CERAGON

Datasheet

IP-50E

January 2020 | Rev. C

Note:	For feature availability, check the Release Notes for the CeraOS version you are using.

Radio

[1]

Supported Frequency Range

71-76 GHz, 81-86 GHz

Radio Configurations

1+0, 2+0 (XPIC)

Radio Features

- ATPC*
- High spectral utilization: BPSK to 512 QAM w/ACMB
- Built-in frequency scanner to determine the current interference level for each channel
- Adaptive Bandwidth Notification (EOAM)*
- XPIC
- Multiband (with IP-20C, IP-20C-HP, IP-20S, IP-20N, IP-20A, or third-party radio carrier)

Ethernet

Ethernet Interfaces

Port 1:

- DC port

Port 2:

- RJ-45 1GE/Management/PoE Port (no traffic)

Port 3:

- SFP – 1/2.5GE Multiband port

Port 4:

- QSFP – 4 x 1/10GE, 1 x 1/10GE, or 1x40GE traffic interface (QSFP+)
- Option for SFP+ (1x10GE) with adaptor

Port 5:

- SFP –1 GE and 10 GE traffic interface (SFP+)

Notes:	For information on which interfaces are supported, refer to the Release Notes for the CeraOS release you are using. SFP+ and QSFP+ devices must be of industrial grade (-40°C to +85°C, -40°F to +185°F)

Ethernet Features

MTU – 9612 Bytes

Quality of Service

- Multiple Classification criteria (VLAN ID, P-bits, IPv4 DSCP, IPv6 TC, MPLS EXP)
- 8 CoS queues per port
- Deep buffering (configurable up to 64 Mbit per queue)
- WRED
- P-bit marking/remarking

4K VLANs

VLAN add/remove

Y.1731 Ethernet OAM

Y.1731 Ethernet Bandwidth Notification (ETH-BN)

Management Protocols

SNMP

REST

SDN Support:

- NETCONF/YANG

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)

Precision Time Protocol (version 2, IEEE1588-2008)

Standards

MEF

Carrier Ethernet 2.0 (CE 2.0)

Supported Ethernet 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

* Planned for future release.

Security

Radio Encryption – AES 256*

Secured protocols:

- HTTPS
- SNMPv3
- SSH
- SFTP

RADIUS authentication and authorization

TACACS+ authentication and authorization (session-based)

Standards Compliance

Radio Spectral Efficiency: EN 302 217-2
Certification ordinance Article 2-1-31-5, Land Mobile Station in the 80GHz band (Japan)

EMC: EN 301 489-1, EN 301 489-4, Class A (Europe)
FCC 47 CFR, part 15, subpart B, class A (US)
ICES-003, Class A (Canada)
TEC/SD/DD/EMC-221/05
TEC/SD/DD/EMC-221/05/OCT-16, Class A (India)
IEC 61000-4-29

Surge: EN61000-4-5, Class 4 (for PWR and ETH1/PoE ports)

Safety: EN 60950-1, EN 62368-1, IEC 60950-1,IEC 62368-1, UL 60950-1, UL 62368-1, CAN/CSA C22.2 NO 60950-1, CAN/CSA C22.2 NO 62368-1, EN 60950-22, IEC 60950-22, UL 60950-22, CAN/CSA C22.2 NO 60950-22

Storage: ETSI EN 300 019-1-1 Class 1.2

Transportation: ETSI EN 300 019-1-2 Class 2.3

Power Consumption Specifications

Active – 58W; Standby – 47W

Product Images

IP-50E

Technical Specifications

Mechanical Specifications

Dimensions (Direct Mount HW) –

322mm(H), 227/270mm(W), 86mm(D), 5.5kg
12.67”(H), 8.93”/10.62”(W), 3.38”(D), 12.12 lbs.

Dimensions (43dBi Integrated Antenna) -
341mm(H), 270/276mm(W), 103mm(D), 7kg
13.42”(H), 10.62/10.86”(W), 4.05”(D), 15.43 lbs.

Pole Diameter Range (for Remote Mount Installation)
8.89cm – 11.43cm; 3.5” – 4.5”

Environmental Specifications

-33°C to +55°C (-45°C to +60°C extended)
-27°F to +131°F (-49°F to +140°F extended)

Power Input Specifications

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

Power Redundancy option by using both a DC power input and a passive PoE injector simultaneously.

Radio Specifications

Note that the modulation per profile differs per channel bandwidth. For 25-2000 MHz channels, IP-50E implements ACMB with eleven available working points, as shown in the following table:

Profile and Modulation	62.5 MHz
Profile 0	BPSK – ¼ channel spacing
Profile 1	BPSK – ½ channel spacing
Profile 2	BPSK – full channel spacing
Profile 3	QPSK
Profile 4	8 PSK
Profile 5	16 QAM
Profile 6	32 QAM
Profile 7	64 QAM
Profile 8	128 QAM
Profile 9	256 QAM
Profile 10	512 QAM

For 62.5 channels, Profile 0 is BPSK with the normal (62.5 MHz) channel spacing, Profile 1 is QPSK, and so on.
For 125 MHz channels, Profile 0 is BPSK with ½ channel spacing. Profile 1 BPSK is BPSK with the normal channel spacing, Profile 2 is QPSK, and so on.

Ethernet Capacity [Mbps]

Profile	62.5	125	250	500	1000	2000
0	37-48	39-51	46-60	95-123	185-239	323-419
1	77-99	81-104	92-120	192-248	370-480	663-859
2	116-150	163-211	186-241	384-498	761-985	1326-1717
3	155-201	246-318	373-484	791-1024	1524-1974	2652-3436
4	195-252	328-425	576-747	1188-1539	2287-2962	4128-5347
5	234-303	421-546	768-995	1585-2053	3050-3951	5505-7131
6	273-354	505-654	960-1244	1982-2567	3813-4939	6869-8897
7	313-405	590-764	1154-1494	2377-3080	4575-5927	8243-9439
8	–	674-873	1346-1743	2774-3594	5339-6916	9439-9941
9	–	759-983	1538-1993	3171-4108	6101-7904	–
10	–	–	1731-2242	3568-4622	–	–

Transmit Power [dBm]

Note: The accuracy of these values is up to +/-2dB.

Channel Spacing (MHz)	62.5	125	250	500	1000	2000
BPSK	18	18	18	18	18	18
4 QAM	18	18	18	18	18	18
8 QAM	17	17	17	17	17	16
16 QAM	17	17	17	17	17	16
32 QAM	17	17	17	17	17	16
64 QAM	16	16	16	16	16	15
128 QAM	16	16	16	16	16	15
256 QAM	15	15	15	15	15	–
512 QAM	–	14	14	14	–	–

Receive Level Threshold [dBm@10E-6]

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

Channel Spacing (MHz)	62.5	125	250	500	1000	2000
BPSK	-80.0	-78.8	-75.8	-72.8	-69.8	-67.4
4 QAM	-78.0	-76.7	-73.7	-70.5	-67.6	-64.9
8 QAM	-73.2	-72.1	-69.1	-65.8	-62.8	-59.9
16 QAM	-71.3	-70.3	-67.3	-64.3	-61.2	-58.6
32 QAM	-70.0	-67.8	-64.8	-60.7	-58.6	-55.5
64 QAM	-68.3	-65.5	-61.9	-57.6	-55.7	-52.4
128 QAM	-64.1	-63.0	-58.9	-54.7	-52.6	-48.0
256 QAM	-61.0	-59.5	-56.0	-50.4	-49.8	–
512 QAM	–	-55.4	-52.4	-49.4	–	–

Technical Description

IP-50E

March 2020 | Rev A.04

CeraOS: 11.0

Notice

Trademarks

Statement of Conditions

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-50E system.

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

Related Documents

- Release Notes for IP-50E, CeraOS 11.0
- User Guide for IP-50E, CeraOS 11.0
- IP-50E MIB Reference, CeraOS 11.0
- IP-50E Installation Guide

1. Synonyms and Acronyms

Acronym	Equivalent Term
ACAP	Adjacent Channel Alternate Polarization
ACCP	Adjacent Channel Co-Polarization
ACM	Adaptive Coding Modulation
ACMB	Adaptive Coding Modulation and Bandwidth
AES	Advanced Encryption Standard
AIS	Alarm Indication Signal
ATPC	Automatic Tx Power Control
BER	Bit Error Ratio
BBU	Baseband Unit
BPDU	Bridge Protocol Data Units
C-RAN	Cloud RAN (Radio Access Network)
CBS	Committed Burst Size
CE	Customer Equipment
CET	Carrier-Ethernet Transport
CIR	Committed Information Rate
CLI	Command Line Interface
CoS	Class of Service
CPRI	Common Public Radio Interface
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
ESE	Electrical SFP Electrical
ESP	Electrical SFP+ 10G
ESS	Electrical SFP
ETH-BN	Ethernet Bandwidth Notification
EVPL	Ethernet Virtual Private Line
EVC	Ethernet Virtual Connection

Acronym	Equivalent Term
FM	Fault Management
FTP (SFTP)	File Transfer Protocol (Secured File Transfer Protocol)
GbE	Gigabit Ethernet
HTTP (HTTPS)	Hypertext Transfer Protocol (Secured HTTP)
LAN	Local area network
LLF	Link Loss Forwarding
LOC	Loss of Carrier
LOF	Loss of Frame
LOS	Loss of Signal
LTE	Long-Term Evolution
MEN	Metro Ethernet Network
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
PLL	Phase-Locked Loop
PM	Performance Monitoring
PTP	Precision Timing-Protocol
QoE	Quality of-Experience
QoS	Quality of Service
RBAC	Role-Based Access Control
RDI	Remote Defect Indication
RE	Radio Equipment
REC	Radio Equipment Control
RMON	Ethernet Statistics
RRH	Remote Radio Head

Acronym	Equivalent Term
RSL	Received Signal Level
RSTP	Rapid Spanning Tree Protocol
SAP	Service Access Point
SDN	Software-Defined Networking
SFTP	Secure FTP
SLA	Service level agreements
SNMP	Simple Network Management Protocol
SNP	Service Network Point
SNTP	Simple Network Time Protocol
SP	Service Point
STP	Spanning Tree Protocol
SSH	Secured Shell (Protocol)
SSM	Synchronization Status Messages
SyncE	Synchronous Ethernet
TACACS+	Terminal Access Controller Access-Control System Plus
TOS	Type of Service
UNI	User Network Interface
UTC	Coordinated Universal Time
Web EMS	Web-Based Element Management System
WFQ	Weighted Fair Queue
WRED	Weighted Random Early Detection
XPIC	Cross Polarization Interference Cancellation

2. Introduction

IP-50E is a high-capacity, all-outdoor Ethernet backhaul system designed to operate in the E-Band frequency range. IP-50E provides up to 10 Gbps capacity in 1+0 configurations, and up to 20 Gbps capacity with 2+0 XPIC. IP-50E can operate over 62.5, 125, 250, 500, 1000, and 2000 MHz channels, with modulations of BPSK to 512[1] QAM and a rich feature set.

This chapter includes:

- Product Overview
- System Configurations
- New Features in CeraOS 11.0

[1] Supported maximum modulation may depend on the configured channel spacing. For details, see *Radio Capacity Specifications* on page 170.

2.1 Product Overview

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

IP-50E operates over 62.5, 125, 250, 500, 1000 and 2000 MHz channels to deliver up to 20 Gbps of Ethernet throughput in several system configurations.

IP-50E can also be used in Multiband configurations with IP-20C, IP-20C-HP, IP-20S, IP-20N, IP-20A, or third-party microwave radios to provide robust links of up to 10 Gbps. In a Multiband configuration, the very high availability of microwave effectively provides a backup for the high-capacity E-Band link, thus enabling operators to benefit simultaneously from the high capacity of E-Band and the high reliability of microwave.

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

- Macro site backhaul
- Macro site aggregation
- Ultra-high capacity to POP
- Small cell backhaul

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

- Integrated Carrier Ethernet services switch, MEF CE 2.0 compliant
  - Rich packet processing feature set for support of engineered end-to-end Carrier Ethernet services with strict SLA.
  - High precision, flexible packet synchronization solution combining SyncE and 1588v2.
- ACMB – Adaptive Coding Modulation and Bandwidth: Hitless transmission between modulation steps (BPSK to 512 QAM[2]) and, at BPSK, hitless modification of the channel spacing when necessary by reducing the channel spacing to one half or one quarter, to increase link survivability and provide seamless capacity increases of up to 10 Gbps over the air, 20 Gbps for 2+0 XPIC links.
- Header De-Duplication – enables to achieve high capacity with narrower channels and lower modulations to increase system.

[2] Supported maximum modulation may depend on the configured channel spacing. For details, see *Radio Capacity Specifications* on page 170.

- In-band and out-of-band management options.
- Network Management – Full suite of secured network management capabilities within IP-50E and seamless connection to Ceragon's Network Management System (NMS) applications for secure remote management.
- Electrical and optical GbE interfaces.
- Ceragon-approved PoE.
- Power redundancy option with simultaneous DC feed and passive PoE injector

2.2 System Configurations

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

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

2.2.1 1+0 – Direct Mount

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

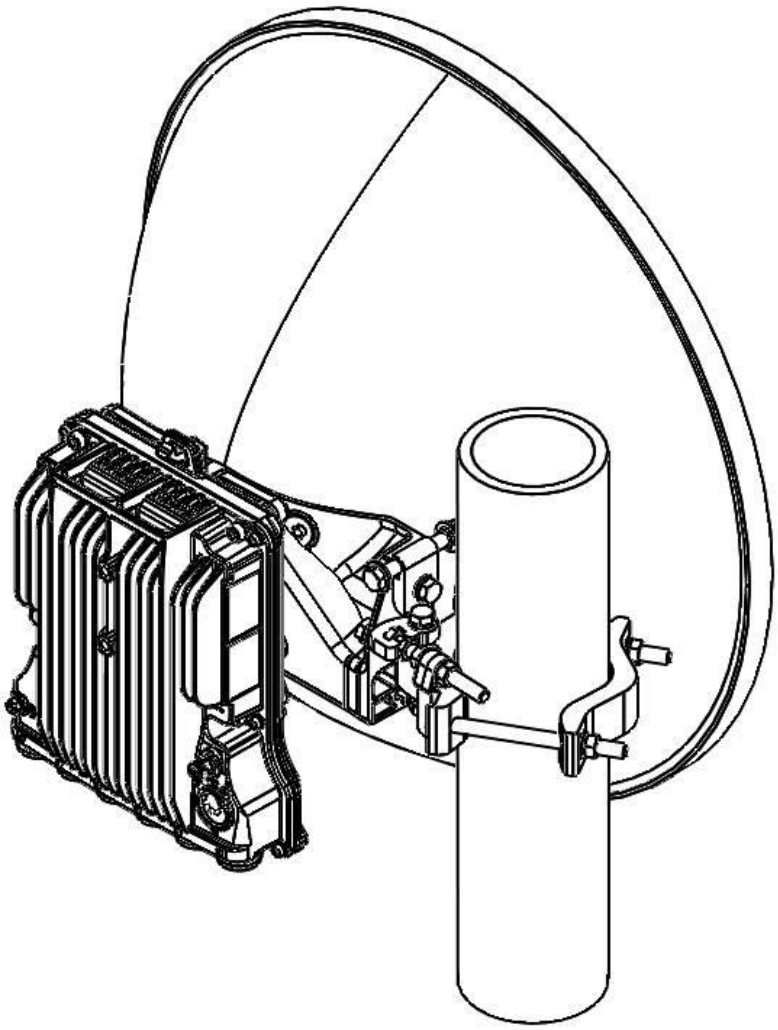


Figure 1: IP-50E 1+0 Direct Mount

2.2.2 1+0 – Low Visual Impact

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

Note:	For this configuration, IP-50E must be ordered together with the antenna mounting kit. See *Table 1*.

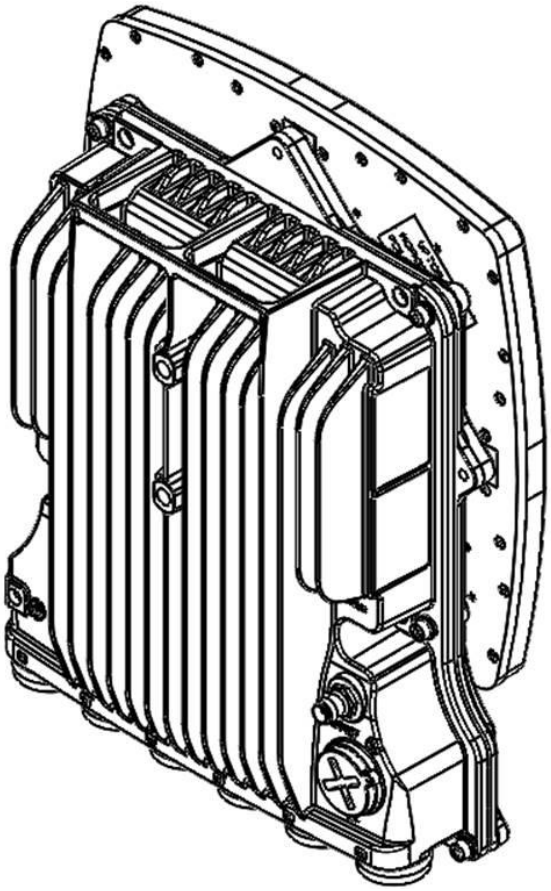


Figure 2: Integrated 43dBi Antenna

Table 1: IP-50E Antenna Mounting Kit

Marketing Model	Description
Integrated_Ant_Mounting_Kit	Integrated Antenna Mounting Kit

2.2.3 2+0 XPIC – Direct Mount

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

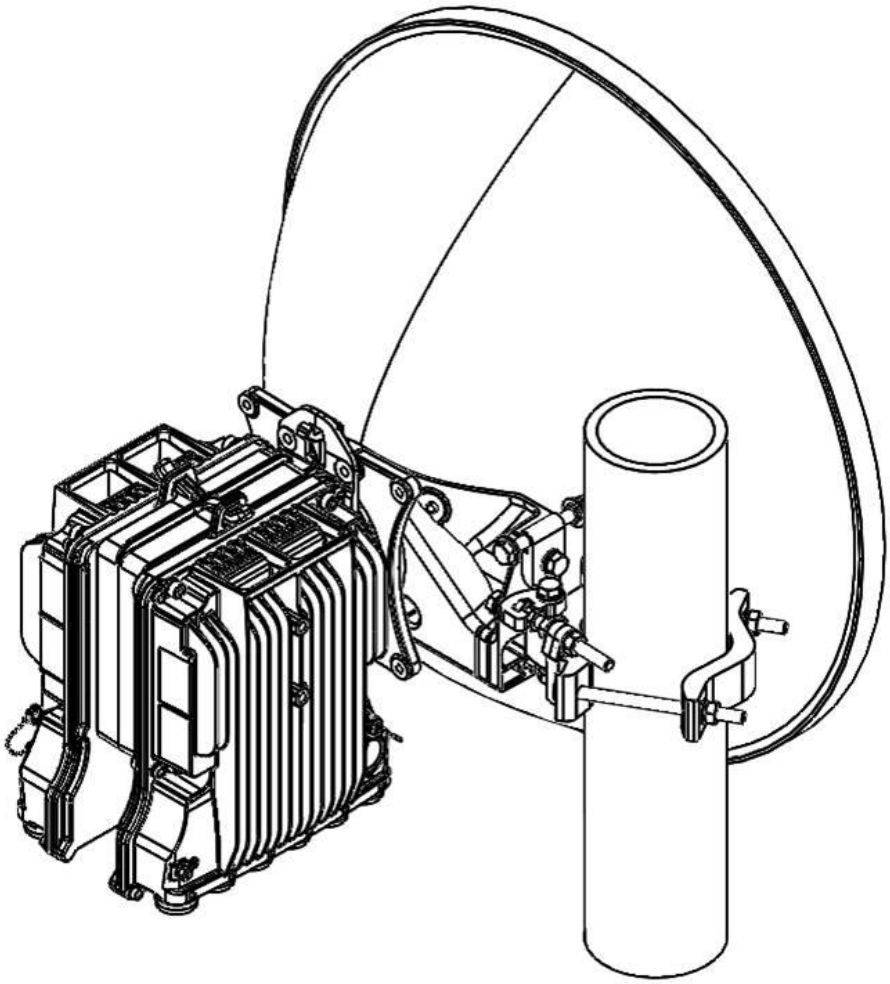


Figure 3: IP-50E 2+0 SP/DP Direct Mount

2.2.4 2+0 XPIC – Low Visual Impact

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

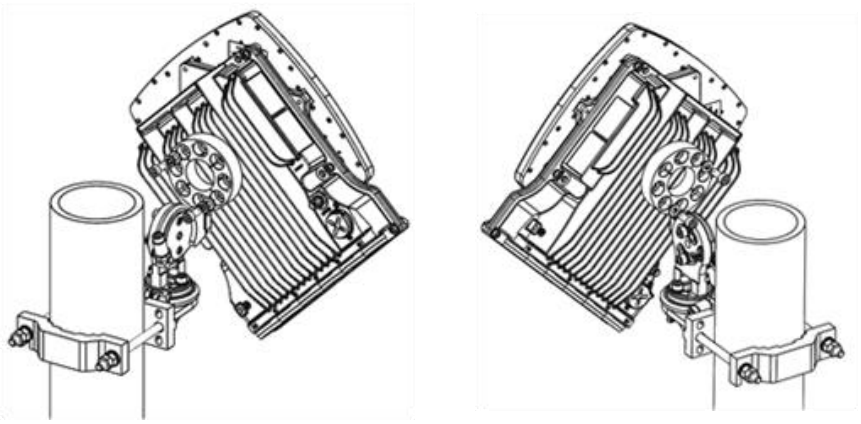


Figure 4: IP-50E 2+0 DP Low Visual Impact

2.3 New Features in CeraOS 11.0

The following table lists the features that have been added in CeraOS version 11.0, and indicates where further information can be found on the new features in this manual and where configuration instructions can be found in the User Guide.

Table 2: New Features in CeraOS 11.0

Feature	Further Information	Configuration Instructions in the User's Guide
2+0 XPIC	*Cross Polarization Interference Canceller (XPIC)* on page 59	For hardware assembly instructions (including cables): IP-50E Installation Guide, Section 5.5, *2+0 (XPIC) with 43 dBi Flat Antenna and Alignment Device* or Section 6.3, *2+0 Direct Mount Dual Polarization (XPIC)* For software configuration instructions (including alignment): IP-50E User Guide, Section 3.4, *Configuring XPIC*
IEEE-1588v2 Boundary Clock	*IEEE-1588v2 PTP Optimized Transport* on page 155	Section 8.4, *Configuring 1588 Boundary Clock*
Multiband with IP-20N or IP-20A	*Multiband (Enhanced Multi-Carrier ABC)* on page 53	Section 3.3, *Configuring Multiband*
TACACS+	*TACACS+ Support* on page 184	Section 10.7, *Configuring TACACS+*,
Ethernet Bandwidth Notification (ETH-BN)	*Ethernet Bandwidth Notification (ETH-BN)* on page 151	Section 8.1, *Configuring Ethernet Bandwidth Notification (ETH-BN)*
Customer-Defined RSA Private Key	*RSA Keys* on page 186	Section 10.11, *Downloading and Installing an RSA Key*
Quick Security Configuration Pages	*Web-Based Element Management System (Web EMS)* on page 170	Section 10.1, *Quick Security Configuration*
Security Summary Page	*Web-Based Element Management System (Web EMS)* on page 170	Section 1.4.5, *The Security Summary Page*

3. IP-50E Hardware Description

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

This chapter includes:

- IP-50E Unit Description
- IP-50E Interfaces
- QSFP Port for 4x10G and 1G Configurations
- CPRI Module (Optional)
- PoE Injector
- Voltage Alarm Thresholds and PMs

3.1 IP-50E Unit Description

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

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

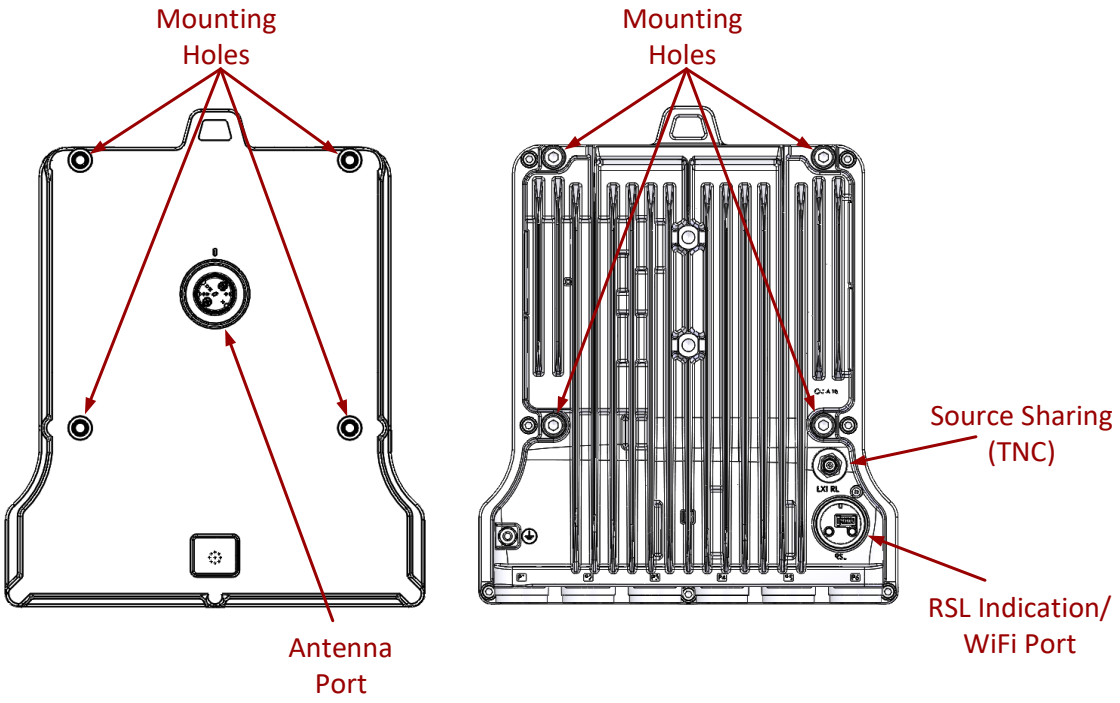


Figure 5: IP-50E Direct Mount HW Ready – Rear View (Left) and Front View (Right)

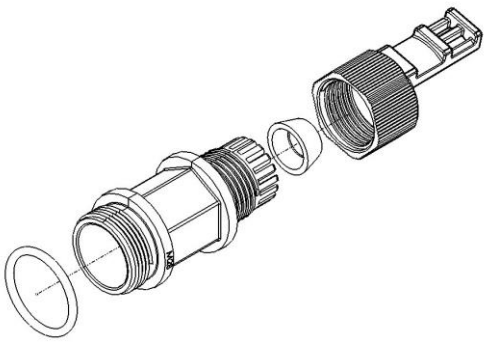


Figure 6: Cable Gland Construction

3.2 IP-50E Interfaces

The IP-50E has an optical SFP cage, an optical SFP/SFP+ cage, and a QSFP cage for traffic and one RJ-45 port for management and PoE.

For power, the IP-50E has a DC power interface (-48V) (Port 1). Optionally, when used in all-outdoor configurations, the IP-50E can also receive PoE power from a Ceragon-approved PoE injector via P2, an RJ-45 port that is also used for management.

Power redundancy can be achieved by using both a DC power input and a passive PoE injector simultaneously. The IP-50E monitors both power feeds and uses the best power source at any given moment.

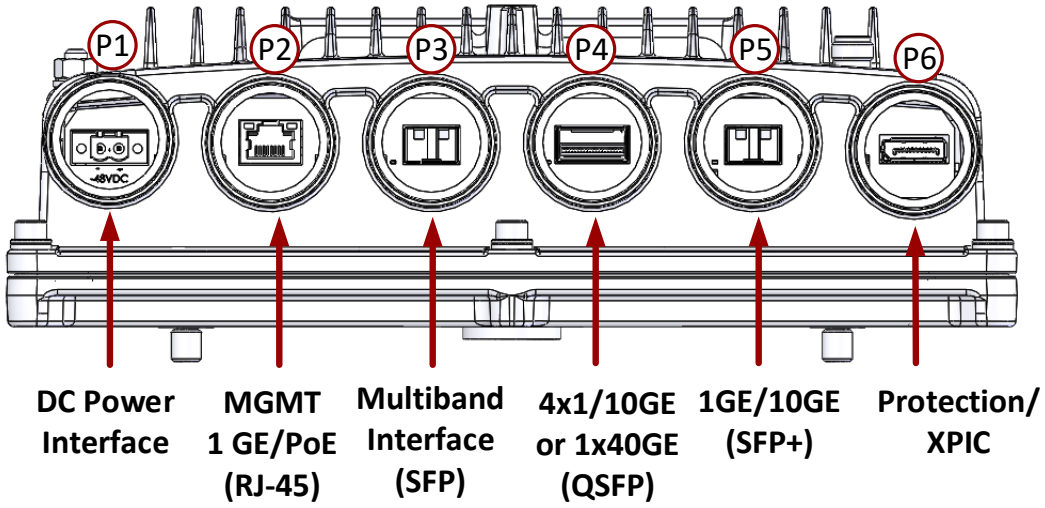


Figure 7: IP-50E Interfaces

- Port 1 – Power Interface (-48V)
- Port 2 (MNG 1/Eth 1):
  - Electric: 10/100/1000Base-T RJ-45
  - Management port (no traffic)
  - PoE
- Port 3 (Eth 2):
  - SFP cage which supports SFP standard
  - 1/2.5GE Multiband port (user-configurable)

Note:	In CeraOS 11.0, Port 3 can only be used for Multiband and only 1GE is supported.

- Port 4 (Eth 3, Eth 4, Eth 5, Eth 6):
  - QSFP cage which supports QSFP standard
  - 4x1GE/10GE or 1x40GE Eth traffic (user configurable)
  - Option for SFP or SFP+ (1x1/10GE) with adaptor
  - Option for CPRI with adaptor

Note:	In CeraOS 11.0, 4x1/10G is supported.

- Port 5 (Eth 7):
  - SFP cage which supports SFP and SFP+ standards
  - 1GE or 10GE Eth traffic
- Port 6:
  - External Connection – Used for XPIC and HSB protection.

Note: In CeraOS 11.0, only Ports 4 and 5 are supported for traffic.

- Antenna Port – Ceragon proprietary flange (flange compliant with UG385/U)
- RSL interface – DVM interface to enable voltage measurement for RSL indication. The RSL measurement is performed using standard DVM testing probes. To access the RSL interface, the user must remove the port's cover and insert the DVM plugs into the sockets, according to the polarization markings.
- Grounding screw

3.3 QSFP Port for 4x10G and 1G Configurations

In CeraOS 11.0, the QSFP port on the IP-50E (Port 4) can be used for 4x1/10 Gbps configurations. Both 1G and 10G links can be used simultaneously with the same unit.

In a 4x1/10G configuration, the QSFP port can provide four Ethernet interfaces: Eth3, Eth4, Eth 5, and Eth6. In this configuration, a QSFP transceiver is attached to the QSFP port, and an MPO-MPO cable is connected between the transceiver and a splitter. The splitter splits the traffic between four Ethernet cables connecting the splitter to the customer equipment. These accessories are listed in *Table 3*.

Notes:

The Ethernet cables connecting the splitter to the customer equipment, and the SFP transceivers attached to the customer equipment, must be multimode type.

1x40G configurations are planned for future release.

Table 3: QSFP Accessories

Component	Marketing Model	Description
QSFP Transceiver	QSFP+40GE-OPT-EXT-TEMP	In 4x10Gbps configurations, the transceiver is attached to the QSFP port on the IP-50E.
MPO-MPO Cable	See Section 3.6.3, *MPO-MPO Cables for QSFP Links*, in the Installation Guide for IP-50E	In 4x10Gbps configurations, an MPO-MPO cable is connected between the QSFP transceiver on the IP-50E and the splitter.
Indoor Splitter	QSFP_to_4xLC_module_indoor	In 4x10Gbps configurations in which the IP-50E is connected to an indoor switch, the MPO-MPO cable is connected to this splitter. In turn, four Ethernet cables are connected from the splitter to the switch.
Indoor Splitter Chassis	19in_Chassis_QSFP-4xLC_module	Houses up to six Indoor Splitter modules (QSFP_to_4xLC_module_indoor).
Outdoor Splitter	FO_MM_out_distrib_MPO_to_4xLC	In 4x10Gbps configurations in which the IP-50E is connected to an outdoor switch or radio, the MPO-MPO cable is connected to this splitter. In turn, four Ethernet cables are connected from the splitter to the switch or radio.

3.4 CPRI Module (Optional)

Note: The CPRI module is planned for future release.

