables the user to determine the point at which the group is placed in a Down state. This can be used in conjunction with Automatic State Propagation (ASP) to ensure that link degradation is propagated to an upstream switch whenever the link provides less than the desired capacity.

Each carrier can change its ACM profile, with a maximum of 30 msec between each switch in modulation. There is no limitation upon the profile difference between carriers, so that one carrier can be operating at the lowest possible profile (BPSK) while the other is operating at the highest possible profile (4096 QAM).

5.2.3.3 Configuring Enhanced Multi-Carrier ABC

It is recommended to use the same radio script and ACM settings on both radio carriers in the Multi-Carrier ABC group. The user must create an Enhanced Multi-Carrier ABC group containing both radio carriers.

To delete the Enhanced Multi-Carrier ABC group, the user must first remove the members from the group, and then delete the group.

5.2.4 Layer 1 Link Aggregation

Note:	ETH-BN with Layer 1 Link Aggregation is planned for future release.

Layer 1 Link Aggregation provides an efficient way to group radio links with an Ethernet interface so as to combine the radio links into a single high-capacity link, connected by a single cable to the external switch. The links can include different channels and frequencies, enabling the use of creative solutions that optimize the available frequency spectrum.

Layer 1 Aggregation configurations with IP-50CX utilize an IP-50CX as the main unit and/or the attached unit. When the IP-50CX is the main unit, it is connected to the switch and performs traffic distribution based on IP-50CX's Enhanced Multi-Carrier ABC technology.

CeraOS 13.1 supports 4+0 Layer 1 Link Aggregation. The following configurations are available:

- 4+0 with two IP-50CX devices
- 4+0 with IP-50CX (main) and IP-20C (attached)
- 3+0 with IP-50CX (main) and a third-party device (attached)

Additionally, the following IP-50CX Layer 1 Aggregation configuration is planned for future release:

- 4+0 Layer 1 Aggregation using an IP-50CX and an IP-50C

5.2.4.1 4+0 Layer 1 Link Aggregation

4+0 Layer 1 Link Aggregation aggregates an Ethernet link and four radio carriers into a single link with a single-cable connection to the switch, enabling operators to double the capacity of a 2+0 link. A 4+0 link with Layer 1 Link Aggregation using two IP-50CX devices can provide 2.5 Gbps connectivity between the devices, enabling total link capacity of up to 6 Gbps when wide channels are used.

In a 4+0 Aggregation configuration, each device can use a different frequency, providing operators with more flexibility to utilize the available frequency spectrum in whatever way is most efficient.

A 4+0 Link Aggregation link consists of a main and attached unit:

- **Main Unit** – Connected to the external switch and performs traffic distribution between itself and the attached unit based on IP-50CX's Enhanced Multi-Carrier ABC technology. The main unit must be an IP-50CX.
- **Attached Unit** – Receives a portion of the traffic from the main unit and forwards it to a Multi-Carrier ABC group for transmission. The attached unit can be an IP-50CX, an IP-20C, or a third party device.

Note:	The third-party device can be a single-carrier device for a 3+0 link.

The main unit is connected to the external switch (the Ingress port). It is recommended to use Eth 3 (P4) as the Ingress port.

Traffic is passed between the main and attached units via a data cable that connects Ethernet ports on the main unit and the attached unit (the Traffic Connection). For configurations using two IP-50CX devices, this connection supports up to 2.5 Gbps, for a total capacity of up to 6 Gbps. For other configurations, this is a 1 Gbps connection.

It is recommended to use the following ports for the Traffic Connection:

- IP-50CX (main or attached): Eth 2 (P3)
- IP-20C (attached): Eth 2
- Third-party device: Any appropriate Ethernet port

Make sure the port speed is configured the same on the main and attached units.

A Multi-Carrier ABC group will generally be configured on each unit. Each group should include both of the unit's radio carriers. On the main unit, the Ethernet interface connected to the attached unit (the "Traffic Port") must be added to the group using Enhanced Multi-Carrier ABC technology.

Note: It is also possible to use only one carrier on the attached unit, for a 3+0 configuration.

You must configure services for traffic on both the main unit and the attached unit. The service on the main unit connects the Ingress port and the Enhanced Multi-Carrier ABC group. The service on the attached unit connects the Traffic port and the Multi-Carrier ABC group.

Each unit is managed separately and independently. In-band management can be configured so that both units are managed over the link. Management is passed to and from the attached unit via the Traffic Connection.

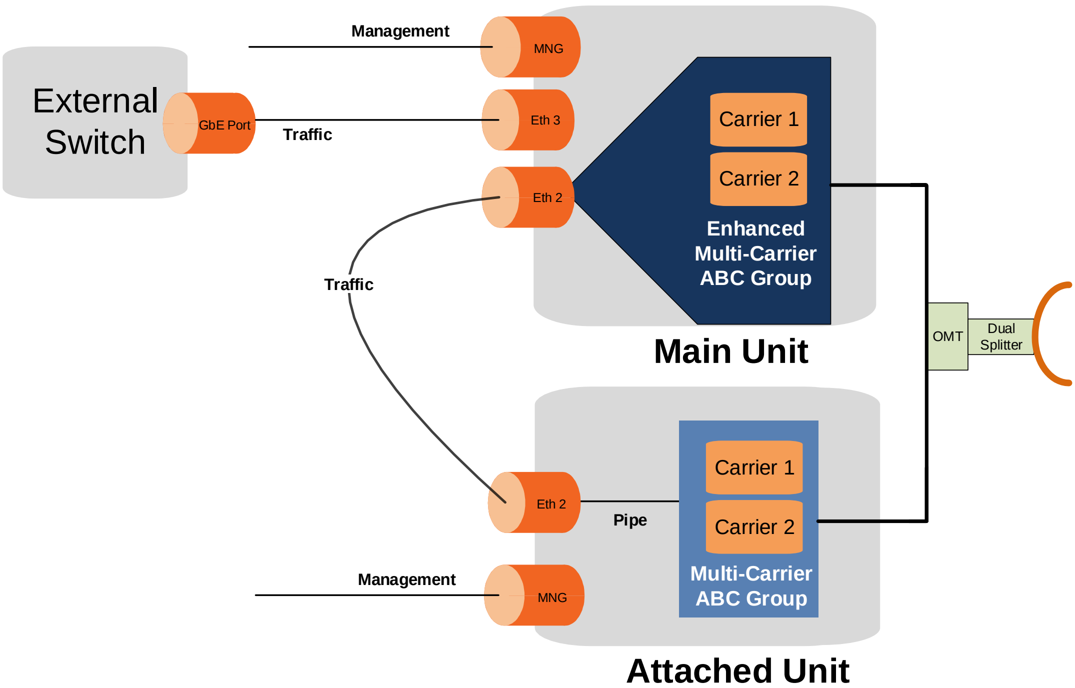


Figure 13: 4+0 Layer 1 Link Aggregation

The two IP-50CX units, or an IP-50CX and IP-20C, can be connected to a single antenna using a Dual Splitter and an OMT. Remote-mount configurations are also available. The hardware configuration for 4+0 Link Aggregation uses the same mediation devices as IP-50C and IP-20C.

5.2.4.2 Layer 1 Link Aggregation and Line Redundancy

Line redundancy is available for 4+0 Layer 1 Link Aggregation with two IP-50CX units.

Note:	Line Redundancy is not available if the attached unit is an IP-20C or third-party device. In CeraOS 13.1, AES payload encryption cannot be used in a Layer 1 Link Aggregation configuration with Line Redundancy.

Line Redundancy means the external switch is connected to both the main and the attached units via an optical splitter. The optical splitter routes traffic between the Ethernet port on the external switch and an Ethernet port on both the main and the attached unit.

Optionally, Line Redundancy can include management redundancy for external management, using an additional split cable between the management ports of each unit and an external management station.

In normal operation, traffic and management pass only between the external switch and the main unit, and the interface between the switch and the attached unit is turned off. In the event of switchover, the link between the external switch and the attached unit is automatically activated by switching off the interface between the external switch and the main unit and switching on the interface between the external switch and the attached unit so that traffic and management are passed between the external switch and the attached unit.

A set of services for traffic and management must be configured on the attached unit in parallel to the services on the main unit. These services are configured in Operational state. The Line Redundancy mechanism deactivates the services in normal operating state based on the Line Redundancy role configurations, and activates them only in the event of switchover to support the flow of traffic and management from the external switch to the attached unit’s radio.

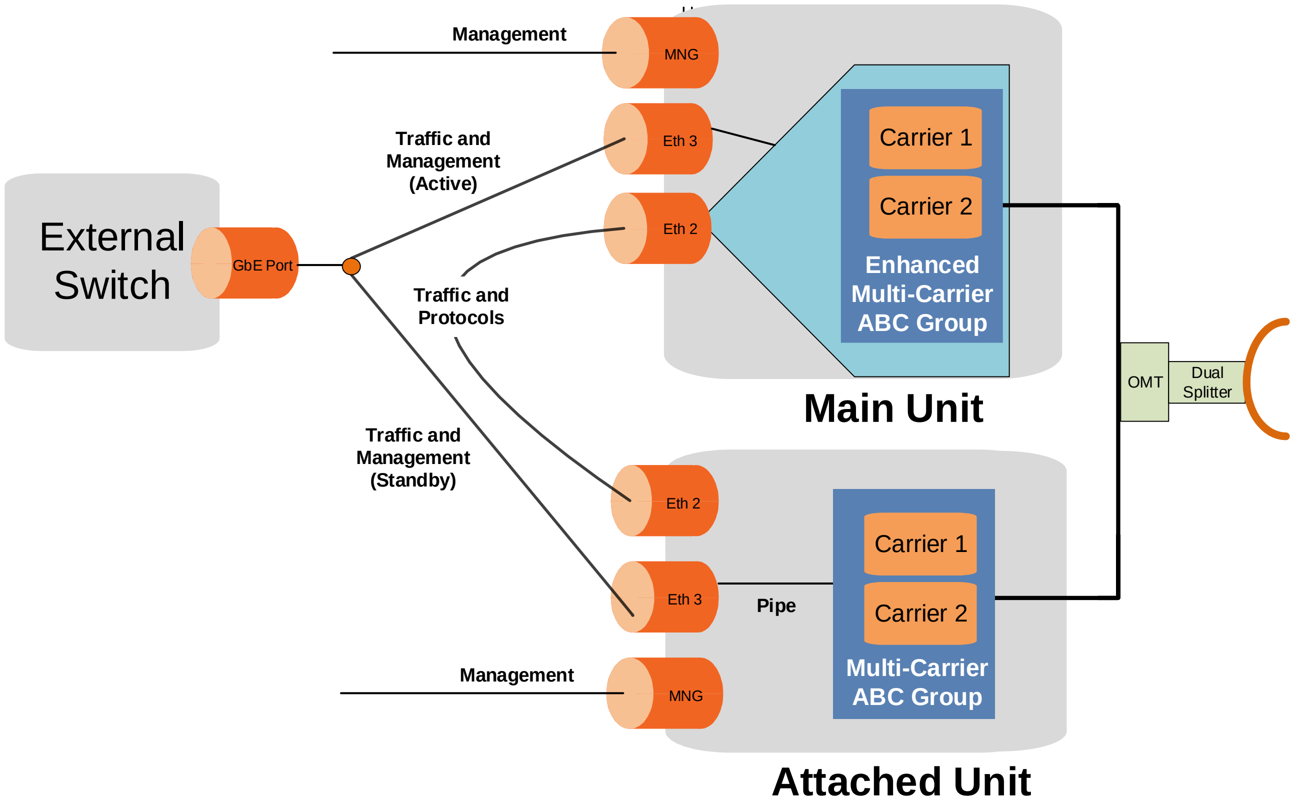


Figure 14: 4+0 IP-50CX with Layer 1 Link Aggregation and Line Redundancy

The following events trigger traffic switchover:

Note:	Radio failure on the main unit does not trigger switchover. Since traffic continues to be passed between the main unit and the attached unit, the attached unit's radio link continues to operate.

- Failure of traffic cable between external switch and main unit:
  - Traffic interfaces with the external switch on local and remote main units are automatically set to Down.
  - Traffic services are automatically disabled on the local and remote main units.
  - Traffic interfaces with the external switch on local and remote attached units are automatically set to Up.
  - Traffic services are automatically enabled on the local and remote attached units.
  - The management service points on the radio of the local and remote attached units are automatically enabled.
- Traffic cable between the main and attached unit fails:
  - The management service points on the radio of the local and remote attached units are automatically enabled.
  - On the remote side of the link, the interfaces connecting the traffic cable between the main and attached unit are automatically set to Down.

- Failure of main unit:
  - Traffic interfaces with the external switch on the remote main unit is automatically set to Down.
  - Traffic services are automatically disabled on the remote main unit.
  - Traffic interfaces with the external switch on local and remote attached units are automatically set to Up.
  - Traffic services are automatically enabled on the local and remote attached units.
  - The management service points on the radio of the local and remote attached units are automatically enabled.
  - On the remote side of the link, the interfaces connecting the traffic cable between the main and attached unit are automatically set to Down.

When the failure is rectified, the configuration automatically reverts to its normal operational configuration after expiration of a Wait to Restore (WTR) timer. Revertive mode cannot be disabled. However, the WTR timer is user-configurable.

Lockout and forced switch are available to manually change the state of the configuration (force-switch) or to manually force the configuration to remain in its current state (lockout). Lockout can be used to override Revertive mode and keep the configuration in switchover mode, should this be necessary.

Redundancy for external management operates independently of Line Redundancy for traffic. Using a split management cable attached to the management ports of each unit and an external management station, you can ensure that external management remains available even if management connectivity to one of the units is lost.

The following table lists the cable recommended for external management redundancy.

Table 7: Cable for External Management Redundancy

Cable	Marketing Model	Description
Management Splitter Cable (P2 to P2 and External Management Station)	CBL-IP20-EXT-PROT+MGMT	CABLE,RJ45F TO 2XRJ45,1.34M,CAT-5E,WITH MALE TO MALE CONNECTION

With external management redundancy, only one management port is up at any one time. External management switching is independent of traffic switchover. The following events trigger external management switchover:

- Management interface failure
- Unit failure
- On main unit, Enhanced Multi-Carrier ABC group operational status is Down

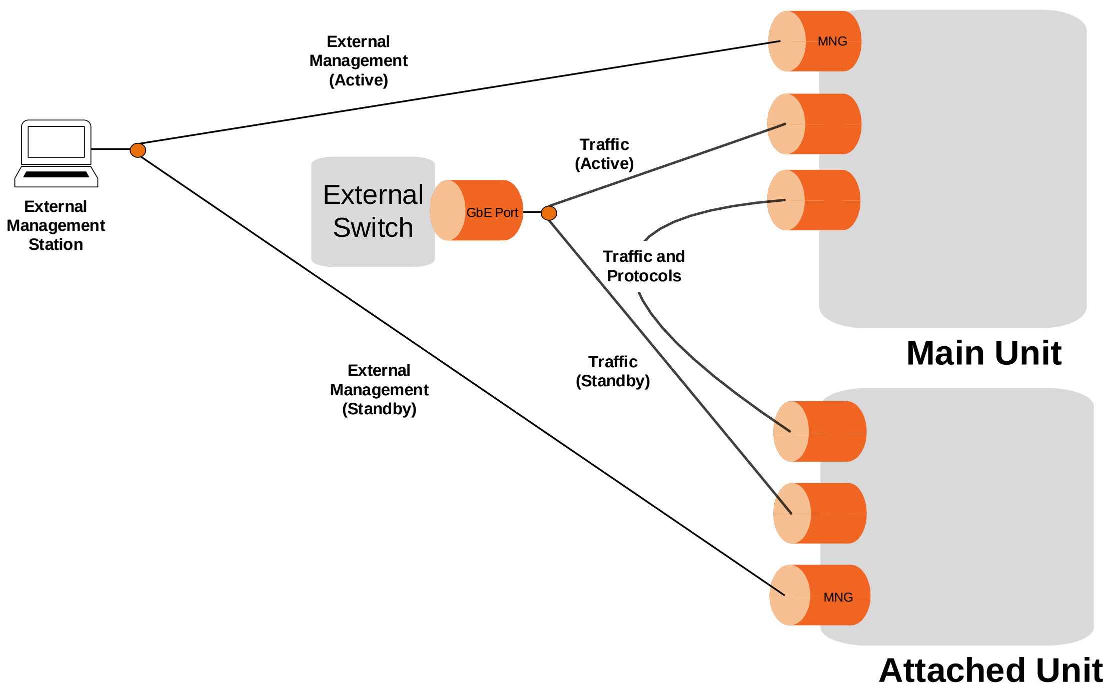


Figure 15: Layer 1 Link Aggregation with Line and External Management Redundancy

5.2.4.3 Synchronization in a Layer 1 Link Aggregation Link

SyncE and 1588 PTP can be used with Layer 1 Aggregation. SyncE and 1588 PTP can be configured for both the main unit and the attached unit. Synchronization messages are passed between the units via the traffic cable between the units.

5.2.5 Multiband with Layer 1 Link Bonding

IP-50CX can be used in Multiband configurations with IP-50E.

Multiband bundles E-Band and microwave radios in a single group that is shared with an Ethernet interface.

Layer 1 Link Bonding enables operators to optimize the capacity of a Multiband link by combining the capacity of the E-Band and Multiband links into a single link of up to 14 Gbps. This is achieved when the IP-50E is used in 2000 MHz channels, providing 10 Gbps, while the IP-50CX is operating in XPIC mode over 224 MHz channels, providing 4 Gbps at high profiles.

A Multiband link with Layer 1 Link Bonding is highly resilient because it combines the high capacity of E-Band with the high resiliency of Microwave. The advantage of Layer 1 Link Bonding is that it enables the E-Band and Microwave links to aggregate their capacity, rather than utilizing the Microwave link as more of a backup to 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.

A special Multiband antenna can be used for Multiband configurations. This antenna transmits and receives both E-band and microwave signals. Both units (IP-50E and IP-50CX) are connected to this antenna via direct mount.

The marketing model for Multiband antennas uses the following syntax:

Am-B3-d-ff/80-pl/ph-vn

Where:

- 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: Rosenberger, 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 both radios are operating with Single Polarization. The manufacturer is MTI.

Am-2-18/80-SP/SP-MT

For a full list of available Multiband antennas, refer to the Price List or check with your Ceragon representative. For a fuller description of Multiband with Layer 1 Link Bonding, refer to the Technical Description for the IP-50E.

Note:	IP-50CX can also be used in Link Bonding configurations with IP-20N and IP-20A units using TCC-U. For more information, refer to the Technical Description for IP-20N and IP-20A.

5.2.6 Adaptive Coding Modulation (ACM)

Related topics:

- Cross Polarization Interference Canceller (XPIC)
- Quality of Service (QoS)

IP-50CX employs full-range dynamic ACM. IP-50CX's ACM mechanism copes with 100 dB per second fading in order to ensure high transmission quality. IP-50CX's ACM mechanism is designed to work with IP-50CX'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-50CX'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 throughout decrease while these sessions recover.

5.2.6.1 Eleven Working Points

IP-50CX implements ACM with 13 available working points, as shown in the following table:

Table 8: ACM Working Points (Profiles)

Working Point (Profile)	Modulation
Profile 0	BPSK
Profile 1	QPSK
Profile 2	8 QAM
Profile 3	16 QAM
Profile 4	32 QAM
Profile 5	64 QAM
Profile 6	128 QAM
Profile 7	256 QAM
Profile 8	512 QAM
Profile 9	1024 QAM (Strong FEC)
Profile 10	1024 QAM (Light FEC)
Profile 11	2048 QAM
Profile 12	4096 QAM

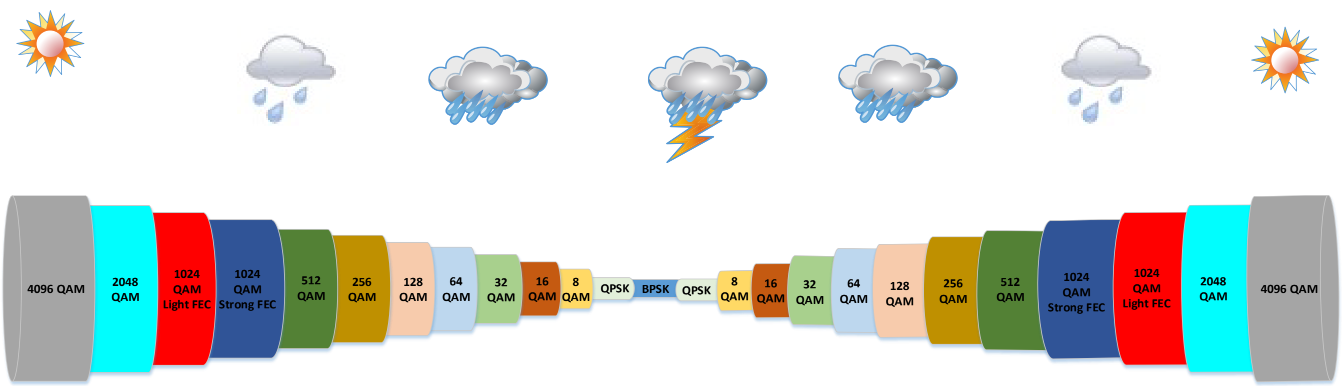


Figure 16: Adaptive Coding and Modulation with 13 Working Points

5.2.6.2 Hitless and Errorless Step-by Step Adjustments

ACM works as follows. Assuming a system configured for 128 QAM with ~170 Mbps capacity over a 28 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 to ~140 Mbps. 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.

In IP-50CX units that are utilizing two cores, ACM profile switches are performed independently for each core.

5.2.6.3 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.

In the case of XPIC/ACM scripts, all the required conditions for XPIC apply.

The user can define a minimum and maximum profile. For example, if the user selects a maximum profile of 10, the system will not climb above the profile 10, even if channel fading conditions allow it.

5.2.6.4 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.

5.2.6.5 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.

5.2.6.6 ACM Benefits

The advantages of IP-50CX's dynamic ACM include:

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

5.2.6.7 ACM and Built-In QoS

IP-50CX's ACM mechanism is designed to work with IP-50CX'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-50CX to discard only low priority frames as conditions deteriorate.

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

5.2.6.8 ACM in MultiCore HSB Configurations

When ACM is activated in a protection scheme such as 1+1 HSB, the following ACM behavior should be expected:

- In the TX direction, the Active TX will follow the remote Active RX ACM requests (according to the remote Active Rx MSE performance).
- The Standby TX might have the same profile as the Active TX, or might stay at the lowest profile (profile 0). That depends on whether the Standby TX was able to follow the remote RX Active unit's ACM requests (only the active remote RX sends ACM request messages).
- In the RX direction, both the active and the standby units follow the remote Active TX profile (which is the only active transmitter).

5.2.6.9 ACM with Adaptive Transmit Power

This feature requires:

- ACM script

When planning ACM-based radio links, the radio planner attempts to apply the lowest transmit power that will perform satisfactorily at the highest level of modulation. During fade conditions requiring a modulation drop, most radio systems cannot increase transmit power to compensate for the signal degradation, resulting in a deeper reduction in capacity. IP-50CX is capable of adjusting power on the fly, and optimizing the available capacity at every modulation point.

The following figure contrasts the transmit output power achieved by using ACM with Adaptive Power to the transmit output power at a fixed power level, over an 18-23 GHz link. This figure shows how without Adaptive Transmit Power, operators that want to use ACM to benefit from high levels of modulation (e.g., 2048 QAM) must settle for low system gain, in this case, 16 dB, for all the other modulations as well. In contrast, with IP-50CX's Adaptive Transmit Power feature, operators can automatically adjust power levels, achieving the extra system gain that is required to maintain optimal throughput levels under all conditions.

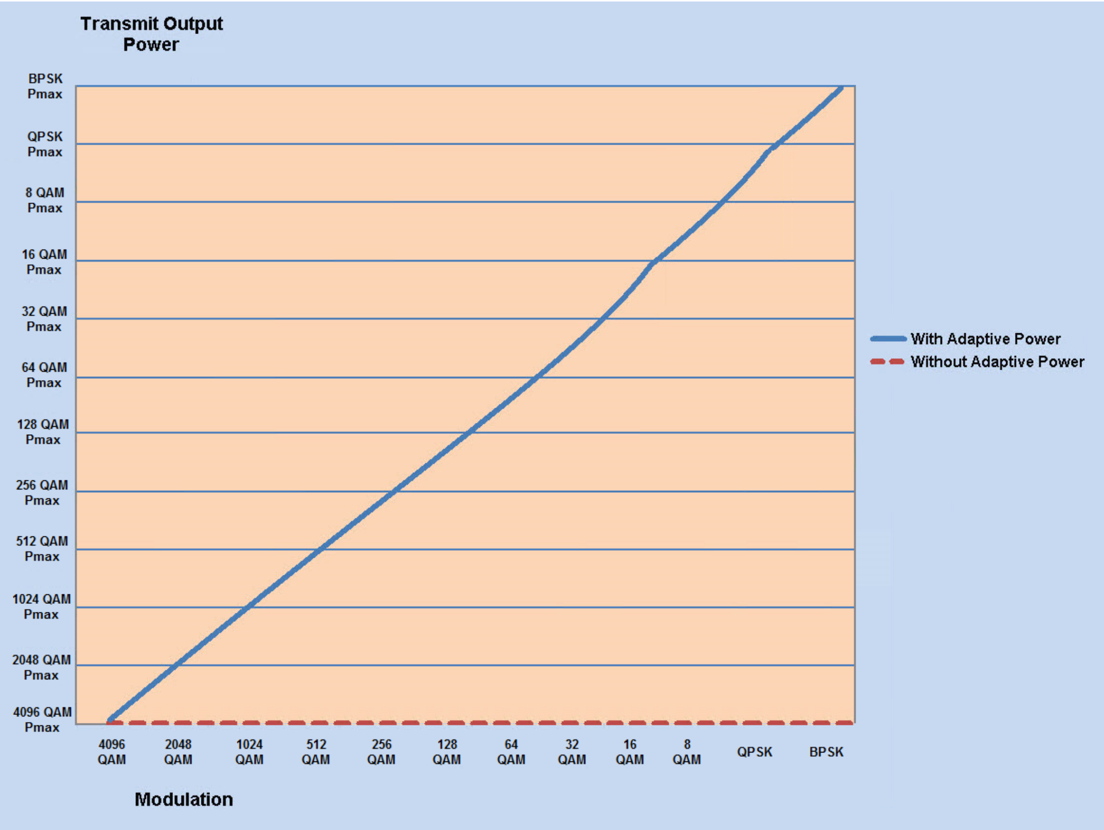


Figure 17: IP-50CX ACM with Adaptive Power Contrasted to Other ACM Implementations

5.2.7 Cross Polarization Interference Canceller (XPIC)

This feature requires:

- 2+0, 2+2
- Enhanced Multi-Carrier ABC for each XPIC pair
- XPIC script

XPIC is one of the best ways to break the barriers of spectral efficiency. Using dual-polarization radio over a single-frequency channel, a single dual core IP-50CX unit transmits two separate carrier waves over the same frequency, but using alternating polarities. 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.

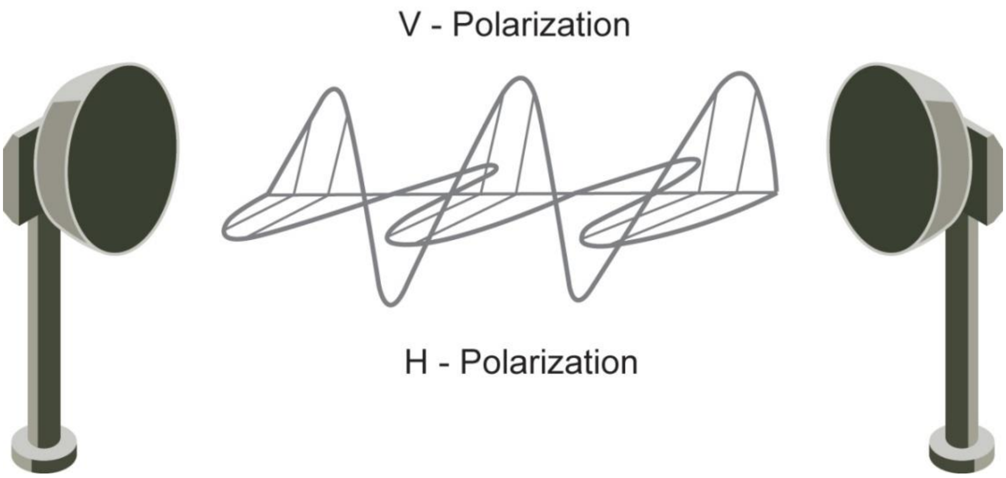


Figure 18: Dual Polarization

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-50CX's XPIC algorithm enables detection of both streams even under the worst levels of XPD such as 10 dB. IP-50CX accomplishes this by adaptively subtracting from each carrier the interfering cross carrier, at the right phase and level. For high-modulation schemes such as 2048 QAM, operating at a frequency of 28 GHz, an improvement factor of more than 23 dB is required so that cross-interference does not adversely affect performance. In this scenario, IP-50CX's XPIC implementation provides an improvement factor of approximately 26 db.