Optionally, IP-50E can be used with a CPRI module. The CPRI module is inserted in the IP-50E's QSFP port (P4), and provides up to 10 Gbps capacity for CPRI traffic. The CPRI module converts CPRI signals to Ethernet and Ethernet to CPRI in accordance with Radio over Ethernet (RoE) standard IEEE 1914.3 and CPRI specification v7.0.

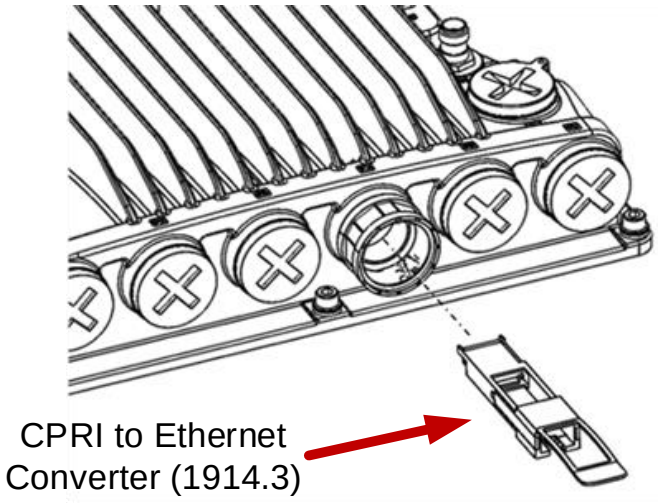


Figure 8: Inserting CPRI Module in QSFP Port

3.4.1 CPRI Overview

Many Fronthaul networks use a C-RAN architecture that separates the BBU (Baseband Unit) from the RRH (Remote Radio Head) network elements. This provides many advantages, including the ability to place RRHs in close proximity to antennas, and the ability to place BBUs in a central location, in close proximity to a network infrastructure that facilitates the transfer of data from the BBU into the Backhaul network. C-RAN architecture also facilitates the placement of multiple BBUs in a single location.

CPRI plays a key role in Fronthaul, particularly with the use of C-RAN network architecture. CPRI is the standard interface between the BBU and the RRH, and was developed specifically for the purpose of supporting the split base station architecture in which the baseband processing function is separated from the radio function.

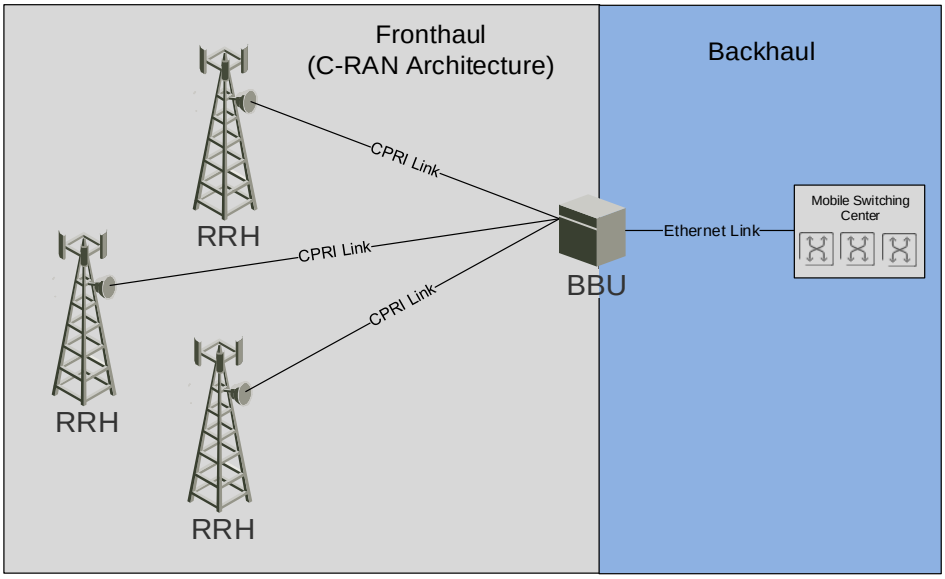


Figure 9: CPRI in C-RAN Fronthaul Network

CPRI is a digitized interface that connects between Radio Equipment Control (REC) and Radio Equipment (RE).

Note:	In the terminology commonly used in Fronthaul networking, the REC is implemented as a BBU and the RE is implemented as an RRH.

In CPRI, three information flows are multiplexed over the interface:

- User Plane data
- Control and Management Plane data
- Synchronization Plane data

The CPRI specification covers Layers 1 and 2. The physical layer (Layer 1) supports both an electrical interface and an optical interface. Layer 2 is designed to support flexibility and scalability.

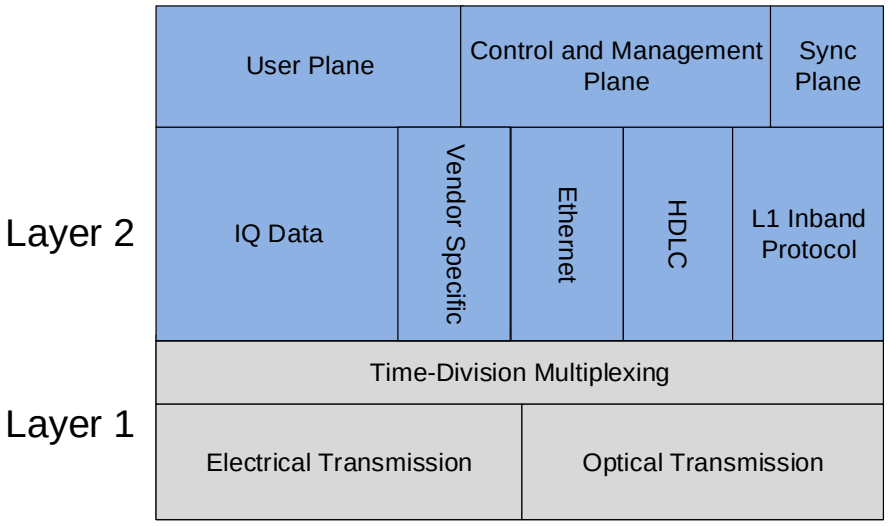


Figure 10: CPRI Protocol Layers

CPRI can be used between one BBU and RRU, or between one BBU and multiple RRHs in daisy-chain or star configurations. CPRI signals are specified at various bit rates up to 24.3 Gbps.

- CPRI line bit rate option 3: 2457.6 Mbit/s, 8B/10B line coding
- CPRI line bit rate option 4: 3072.0 Mbit/s, 8B/10B line coding
- CPRI line bit rate option 5: 4915.2 Mbit/s, 8B/10B line coding
- CPRI line bit rate option 6: 6144.0 Mbit/s, 8B/10B line coding
- CPRI line bit rate option 7: 9830.4 Mbit/s, 8B/10B line coding
- CPRI line bit rate option 7A: 8110.08 Mbit/s, 64B/66B line coding
- CPRI line bit rate option 8: 10137.6 Mbit/s, 64B/66B line coding
- CPRI line bit rate option 9: 12165.12 Mbit/s, 64B/66B line coding

IP-50E with the CPRI module supports rates up to 9830.4 Mbps (Option 7).

3.4.2 IP-50E with CPRI

With its CPRI module, IP-50E can perform as an economical, high-capacity wireless Fronthaul carrier, serving in place of fiber to connect the RRH and BBU. The BBU transmits CPRI data to the IP-50E via the IP-50E CPRI module. The CPRI module converts the data to Ethernet, and transmits it over the radio to an IP-50E connected to the RRH, where the data is processed and converted back to CPRI in the CPRI module of the second IP-50E.

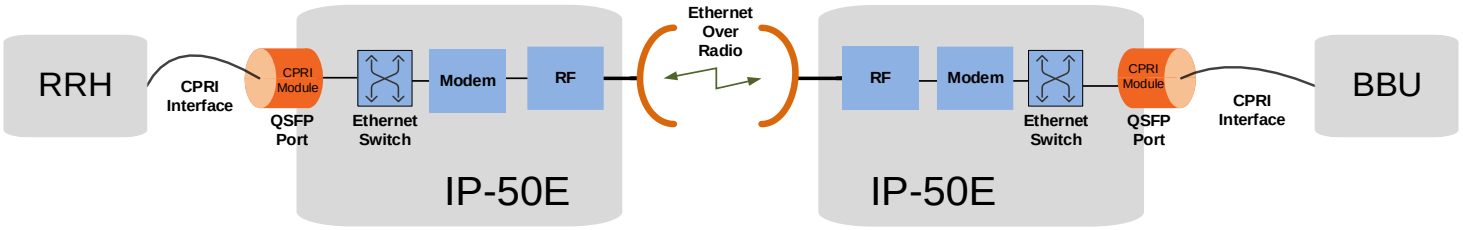


Figure 11: IP-50E with CPRI Module in Fronthaul Network

The IP-50E CPRI module supports the following CPRI bit rates (user-configurable), as defined in IEEE 1914.3:

- CPRI Line Bit Rate Option 3: 2457.6 Mbit/s
- CPRI Line Bit Rate Option 5: 4915.2 Mbit/s
- CPRI Line Bit Rate Option 7: 9830.4 Mbit/s

The IP-50E CPRI module supports the following CPRI modes (user-configurable):

- Structure-Agnostic Simple Tunneling Mode – Supports Bit Rate Options 3 and 5.
- Structure-Agnostic Mode with Removal of Line Coding – Supports Bit Rate Options 3, 5, and 7.

Table 4 shows the CPRI capacity per CPRI mode and Bit Rate Option. For Tunneling Mode, capacity is based on the bit rate with 5% added for overhead. For Removal of Line Coding mode, capacity is based on 80% of the CPRI, with 5% added for overhead.

Table 4: CPRI Capacity

CPRI Mode	Bit Rate Option	Ethernet Capacity (Mbps)
Structure-Agnostic Simple Tunneling Mode	3 (2457.6 Mbps)	2580.48
Structure-Agnostic Simple Tunneling Mode	5 (4915.2 Mbps)	5160.96
Structure-Agnostic Mode with Removal of Line Coding	3 (2457.6 Mbps)	2064.38
Structure-Agnostic Mode with Removal of Line Coding	5 (4915.2 Mbps)	4128.77
Structure-Agnostic Mode with Removal of Line Coding	7 (9830.4 Mbps)	8257.54

To achieve the desired capacity, make sure to use an MRMC script and modulation that supports the desired capacity level or higher. See *Radio Capacity Specifications* on page 196.

All standard SFP and SFP+ modules are supported with the IP-50E CPRI module.

Note: It is recommended to use Fixed ACM mode with CPRI.

Automatic State Propagation (ASP) is available for CPRI. As with Ethernet, ASP for CPRI enables propagation of radio failures back to the CPRI port. Users can also configure ASP to close the CPRI port based on a radio failure at the remote carrier.

When configuring a service to carry the data between the CPRI module to the radio, the service should be assigned the highest QoS priority.

3.4.3 Synchronization with CPRI

Synchronization is implemented using SyncE, with the BBU configured as the Master Reference Clock. This enables the CPRI module to produce fully synchronized Ethernet and fully synchronized CPRI.

The CPRI module recovers clock from incoming Ethernet and incoming CPRI, and uses the recovered clock to recreate fully synchronized CPRI and Ethernet, respectively.

The recovered clock is cleaned by an external PLL. This includes clock recovered from both the CPRI side and the Ethernet side.

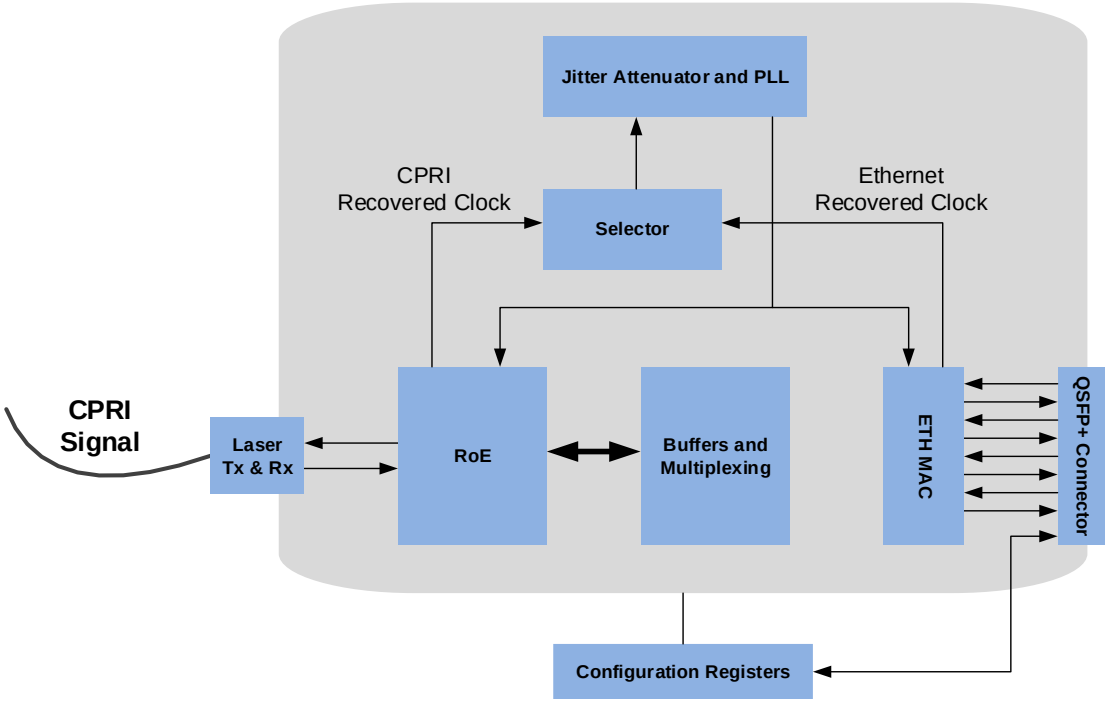


Figure 12: SyncE with CPRI Module – Block Diagram

3.4.4 Low Latency with CPRI

The IP-50E CPRI solution provides low latency according to the bit rate, as follows:

- CPRI line bit rate option 7: Under 50 µs
- CPRI line bit rate option 5: Under 100 µs
- CPRI line bit rate option 3: Under 100 µs

3.5 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-50E system. PoE is only available for non-XPIC configurations.

Note:	An AC-power PoE Injector option is also available. Contact your Ceragon representative for details.

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.

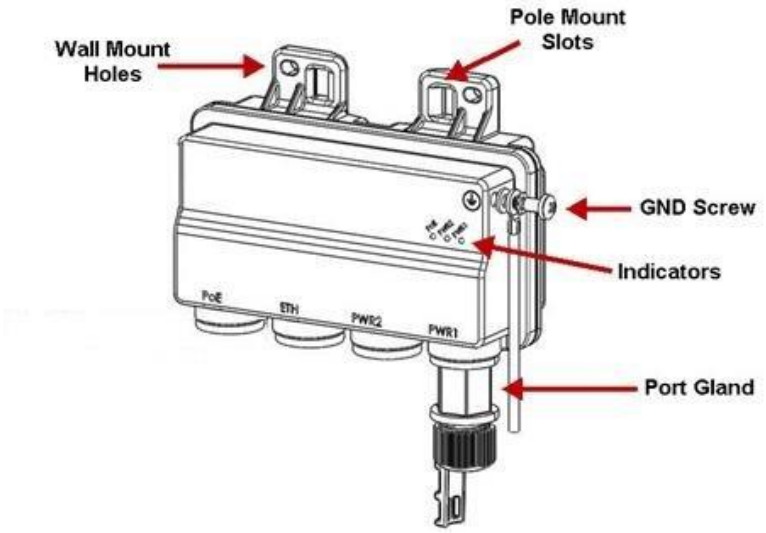


Figure 13: PoE Injector

Two models of the PoE Injector are available:

- **PoE_Inj_AO_2DC_24V_48V** – Includes two DC power ports with power input ranges of -(18-60)V each.
- **PoE_Inj_AO** – Includes one DC power port (DC Power Port #1), with a power input range of -(40-60)V.

For power redundancy, a passive PoE injector is required. The following passive PoE Injector model is available for power redundancy:

- AC_POE_STD_PWR_INDOOR – Includes one DC power port with a power input range of 90VAC to 264VAC.

3.5.1 PoE Injector Interfaces – Standard PoE

- 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

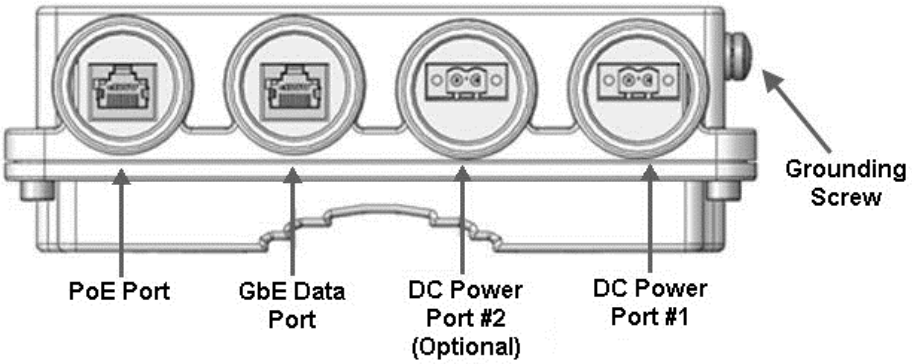


Figure 14: PoE Injector Ports

3.6 Voltage Alarm Thresholds and PMs

The allowed power input range for the IP-50E 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-50E 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-50E's activation key model. IP-50E 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-50E unit is considered a distinct device. Each device contains a single activation key.

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-50E. 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.

4.3 Activation Key Reclaim

If a customer needs to deactivate an IP-50E 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 Smart Pipe (L1) service per each GbE port covered by the activation key.
- A single 1 x GbE port for traffic.
- Full QoS with basic queue buffer management (fixed queues with 1 Mbit buffer size limit, tail-drop only).
- LAG[3]
- No synchronization

Note: As described in more detail below, a CET Node activation key allows all CET service/EVC types including Smart Pipe, Point-to-Point, and Multipoint 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 5: Activation Key Types

Marketing Model	Description	For Addition Information
Refer to *Capacity Activation Keys* on page 41	Enables you to increase your system's radio capacity in gradual steps by upgrading your capacity activation key. Without a capacity activation key, each IP-50E unit has a capacity of 10 Mbps.	Radio Capacity Specifications
SL-NETCONF/YANG	Enables use of NETCONF/YANG protocols, enabling customers to manage, configure, and monitor network elements within the paradigm of SDN network architecture using Ceragon's SDN Master controller.	SDN Support
SL-LLF	Enables you to use 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.	Automatic State Propagation and Link Loss Forwarding
SL-ACM	Enables the use of Adaptive Coding and Modulation (ACM) scripts.	Adaptive Coding Modulation and Bandwidth (ACMB)
SL-ACMB	Enables the use of ACMB. This activation key is required in order to use Profiles 0 and 1 with ACM scripts.	Adaptive Coding Modulation and Bandwidth (ACMB)

[3] LAG is planned for future release.

Marketing Model	Description	For Addition Information
SL-Header-DeDuplication	Enables the use of Header De-Duplication.[4]	Header De-Duplication
SL-mmw-XPIC	Enables the use of Cross Polarization Interference Canceller (XPIC). A separate activation key is required for each core in the XPIC pair.	Cross Polarization Interference Canceller (XPIC)
SL-GE-Port	Per port. Enables the use of an Ethernet port in GbE mode (10/100/1000baseT or 1000baseX). An activation key is required for each additional traffic port that is used on the device, beyond the one GbE traffic port that is enabled via the default activation key. Any of these activation keys can be installed multiple times with dynamic allocation inside the unit. **Note:** Two Ethernet ports are enabled in FE mode (10/100baseT) by default without requiring any activation key.	IP-50E Interfaces
SL-10GE-Port	Enables the use of a 10GE Ethernet traffic port	IP-50E Interfaces
Refer to *Edge CET Node Activation Keys* on page 43.	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.[5] • Full QoS for all services including basic queue buffer management (fixed queues buffer size limit, tail-drop only) and eight queues per port, no H-QoS.	• Ethernet Service Model • Quality of Service (QoS)
SL-Network-Resiliency	Enables G.8032 for improving network resiliency.	Network Resiliency
SL-Enh-MC-ABC	Enables the configuration and use of a Multiband (Enhanced Multi-Carrier ABC) link. Two activation keys are required per Multiband node, on the IP-50E. One of these activation keys is for the radio port, the other is for the Ethernet port carrying traffic to the unit paired with the IP-50E. No activation key is required for the unit paired with the IP-50E.	Multiband (Enhanced Multi-Carrier ABC)

[4] Header De-Duplication is planned for future release.

[5] Network resiliency protocols are planned for future release.

Marketing Model	Description	For Addition Information
SL-H-QoS	Enables H-QoS. This activation key is required to add service-bundles with dedicated queues to interfaces. Without this activation key, only the default eight queues per port are supported.	Quality of Service (QoS)
SL-Enh-Packet-Buffer	Enables configurable (non-default) queue buffer size limit for Green and Yellow frames. Also enables WRED. The default queue buffer size limit is 1Mbits for Green frames and 0.5 Mbits for Yellow frames.	Quality of Service (QoS)
SL-Sync-Unit	Enables the G.8262 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).	Synchronization
SL-IEEE-1588-TC	Enables IEEE-1588 transparent clock support	IEEE-1588v2 PTP Optimized Transport
SL-IEEE-1588-BC	Enables IEEE-1588 Boundary Clock.	IEEE-1588v2 PTP Optimized Transport
SL-Secure-Management	Enables secure management protocols (SSH, HTTPS, SFTP, SNMPv3, TACACS+, and RADIUS)	Secure Communication Channels
SL-Eth-OAM-FM	Enables Connectivity Fault Management (FM) per Y.1731.	Connectivity Fault Management (FM)
SL-Eth-OAM-PM	Enables performance monitoring pursuant to Y.1731 (CET mode only).	
SL-LACP	Enables Link Aggregation Control Protocol (LACP).	Link Aggregation Groups (LAG) and LACP

Table 6: 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	
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	

Marketing Model	Marketing Description	Notes
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-Capacity-2.5G	IP-20 SL - Capacity 2.5G	
SL-Capacity-3Gbps	IP-20 SL - Capacity 3G	
SL-Capacity-4G	IP-20 SL - Capacity 4G	
SL-Capacity-5G	IP-20 SL - Capacity 5G	
SL-Capacity-6G	IP-20 SL - Capacity 6G	
Capacity-7G	IP-20 SL - Capacity 7G	
Capacity-8G	IP-20 SL - Capacity 8G	
Capacity-9G	IP-20 SL - Capacity 9G	
Capacity-10G	IP-20 SL - Capacity 10G	
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	
SL-Upg-2G-2.5G	IP-20 SL - Upg 2G - 2.5G	
SL-Upg-2.5G - 5G	IP-20 Act.Key - Upg 2.5G - 5G	
SL-Upg-2.5G - 7G	IP-20 Act.Key - Upg 2.5G - 7G	
SL-Upg-2.5G - 10G	IP-20 Act.Key - Upg 2.5G - 10G	

Marketing Model	Marketing Description	Notes
SL-Upg-5G - 10G	IP-20 Act.Key - Upg 5G - 10G	
SL-Upg-7G - 10G	IP-20 Act.Key - Upg 7G - 10G	

Table 7: Edge CET Node Activation Keys

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

If a CET activation key is not generated on the IP-50E 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 simply choose the appropriate activation key from the options listed in *Table 7*.

5. Feature Description

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

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

This chapter includes:

- Capacity Summary
- Ethernet Features
- Frequency Scanner
- Synchronization

5.1 Innovative Techniques to Boost Capacity and Reduce Latency

IP-50E utilizes Ceragon's innovative technology to provide a high-capacity low-latency solution. IP-50E's Header De-Duplication option enables IP-50E to boost capacity and provide operators with efficient spectrum utilization, with no disruption of traffic and no addition of latency.

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

IP-50E employs full-range dynamic ACM, with modulations in the range of BPSK to 512 QAM.[6] IP-50E takes ACM a step further by introducing Adaptive Coding Modulation and Bandwidth (ACMB). ACMB enhances standard ACM by decreasing channel spacing at BPSK when necessary to mitigate against fading.

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

This section includes:

- Capacity Summary
- Header De-Duplication
- Adaptive Coding Modulation and Bandwidth (ACMB)
- Multiband (Enhanced Multi-Carrier ABC)
- Cross Polarization Interference Canceller (XPIC)
- External Protection
- ATPC
- Radio Signal Quality PMs
- Radio Utilization PMs

[6] Certain modulations are only supported with specific channels. For details, see *Radio Capacity Specifications* on page 170.

5.1.1 Capacity Summary

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

- **Supported Channels** – 62.5/125/250/500/1000/2000 MHz channels
- **E-Band Frequency Bands** – 71-76 GHz, 81-86 GHz
- **Supported Modulation Range** – 2 QAM (BPSK) to 512 QAM[7]

For additional information:

- Radio Capacity Specifications

[7] Certain modulations are only supported with specific channels. For details, see *Radio Capacity Specifications* on page 170.

5.1.2 Header De-Duplication

IP-50E offers the option of Header De-Duplication, enabling operators to significantly improve Ethernet throughout over the radio link without affecting user traffic. Header De-Duplication can be configured to operate on various layers of the protocol stack, saving bandwidth by reducing unnecessary header overhead. Header De-duplication is also sometimes known as header compression.

Note:	Header De-Duplication is planned for future release.

5.1.3 Adaptive Coding Modulation and Bandwidth (ACMB)

Related topics:

- Quality of Service (QoS)

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

IP-50E employs full-range dynamic ACMB. IP-50E's ACMB mechanism copes with 100 dB per second fading in order to ensure high transmission quality. IP-50E's ACM mechanism is designed to work with IP-50E'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-50E'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.

5.1.3.1 Eleven Working Points

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

Table 8: ACM Working Points (Profiles)

Profile 0	BPSK – ¼ channel spacing
Profile 1	BPSK – ½ channel spacing
Profile 2	BPSK – full channel spacing
Profile 3	QPSK
Profile 4	8 PSK
Profile 5	16 QAM
Profile 6	32 QAM
Profile 7	64 QAM
Profile 8	128 QAM
Profile 9	256 QAM
Profile 10	512 QAM

Note: ACMB is not applicable to 62.5 channels. For 62.5 channels, Profile 0 is BPSK with the normal (62.5 MHz) channel spacing, Profile 1 is QPSK, and so on.
For 125 MHz channels, Profile 0 is BPSK with ½ channel spacing. Profile 1 BPSK is BPSK with the normal channel spacing, Profile 2 is QPSK, and so on.

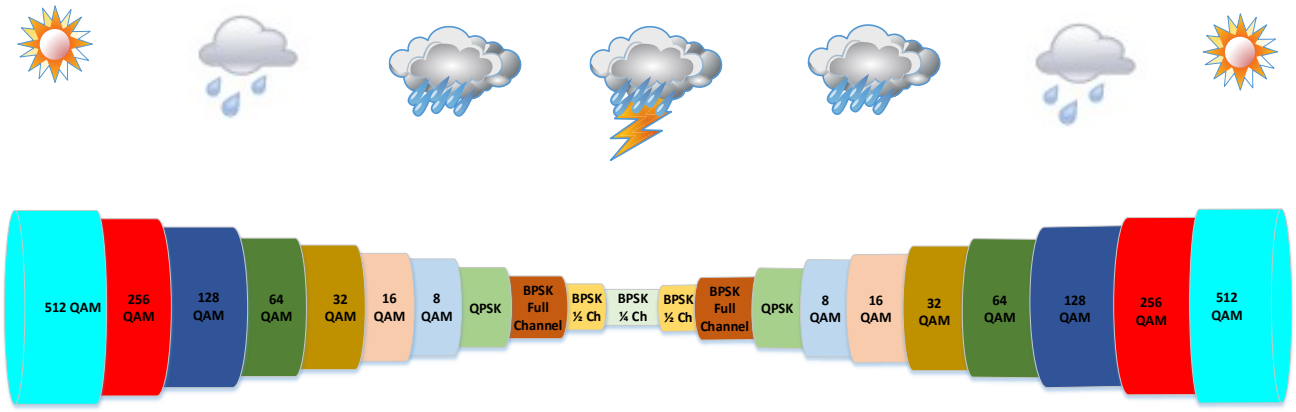


Figure 15: Adaptive Coding and Modulation with Eleven Working Points

5.1.3.2 Hitless and Errorless Step-by Step Adjustments

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

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

5.1.3.3 ACM Radio Scripts

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

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

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

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

ACM scripts can be activated in one of two modes:

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

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

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

Note: The default minimum profile is Profile 2.

5.1.3.4 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.

5.1.3.5 ACMB Benefits

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

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

5.1.3.6 ACM and Built-In QoS

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

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

5.1.3.7 ACMB with Adaptive Transmit Power

This feature requires:

- ACM script

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

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

5.1.4 Multiband (Enhanced Multi-Carrier ABC)

This feature requires:

- When used with IP-20C, IP-20C-HP, or IP-20S, an ESS hardware version (two SFP ports) is required in order to configure synchronization and/or in-band management for the IP-20C, IP-20C-HP, or IP-20S. For IP-20C, a 2E2SX hardware version can also be used.

IP-50E can be used in Multiband configurations with IP-20C, IP-20C-HP, IP-20S, IP-20N, IP-20A, or third-party microwave radios. When used with IP-20N or IP-20A, the IP-50E is paired with an RFU-D, RFU-D-HP, or RFU-C microwave radio.

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

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

5.1.4.1 Multiband Antenna

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

Table 9: Multiband Antenna Marketing Models

Microwave Frequency	Marketing Model	Description
18 GHz	Am-2-18/80-SP/SP-MT	ANT,2FT,MB,17.7-19.7,SP,RFU-C/UBR220,71.0-86.0GHz,SP,RFU-C
18 GHz	Am-2-18/80-DP/SP-MT	ANT,2FT,MB,17.7-19.7,DP,RFU-C/CIRC,71.0-86.0GHz,SP,RFU-C
23 GHz	Am-2-23/80-SP/SP-MT	ANT,2FT,MB,21.2-23.6,SP,RFU-C/UBR220,71.0-86.0GHz,SP,RFU-C
23 GHz	Am-2-23/80-DP/SP-MT	ANT,2FT,MB,21.2-23.6,DP,RFU-C/CIRC,71.0-86.0GHz,SP,RFU-C

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

5.1.4.2 Multiband Operation

In a Multiband configuration, all traffic enters the node via the SFP/SFP+ traffic port (P5) or the QSFP port (P4). Traffic is passed to a Multiband group that includes the Multiband port (P3) and the radio carrier.

The unit paired with the IP-50E acts as a pipe. When traffic is passed from the IP-50E to the paired unit, it is transmitted to either a single radio carrier or 2+0 Multi-Carrier ABC group.

In most circumstances, traffic is passed to the paired unit only when the IP-50E radio has reached full capacity, or if the ACM profile drops to a point where the IP-50E's capacity is temporarily less than the traffic load. If the IP-50E reaches its minimum configured profile, all traffic is passed to the paired unit until the profile rises to a level above the minimum.

To ensure a smooth traffic flow, certain configurations must be performed on the paired unit.

When the IP-50E is paired with an IP-20 microwave radio, the following must be configured on the microwave radio:

- Automatic State Propagation, with **ASP trigger by remote fault** enabled.
- Radio BNM.

When the IP-50E is paired with a third-party unit , the following must be configured on the third-party unit:

- The unit's switching mechanism must be set to Pipe mode
- Automatic State Propagation must be configured, with **ASP trigger by remote fault** enabled.
- 802.3X Flow Control must be enabled

A service must be configured between the Ethernet port connected to the IP-50E and the paired unit's radio or radio group.

Notes:	If the paired unit is an IP-20C, IP-20C-HP, IP-20S, or third-party microwave radio, the service must be a Pipe service. If the paired unit is an IP-20N or IP-20A, any service type can be used. However, this service *must* be given higher priority than any other service attached to the interfaces used for Multiband. The latency differential between the IP-50E and the paired unit cannot be more than 1.6 ms. That means that under all foreseeable conditions, such as a high ACMB profile on one unit and a low ACMB profile on the other unit, there should be no more than a 1.6 ms difference between the latency of the two radio carriers in the Multiband link.

Figure 16 illustrates Multiband operation with an IP-50E and IP-20C. *Figure 16* illustrates a configuration that includes synchronization and management of the IP-20C via the IP-50E. Both of these items are optional, and require an optical cable between Eth3 on the IP-20C (or IP-20C-HP or IP-20S) and any free 1G Ethernet port on the IP-50E, as described in the following sections.