5.2.7.1 XPIC Benefits

The advantages of IP-50CX's XPIC option include BER of 10e-6 at a co-channel sensitivity of 10 dB.

XPIC enables IP-50CX links of up to 2 Gbps, consisting of 1 Gbps per carrier. XPIC can be installed in either of the following configurations:

- Direct Mount – The IP-50CX unit is connected to the antenna via an OMT.
- Remote Mount – The IP-50CX unit is connected to the antenna via two flexible waveguides. Some configurations also require an OMT.

5.2.7.2 XPIC-Ready 1+0 Links

An IP-50CX can be installed initially in single-core mode, hardware ready for 2+0 Dual Polarization (XPIC). Later, when the operator is ready to expand network capacity, the link can be converted to a 2+0 XPIC link remotely by uploading and installing the activation keys for XPIC and for the second core and activating the second core and XPIC.

When installing a 1+0 link which is hardware ready for 2+0 XPIC, the operator must plan and install the link as if it is immediately being configured as an XPIC link. This includes both link budget calculation and hardware installation.

The OMTs must be carefully aligned according to the XPIC alignment procedure. Activation key Demo Mode can be used to activate the second radio interface for purposes of alignment. After completing alignment, the regular activation key should be installed and the link configured for 1+0 operation.

Failure to follow these steps may limit the ability to remotely upgrade a 1+0 link to a 2+0 XPIC link at a later date.

5.2.7.3 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.

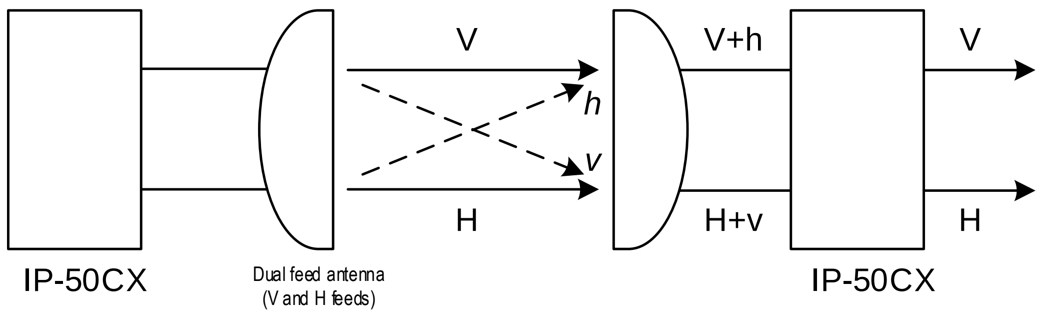


Figure 19: XPIC Implementation

Note:	For the sake of simplicity, a dual feed V and H antenna is depicted. IP-50CX can be directly mounted using a mediation device in this configuration.

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.

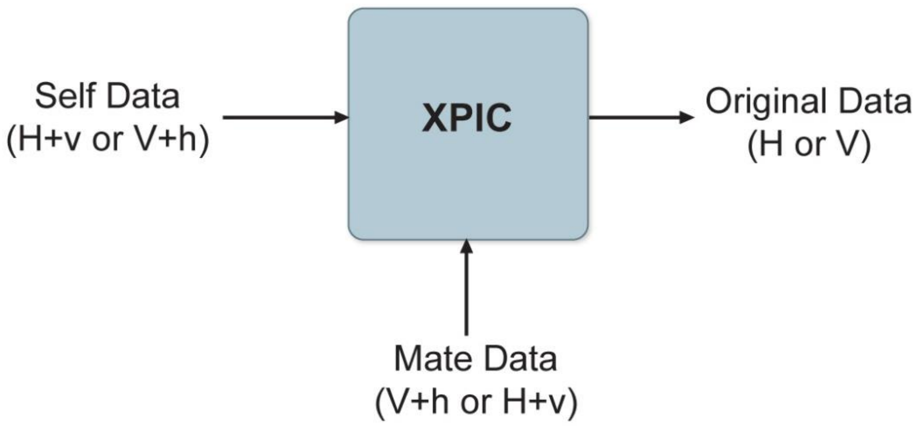


Figure 20: XPIC – Impact of Misalignments and Channel Degradation

IP-50CX's XPIC reaches a BER of 10e-6 at a co-channel sensitivity of 10 dB. The improvement factor in an XPIC system is defined as the SNR@threshold of 10e-6, with or without the XPIC mechanism.

5.2.7.4 Conditions for XPIC

Most IP-50CX radio scripts support XPIC. See *Radio Scripts* on page 168.

The user must enable XPIC, after loading the script.

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.

If any of these conditions is not met, an alarm will alert the user. In addition, events will inform the user which conditions are not met.

5.2.8 Unit Redundancy

IP-50CX offers 1+1 and 2+2 HSB protection configurations, which include HSB radio protection and unit redundancy.

1+1 unit protection utilizes two IP-50CX units operating in single core mode, with a single antenna. This provides hardware redundancy for Ethernet traffic and HSB radio redundancy. One IP-50CX operates in active mode and the other operates in standby mode. If a switchover occurs, the roles are switched. The active unit goes into standby mode and the standby unit goes into active mode.

2+2 HSB protection utilizes two IP-50CX units operating in dual core mode, with a single antenna, to provide hardware redundancy for Ethernet traffic and HSB radio redundancy in a dual core configuration. In effect, a MultiCore 2+2 HSB configuration is a protected MultiCore 2+0 configuration.

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.

Redundancy for the Ethernet interfaces is provided as follows:

- **Split Protection Mode** – For the SFP ports (Eth 2 and Eth 3), the port on the active unit and the port on the standby unit are connected to a single port on the external switch via an optical Y-cable.
- **Line Protection Mode** – For the RJ-45 traffic port (Eth 1), as well as SFP ports with electrical SFPs, traffic is routed from two Ethernet ports on the external switch to Eth 1 on the active unit and Eth 1 on the standby unit.

Notes:	Line Protection Mode is planned for future release. For Line Protection mode, the external switch must support LACP.

In a 2+2 HSB configuration, each IP-50CX monitors both of its radio carriers. If the active IP-50CX detects a radio failure in either of its radio carriers, it initiates a switchover to the standby IP-50CX.

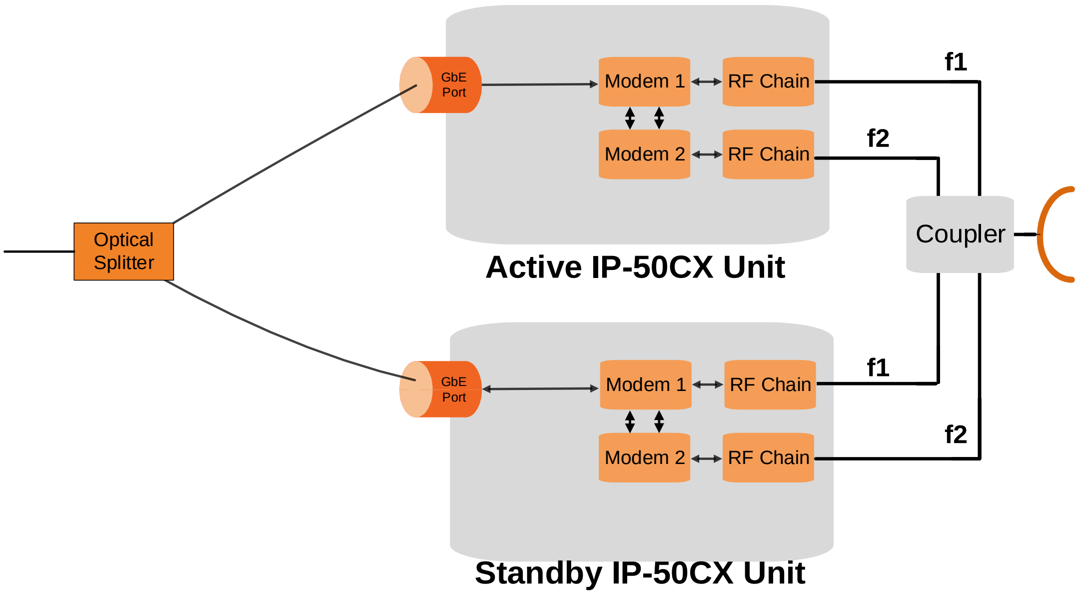


Figure 21: 2+2 Unit Redundancy and HSB – Split Protection Mode

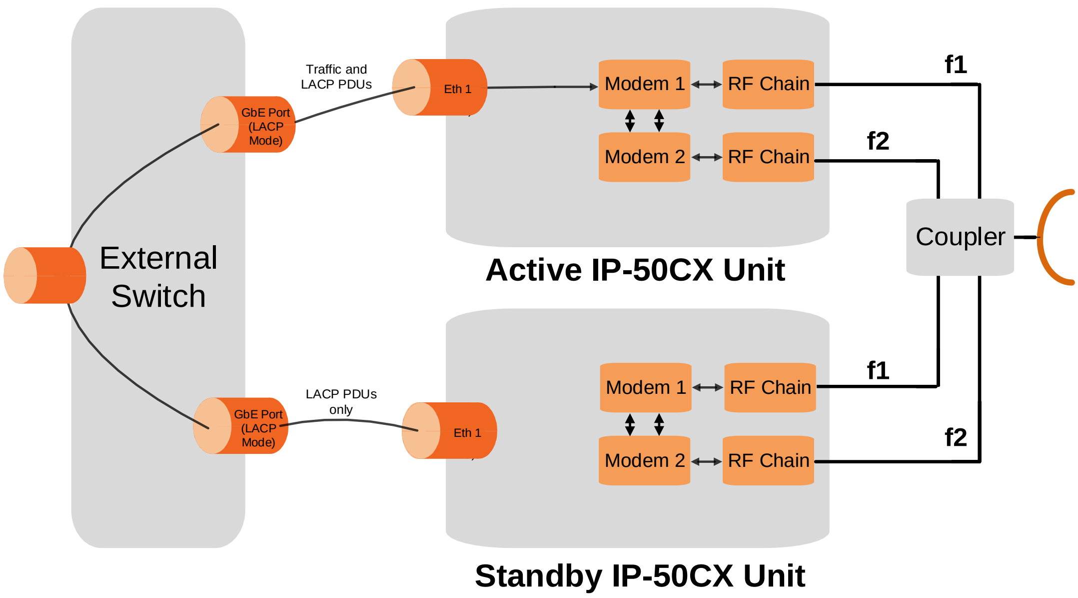


Figure 22: 2+2 Unit Redundancy and HSB – Line Protection Mode

5.2.8.1 Management for Unit Redundancy

In a Unit Redundancy configuration, the standby unit is managed via the active unit. A protection cable connects the two IP-50CX units via their MGT/PROT ports (P5). A protection splitter cable is used, which includes an interface for connection to an external management station if local management is needed.

Table 9: Protection Management Cable

Marketing Model	Description
IP-20C_PROT-SPLIT_CBL	CABLE,RJ45F TO 2xRJ45M,0.4M, WITH GLANDS, UV PROTECTED Management splitter cable for protection (P5 to P5 and External Management Station)

A single IP address is used for both IP-50CX units, to ensure that management is not lost in the event of switchover.

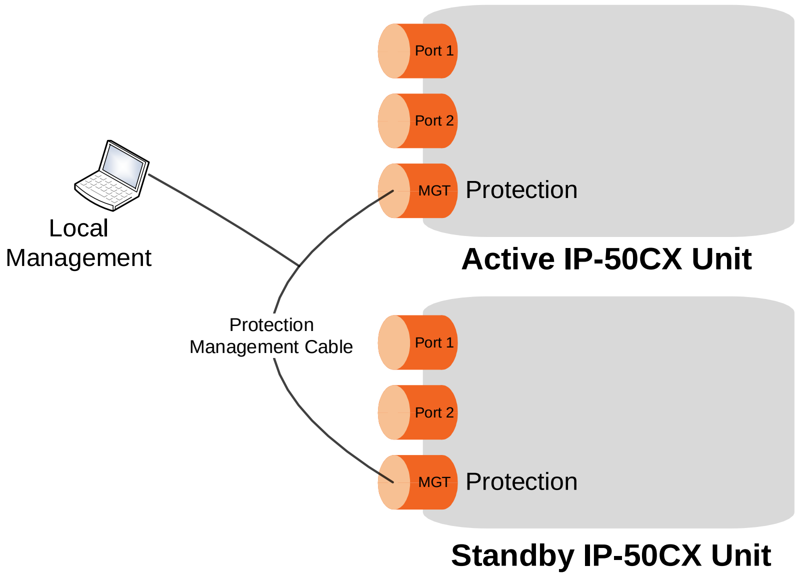


Figure 23: Internal and Local Management

The active and standby units must have the same configuration. The configuration of the active unit can be manually copied to the standby unit.

Note:	While the system is performing the copy-to-mate operation, a temporary loss of management connection occurs.

5.2.8.2 Unit Redundancy Revertive Mode

IP-50CX supports revertive HSB protection. In revertive HSB protection mode, the user defines the primary radio on each side of the link. The primary radio should be the radio on the coupler's main path and the secondary radio should be the radio on the coupling path.

The system monitors the availability of the primary path at all times. Whenever the primary path is operational and available, without any alarms, but the secondary path is active, a timer is activated. The timer is user-configurable from ten seconds to ten minutes. The default values is 60 seconds.

If the primary path remains operational and available for the period of the timer, the system initiates a revertive unit switchover. Every revertive unit switchover is recorded as an event in the event log.

Note: Each switchover causes traffic disruption.

5.2.8.3 Switchover

In the event of switchover, the standby unit becomes the active unit and the active unit becomes the standby unit. In most cases, switchover takes less than 50msec.

The following events trigger switchover for Unit Redundancy according to their priority, with the highest priority triggers listed first:

1. Force switch
2. Radio Failures (LOF, Excessive BER)
3. Line Failures
4. Manual switch

5.2.9 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.

5.2.9.1 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-50CX 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).

In a configuration with Unit Redundancy, the ATPC override state is propagated to the standby unit in the event of switchover.

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

5.2.10 Radio Signal Quality PMs

IP-50CX 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 150. Users can also configure an alarm that is raised if the RSL falls beneath a user-defined threshold. See *RSL Threshold Alarm* on page 150.

5.2.11 Traffic Utilization PMs

IP-50CX supports the following counters, as well as additional PMs based on these counters. Utilization and Throughput PMs are available for Multi-Carrier ABC groups, radio interfaces, and Ethernet interfaces used as part of a Multiband or Layer 1 Link Aggregation group (Enhanced Multi-Carrier ABC) to pass traffic from a main to attached unit. Capacity PMs are available for either Multi-Carrier ABC groups or individual radio interfaces, but only if the radio interfaces do not belong to a Multi-Carrier ABC group.

- 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%).

Note: For Ethernet Traffic ports in an Enhanced Multi-Carrier ABC group, the utilization percentage represents a percentage of the attached unit's radio capacity utilization.

- Traffic Throughput – Measures the total effective Layer 2 traffic sent through the interface (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 interface (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.

5.3 Ethernet Features

IP-50CX'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-50CX 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-50CX'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

5.3.1 IP-50CX's Ethernet Capabilities

IP-50CX 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-50CX'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-50CX'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 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

5.3.2 Ethernet Service Model

IP-50CX'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-50CX'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).

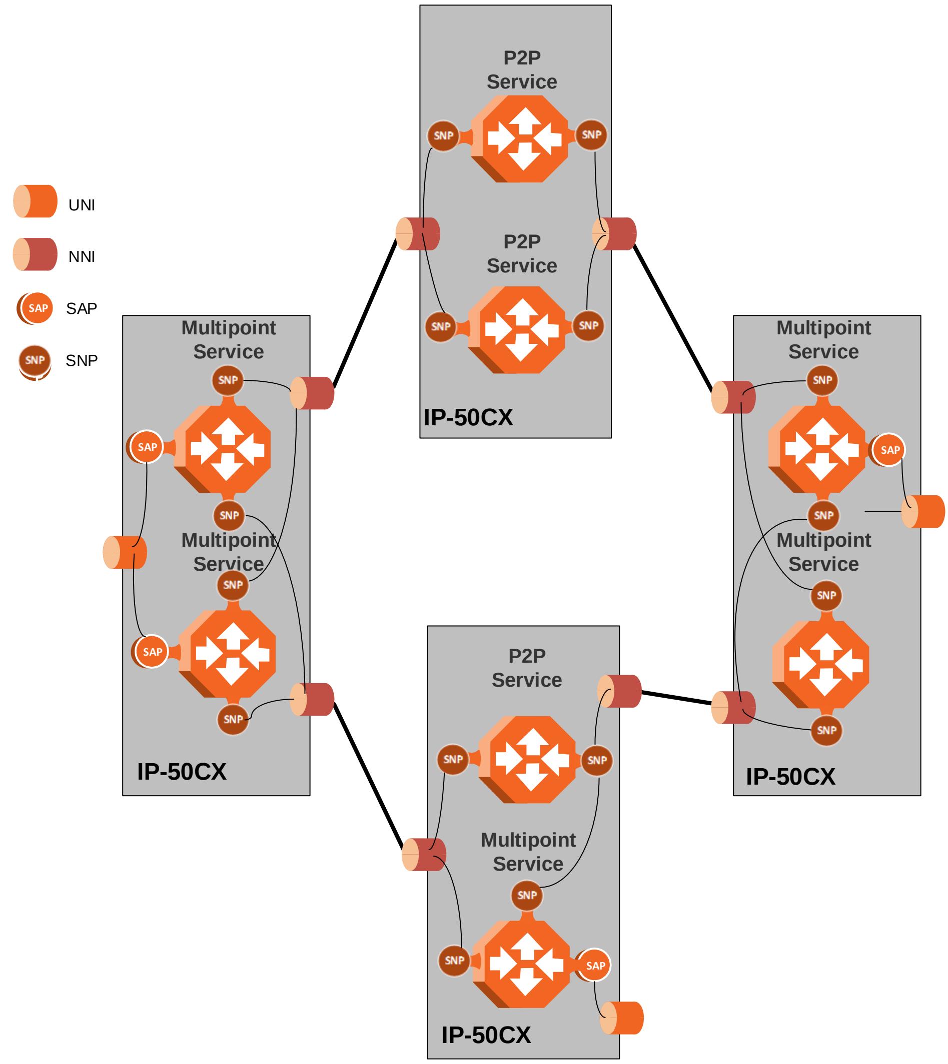


Figure 24: IP-50CX Services Model

The IP-50CX 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-50CX. 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-50CX 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-50CX services model, with traffic entering and leaving the network element. IP-50CX'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.

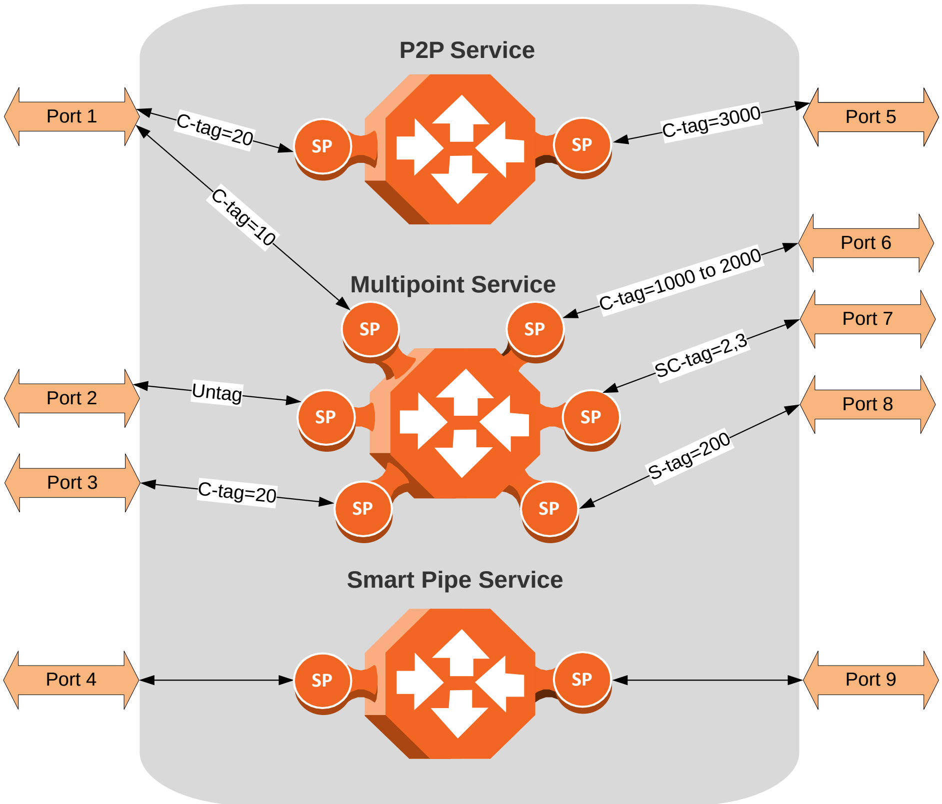


Figure 25: IP-50CX Services Core

5.3.2.1 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-50CX.
- 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.

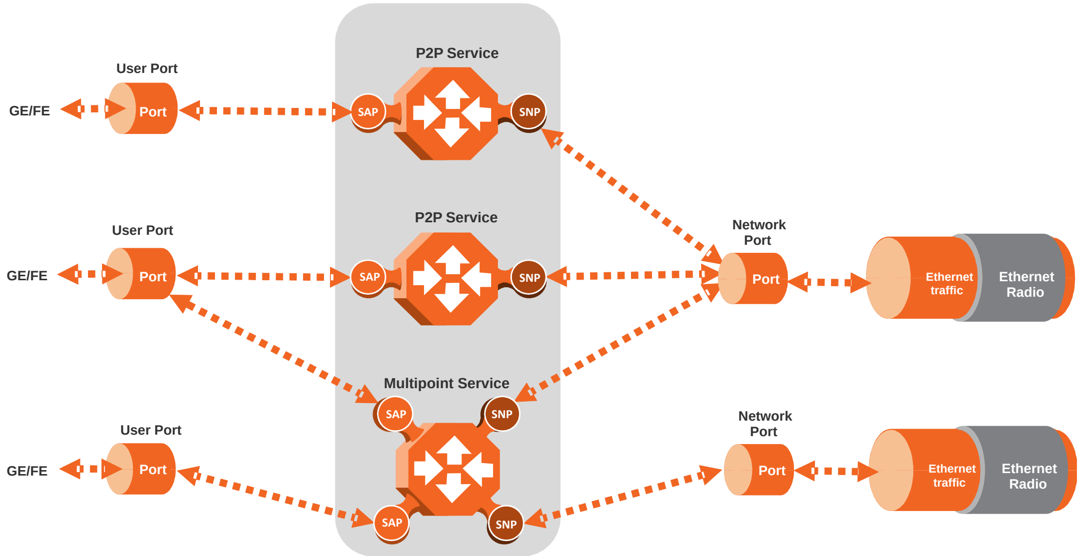


Figure 26: IP-50CX Services Flow

IP-50CX 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.

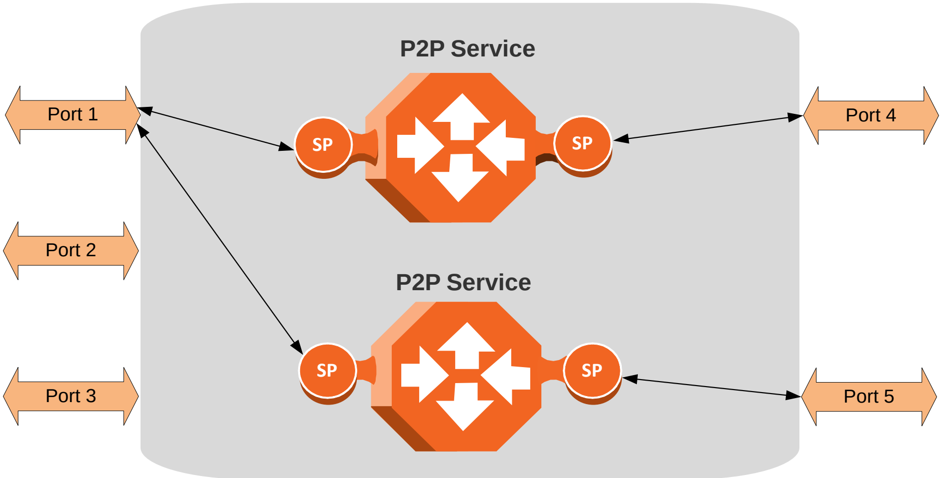


Figure 27: Point-to-Point Service

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.

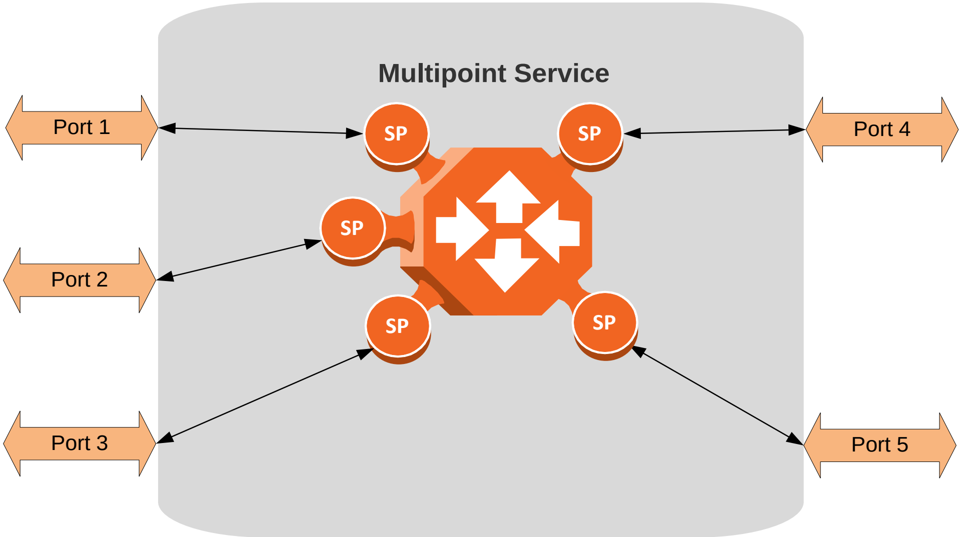


Figure 28: Multipoint Service

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-50CX can learn up to 32K Ethernet source MAC addresses. If necessary due to security issues or resource limitations, users can limit the size of the MAC forwarding table. The maximum size of the MAC forwarding table is configurable per device, but not per service.

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 10: 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
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. These user entries are not considered when determining the maximum size of the MAC forwarding table.

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.

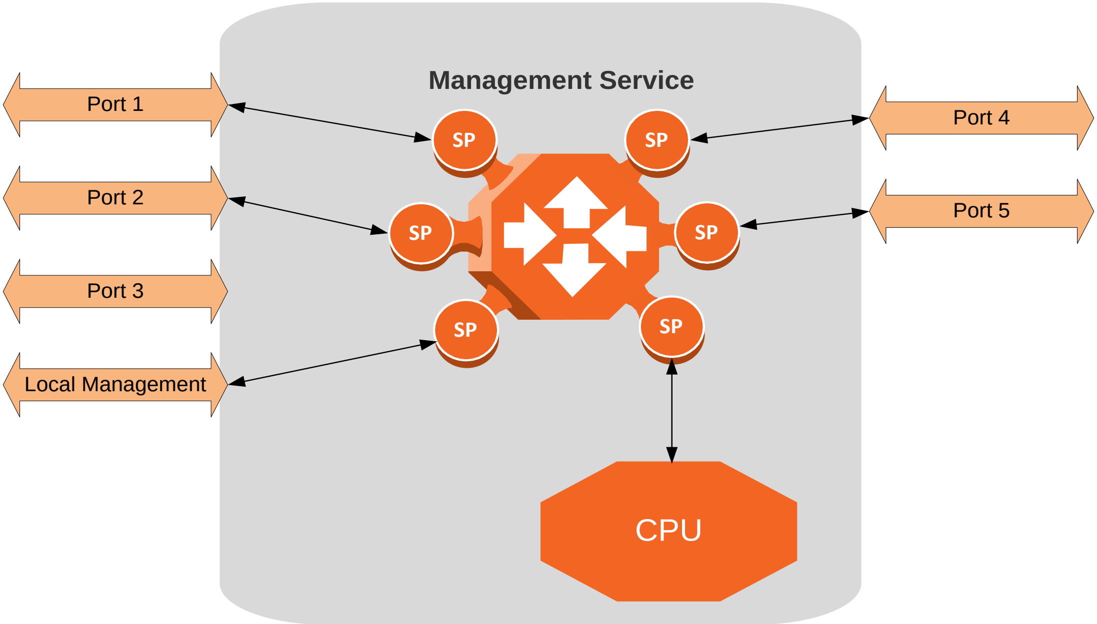


Figure 29: Management Service

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-50CX 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-50CX's hierarchical classification mechanism, refer to *Classification* on page 95.
- **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.

5.3.2.2 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-50CX 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.

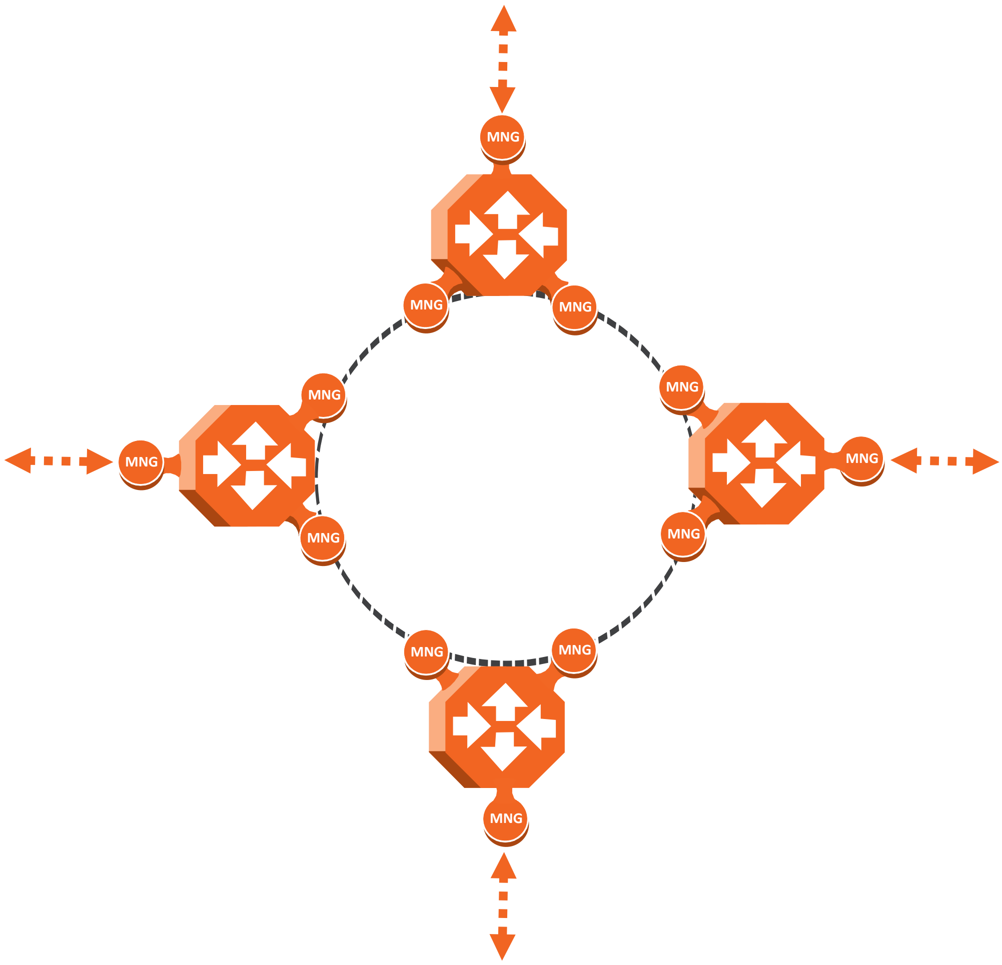


Figure 30: Management Service and its Service Points

- **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.

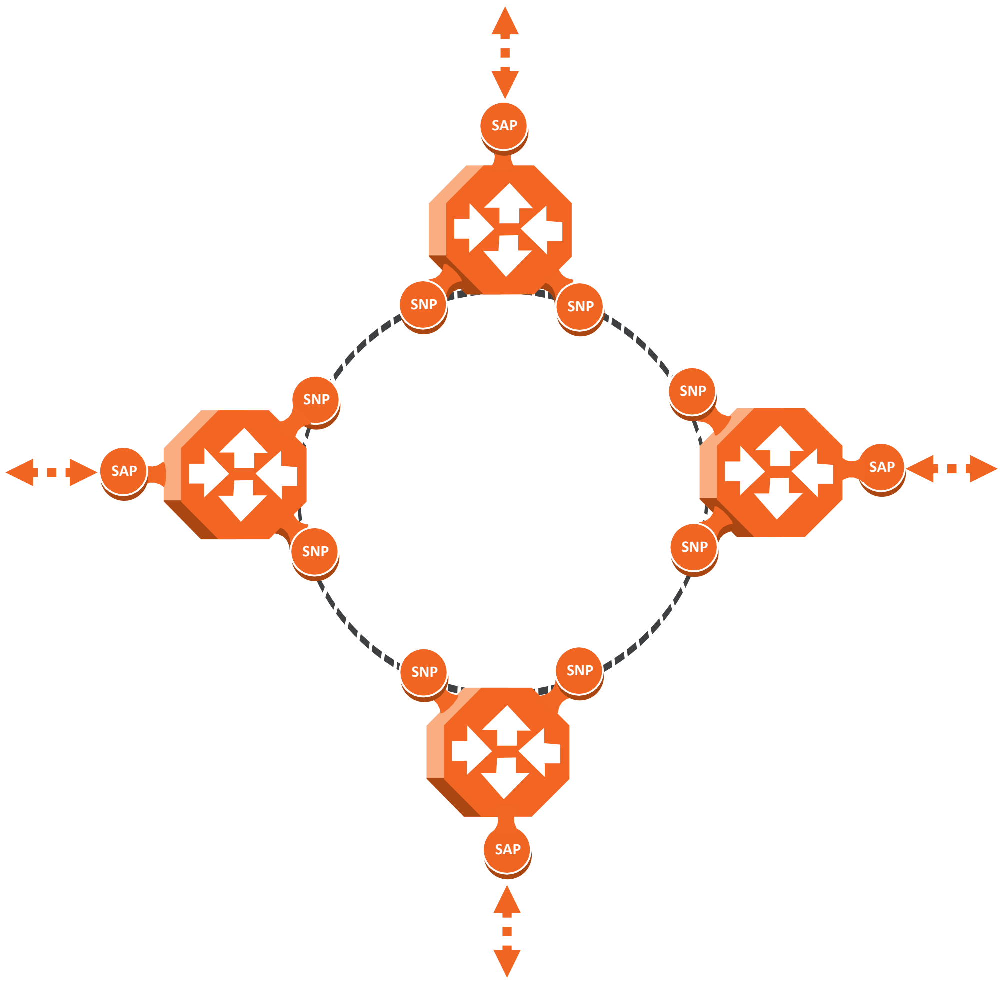


Figure 31: SAPs and SNPs

- **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 and Multipoint 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.

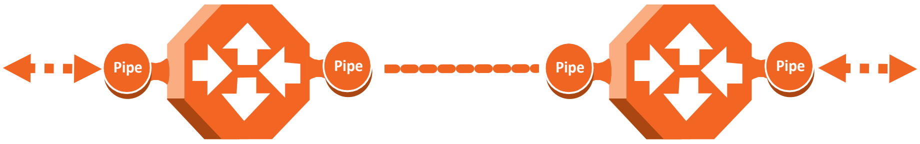


Figure 32: Pipe Service Points

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.

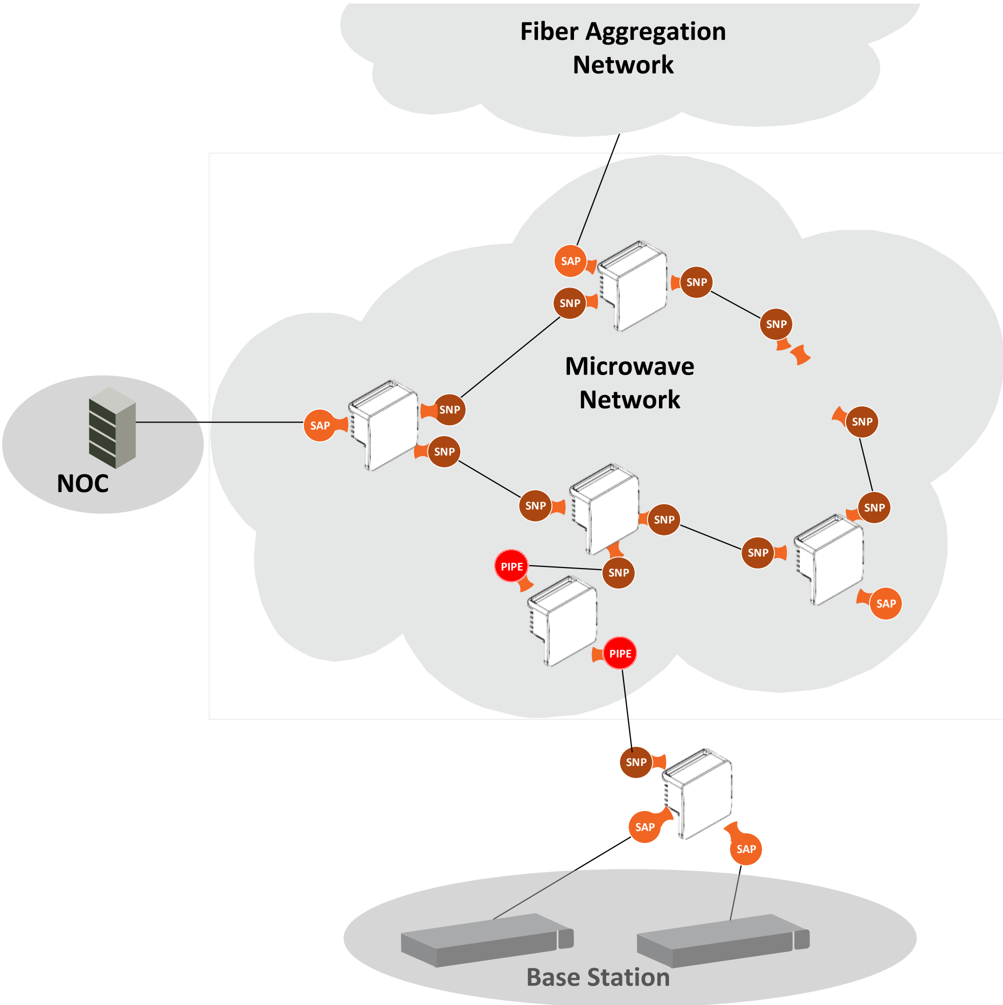


Figure 33: SAP, SNP and Pipe Service Points in a Microwave Network

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

Table 11: 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	Yes

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 – Attached Interface Type combinations can co-exist on the same interface.

.

Table 12: 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:

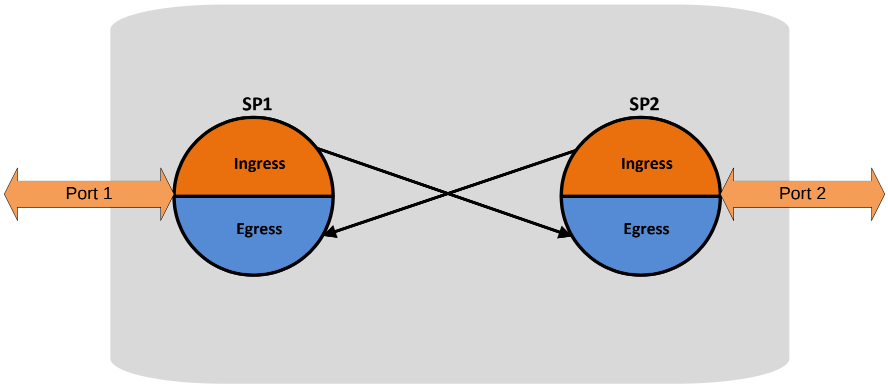


Figure 34: Service Path Relationship on Point-to-Point Service Path

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.

5.3.3 Ethernet Interfaces

The IP-50CX 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-50CX 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.

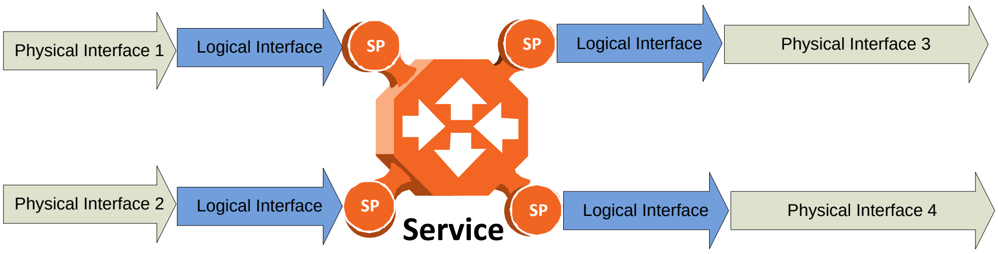


Figure 35: Physical and Logical Interfaces

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-50CX 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.

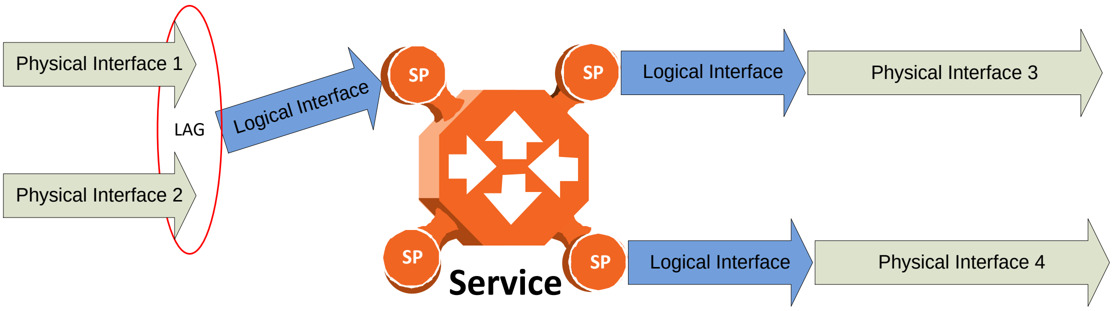


Figure 36: Grouped Interfaces as a Single Logical Interface on Ingress Side

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.

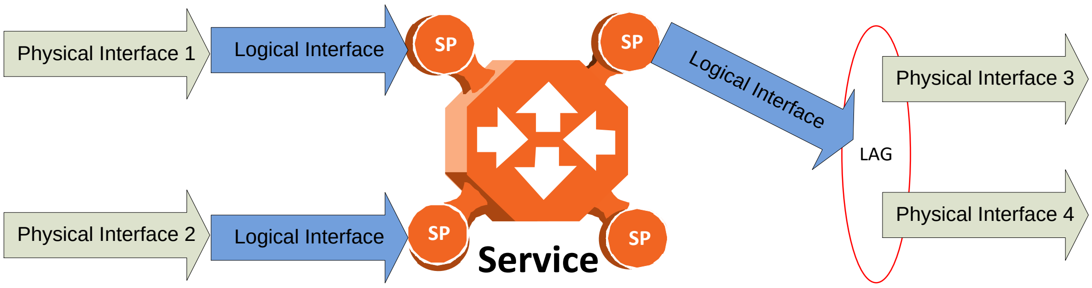


Figure 37: Grouped Interfaces as a Single Logical Interface on Egress Side

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

5.3.3.1 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.
- **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-50CX 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

5.3.3.2 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.

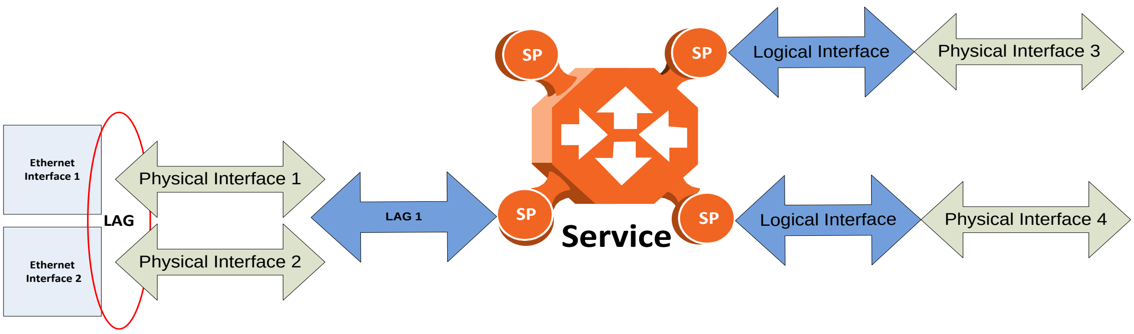


Figure 38: Relationship of Logical Interfaces to the Switching Fabric

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 CoS 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 CoS 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 CoS 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 96.

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) with a specific rate meter (policer) profile.

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 87, if the logical interface represents a group, such as a LAG, the IP-50CX 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

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

Note:	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-50CX 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.

5.3.4 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-50CX's personalized QoS enables operators to handle a wide and diverse range of scenarios. IP-50CX'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-50CX'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."

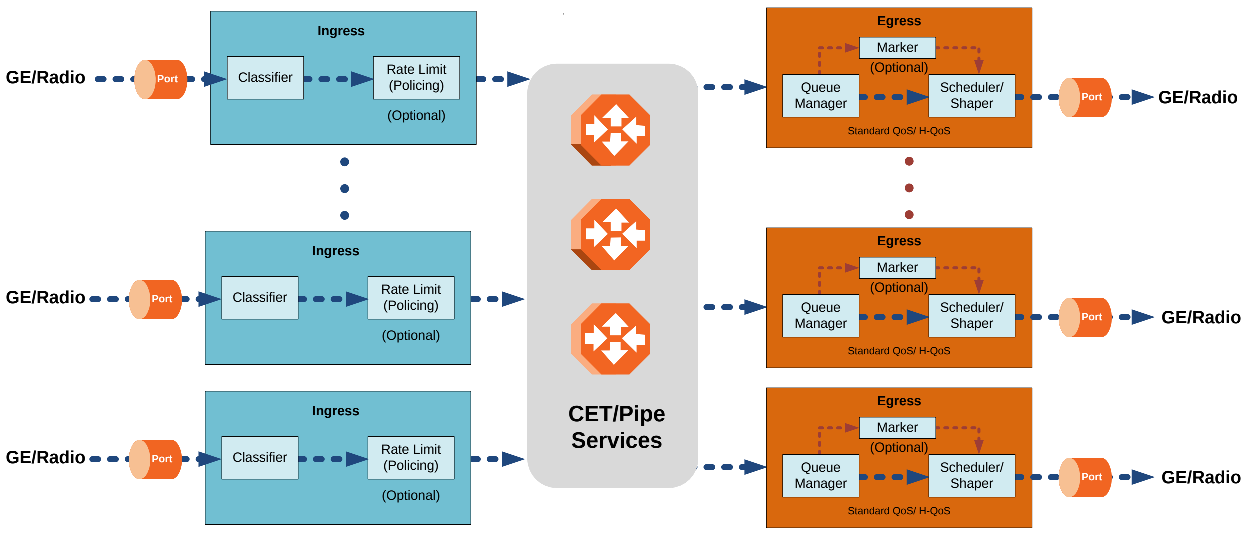


Figure 39: QoS Block Diagram

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.

5.3.4.1 QoS on the Ingress Path

Classification

IP-50CX 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.

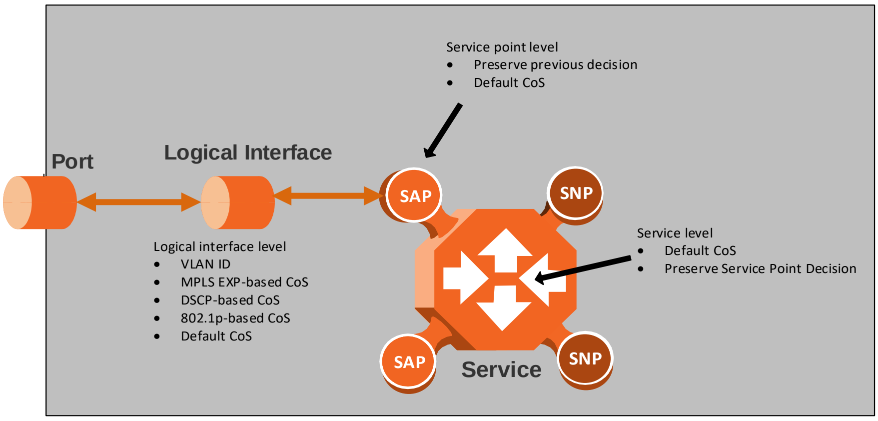


Figure 40: Hierarchical Classification

Logical Interface-Level Classification

Logical interface-level classification enables users to configure classification on a single interface or on a number of interfaces grouped tougher, 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-50CX 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.

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 89.

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 13: 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 14: 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
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

DSCP	DSCP (bin)	Description	CoS (Configurable)	Color (Configurable)
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 15: 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
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 16: 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-50CX'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-50CX 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-50CX'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-50CX 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 10 Gbps, with a minimum granularity of 32Kbps.
- **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 4096 Kbytes, with a minimum granularity of 2 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 10 Gbps, with a minimum granularity of 32 Kbps.
- **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 4096 Kbytes, with a minimum granularity of 2 Kbytes.

Note: EIR and EBS are only relevant for rate meters assigned to logical interfaces.

- **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.

5.3.4.2 QoS on the Egress Path

Queue Manager

The queue manager (QM) is responsible for managing the output transmission queues. IP-50CX 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 102.

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.

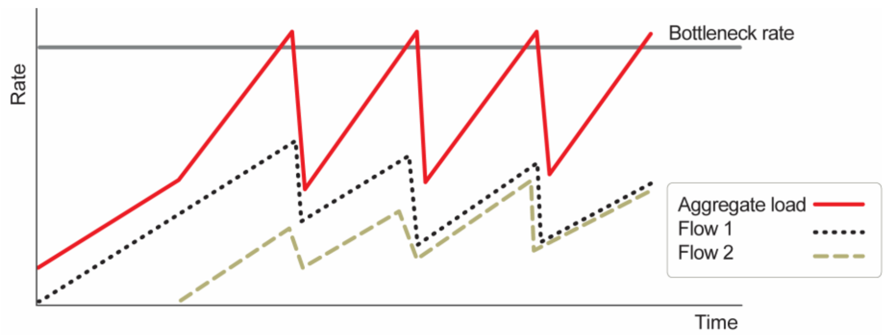


Figure 41: Synchronized Packet Loss

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.

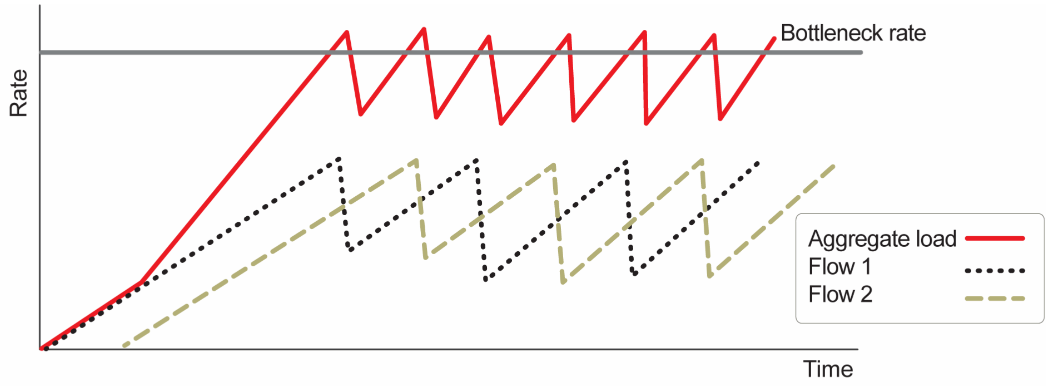


Figure 42: Random Packet Loss with Increased Capacity Utilization Using WRED

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-50CX 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-50CX 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-50CX 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.

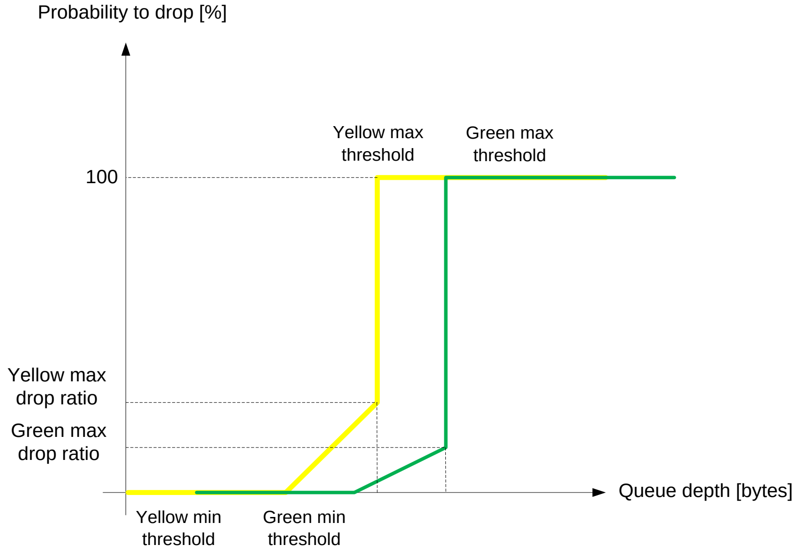


Figure 43: WRED Profile Curve

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-50CX 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.

Note:	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.

Note:	Queue shapers cannot be assigned to radio interfaces. This ability is planned for future release.

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 101.

Egress Scheduling

Egress scheduling is responsible for transmission from the priority queues. IP-50CX 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.

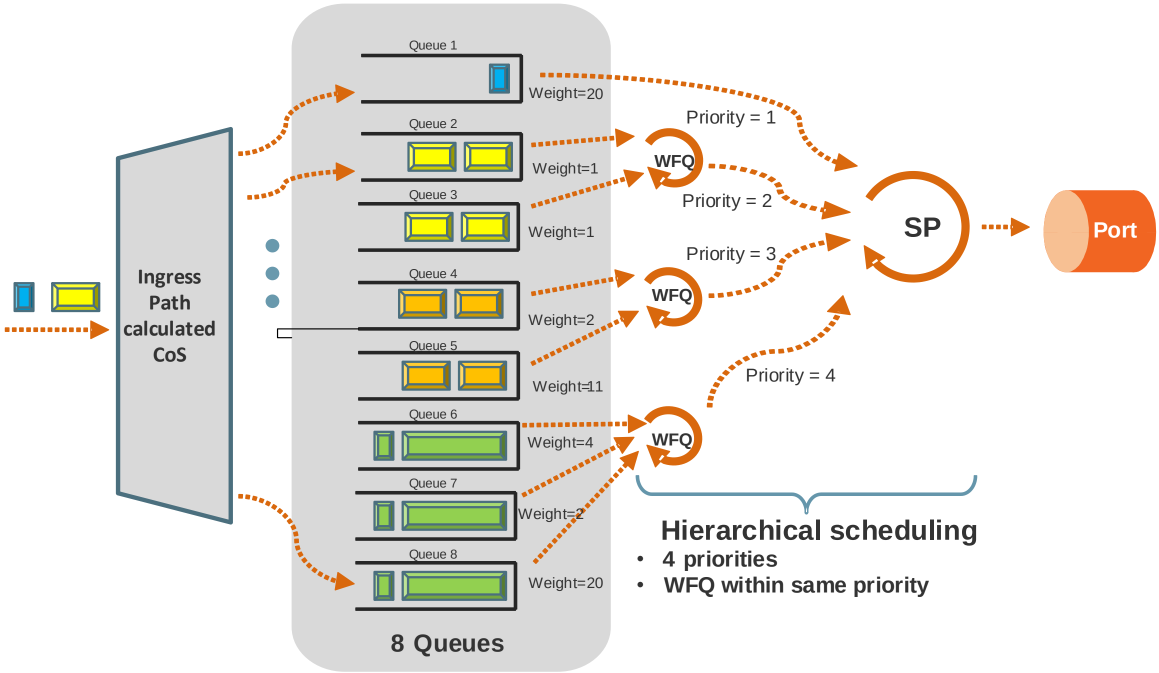


Figure 44: Scheduling Mechanism for a Single Service Bundle

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 17: QoS Priority Profile Example

		Profile ID (1-9)	
CoS	**Green Priority (user defined)**	**Yellow Priority (read only)**	**Description**
0	1	1	Best Effort
1	2	2	Data Service 4
2	2	2	Data Service 3
3	2	2	Data Service 2
4	2	2	Data Service 1
5	3	3	Real Time 2 (Video with large buffer)
6	3	3	Real Time 1 (Video with small buffer)
7	4	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 two interface priority profiles. Profile 9 is the pre-defined read-only default interface priority profile. The user can configure one additional 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 two WFQ profiles. Profile ID 1 is a pre-defined read-only profile, and is used as the default profile. An additional profile can be defined by the user.

Egress PMs and Statistics

Queue-Level Statistics

IP-50CX 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 87.

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 18: 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

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-50CX QoS mechanism.

Table 19: QoS Summary

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

5.3.5 Global Switch Configuration

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

- **S- VLAN Ethertype** –Defines the ethertype recognized by the system as the S-VLAN ethertype. IP-50CX 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-50CX 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.

5.3.6 Automatic State Propagation and Link Loss Forwarding

Related topics:

- Network Resiliency
- Unit Redundancy
- 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.

5.3.6.1 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.

5.3.6.2 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.

5.3.6.3 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-50CX unit is an element in the following network topologies:

- Ring or mesh network topology.
- An IP-20N connected to an IP-50CX 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-50CX unit being utilized as a pipe is running one MSTP instance for spanning in-band management.

5.3.7 Network Resiliency

IP-50CX 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.

5.3.7.1 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.