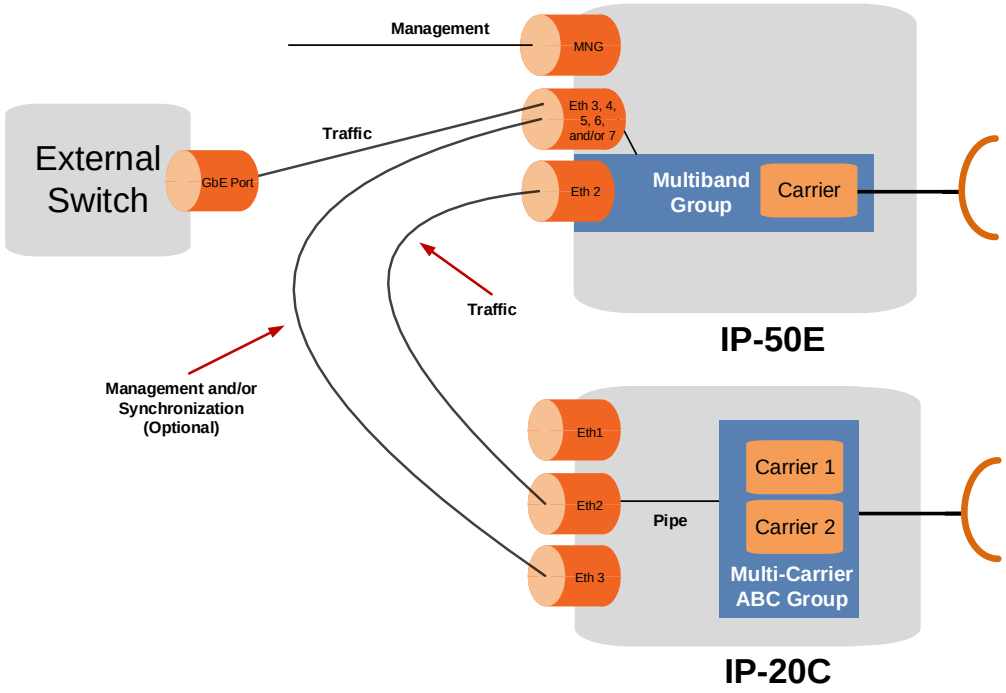


Figure 16: Multiband Operation – IP-50E and IP-20C

Figure 17 illustrates a split-mount Multiband configuration in which an IP-50E operates with an IP-20N or an IP-20A IDU connected to an RFU-D or an RFU-D-HP. In this figure, the RFU carriers are configured in an RFU-based Multi-Carrier ABC group. Multiband can also be configured using a single-carrier RFU-D or RFU-D-HP configuration, or with an RFU-C connected to an RMC-B.

Note:	TCC-based Multi-Carrier ABC and TCC Redundancy cannot be used with Multiband.

Figure 17 illustrates a configuration that includes synchronization and management of the IP-20N or IP-20A unit via the IP-50E. Both of these items are optional, and require an optical cable between any free 1 Gbps optical SFP port on the IP-50E and any free 1G SFP port on the IP-50E, as described in the following sections.

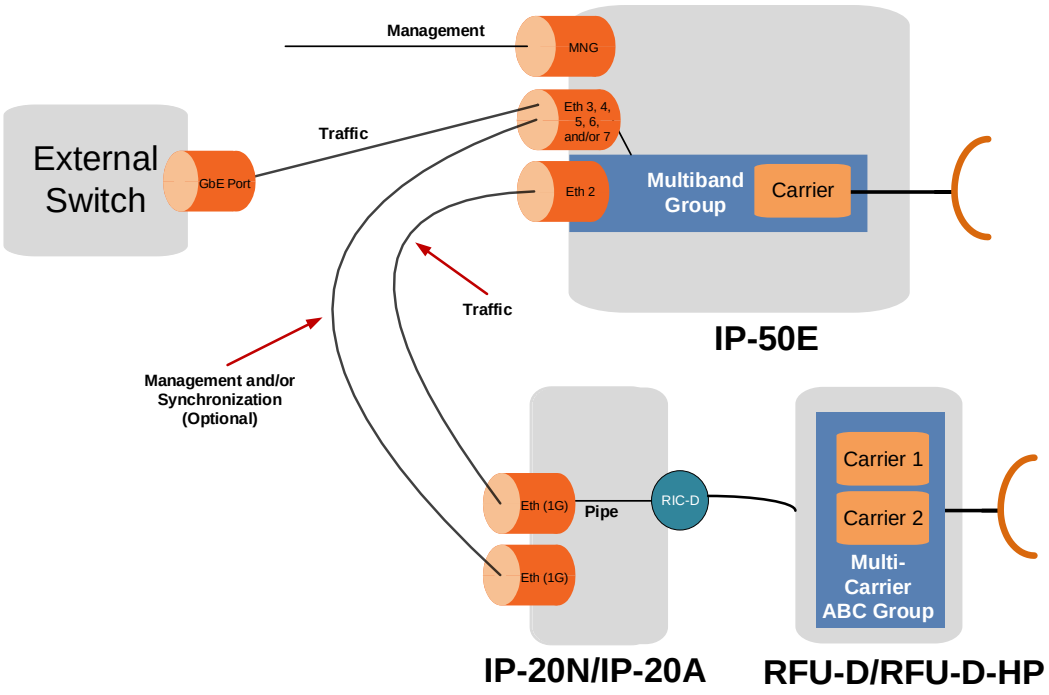


Figure 17: Multiband Operation – IP-50E and IP-20N or IP-20A

Figure 18 illustrates Multiband operation with an IP-50E and a third-party unit. *Figure 18* illustrates a configuration that includes synchronization and management of the third-party unit via the IP-50E. Synchronization via the IP-50E requires an optical cable between an Ethernet port on the third-party unit and any free 1 Gbps optical SFP port on the IP-50E, as described in the following sections.

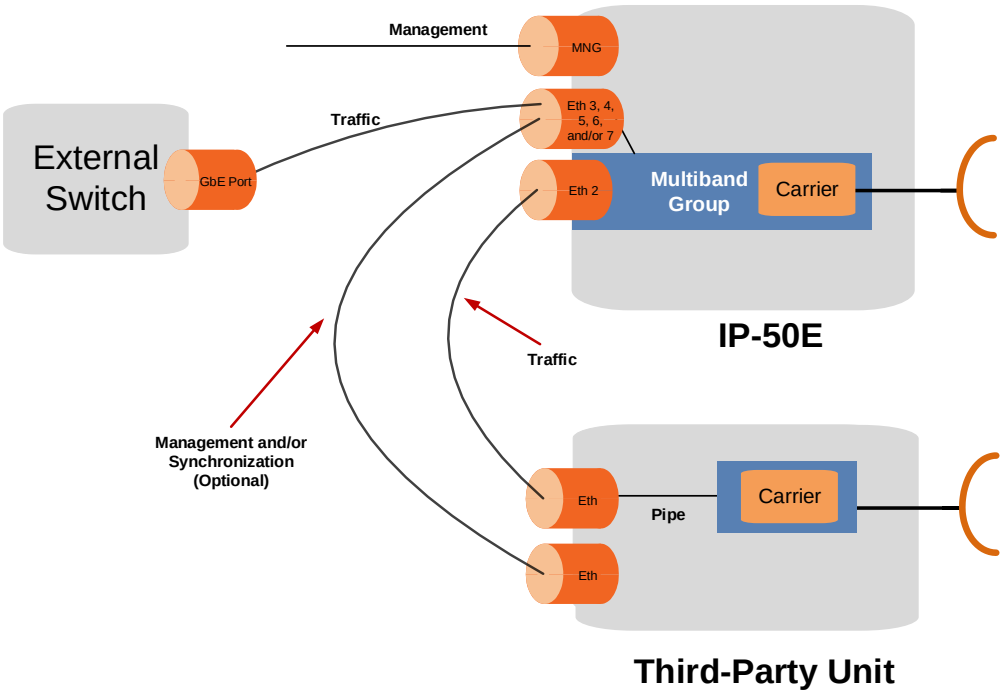


Figure 18: Multiband Operation – IP-50E and Third-Party Unit

5.1.4.3 Synchronization with Multiband Operation

SyncE and 1588 PTP can be used in Multiband nodes. SyncE and 1588 PTP can be configured for both the IP-50E and the unit paired with the IP-50E. Synchronization packets are carried via the Microwave link.

For synchronization via the IP-50E, the paired unit must have at least two free SFP ports. When the paired unit is an IP-20C, IP-20C-HP, or IP-20S, this requires an ESS hardware version for the IP-20C, IP-20C-HP, or IP-20S. For IP-20C, a 2E2SX hardware version can also be used. synchronization for the paired unit requires an optical cable between any free 1 Gbps optical SFP port on the IP-50E and Eth3 on the IP-20C, IP-20C-HP, or IP-20S or a 1 Gbps optical SFP port on the IP-20N, IP-20A, or third-party unit. The same cable can be used for both synchronization and in-band management.

Notes:	When an IP-20N or IP-20A is paired with the IP-20E, 1588 PTP can only be used with RMC-B, not with RIC-D. When a third-party unit is paired with the IP-50E, it is a prerequisite that the third-party radio unit support SyncE and, if required, 1588 PTP in order to provide synchronization for the Multiband node.

5.1.4.4 Multiband Management

The IP-50E unit in a Multiband configuration can be managed normally, as in any other configuration.

The paired unit can be managed directly via its Management port, or via the IP-50E. For in-band management via the IP-50E, the paired unit must have at least two free SFP ports. When the paired unit is an IP-20C, IP-20C-HP, or IP-20S, this requires an ESS hardware version for the IP-20C, IP-20C-HP, or IP-20S. For IP-20C, a 2E2SX hardware version can also be used. For management of the paired unit via the IP-50E, an optical cable must be connected between any free 1 Gbps optical SFP port on the IP-50E and Eth3 on the IP-20C, IP-20C-HP, or IP-20S or data 1 Gbps optical SFP port on the IP-20N, IP-20A, or third-party unit.

A management service must be defined between the management port of the IP-50E and the port on the IP-50E that is connected to the paired unit for management. This transmits management to the paired unit.

The paired unit's management service should only have a service point for the Ethernet port connected to the IP-50E for management. No service point should be defined on the radio or Multi-Carrier ABC group.

Note:	To avoid loops, in-band management *must not* be configured on the paired unit.

5.1.4.5 Limitations and Interoperability of Multiband with other Features

- Multiband is fully compatible with ACMB.
- The maximum capacity of a Multiband node is 10 Gbps.
- LLDP is not supported between P3 of the IP-50E and the port receiving Multiband traffic on the paired unit.

5.1.5 Cross Polarization Interference Canceller (XPIC)

Note: Power redundancy and PoE cannot be used with XPIC.

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

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

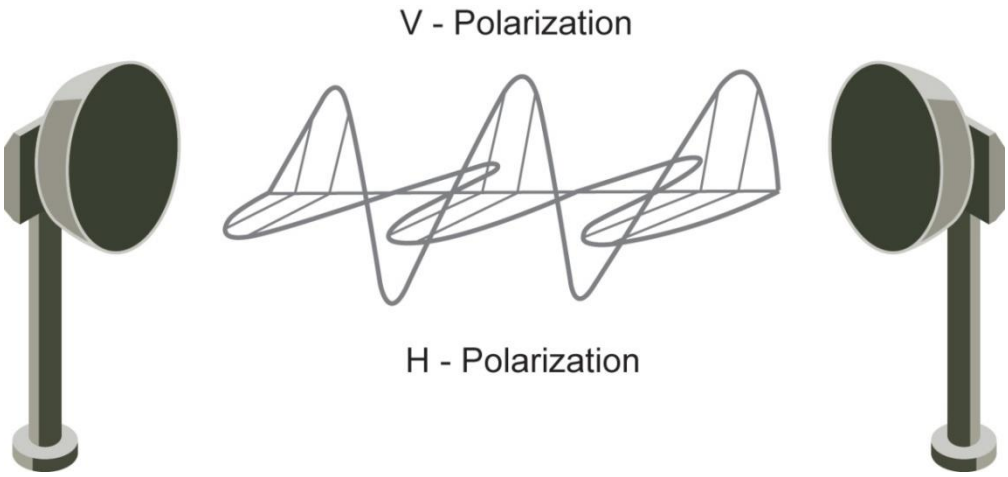


Figure 19: Dual Polarization

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-50E's XPIC algorithm enables detection of both streams even under the worst levels of XPD such as 10 dB. IP-50E accomplishes this by adaptively subtracting from each carrier the interfering cross carrier, at the right phase and level.

5.1.5.1 XPIC Implementation

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

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

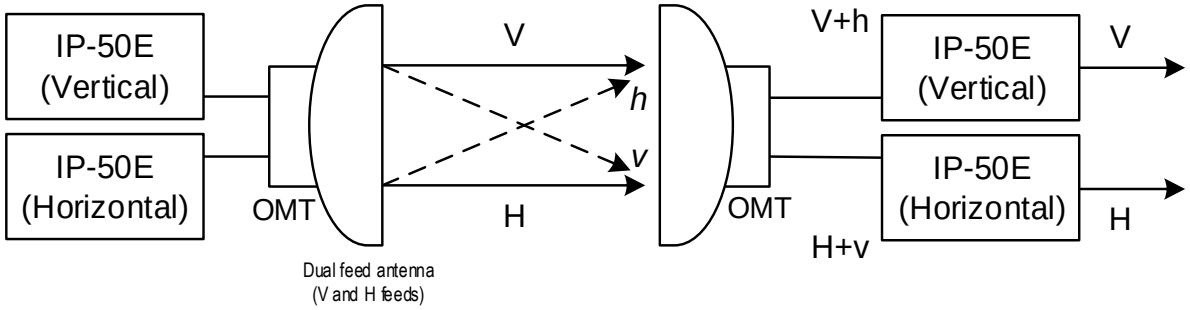


Figure 20: XPIC Implementation – Direct Mount

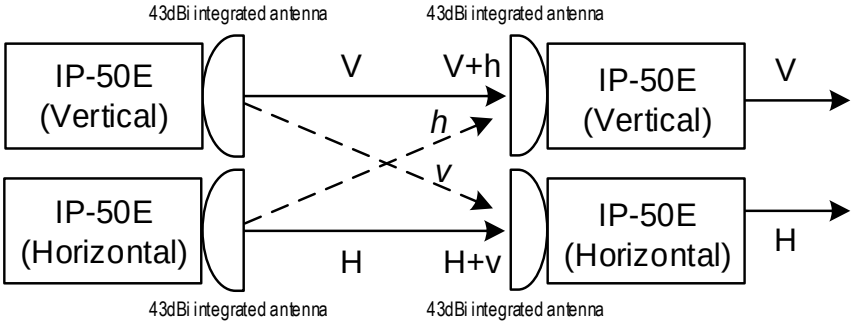


Figure 21: XPIC Implementation – Integrated Antenna

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

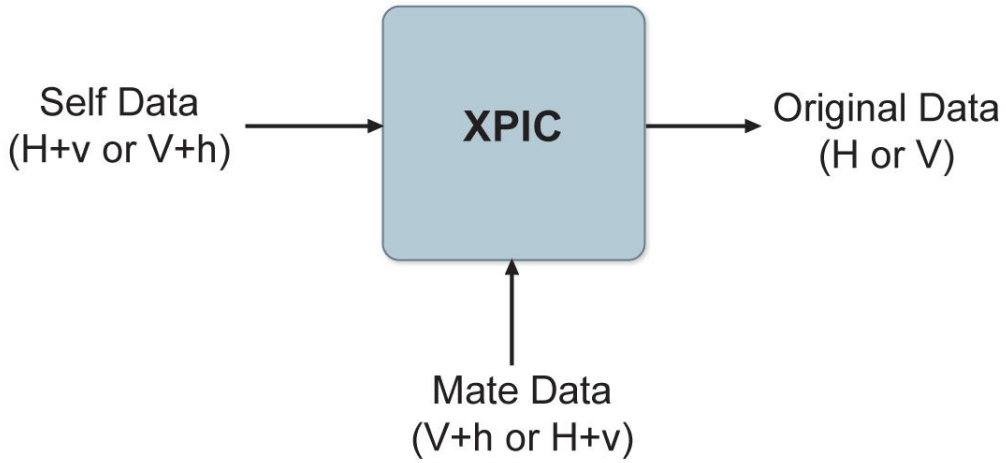


Figure 22: XPIC – Impact of Misalignments and Channel Degradation

5.1.5.2 XPIC Configuration

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

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

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

- An XPIC cable must be connected between the Protection/XPIC ports (P6) of each unit. This cable carries the data necessary for each unit to perform interference cancellation.
- A Clock Sharing cable must be connected between the TNC ports of each unit. This cable transmits clock frequency information between the two units, enabling synchronization.

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

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

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

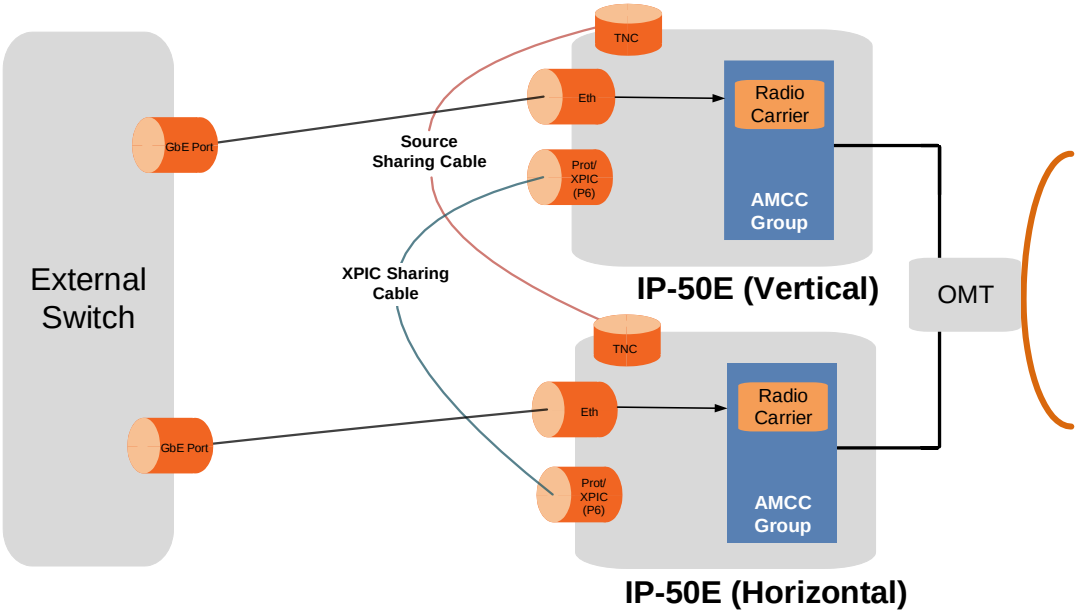


Figure 23: 2+0 XPIC Configuration – Direct Mount

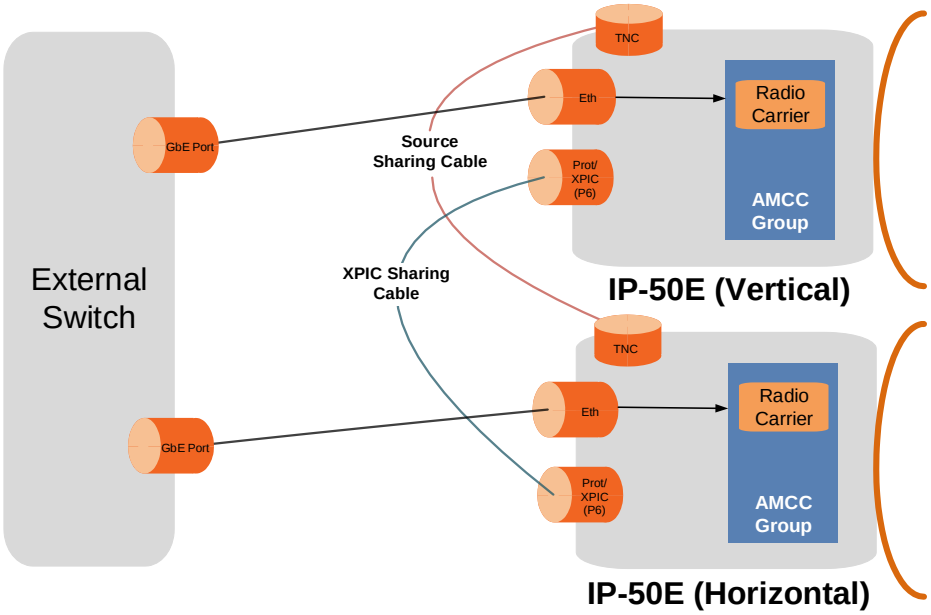


Figure 24: 2+0 XPIC Configuration – Integrated Antenna

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.

5.1.6 External Protection

Note: External protection is planned for future release.

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

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

One GbE port on each IP-50E is connected to an optical splitter. Both ports on each IP-50E unit belong to a LAG, with 100% distribution to the port connected to the optical splitter or external switch on each IP-50E unit. Traffic must be routed to an optical GbE port on each IP-50E unit. No forwarding cable is required.

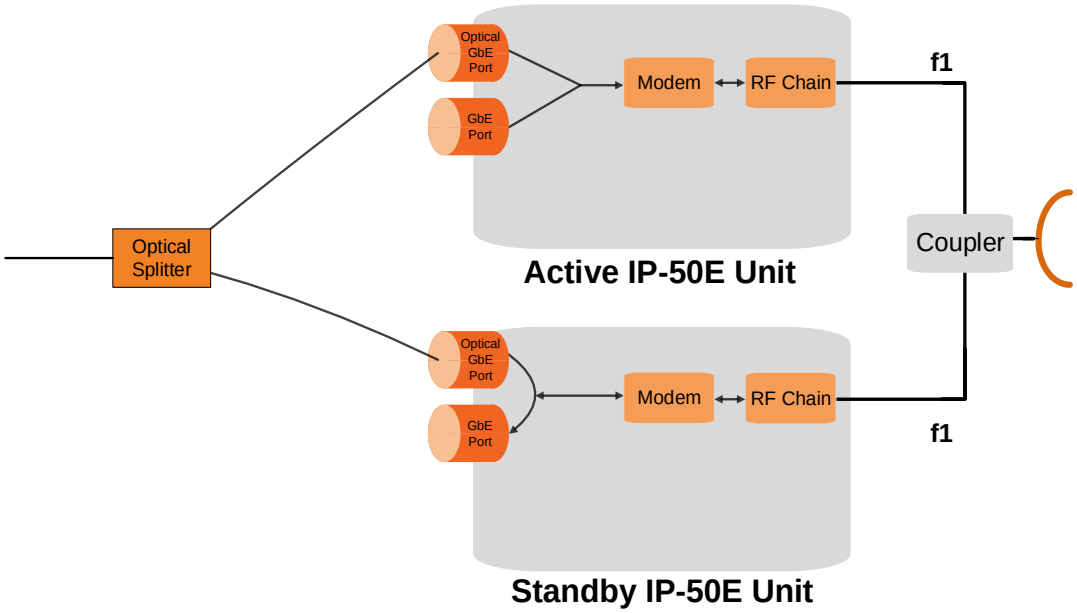


Figure 25: 1+1 HSB Protection

In a 1+1 HSB configuration, each IP-50E monitors its own core. If the active IP-50E detects a radio failure, it initiates a switchover to the standby IP-50E.

5.1.6.1 Management for External Protection

In an external protection configuration, the standby unit is managed via the active unit. A protection cable connects the two IP-50E units via their management ports. This cable is used for internal management. By placing an Ethernet splitter on the protection port, the user can add another cable for local management. A single IP address is used for both IP-50E units, to ensure that management is not lost in the event of switchover.

Note: If in-band management is used, no splitter is necessary.

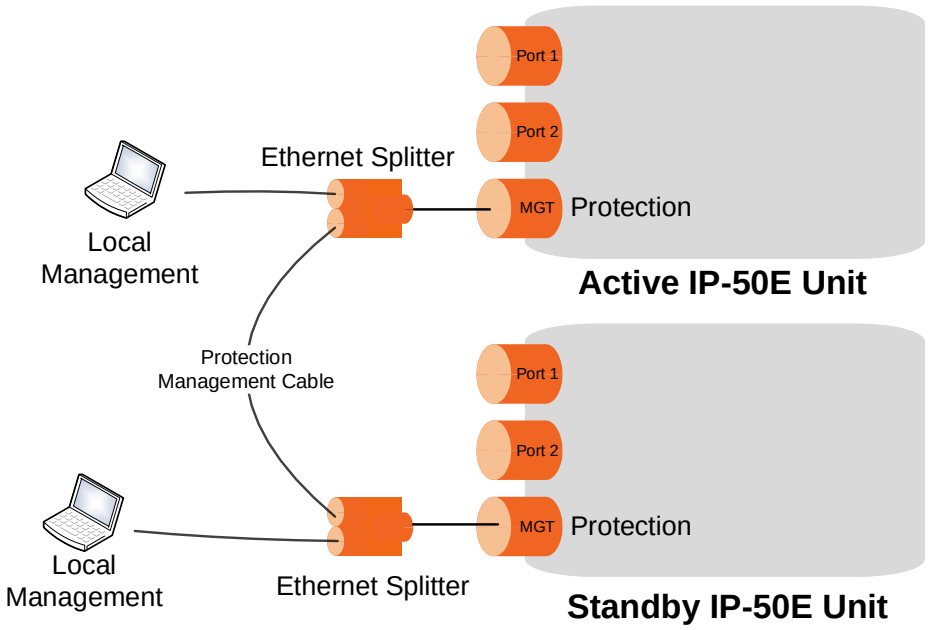


Figure 26: Internal and Local Management

The active and standby units must have the same configuration. The configuration of the active unit can be manually copied to the standby unit. Upon copying, both units are automatically reset. Therefore, it is important to ensure that the units are fully and properly configured when the system is initially brought into service.

5.1.6.2 Switchover

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

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

1 No mate/hardware failure
2 Lockout
3 Force switch
4 Radio/Signal Failures
5 Manual switch
6 Management port failure

5.1.7 ATPC

Note: ATPC is planned for future release.

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.

5.1.7.1 ATPC Override Timer

Note: ATPC Override Timer is planned for future release.

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

The following parameters can be configured:

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

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

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

5.1.8 Radio Signal Quality PMs

IP-50E 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 178. Users can also configure an alarm that is raised if the RSL falls beneath a user-defined threshold. See *RSL Threshold Alarm* on page 178.

5.1.9 Radio Utilization PMs

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

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

5.2 Ethernet Features

IP-50E'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-50E 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:

- Ethernet Services Overview
- IP-50E's Ethernet Capabilities
- Ethernet Service Model
- Ethernet Interfaces
- Quality of Service (QoS)
- Global Switch Configuration
- Automatic State Propagation and Link Loss Forwarding
- Adaptive Bandwidth Notification (EOAM)
- Network Resiliency
- OAM

5.2.1 Ethernet Services Overview

The IP-50E services model is premised on supporting the standard MEF services (MEF 6, 10), and builds upon this support by the use of very high granularity and flexibility. Operationally, the IP-50E Ethernet services model is designed to offer a rich feature set combined with simple and user-friendly configuration, enabling users to plan, activate, and maintain any packet-based network scenario.

This section first describes the basic Ethernet services model as it is defined by the MEF, then goes on to provide a basic overview of IP-50E's Ethernet services implementation.

The following figure illustrates the basic MEF Ethernet services model.

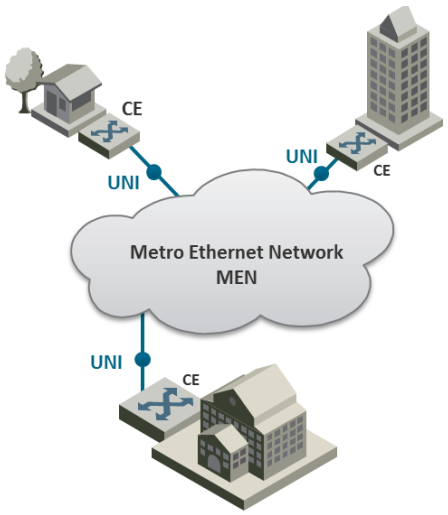


Figure 27: Basic Ethernet Service Model

In this illustration, the Ethernet service is conveyed by the Metro Ethernet Network (MEN) provider. Customer Equipment (CE) is connected to the network at the User Network Interface (UNI) using a standard Ethernet interface (10/100 Mbps, 1 Gbps). The CE may be a router, bridge/switch, or host (end system). A NI is defined as the demarcation point between the customer (subscriber) and provider network, with a standard IEEE 802.3 Ethernet PHY and MAC.

The services are defined from the point of view of the network's subscribers (users). Ethernet services can be supported over a variety of transport technologies and protocols in the MEN, such as SDH/SONET, Ethernet, ATM, MPLS, and GFP. However, from the user's perspective, the network connection at the user side of the UNI is only Ethernet.

5.2.1.1 EVC

Subscriber services extend from UNI to UNI. Connectivity between UNIs is defined as an Ethernet Virtual Connection (EVC), as shown in the following figure.

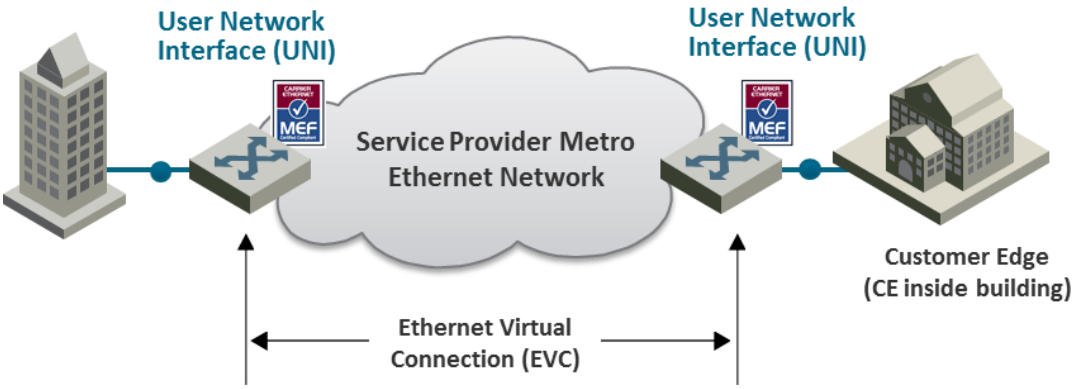


Figure 28: Ethernet Virtual Connection (EVC)

An EVC is defined by the MEF as an association of two or more UNIs that limits the exchange of service frames to UNIs in the Ethernet Virtual Connection. The EVC perform two main functions:

- Connects two or more customer sites (UNIs), enabling the transfer of Ethernet frames between them.
- Prevents data transfer involving customer sites that are not part of the same EVC. This feature enables the EVC to maintain a secure and private data channel.

A single UNI can support multiple EVCs via the Service Multiplexing attribute. An ingress service frame that is mapped to the EVC can be delivered to one or more of the UNIs in the EVC, other than the ingress UNI. It is vital to avoid delivery back to the ingress UNI, and to avoid delivery to a UNI that does not belong to the EVC. An EVC is always bi-directional in the sense that ingress service frames can originate at any UNI in an EVC.

Service frames must be delivered with the same Ethernet MAC address and frame structure that they had upon ingress to the service. In other words, the frame must be unchanged from source to destination, in contrast to routing in which headers are discarded. Based on these characteristics, an EVC can be used to form a Layer 2 private line or Virtual Private Network (VPN).

One or more VLANs can be mapped (bundled) to a single EVC.

The MEF has defined three types of EVCs:

- Point to Point EVC – Each EVC contains exactly two UNIs. The following figure shows two point-to-point EVCs connecting one site to two other sites.

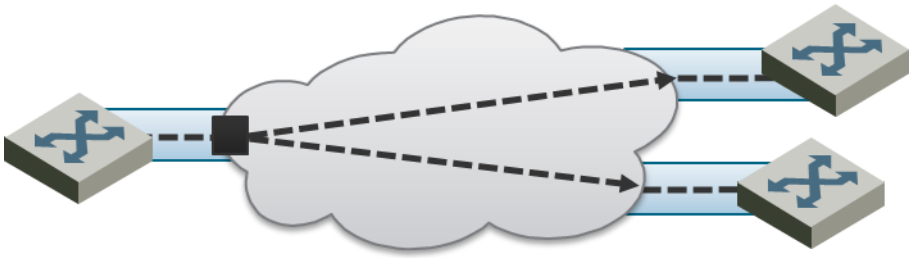


Figure 29: Point to Point EVC

- **Multipoint (Multipoint-to-Multipoint) EVC** – Each EVC contains two or more UNIs. In the figure below, three sites belong to a single Multipoint EVC and can forward Ethernet frames to each other.

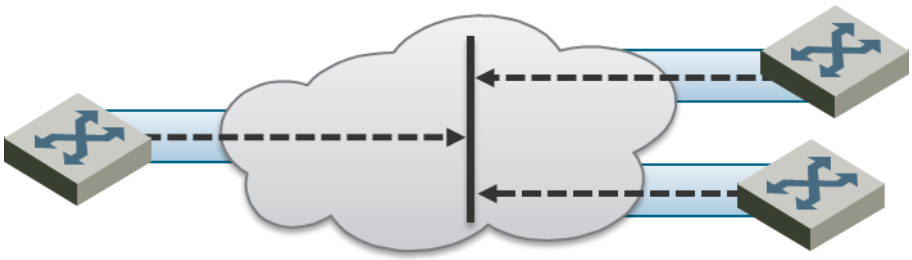


Figure 30: Multipoint to Multipoint EVC

- **Rooted Multipoint EVC** (Point-to-Multipoint) – Each EVC contains one or more UNIs, with one or more UNIs defined as Roots, and the others defined as Leaves. The Roots can forward frames to the Leaves. Leaves can only forward frames to the Roots, but not to other Leaves.

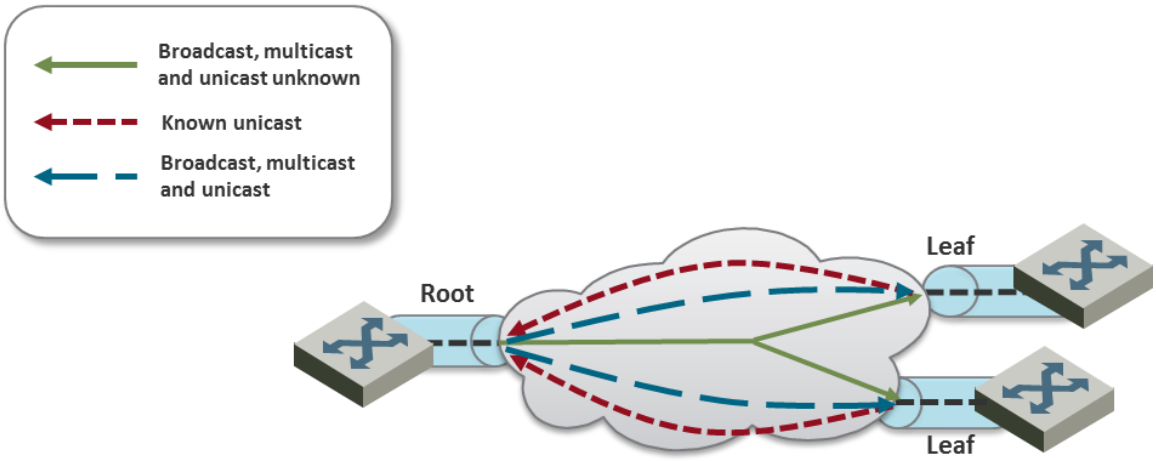


Figure 31: Rooted Multipoint EVC

In the IP-50E, an EVC is defined by either a VLAN or by Layer 1 connectivity (Pipe Mode).

5.2.1.2 Bandwidth Profile

The bandwidth profile (BW profile) is a set of traffic parameters that define the maximum limits of the customer's traffic.

At ingress, the bandwidth profile limits the traffic transmitted into the network:

- Each service frame is checked against the profile for compliance with the profile.
- Bandwidth profiles can be defined separately for each UNI (MEF 10.2).
- Service frames that comply with the bandwidth profile are forwarded.
- Service frames that do not comply with the bandwidth profile are dropped at the ingress interface.

The MEF has defined the following three bandwidth profile service attributes:

- Ingress BW profile per ingress UNI
- Ingress BW profile per EVC
- Ingress BW profile per CoS identifier

The BW profile service attribute consists of four traffic parameters:

- CIR (Committed Information Rate)
- CBS (Committed Burst Size)
- EIR (Excess Information Rate)
- EBS (Excess Burst Size)

Bandwidth profiles can be applied per UNI, per EVC at the UNI, or per CoS identifier for a specified EVC at the UNI.

The Color of the service frame is used to determine its bandwidth profile. If the service frame complies with the CIR and EIR defined in the bandwidth profile, it is marked Green. In this case, the average and maximum service frame rates are less than or equal to the CIR and CBS, respectively.

If the service frame does not comply with the CIR defined in the bandwidth profile, but does comply with the EIR and EBS, it is marked Yellow. In this case, the average service frame rate is greater than the CIR but less than the EIR, and the maximum service frame size is less than the EBS.

If the service frame fails to comply with both the CIR and the EIR defined in the bandwidth profile, it is marked Red and discarded.

In the IP-50E, bandwidth profiles are constructed using a full standardized TrTCM policer mechanism.

5.2.1.3 Ethernet Services Definitions

The MEF provides a model for defining Ethernet services. The purpose of the MEF model is to help subscribers better understand the variations among different types of Ethernet services. IP-50E supports a variety of service types defined by the MEF. All of these service types share some common attributes, but there are also differences as explained below.

Ethernet service types are generic constructs used to create a broad range of services. Each Ethernet service type has a set of Ethernet service attributes that define the characteristics of the service. These Ethernet service attributes in turn are associated with a set of parameters that provide various options for the various service attributes.

Figure 32: MEF Ethernet Services Definition Framework

The MEF defines three generic Ethernet service type constructs, including their associated service attributes and parameters:

- Ethernet Line (E-Line)
- Ethernet LAN (E-LAN)
- Ethernet Tree (E-Tree)

Multiple Ethernet services are defined for each of the three generic Ethernet service types. These services are differentiated by the method for service identification used at the UNIs. Services using All-to-One Bundling UNIs (port-based) are referred to as “Private” services, while services using Service Multiplexed (VLAN-based) UNIs are referred to as “Virtual Private” services. This relationship is shown in the following table.

Table 10: MEF-Defined Ethernet Service Types

Service Type	Port Based (All to One Bundling)	VLAN-BASED (EVC identified by VLAN ID)
E-Line (Point-to-Point EVC)	Ethernet Private Line (EPL)	Ethernet Virtual Private Line (EVPL)
E-LAN (Multipoint-to-Multipoint EVC)	Ethernet Private LAN (EP-LAN)	Ethernet Virtual Private LAN (EVP-LAN)
E-Tree (Rooted Multipoint EVC)	Ethernet Private Tree (EP-Tree)	Ethernet Virtual Private Tree (EVP-Tree)

All-to-One Bundling refers to a UNI attribute in which all Customer Edge VLAN IDs (CE-VLAN IDs) entering the service via the UNI are associated with a single EVC.

Bundling refers to a UNI attribute in which more than one CE-VLAN ID can be associated with an EVC.

To fully specify an Ethernet service, additional service attributes must be defined in addition to the UNI and EVC service attributes. Theses service attributes can be grouped under the following categories:

- Ethernet physical interfaces
- Traffic parameters
- Performance parameters
- Class of service
- Service frame delivery
- VLAN tag support
- Service multiplexing
- Bundling
- Security filters

E-Line Service

The Ethernet line service (E-Line service) provides a point-to-point Ethernet Virtual Connection (EVC) between two UNIs. The E-Line service type can be used to create a broad range of Ethernet point-to-point services and to maintain the necessary connectivity. In its simplest form, an E-Line service type can provide symmetrical bandwidth for data sent in either direction with no performance assurances, e.g., best effort service between two FE UNIs. In more sophisticated forms, an E-Line service type can provide connectivity between two UNIs with different line rates and can be defined with performance assurances such as CIR with an associated CBS, EIR with an associated EBS, delay, delay variation, loss, and availability for a given Class of Service (CoS) instance. Service multiplexing can occur at one or both UNIs in the EVC. For example, more than one point-to-point EVC can be offered on the same physical port at one or both of the UNIs.

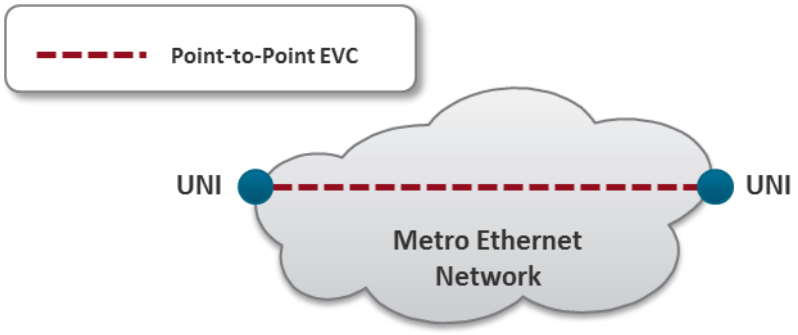


Figure 33: E-Line Service Type Using Point-to-Point EVC

Ethernet Private Line Service

An Ethernet Private Line (EPL) service is specified using an E-Line Service type. An EPL service uses a point-to-point EVC between two UNIs and provides a high degree of transparency for service frames between the UNIs that it interconnects such that the service frame's header and payload are identical at both the source and destination UNI when the service frame is delivered (L1 service). A dedicated UNI (physical interface) is used for the service and service multiplexing is not allowed. All service frames are mapped to a single EVC at the UNI. In cases where the EVC speed is less than the UNI speed, the CE is expected to shape traffic to the ingress bandwidth profile of the service to prevent the traffic from being discarded by the service. The EPL is a port-based service, with a single EVC across dedicated UNIs providing site-to-site connectivity. EPL is the most popular Ethernet service type due to its simplicity, and is used in diverse applications such as replacing a TDM private line.

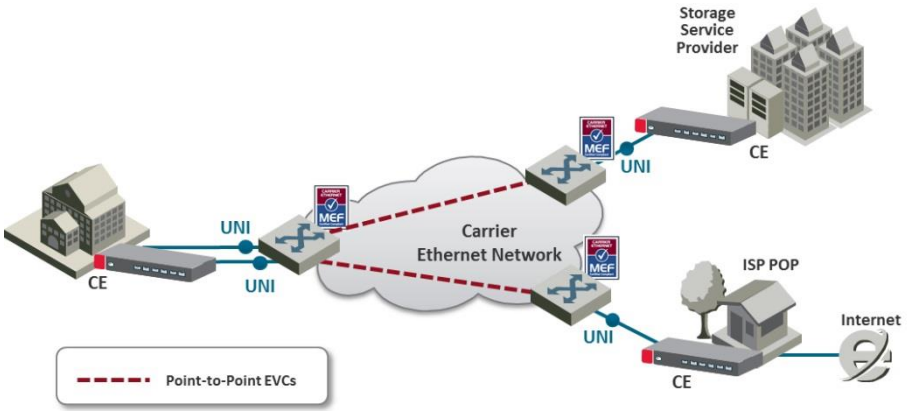


Figure 34: EPL Application Example

Ethernet Virtual Private Line Service

An Ethernet Virtual Private Line (EVPL) is created using an E-Line service type. An EVPL can be used to create services similar to EPL services. However, several characteristics differ between EPL and EVPL services.

First, an EVPL provides for service multiplexing at the UNI, which means it enables multiple EVCs to be delivered to customer premises over a single physical connection (UNI). In contrast, an EPL only enables a single service to be delivered over a single physical connection.

Second, the degree of transparency for service frames is lower in an EVPL than in an EPL.

Since service multiplexing is permitted in EVPL services, some service frames may be sent to one EVC while others may be sent to other EVCs. EVPL services can be used to replace Frame Relay and ATM L2 VPN services, in order to deliver higher bandwidth, end-to-end services.

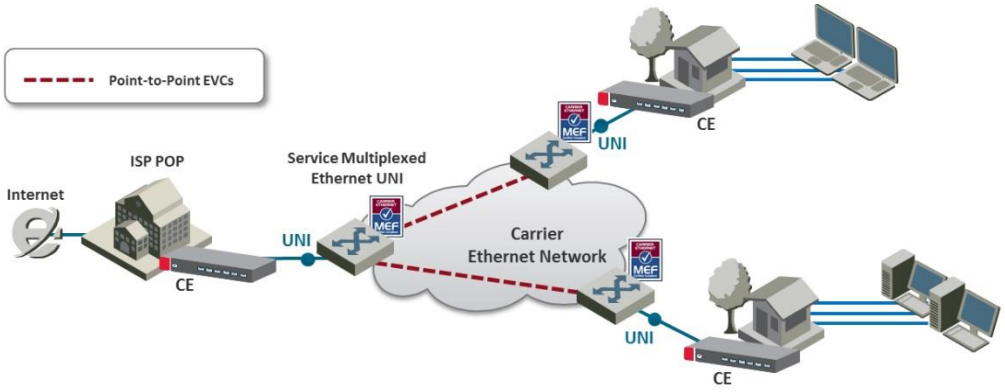


Figure 35: EVPL Application Example

E-LAN Service

The E-LAN service type is based on Multipoint to Multipoint EVCs, and provides multipoint connectivity by connecting two or more UNIs. Each site (UNI) is connected to a multipoint EVC, and customer frames sent from one UNI can be received at one or more UNIs. If additional sites are added, they can be connected to the same multipoint EVC, simplifying the service activation process. Logically, from the point of view of a customer using an E-LAN service, the MEN can be viewed as a LAN.

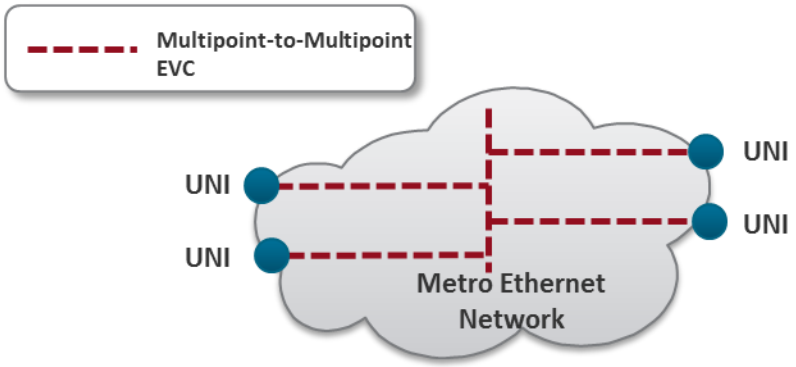


Figure 36: E-LAN Service Type Using Multipoint-to-Multipoint EVC

The E-LAN service type can be used to create a broad range of services. In its basic form, an E-LAN service can provide a best effort service with no performance assurances between the UNIs. In more sophisticated forms, an E-LAN service type can be defined with performance assurances such as CIR with an associated CBS, EIR with an associated EBS, delay, delay variation, loss, and availability for a given CoS instance.

For an E-LAN service type, service multiplexing may occur at none, one, or more than one of the UNIs in the EVC. For example, an E-LAN service type (Multipoint-to-Multipoint EVC) and an E-Line service type (Point-to-Point EVC) can be service multiplexed at the same UNI. In such a case, the E-LAN service type can be used to interconnect other customer sites while the E-Line service type is used to connect to the Internet, with both services offered via service multiplexing at the same UNI.

E-LAN services can simplify the interconnection among a large number of sites, in comparison to hub/mesh topologies implemented using point-to-point networking technologies such as Frame Relay and ATM.

For example, consider a point-to-point network configuration implemented using E-Line services. If a new site (UNI) is added, it is necessary to add a new, separate EVC to all of the other sites in order to enable the new UNI to communicate with the other UNIs, as shown in the following figure.

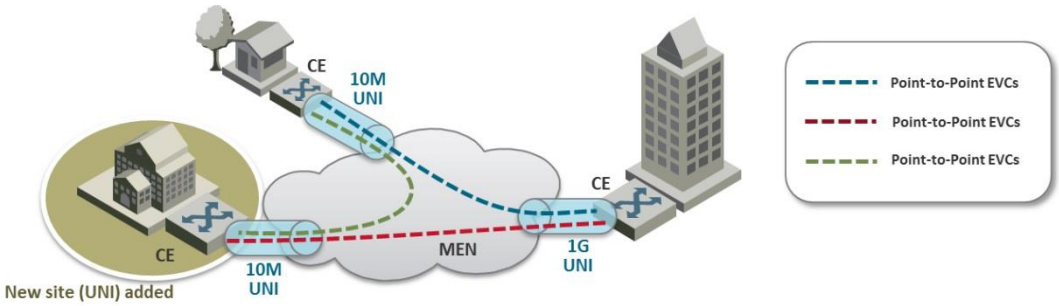


Figure 37: Adding a Site Using an E-Line Service

In contrast, when using an E-LAN service, it is only necessary to add the new UNI to the multipoint EVC. No additional EVCs are required, since the E-LAN service uses a multipoint to multipoint EVC that enables the new UNI to communicate with each of the others UNIs. Only one EVC is required to achieve multi-site connectivity, as shown in the following figure.

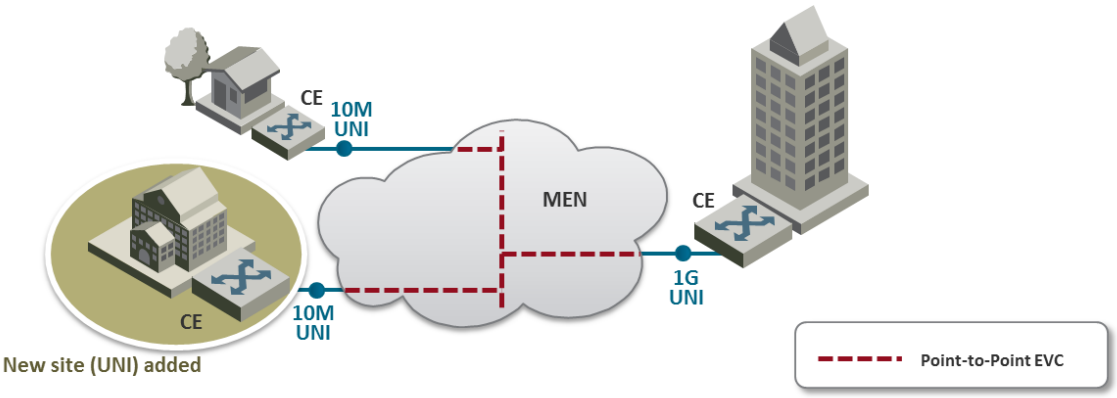


Figure 38: Adding a Site Using an E-LAN Service

The E-LAN service type can be used to create a broad range of services, such as private LAN and virtual private LAN services.

Ethernet Private LAN Service

It is often desirable to interconnect multiple sites using a Local Area Network (LAN) protocol model and have equivalent performance and access to resources such as servers and storage. Customers commonly require a highly transparent service that connects multiple UNIs. The Ethernet Private LAN (EP-LAN) service is defined with this in mind, using the E-LAN service type. The EP-LAN is a Layer 2 service in which each UNI is dedicated to the EP-LAN service. A typical use case for EP-LAN services is Transparent LAN.

The following figure shows an example of an EP-LAN service in which the service is defined to provide Customer Edge VLAN (CE-VLAN) tag preservation and tunneling for key Layer 2 control protocols. Customers can use this service to configure VLANs across the sites without the need to coordinate with the service provider. Each interface is configured for All-to-One Bundling, which enables the EP-LAN service to support CE-VLAN ID preservation. In addition, EP-LAN supports CE-VLAN CoS preservation.

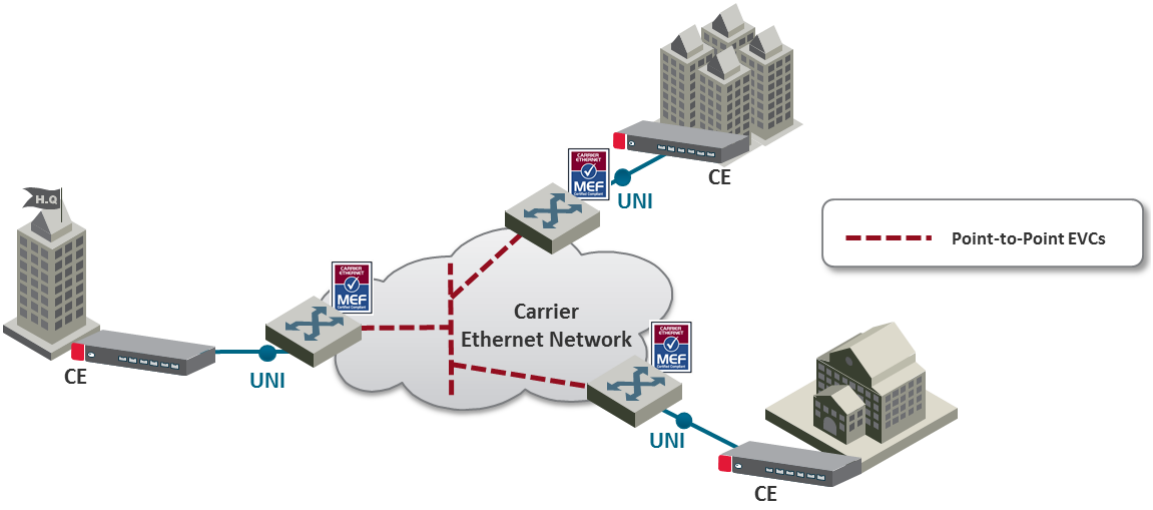


Figure 39: MEF Ethernet Private LAN Example

Ethernet Virtual Private LAN Service

Customers often use an E-LAN service type to connect their UNIs in an MEN, while at the same time accessing other services from one or more of those UNIs. For example, a customer might want to access a public or private IP service from a UNI at the customer site that is also used to provide E-LAN service among the customer's several metro locations. The Ethernet Virtual Private LAN (EVP-LAN) service is defined to address this need. EVP-LAN is actually a combination of EVPL and E-LAN.

Bundling can be used on the UNIs in the Multipoint-to-Multipoint EVC, but is not mandatory. As such, CE-VLAN tag preservation and tunneling of certain Layer 2 control protocols may or may not be provided. Service multiplexing is allowed on each UNI. A typical use case would be to provide Internet access a corporate VPN via one UNI.

The following figure provides an example of an EVP-LAN service.

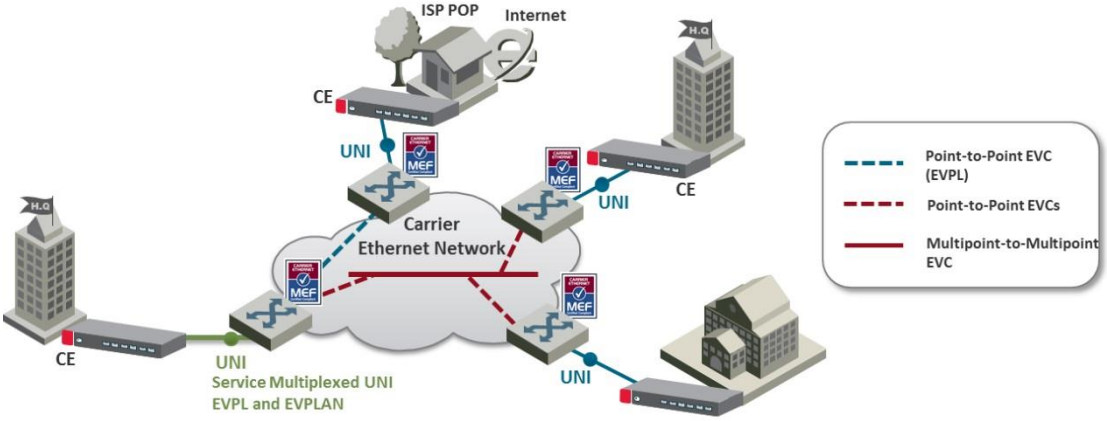


Figure 40: MEF Ethernet Virtual Private LAN Example

E-Tree Service

The E-Tree service type is an Ethernet service type that is based on Rooted-Multipoint EVCs. In its basic form, an E-Tree service can provide a single Root for multiple Leaf UNIs. Each Leaf UNI can exchange data with only the Root UNI. A service frame sent from one Leaf UNI cannot be delivered to another Leaf UNI. This service can be particularly useful for Internet access, and video-over-IP applications such as multicast/broadcast packet video. One or more CoS values can be associated with an E-Tree service.

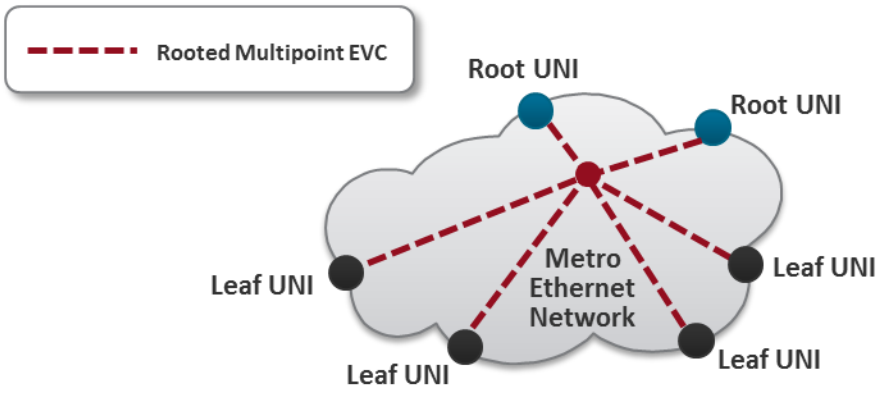


Figure 41: E-Tree Service Type Using Rooted-Multipoint EVC

Two or more Root UNIs can be supported in advanced forms of the E-Tree service type. In this scenario, each Leaf UNI can exchange data only with the Root UNIs. The Root UNIs can communicate with each other. Redundant access to the Root can also be provided, effectively allowing for enhanced service reliability and flexibility.

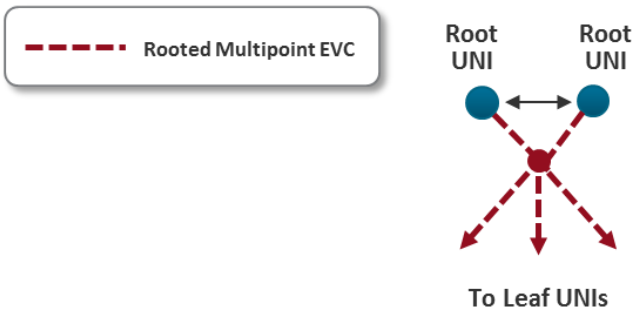


Figure 42: E-Tree Service Type Using Multiple Roots

Service multiplexing is optional and may occur on any combination of UNIs in the EVC. For example, an E-Tree service type using a Rooted-Multipoint EVC, and an E-Line service type using a Point-to-Point EVC, can be service multiplexed on the same UNI. In this example, the E-Tree service type can be used to support a specific application at the Subscriber UNI, e.g., ISP access to redundant PoPs (multiple Roots at ISP PoPs), while the E-Line Service type is used to connect to another enterprise site with a Point-to-Point EVC.

Ethernet Private Tree Service

The Ethernet Private Tree service (EP-Tree) is designed to supply the flexibility for configuring multiple sites so that the services are distributed from a centralized site, or from a few centralized sites. In this setup, the centralized site or sites are designed as Roots, while the remaining sites are designated as Leaves. CE-VLAN tags are preserved and key Layer 2 control protocols are tunneled. The advantage of such a configuration is that the customer can configure VLANs across its sites without the need to coordinate with the service provider. Each interface is configured for All-to-One Bundling, which means that EP-Tree services support CE-VLAN ID preservation. EP-Tree also supports CE-VLAN CoS preservation. EP-Tree requires dedication of the UNIs to the single EP-Tree service.

The following figure provides an example of an EP-Tree service.

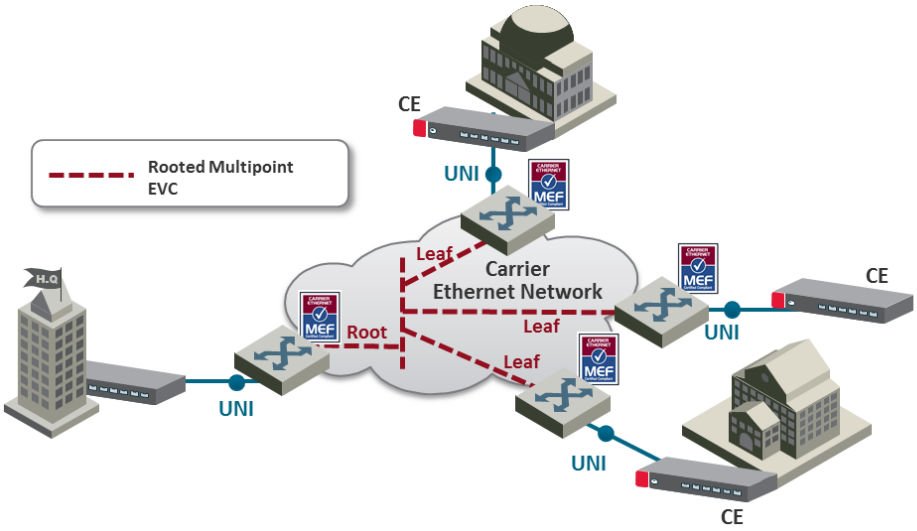


Figure 43: MEF Ethernet Private Tree Example

Ethernet Virtual Private Tree Service

In order to access several applications and services from well-defined access points (Root), the UNIs are attached to the service in a Rooted Multipoint connection. Customer UNIs can also support other services, such as EVPL and EVP-LAN services. An EVP-Tree service is used in such cases. Bundling can be used on the UNIs in the Rooted Multipoint EVC, but it is not mandatory. As such, CE-VLAN tag preservation and tunneling of certain Layer 2 Control Protocols may or may not be provided. EVP-Tree enables each UNI to support multiple services. A good example would be a customer that has an EVP-LAN service providing data connectivity among three UNIs, while using an EVP-Tree service to provide video broadcast from a video hub location. The following figure provides an example of a Virtual Private Tree service.

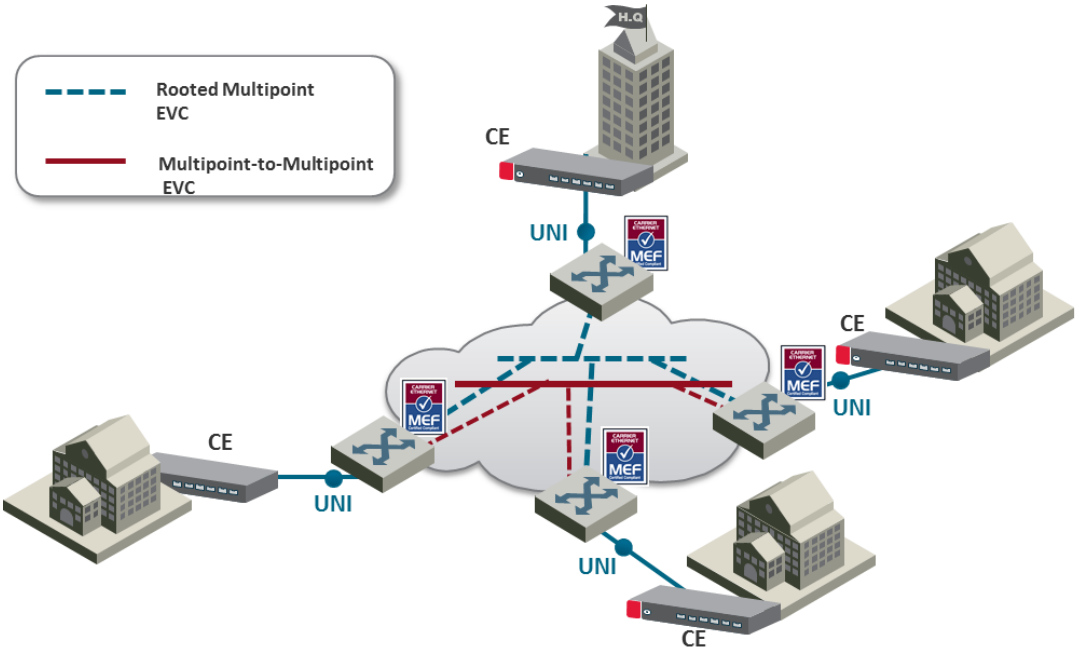


Figure 44: Ethernet Virtual Private Tree Example

IP-50E enables network connectivity for **Mobile Backhaul** cellular infrastructure, fixed networks, private networks and enterprises.

Mobile Backhaul refers to the network between the Base Station sites and the Network Controller/Gateway sites for all generations of mobile technologies. Mobile equipment and networks with ETH service layer functions can support MEF Carrier Ethernet services using the service attributes defined by the MEF.