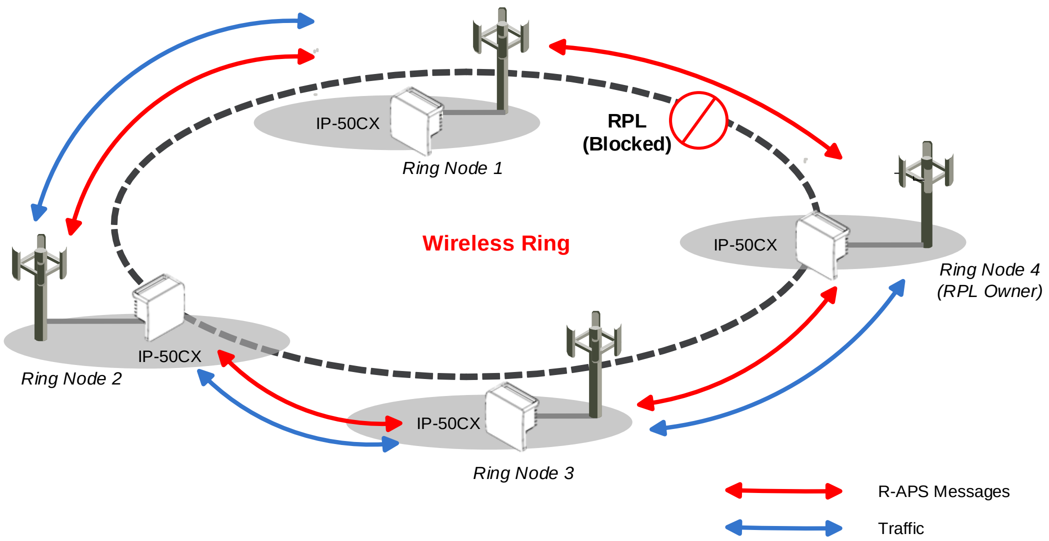


Figure 45: G.8032 Ring in Idle (Normal) State

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.

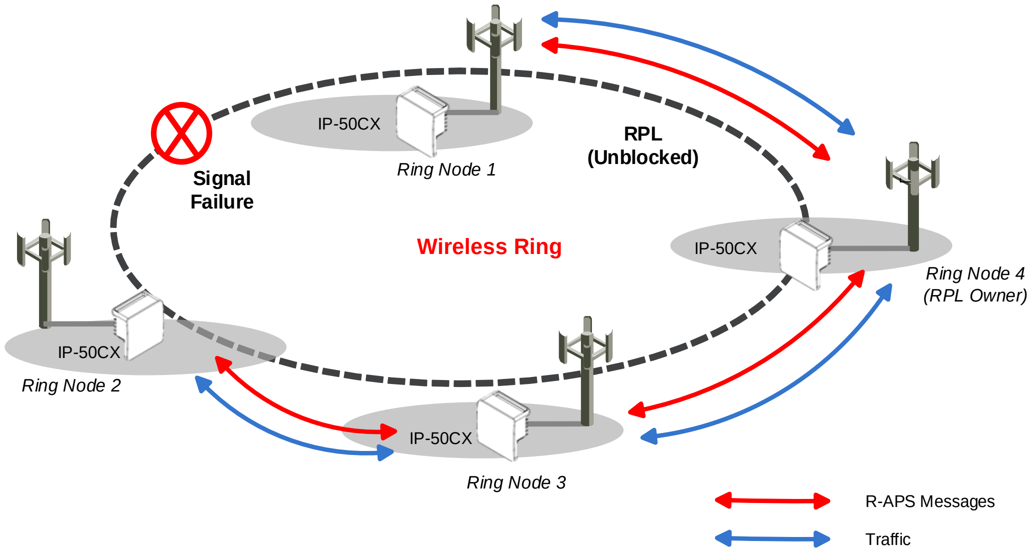


Figure 46: G.8032 Ring in Protecting State

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.

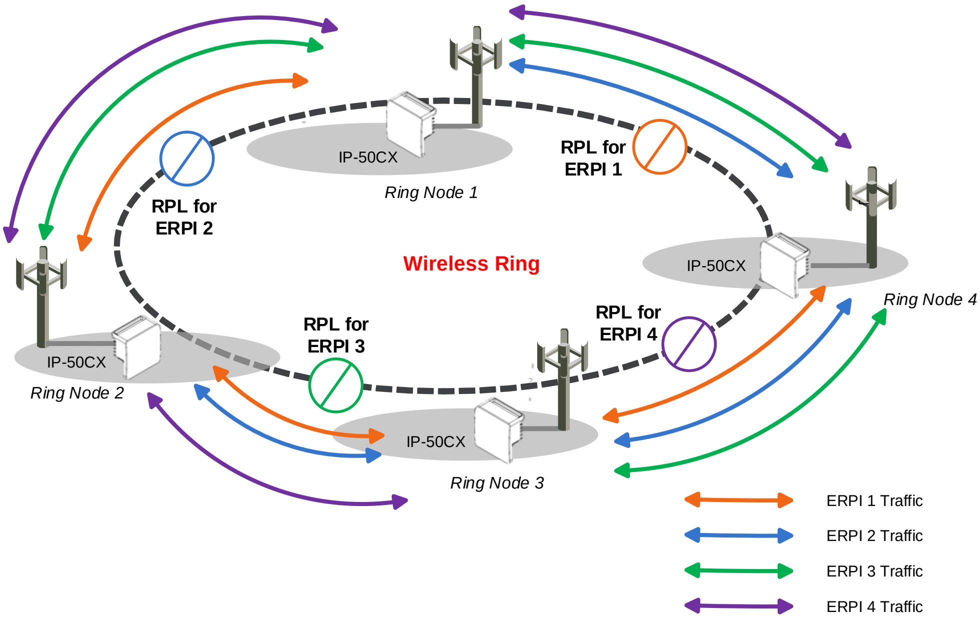


Figure 47: Load Balancing Example in G.8032 Ring

5.3.7.2 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-50CX 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-50CX units is interoperable with:

- IP-20 AND IP-50 units running MSTP.
- Third-party bridges running MSTP.
- Third-party bridges running RSTP

5.3.8 OAM

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

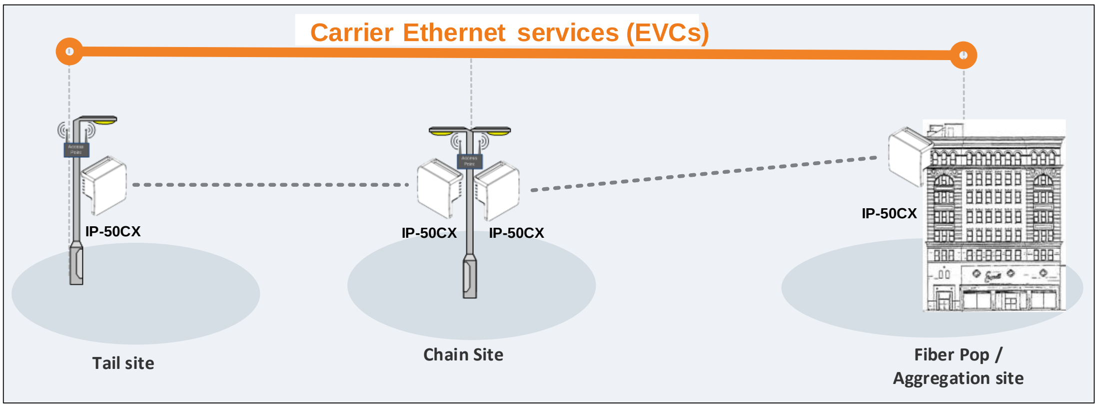


Figure 48: IP-50CX End-to-End Service Management

5.3.8.1 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-50CX 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.

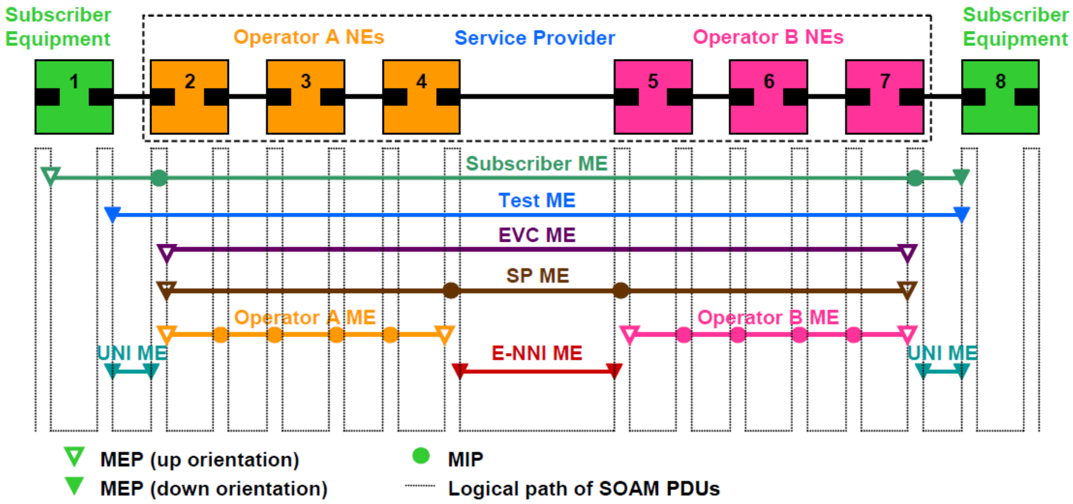


Figure 49: SOAM Maintenance Entities (Example)

- 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.

5.3.8.2 SFP DDM and Inventory Monitoring

IP-50CX supports static and dynamic monitoring for all SFP transceivers, including all SFP, SFP+, and SFP28 transceivers 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)
- Supply Voltage (VCC)

Inventory monitoring enables users to display the following information about each SFP transceiver installed in the IP-50CX 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)
- Minimum voltage (VCC) received by the SFP transceiver during the interval
- Average voltage (VCC) received by the SFP transceiver during the interval
- Maximum voltage (VCC) received by the SFP transceiver during the interval

Note: DDM parameters are not relevant for electrical SFPs.

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

5.3.8.3 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 Layer 1 Aggregation group, a Multi-Carrier ABC group, 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.

5.4 Synchronization

This section describes IP-50CX'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 ACM and narrow channels.
- Native Sync Distribution, for end-to-end distribution using GbE.

This section includes:

Related topics:

- NTP Support

5.4.1 IP-50CX 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 ACM 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.

5.4.2 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 20: Synchronization Interface Options

Available interfaces as frequency input (reference sync source)	Available interfaces as frequency output
• Radio carrier • GbE Ethernet interfaces	• Radio carrier • GbE Ethernet interfaces

It is possible to configure up to six 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.

5.4.3 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 transceivers.

5.4.4 IEEE-1588v2 PTP Optimized Transport

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

IP-50CX supports PTP optimized transport, a message-based protocol that can be implemented across packet-based networks. To ensure minimal packet delay variation (PDV), IP-50CX'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.

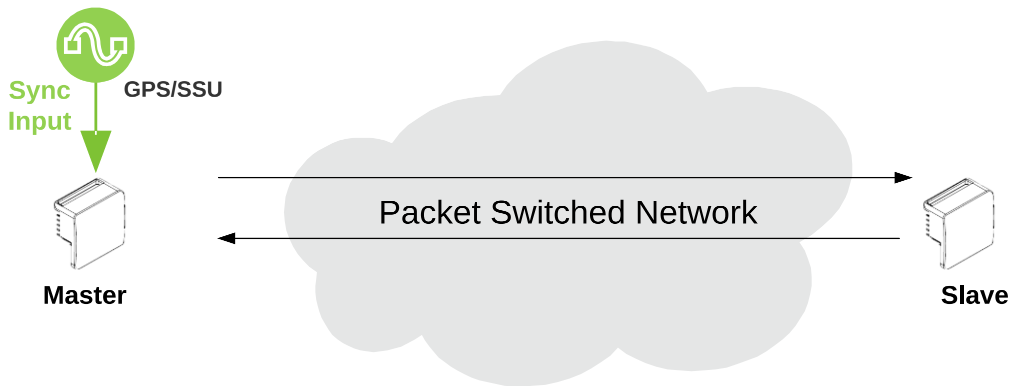


Figure 50: IEEE-1588v2 PTP Optimized Transport – General Architecture

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.

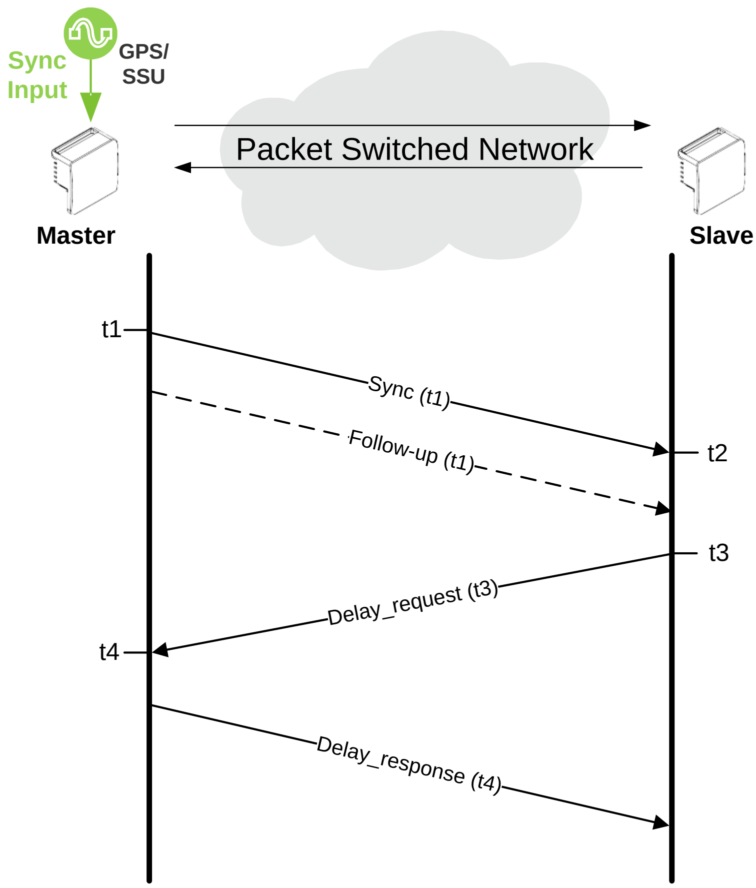


Figure 51: Calculating the Propagation Delay for PTP Packets

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:

Offset = [(t2 – t1) – (t4 – t3)]/2

Propagation Delay = [(t2 – t1) + (t4 – t3)]/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-50CX's IEEE-1588v2 implementations mitigate these factors, see *Mitigating PDV* on page 128.

5.4.4.1 IEEE-1588v2 Characteristics

IEEE-1588v2 provides packet-based synchronization that can transmit both frequency accuracy and phase information. This is essential for LTE applications, and adds the ability to transmit phase information to 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 128).
- Minimal consumption of bandwidth and processing power.
- Simple configuration.

5.4.4.2 Mitigating PDV

To get the most out of PTP and minimize PDV, IP-50CX 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 ACM, 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.

Note:	When bandwidth is reduced due to lowering of the ACM modulation point, it is essential that high priority traffic carrying IEEE-1588 packets be given the highest priority using IP-50CX'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-50CX's synchronization solution includes 1588v2-compliant Transparent Clock and Boundary Clock synchronization protocols. The following section describes Transparent Clock and how it counters PDV.

5.4.4.3 Transparent Clock

IP-50CX 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.

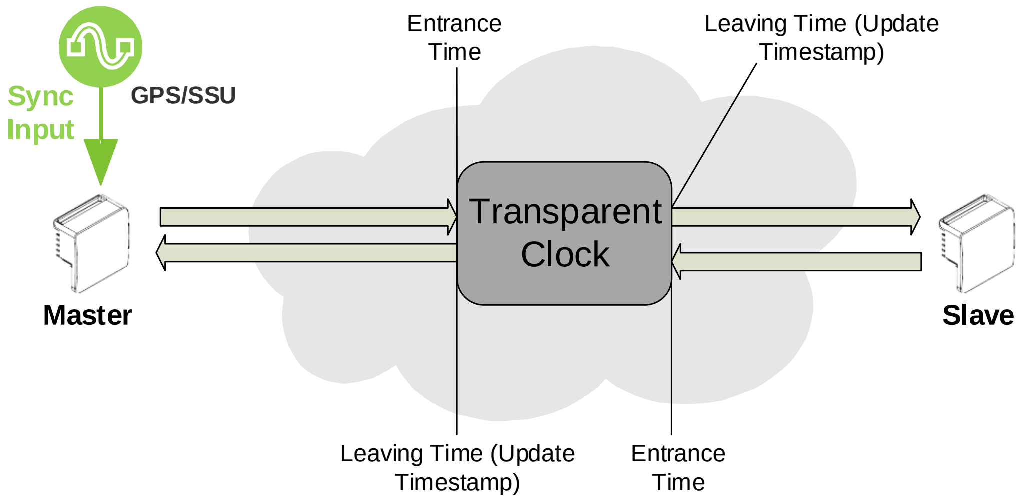


Figure 52: Transparent Clock – General Architecture

IP-50CX 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-50CX 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-50CX 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).

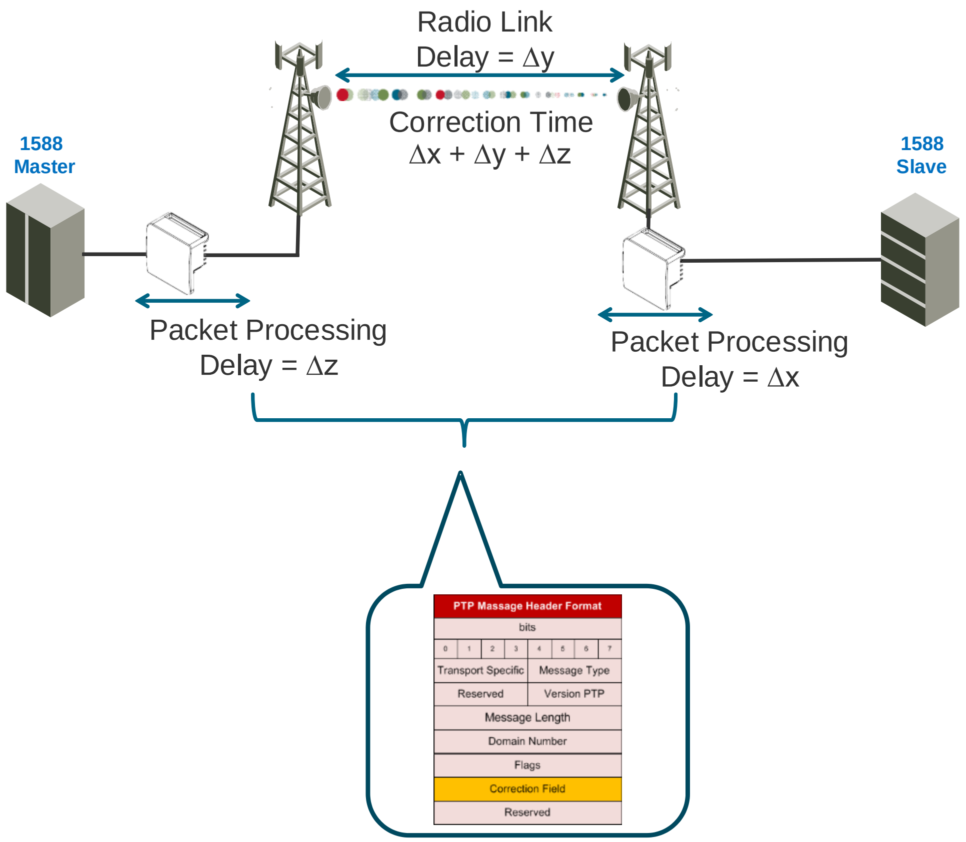


Figure 53: Transparent Clock Delay Compensation

5.4.4.4 Boundary Clock

Boundary Clock provides better performance than other synchronization methods, enabling compliance with ITU-T Telecom Profile G.8275.1. This enables IP-50CX, 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.

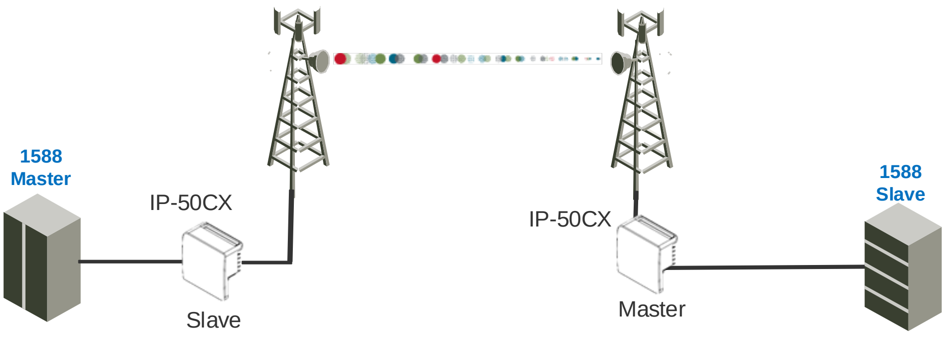


Figure 54: Boundary Clock – General Architecture

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 21: 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 22: 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

Users can configure the following parameters for the sending of PTP messages:

- UDP/IPv4, per IEEE 1588 Annex D, or IEEE 802.3 Ethernet, per IEEE 1588 Annex F.
- Unicast or multicast mode.

5.4.5 SSM Support and Loop Prevention

In order to provide topological resiliency for synchronization transfer, IP-50CX implements the passing of SSM messages over the radio interfaces. SSM timing in IP-50CX 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.

5.5 AES-256 Payload Encryption

IP-50CX supports AES-256 payload encryption. On an IP-50CX device, AES-256 payload encryption can be enabled on radio interface 1 or on a Multi-Carrier ABC group.

Only IP-50CX models with the following marketing model syntax support AES-256 payload encryption:

- IP-50CX Basic ODU XGHz
- IP-50CX-X-XXw-Y-Z

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

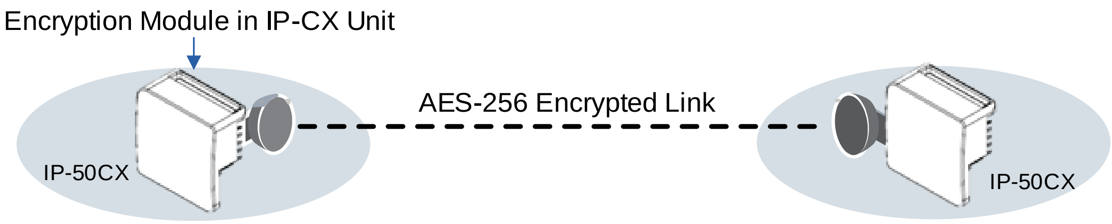


Figure 55 AES-256 Encrypted Link

Notes:	The AES-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. In CeraOS 13.1, AES payload encryption cannot be used in a Layer 1 Link Aggregation configuration with Line Redundancy.

5.5.1 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

5.5.2 IP-50CX AES Implementation

In IP-50CX, 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.

IP-50CX 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-256 encryption algorithm. For IP-50CX, session keys are regenerated at two-minute 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.

The unit must be reset after changing the AES-256 Admin mode, whether it is to enable or disable AES-256. When the user applies the change, an alarm is raised and the alarm is not cleared until the reset has been performed.

Note that when AES-256 is enabled, the maximum ACM profile may be reduced by one in certain cases. For more details, see *Supported Modulations per Frequency and Channel Bandwidth* on page 169.

6. 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

6.1 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-50CX 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-50CX supports NETCONF/YANG, enabling customers to manage, configure, and monitor network elements within the paradigm of SDN network architecture.

In addition, IP-50CX 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-50CX supports the Link Layer Discovery Protocol (LLDP).

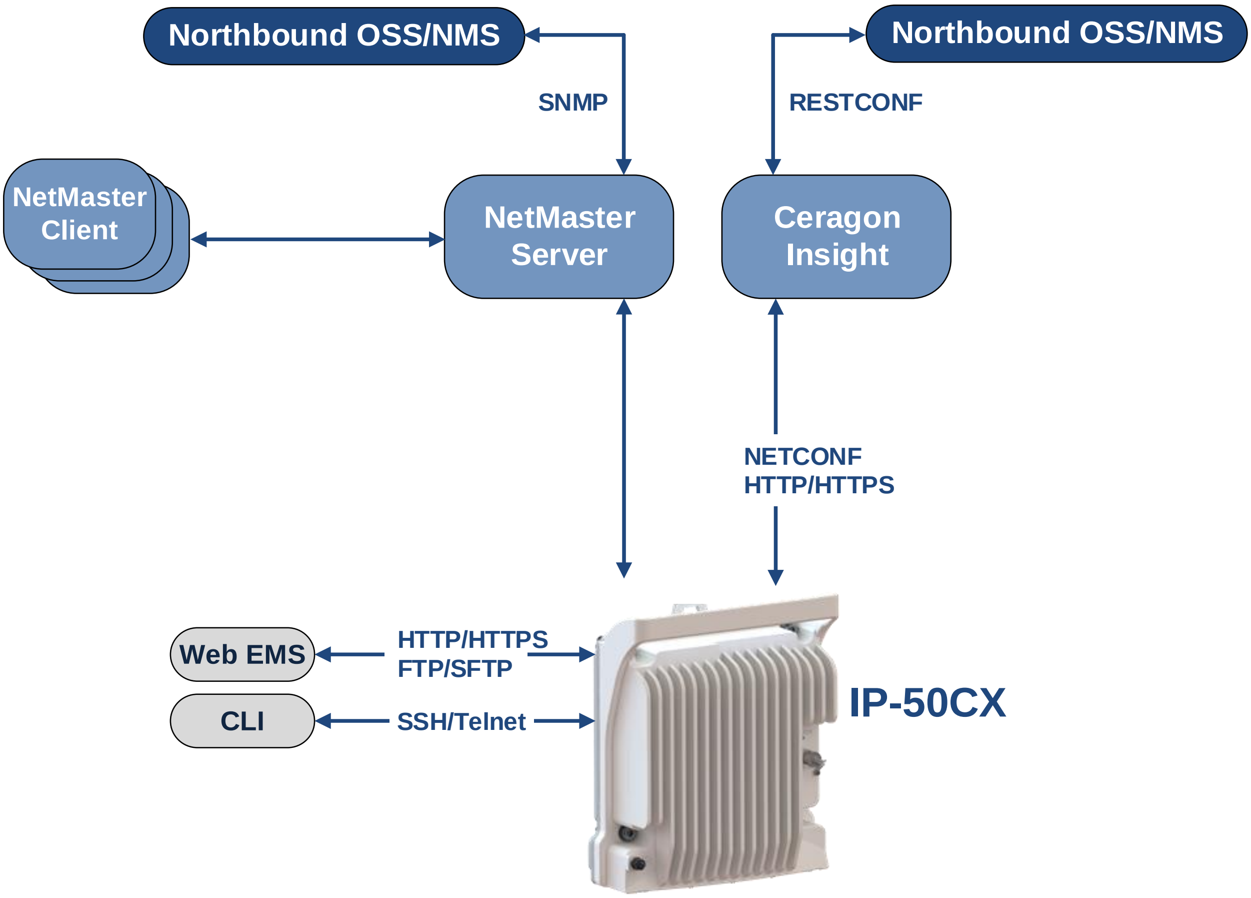


Figure 56: Integrated Management Tools

6.2 Automatic Network Topology Discovery with LLDP Protocol

IP-50CX 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-50CX'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-50CX units enables the NMS to:

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

6.3 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 23: 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 **Note:** When HTTPS is used, users can configure Port 80 to be closed and traffic redirected to Port 443.
443	HTTPS	TCP	Manages devices (optional)
444	HTTPS	TCP	Used for Smart Activation Key
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)

Port number	Protocol	Frame structure	Details
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.
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

6.4 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-50CX 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-50CX security features.
- **User Management** – Enables you to define users and user profiles.

A Web-Based EMS connection to the IP-50CX 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.

Note:	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-256 payload encryption
- 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:

- Session Timeout
- Login Banner
- AES-256 payload encryption status
- 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.

6.5 SDN Support

IP-50CX 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-50CX'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-50CX'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*.

6.6 Command Line Interface (CLI)

A CLI connection to the IP-50CX 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.

6.7 Configuration Management

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

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

6.8 Software Management

The IP-50CX 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-50CX.
- **Reset** – The IP-50CX is restarted in order to boot the new software and firmware versions.

IP-50CX 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-50CX 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-50CX 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-50CX 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.

6.9 Using Pre-Defined Configuration Files

IP-50CX 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-50CX 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.

6.10 IPv6 Support

IP-50CX 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.

6.11 In-Band Management

IP-50CX 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 74.

6.12 Local Management

IP-50CX includes an electrical GbE management port.

6.13 Alarms

6.13.1 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.

6.13.2 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.

6.13.3 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.

6.13.4 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.

6.14 NTP Support

Related topics:

- Synchronization

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

6.15 UTC Support

IP-50CX 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-50CX 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.

6.16 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.

6.17 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.

6.17.1 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.

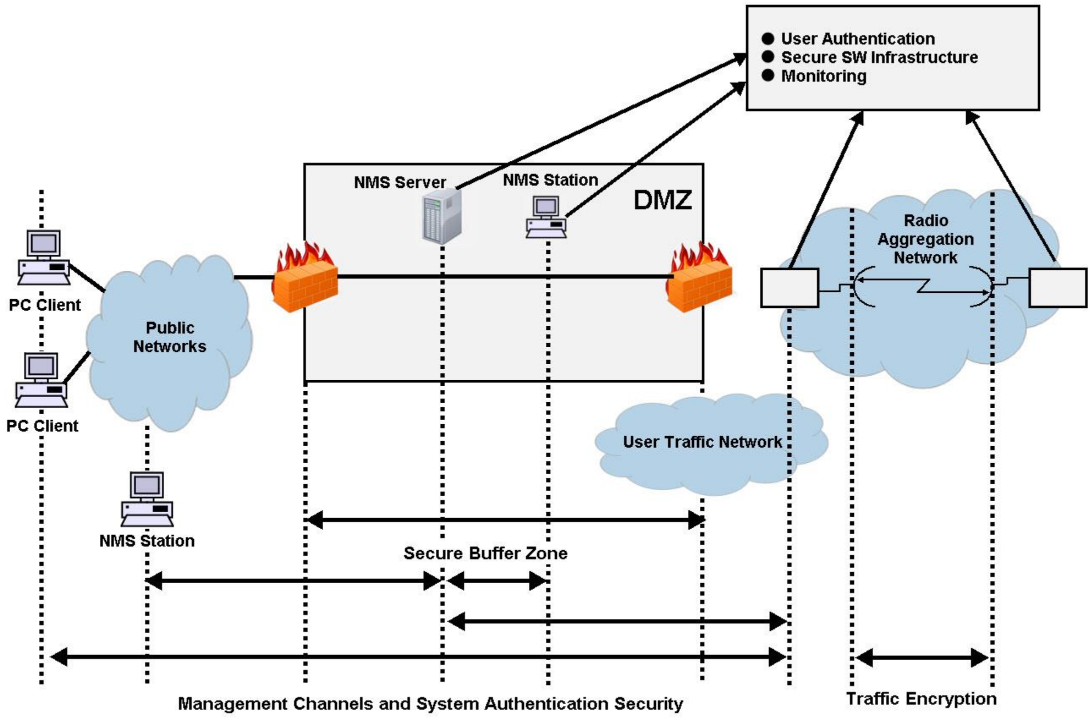


Figure 57: Security Solution Architecture Concept

6.17.2 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

6.17.3 Defenses in User and System Authentication Procedures

6.17.3.1 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-50CX 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.

6.17.3.2 User Identification

IP-50CX 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.

6.17.3.3 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.

6.17.3.4 RADIUS Support

The RADIUS protocol provides centralized user management services. IP-50CX 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-50CX 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-50CX 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-50CX, or notifies the IP-50CX 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-50CX 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-50CX - 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

6.17.3.5 TACACS+ Support

IP-50CX 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.

6.17.3.6 SSO Web Login with Microsoft Entra ID

CeraOS devices support remote user login via Microsoft Entra ID. Microsoft Entra ID is a cloud-based identity and access management service. It helps organizations securely manage users, applications, and devices by providing authentication, authorization, and identity protection. Through Entra ID, users can securely access external resources.

The following options are available for CeraOS devices:

- **Single Sign-On (SSO)** – Enables users to log in once and access multiple applications without needing to re-enter credentials.
- **Multi-Factor Authentication (MFA)** – Adds an extra layer of security beyond just a password. MFA is optional, and must be arranged by the operator as part of the operator’s Microsoft Entra ID implementation.

SSO is only active for the browser type on which the user logs in with Microsoft. For example, if the user logs in with a Microsoft Edge browser, the user will be logged in via SSO while using a Microsoft Edge browser but will not be logged in via SSO from a Google Chrome browser, and vice versa.

When a user logs into a device with SSO enabled, the user is given the option to log in normally with the user’s credentials or to log in via Microsoft.

When a user logs out of a device to which the user is logged in with SSO, the user is given the option to log out of the local session only or to log out of Microsoft.

6.17.4 Secure Communication Channels

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

6.17.4.1 SSH (Secured Shell)

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

- 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-50CX’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.

6.17.4.2 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-50CX 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.

6.17.4.3 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

6.17.4.4 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.

6.17.4.5 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.

6.17.4.6 SNMP

IP-50CX 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-50CX 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.

6.17.4.7 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.

6.17.5 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 user added or deleted
  - 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

6.17.6 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.

7. Standards and Certifications

This chapter includes:

- Supported Ethernet Standards
- MEF Specifications for Ethernet Services

7.1 Supported Ethernet Standards

Table 24: 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

7.2 MEF Specifications for Ethernet Services

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

Table 25: 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)

8. Specifications

This chapter includes:

- General Radio Specifications
- Radio Scripts
- Supported Modulations per Frequency and Channel Bandwidth
- Radio Capacity Specifications
- Transmit Power Specifications
- Receiver Threshold Specifications
- Frequency Bands
- Ethernet Latency Specifications
- Mediation Device Losses
- Interface Specifications
- Carrier Ethernet Functionality
- Synchronization
- Network Management, Diagnostics, Status, and Alarms
- Mechanical Specifications
- Standards Compliance
- Environmental Specifications
- Antenna Specifications
- Power Input Specifications
- Typical Power Consumption
- Power Connection Options
- PoE Injector Specifications
- Cable Specifications
- Mean Time Between Failures (MTBF)

Related Topics:

- Standards and Certifications

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

8.1 General Radio Specifications

Table 26: Radio Frequencies

Frequency (GHz)	Operating Frequency Range (GHz)	Tx/Rx Spacing (MHz)
6L,6H	5.85-6.45, 6.4-7.1	252.04, 240, 266, 300, 340, 160, 170, 500
7,8	7.1-7.9, 7.7-8.5	154, 119, 161, 168, 182, 196, 208, 245, 250, 266, 300,310, 311.32, 500, 530
10	10.0-10.7	91, 168,350, 550
11	10.7-11.7	490, 520, 530
13	12.75-13.3	266
15	14.4-15.35	315, 420, 475, 644, 490, 728
18	17.7-19.7	1010, 1120, 1008, 1560
23	21.2-23.65	1008, 1200, 1232
24UL	24.0-24.25	Customer-defined
26	24.2-26.5	800, 1008
28	27.35-29.5	350, 450, 490, 1008
32	31.8-33.4	812
38	37-40	1000, 1260, 700
42	40.55-43.45	1500

Table 27: General Radio Specifications

Standards	ETSI, ITU-R, CEPT
Frequency Source	Synthesizer
RF Channel Selection	Via EMS/NMS
Tx Range (Manual/ATPC)	The dynamic TX range with ATPC is the same as the manual TX range, and depends on the frequency and the ACM profile. The maximum TX power with ATPC is no higher than the maximum manually configured TX power.

8.2 Radio Scripts

Table 28: Radio Scripts

Script ID	Channel BW	Occupied BW	Standard	ETSI System Class	XPIC (CCDP)	SD	Highest Spectral Efficiency Class	Max Profile (ACM)	Max Profile (Fixed)
4509	14	13.3	ETSI	ACCP	Yes	No	7B	11 (2048 QAM)	10 (1024 QAM Light FEC)
4521	20	18.57	FCC	n/a	Yes	No	n/a	11 (2048 QAM)	10 (1024 QAM Light FEC)
4525	25	23.4	FCC	n/a	Yes	No	n/a	12 (4096 QAM)	11 (2048 QAM)
4504	28	26.5	ETSI	ACCP	Yes	No	8B	12	11
4505	28/30	28	ETSI/FCC	ACAP	Yes	No	8A	12	11
4514[4]	28	26	ETSI	ACCP	Yes	Yes	8B	12	11
4507	40	37.4	ETSI/FCC	ACCP	Yes	No	8B	12	11
4510	50	47.2	FCC	n/a	Yes	No	n/a	12	11
4502	56	53	ETSI	ACCP	Yes	No	8B	12	11
4506	56/60	55.7	ETSI/FCC	ACAP	Yes	No	8A	12	11
4513	70	64.8	ETSI	ACCP	Yes	No	8B	12	11
4501[5]	80	74	ETSI/FCC	ACCP	Yes	No	8B	12	11
4588	80	79.2	ETSI	ACAP	Yes	No	8A	12	11
4511[5]	112	106	ETSI	ACCP	Yes	No	8B	12	11
4518	140	127.5	ETSI	ACCP	Yes	No	8B	10 (2048 QAM)	9 (1024 QAM)
4515	150	141.6	FCC	ACCP	Yes	No	8B	10	9
4516	160	148.2	FCC	ACCP	Yes	No	8B	10	9
4524	224	212	ETSI	ACCP	Yes	No	8B	10	9

[4] Planned for future release.

[5] The maximum profiles listed for this script are relevant for 1+0 and 2+0 XPIC configurations. For configurations using system class ACCP, the maximum profile is limited to Profile 10 (1024 QAM).

8.3 Supported Modulations per Frequency and Channel Bandwidth

Table 29 shows the highest modulation possible for each frequency and channel bandwidth combination.

Table 29: Supported Modulations per Frequency and Channel Bandwidth

	14-20 MHz	25-30 MHz	40 MHz	50-60 MHz	80 MHz	112 MHz	120-224 MHz
6 GHz	2048QAM	4096QAM	4096QAM	4096QAM	4096QAM	4096QAM[7]	NA
7-8 GHz	2048QAM	4096QAM	4096QAM	4096QAM	4096QAM	4096QAM[7]	NA
10 GHz	2048QAM	4096QAM	4096QAM	4096QAM	4096QAM	4096QAM[7]	2048QAM
11 GHz	2048QAM	4096QAM	4096QAM	4096QAM	4096QAM	4096QAM[7]	2048QAM
13 GHz	2048QAM	4096QAM	4096QAM	4096QAM	4096QAM	4096QAM[7]	NA
15 GHz	2048QAM	4096QAM	4096QAM	4096QAM	4096QAM	4096QAM[7]	2048QAM
18 GHz	2048QAM	4096QAM	4096QAM	4096QAM	4096QAM	4096QAM[7]	2048QAM[7]
23 GHz	2048QAM	4096QAM	4096QAM	4096QAM[7]	4096QAM[7]	4096QAM[6,7]	2048QAM[7]
26 GHz	2048QAM	4096QAM[7]	4096QAM[7]	4096QAM[7]	4096QAM[7]	2048QAM[7]	2048QAM[7]
28 GHz	2048QAM	4096QAM[7]	4096QAM[7]	2048QAM	4096QAM[7]	4096QAM[6,7]	2048QAM[7]
32 GHz	2048QAM	4096QAM[7]	4096QAM[7]	2048QAM	4096QAM[7]	4096QAM[6,7]	2048QAM[7]
36 GHz	2048QAM	2048QAM	2048QAM	2048QAM	2048QAM	2048QAM	2048QAM[7]
38 GHz	2048QAM	2048QAM	2048QAM	2048QAM	2048QAM	2048QAM	2048QAM[7]
42 GHz	2048QAM	2048QAM	2048QAM	2048QAM	2048QAM[6]	2048QAM[6]	2048QAM[6,7]

6 Not supported for all sub-bands.

7 One profile lower for certain hardware models or when AES is enabled. For details, consult with your Ceragon representative.

8.4 Radio Capacity Specifications

Notes:	The figures in this section are indicative only. Exact results will depend on multiple factors, such as packet size, type of traffic, headers, etc. Ethernet capacity depends on average frame size. ACAP and ACCP represent compliance with different ETSI mask requirements. ACCP represents compliance with more stringent interference requirements.

8.4.1 14 MHz – Script ID 4509 (ETSI)

Table 30: Radio Capacity with 14 MHz (Script 4509)

Profile	Modulation	Minimum required capacity activation key	Ethernet Throughput (Mbps)
0	BPSK	10	6-8
1	QPSK	50	16-20
2	8 QAM	50	26-32
3	16 QAM	50	37-46
4	32 QAM	50	50-61
5	64 QAM	50	62-76
6	128 QAM	100	76-93
7	256 QAM	100	87-106
8	512 QAM	100	96-118
9	1024 QAM (Strong FEC)	100	102-125
10	1024 QAM (Light FEC)	100	108-132
11	2048 QAM	100	113-138

8.4.2 20 MHz – Script ID 4521 (ANSI)

Table 31: Radio Capacity with 20 MHz (Script 4521)

Profile	Modulation	Minimum required capacity activation key	Ethernet Throughput (Mbps)
0	BPSK	10	11-13
1	QPSK	50	25-30
2	8 QAM	50	39-47
3	16 QAM	50	54-66
4	32 QAM	100	72-88
5	64 QAM	100	89-109
6	128 QAM	100	108-132
7	256 QAM	150	123-150
8	512 QAM	150	134-164
9	1024 QAM (Strong FEC)	150	143-175
10	1024 QAM (Light FEC)	150	152-186
11	2048 QAM	150	162-198

8.4.3 25 MHz – Script ID 4525

Table 32: Radio Capacity with 25 MHz (Script 4525)

Profile	Modulation	Minimum required capacity activation key	Ethernet throughput (Mbps)
0	BPSK	50	15-18
1	QPSK	50	33-40
2	8 QAM	50	50-61
3	16 QAM	100	69-85
4	32 QAM	100	92-113
5	64 QAM	100	113-139
6	128 QAM	150	137-168
7	256 QAM	150	157-193
8	512 QAM	200	173-213
9	1024 QAM (Strong FEC)	200	184-227
10	1024 QAM (Light FEC)	200	196-241
11	2048 QAM	225	210-259
12	4096 QAM	225	228-280

8.4.4 28 MHz – Script ID 4504 (ETSI)

0	BPSK	50	17-20
1	QPSK	50	37-45
2	8 QAM	50	57-70
3	16 QAM	100	79-96
4	32 QAM	100	105-128
5	64 QAM	150	130-158
6	128 QAM	150	157-191
7	256 QAM	200	179-218
8	512 QAM	200	198-242
9	1024 QAM (Strong FEC)	225	210-257
10	1024 QAM (Light FEC)	225	223-273
11	2048 QAM	250	240-293
12	4096 QAM	300	259-317

8.4.5 28/30 MHz – Script ID 4505 (ETSI and ANSI)

Table 34: Radio Capacity with 28/30 MHz (Script 4505)

Profile	Modulation	Minimum required capacity activation key	Ethernet throughput (Mbps)
0	BPSK	50	18-22
1	QPSK	50	40-49
2	8 QAM	50	59-72
3	16 QAM	100	84-103
4	32 QAM	100	111-136
5	64 QAM	150	137-169
6	128 QAM	150	165-203
7	256 QAM	200	191-235
8	512 QAM	200	204-250
9	1024 QAM (Strong FEC)	225	222-273
10	1024 QAM (Light FEC)	225	236-290
11	2048 QAM	250	257-316
12	4096 QAM	300	274-337

8.4.6 28 MHz – Script ID 4514 (ETSI)

Note: This script is planned for future release.

Table 35: Radio Capacity with 28 MHz (Script 4514)

Profile	Modulation	Minimum required capacity activation key	Ethernet throughput (Mbps)
0	BPSK	50	16-19
1	QPSK	50	36-44
2	8 QAM	50	55-67
3	16 QAM	100	76-93
4	32 QAM	100	101-124
5	64 QAM	150	126-153
6	128 QAM	150	151-185
7	256 QAM	150	173-211
8	512 QAM	200	191-234
9	1024 QAM (Strong FEC)	200	204-249
10	1024 QAM (Light FEC)	225	216-264
11	2048 QAM	225	232-284
12	4096 QAM	250	247-302

8.4.7 40 MHz – Script ID 4507 (ETSI and ANSI)

Table 36: Radio Capacity with 40 MHz (Script 4507)

Profile	Modulation	Minimum required capacity activation key	Ethernet throughput (Mbps)
0	BPSK	50	25-31
1	QPSK	50	54-67
2	8 QAM	100	83-101
3	16 QAM	100	113-139
4	32 QAM	150	150-184
5	64 QAM	200	185-227
6	128 QAM	225	225-275
7	256 QAM	250	242-296
8	512 QAM	300	265-324
9	1024 QAM (Strong FEC)	300	301-368
10	1024 QAM (Light FEC)	300	320-391
11	2048 QAM	350	346-423
12	4096 QAM	400	366-448

8.4.8 50 MHz – Script ID 4510 (ANSI)

Table 37: Radio Capacity with 50 MHz (Script 4510)

Profile	Modulation	Minimum required capacity activation key	Ethernet throughput (Mbps)
0	BPSK	50	33-40
1	QPSK	100	67-82
2	8 QAM	100	105-129
3	16 QAM	150	144-176
4	32 QAM	200	181-222
5	64 QAM	225	235-287
6	128 QAM	300	275-336
7	256 QAM	300	326-399
8	512 QAM	350	354-433
9	1024 QAM (Strong FEC)	400	386-472
10	1024 QAM (Light FEC)	400	410-501
11	2048 QAM	450	442-541
12	4096 QAM	450	459-561

8.4.9 56 MHz – Script ID 4502 (ETSI)

Table 38: Radio Capacity with 56 MHz (Script 4502)

Profile	Modulation	Minimum required capacity activation key	Ethernet throughput (Mbps)
0	BPSK	50	37-46
1	QPSK	100	79-97
2	8 QAM	100	119-146
3	16 QAM	150	163-200
4	32 QAM	225	216-264
5	64 QAM	300	265-324
6	128 QAM	300	322-393
7	256 QAM	400	368-450
8	512 QAM	400	400-489
9	1024 QAM (Strong FEC)	450	435-532
10	1024 QAM (Light FEC)	450	462-565
11	2048 QAM	500	487-595
12	4096 QAM	500	516-631

8.4.10 56/60 MHz – Script ID 4506 (ETSI and ANSI)

Table 39: Radio Capacity for 56/60 MHz (Script 4506)

Profile	Modulation	Minimum required capacity activation key	Ethernet throughput (Mbps)
0	BPSK	50	40-49
1	QPSK	100	83-102
2	8 QAM	150	123-150
3	16 QAM	200	172-210
4	32 QAM	225	227-277
5	64 QAM	300	279-341
6	128 QAM	350	338-413
7	256 QAM	400	391-478
8	512 QAM	450	420-514
9	1024 QAM (Strong FEC)	450	457-559
10	1024 QAM (Light FEC)	500	486-594
11	2048 QAM	500	527-644
12	4096 QAM	500	542-663

8.4.11 70 MHz – Script ID 4513 (ETSI)

Table 40: Radio Capacity for 70 MHz (Script 4513)

Profile	Modulation	Minimum required capacity activation key	Ethernet throughput (Mbps)
0	BPSK	50	47-57
1	QPSK	100	96-118
2	8 QAM	150	138-169
3	16 QAM	200	198-242
4	32 QAM	250	261-319
5	64 QAM	300	319-390
6	128 QAM	400	378-462
7	256 QAM	450	436-533
8	512 QAM	500	479-585
9	1024 QAM (Strong FEC)	500	521-637
10	1024 QAM (Light FEC)	650	554-677
11	2048 QAM	650	586-716
12	4096 QAM	650	619-756

8.4.12 80 MHz – Script ID 4501 (ETSI and ANSI)

Table 41: Radio Capacity for 80 MHz (Script 4501)

Profile	Modulation	Minimum required capacity activation key	Ethernet throughput (Mbps)
0	BPSK	50	54-66
1	QPSK	100	113-138
2	8 QAM	150	161-197
3	16 QAM	225	227-277
4	32 QAM	300	301-368
5	64 QAM	400	370-452
6	128 QAM	450	444-543
7	256 QAM	500	510-623
8	512 QAM	650	560-685
9	1024 QAM (Strong FEC)	650	601-735
10	1024 QAM (Light FEC)	650	640-783
11	2048 QAM	650	678-828
12	4096 QAM	650	713-872

8.4.13 80 MHz – Script ID 4588 (ETSI)

Table 42: Radio Capacity for 80 MHz (Script 4588)

Profile	Modulation	Minimum required capacity activation key	Ethernet throughput (Mbps)
0	BPSK	50	59-72
1	QPSK	100	122-149
2	8 QAM	200	174-213
3	16 QAM	250	245-299
4	32 QAM	300	325-398
5	64 QAM	400	399-488
6	128 QAM	500	479-586
7	256 QAM	500	550-673
8	512 QAM	650	604-739
9	1024 QAM (Strong FEC)	650	649-793
10	1024 QAM (Light FEC)	650	691-844
11	2048 QAM	1000	731-894
12	4096 QAM	1000	769-940

8.4.14 112 MHz - Script ID 4511 (ETSI)

Table 43: Radio Capacity for 112 MHz (Script 4511)

Profile	Modulation	Minimum required capacity activation key	Ethernet throughput (Mbps)
0	BPSK	100	79-97
1	QPSK	150	162-198
2	8 QAM	250	242-296
3	16 QAM	350	330-404
4	32 QAM	450	435-532
5	64 QAM	500	535-654
6	128 QAM	650	647-791
7	256 QAM	1000	740-905
8	512 QAM	1000	804-983
9	1024 QAM (Strong FEC)	1000	872-1066
10	1024 QAM (Light FEC)	1000	926-1132
11	2048 QAM	1000	999-1221
12	4096 QAM	1000	1034-1264

8.4.15 140 MHz – Script ID 4518 (ETSI)

Table 44: Radio Capacity for 140 MHz (Script 4518)

Profile	Modulation	Minimum required capacity activation key	Ethernet throughput (Mbps)
0	BPSK	100	100-122
1	QPSK	200	204-249
2	8 QAM	300	304-371
3	16 QAM	400	414-506
4	32 QAM	500	545-667
5	64 QAM	650	694-848
6	128 QAM	1000	810-990
7	256 QAM	1000	926-1132
8	512 QAM	1000	1047-1280
9	1024 QAM	1600	1163-1422
10	2048 QAM	1600	1280-1564

8.4.16 150 MHz – Script ID 4515 (ANSI)

Table 45: Radio Capacity for 150 MHz (Script 4515)

Profile	Modulation	Minimum required capacity activation key	Ethernet throughput (Mbps)
0	BPSK	100	107-131
1	QPSK	225	218-267
2	8 QAM	300	326-398
3	16 QAM	450	443-542
4	32 QAM	650	584-713
5	64 QAM	1000	743-908
6	128 QAM	1000	867-1059
7	256 QAM	1000	991-1212
8	512 QAM	1600	1121-1370
9	1024 QAM	1600	1245-1522
10	2048 QAM	1600	1370-1674

8.4.17 160 MHz – Script ID 4516 (ANSI)

Table 46: Radio Capacity with 160 MHz (Script 4516)

Profile	Modulation	Minimum required capacity activation key	Ethernet Throughput (Mbps)
0	BPSK	100	113-138
1	QPSK	225	229-280
2	8 QAM	350	341-417
3	16 QAM	500	464-567
4	32 QAM	650	611-747
5	64 QAM	1000	778-951
6	128 QAM	1000	908-1110
7	256 QAM	1000	1038-1268
8	512 QAM	1600	1173-1434
9	1024 QAM	1600	1302-1592
10	2048 QAM	1600	1431-1750

8.4.18 224 MHz – Script ID 4524 (ETSI)

Table 47: Radio Capacity for 224 MHz (Script 4524)

Profile	Modulation	Minimum required capacity activation key	Ethernet throughput (Mbps)
0	BPSK	150	162-198
1	QPSK	350	328-401
2	8 QAM	500	489-597
3	16 QAM	650	665-812
4	32 QAM	1000	875-1069
5	64 QAM	1600	1111-1358
6	128 QAM	1600	1298-1587
7	256 QAM	1600	1484-1815
8	512 QAM	1600	1678-2051
9	1024 QAM (Strong FEC)	2000	1860-2274
10	2048 QAM	2000	2009-2456

8.5 Transmit Power Specifications

Notes: Nominal TX power is subject to change until the relevant frequency band is formally released. See the frequency rollout plan.

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

When using a 28 MHz script for the 6-8 GHz frequency band with diplexer bandwidth more than twice the channel bandwidth, the maximum Transmit Power level should be limited to no more than 27 dBm for ETSI compliance.

Table 48: Transmit Power Specifications (dBm)

Modulation	6 GHz	7-8 GHz	10-11 GHz	13 GHz	15 GHz	18 GHz	23 GHz	26 GHz	28 GHz	32 GHz	38 GHz	42 GHz
BPSK	28	28	28	26	25	24	24	22	22	22	22	15
QPSK	28	28	28	26	25	24	24	22	22	22	22	15
8 QAM	28	28	28	26	25	24	24	22	22	22	22	15
16 QAM	28	27	28	25	24	24	24	22	21	21	21	15
32 QAM	28	27	28	24	24	24	24	22	21	21	21	14
64 QAM	28	26	27	24	24	23	24	21	20	20	20	13
128 QAM	27	26	26	24	24	23	24	21	20	20	20	13
256 QAM	27	26	26	24	23	23	23	20	19	19	19	13
512 QAM	27	25	26	23	22	22	22	20	19	19	19	11
1024 QAM	26	24	25	22	21	21	21	20	18	18	18	11
2048 QAM	25	23	24	21	21	20	20	19	18	18	18	10
4096 QAM	24	21	22	20	20	19	19	18	17	17	17	

8.5.1 Pmin Power

Table 49: Pmin Power

Frequency Band	Pmin	Frequency Band	Pmin
6-11 GHz	4	18 GHz	1
13, 15, and 23 GHz	2	26 GHz	-1
28-42 GHz	2		

8.6 Receiver Threshold Specifications (dBm@ 10E^{-6})

Notes: 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 50: Receiver Thresholds (6-18 GHz)

Profile	Modulation	Channel Spacing	6	7	8	10	11	13	15	18
0	BPSK	14 MHz	-93.5	-93.0	-93.0	-92.0	-92.0	-92.0	-92.0	-93.0
1	QPSK		-90.6	-90.1	-90.1	-89.1	-89.1	-89.1	-89.1	-90.1
2	8 QAM		-86.7	-86.2	-86.2	-85.2	-85.2	-85.2	-85.2	-86.2
3	16 QAM		-83.6	-83.1	-83.1	-82.1	-82.1	-82.1	-82.1	-83.1
4	32 QAM		-80.3	-79.8	-79.8	-78.8	-78.8	-78.8	-78.8	-79.8
5	64 QAM		-77.1	-76.6	-76.6	-75.6	-75.6	-75.6	-75.6	-76.6
6	128 QAM		-74.0	-73.5	-73.5	-72.5	-72.5	-72.5	-72.5	-73.5
7	256 QAM		-70.6	-70.1	-70.1	-69.1	-69.1	-69.1	-69.1	-70.1
8	512 QAM		-67.7	-67.2	-67.2	-66.2	-66.2	-66.2	-66.2	-67.2
9	1024 QAM (Strong FEC)		-64.2	-63.7	-63.7	-62.7	-62.7	-62.7	-62.7	-63.7
10	1024 QAM (Light FEC)		-63.3	-62.8	-62.8	-61.8	-61.8	-61.8	-61.8	-62.8
11	2048 QAM		-60.1	-59.6	-59.6	-58.6	-58.6	-58.6	-58.6	-59.6
0	BPSK	20 MHz	-92.1	-91.6	-91.6	-90.6	-90.6	-90.6	-90.6	-91.6
1	QPSK		-89.2	-88.7	-88.7	-87.7	-87.7	-87.7	-87.7	-88.7
2	8 QAM		-85.2	-84.7	-84.7	-83.7	-83.7	-83.7	-83.7	-84.7
3	16 QAM		-82.3	-81.8	-81.8	-80.8	-80.8	-80.8	-80.8	-81.8
4	32 QAM		-78.9	-78.4	-78.4	-77.4	-77.4	-77.4	-77.4	-78.4
5	64 QAM		-75.7	-75.2	-75.2	-74.2	-74.2	-74.2	-74.2	-75.2
6	128 QAM		-72.7	-72.2	-72.2	-71.2	-71.2	-71.2	-71.2	-72.2
7	256 QAM		-69.6	-69.1	-69.1	-68.1	-68.1	-68.1	-68.1	-69.1
8	512 QAM		-66.8	-66.3	-66.3	-65.3	-65.3	-65.3	-65.3	-66.3
9	1024 QAM (Strong FEC)		-63.9	-63.4	-63.4	-62.4	-62.4	-62.4	-62.4	-63.4
10	1024 QAM (Light FEC)		-63.2	-62.7	-62.7	-61.7	-61.7	-61.7	-61.7	-62.7
11	2048 QAM		-60.7	-60.2	-60.2	-59.2	-59.2	-59.2	-59.2	-60.2