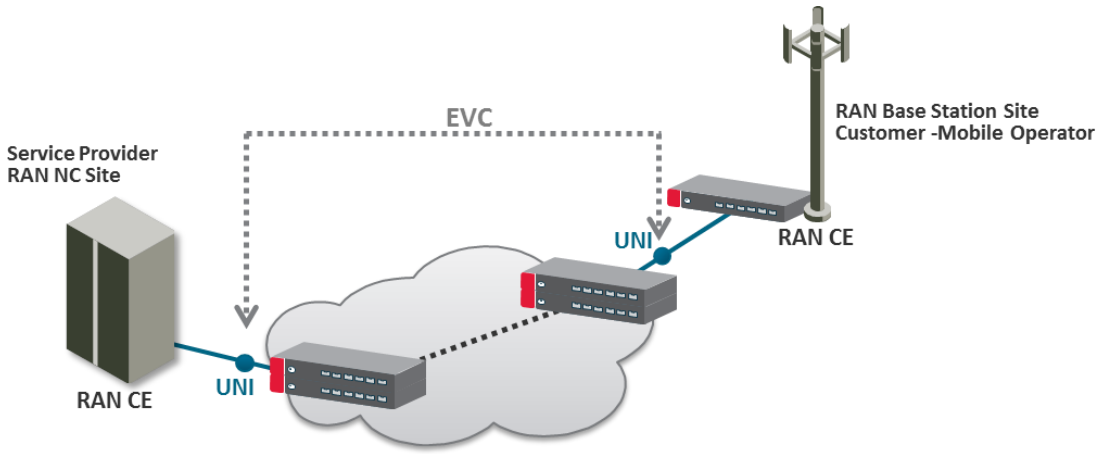


Figure 45: Mobile Backhaul Reference Model

The IP-50E services concept is purpose built to support the standard MEF services for mobile backhaul (MEF 22, mobile backhaul implementation agreement), as an addition to the baseline definition of MEF Services (MEF 6) using service attributes (as well as in MEF 10). E-Line and E-LAN services are well defined as the standard services.

5.2.1.4 IP-50E Universal Packet Backhaul Services Core

IP-50E addresses the customer demand for multiple services of any of the aforementioned types (EPL, EVPL, EP –LAN, EVP-LAN, EP-Tree, and EVP-Tree) through its rich service model capabilities and flexible integrated switch application. Additional Layer 1 point-based services are supported as well, as explained in more detail below.

Services support in the mobile backhaul environment is provided using the IP-50E services core, which is structured around the building blocks shown in the figure below. IP-50E provides rich and secure packet backhaul services over any transport type with unified, simple, and error-free operation.

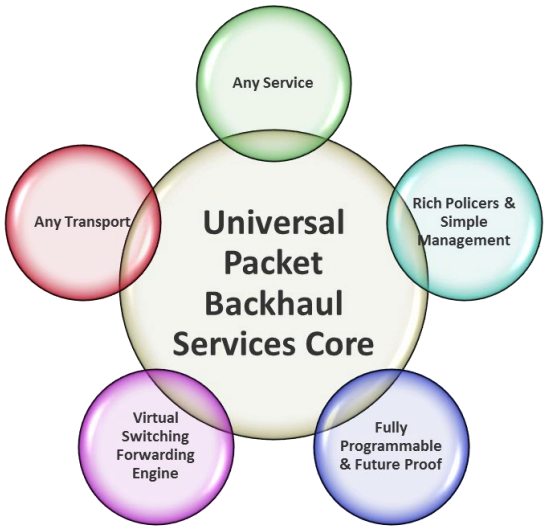


Figure 46: Packet Service Core Building Blocks

Any Service

- Ethernet services (EVCs)
  - E-Line (Point-to-Point)
  - E-LAN (Multipoint)
- Port based (Smart Pipe) services

Any Transport

- Native Ethernet (802.1Q/Q-in-Q)
- Any topology and any mix of radio and fiber interfaces
- Seamless interworking with any optical network (NG-SDH, packet optical transport, IP/MPLS service/VPN routers)

Virtual Switching/Forwarding Engine

- Clear distinction between user facing service interfaces (UNI) and intra-network interfaces
- Fully flexible C-VLAN and S-VLAN encapsulation (classification/preservation/ translation)
- Improved security/isolation without limiting C-VLAN reuse by different customers
- Per-service MAC learning with 64K MAC addresses support

Fully Programmable and Future-Proof

- Network-processor-based services core
- Ready today to support emerging and future standards and networking protocols

Rich Policies and Tools with Unified and Simplified Management

- Personalized QoS (H-QoS)
- Superb service OAM (CFM, EFM, PM)
- Carrier-grade service resiliency (G.8032)

5.2.2 IP-50E's Ethernet Capabilities

IP-50E 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-50E's services core includes a rich set of tools that includes:

- Service-based Quality of Service (QoS).
- Service OAM, including granular PMs, and service activation.
- Carrier-grade service resiliency using G.8032

The following are IP-50E'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
- All service types:
  - Multipoint (E-LAN)
  - Point-to-Point (E-Line)
  - Smart Pipe
  - Management
- 64K MAC learning table, with separate learning per service (including limiters)
- Flexible transport and encapsulation via 802.1q and 802.1ad (Q-in-Q), with tag manipulation possible at ingress and egress
- High precision, flexible frame synchronization solution combining SyncE and 1588v2
- Hierarchical QoS with 8,192 service level queues, deep buffering, hierarchical scheduling via WFQ and Strict priority, and shaping at each level
- 1K hierarchical two-rate three-Color policers
  - Port based – Unicast, Multicast, Broadcast, Ethertype
  - Service-based
  - CoS-based
- Up to four link aggregation groups (LAG)
  - Hashing based on L2, L3, and MPLS
- Enhanced <50msec network level resiliency (G.8032) for ring/mesh support

5.2.3 Ethernet Service Model

IP-50E'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-50E'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).

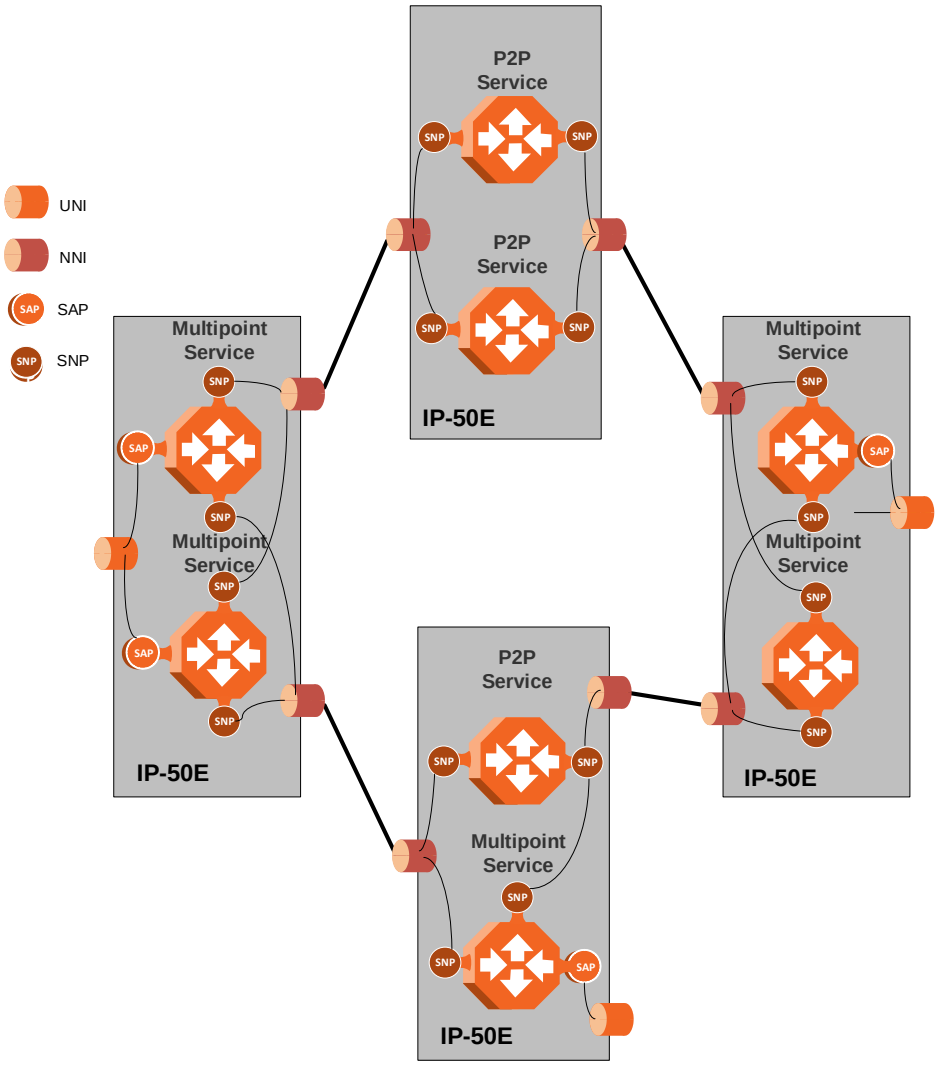


Figure 47: IP-50E Services Model

The IP-50E 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.

Users can define up to 1024 services on a single IP-50E. 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-50E 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-50E services model, with traffic entering and leaving the network element. IP-50E'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.

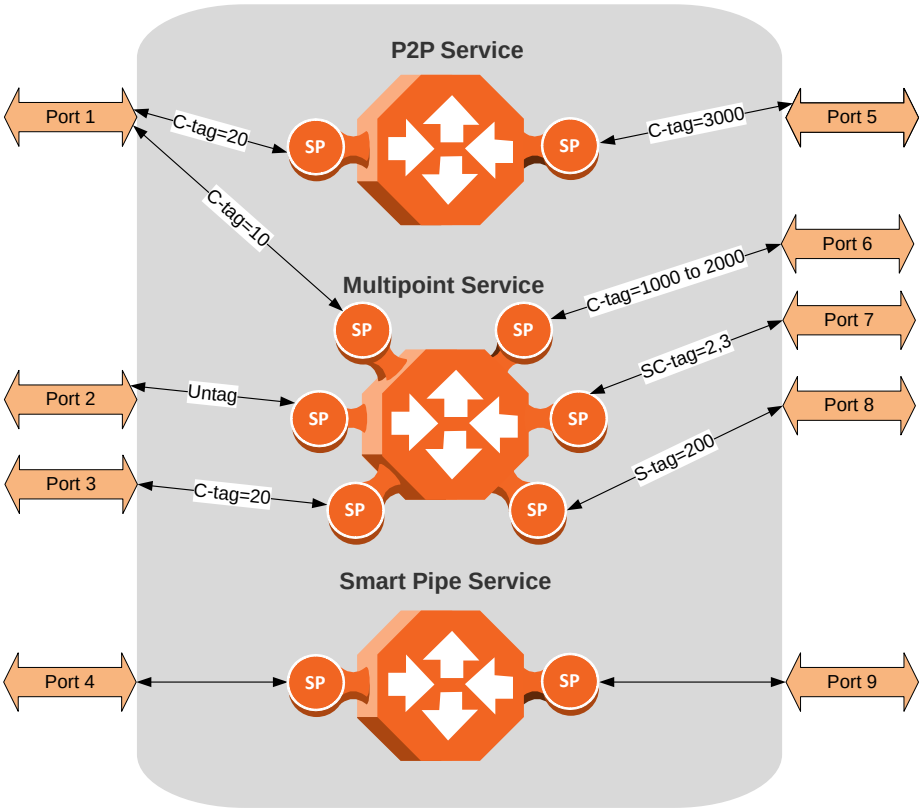


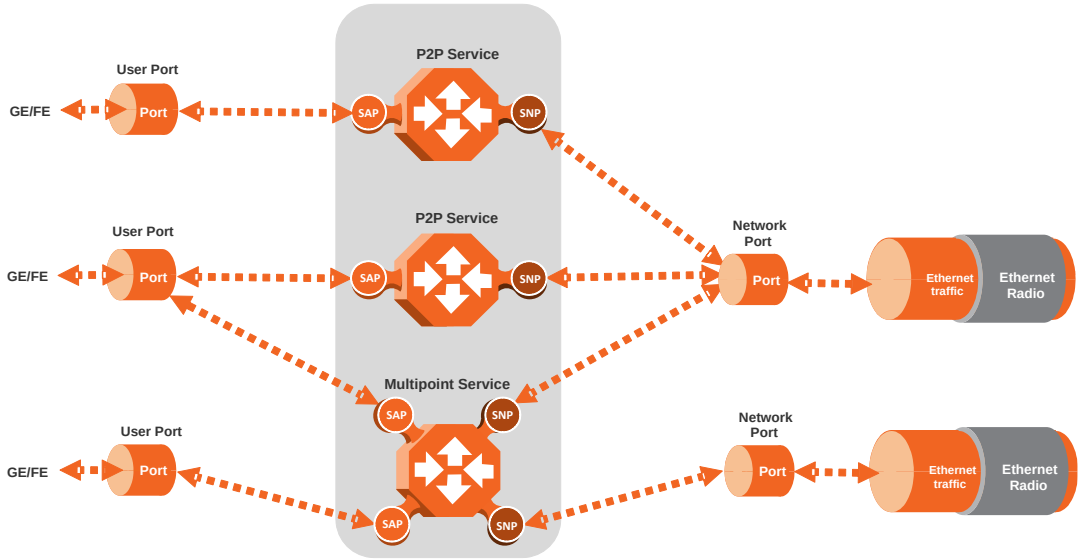
Figure 48: IP-50E Services Core

5.2.3.1 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-50E.
- 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. Services include a MAC entry table of up to 65,536 entries, with a global aging timer and a maximum learning limiter that are configurable per-service.



Service Types Figure 49: IP-50E Services Flow

IP-50E 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.

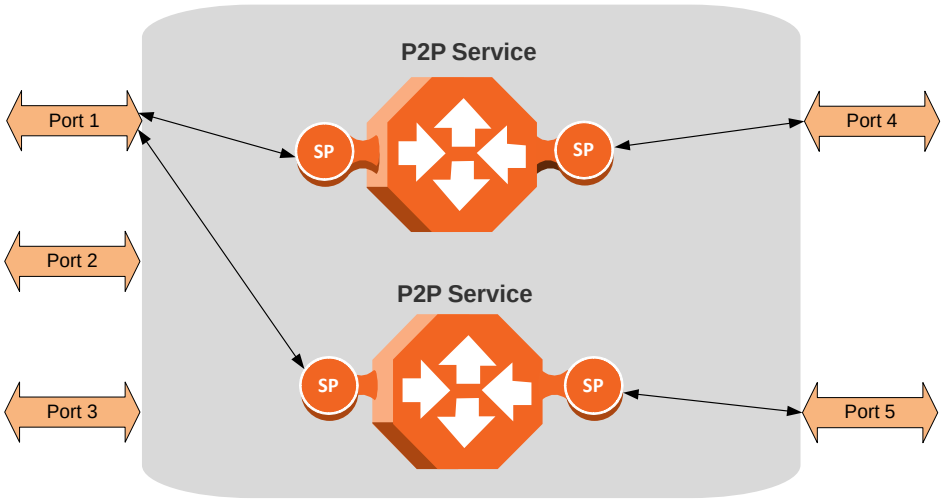


Figure 50: Point-to-Point Service

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

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.

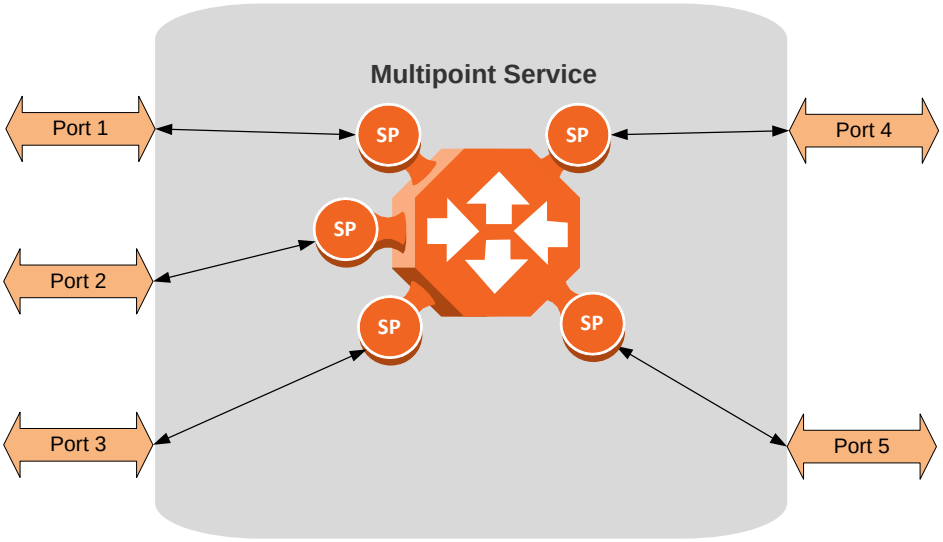


Figure 51: Multipoint Service

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-50E can learn up to 65,536 Ethernet source MAC addresses. IP-50E performs learning per service in order to enable the use of 1024 virtual bridges in the network element. 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 service in granularity of 16 entries.

When a frame arrives via a specific service point, the learning mechanism checks the MAC forwarding table for the service to which the service point belongs to determine whether that 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.

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 11: 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.[8]

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

[8] Resiliency protocols are planned for future release.

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.

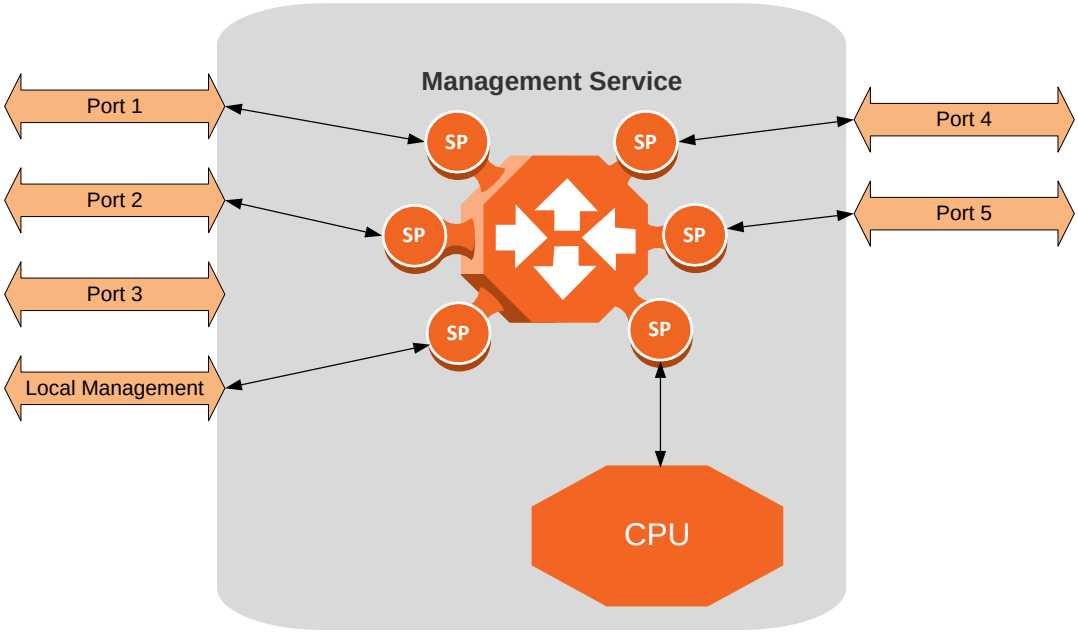


Figure 52: Management Service

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-50E 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.
- **Maximum Dynamic MAC Address Learning per Service** – Defines the maximum number of dynamic Ethernet MAC address that the service can learn. This parameter is configured with a granularity of 16, and only applies to dynamic, not static, MAC addresses.
- **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 65,536 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-50E's hierarchical classification mechanism, refer to *Classification* on page 113.
- **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.

5.2.3.2 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-50E 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.

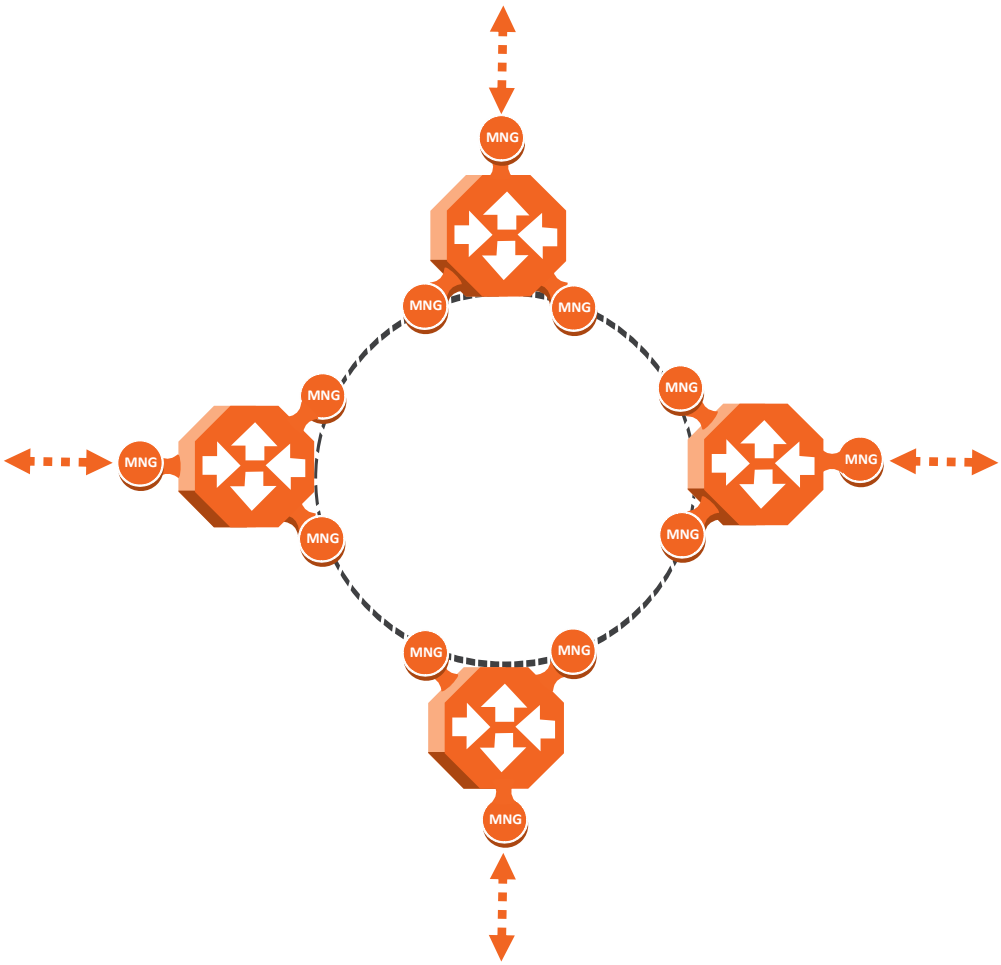


Figure 53: Management Service and its Service Points

- **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.

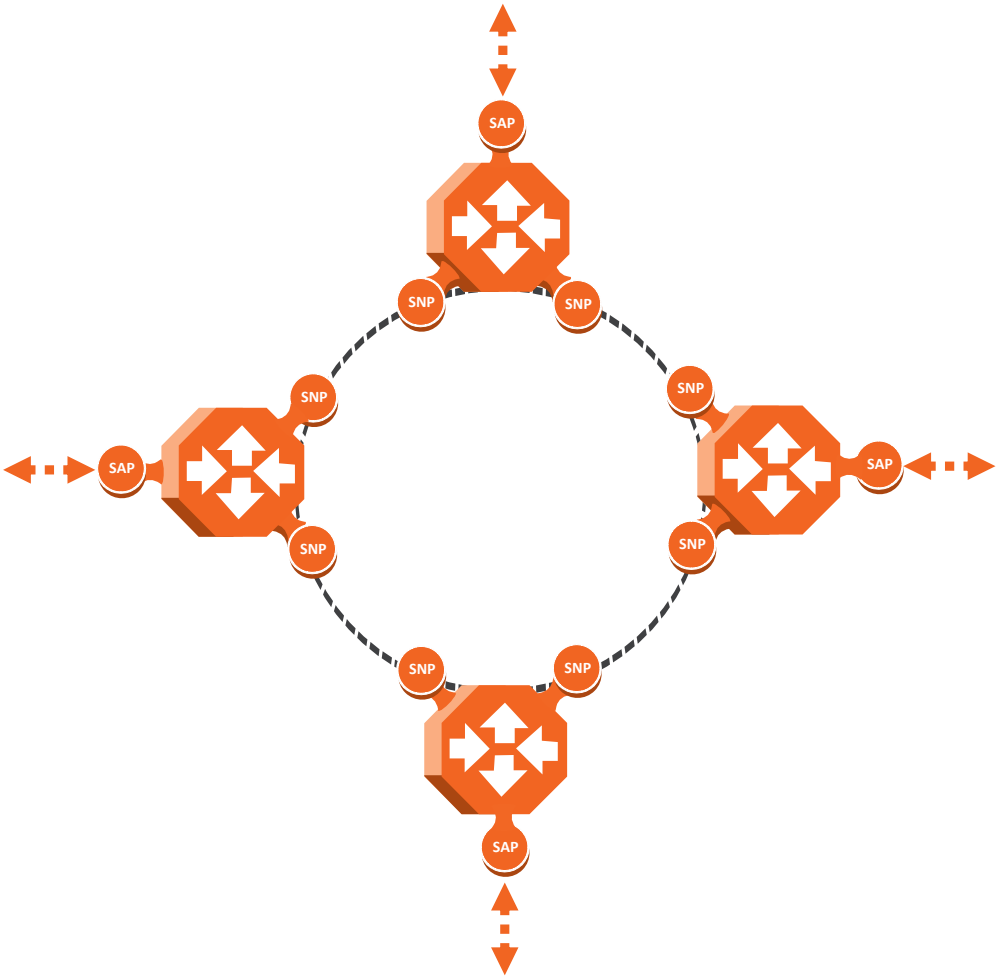


Figure 54: SAPs and SNPs

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

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

Figure 55: 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. A Smart Pipe is also used, to provide connectivity between elements that require port-based connectivity.

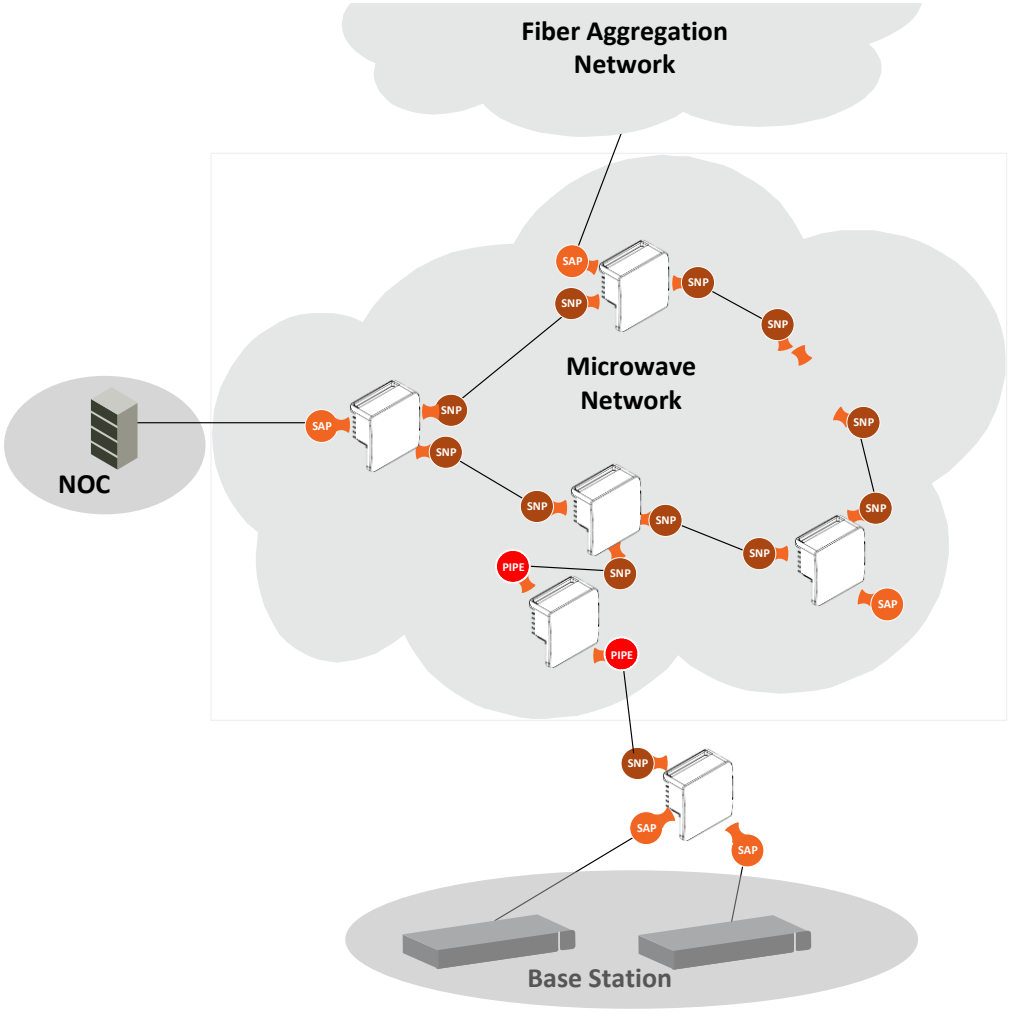


Figure 56: SAP, SNP and Pipe Service Points in a Microwave Network

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

Table 12: Service Point Types per Service Type

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

Service Point Classification

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

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

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

SAP Classification

SAPs can be used with the following Attached Interface Types:

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

SNP classification

SNPs can be used with the following Attached Interface Types:

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

PIPE classification

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

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

MNG classification

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

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

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

Table 13: Service Point Types that can Co-Exist on the Same Interface

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

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

.

Table 14: 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 and MAC address learning.
- **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:

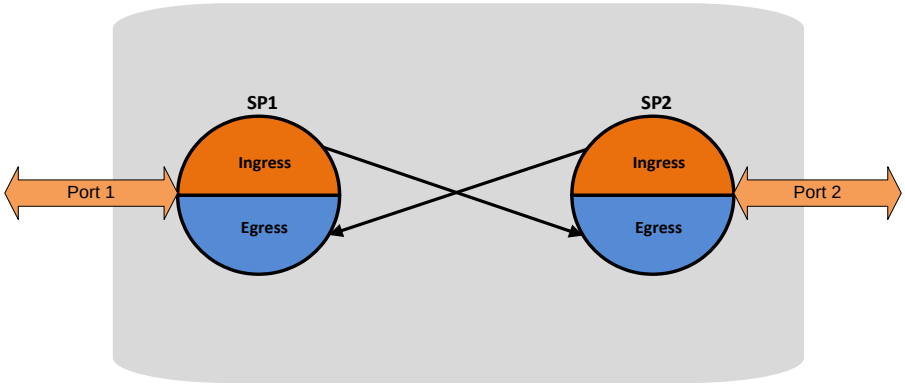


Figure 57: Service Path Relationship on Point-to-Point Service Path

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.
- **Token Bucket Profile** – This attribute can be used to attach a rate meter profile to the service point. Permitted values are 1– 250.
- **CoS Token Bucket Profile** – This attribute can be used to attach a rate meter profile to the service point at the CoS level. Users can define a rate meter for each of the eight CoS values of the service point. Permitted values are 1-250 for CoS 0–7.
- **CoS Token Bucket Admin** – Enables or disables the rate meter at the service point CoS level.

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 and the DEI or CFI bit to a defined CoS and Color value.
- **Service Bundle ID** – This attribute can be used to assign one of the available service bundles from the H-QoS hierarchy queues to the service point. This enables users to personalize the QoS egress path. For details, refer to *Standard QoS and Hierarchical* QoS (H-QoS)on page 126.

5.2.4 Ethernet Interfaces

The IP-50E 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-50E 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.

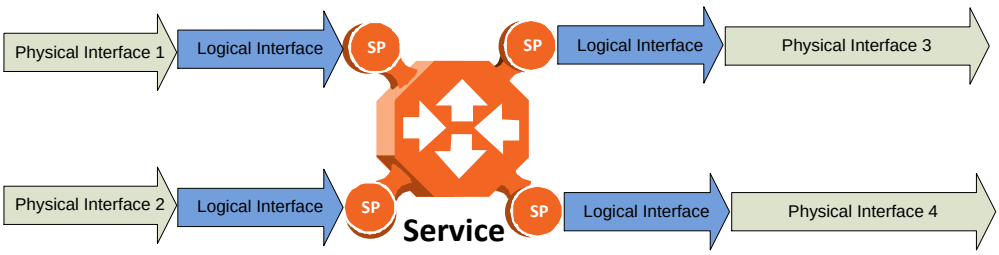


Figure 58: Physical and Logical Interfaces

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-50E 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.

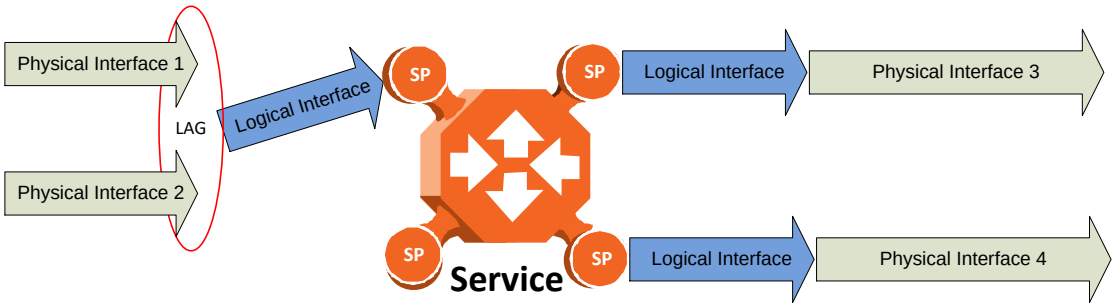


Figure 59: Grouped Interfaces as a Single Logical Interface on Ingress Side

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.