Profile	Modulation	Channel Spacing	6	7	8	10	11	13	15	18
0	BPSK	25 MHz	-91.1	-90.6	-90.6	-89.6	-89.6	-89.6	-89.6	-90.6
1	QPSK		-88.1	-87.6	-87.6	-86.6	-86.6	-86.6	-86.6	-87.6
2	8 QAM		-84.1	-83.6	-83.6	-82.6	-82.6	-82.6	-82.6	-83.6
3	16 QAM		-81.2	-80.7	-80.7	-79.7	-79.7	-79.7	-79.7	-80.7
4	32 QAM		-77.9	-77.4	-77.4	-76.4	-76.4	-76.4	-76.4	-77.4
5	64 QAM		-74.8	-74.3	-74.3	-73.3	-73.3	-73.3	-73.3	-74.3
6	128 QAM		-71.7	-71.2	-71.2	-70.2	-70.2	-70.2	-70.2	-71.2
7	256 QAM		-68.6	-68.1	-68.1	-67.1	-67.1	-67.1	-67.1	-68.1
8	512 QAM		-65.7	-65.2	-65.2	-64.2	-64.2	-64.2	-64.2	-65.2
9	1024 QAM (Strong FEC)		-62.8	-62.3	-62.3	-61.3	-61.3	-61.3	-61.3	-62.3
10	1024 QAM (Light FEC)		-61.9	-61.4	-61.4	-60.4	-60.4	-60.4	-60.4	-61.4
11	2048 QAM		-59.8	-59.3	-59.3	-58.3	-58.3	-58.3	-58.3	-59.3
12	4096 QAM		-55.7	-55.2	-55.2	-54.2	-54.2	-54.2	-54.2	-55.2
0	BPSK	28 MHz	-90.5	-90.0	-90.0	-89.0	-89.0	-89.0	-89.0	-90.0
1	QPSK		-87.5	-87.0	-87.0	-86.0	-86.0	-86.0	-86.0	-87.0
2	8 QAM		-83.6	-83.1	-83.1	-82.1	-82.1	-82.1	-82.1	-83.1
3	16 QAM		-80.6	-80.1	-80.1	-79.1	-79.1	-79.1	-79.1	-80.1
4	32 QAM		-77.3	-76.8	-76.8	-75.8	-75.8	-75.8	-75.8	-76.8
5	64 QAM		-74.3	-73.8	-73.8	-72.8	-72.8	-72.8	-72.8	-73.8
6	128 QAM		-71.2	-70.7	-70.7	-69.7	-69.7	-69.7	-69.7	-70.7
7	256 QAM		-68.1	-67.6	-67.6	-66.6	-66.6	-66.6	-66.6	-67.6
8	512 QAM		-65.3	-64.8	-64.8	-63.8	-63.8	-63.8	-63.8	-64.8
9	1024 QAM (Strong FEC)		-62.4	-61.9	-61.9	-60.9	-60.9	-60.9	-60.9	-61.9
10	1024 QAM (Light FEC)		-61.7	-61.2	-61.2	-60.2	-60.2	-60.2	-60.2	-61.2
11	2048 QAM		-59.2	-58.7	-58.7	-57.7	-57.7	-57.7	-57.7	-58.7
12	4096 QAM		-55.2	-54.7	-54.7	-53.7	-53.7	-53.7	-53.7	-54.7

Profile	Modulation	Channel Spacing	6	7	8	10	11	13	15	18
0	BPSK	30 MHz	-90.4	-89.9	-89.9	-88.9	-88.9	-88.9	-88.9	-89.9
1	QPSK		-87.4	-86.9	-86.9	-85.9	-85.9	-85.9	-85.9	-86.9
2	8 QAM		-83.4	-82.9	-82.9	-81.9	-81.9	-81.9	-81.9	-82.9
3	16 QAM		-80.4	-79.9	-79.9	-78.9	-78.9	-78.9	-78.9	-79.9
4	32 QAM		-77.1	-76.6	-76.6	-75.6	-75.6	-75.6	-75.6	-76.6
5	64 QAM		-74.0	-73.5	-73.5	-72.5	-72.5	-72.5	-72.5	-73.5
6	128 QAM		-71.0	-70.5	-70.5	-69.5	-69.5	-69.5	-69.5	-70.5
7	256 QAM		-67.8	-67.3	-67.3	-66.3	-66.3	-66.3	-66.3	-67.3
8	512 QAM		-65.5	-65.0	-65.0	-64.0	-64.0	-64.0	-64.0	-65.0
9	1024 QAM (Strong FEC)		-62.2	-61.7	-61.7	-60.7	-60.7	-60.7	-60.7	-61.7
10	1024 QAM (Light FEC)		-61.4	-60.9	-60.9	-59.9	-59.9	-59.9	-59.9	-60.9
11	2048 QAM		-58.9	-58.4	-58.4	-57.4	-57.4	-57.4	-57.4	-58.4
12	4096 QAM		-55.2	-54.7	-54.7	-53.7	-53.7	-53.7	-53.7	-54.7
0	BPSK	40 MHz	-89.3	-88.8	-88.8	-87.8	-87.8	-87.8	-87.8	-88.8
1	QPSK		-86.1	-85.6	-85.6	-84.6	-84.6	-84.6	-84.6	-85.6
2	8 QAM		-82.1	-81.6	-81.6	-80.6	-80.6	-80.6	-80.6	-81.6
3	16 QAM		-79.2	-78.7	-78.7	-77.7	-77.7	-77.7	-77.7	-78.7
4	32 QAM		-75.8	-75.3	-75.3	-74.3	-74.3	-74.3	-74.3	-75.3
5	64 QAM		-72.7	-72.2	-72.2	-71.2	-71.2	-71.2	-71.2	-72.2
6	128 QAM		-69.7	-69.2	-69.2	-68.2	-68.2	-68.2	-68.2	-69.2
7	256 QAM		-67.4	-66.9	-66.9	-65.9	-65.9	-65.9	-65.9	-66.9
8	512 QAM		-64.6	-64.1	-64.1	-63.1	-63.1	-63.1	-63.1	-64.1
9	1024 QAM (Strong FEC)		-61.1	-60.6	-60.6	-59.6	-59.6	-59.6	-59.6	-60.6
10	1024 QAM (Light FEC)		-60.4	-59.9	-59.9	-58.9	-58.9	-58.9	-58.9	-59.9
11	2048 QAM		-58.1	-57.6	-57.6	-56.6	-56.6	-56.6	-56.6	-57.6
12	4096 QAM		-55.0	-54.5	-54.5	-53.5	-53.5	-53.5	-53.5	-54.5

Profile	Modulation	Channel Spacing	6	7	8	10	11	13	15	18
0	BPSK	50 MHz	-88.2	-87.7	-87.7	-86.7	-86.7	-86.7	-86.7	-87.7
1	QPSK		-85.3	-84.8	-84.8	-83.8	-83.8	-83.8	-83.8	-84.8
2	8 QAM		-81.0	-80.5	-80.5	-79.5	-79.5	-79.5	-79.5	-80.5
3	16 QAM		-78.1	-77.6	-77.6	-76.6	-76.6	-76.6	-76.6	-77.6
4	32 QAM		-75.1	-74.6	-74.6	-73.6	-73.6	-73.6	-73.6	-74.6
5	64 QAM		-71.7	-71.2	-71.2	-70.2	-70.2	-70.2	-70.2	-71.2
6	128 QAM		-69.2	-68.7	-68.7	-67.7	-67.7	-67.7	-67.7	-68.7
7	256 QAM		-65.6	-65.1	-65.1	-64.1	-64.1	-64.1	-64.1	-65.1
8	512 QAM		-63.1	-62.6	-62.6	-61.6	-61.6	-61.6	-61.6	-62.6
9	1024 QAM (Strong FEC)		-59.7	-59.2	-59.2	-58.2	-58.2	-58.2	-58.2	-59.2
10	1024 QAM (Light FEC)		-58.9	-58.4	-58.4	-57.4	-57.4	-57.4	-57.4	-58.4
11	2048 QAM		-56.6	-56.1	-56.1	-55.1	-55.1	-55.1	-55.1	-56.1
12	4096 QAM		-53.1	-52.6	-52.6	-51.6	-51.6	-51.6	-51.6	-52.6
0	BPSK	56 MHz	-87.7	-87.2	-87.2	-86.2	-86.2	-86.2	-86.2	-87.2
1	QPSK		-84.5	-84.0	-84.0	-83.0	-83.0	-83.0	-83.0	-84.0
2	8 QAM		-80.4	-79.9	-79.9	-78.9	-78.9	-78.9	-78.9	-79.9
3	16 QAM		-77.5	-77.0	-77.0	-76.0	-76.0	-76.0	-76.0	-77.0
4	32 QAM		-74.2	-73.7	-73.7	-72.7	-72.7	-72.7	-72.7	-73.7
5	64 QAM		-71.2	-70.7	-70.7	-69.7	-69.7	-69.7	-69.7	-70.7
6	128 QAM		-68.3	-67.8	-67.8	-66.8	-66.8	-66.8	-66.8	-67.8
7	256 QAM		-65.1	-64.6	-64.6	-63.6	-63.6	-63.6	-63.6	-64.6
8	512 QAM		-62.5	-62.0	-62.0	-61.0	-61.0	-61.0	-61.0	-62.0
9	1024 QAM (Strong FEC)		-59.2	-58.7	-58.7	-57.7	-57.7	-57.7	-57.7	-58.7
10	1024 QAM (Light FEC)		-58.3	-57.8	-57.8	-56.8	-56.8	-56.8	-56.8	-57.8
11	2048 QAM		-56.5	-56.0	-56.0	-55.0	-55.0	-55.0	-55.0	-56.0
12	4096 QAM		-52.6	-52.1	-52.1	-51.1	-51.1	-51.1	-51.1	-52.1

Profile	Modulation	Channel Spacing	6	7	8	10	11	13	15	18
0	BPSK	60 MHz	-87.5	-87.0	-87.0	-86.0	-86.0	-86.0	-86.0	-87.0
1	QPSK		-84.3	-83.8	-83.8	-82.8	-82.8	-82.8	-82.8	-83.8
2	8 QAM		-80.5	-80.0	-80.0	-79.0	-79.0	-79.0	-79.0	-80.0
3	16 QAM		-77.3	-76.8	-76.8	-75.8	-75.8	-75.8	-75.8	-76.8
4	32 QAM		-74.0	-73.5	-73.5	-72.5	-72.5	-72.5	-72.5	-73.5
5	64 QAM		-70.9	-70.4	-70.4	-69.4	-69.4	-69.4	-69.4	-70.4
6	128 QAM		-68.1	-67.6	-67.6	-66.6	-66.6	-66.6	-66.6	-67.6
7	256 QAM		-64.9	-64.4	-64.4	-63.4	-63.4	-63.4	-63.4	-64.4
8	512 QAM		-62.4	-61.9	-61.9	-60.9	-60.9	-60.9	-60.9	-61.9
9	1024 QAM (Strong FEC)		-59.1	-58.6	-58.6	-57.6	-57.6	-57.6	-57.6	-58.6
10	1024 QAM (Light FEC)		-58.3	-57.8	-57.8	-56.8	-56.8	-56.8	-56.8	-57.8
11	2048 QAM		-56.0	-55.5	-55.5	-54.5	-54.5	-54.5	-54.5	-55.5
12	4096 QAM		-52.2	-51.7	-51.7	-50.7	-50.7	-50.7	-50.7	-51.7
0	BPSK	70 MHz	-86.7	-86.2	-86.2	-85.2	-85.2	-85.2	-85.2	-86.2
1	QPSK		-83.9	-83.4	-83.4	-82.4	-82.4	-82.4	-82.4	-83.4
2	8 QAM		-80.2	-79.7	-79.7	-78.7	-78.7	-78.7	-78.7	-79.7
3	16 QAM		-77.2	-76.7	-76.7	-75.7	-75.7	-75.7	-75.7	-76.7
4	32 QAM		-73.6	-73.1	-73.1	-72.1	-72.1	-72.1	-72.1	-73.1
5	64 QAM		-70.7	-70.2	-70.2	-69.2	-69.2	-69.2	-69.2	-70.2
6	128 QAM		-67.9	-67.4	-67.4	-66.4	-66.4	-66.4	-66.4	-67.4
7	256 QAM		-65.1	-64.6	-64.6	-63.6	-63.6	-63.6	-63.6	-64.6
8	512 QAM		-62.4	-61.9	-61.9	-60.9	-60.9	-60.9	-60.9	-61.9
9	1024 QAM (Strong FEC)		-59.5	-59.0	-59.0	-58.0	-58.0	-58.0	-58.0	-59.0
10	1024 QAM (Light FEC)		-58.8	-58.3	-58.3	-57.3	-57.3	-57.3	-57.3	-58.3
11	2048 QAM		-56.6	-56.1	-56.1	-55.1	-55.1	-55.1	-55.1	-56.1
12	4096 QAM		-53.2	-52.7	-52.7	-51.7	-51.7	-51.7	-51.7	-52.7

Profile	Modulation	Channel Spacing	6	7	8	10	11	13	15	18
0	BPSK	80 MHz	-86.1	-85.6	-85.6	-84.6	-84.6	-84.6	-84.6	-85.6
1	QPSK		-83.3	-82.8	-82.8	-81.8	-81.8	-81.8	-81.8	-82.8
2	8 QAM		-79.8	-79.3	-79.3	-78.3	-78.3	-78.3	-78.3	-79.3
3	16 QAM		-76.8	-76.3	-76.3	-75.3	-75.3	-75.3	-75.3	-76.3
4	32 QAM		-73.2	-72.7	-72.7	-71.7	-71.7	-71.7	-71.7	-72.7
5	64 QAM		-70.1	-69.6	-69.6	-68.6	-68.6	-68.6	-68.6	-69.6
6	128 QAM		-67.0	-66.5	-66.5	-65.5	-65.5	-65.5	-65.5	-66.5
7	256 QAM		-64.2	-63.7	-63.7	-62.7	-62.7	-62.7	-62.7	-63.7
8	512 QAM		-61.3	-60.8	-60.8	-59.8	-59.8	-59.8	-59.8	-60.8
9	1024 QAM (Strong FEC)		-58.5	-58.0	-58.0	-57.0	-57.0	-57.0	-57.0	-58.0
10	1024 QAM (Light FEC)		-57.4	-56.9	-56.9	-55.9	-55.9	-55.9	-55.9	-56.9
11	2048 QAM		-54.9	-54.4	-54.4	-53.4	-53.4	-53.4	-53.4	-54.4
12	4096 QAM		-51.7	-51.2	-51.2	-50.2	-50.2	-50.2	-50.2	-51.2
0	BPSK	112 MHz	-84.0	-83.5	-83.5	-82.5	-82.5	-82.5	-82.5	-83.5
1	QPSK		-81.6	-81.1	-81.1	-80.1	-80.1	-80.1	-80.1	-81.1
2	8 QAM		-77.6	-77.1	-77.1	-76.1	-76.1	-76.1	-76.1	-77.1
3	16 QAM		-74.7	-74.2	-74.2	-73.2	-73.2	-73.2	-73.2	-74.2
4	32 QAM		-71.3	-70.8	-70.8	-69.8	-69.8	-69.8	-69.8	-70.8
5	64 QAM		-68.3	-67.8	-67.8	-66.8	-66.8	-66.8	-66.8	-67.8
6	128 QAM		-65.4	-64.9	-64.9	-63.9	-63.9	-63.9	-63.9	-64.9
7	256 QAM		-62.4	-61.9	-61.9	-60.9	-60.9	-60.9	-60.9	-61.9
8	512 QAM		-60.0	-59.5	-59.5	-58.5	-58.5	-58.5	-58.5	-59.5
9	1024 QAM (Strong FEC)		-57.0	-56.5	-56.5	-55.5	-55.5	-55.5	-55.5	-56.5
10	1024 QAM (Light FEC)		-56.3	-55.8	-55.8	-54.8	-54.8	-54.8	-54.8	-55.8
11	2048 QAM		-53.7	-53.2	-53.2	-52.2	-52.2	-52.2	-52.2	-53.2
12	4096 QAM		-51.0	-50.5	-50.5	-49.5	-49.5	-49.5	-49.5	-50.5

Profile	Modulation	Channel Spacing	6	7	8	10	11	13	15	18
0	BPSK	140 MHz		-83.4	-83.4	-82.4	-82.4	-82.4	-82.4	-83.4
1	QPSK			-80.1	-80.1	-79.1	-79.1	-79.1	-79.1	-80.1
2	8 QAM			-76.5	-76.5	-75.5	-75.5	-75.5	-75.5	-76.5
3	16 QAM			-73.4	-73.4	-72.4	-72.4	-72.4	-72.4	-73.4
4	32 QAM			-69.8	-69.8	-68.8	-68.8	-68.8	-68.8	-69.8
5	64 QAM			-66.4	-66.4	-65.4	-65.4	-65.4	-65.4	-66.4
6	128 QAM			-63.9	-63.9	-62.9	-62.9	-62.9	-62.9	-63.9
7	256 QAM			-60.9	-60.9	-59.9	-59.9	-59.9	-59.9	-60.9
8	512 QAM			-58.0	-58.0	-57.0	-57.0	-57.0	-57.0	-58.0
9	1024 QAM			-54.9	-54.9	-53.9	-53.9	-53.9	-53.9	-54.9
11	2048 QAM			-51.8	-51.8	-50.8	-50.8	-50.8	-50.8	-51.8
0	BPSK	150 MHz		-84.1	-83.6	-83.1	-83.1	-82.1	-82.1	-82.1
1	QPSK			-81.0	-80.5	-80.0	-80.0	-79.0	-79.0	-79.0
2	8 QAM			-77.2	-76.7	-76.2	-76.2	-75.2	-75.2	-75.2
3	16 QAM			-74.0	-73.5	-73.0	-73.0	-72.0	-72.0	-72.0
4	32 QAM			-70.6	-70.1	-69.6	-69.6	-68.6	-68.6	-68.6
5	64 QAM			-67.2	-66.7	-66.2	-66.2	-65.2	-65.2	-65.2
6	128 QAM			-64.7	-64.2	-63.7	-63.7	-62.7	-62.7	-62.7
7	256 QAM			-61.7	-61.2	-60.7	-60.7	-59.7	-59.7	-59.7
8	512 QAM			-58.8	-58.3	-57.8	-57.8	-56.8	-56.8	-56.8
9	1024 QAM			-55.8	-55.3	-54.8	-54.8	-53.8	-53.8	-53.8
10	2048 QAM			-52.5	-52.0	-51.5	-51.5	-50.5	-50.5	-50.5

Profile	Modulation	Channel Spacing	6	7	8	10	11	13	15	18
0	BPSK	160 MHz		-82.0	-82.0	-81.0	-81.0	-81.0	-81.0	-82.0
1	QPSK			-79.8	-79.8	-78.8	-78.8	-78.8	-78.8	-79.8
2	8 QAM			-75.3	-75.3	-74.3	-74.3	-74.3	-74.3	-75.3
3	16 QAM			-72.9	-72.9	-71.9	-71.9	-71.9	-71.9	-72.9
4	32 QAM			-69.5	-69.5	-68.5	-68.5	-68.5	-68.5	-69.5
5	64 QAM			-66.2	-66.2	-65.2	-65.2	-65.2	-65.2	-66.2
6	128 QAM			-63.4	-63.4	-62.4	-62.4	-62.4	-62.4	-63.4
7	256 QAM			-60.3	-60.3	-59.3	-59.3	-59.3	-59.3	-60.3
8	512 QAM			-57.6	-57.6	-56.6	-56.6	-56.6	-56.6	-57.6
9	1024 QAM			-54.3	-54.3	-53.3	-53.3	-53.3	-53.3	-54.3
10	2048 QAM			-50.5	-50.5	-49.5	-49.5	-49.5	-49.5	-50.5
0	BPSK	224 MHz[8]		-81.3	-81.3	-80.3	-80.3	-80.3	-80.3	-81.3
1	QPSK			-78.2	-78.2	-77.2	-77.2	-77.2	-77.2	-78.2
2	8 QAM			-74.4	-74.4	-73.4	-73.4	-73.4	-73.4	-74.4
3	16 QAM			-71.4	-71.4	-70.4	-70.4	-70.4	-70.4	-71.4
4	32 QAM			-67.8	-67.8	-66.8	-66.8	-66.8	-66.8	-67.8
5	64 QAM			-64.5	-64.5	-63.5	-63.5	-63.5	-63.5	-64.5
6	128 QAM			-61.9	-61.9	-60.9	-60.9	-60.9	-60.9	-61.9
7	256 QAM			-58.9	-58.9	-57.9	-57.9	-57.9	-57.9	-58.9
8	512 QAM			-55.5	-55.5	-54.5	-54.5	-54.5	-54.5	-55.5
9	1024 QAM			-51.9	-51.9	-50.9	-50.9	-50.9	-50.9	-51.9
10	2048 QAM			-48.2	-48.2	-47.2	-47.2	-47.2	-47.2	-48.2

[8] 224 MHz is only supported with certain hardware versions. For details, ask your Ceragon representative.

Table 51: Receiver Thresholds (23-42 GHz)

Profile	Modulation	Channel Spacing	23	24[9]	26	28-31	32	36	38	42
0	BPSK	14 MHz	-92.0	-91.0	-91.5	-91.5	-91.5	-91.5	-91.5	-90.5
1	QPSK		-89.1	-88.1	-88.6	-88.6	-88.6	-88.6	-88.6	-87.6
2	8 QAM		-85.2	-84.2	-84.7	-84.7	-84.7	-84.7	-84.7	-83.7
3	16 QAM		-82.1	-81.1	-81.6	-81.6	-81.6	-81.6	-81.6	-80.6
4	32 QAM		-78.8	-77.8	-78.3	-78.3	-78.3	-78.3	-78.3	-77.3
5	64 QAM		-75.6	-74.6	-75.1	-75.1	-75.1	-75.1	-75.1	-74.1
6	128 QAM		-72.5	-71.5	-72.0	-72.0	-72.0	-72.0	-72.0	-71.0
7	256 QAM		-69.1	-68.1	-68.6	-68.6	-68.6	-68.6	-68.6	-67.6
8	512 QAM		-66.2	-65.2	-65.7	-65.7	-65.7	-65.7	-65.7	-64.7
9	1024 QAM (Strong FEC)		-62.7	-61.7	-62.2	-62.2	-62.2	-62.2	-62.2	-61.2
10	1024 QAM (Light FEC)		-61.8	-60.8	-61.3	-61.3	-61.3	-61.3	-61.3	-60.3
11	2048 QAM		-58.6	-57.6	-58.1	-58.1	-58.1	-58.1	-58.1	-57.0
0	BPSK	20 MHz	-90.6	-89.6	-90.1	-90.1	-90.1	-90.1	-90.1	
1	QPSK		-87.7	-86.7	-87.2	-87.2	-87.2	-87.2	-87.2	
2	8 QAM		-83.7	-82.7	-83.2	-83.2	-83.2	-83.2	-83.2	
3	16 QAM		-80.8	-79.8	-80.3	-80.3	-80.3	-80.3	-80.3	
4	32 QAM		-77.4	-76.4	-76.9	-76.9	-76.9	-76.9	-76.9	
5	64 QAM		-74.2	-73.2	-73.7	-73.7	-73.7	-73.7	-73.7	
6	128 QAM		-71.2	-70.2	-70.7	-70.7	-70.7	-70.7	-70.7	
7	256 QAM		-68.1	-67.1	-67.6	-67.6	-67.6	-67.6	-67.6	
8	512 QAM		-65.3	-64.3	-64.8	-64.8	-64.8	-64.8	-64.8	
9	1024 QAM (Strong FEC)		-62.4	-61.4	-61.9	-61.9	-61.9	-61.9	-61.9	
10	1024 QAM (Light FEC)		-61.7	-60.7	-61.2	-61.2	-61.2	-61.2	-61.2	
11	2048 QAM		-59.2	-58.2	-58.7	-58.7	-58.7	-58.7	-58.7	

[9] Customers in countries following EC Directive 2006/771/EC (incl. amendments) must observe the 100mW EIRP obligation by adjusting transmit power according to antenna gain and RF line losses.

Profile	Modulation	Channel Spacing	23	24[9]	26	28-31	32	36	38	42
0	BPSK	25 MHz	-89.6	-88.6	-89.1	-89.1	-89.1	-89.1	-89.1	
1	QPSK		-86.6	-85.6	-86.1	-86.1	-86.1	-86.1	-86.1	
2	8 QAM		-82.6	-81.6	-82.1	-82.1	-82.1	-82.1	-82.1	
3	16 QAM		-79.7	-78.7	-79.2	-79.2	-79.2	-79.2	-79.2	
4	32 QAM		-76.4	-75.4	-75.9	-75.9	-75.9	-75.9	-75.9	
5	64 QAM		-73.3	-72.3	-72.8	-72.8	-72.8	-72.8	-72.8	
6	128 QAM		-70.2	-69.2	-69.7	-69.7	-69.7	-69.7	-69.7	
7	256 QAM		-67.1	-66.1	-66.6	-66.6	-66.6	-66.6	-66.6	
8	512 QAM		-64.2	-63.2	-63.7	-63.7	-63.7	-63.7	-63.7	
9	1024 QAM (Strong FEC)		-61.3	-60.3	-60.8	-60.8	-60.8	-60.8	-60.8	
10	1024 QAM (Light FEC)		-60.4	-59.4	-59.9	-59.9	-59.9	-59.9	-59.9	
11	2048 QAM		-58.3	-57.3	-57.8	-57.8	-57.8	-57.8	-57.8	
12	4096 QAM		-54.2	-53.2	-53.7	-53.7	-53.7			
0	BPSK	28 MHz	-89.0	-88.0	-88.5	-88.5	-88.5	-88.5	-88.5	-87.5
1	QPSK		-86.0	-85.0	-85.5	-85.5	-85.5	-85.5	-85.5	-84.5
2	8 QAM		-82.1	-81.1	-81.6	-81.6	-81.6	-81.6	-81.6	-80.6
3	16 QAM		-79.1	-78.1	-78.6	-78.6	-78.6	-78.6	-78.6	-77.6
4	32 QAM		-75.8	-74.8	-75.3	-75.3	-75.3	-75.3	-75.3	-74.3
5	64 QAM		-72.8	-71.8	-72.3	-72.3	-72.3	-72.3	-72.3	-71.3
6	128 QAM		-69.7	-68.7	-69.2	-69.2	-69.2	-69.2	-69.2	-68.2
7	256 QAM		-66.6	-65.6	-66.1	-66.1	-66.1	-66.1	-66.1	-65.1
8	512 QAM		-63.8	-62.8	-63.3	-63.3	-63.3	-63.3	-63.3	-62.3
9	1024 QAM (Strong FEC)		-60.9	-59.9	-60.4	-60.4	-60.4	-60.4	-60.4	-59.4
10	1024 QAM (Light FEC)		-60.2	-59.2	-59.7	-59.7	-59.7	-59.7	-59.7	-58.7
11	2048 QAM		-57.7	-56.7	-57.2	-57.2	-57.2	-57.2	-57.2	-56.2
12	4096 QAM		-53.7	-52.7	-53.2	-53.2	-53.2	-	-	-

Profile	Modulation	Channel Spacing	23	24[9]	26	28-31	32	36	38	42
0	BPSK	30 MHz	-88.9	-87.9	-88.4	-88.4	-88.4	-88.4	-88.4	
1	QPSK		-85.9	-84.9	-85.4	-85.4	-85.4	-85.4	-85.4	
2	8 QAM		-81.9	-80.9	-81.4	-81.4	-81.4	-81.4	-81.4	
3	16 QAM		-78.9	-77.9	-78.4	-78.4	-78.4	-78.4	-78.4	
4	32 QAM		-75.6	-74.6	-75.1	-75.1	-75.1	-75.1	-75.1	
5	64 QAM		-72.5	-71.5	-72.0	-72.0	-72.0	-72.0	-72.0	
6	128 QAM		-69.5	-68.5	-69.0	-69.0	-69.0	-69.0	-69.0	
7	256 QAM		-66.3	-65.3	-65.8	-65.8	-65.8	-65.8	-65.8	
8	512 QAM		-64.0	-63.0	-63.5	-63.5	-63.5	-63.5	-63.5	
9	1024 QAM (Strong FEC)		-60.7	-59.7	-60.2	-60.2	-60.2	-60.2	-60.2	
10	1024 QAM (Light FEC)		-59.9	-58.9	-59.4	-59.4	-59.4	-59.4	-59.4	
11	2048 QAM		-57.4	-56.4	-56.9	-56.9	-56.9	-56.9	-56.9	
12	4096 QAM		-53.7	-52.7	-53.2	-53.2	-53.2	-	-	
0	BPSK	40 MHz	-87.8	-86.8	-87.3	-87.3	-87.3	-87.3	-87.3	-86.3
1	QPSK		-84.6	-83.6	-84.1	-84.1	-84.1	-84.1	-84.1	-83.1
2	8 QAM		-80.6	-79.6	-80.1	-80.1	-80.1	-80.1	-80.1	-79.1
3	16 QAM		-77.7	-76.7	-77.2	-77.2	-77.2	-77.2	-77.2	-76.2
4	32 QAM		-74.3	-73.3	-73.8	-73.8	-73.8	-73.8	-73.8	-72.8
5	64 QAM		-71.2	-70.2	-70.7	-70.7	-70.7	-70.7	-70.7	-69.7
6	128 QAM		-68.2	-67.2	-67.7	-67.7	-67.7	-67.7	-67.7	-66.7
7	256 QAM		-65.9	-64.9	-65.4	-65.4	-65.4	-65.4	-65.4	-64.4
8	512 QAM		-63.1	-62.1	-62.6	-62.6	-62.6	-62.6	-62.6	-61.6
9	1024 QAM (Strong FEC)		-59.6	-58.6	-59.1	-59.1	-59.1	-59.1	-59.1	-58.1
10	1024 QAM (Light FEC)		-58.9	-57.9	-58.4	-58.4	-58.4	-58.4	-58.4	-57.4
11	2048 QAM		-56.6	-55.6	-56.1	-56.1	-56.1	-56.1	-56.1	-55.1
12	4096 QAM		-53.5	-52.5	-53.0	-53.0	-53.0	-	-	-

Profile	Modulation	Channel Spacing	23	24[9]	26	28-31	32	36	38	42
0	BPSK	50 MHz	-86.7	-85.7	-86.2	-86.2	-86.2	-86.2	-86.2	
1	QPSK		-83.8	-82.8	-83.3	-83.3	-83.3	-83.3	-83.3	
2	8 QAM		-79.5	-78.5	-79.0	-79.0	-79.0	-79.0	-79.0	
3	16 QAM		-76.6	-75.6	-76.1	-76.1	-76.1	-76.1	-76.1	
4	32 QAM		-73.6	-72.6	-73.1	-73.1	-73.1	-73.1	-73.1	
5	64 QAM		-70.2	-69.2	-69.7	-69.7	-69.7	-69.7	-69.7	
6	128 QAM		-67.7	-66.7	-67.2	-67.2	-67.2	-67.2	-67.2	
7	256 QAM		-64.1	-63.1	-63.6	-63.6	-63.6	-63.6	-63.6	
8	512 QAM		-61.6	-60.6	-61.1	-61.1	-61.1	-61.1	-61.1	
9	1024 QAM (Strong FEC)		-58.2	-57.2	-57.7	-57.7	-57.7	-57.7	-57.7	
10	1024 QAM (Light FEC)		-57.4	-56.4	-56.9	-56.9	-56.9	-56.9	-56.9	
11	2048 QAM		-55.1	-54.1	-54.6	-54.6	-54.6	-54.6	-54.6	
12	4096 QAM		-51.6	-50.6	-51.1	-	-	-	-	
0	BPSK	56 MHz	-86.2	-85.2	-85.7	-85.7	-85.7	-85.7	-85.7	-84.7
1	QPSK		-83.0	-82.0	-82.5	-82.5	-82.5	-82.5	-82.5	-81.5
2	8 QAM		-78.9	-77.9	-78.4	-78.4	-78.4	-78.4	-78.4	-77.4
3	16 QAM		-76.0	-75.0	-75.5	-75.5	-75.5	-75.5	-75.5	-74.5
4	32 QAM		-72.7	-71.7	-72.2	-72.2	-72.2	-72.2	-72.2	-71.2
5	64 QAM		-69.7	-68.7	-69.2	-69.2	-69.2	-69.2	-69.2	-68.2
6	128 QAM		-66.8	-65.8	-66.3	-66.3	-66.3	-66.3	-66.3	-65.3
7	256 QAM		-63.6	-62.6	-63.1	-63.1	-63.1	-63.1	-63.1	-62.1
8	512 QAM		-61.0	-60.0	-60.5	-60.5	-60.5	-60.5	-60.5	-59.5
9	1024 QAM (Strong FEC)		-57.7	-56.7	-57.2	-57.2	-57.2	-57.2	-57.2	-56.2
10	1024 QAM (Light FEC)		-56.8	-55.8	-56.3	-56.3	-56.3	-56.3	-56.3	-55.3
11	2048 QAM		-55.0	-54.0	-54.5	-54.5	-54.5	-54.5	-54.5	-53.5
12	4096 QAM		-51.1	-50.1	-50.6	-	-	-	-	-

Profile	Modulation	Channel Spacing	23	24[9]	26	28-31	32	36	38	42
0	BPSK	60 MHz	-86.0	-85.0	-85.5	-85.5	-85.5	-85.5	-85.5	
1	QPSK		-82.8	-81.8	-82.3	-82.3	-82.3	-82.3	-82.3	
2	8 QAM		-79.0	-78.0	-78.5	-78.5	-78.5	-78.5	-78.5	
3	16 QAM		-75.8	-74.8	-75.3	-75.3	-75.3	-75.3	-75.3	
4	32 QAM		-72.5	-71.5	-72.0	-72.0	-72.0	-72.0	-72.0	
5	64 QAM		-69.4	-68.4	-68.9	-68.9	-68.9	-68.9	-68.9	
6	128 QAM		-66.6	-65.6	-66.1	-66.1	-66.1	-66.1	-66.1	
7	256 QAM		-63.4	-62.4	-62.9	-62.9	-62.9	-62.9	-62.9	
8	512 QAM		-60.9	-59.9	-60.4	-60.4	-60.4	-60.4	-60.4	
9	1024 QAM (Strong FEC)		-57.6	-56.6	-57.1	-57.1	-57.1	-57.1	-57.1	
10	1024 QAM (Light FEC)		-56.8	-55.8	-56.3	-56.3	-56.3	-56.3	-56.3	
11	2048 QAM		-54.5	-53.5	-54.0	-54.0	-54.0	-54.0	-54.0	
12	4096 QAM		-50.7	-49.7	-50.2	-	-	-	-	
0	BPSK	70 MHz	-85.2	-84.2	-84.7	-84.7	-84.7	-84.7	-84.7	-83.7
1	QPSK		-82.4	-81.4	-81.9	-81.9	-81.9	-81.9	-81.9	-80.9
2	8 QAM		-78.7	-77.7	-78.2	-78.2	-78.2	-78.2	-78.2	-77.2
3	16 QAM		-75.7	-74.7	-75.2	-75.2	-75.2	-75.2	-75.2	-74.2
4	32 QAM		-72.1	-71.1	-71.6	-71.6	-71.6	-71.6	-71.6	-70.6
5	64 QAM		-69.2	-68.2	-68.7	-68.7	-68.7	-68.7	-68.7	-67.7
6	128 QAM		-66.4	-65.4	-65.9	-65.9	-65.9	-65.9	-65.9	-64.9
7	256 QAM		-63.6	-62.6	-63.1	-63.1	-63.1	-63.1	-63.1	-62.1
8	512 QAM		-60.9	-59.9	-60.4	-60.4	-60.4	-60.4	-60.4	-59.4
9	1024 QAM (Strong FEC)		-58.0	-57.0	-57.5	-57.5	-57.5	-57.5	-57.5	-56.5
10	1024 QAM (Light FEC)		-57.3	-56.3	-56.8	-56.8	-56.8	-56.8	-56.8	-55.8
11	2048 QAM		-55.1	-54.1	-54.6	-54.6	-54.6	-54.6	-54.6	-53.6
12	4096 QAM		-51.7	-50.7	-51.2	-51.2	-51.2			

Profile	Modulation	Channel Spacing	23	24[9]	26	28-31	32	36	38	42
0	BPSK	80 MHz	-84.6	-83.6	-84.1	-84.1	-84.1	-84.1	-84.1	-83.1
1	QPSK		-81.8	-80.8	-81.3	-81.3	-81.3	-81.3	-81.3	-80.3
2	8 QAM		-78.3	-77.3	-77.8	-77.8	-77.8	-77.8	-77.8	-76.8
3	16 QAM		-75.3	-74.3	-74.8	-74.8	-74.8	-74.8	-74.8	-73.8
4	32 QAM		-71.7	-70.7	-71.2	-71.2	-71.2	-71.2	-71.2	-70.2
5	64 QAM		-68.6	-67.6	-68.1	-68.1	-68.1	-68.1	-68.1	-67.1
6	128 QAM		-65.5	-64.5	-65.0	-65.0	-65.0	-65.0	-65.0	-64.0
7	256 QAM		-62.7	-61.7	-62.2	-62.2	-62.2	-62.2	-62.2	-61.2
8	512 QAM		-59.8	-58.8	-59.3	-59.3	-59.3	-59.3	-59.3	-58.3
9	1024 QAM (Strong FEC)		-57.0	-56.0	-56.5	-56.5	-56.5	-56.5	-56.5	-55.5
10	1024 QAM (Light FEC)		-55.9	-54.9	-55.4	-55.4	-55.4	-55.4	-55.4	-54.4
11	2048 QAM		-53.4	-52.4	-52.9	-52.9	-52.9	-52.9	-52.9	-51.9
12	4096 QAM		-50.2	-49.2	-49.7	-49.7	-49.7		-	-
0	BPSK	112 MHz	-82.5	-81.5	-82.0	-82.0	-82.0	-82.0	-82.0	-81.0
1	QPSK		-80.1	-79.1	-79.6	-79.6	-79.6	-79.6	-79.6	-78.6
2	8 QAM		-76.1	-75.1	-75.6	-75.6	-75.6	-75.6	-75.6	-74.6
3	16 QAM		-73.2	-72.2	-72.7	-72.7	-72.7	-72.7	-72.7	-71.7
4	32 QAM		-69.8	-68.8	-69.3	-69.3	-69.3	-69.3	-69.3	-68.3
5	64 QAM		-66.8	-65.8	-66.3	-66.3	-66.3	-66.3	-66.3	-65.3
6	128 QAM		-63.9	-62.9	-63.4	-63.4	-63.4	-63.4	-63.4	-62.4
7	256 QAM		-60.9	-59.9	-60.4	-60.4	-60.4	-60.4	-60.4	-59.4
8	512 QAM		-58.5	-57.5	-58.0	-58.0	-58.0	-58.0	-58.0	-57.0
9	1024 QAM (Strong FEC)		-55.5	-54.5	-55.0	-55.0	-55.0	-55.0	-55.0	-54.0
10	1024 QAM (Light FEC)		-54.8	-53.8	-54.3	-54.3	-54.3	-54.3	-54.3	-53.3
11	2048 QAM		-52.2	-51.2	-51.7	-51.7	-51.7	-51.7	-51.7	-50.7
12	4096 QAM		-49.5	-48.5	-49.0	-49.0	-49.0	-	-	-

Profile	Modulation	Channel Spacing	23	24[9]	26	28-31	32	36	38	42
0	BPSK	140 MHz	-82.4	-81.4	-81.9	-81.9	-81.9	-81.9	-81.9	-80.9
1	QPSK		-79.1	-78.1	-78.6	-78.6	-78.6	-78.6	-78.6	-77.6
2	8 QAM		-75.5	-74.5	-75.0	-75.0	-75.0	-75.0	-75.0	-74.0
3	16 QAM		-72.4	-71.4	-71.9	-71.9	-71.9	-71.9	-71.9	-70.9
4	32 QAM		-68.8	-67.8	-68.3	-68.3	-68.3	-68.3	-68.3	-67.3
5	64 QAM		-65.4	-64.4	-64.9	-64.9	-64.9	-64.9	-64.9	-63.9
6	128 QAM		-62.9	-61.9	-62.4	-62.4	-62.4	-62.4	-62.4	-61.4
7	256 QAM		-59.9	-58.9	-59.4	-59.4	-59.4	-59.4	-59.4	-58.4
8	512 QAM		-57.0	-56.0	-56.5	-56.5	-56.5	-56.5	-56.5	-55.5
9	1024 QAM		-53.9	-52.9	-53.4	-53.4	-53.4	-53.4	-53.4	-52.4
10	2048 QAM		-50.8	-49.8	-50.3	-50.3	-50.3	-50.3	-50.3	-49.3
0	BPSK	150 MHz	-83.1	-82.1	-81.1	-81.6	-81.6	-81.6	-81.6	-81.6
1	QPSK		-80.0	-79.0	-78.0	-78.5	-78.5	-78.5	-78.5	-78.5
2	8 QAM		-76.2	-75.2	-74.2	-74.7	-74.7	-74.7	-74.7	-74.7
3	16 QAM		-73.0	-72.0	-71.0	-71.5	-71.5	-71.5	-71.5	-71.5
4	32 QAM		-69.6	-68.6	-67.6	-68.1	-68.1	-68.1	-68.1	-68.1
5	64 QAM		-66.2	-65.2	-64.2	-64.7	-64.7	-64.7	-64.7	-64.7
6	128 QAM		-63.7	-62.7	-61.7	-62.2	-62.2	-62.2	-62.2	-62.2
7	256 QAM		-60.7	-59.7	-58.7	-59.2	-59.2	-59.2	-59.2	-59.2
8	512 QAM		-57.8	-56.8	-55.8	-56.3	-56.3	-56.3	-56.3	-56.3
9	1024 QAM		-54.8	-53.8	-52.8	-53.3	-53.3	-53.3	-53.3	-53.3
10	2048 QAM		-51.5	-50.5	-49.5	-50.0	-50.0	-50.0	-50.0	-50.0

Profile	Modulation	Channel Spacing	23	24[9]	26	28-31	32	36	38	42
0	BPSK	160 MHz	-81.0	-80.0	-80.5	-80.5	-80.5	-80.5	-80.5	-79.5
1	QPSK		-78.8	-77.8	-78.3	-78.3	-78.3	-78.3	-78.3	-77.3
2	8 QAM		-74.3	-73.3	-73.8	-73.8	-73.8	-73.8	-73.8	-72.8
3	16 QAM		-71.9	-70.9	-71.4	-71.4	-71.4	-71.4	-71.4	-70.4
4	32 QAM		-68.5	-67.5	-68.0	-68.0	-68.0	-68.0	-68.0	-67.0
5	64 QAM		-65.2	-64.2	-64.7	-64.7	-64.7	-64.7	-64.7	-63.7
6	128 QAM		-62.4	-61.4	-61.9	-61.9	-61.9	-61.9	-61.9	-60.9
7	256 QAM		-59.3	-58.3	-58.8	-58.8	-58.8	-58.8	-58.8	-57.8
8	512 QAM		-56.6	-55.6	-56.1	-56.1	-56.1	-56.1	-56.1	-55.1
9	1024 QAM		-53.3	-52.3	-52.8	-52.8	-52.8	-52.8	-52.8	-51.8
10	2048 QAM		-49.5	-48.5	-49.0	-49.0	-49.0	-49.0	-49.0	-48.0
0	BPSK	224 MHz[10]	-80.3	-79.3	-79.8	-79.8	-79.8	-79.8	-79.8	-78.8
1	QPSK		-77.2	-76.2	-76.7	-76.7	-76.7	-76.7	-76.7	-75.7
2	8 QAM		-73.4	-72.4	-72.9	-72.9	-72.9	-72.9	-72.9	-71.9
3	16 QAM		-70.4	-69.4	-69.9	-69.9	-69.9	-69.9	-69.9	-68.9
4	32 QAM		-66.8	-65.8	-66.3	-66.3	-66.3	-66.3	-66.3	-65.3
5	64 QAM		-63.5	-62.5	-63.0	-63.0	-63.0	-63.0	-63.0	-62.0
6	128 QAM		-60.9	-59.9	-60.4	-60.4	-60.4	-60.4	-60.4	-59.4
7	256 QAM		-57.9	-56.9	-57.4	-57.4	-57.4	-57.4	-57.4	-56.4
8	512 QAM		-54.5	-53.5	-54.0	-54.0	-54.0	-54.0	-54.0	-53.0
9	1024 QAM		-50.9	-49.9	-50.4	-50.4	-50.4	-50.4	-50.4	-49.4
10	2048 QAM		-47.2	-46.2	-46.7	-46.7	-46.7	-46.7	-46.7	-45.7

8.6.1 Overload Thresholds

The overload threshold for all modulations is -20dBm.

[10] 224 MHz is only supported with certain hardware versions. For details, ask your Ceragon representative.

8.7 Frequency Bands

Table 52: Frequency Bands

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
6L GHz	6332.5-6393	5972-6093	300A
	5972-6093	6332.5-6393	
	6191.5-6306.5	5925.5-6040.5	266A
	5925.5-6040.5	6191.5-6306.5	
	6303.5-6418.5	6037.5-6152.5	
	6037.5-6152.5	6303.5-6418.5	
	6245-6290.5	5939.5-6030.5	260A
	5939.5-6030.5	6245-6290.5	
	6365-6410.5	6059.5-6150.5	
	6059.5-6150.5	6365-6410.5	
	6226.89-6286.865	5914.875-6034.825	252B
	5914.875-6034.825	6226.89-6286.865	
	6345.49-6405.465	6033.475-6153.425	
	6033.475-6153.425	6345.49-6405.465	
	6179.415-6304.015	5927.375-6051.975	252A
	5927.375-6051.975	6179.415-6304.015	
	6238.715-6363.315	5986.675-6111.275	
	5986.675-6111.275	6238.715-6363.315	
	6298.015-6422.615	6045.975-6170.575	
	6045.975-6170.575	6298.015-6422.615	
	6235-6290.5	5939.5-6050.5	240A
	5939.5-6050.5	6235-6290.5	
	6355-6410.5	6059.5-6170.5	
	6059.5-6170.5	6355-6410.5	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
6H GHz	6920-7080	6420-6580	500A
	6420-6580	6924.5-7075.5	
	7032.5-7091.5	6692.5-6751.5	340C
	6692.5-6751.5	7032.5-7091.5	
	6764.5-6915.5	6424.5-6575.5	340B
	6424.5-6575.5	6764.5-6915.5	
	6924.5-7075.5	6584.5-6735.5	
	6584.5-6735.5	6924.5-7075.5	
	6781-6939	6441-6599	340A
	6441-6599	6781-6939	
	6941-7099	6601-6759	
	6601-6759	6941-7099	
	6707.5-6772.5	6537.5-6612.5	160A
	6537.5-6612.5	6707.5-6772.5	
	6767.5-6832.5	6607.5-6672.5	
	6607.5-6672.5	6767.5-6832.5	
	6827.5-6872.5	6667.5-6712.5	
	6667.5-6712.5	6827.5-6872.5	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
7 GHz	7783.5-7898.5	7538.5-7653.5	245A
	7538.5-7653.5	7783.5-7898.5	
	7301.5-7388.5	7105.5-7192.5	196A
	7105.5-7192.5	7301.5-7388.5	
	7357.5-7444.5	7161.5-7248.5	
	7161.5-7248.5	7357.5-7444.5	
	7440.5-7499.5	7622.5-7681.5	182A
	7678.5-7737.5	7496.5-7555.5	
	7496.5-7555.5	7678.5-7737.5	
	7580.5-7639.5	7412.5-7471.5	168C
	7412.5-7471.5	7580.5-7639.5	
	7608.5-7667.5	7440.5-7499.5	
	7440.5-7499.5	7608.5-7667.5	
	7664.5-7723.5	7496.5-7555.5	
	7496.5-7555.5	7664.5-7723.5	
	7609.5-7668.5	7441.5-7500.5	168B
	7441.5-7500.5	7609.5-7668.5	
	7637.5-7696.5	7469.5-7528.5	
	7469.5-7528.5	7637.5-7696.5	
	7693.5-7752.5	7525.5-7584.5	
	7525.5-7584.5	7693.5-7752.5	
	7273.5-7332.5	7105.5-7164.5	168A
	7105.5-7164.5	7273.5-7332.5	
	7301.5-7360.5	7133.5-7192.5	
	7133.5-7192.5	7301.5-7360.5	
	7357.5-7416.5	7189.5-7248.5	
	7189.5-7248.5	7357.5-7416.5	
	7280.5-7339.5	7119.5-7178.5	161P
	7119.5-7178.5	7280.5-7339.5	
	7308.5-7367.5	7147.5-7206.5	
	7147.5-7206.5	7308.5-7367.5	
	7336.5-7395.5	7175.5-7234.5	
	7175.5-7234.5	7336.5-7395.5	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
	7364.5-7423.5	7203.5-7262.5	
	7203.5-7262.5	7364.5-7423.5	
	7597.5-7622.5	7436.5-7461.5	161O
	7436.5-7461.5	7597.5-7622.5	
	7681.5-7706.5	7520.5-7545.5	
	7520.5-7545.5	7681.5-7706.5	
	7587.5-7646.5	7426.5-7485.5	161M
	7426.5-7485.5	7587.5-7646.5	
	7615.5-7674.5	7454.5-7513.5	
	7454.5-7513.5	7615.5-7674.5	
	7643.5-7702.5	7482.5-7541.5	161K
	7482.5-7541.5	7643.5-7702.5	
	7671.5-7730.5	7510.5-7569.5	
	7510.5-7569.5	7671.5-7730.5	
	7580.5-7639.5	7419.5-7478.5	161J
	7419.5-7478.5	7580.5-7639.5	
	7608.5-7667.5	7447.5-7506.5	
	7447.5-7506.5	7608.5-7667.5	
	7664.5-7723.5	7503.5-7562.5	
	7503.5-7562.5	7664.5-7723.5	
	7580.5-7639.5	7419.5-7478.5	161I
	7419.5-7478.5	7580.5-7639.5	
	7608.5-7667.5	7447.5-7506.5	
	7447.5-7506.5	7608.5-7667.5	
	7664.5-7723.5	7503.5-7562.5	
	7503.5-7562.5	7664.5-7723.5	
	7273.5-7353.5	7112.5-7192.5	161F
	7112.5-7192.5	7273.5-7353.5	
	7322.5-7402.5	7161.5-7241.5	
	7161.5-7241.5	7322.5-7402.5	
	7573.5-7653.5	7412.5-7492.5	
	7412.5-7492.5	7573.5-7653.5	
	7622.5-7702.5	7461.5-7541.5	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
	7461.5-7541.5	7622.5-7702.5	
	7709-7768	7548-7607	161D
	7548-7607	7709-7768	
	7737-7796	7576-7635	
	7576-7635	7737-7796	
	7765-7824	7604-7663	
	7604-7663	7765-7824	
	7793-7852	7632-7691	
	7632-7691	7793-7852	
	7584-7643	7423-7482	161C
	7423-7482	7584-7643	
	7612-7671	7451-7510	
	7451-7510	7612-7671	
	7640-7699	7479-7538	
	7479-7538	7640-7699	
	7668-7727	7507-7566	
	7507-7566	7668-7727	
	7409-7468	7248-7307	161B
	7248-7307	7409-7468	
	7437-7496	7276-7335	
	7276-7335	7437-7496	
	7465-7524	7304-7363	
	7304-7363	7465-7524	
	7493-7552	7332-7391	
	7332-7391	7493-7552	
	7284-7343	7123-7182	161A
	7123-7182	7284-7343	
	7312-7371	7151-7210	
	7151-7210	7312-7371	
	7340-7399	7179-7238	
	7179-7238	7340-7399	
	7368-7427	7207-7266	
	7207-7266	7368-7427	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
	7280.5-7339.5	7126.5-7185.5	154C
	7126.5-7185.5	7280.5-7339.5	
	7308.5-7367.5	7154.5-7213.5	
	7154.5-7213.5	7308.5-7367.5	
	7336.5-7395.5	7182.5-7241.5	
	7182.5-7241.5	7336.5-7395.5	
	7364.5-7423.5	7210.5-7269.5	
	7210.5-7269.5	7364.5-7423.5	
	7594.5-7653.5	7440.5-7499.5	154B
	7440.5-7499.5	7594.5-7653.5	
	7622.5-7681.5	7468.5-7527.5	
	7468.5-7527.5	7622.5-7681.5	
	7678.5-7737.5	7524.5-7583.5	
	7524.5-7583.5	7678.5-7737.5	
	7580.5-7639.5	7426.5-7485.5	154A
	7426.5-7485.5	7580.5-7639.5	
	7608.5-7667.5	7454.5-7513.5	
	7454.5-7513.5	7608.5-7667.5	
	7636.5-7695.5	7482.5-7541.5	
	7482.5-7541.5	7636.5-7695.5	
	7664.5-7723.5	7510.5-7569.5	
	7510.5-7569.5	7664.5-7723.5	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
8 GHz	8396.5-8455.5	8277.5-8336.5	119A
	8277.5-8336.5	8396.5-8455.5	
	8438.5 – 8497.5	8319.5 – 8378.5	
	8319.5 – 8378.5	8438.5 – 8497.5	
	8274.5-8305.5	7744.5-7775.5	530A
	7744.5-7775.5	8274.5-8305.5	
	8304.5-8395.5	7804.5-7895.5	500A
	7804.5-7895.5	8304.5-8395.5	
	8023-8186.32	7711.68-7875	311C-J

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
	7711.68-7875	8023-8186.32	
	8028.695-8148.645	7717.375-7837.325	311B
	7717.375-7837.325	8028.695-8148.645	
	8147.295-8267.245	7835.975-7955.925	
	7835.975-7955.925	8147.295-8267.245	
	8043.52-8163.47	7732.2-7852.15	311A
	7732.2-7852.15	8043.52-8163.47	
	8162.12-8282.07	7850.8-7970.75	
	7850.8-7970.75	8162.12-8282.07	
	8212-8302	7902-7992	310D
	7902-7992	8212-8302	
	8240-8330	7930-8020	
	7930-8020	8240-8330	
	8296-8386	7986-8076	
	7986-8076	8296-8386	
	8212-8302	7902-7992	310C
	7902-7992	8212-8302	
	8240-8330	7930-8020	
	7930-8020	8240-8330	
	8296-8386	7986-8076	
	7986-8076	8296-8386	
	8380-8470	8070-8160	
	8070-8160	8380-8470	
	8408-8498	8098-8188	
	8098-8188	8408-8498	
	8039.5-8150.5	7729.5-7840.5	310A
	7729.5-7840.5	8039.5-8150.5	
	8159.5-8270.5	7849.5-7960.5	
	7849.5-7960.5	8159.5-8270.5	
	8024.5-8145.5	7724.5-7845.5	300A
	7724.5-7845.5	8024.5-8145.5	
	8144.5-8265.5	7844.5-7965.5	
	7844.5-7965.5	8144.5-8265.5	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
	8302.5-8389.5	8036.5-8123.5	266C
	8036.5-8123.5	8302.5-8389.5	
	8190.5-8277.5	7924.5-8011.5	266B
	7924.5-8011.5	8190.5-8277.5	
	8176.5-8291.5	7910.5-8025.5	266A
	7910.5-8025.5	8176.5-8291.5	
	8288.5-8403.5	8022.5-8137.5	
	8022.5-8137.5	8288.5-8403.5	
	8226.52-8287.52	7974.5-8035.5	252A
	7974.5-8035.5	8226.52-8287.52	
	8270.5-8349.5	8020.5-8099.5	250A
	8016.5-8156.5	7733-7873	283A
	7733-7873	8016.5-8156.5	
	8128.5-8268.5	7845-7985	
	7845-7985	8128.5-8268.5	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
10 GHz	10501-10563	10333-10395	168A
	10333-10395	10501-10563	
	10529-10591	10361-10423	
	10361-10423	10529-10591	
	10585-10647	10417-10479	
	10417-10479	10585-10647	
	10501-10647	10151-10297	350A
	10151-10297	10501-10647	
	10498-10652	10148-10302	350B
	10148-10302	10498-10652	
	10561-10707	10011-10157	550A
	10011-10157	10561-10707	
	10701-10847	10151-10297	
	10151-10297	10701-10847	
	10590-10622	10499-10531	91A

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
	10499-10531	10590-10622	
	10618-10649	10527-10558	
	10527-10558	10618-10649	
	10646-10677	10555-10586	
	10555-10586	10646-10677	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
11 GHz	11425-11725	10915-11207	All
	10915-11207	11425-11725	
	11185-11485	10695-10955	
	10695-10955	11185-11485	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
13 GHz	13002-13141	12747-12866	266
	12747-12866	13002-13141	
	13127-13246	12858-12990	
	12858-12990	13127-13246	
	12807-12919	13073-13185	266A
	13073-13185	12807-12919	
	12700-12775	12900-13000	200
	12900-13000	12700-12775	
	12750-12825	12950-13050	
	12950-13050	12750-12825	
	12800-12870	13000-13100	
	13000-13100	12800-12870	
	12850-12925	13050-13150	
	13050-13150	12850-12925	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
15 GHz	15110-15348	14620-14858	490
	14620-14858	15110-15348	
	14887-15117	14397-14627	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
	14397-14627	14887-15117	
	15144-15341	14500-14697	644
	14500-14697	15144-15341	
	14975-15135	14500-14660	475
	14500-14660	14975-15135	
	15135-15295	14660-14820	
	14660-14820	15135-15295	
	14921-15145	14501-14725	420
	14501-14725	14921-15145	
	15117-15341	14697-14921	
	14697-14921	15117-15341	
	14963-15075	14648-14760	315
	14648-14760	14963-15075	
	15047-15159	14732-14844	
	14732-14844	15047-15159	
	15229-15375	14500-14647	728
	14500-14647	15229-15375	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
18 GHz	19160-19700	18126-18690	1010
	18126-18690	19160-19700	
	18710-19220	17700-18200	
	17700-18200	18710-19220	
	19260-19700	17700-18140	1560
	17700-18140	19260-19700	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
23 GHz	23000-23600	22000-22600	1008
	22000-22600	23000-23600	
	22400-23020	21200-21800	1232 /1200
	21200-21800	22400-23020	
	23000-23600	21780-22400	
	21780-22400	23000-23600	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
24UL GHz[11]	24000 - 24250	24000 - 24250	All

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
26 GHz	25530-26030	24520-25030	1008
	24520-25030	25530-26030	
	25980-26480	24970-25480	
	24970-25480	25980-26480	
	25266-25350	24466-24550	800
	24466-24550	25266-25350	
	25050-25250	24250-24450	
	24250-24450	25050-25250	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
28 GHz	28150-28350	27700-27900	450
	27700-27900	28150-28350	
	27950-28150	27500-27700	
	27500-27700	27950-28150	
	28050-28200	27700-27850	350
	27700-27850	28050-28200	
	27960-28110	27610-27760	
	27610-27760	27960-28110	
	28090-28315	27600-27825	490
	27600-27825	28090-28315	
	29004-29453	27996-28445	1008
	27996-28445	29004-29453	
	28556-29005	27548-27997	
	27548-27997	28556-29005	
	29100-29125	29225-29250	125
	29225-29250	29100-29125	

[11] Customers in countries following EC Directive 2006/771/EC (incl. amendments) must observe the 100mW EIRP obligation by adjusting transmit power according to antenna gain and RF line losses.