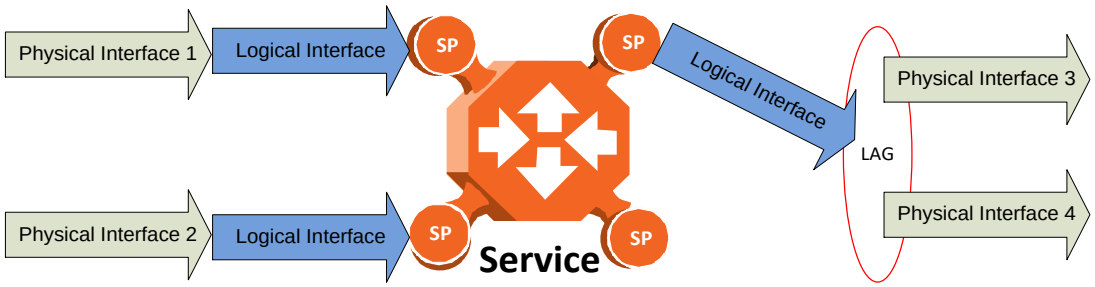


Figure 60: Grouped Interfaces as a Single Logical Interface on Egress Side

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

5.2.4.1 Physical Interfaces

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

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

Physical Interface Attributes

The following physical interface parameters can be configured by users:

- **Admin** – Enables or disables the physical interface. This attribute is set via the Interface Manager section of the Web EMS.
- **Auto Negotiation** – Enables or disables auto-negotiation on the physical interface. Auto Negotiation is always off for radio and SFP interfaces.
- **Speed and Duplex** – The physical interface speed and duplex mode. Permitted values are:
  - **Ethernet RJ-45 interfaces**: 100Mbps and 1000Mbps FD.
  - **Ethernet SFP interfaces**: Only 1000Mbps FD is supported
  - **Ethernet SFP+ interface**: Only 10000Mbps FD is supported
  - **Ethernet QSFP interface:** 1000Mbps and 10000Mbps FD are supported
  - **Radio interfaces**: The parameter is read-only and set by the system to 10G FD.
- **Flow Control** – The physical port flow control capability. Permitted values are: Symmetrical Pause and/or Asymmetrical Pause. This parameter is only relevant in Full Duplex mode.
- **IFG** – The physical port Inter-frame gap. Although users can modify the IFG field length, it is strongly recommended not to modify the default value of 12 bytes without a thorough understanding of how the modification will impact traffic. Permitted values are 6 to 15 bytes.
- **Preamble** – The physical port preamble value. Although users can modify the preamble field length, it is strongly recommended not to modify the default values of 8 bytes without a thorough understanding of how the modification will impact traffic. Permitted values are 6 to 15 bytes.
- **Interface description** – A text description of the interface, up to 40 characters.

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

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

Ethernet Statistics

The IP-50E 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 frame transmitted
- FCS error frames
- Oversized frames – frames with length > 1518 bytes (1522 bytes for VLAN-tagged frames) without errors
- Undersized frames (good only)
- Fragments frames (undersized bad)
- Jabber frames – frames with length > 1518 bytes (1522 for VLAN-tagged frames) with 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
- Frames with length 1519-1522 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 frame received
- FCS error frames
- Counts oversized frames – frames with length > 1518 bytes (1522 bytes for VLAN-tagged frames) without errors *and* frames with length > MAX_LEN without errors
- Undersized frames (good only)
- Fragments frames (undersized bad)
- Counts jabber frames – frames with length > 1518 bytes (1522 for VLAN-tagged frames) with 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
- VLAN-tagged frames with length 1519-1522 bytes, good or bad

5.2.4.2 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 radio 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.

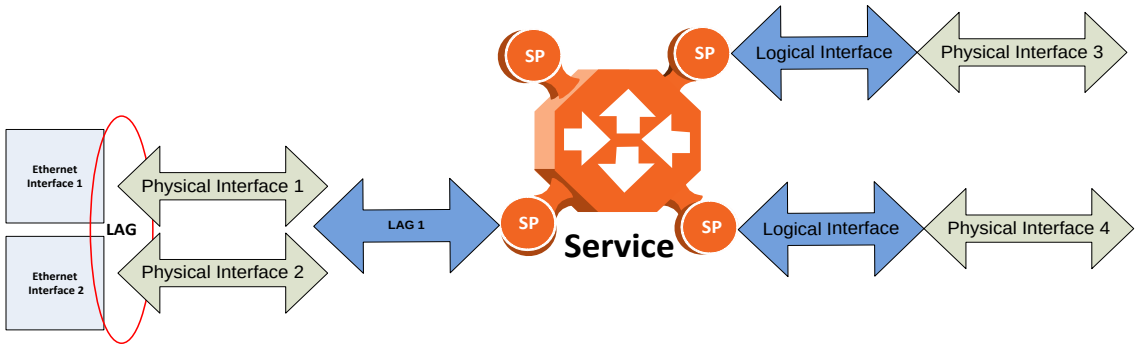


Figure 61: Relationship of Logical Interfaces to the Switching Fabric

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.

- **VLAN ID** – Users can specify a specific CoS and Color for a specific VLAN ID. In the case of double-tagged frames, the match must be with the frame's outer VLAN. Permitted values are CoS 0 to 7 and Color Green or Yellow per VLAN ID. This is the highest classification priority on the logical interface level, and overwrites any other classification criteria at the logical interface level.
- **MPLS Trust Mode** – When this attribute is set to Trust mode and the arriving packet has MPLS EXP priority bits, the interface performs QoS and Color classification according to a user-configurable MPLS EXP bit to CoS and Color classification table.
- **DSCP Trust Mode** –When this attribute is set to Trust mode and the arriving packet has DSCP priority bits, the interface performs QoS and Color classification according to a user-configurable DSCP bit to CoS and Color classification table. If MPLS EXP priority bits are present, DSCP is not considered regardless of the Trust mode setting and regardless of whether an MPLS match was found.
- **802.1p Trust Mode** – When this attribute is set to Trust mode and the arriving packet is 802.1Q or 802.1AD, the interface performs QoS and Color classification according to user-configurable tables for 802.1q UP bit (C-VLAN frames) or 802.1AD UP bit (S-VLAN frames) to CoS and Color classification. MPLS and DSCP classification have priority over 802.1p Trust Mode, so that if a match is found on the MPLS or DSCP level, 802.1p bits are not considered.
- **Default CoS** – The default CoS value for frames passing through the interface. This value can be overwritten on the service point and service level. The Color is assumed to be Green.

For more information about classification at the logical interface level, refer to *Logical Interface-Level Classification* on page 114.

Ingress Path Rate Meters at Logical Interface Level

- **Unicast or Unknown-Unicast Traffic Rate Meter Admin** – Enables or disables the unicast rate meter (policer) on the logical interface.
- **Unicast or Unknown-Unicast Traffic Rate Meter Profile** – Associates the rate meter (policer) with a specific rate meter (policer) profile.
- **Multicast or Unknown-Multicast Traffic Rate Meter Admin** – Enables or disables the multicast rate meter (policer) on the logical interface.
- **Multicast or Unknown-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.
- **Ethertype 1 Rate Meter Admin** – Enables or disables the Ethertype 1 rate meter (policer) on the logical interface.
- **Ethertype 1 Rate Meter Profile** – Associates the rate meter (policer) with a specific rate meter (policer) profile.
- **Ethertype 1 Value** – The Ethertype value to which the user wants to apply this rate meter (policer). The field length is 4 nibbles (for example, 0x0806 - ARP).
- **Ethertype 2 Rate Meter Admin** – Enables or disables the Ethertype 2 rate meter (policer) on the logical interface.
- **Ethertype 2 Rate Meter Profile** – Associates the rate meter (policer) with a specific rate meter (policer) profile.
- **Ethertype 2 Value** – The Ethertype value to which the user wants to apply the rate meter (policer). The field length is 4 nibbles (for example, 0x0806 - ARP).
- **Ethertype 3 Rate Meter Admin** – Enables or disables the Ethertype 3 rate meter (policer) on the logical interface.
- **Ethertype 3 Rate Meter Profile** – Associates the rate meter (policer) with a specific rate meter (policer) profile.
- **Ethertype 3 Value** – The Ethertype value to which the user wants to apply the rate meter (policer). The field length is 4 nibbles (for example, 0x0806 - ARP).
- **Inline Compensation** – The logical interface's ingress compensation value. The rate meter (policer) attached to the logical interface uses this value to compensate for Layer 1 non-effective traffic bytes.

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 104, if the logical interface represents a group, such as a LAG, the IP-50E platform stores and displays RMON and RMON2 statistics for the logical interface.

Ingress Frame and Byte per Color Statistics at Logical Interface Level

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

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

Link Aggregation Groups (LAG) and LACP

Note: LAG is planned for future release.

Link aggregation (LAG) enables users to group several physical interfaces into a single logical interface bound to a single MAC address. This logical interface is known as a LAG group. Traffic sent to the interfaces in a LAG group is distributed by means of a load balancing function. IP-50E uses a distribution function of up to Layer 3 in order to generate the most efficient distribution among the LAG physical ports, taking into account:

- MAC DA and MAC SA
- IP DA and IP SA
- C-VLAN
- S-VLAN
- Layer 3 Protocol Field
- MPLS Label

The LAG distribution function is implemented as follows:

- The hashing is done over the packets header, up to L4
- The 4 LSBs of hashing provide 16 possibilities for streams to hit
- Per each result one port out of 16 LAG members is assigned
- The default assignment is cyclic. For example, for 3-port LAG the ports are assigned as 1-2-3-1-2-3-1-2-3-1-2-3-1-2-3-1

The user must analyze the Tx traffic load over the link members of the LAG and decide whether the load balancing is appropriate. If it is not, the user should select a different distribution function from the list of predefined functions and check the result again.

For LAG groups that consist of exactly two interfaces, users can change the distribution function by selecting from ten pre-defined LAG distribution schemes. The feature includes a display of the TX throughput for each interface in the LAG, to help users identify the best LAG distribution scheme for their specific link.

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

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-50E'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 Enhanced LAG Distribution or with the LAG Group Shutdown in Case of Degradation Event feature.

LAG groups can include interfaces with the following constraints:

- Only physical interfaces (including radio interfaces), not logical interfaces, can belong to 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-50E 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.

5.2.5 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-50E's personalized QoS enables operators to handle a wide and diverse range of scenarios. IP-50E'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-50E'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."

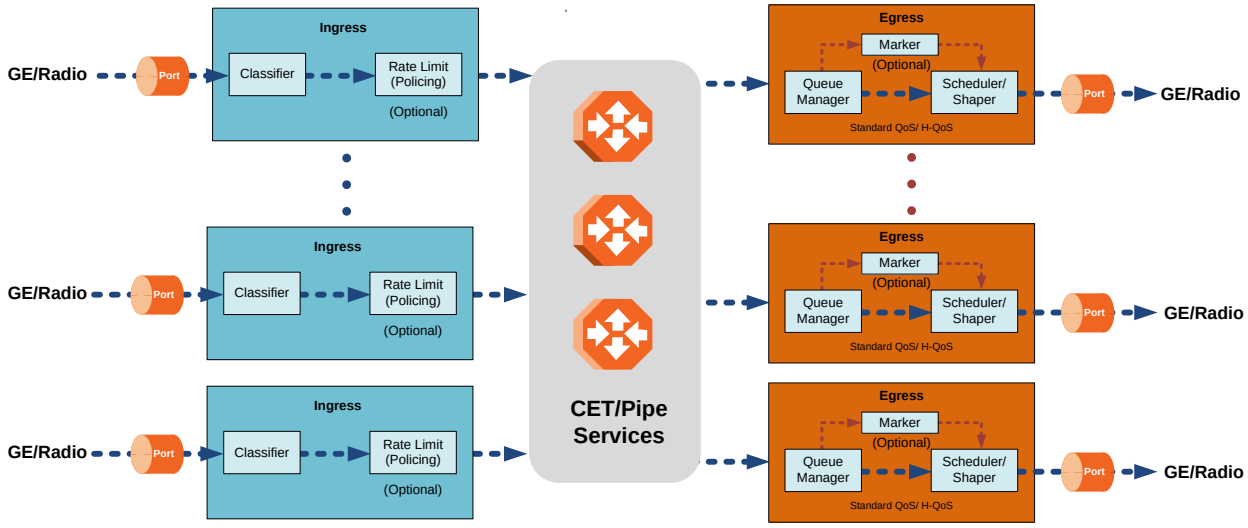


Figure 62: QoS Block Diagram

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 three different levels: interface, service point, and service point CoS. 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, per service bundle, and per port).
- **Marker** – This mechanism provides the ability to modify priority bits in frames based on the calculated CoS and Color.

The following two modes of operation are available on the egress path:

- **Standard QoS** – This mode provides eight transmission queues per port.
- **Hierarchical QoS (H-QoS)** – In this mode, users can associate services from the service model to configurable groups of eight transmission queues (service bundles), from a total 8K queues. In H-QoS mode, IP-50E performs QoS in a hierarchical manner in which the egress path is managed on three levels: ports, service bundles, and specific queues. This enables users to fully distinguish between streams, therefore providing a true SLA to customers.

The following figure illustrates the difference between how standard QoS and H-QoS handle traffic:

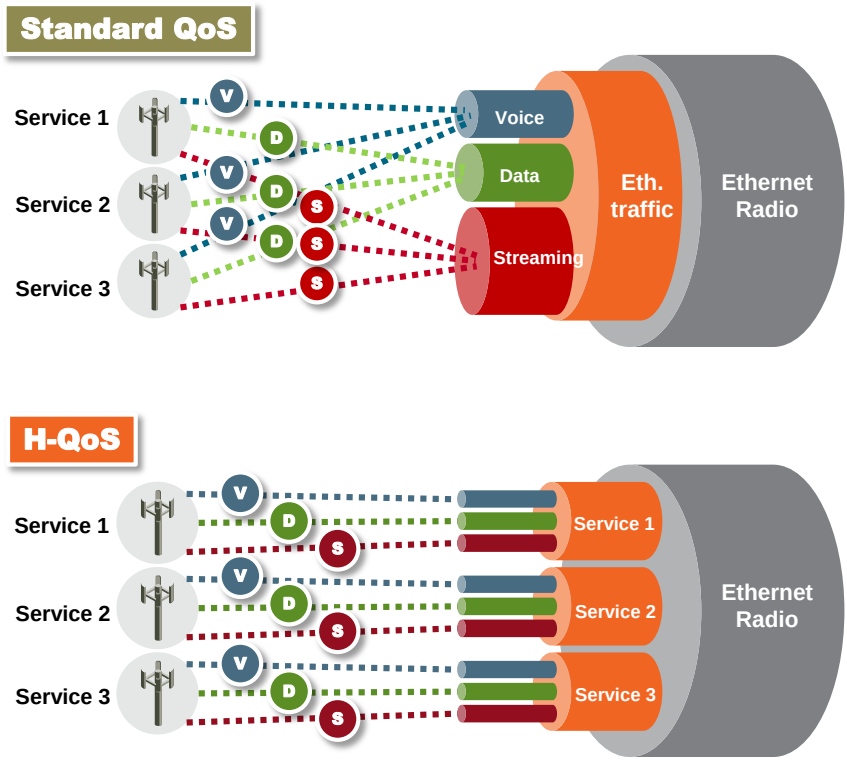


Figure 63: Standard QoS and H-QoS Comparison

5.2.5.1 QoS on the Ingress Path

Classification

IP-50E 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.

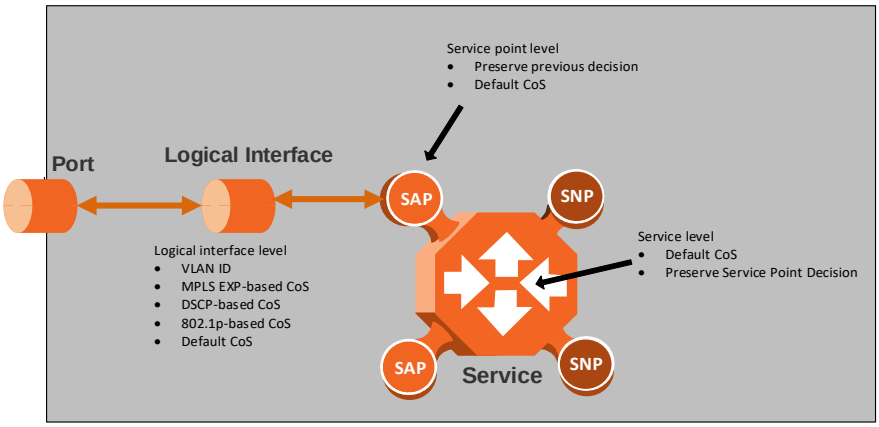


Figure 64: Hierarchical Classification

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:

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

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

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

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

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

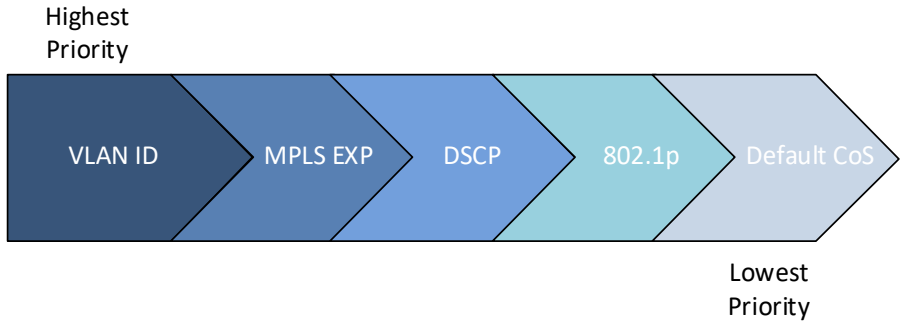


Figure 65: Classification Method Priorities

Interface-level classification is configured as part of the logical interface configuration. For details, refer to *Ingress Path Classification at Logical Interface Level* on page 107.

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 15: 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 16: DSCP Default Mapping to CoS and Color

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

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

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

Table 17: 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

802.1 UP	CFI	CoS (configurable)	Color (configurable)
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 18: 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-50E'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-50E 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
- Service point CoS-level rate meter

MEF 10.2 is the de-facto standard for SLA definitions, and IP-50E'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, and even at the level of a specific CoS within a specific service point.

This option enables users to customize a set of eight policers for a variety of traffic flows within a single service point in a service.

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-50E 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 three levels:

- Logical Interface:
  - Per frame type (unicast, multicast, and broadcast)
  - Per frame ethertype
- Per Service Point
- Per Service Point CoS

Note: Ingress rate meters can be configure per service point or per service point CoS, but not on both.

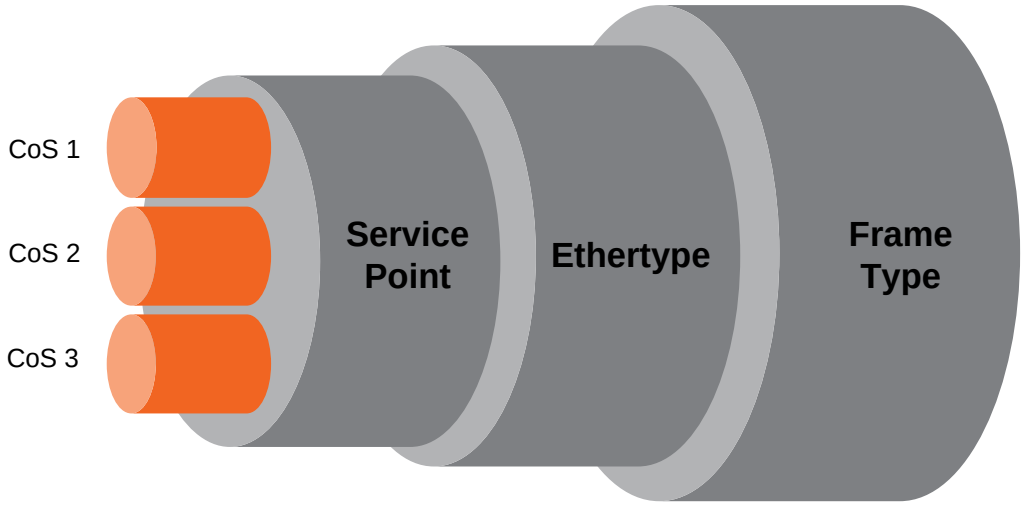


Figure 66: Ingress Policing Model

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

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.

The following parameter is neither a profile parameter, nor specifically a rate meter parameter, but rather, is a logical interface parameter. For more information about logical interfaces, refer to *Logical Interfaces* on page 106.

- **Line Compensation** – A rate meter can measure CIR and EIR at Layer 1 or Layer 2 rates. Layer 1 capacity is equal to Layer 2 capacity plus 20 additional bytes for each frame due to the preamble and Inter Frame Gap (IFG). In most cases, the preamble and IFG equals 20 bytes, but other values are also possible. Line compensation defines the number of bytes to be added to each frame for purposes of CIR and EIR calculation. When Line Compensation is 20, the rate meter operates as Layer 1. When Line Compensation is 0, the rate meter operates as Layer 2. This parameter is very important to users that want to distinguish between Layer 1 and Layer 2 traffic. For example, 1 Gbps of traffic at Layer 1 is equal to ~760 Mbps if the frame size is 64 bytes, but ~986 Mbps if the frame size is 1500 bytes. This demonstrates that counting at Layer 2 is not always fair in comparison to counting at Layer 1, that is, the physical level.

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.

5.2.5.2 QoS on the Egress Path

Queue Manager

The queue manager (QM) is responsible for managing the output transmission queues. IP-50E supports up to 8,192 service-level transmission queues, with configurable buffer size. Users can specify the buffer size of each queue independently. The total amount of memory dedicated to the queue buffers is 2 Gigabits.

The following considerations should be taken into account in determining the proper buffer size:

- **Latency considerations** – If low latency is required (users would rather drop frames in the queue than increase latency) small buffer sizes are preferable.
- **Throughput immunity to fast bursts** – When traffic is characterized by fast bursts, it is recommended to increase the buffer sizes to prevent packet loss. Of course, this comes at the cost of a possible increase in latency.

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

The 8,192 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.

The following figure depicts the queue manager. Physically, the queue manager is located between the ingress path and the egress path.

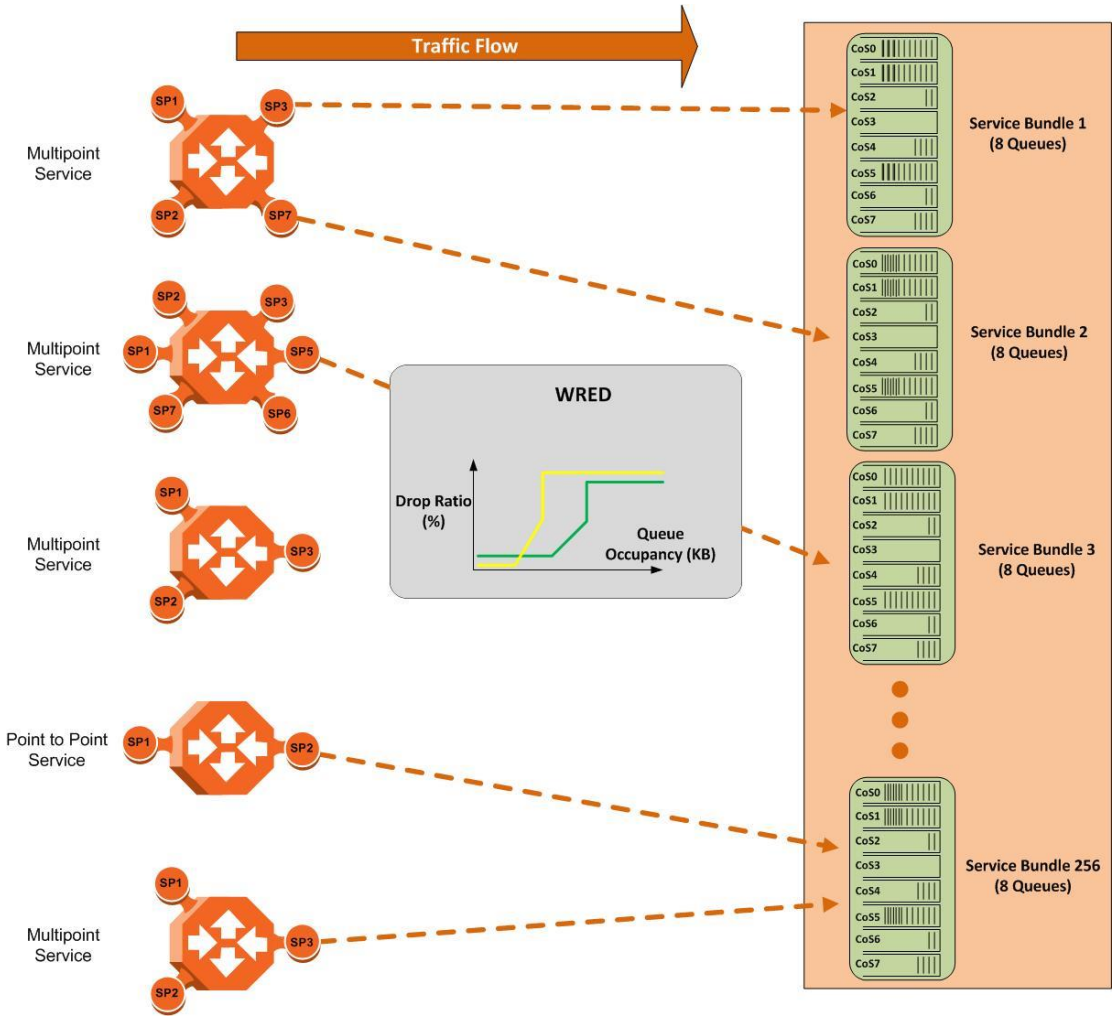


Figure 67: IP-50E Queue Manager

In the figure above, traffic is passing from left to right. The traffic passing from the ingress path is routed to the correct egress destination interfaces via the egress service points. As part of the assignment of the service points to the interfaces, users define the group of eight queues through which traffic is to be transmitted out of the service point. This is part of the service point egress configuration.

After the traffic is tunneled from the ingress service points to the egress service points, it is aggregated into one of the eight queues associated with the specific service point. The exact queue is determined by the CoS calculated by the ingress path. For example, if the calculated CoS is 6, the traffic is sent to queue 6, and so on.

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 2K queues share a single memory of 2 Gbits. IP-50E enables users to define a specific size for each queue which is different from the default size. Moreover, users can create an over-subscription scenario among the queues for when the buffer size of the aggregate queues is lower than the total memory allocated to all the queues. In doing this, the user must understand both the benefits and the potential hazards, namely, that if a lack of buffer space occurs, the queue manager will drop incoming frames without applying the usual priority rules among frames.

The queue size is defined by the WRED profile that is associated with the queue. For more details, refer to *WRED* on page 123.

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.

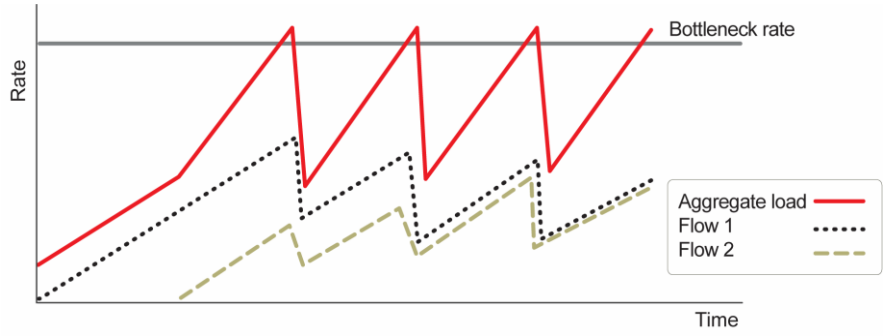


Figure 68: Synchronized Packet Loss

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.

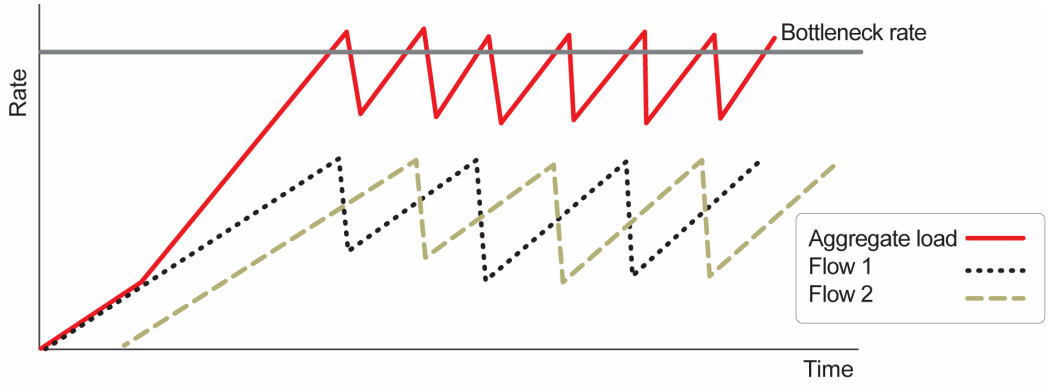


Figure 69: Random Packet Loss with Increased Capacity Utilization Using WRED

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-50E 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-50E enables users to define up to 30 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-50E 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.
  - Yellow maximum drop is 100%
  - Green maximum drop is 100%
- 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.

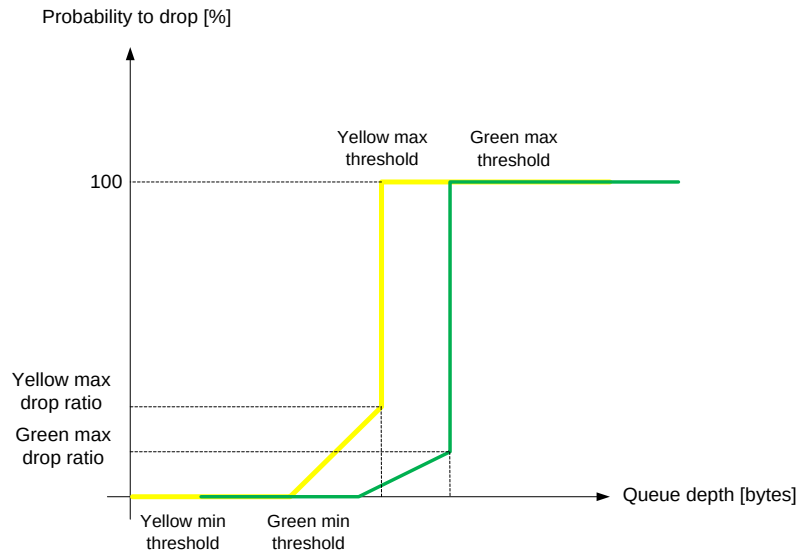


Figure 70: WRED Profile Curve

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.

Global WRED Profile Configuration

IP-50E supports 30 user-configurable WRED profiles and one pre-defined (default) profile. The following are the WRED profile attributes:

- **Green Minimum Threshold** – Permitted values are 24 Kbytes to 8 Mbytes, with granularity of 8 Kbytes.
- **Green Maximum Threshold** – Permitted values are 24 Kbytes to 8 Mbytes, with granularity of 8 Kbytes.
- **Green-Maximum Drop** – Permitted values are 1% to 100%, with 1% drop granularity.
- **Yellow Minimum Threshold** – Permitted values are 24 Kbytes to 8 Mbytes, with granularity of 8 Kbytes.
- **Yellow Maximum Threshold** – Permitted values are 24 Kbytes to 8 Mbytes, with granularity of 8 Kbytes.
- **Yellow Maximum Drop** – Permitted values are 1% to 100%, with 1% drop granularity.

Notes:	K is equal to 1024. Users can enter any value 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.

For each curve, frames are passed on and not dropped up to the minimum Green and Yellow thresholds. From this point, WRED performs a pseudo-random drop with a ratio based on the curve up to the maximum Green and Yellow thresholds. Beyond this point, 100% of frames with the applicable Color are dropped.

The system automatically assigns the default “tail drop” WRED profile (Profile ID 31) to every queue. Users can change the WRED profile per queue based on the application served by the queue.

Standard QoS and Hierarchical QoS (H-QoS)

In a standard QoS mechanism, egress data is mapped to a single egress interface. This single interface supports up to eight priority queues, which correspond to the CoS of the data. Since all traffic for the interface egresses via these queues, there is no way to distinguish between different services and traffic streams within the same priority.

The figure below shows three services, each with three distinct types of traffic streams:

- Voice – high priority
- Data – medium priority
- Streaming – lower priority

While the benefits of QoS on the egress path can be applied to the aggregate streams, without H-QoS they will not be able to distinguish between the various services included in these aggregate streams. Moreover, different behavior among the different traffic streams that constitute the aggregate stream can cause unpredictable behavior between the streams. For example, in a situation in which one traffic stream can transmit 50 Mbps in a shaped manner while another can transmit 50 Mbits in a burst, frames may be dropped in an unexpected way due to a lack of space in the queue resulting from a long burst.

Hierarchical QoS (H-QoS) solves this problem by enabling users to create a real egress tunnel for each stream, or for a group of streams that are bundled together. This enables the system to fully perform H-QoS with a top-down resolution, and to fully control the required SLA for each stream.

H-QoS Hierarchy

The egress path hierarchy is based on the following levels:

- Queue level
- Service bundle level
- Logical interface level

The queue level represents the physical priority queues. This level holds 2K queues. Each eight queues are bundled and represent eight CoS priority levels. One or more service points can be attached to a specific bundle, and the traffic from the service point to one of the eight queues is based on the CoS that was calculated on the ingress path.

Note:	With standard QoS, all services are assigned to a single default service bundle.

The service bundle level represents the groups of eight priority queues. Every eight queues are managed as a single service bundle.

The interface level represents the physical port through which traffic from the specified service point egresses.

The following summarizes the egress path hierarchy:

- Up to 5 physical interfaces
- One service bundle per interface in standard QoS / 32 service bundles per interface in H-QoS.
- Eight queues per service bundle

H-QoS on the Interface Level

Users can assign a single leaky bucket shaper to each interface. The shaper on the interface level stops traffic from the interface if a specific user-defined peak information rate (PIR) has been exceeded.

In addition, users can configure scheduling rules for the priority queues, as follows:

- Scheduling (serve) priorities among the eight priority queues.
- Weighted Fair Queuing (WFQ) among queues with the same priority.

Note:	The system assigns the rules for all service bundles under the interface.

RMON counters are valid on the interface level.

H-QoS on the Service Bundle Level

Users can assign a dual leaky bucket shaper to each service bundle. On the service bundle level, the shaper changes the scheduling priority if traffic via the service bundle is above the user-defined CIR and below the PIR. If traffic is above the PIR, the scheduler stops transmission for the service bundle.

Service bundle traffic counters are valid on this level.

Note:	With standard QoS, users assign the egress traffic to a single service bundle (Service Bundle ID 1).

H-QoS on the Queue Level

The egress service point points to a specific service bundle. Depending on the user application, the user can connect either a single service point or multiple service points to a service bundle. Usually, if multiple service points are connected to a service bundle, the service points will share the same traffic type and characteristics. Mapping to the eight priority queues is based on the CoS calculated on the ingress path, before any marking operation, which only changes the egress CoS and Color.

Users can assign a single leaky bucket to each queue. The shaper on the queue level stops traffic from leaving the queue if a specific user-defined PIR has been exceeded.

Traffic counters are valid on this level.

H- QoS Mode

As discussed above, users can select whether to work in Standard QoS mode or H-QoS mode.

- If the user configured all the egress service points to transmit traffic via a single service bundle, the operational mode is Standard QoS. In this mode, only Service Bundle 1 is active and there are eight output transmission queues.
- If the user configured the egress service points to transmit traffic via multiple service bundles, the operational mode is H-QoS. H-QoS mode enables users to fully distinguish among the streams and to achieve SLA per service.

Shaping on the Egress Path

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

Queue Shapers

Users can configure up to 31 dual 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 - 40 Gbps – granularity of 81 Kbps

The CBS value can be set to the following values:

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

The EIR value can be set to the following values:

- 0 - 40 Gbps – granularity of 81 Kbps

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.

Service Bundle Shapers

Users can configure up to 255 dual leaky bucket shaper profiles. The profiles can be configured as follows:

- Valid CIR values are:
  - 0 - 40 Gbps – granularity of 81 Kbps
- Valid PIR values are:
  - 0 - 40 Gbps – granularity of 81 Kbps

Note:	Users can enter any value 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 service bundle shaper profiles to each service bundle. If no profile is attached to the service bundle, no egress shaping is performed on that service bundle.

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 120.

Egress Scheduling

Egress scheduling is responsible for transmission from the priority queues. IP-50E 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 for a single service bundle (equivalent to Standard QoS). When a user assigns traffic to more than single service bundle (H-QoS mode), multiple instances of this model (up to 32 per port) are valid.

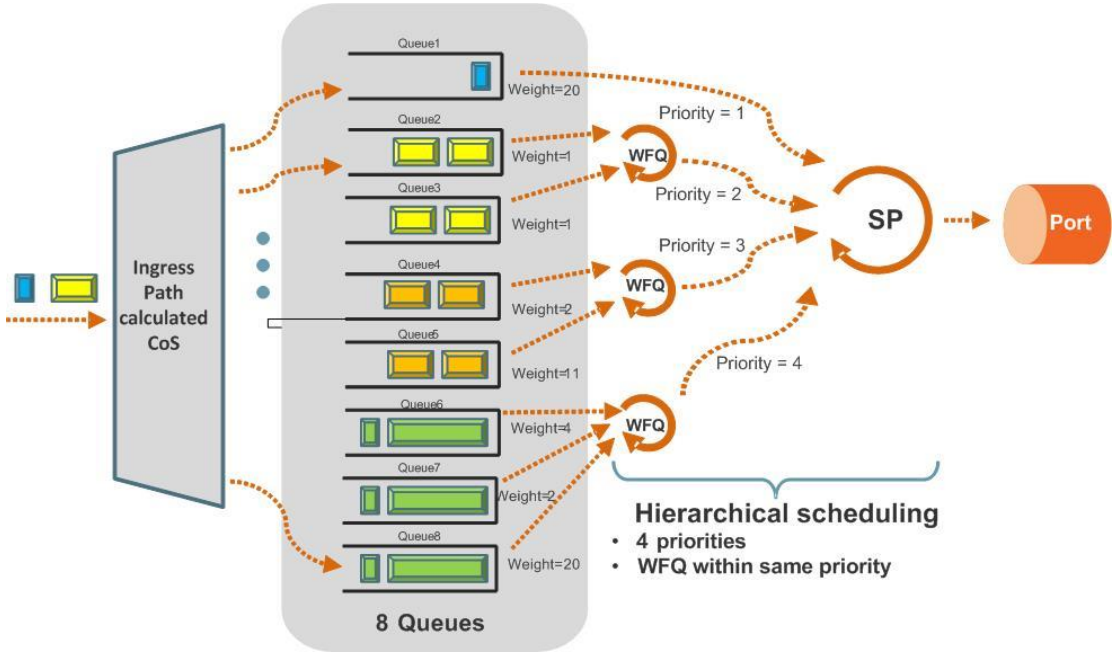


Figure 71: Scheduling Mechanism for a Single Service Bundle

Interface Priority

The profile defines the exact order for serving the eight priority queues in a single service bundle.

The priority mechanism distinguishes between two states of the service bundle:

- Green State – Committed state
- Yellow state – Best effort state

Green State refers to any time when the *service bundle total rate* is below the user-defined CIR. Yellow State refers to any time when the *service bundle total rate* is above the user-defined CIR but below the PIR.

User can define up to four Green priority profiles, from 4 (highest) to 1 (lowest). An additional four Yellow priority profiles are defined automatically.

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

Table 19: 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

Profile ID (1-9)			
CoS	**Green Priority (user defined)**	**Yellow Priority (read only)**	**Description**
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.)

When the service bundle state is Green (committed state), the service bundle priorities are as defined in the Green Priority column. When the service bundle state is Yellow (best effort state), the service bundle priorities are system-defined priorities shown in the Yellow Priority column.

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

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

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

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

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

Weighted Fair Queuing (WFQ)

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

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

The following table provides an example of a WFQ profile.

Table 20: WFQ Profile Example

	Profile ID (1-7)	
CoS	**CIR Queue Weight**	**EIR Queue Weight**
0	20	20
1	20	20
2	20	20
3	20	20
4	20	20
5	20	20
6	20	20
7	20	20

For each CoS, the user can define;

- **Profile ID** – Profile ID number. Permitted values are 2 to 6.
- **CIR Weight** – Transmission quota for CIR traffic. Permitted values are 1 to 20.
- **EIR Weight** – Transmission quota for EIR traffic. Permitted values are 1 to 20.

Users can attach one of the configured WFQ profiles to each interface. By default, the interface is assigned Profile ID 1, the pre-defined system profile.

Egress PMs and Statistics

Queue-Level Statistics

IP-50E 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)

Service Bundle-Level Statistics

IP-50E supports the following counters per service bundle at the service bundle level:

- Transmitted Green Packets (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)

Advanced Queue and Service Bundle-Level PMs

For each logical interface, users can configure thresholds for Green and Yellow traffic per queue. Users can then display the following PMs for 15-minute and 24-hour intervals, per queue and color:

- Maximum bytes passed per second
- Minimum bytes passed per second
- Average bytes passed per second
- Maximum bytes dropped per second
- Minimum bytes dropped per second
- Average bytes dropped per second
- Maximum packets passed per second
- Minimum packets passed per second
- Average packets passed per second
- Maximum packets dropped per second
- Minimum packets dropped per second
- Average packets dropped per second
- Seconds bytes per second were over the configured threshold per interval

Interface-Level Statistics

For information on statistics at the interface level, refer to *Ethernet Statistics* on page 104.

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 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.

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 21: 802.1q UP Marking Table (C-VLAN)

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

Table 22: 802.1ad UP Marking Table (S-VLAN)

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

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

Standard QoS and Hierarchical QoS (H-QoS) Summary

The following table summarizes and compares the capabilities of standard QoS and H-QoS.

Table 23: Summary and Comparison of Standard QoS and H-QoS

Capability	Standard QoS	Hierarchical QoS
Number of transmission queues per port	8	256
Number of service bundles	1 (always service bundle id equal 1)	32
WRED	Per queue (two curves – for green traffic and for yellow traffic via the queue)	Per queue (two curves – for green traffic and for yellow traffic via the queue)
Shaping at queue level	Dual leaky bucket	Dual leaky bucket
Shaping at service bundle level	Dual leaky bucket	Dual leaky bucket
Shaping at port level	None	Dual leaky bucket
Transmission queues priority	Per queue priority (4 priorities).	Per queue priority (4 priorities). All service bundles for a specific port inherit the 8-queues priority settings.
Weighted fair Queue (WFQ)	Queue level (between queues)	Queue level (between queues) Service Bundle level (between service bundles)
Marker	Supported	Supported
Statistics	Queue level (8 queues) Service bundle level (1 service bundle) Port level	Queue level (256 queues) Service bundle level (32 service bundles) Port level

5.2.6 Global Switch Configuration

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

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

5.2.7 Automatic State Propagation and Link Loss Forwarding

Related topics:

- Network Resiliency
- External Protection
- 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.

5.2.7.1 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.

5.2.7.2 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 switch.

5.2.7.3 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-50E unit is an element in the following network topologies:

- Ring or mesh network topology.
- An IP-20N connected to an IP-50E unit being utilized as a pipe via an Ethernet interface (back-to-back on the same site).[9]
- Payload traffic is spanned by G.8032 in the network.
- In-band management is spanned by MSTP in the network.
- An IP-50E unit being utilized as a pipe is running one MSTP instance for spanning in-band management.

[9] ASP interoperability among IP-20 units requires that all units be running software version 7.7 or higher.

5.2.8 Adaptive Bandwidth Notification (EOAM)

Note: ABN is planned for future release.

Adaptive Bandwidth Notification (ABN, also known as EOAM) enables third party applications to learn about bandwidth changes in a radio link when ACMB is active. Once ABN is enabled, the radio unit reports bandwidth information to third-party switches.

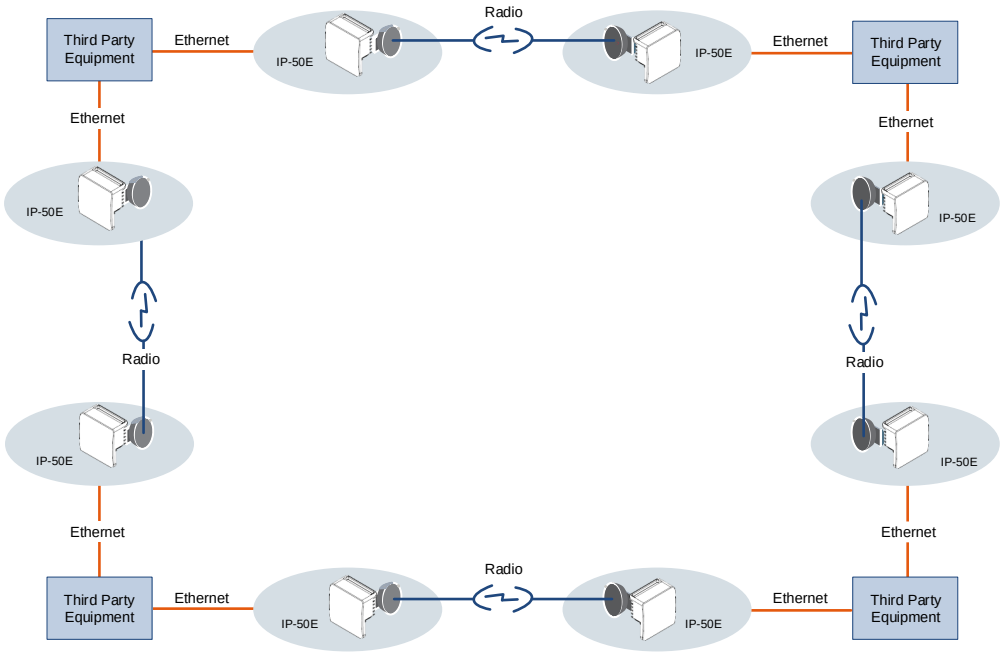


Figure 72: Network Topology with IP-50E Units and Third-Party Equipment

The ABN entity creates a logical relationship between a radio interface, called the Monitored Interface, and an Ethernet interface or a logical group of Ethernet interfaces, called the Control Interface. When bandwidth degrades from the nominal bandwidth value in the Monitored Interface, messages relaying the actual bandwidth values are periodically sent over the Control Interface. A termination message is sent once the bandwidth returns to its nominal level.

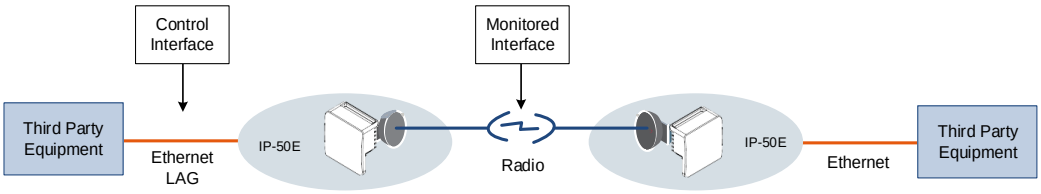


Figure 73: ABN Entity

The nominal bandwidth is calculated by the system based on the maximum bandwidth profile. The ABN entity measures the bandwidth in samples once a change in profile takes place. A weighted average is calculated based on the samples at regular, user-defined intervals to determine whether a bandwidth degradation event has occurred. Bandwidth degradation is reported only if the measured bandwidth remains below the nominal bandwidth at the end of a user-

defined holdoff period. This prevents the IP-50E from reporting bandwidth degradation due to short fading events.

5.2.9 Network Resiliency

IP-50E 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.

Note: Support for G.8032 and MSTP is planned for future release.

5.2.9.1 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.

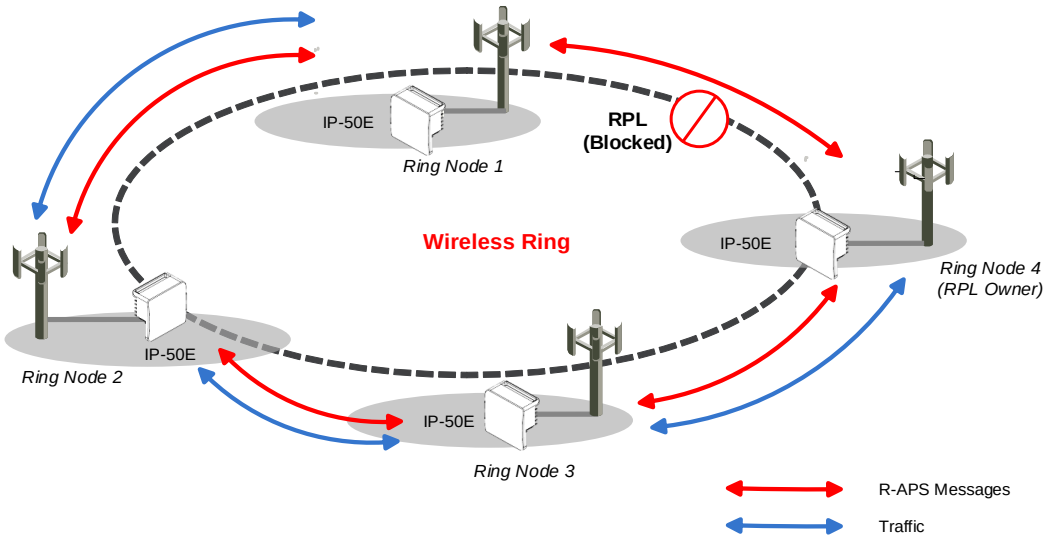


Figure 74: G.8032 Ring in Idle (Normal) State

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.

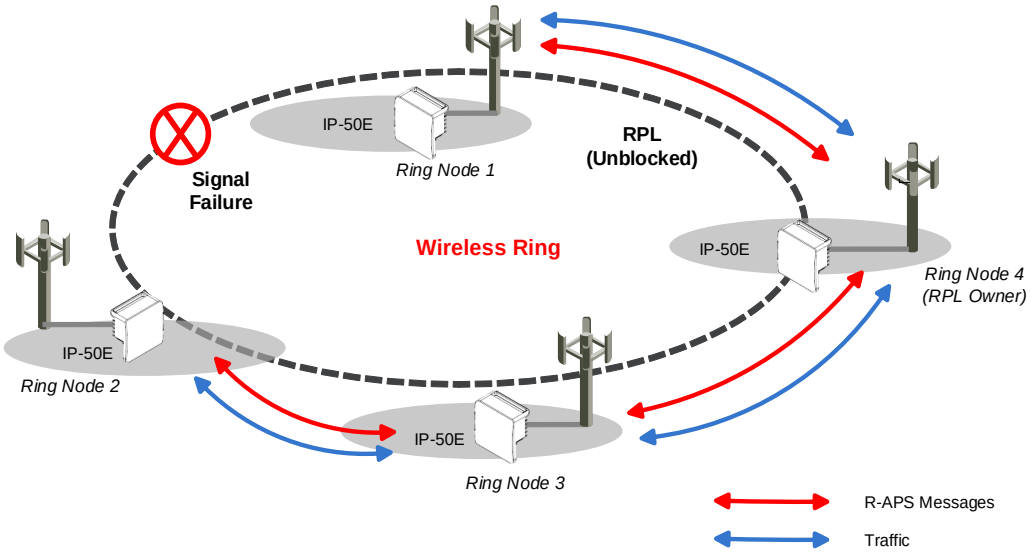


Figure 75: G.8032 Ring in Protecting State

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.

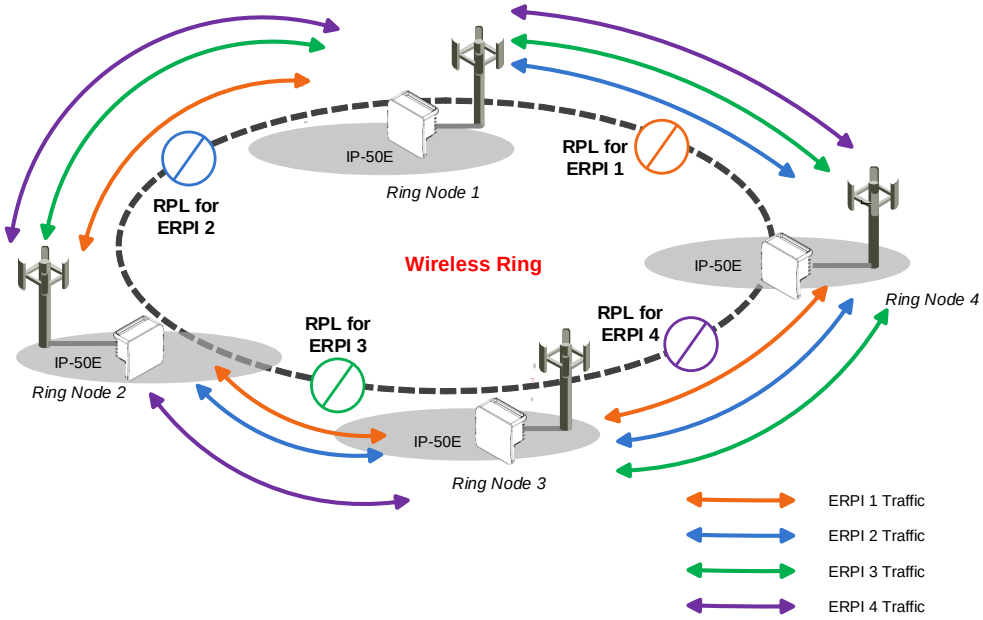


Figure 76: Load Balancing Example in G.8032 Ring

5.2.9.2 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-50E supports MSTP according to the following IEEE standards:

- 802.1q
- 802.1ad amendment (Q-in-Q)
- 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-50E units is interoperable with:

- IP-10 and IP-20 units running RSTP.
- Third-party bridges running MSTP.
- Third-party bridges running RSTP

5.2.10 OAM

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

- Fault management status and alarms.
- Maintenance signals, such as AIS, and RDI.
- Maintenance commands, such as loopbacks and Linktrace commands.
- Ethernet Bandwidth Notification (ETH-BN)

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

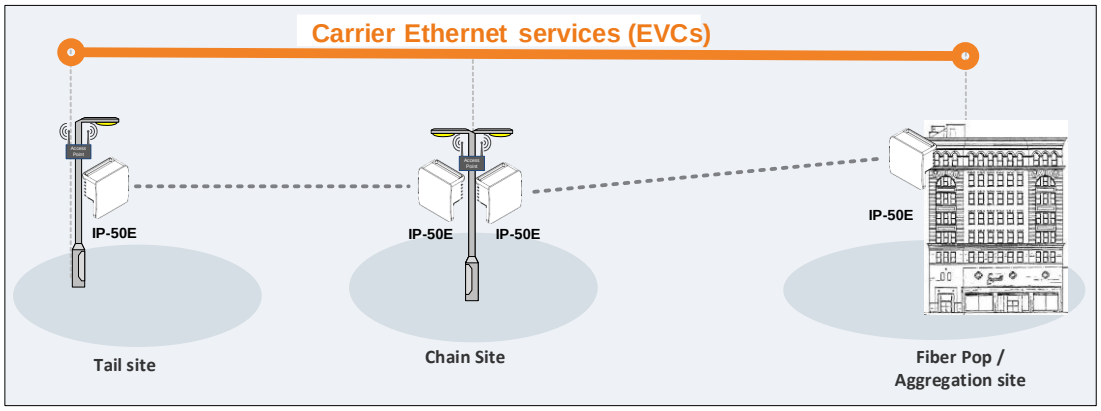


Figure 77: IP-50E End-to-End Service Management

5.2.10.1 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
- Link trace
- Loopback.

IP-50E 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.

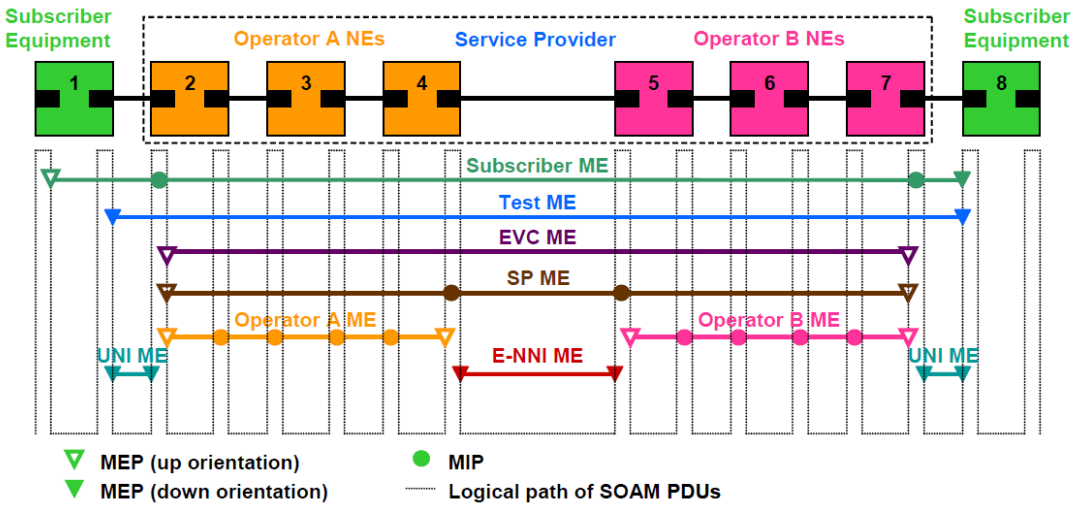


Figure 78: SOAM Maintenance Entities (Example)

- 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.
  - Linktrace: The LTM/LTR mechanism is an on-demand mechanism. It can detect the route of the data from any MEP to any other MEP in the MA/MEG. It can be used for the following purposes:
    - Adjacent relation retrieval – The ETH-LT function can be used to retrieve the adjacency relationship between an MEP and a remote MEP or MIP. The result of running ETH-LT function is a sequence of MIPs from the source MEP until the target MIP or MEP.
    - Fault localization – The ETH-LT function can be used for fault localization. When a fault occurs, the sequence of MIPs and/or MEP will probably be different from the expected sequence. The difference between the sequences provides information about the fault location.
    - AIS: AIS (defined in G.8013/Y.1731O) is the Ethernet alarm indication signal function used to suppress alarms following detection of defect conditions at the server (sub) layer.

5.2.10.2 SFP DDM and Inventory Monitoring

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

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

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

Note: Tx Power level DDM is not supported for QSFP (P4) – not part of the standard.

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

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

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

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

Note: DDM parameters are not relevant for electrical SFPs.

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

5.2.10.3 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 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:

- Only single interfaces, not groups, can be used as the Monitored Interface and the Control Interface.
- ETH-BN can only be used with 1+0 radio links.
- If CFM MEPs are being used, the MEL for ETH-BN must be set to a value greater than the MEG level of the MEP. Otherwise, the BNM frames will be dropped. – this is correct.
- 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.

5.3 Frequency Scanner

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

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

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

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

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

5.4 Synchronization

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

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

This section includes:

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

Related topics:

- NTP Support

5.4.1 IP-50E Synchronization Solution

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

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

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 24: 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 eight 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.

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

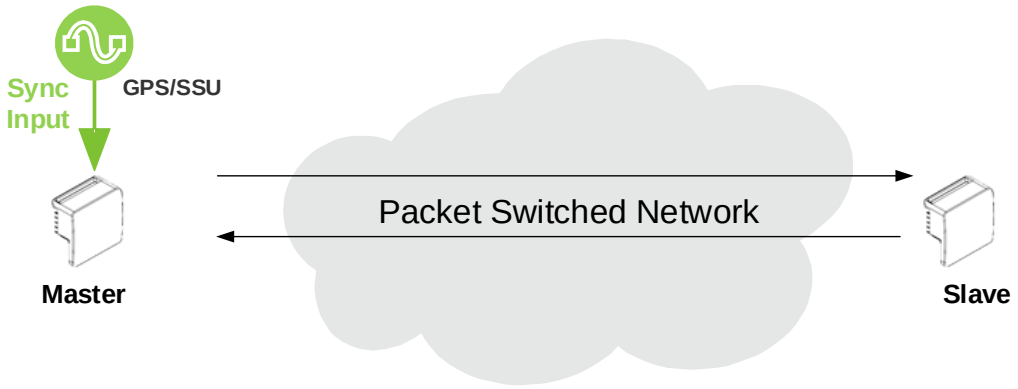


Figure 79: IEEE-1588v2 PTP Optimized Transport – General Architecture

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.

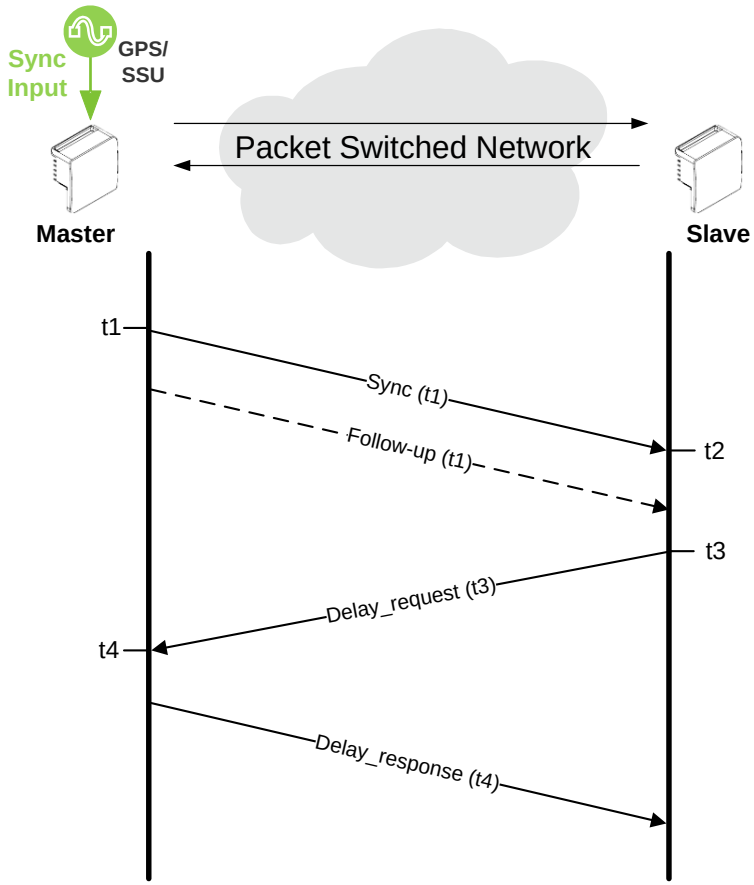


Figure 80: Calculating the Propagation Delay for PTP Packets

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-50E's IEEE-1588v2 implementations mitigate these factors, see *Mitigating PDV* on page 157.

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 LTE-A 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 157).
- 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-50E supports Transparent Clock and Boundary Clock.

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

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

Packet processing delay variation can be caused by:

- Queuing Delay – Delay associated with incoming and outgoing packet buffer queuing.
- Head of Line Blocking – Occurs when a high priority frame, such as a frame that contains IEEE-1588 information, is forced to wait until a lower-priority frame that has already started to be transmitted completes its transmission.

- Store and Forward – Used to determine where to send individual packets. Incoming packets are stored in local memory while the MAC address table is searched and the packet's cyclic redundancy field is checked before the packet is sent out on the appropriate port. This process introduces variations in the time latency of packet forwarding due to packet size, flow control, MAC address table searches, and CRC calculations.

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

Note:	When bandwidth is reduced due to lowering of the ACMB modulation point, it is essential that high priority traffic carrying IEEE-1588 packets be given the highest priority using IP-50E'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-50E'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-50E 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.

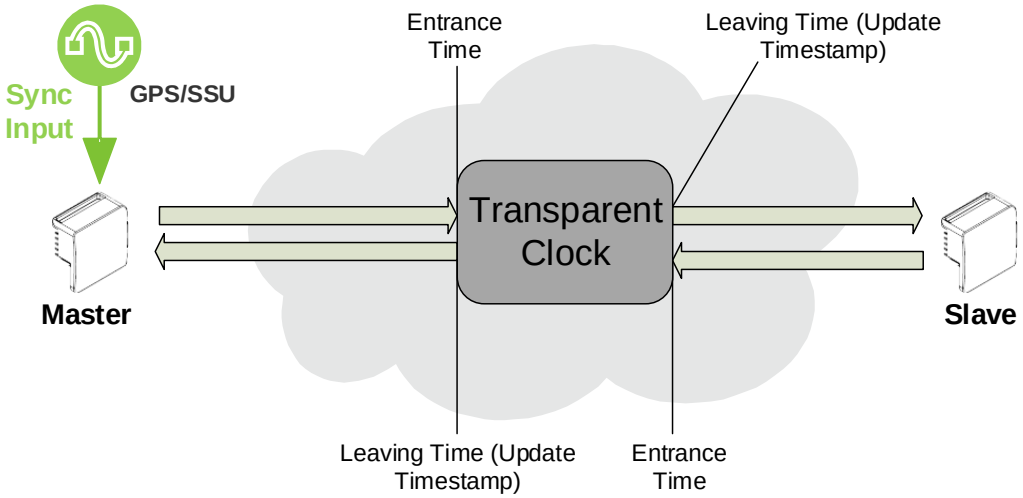


Figure 81: Transparent Clock – General Architecture

IP-50E 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-50E 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-50E 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).