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
31 GHz	31000-31085	31215-31300	175
	31215-31300	31000-31085	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
32 GHz	31815-32207	32627-33019	812
	32627-33019	31815-32207	
	32179-32571	32991-33383	
	32991-33383	32179-32571	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
38 GHz	38820-39440	37560-38180	1260
	37560-38180	38820-39440	
	38316-38936	37045-37676	
	37045-37676	38316-38936	
	39650-40000	38950-39300	700
	38950-39300	39500-40000	
	39300-39650	38600-38950	
	38600-38950	39300-39650	
	37700-38050	37000-37350	
	37000-37350	37700-38050	
	38050-38400	37350-37700	
	37350-37700	38050-38400	

Frequency Band	TX Range	RX Range	Tx/Rx Spacing
42 GHz	40550-41278	42050-42778	1500
	42050-42778	40550-41278	
	41222-41950.5	42722-43450	
	42722-43450	41222-41950.5	

8.8 Ethernet Latency Specifications

The specifications in this section are for 1+0 configurations.

8.8.1 Ethernet Latency – 14 MHz Channel Bandwidth

Table 53: Ethernet Latency with 14 MHz Channel Bandwidth (Script 4509)

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
1	QPSK		1013	1013	1014	1265	1516	1768
2	8 QAM		675	675	679	834	992	1150
3	16 QAM		490	490	492	603	714	826
4	32 QAM		393	393	395	477	561	644
5	64 QAM		335	335	338	403	471	538
6	128 QAM		292	293	295	349	404	460
7	256 QAM		260	260	262	309	358	407
8	512 QAM		265	265	267	309	353	397
9	1024 QAM (Strong FEC)		247	247	249	289	331	372
10	1024 QAM (Light FEC)		242	243	245	283	322	361
11	2048 QAM		235	235	237	274	311	349

8.8.2 Ethernet Latency – 20 MHz Channel Bandwidth

Table 54: Ethernet Latency – 20 MHz Channel Bandwidth (Script 4521)

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		1483	1484	1488	1880	2275	2671
1	QPSK		686	687	691	859	1031	1203
2	8 QAM		472	472	474	585	697	808
3	16 QAM		347	348	351	431	512	594
4	32 QAM		281	282	285	345	408	470
5	64 QAM		241	242	245	294	346	397
6	128 QAM		212	212	215	256	300	343
7	256 QAM		190	191	193	230	269	307
8	512 QAM		196	197	199	233	269	305
9	1024 QAM (Strong FEC)		182	183	185	218	252	285
10	1024 QAM (Light FEC)		178	179	181	212	244	276
11	2048 QAM		169	170	172	201	232	262

8.8.3 Ethernet Latency – 25 MHz Channel Bandwidth

Table 55: Ethernet Latency – 25 MHz Channel Bandwidth (Script 4525)

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		1128	1128	1136	1420	1713	2005
1	QPSK		530	530	532	659	787	916
2	8 QAM		368	368	371	452	536	620
3	16 QAM		273	273	276	334	396	457
4	32 QAM		221	221	223	268	314	360
5	64 QAM		190	190	192	228	266	303
6	128 QAM		167	167	169	199	230	261
7	256 QAM		149	150	151	177	205	233
8	512 QAM		152	153	154	178	203	228
9	1024 QAM (Strong FEC)		142	142	144	166	190	213
10	1024 QAM (Light FEC)		139	140	141	162	185	207
11	2048 QAM		132	132	133	153	174	195
12	4096 QAM		129	129	131	149	168	188

8.8.4 Ethernet Latency – 28/30 MHz Channel Bandwidth

Table 56: Ethernet Latency – 28 MHz Channel Bandwidth (Script 4504)

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		965	966	967	1213	1461	1708
1	QPSK		463	463	465	575	687	799
2	8 QAM		323	323	325	397	470	544
3	16 QAM		240	240	242	294	347	401
4	32 QAM		195	195	197	236	277	317
5	64 QAM		167	168	170	201	234	267
6	128 QAM		148	148	150	176	204	231
7	256 QAM		132	133	134	157	182	206
8	512 QAM		135	136	137	158	180	202
9	1024 QAM (Strong FEC)		126	126	128	148	169	189
10	1024 QAM (Light FEC)		124	124	125	144	164	184
11	2048 QAM		117	117	119	136	155	173
12	4096 QAM		114	115	116	132	150	167

Table 57: Ethernet Latency – 28 MHz Channel Bandwidth (Script 4514)

Note: This script is planned for future release.

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		1019	1019	1022	1279	1539	1799
1	QPSK		488	488	490	604	721	836
2	8 QAM		344	344	347	421	498	574
3	16 QAM		258	259	261	314	370	422
4	32 QAM		212	212	214	255	297	339
5	64 QAM		183	184	185	218	253	285
6	128 QAM		162	163	164	192	221	249
7	256 QAM		147	147	149	173	199	224
8	512 QAM		150	151	152	174	197	220
9	1024 QAM (Strong FEC)		141	141	142	163	185	207
10	1024 QAM (Light FEC)		138	138	139	159	180	200
11	2048 QAM		131	132	133	151	171	190
12	4096 QAM		124	125	126	143	162	180

Table 58: Ethernet Latency – 28/30 MHz Channel Bandwidth (Script 4505)

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		909	910	914	1143	1377	1610
1	QPSK		437	438	439	543	649	754
2	8 QAM		306	306	308	378	449	520
3	16 QAM		226	227	229	277	328	378
4	32 QAM		185	185	187	224	263	301
5	64 QAM		158	159	160	190	222	253
6	128 QAM		140	140	142	167	193	219
7	256 QAM		130	130	132	153	176	199
8	512 QAM		129	130	131	151	173	194
9	1024 QAM (Strong FEC)		120	120	121	140	160	180
10	1024 QAM (Light FEC)		117	118	119	137	156	174
11	2048 QAM		109	110	111	127	145	162
12	4096 QAM		109	109	110	126	142	158

8.8.5 Ethernet Latency – 40 MHz Channel Bandwidth

Table 59: Ethernet Latency– 40 MHz Channel Bandwidth (Script 4507)

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		649	649	653	813	977	1138
1	QPSK		322	323	325	400	477	553
2	8 QAM		228	229	231	280	331	382
3	16 QAM		171	171	173	209	247	284
4	32 QAM		140	140	142	169	198	227
5	64 QAM		121	121	123	145	169	192
6	128 QAM		107	107	109	127	147	166
7	256 QAM		96	96	98	115	134	152
8	512 QAM		98	98	100	115	132	149
9	1024 QAM (Strong FEC)		92	92	94	108	123	138
10	1024 QAM (Light FEC)		90	91	92	105	119	133
11	2048 QAM		85	85	87	99	112	125
12	4096 QAM		80	81	82	94	106	119

8.8.6 Ethernet Latency – 50 MHz Channel Bandwidth

Table 60: Ethernet Latency– 50 MHz Channel Bandwidth (Script 4510)

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		504	505	506	632	758	884
1	QPSK		264	264	266	327	390	452
2	8 QAM		181	181	183	222	262	302
3	16 QAM		137	137	139	167	197	227
4	32 QAM		113	114	115	138	162	186
5	64 QAM		97	98	99	117	136	154
6	128 QAM		86	86	88	103	119	135
7	256 QAM		77	78	79	92	106	120
8	512 QAM		79	80	81	93	106	119
9	1024 QAM (Strong FEC)		74	74	76	87	99	111
10	1024 QAM (Light FEC)		72	73	74	84	96	107
11	2048 QAM		69	69	70	80	91	101
12	4096 QAM		66	66	68	77	87	97

8.8.7 Ethernet Latency – 56/60 MHz Channel Bandwidth

Table 61: Ethernet Latency – 56 MHz Channel Bandwidth (Script 4502)

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		447	447	449	559	670	780
1	QPSK		226	226	228	280	333	386
2	8 QAM		161	161	163	198	234	269
3	16 QAM		122	123	124	150	176	202
4	32 QAM		101	101	103	122	143	163
5	64 QAM		88	88	89	105	122	139
6	128 QAM		78	78	79	93	107	121
7	256 QAM		70	70	72	83	96	108
8	512 QAM		72	72	73	84	96	107
9	1024 QAM (Strong FEC)		67	67	69	79	90	100
10	1024 QAM (Light FEC)		66	66	67	77	87	97
11	2048 QAM		63	63	64	73	83	93
12	4096 QAM		60	60	62	70	80	89

Table 62: Ethernet Latency – 56/60 MHz Channel Bandwidth (Script 4506)

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		426	426	427	531	636	740
1	QPSK		216	217	219	267	318	369
2	8 QAM		169	170	172	205	240	274
3	16 QAM		117	117	119	143	168	193
4	32 QAM		97	97	99	117	137	156
5	64 QAM		84	84	86	101	117	133
6	128 QAM		75	75	76	89	103	116
7	256 QAM		70	70	71	82	94	106
8	512 QAM		69	69	71	81	92	103
9	1024 QAM (Strong FEC)		65	65	66	76	86	96
10	1024 QAM (Light FEC)		63	64	65	74	84	93
11	2048 QAM		60	60	61	70	79	88
12	4096 QAM		58	58	59	67	76	85

8.8.8 Ethernet Latency – 70 MHz Channel Bandwidth

Table 63: Ethernet Latency – 70 MHz Channel Bandwidth (Script 4513)

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		369	369	372	463	557	649
1	QPSK		191	192	194	240	288	336
2	8 QAM		139	140	142	176	211	246
3	16 QAM		106	106	108	133	159	185
4	32 QAM		88	89	91	110	131	152
5	64 QAM		77	78	80	97	115	133
6	128 QAM		70	71	73	88	104	120
7	256 QAM		70	70	72	86	101	115
8	512 QAM		64	65	67	80	93	107
9	1024 QAM (Strong FEC)		60	61	63	75	88	101
10	1024 QAM (Light FEC)		59	60	62	73	86	98
11	2048 QAM		57	57	59	70	82	94
12	4096 QAM		54	55	57	68	80	91

8.8.9 Ethernet Latency – 80 MHz Channel Bandwidth

Table 64: Ethernet Latency – 80 MHz Channel Bandwidth (Script 4501)

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		316	316	318	394	471	548
1	QPSK		162	163	165	201	239	276
2	8 QAM		119	119	121	147	174	200
3	16 QAM		91	91	93	111	130	150
4	32 QAM		75	75	77	91	106	121
5	64 QAM		66	66	68	79	92	104
6	128 QAM		59	60	61	71	81	92
7	256 QAM		59	59	61	69	79	88
8	512 QAM		54	55	56	64	73	81
9	1024 QAM (Strong FEC)		51	52	53	60	69	77
10	1024 QAM (Light FEC)		50	51	52	59	67	74
11	2048 QAM		48	48	50	56	64	71
12	4096 QAM		46	47	48	54	62	68

Table 65: Ethernet Latency – 80 MHz Channel Bandwidth (Script 4588)

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		294	295	297	367	439	511
1	QPSK		152	152	154	188	224	259
2	8 QAM		111	111	113	137	162	187
3	16 QAM		85	86	87	104	123	141
4	32 QAM		71	71	73	86	100	114
5	64 QAM		62	63	64	75	86	98
6	128 QAM		56	56	58	67	77	87
7	256 QAM		56	56	57	65	74	83
8	512 QAM		51	52	53	60	68	76
9	1024 QAM (Strong FEC)		49	49	50	57	65	72
10	1024 QAM (Light FEC)		48	48	49	56	63	70
11	2048 QAM		45	46	47	53	60	67
12	4096 QAM		44	44	46	51	58	65

8.8.10 Ethernet Latency – 112 MHz Channel Bandwidth

Table 66: Ethernet Latency – 112 MHz Channel Bandwidth (Script 4511)

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		220	221	223	274	328	381
1	QPSK		115	116	117	143	170	196
2	8 QAM		84	84	86	103	122	140
3	16 QAM		65	65	67	79	93	107
4	32 QAM		55	55	56	66	77	88
5	64 QAM		48	48	50	58	67	76
6	128 QAM		43	43	45	52	59	67
7	256 QAM		39	40	41	47	54	61
8	512 QAM		40	41	42	47	54	60
9	1024 QAM (Strong FEC)		38	38	40	45	51	57
10	1024 QAM (Light FEC)		37	38	39	44	50	55
11	2048 QAM		36	36	37	42	48	53
12	4096 QAM		34	35	36	41	46	51

8.8.11 Ethernet Latency – 140 MHz Channel Bandwidth

Table 67: Ethernet Latency – 140 MHz Channel Bandwidth (Script 4518)

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		177	177	179	220	262	304
1	QPSK		94	94	95	116	137	158
2	8 QAM		69	69	71	85	99	114
3	16 QAM		53	54	55	65	77	88
4	32 QAM		45	46	47	55	64	72
5	64 QAM		40	40	41	48	55	62
6	128 QAM		36	37	38	43	50	56
7	256 QAM		33	33	35	40	45	51
8	512 QAM		34	35	36	40	46	51
9	1024 QAM		32	33	34	38	43	47
10	2048 QAM		31	31	32	36	40	45

8.8.12 Ethernet Latency – 150 MHz Channel Bandwidth

Table 68: Ethernet Latency – 150 MHz Channel Bandwidth (Script 4515)

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		166	167	168	207	246	286
1	QPSK		89	89	91	110	130	150
2	8 QAM		66	66	67	80	94	108
3	16 QAM		51	52	53	62	73	84
4	32 QAM		43	44	45	52	61	69
5	64 QAM		38	39	40	46	53	60
6	128 QAM		35	35	36	42	48	54
7	256 QAM		32	32	34	38	44	49
8	512 QAM		33	34	35	39	44	49
9	1024 QAM		31	32	33	37	41	46
10	2048 QAM		30	30	31	35	39	43

8.8.13 Ethernet Latency – 160 MHz Channel Bandwidth

Table 69: Ethernet Latency – 160 MHz Channel Bandwidth (Script 4516)

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		159	159	161	198	236	273
1	QPSK		85	85	87	105	124	143
2	8 QAM		63	63	65	77	90	103
3	16 QAM		49	50	51	60	70	80
4	32 QAM		42	42	43	50	59	66
5	64 QAM		37	37	38	44	51	57
6	128 QAM		34	34	35	40	46	52
7	256 QAM		31	31	32	37	42	47
8	512 QAM		32	32	34	38	42	47
9	1024 QAM		30	31	32	35	40	44
10	2048 QAM		29	29	30	33	38	42

8.8.14 Ethernet Latency – 224 MHz Channel Bandwidth

Table 70: Ethernet Latency – 224 MHz Channel Bandwidth (Script 4524)

ACM Working Point	Modulation	Latency (µsec) with GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		113	113	115	140	167	193
1	QPSK		62	62	64	76	90	104
2	8 QAM		46	47	48	57	67	76
3	16 QAM		37	37	39	45	53	60
4	32 QAM		32	32	34	39	45	51
5	64 QAM		29	29	30	34	40	44
6	128 QAM		26	27	28	32	36	41
7	256 QAM		24	25	26	29	34	37
8	512 QAM		25	26	27	30	34	37
9	1024 QAM		24	24	26	28	32	35
10	2048 QAM		23	24	25	27	31	34

8.9 Mediation Device Losses

Table 71: Mediation Device Losses

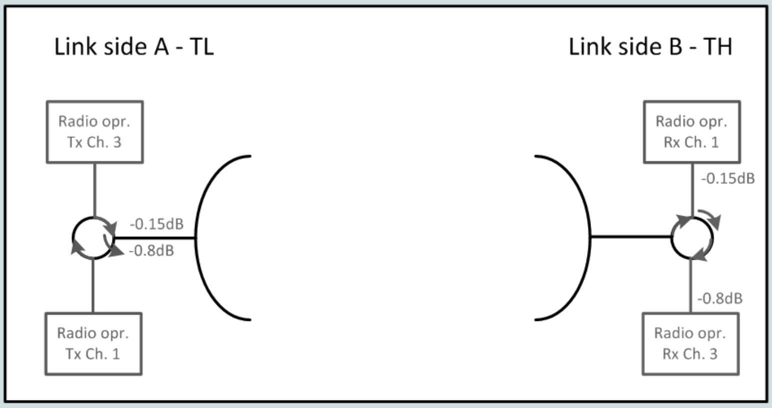
Mediation Devices	Signal Path / Remarks	Maximum Insertion Loss [dB]						
		5.7-8 GHz	11 GHz	13-15 GHz	f18 GHz	23-26 GHz	28-38 GHz	42 GHz
Flex WG	Size varies per frequency.	0.5	0.5	1.2	1.2	1.5	1.8	2.5
OMT	Radio to antenna ports (V or H)	0.3	0.3	0.3	0.3	0.5	0.5	0.5
Splitter	Radio to antenna port	3.6	3.7	3.7	3.7	3.7	4.0	4.0
Dual Coupler	Main Paths	1.6	1.6	1.6	1.8	1.8	2.0	2.0
	Secondary Paths	6±0.7	6±0.7	6±0.7	6±0.8	6±0.8	6±1.0	6±1.0
Dual Splitter	Radio to antenna port	3.6	3.7	3.7	3.7	3.7	4.0	4.0
Dual Circulator	Radio adjacent to antenna port	0.2	0.2	0.2	0.5	0.5	0.5	0.5
	Radio farthest from antenna port	1.4	1.4	1.4	1.4	1.4	1.4	1.4

Notes: The antenna interface is always the IP-50CX interface.

If other antennas are to be used, an adaptor with a 0.1 dB loss should be considered.

The numbers above represent the maximum loss per component.

The following diagram explains the circulators insertion loss:



8.10 Interface Specifications

8.10.1 Ethernet Interface Specifications

Supported Ethernet Interfaces for Traffic	1x 100BASE-T, 1000BASE-T 1x1000BASE-X, 10GBASE-X, 25GBASE-X (optical) OR 1x1000BASE-T 1x1000BASE-X or 10GBASE-X OR 1x1000BASE-T
Supported Ethernet Interfaces for Management	100Base-T (RJ-45)

Table 72: Approved SFP Transceivers

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 **Note:** Not all SFPs with this marketing model are approved for use with IP-50CX. See *Table 73* for a list of approved electrical SFP transceivers per manufacturer and manufacturer part number.

Table 73: Approved Electrical SFP Transceivers per Manufacturer

Ceragon Part Number	Manufacturer	Manufacturer Part Number
AO-0228-0	Linktel Technologies Co LTD	LX1801INX-CER
AO-0228-0	Finisar Corporation	FCLF8521P2BTL-RG

Table 74: Approved 2.5 GbE SFP Transceivers

Marketing Model	Marketing Description	Item Description
SFP-3.7G-SX-EXT-TEMP	SFP-3.7G-SX-EXT-TEMP	XCVR,SFP,850nm,MM,3.7 Gbit/s, INDUSTRIAL GRADE
SFP-3.7G-LX-EXT-TEMP	SFP-3.7G-LX-EXT-TEMP	XCVR,SFP,1310nm,SM,10km,3.7 Gbit/s, INDUSTRIAL GRADE

Table 75: Approved 10 GbE SFP+ Transceivers

Note: Approved SFP+ modules can also be used with 2.5 GbE interfaces.

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 76: Approved SFP28 Transceivers

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,

8.11 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 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
Network resiliency	MSTP ERP (G.8032)
OAM	CFM (802.1ag)
Performance Monitoring	Per port Ethernet counters (RMON/RMON2) Radio ACM statistics
Supported Ethernet/IP Standards	10/100/1000base-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

8.12 Synchronization Protocols

- Enhanced Ethernet Equipment Clock (eEEC) Specification (G.8262.1)
- PTP Telecom Boundary Clock (T-BC) and Time Slave Clock (T-TSC) Specification (G.8273.2)
- PTP Telecom 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)

8.13 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-50CX[12], and NMS
Performance Monitoring	Integral with onboard memory per ITU-T G.826/G.828

12 The voltage at the RSL port is 1.XX where XX is the RSL level. For example: 1.59V 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).

8.14 Mechanical Specifications

Table 77: Mechanical Specifications

Module Dimensions	270mm(H), 230mm(W), 98mm(D)
Module Weight	5.3 kg
Pole Diameter Range (for Remote Mount Installation)	8.89 cm – 11.43 cm

8.15 Standards Compliance

Specification	Standard	
Radio Spectral Efficiency	ETSI: EN 302 217-2 FCC Part 101	*For the applicable frequency bands.
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)	
Surge Protection	Surge: EN61000-4-5, Class 4 (for PWR and ETH1/PoE ports)	
Safety	EN 62368-1 (Europe) IEC 62368-1 (International) UL 62368-1 (US) CSA-C22.2 No.62368-1 (Canada)	

8.16 Environmental Specifications

- Operating: ETSI EN 300 019-1-4 Class 4.1
  - Temperature range: **-33°C to +55°C/-27°F to +131°F**
    - Low temperature (-33°C/-27°F) according to EN 300 019-1-4 (Class 4.1)
    - High temperature (+55°C/+131°F) according to EN 300 019-1-4 (Class 4.2H)
  - Humidity**: 5%RH to 100%RH**
    IEC529 IP67
- Storage: ETSI EN 300 019-1-1 Class 1.2
- Transportation: ETSI EN 300 019-1-2 Class 2

IP-50CX 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-50CX complies with the 1972 Noise Control Act.

IP-50CX does not include any noise generating components.

8.17 Antenna Specifications

- Direct Mount:

CommScope (VHLP), RFS, Xian Putian (WTG), and Radio Wave

- Remote Mount:

Table 78: Antenna Specifications, Remote Mount

Frequency (GHz)	Waveguide Standard	Waveguide Flange	Antenna Flange
6	WR137	PDR70	UDR70
7/8	WR112	PBR84	UBR84
10/11	WR90	PBR100	UBR100
13	WR75	PBR120	UBR120
15	WR62	PBR140	UBR140
18-26	WR42	PBR220	UBR220
28-38	WR28	PBR320	UBR320
42	WR22	UG383/U	UG383/U

If a different antenna type (CPR flange) is used, a flange adaptor is required. Please contact your Ceragon representative for details.

8.18 Power Input Specifications

Standard Input	-48 VDC
DC Input range	-40.5 to -60 VDC

8.19 Typical Power Consumption

Typical Power Consumption	**6-11 GHz**	**13-18 GHz**
2+0 Operation	85W	66W
1+0 Operation (one of the carriers is muted)	66W	58W
Both carriers muted	41W	43W

8.20 Power Connection Options

Table 79: Power Connection Options

Interface	Cable Type	Maximum Length	
		11 GHz	15 GHz
DC Power	DC (18 AWG)	50m	70m
	DC (14 AWG)	130m	180m
	DC (12 AWG)	200m	280m
	DC (10 AWG)	300m	n/a
P2 (RJ-45) with PoE_Inj_AO_2DC_24V_48V	CAT5e and above	100m	

Note: For details and marketing models of the recommended PoE options and when they are used, see *PoE Injector* on page 24.

8.21 PoE Injector Specifications

The specifications in this section are for the standard PoE Injector unit with the following marketing model:

- PoE_Inj_AO_2DC_24V_48V

8.21.1 Power Input

Standard Input	-48 VDC
DC Input range	-(18/40.5 to 60) VDC

8.21.2 Environmental

- Operating: ETSI EN 300 019-1-4 Class 4.1
  - Temperature range for continuous operating temperature with high reliability: -33°C to +55°C/-27°F to +131°F
  - Humidity: 5%RH to 100%RH (IEC529 IP66)
- Storage: ETSI EN 300 019-1-1 Class 1.2
- Transportation: ETSI EN 300 019-1-2 Class 2.3

8.21.3 Standards Requirements

Specification	Standard
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 IEC 62368-1 UL 62368-1 CSA-C22.2 No.62368-1

8.21.4 Mechanical

Module Dimensions	(H)134mm x (W)190mm x (D)62mm (H)5.28inch x (W) 7.48inch(D)2.44inch
Module Weight	1kg/2.2lbs

8.22 Cable Specifications

8.22.1 Outdoor Ethernet Cable Specifications

Electrical Requirements

Cable type	**CAT-5e SFUTP**, 4 pairs, according to ANSI/TIA/EIA-568-B-2
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

8.22.2 Outdoor DC Cable Specifications

Electrical Requirements

Cable type	2 tinned copper wires
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

8.23 Mean Time Between Failures (MTBF)

MTBF for IP-50CX is 126 years.

9. Appendix A – Marketing Models

For frequencies of 6 to 11 GHz, IP-50CX uses the Easy Set technology in which two individual units are ordered: a generic radio unit and a diplexer unit.

For frequencies of 13 to 42 GHz, a single IP-50CX unit is ordered, consisting of both the radio and the diplexers.

This section explains how to read IP-50CX marketing models, including marketing models for the diplexer unit for 6-11 GHz links. Constructing a marketing model for the purpose of ordering equipment should always be done using a configurator.

Note:	Not all fields are always necessary to define a valid marketing model. If a specific field is not applicable, it should be omitted.

9.1 Marketing Models for Easy Set IP-50CX Radio and Diplexer Units, 6 to 11 GHz

For frequencies of 6 to 11 GHz, the IP-50CX radio unit and diplexer unit are ordered separately. Using Easy Set technology, the diplexer unit is assembled on the IP-50CX radio unit during link installation in the field. The radio unit is generic; only the diplexer unit (DXU) is sub-band specific, which facilities link planning, ordering, and maintenance as described above.

Table 80 provides the marketing model syntax for the IP-50CX Easy Set radio unit.

Table 81 provides the marketing model syntax for the IP-50CX Easy Set diplexer unit.

Table 80: IP-50CX Marketing Model Syntax, 6 to 11 GHz (Radio Unit)

Marketing Model	Description
IP-50CX-*ff*	IP-50CX, Multicore *ff* GHz, All-Outdoor, Basic Radio

Table 81: IP-50CX Marketing Model Syntax, 6 to 11 GHz (Diplexer Unit)

Marketing Model	Description
DXCX*ff*-xxxY-ccWdd-t	Diplexers Unit, *ff* GHz, Block *xxxY*, *ccWdd,* High/Low

Table 82: IP-50CX Marketing Model Structure– Possible Values (Easy Set - Radio Unit Only)

Placeholder in Marketing Model	Description	Possible Values
ff	Frequency band	06,07,08,10,11

Table 83: IP-50CX Marketing Model Structure– Possible Values (Easy Set - Diplexer Unit Only)

Placeholder in Marketing Model	Description	Possible Values
ff	Frequency band	L6,U6,07,08,10,11
xxxY	TX-RX separation and block indication (Ceragon internal)	*xxx* - TRS 3 figures in [MHz]. *Y* - Letter to indicate frequency block. Example: 266A The frequency block is a Ceragon internal parameter which defines different channelization using the same TRS and frequency band.
ccWdd	Channel indication or LOW/HIGH or blank	{Start ch}W{End ch} Example: 10W15
t	TX low / TX high indication	L – TX Low H – TX high

Table 84 provides examples of specific IP-50CX diplexer unit marketing models based on the syntax described above.

Table 84: IP-50CX Diplexer Unit Marketing Model Examples

Marketing Model Example	Explanation
DXCXL6-252A-01W04-L	IP-50CX Diplexer Unit, Lower 6 GHz, TRS block 252A, Ch 1 to 4, Tx low
DXCX11-500-07W13-H	IP-50CX Diplexer Unit, 11 GHz, TRS block 500, Ch 7 to 13, Tx high

9.2 Marketing Model for IP-50CX Unit, 13-42 GHz

When ordering an IP-50CX, a single unit is ordered as a single unit. The following IP-50CX hardware models are available.

Table 85: IP-50CX Marketing Models

Marketing Model	TX Range	RX Range
IP-50CX-E-13-266-1W4-H	13002-13141	12745.75-12866
IP-50CX-E-13-266-1W4-L	12745.75-12866	13002-13141
IP-50CX-E-15-420-1W8-H	14921-15145	14501-14725
IP-50CX-E-15-420-1W8-L	14501-14725	14921-15145
IP-50CX-E-18-H-H	19160-19700	18126-18690
IP-50CX-E-18-H-L	18126-18690	19160-19700
IP-50CX-E-23-H	23000-23600	22000-22600
IP-50CX-E-23-L	22000-22600	23000-23600