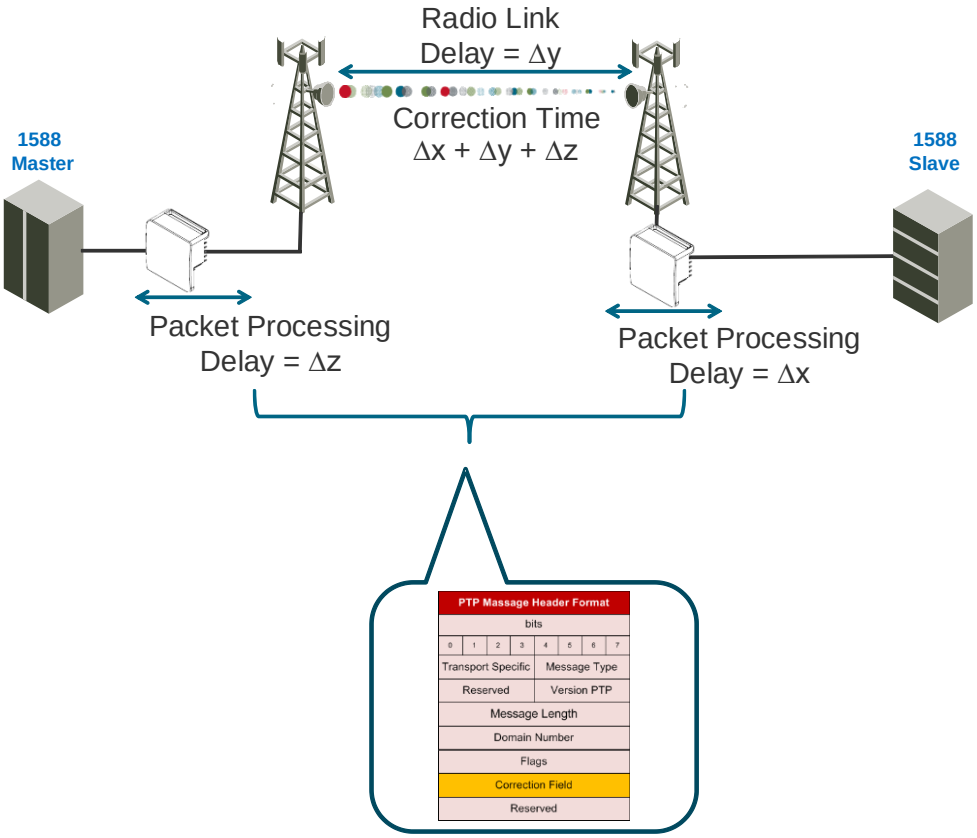


Figure 82: Transparent Clock Delay Compensation

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-50E, 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.

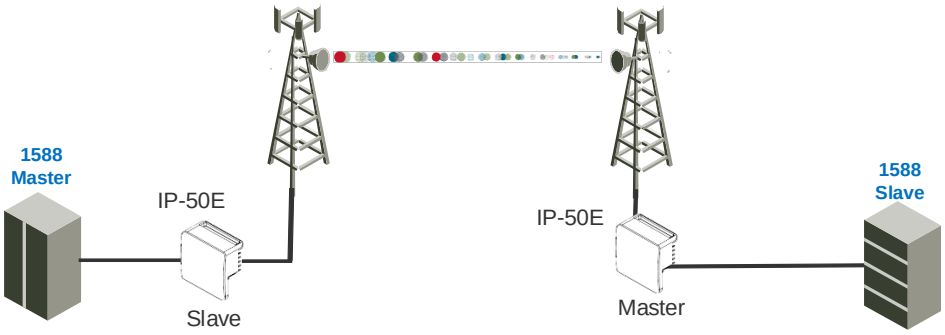


Figure 83: Boundary Clock – General Architecture

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 25: 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 26: 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-50E implements the passing of SSM messages over the radio interfaces. SSM timing in IP-50E 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 (ETSI systems)
  - 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.

6. IP-50E 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
- WiFi Management
- Command Line Interface (CLI)
- Configuration Management
- Software Management
- CeraPlan Service for Creating Pre-Defined Configuration Files
- IPv6 Support
- In-Band Management
- Local Management
- Alarms
- NTP Support
- UTC Support
- System Security Features

6.1 Management Overview

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

- EMS – HTTP web-based EMS
- NEL – Network Element-level CLI
- SDN – Software-Defined Networking, including NETCONF/YANG
- NMS and SML –PolyView/NetMaster platform

Every IP-50E network element includes an HTTP web-based element manager that enables the operator to perform element configuration, performance monitoring, remote diagnostics, alarm reports, and more.

IP-50E devices support SDN, enabling customers to manage, configure, and monitor network elements within the paradigm of SDN network architecture using Ceragon's SDN Master controller.

IP-50E supports SDN, enabling customers to manage, configure, and monitor network elements within the paradigm of SDN network architecture.[10]

IP-50E also provides an SNMP v1/v2c/v3 northbound interface on the IP-50E.

Ceragon offers an NMS solution for providing centralized operation and maintenance capability for the complete range of network elements in an IP-50E system.

In addition, management, configuration, and maintenance tasks can be performed directly via the IP-50E Command Line Interface (CLI). The CLI can be used to perform configuration operations for IP-50E units, as well as to configure several IP-50E units in a single batch command.

[10] SDN support is planned for future release.

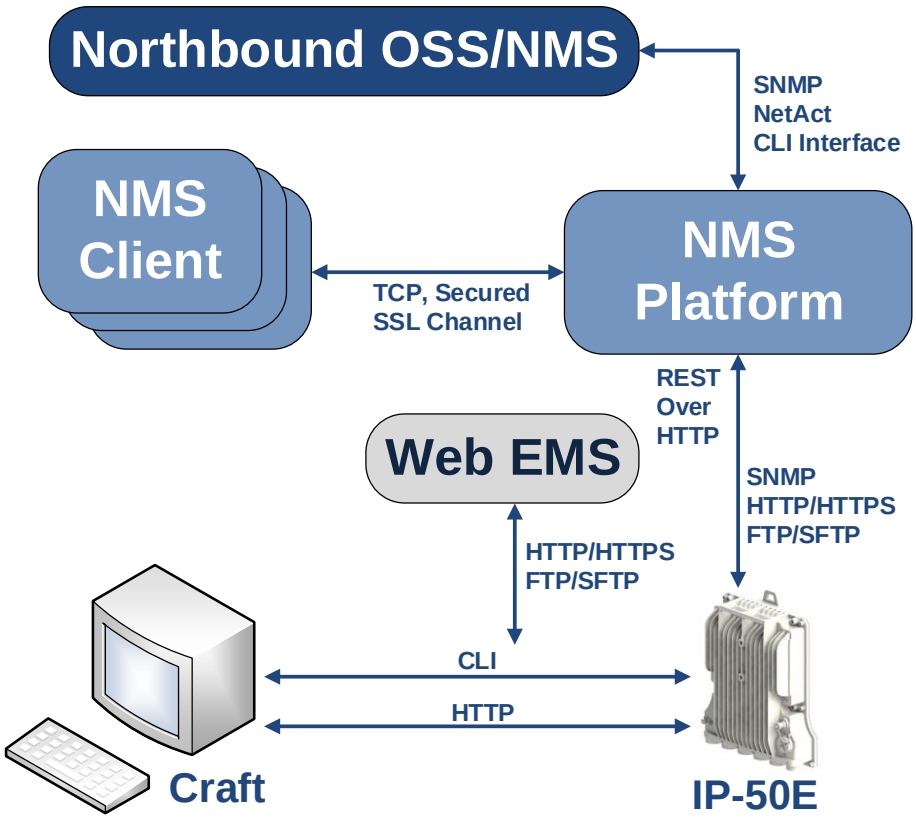


Figure 84: Integrated IP-50E Management Tools

6.2 Automatic Network Topology Discovery with LLDP Protocol

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

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

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

- Automatically detect the IP-50E unit neighboring the managed IP-50E unit, and determine the connectivity state between the two units.
- Automatically detect a third-party switch or router neighboring the managed IP-50E unit, and determine the connectivity state between the IP-50E 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 27: 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)
80	HTTP	TCP	Manages devices
443	HTTPS	TCP	Manages devices (optional)
From port 21 (default) to any remote port (>1023). Initial port (21) is configurable.	FTP Control Port	TCP	Downloads software and configuration files, uploads security and configuration logs, and unit info files. (FTP Server responds to client's control port) (optional)
From Any port (>1023) to any remote port (>1023)	FTP Data Port	TCP	Downloads software and configuration files, uploads security and configuration logs, and unit info files. The FTP server sends ACKs (and data) to client's data port.
From port 22 (default) to any remote port (>1023). Initial port (22) is configurable.	SFTP Control Port	TCP	Downloads software and configuration files, and CSR certificates, uploads security and configuration logs, and unit info files. (SFTP Server responds to client's control port) (optional)
From Any port (>1023) to any remote port (>1023)	SFTP Data Port	TCP	Downloads software and configuration files, and CSR certificates, uploads security and configuration logs, and unit info files. The SFTP server sends ACKs (and data) to client's data port.
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-50E 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-50E security features.
- **User Management** – Enables you to define users and user profiles.

A Web-Based EMS connection to the IP-50E 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 and Radio Summary page that displays the key unit, link, and radio parameters on a single page for quick viewing. This page can be customized to include only specific columns and tables, enabling the user to hide information that he does not need in order to focus on the information that is most relevant to his needs in monitoring and managing the unit.

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 Pipe 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
- HTTP or HTTPS
- Telnet blocking

- 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
- HTTP/HTTPS configuration
- Telnet blocking status
- SNMP parameters
- Login and password security parameters
- Users and their parameters
- Public RSA key currently configured on the device

6.5 SDN Support

IP-50E supports SDN, with NETCONF/YANG capabilities that will enable IP-50E to be fully manageable in the rapidly emerging SDN paradigm.

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-50E'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
- Service configuration

IP-50E's SDN implementation includes the following standard interfaces and protocols:

- NBI:
  - IETF
  - ONF TAPI 2.0 or higher
  - RESTCONF
- SBI:
  - NETCONF RFC 6241
  - Support for get/get-config/edit/copy/delete
  - YANG RFC 6020
  - Information Model (TR-532 and TR-527)

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.

6.6 WiFi Management

Note:	WiFi management is hardware-ready with the addition of a plugin module, and will be supported in future software releases.

The IP-50E is equipped with a WiFi access point supporting 802.11 b/g/n. The WiFi access point does not broadcast its SSID and enables a secure WiFi connection for technical personnel to be able to manage the IP-50E system with no wired connection using a portable device.

6.7 Command Line Interface (CLI)

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

Note: Telnet access can be blocked by user configuration.

6.8 Configuration Management

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

IP-50E configuration files can be imported and exported. This enables you to copy the system configuration to multiple IP-50E 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.[11]

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.

[11] The option to edit the backup configuration is planned for future release.

6.9 Software Management

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

IP-50E 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-50E 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-50E 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-50E 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.

6.10 CeraPlan Service for Creating Pre-Defined Configuration Files

IP-50E 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 is generated by Ceragon Professional Services and provided as a service.

A pre-defined configuration file can be prepared for multiple IP-50E 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 on CeraPlan, consult your Ceragon representative.

6.11 IPv6 Support

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

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

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

6.12 In-Band Management

IP-50E 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 90.

6.13 Local Management

IP-50E includes an electrical GbE management port.

6.14 Alarms

6.14.1 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.

6.14.2 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.

6.14.3 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.

6.14.4 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.

6.15 NTP Support

Related topics:

- Synchronization

IP-50E 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.

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

6.16 UTC Support

IP-50E 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-50E 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.

6.17 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.

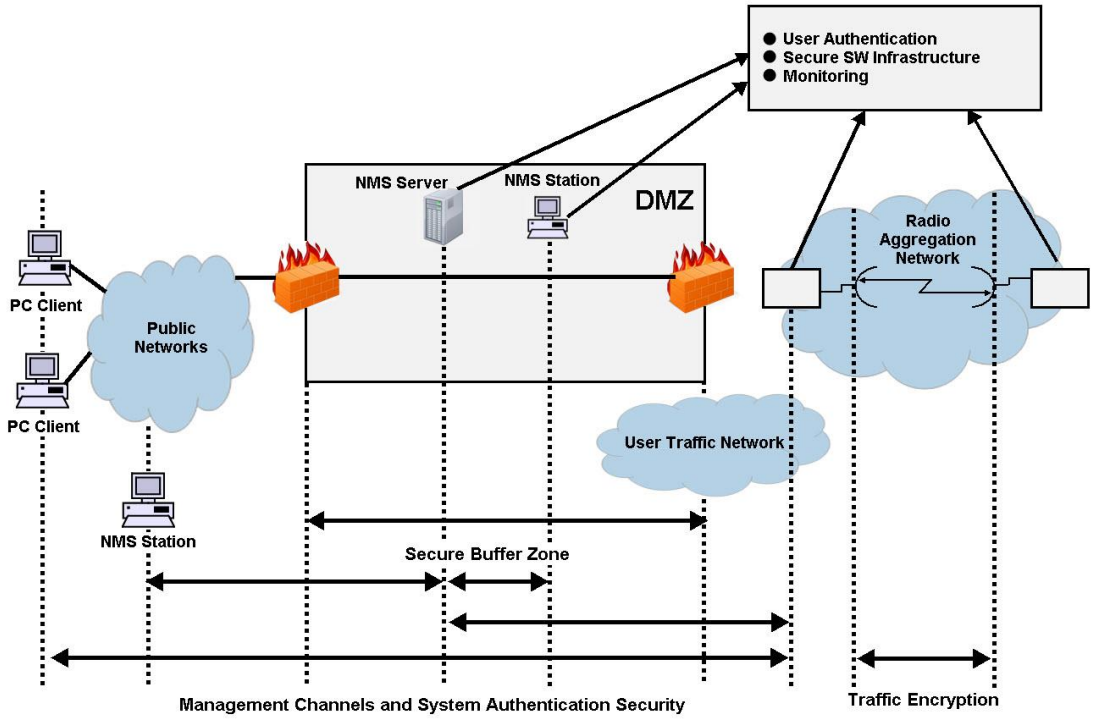


Figure 85: Security Solution Architecture Concept

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-50E 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-50E 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 at least three of the following categories: lower-case characters, upper-case characters, digits, and special characters.
  - When calculating the number of character categories, upper-case letters used as the first character and digits used as the last character of a password are not counted.
  - The password cannot have been used within the user's previous five passwords.

- 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.

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-50E 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-50E 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-50E 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-50E, or notifies the IP-50E 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-50E 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-50E - 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-50E supports TACACS+ for remote access user authentication and authorization. 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.

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.

6.17.4 Secure Communication Channels

IP-50E 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-50E:

- SSHv2 is supported.
- SSH protocol will always be operational. Admin users can choose whether to disable Telnet protocol, which is enabled by default. Server authentication is based on IP-50E'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 SSLv3/TLS (1.0, 1.1, 1.2) protocol to provide encrypted communication and secure identification of a network web server. IP-50E enables administrators to configure secure access via HTTPS protocol.

Users can configure the IP-50E to operate in HTTPS strong mode. In HTTPS strong mode, SSLv3, TLSv1.0, and TLSv1.1 are disabled completely and only certain ciphers are supported for TLSv1.2.

For a list of supported HTTPS ciphers, including an indication of which ciphers are supported in HTTPS strong mode, see *Annex B – 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-50E 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-50E 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 (SSLv3/TLS (1.0, 1.1, 1.1))

- All protocols making use of SSL (such as HTTPS) use SLLv3/TLS (1.0, 1.1, 1.2) 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.

6.17.4.8 Encryption

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

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 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

7. Standards and Certifications

This chapter includes:

- Supported Ethernet Standards
- MEF Specifications for Ethernet Services

7.1 Supported Ethernet Standards

Table 28: Supported Ethernet Standards

Standard	Description
802.3	10base-T
802.3u	100base-T
802.3ab	1000base-T
802.3z	1000base-X
802.3ae	10GBase-LR
802.3ac	Ethernet VLANs
802.1Q	Virtual LAN (VLAN)
802.1p	Class of service
802.1ad	Provider bridges (QinQ)
802.3ad	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-50E supports the specifications listed in the following table.

Table 29: Supported MEF Specifications

Specification	Description
MEF-2	Requirements and Framework for Ethernet Service Protection
MEF-6.1	Metro Ethernet Services Definitions Phase 2
MEF-8	Implementation Agreement for the Emulation of PDH Circuits over Metro Ethernet Networks
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-18	Abstract Test Suite for Circuit Emulation Services
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
- Radio Capacity Specifications
- Transmit Power Specifications
- Receiver Threshold Specifications
- Mediation Device Losses
- Ethernet Latency Specifications
- Interface Specifications
- Carrier Ethernet Functionality
- Synchronization
- Network Management, Diagnostics, Status, and Alarms
- Mechanical Specifications
- Standards Compliance
- Environmental Specifications
- Antenna Specifications
- Integrated Antenna
- Power Input Specifications
- Power Consumption Specifications
- Power Connection Options
- PoE Injector Specifications – Standard PoE
- PoE Injector Specifications – Passive PoE
- Cable Specifications

Related Topics:

- Standards and Certifications

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

8.1 General Radio Specifications

Specification	Description
Standards	ETSI: EN 302 217 FCC: Part 101 (2004) ITU-R CEPT
Operating mode	FDD
System Configurations	1+0, 1+1 HSB, 2+0
Operating Frequency Range	71-76GHz, 81-86GHz
Channel Spacing	62.5, 125, 250 MHz, 500 MHz, 1000 MHz, 2000 MHz
Frequency Stability	±10ppm
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 ACMB profile. The maximum TX power with ATPC is no higher than the maximum manually configured TX power.

Table 30: Frequency Tuning Range:

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

8.2 Radio Scripts

Table 31: Radio Scripts

Script ID	ETSI/FCC	Channel BW	Occupied BW	XPIC	Maximum Profile (ACM)	Maximum Profile (Fixed)
5701	ETSI/FCC	62.5 MHz	54 MHz	No	256 QAM	256 QAM
5702	ETSI/FCC	125 MHz	108 MHz	No	512 QAM	512 QAM
5703	ETSI/FCC	250 MHz	230 MHz	No	512 QAM	512 QAM
5733	ETSI	250 MHz	220 MHz	No	512 QAM	512 QAM
5753	ETSI/FCC	250 MHz	230 MHz	Yes	512 QAM	512 QAM
5704	ETSI/FCC	500 MHz	460 MHz	No	512 QAM	512 QAM
5734	ETSI	500 MHz	445 MHz	No	512 QAM	512 QAM
5754	ETSI/FCC	500 MHz	460 MHz	Yes	512 QAM	512 QAM
5706	ETSI/FCC	1000 MHz	880 MHz	No	256 QAM	256 QAM
5756	ETSI/FCC	1000 MHz	880 MHz	Yes	256 QAM	256 QAM
5710	ETSI/FCC	2000 MHz	1599 MHz	No	128 QAM	128 QAM
5760	ETSI/FCC	2000 MHz	1599 MHz	Yes	128 QAM	128 QAM

8.3 Radio Capacity Specifications

Note:	The figures in this section are indicative only. Exact results will depend on multiple factors, such as packet size, type of traffic, headers, etc. The capacity figures for LTE scenario take into account packets encapsulated inside GTP tunnels with IPv4/UDP encapsulation and double VLAN tagging (QinQ). The minimum and maximum capacity is based on Ethernet frame sizes between 64 and 1518 bytes.

Table 32: Radio Capacity – 62.5 MHz Channel Bandwidth (Script 5701)

Profile	Modulation	Minimum Required Capacity Activation Key (Gbps)	Throughput (Mbps)
0	BPSK	50	37-48
1	QPSK	100	77-99
2	8 PSK	100	116-150
3	16 QAM	150	155-201
4	32 QAM	200	195-252
5	64 QAM	225	234-303
6	128 QAM	300	273-354
7	256 QAM	300	313-405

Table 33: Radio Capacity – 125 MHz Channel Bandwidth (Script 5702)

Profile	Modulation	Minimum Required Capacity Activation Key (Gbps)	Throughput (Mbps)
0	BPSK[12]	50	39-51
1	BPSK	100	81-104
2	QPSK	150	163-211
3	8 PSK	250	246-318
4	16 QAM	350	328-425
5	32 QAM	400	421-546
6	64 QAM	500	505-654
7	128 QAM	500	590-764
8	256 QAM	650	674-873
9	512 QAM	1000	759-983

Table 34: Radio Capacity – 250 MHz Channel Bandwidth (Script 5703)

Profile	Modulation	Minimum Required Capacity Activation Key (Gbps)	Throughput (Mbps)
0	BPSK[13]	50	46-60
1	BPSK[14]	100	92-120
2	BPSK	200	186-241
3	QPSK	400	373-484
4	8 PSK	500	576-747
5	16 QAM	1000	768-995
6	32 QAM	1000	960-1244
7	64 QAM	1600	1154-1494
8	128 QAM	1600	1346-1743
9	256 QAM	1600	1538-1993
10	512 QAM	2000	1731-2242

[12] Profile 0 is BPSK at ½ of the script's normal channel bandwidth.

[13] Profile 0 is BPSK at ¼ of the script's normal channel bandwidth.

[14] Profile 1 is BPSK at ½ of the script's normal channel bandwidth.

Table 35: Radio Capacity – 250 MHz Channel Bandwidth (Script 5733)

Profile	Modulation	Minimum Required Capacity Activation Key (Gbps)	Throughput (Mbps)
0	BPSK[13]	50	44-57
1	BPSK[14]	100	88-115
2	BPSK	200	178-230
3	QPSK	400	357-462
4	8 PSK	500	550-713
5	16 QAM	1000	735-951
6	32 QAM	1000	919-1190
7	64 QAM	1600	1103-1429
8	128 QAM	1600	1288-1668
9	256 QAM	1600	1471-1905
10	512 QAM	1600	1656-2145

Table 36: Radio Capacity – 500 MHz Channel Bandwidth (Script 5704)

Profile	Modulation	Minimum Required Capacity Activation Key (Gbps)	Throughput (Mbps)
0	BPSK[13]	100	95-123
1	BPSK[14]	200	192-248
2	BPSK	400	384-498
3	QPSK	1000	791-1024
4	8 PSK	1600	1188-1539
5	16 QAM	1600	1585-2053
6	32 QAM	2000	1982-2567
7	64 QAM	2500	2377-3080
8	128 QAM	3000	2774-3594
9	256 QAM	4000	3171-4108
10	512 QAM	4000	3568-4622

Table 37: Radio Capacity – 500 MHz Channel Bandwidth (Script 5734)

Profile	Modulation	Minimum Required Capacity Activation Key (Gbps)	Throughput (Mbps)
0	BPSK[13]	100	92-120
1	BPSK[14]	200	186-241
2	BPSK	400	372-482
3	QPSK	1000	766-992
4	8 PSK	1600	1150-1489
5	16 QAM	1600	1533-1986
6	32 QAM	2000	1916-2482
7	64 QAM	2500	2301-2980
8	128 QAM	3000	2684-3476
9	256 QAM	3000	3068-3975
10	512 QAM	4000	3452-4472

Table 38: Radio Capacity – 1000 MHz Channel Bandwidth (Script 5706)

Profile	Modulation	Minimum Required Capacity Activation Key (Gbps)	Throughput (Mbps)
0	BPSK[13]	200	185-239
1	BPSK[14]	400	370-480
2	BPSK	1000	761-985
3	QPSK	1600	1524-1974
4	8 PSK	2500	2287-2962
5	16 QAM	3000	3050-3951
6	32 QAM	4000	3813-4939
7	64 QAM	5000	4575-5927
8	128 QAM	6000	5339-6916
9	256 QAM	6000	6101-7904

Table 39: Radio Capacity – 2000 MHz Channel Bandwidth (Script 5710)

Profile	Modulation	Minimum Required Capacity Activation Key (Gbps)	Throughput (Mbps)
0	BPSK[13]	300	323-419
1	BPSK[14]	650	663-859
2	BPSK	1600	1326-1717
3	QPSK	3000	2652-3436
4	8 PSK	4000	4128-5347
5	16 QAM	6000	5505-7131
6	32 QAM	7000	6869-8897
7	64 QAM	8000	8243-9439
8	128 QAM	10000	9439-9941

8.4 Transmit Power Specifications

Note: The accuracy of these values is up to +/-2dB.

Modulation	62.5MHz channels	125MHz channels	250MHz channels	500MHz channels	1000MHz channels	2000MHz channels
BPSK	18	18	18	18	18	18
QPSK	18	18	18	18	18	18
8 QAM	17	17	17	17	17	16
16 QAM	17	17	17	17	17	16
32 QAM	17	17	17	17	17	16
64 QAM	16	16	16	16	16	15
128 QAM	16	16	16	16	16	15
256 QAM	15	15	15	15	15	–
512 QAM	–	14	14	14	–	–

The Pmin for standard TX power is -2dBm for all supported frequencies and modulations.

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

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

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

Modulation	62.5MHz channels	125MHz channels	250MHz channels	500MHz channels	1000MHz channels	2000MHz channels
BPSK	-80.0	-78.8	-75.8	-72.8	-69.8	-67.4
QPSK	-78.0	-76.7	-73.7	-70.5	-67.6	-64.9
8 PSK	-73.2	-72.1	-69.1	-65.8	-62.8	-59.9
16 QAM	-71.3	-70.3	-67.3	-64.3	-61.2	-58.6
32 QAM	-70.0	-67.8	-64.8	-60.7	-58.6	-55.5
64 QAM	-68.3	-65.5	-61.9	-57.6	-55.7	-52.4
128 QAM	-64.1	-63.0	-58.9	-54.7	-52.6	-48.0
256 QAM	-61.0	-59.5	-56.0	-50.4	-49.8	–
512 QAM	–	-55.4	-52.4	-49.4	–	–

The RSL overload is -10 dBm for all supported frequencies and modulations.

The maximum RSL before damage is +10 dBm.

8.6 Mediation Device Losses

Device Type	Maximum Insertion Loss (Main/Secondary)
OMT	2dB
Splitter 1:2	4.5dB
Coupler 1:4	2.2dB/ 6.5±1dB

8.7 Ethernet Latency Specifications

Table 40: Ethernet Latency – 62.5 MHz Channel Bandwidth (Script 5701)

ACMB Profile	Modulation	Latency (µsec) with 10 GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK		614	614	641	696	812	919
1	QPSK		319	322	337	364	420	474
2	8 QAM		225	226	235	253	291	327
3	16 QAM		175	177	185	199	227	255
4	32 QAM		147	148	154	165	189	210
5	64 QAM		129	129	135	144	163	182
6	128 QAM		114	115	120	128	145	161
7	256 QAM		105	105	109	116	131	145

Table 41: Ethernet Latency – 125 MHz Channel Bandwidth (Script 5702)

ACMB Profile	Modulation	Latency (µsec) with 10 GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK[15]		587	587	612	663	776	875
1	BPSK		301	302	315	342	395	446
2	QPSK		164	164	171	185	212	238
3	8 QAM		118	119	124	133	151	169
4	16 QAM		93	95	99	106	121	134
5	32 QAM		121	121	122	123	125	127
6	64 QAM		105	106	107	108	110	111
7	128 QAM		94	95	96	97	99	100
8	256 QAM		86	86	87	89	90	92
9	512 QAM		80	80	81	83	85	86

[15] Profile 0 is BPSK at ½ of the script's normal channel bandwidth.

Table 42: Ethernet Latency – 250 MHz Channel Bandwidth (Script 5703)

ACMB Profile	Modulation	Latency (µsec) with 10 GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK[16]		510	516	539	584	675	765
1	BPSK[17]		264	268	279	303	349	394
2	BPSK		144	144	151	163	187	210
3	QPSK		84	84	88	94	107	119
4	8 QAM		93	93	94	95	97	99
5	16 QAM		76	76	77	79	80	82
6	32 QAM		66	66	67	68	70	72
7	64 QAM		59	59	60	62	64	65
8	128 QAM		54	55	56	57	59	60
9	256 QAM		51	51	52	53	55	57
10	512 QAM		48	48	49	51	52	54

Table 43: Ethernet Latency – 250 MHz Channel Bandwidth (Script 5733)

ACMB Profile	Modulation	Latency (µsec) with 10 GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK[16]		538	538	562	609	706	798
1	BPSK[17]		276	279	291	315	364	411
2	BPSK		148	150	156	169	194	217
3	QPSK		86	87	90	97	110	123
4	8 QAM		96	96	97	99	100	102
5	16 QAM		78	79	80	81	83	84
6	32 QAM		68	68	69	70	72	74
7	64 QAM		61	61	62	63	65	67
8	128 QAM		56	56	57	58	60	62
9	256 QAM		52	52	53	55	56	58
10	512 QAM		49	50	51	52	54	55

[16] Profile 0 is BPSK at ¼ of the script's normal channel bandwidth.

[17] Profile 1 is BPSK at ½ of the script's normal channel bandwidth.

Table 44: Ethernet Latency – 500 MHz Channel Bandwidth (Script 5704)

ACMB Profile	Modulation	Latency (µsec) with 10 GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK[16]		260	260	271	294	339	383
1	BPSK[17]		140	140	146	158	181	203
2	BPSK		80	80	84	90	102	114
3	QPSK		73	73	74	75	77	79
4	8 QAM		56	56	57	59	61	62
5	16 QAM		48	48	49	51	52	54
6	32 QAM		43	43	45	46	48	49
7	64 QAM		40	40	41	43	44	46
8	128 QAM		38	38	39	40	42	44
9	256 QAM		36	36	37	39	40	42
10	512 QAM		35	35	36	37	39	40

Table 45: Ethernet Latency – 500 MHz Channel Bandwidth (Script 5734)

ACMB Profile	Modulation	Latency (µsec) with 10 GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK[16]		268	268	280	303	350	394
1	BPSK[17]		143	144	151	162	187	209
2	BPSK		81	82	86	92	105	117
3	QPSK		74	75	76	77	79	80
4	8 QAM		57	58	59	60	62	63
5	16 QAM		49	49	50	52	53	55
6	32 QAM		44	44	45	47	48	50
7	64 QAM		41	41	42	43	45	47
8	128 QAM		38	38	39	41	43	44
9	256 QAM		36	37	38	39	41	42
10	512 QAM		35	35	36	38	39	41

Table 46: Ethernet Latency – 1000 MHz Channel Bandwidth (Script 5706)

ACMB Profile	Modulation	Latency (µsec) with 10 GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK[16]		143	144	151	163	187	210
1	BPSK[17]		81	82	86	92	105	117
2	BPSK		73	73	752	76	78	79
3	QPSK		48	48	49	51	52	54
4	8 QAM		40	40	41	42	44	45
5	16 QAM		35	35	36	38	40	41
6	32 QAM		33	33	34	35	37	39
7	64 QAM		31	31	32	34	35	37
8	128 QAM		30	30	31	32	35	36
9	256 QAM		29	29	30	31	33	35

Table 47: Ethernet Latency – 2000 MHz Channel Bandwidth (Script 5710)

ACMB Profile	Modulation	Latency (µsec) with 10 GbE Interface						
		Frame Size	64	128	256	512	1024	1518
0	BPSK[16]		91	92	96	103	118	131
1	BPSK[17]		81	82	83	84	86	87
2	BPSK		52	52	53	54	56	58
3	QPSK		37	37	38	39	41	43
4	8 QAM		32	32	33	34	36	37
5	16 QAM		29	29	30	31	33	35
6	32 QAM		28	29	29	31	33	34
7	64 QAM		27	27	28	29	31	33
8	128 QAM		27	27	28	30	31	33

8.8 Interface Specifications

8.8.1 Ethernet Interface Specifications

Supported Ethernet Interfaces for Traffic	1x1000base-X (Optical SFP) OR 2x10GBASE-LR10 (Optical SFP+)		
Supported Ethernet Interfaces for Management	10/100/1000 Base-T (RJ-45)	1 x 10/100/1000Base-T (RJ-45) for traffic or management	1 x 10/100/1000Base-T (RJ-45) for management

The following table lists recommended SFP modules that can be used with IP-50E.

Table 48: SFP Module Recommendations

Part Number	Marketing Model	Item Description
AO-0098-0	SFP-GE-SX-EXT-TEMP	XCVR,SFP,850nm,MM,1.0625 Gbit/s FC/ 1.25 GBE, INDUSTRIAL GRADE,SINGLE PACK KIT
AO-0097-0	SFP-GE-LX-EXT-TEMP	XCVR,SFP,1310nm,1.25Gb,SM,10km,W.DDM,INDUSTRIAL GRADE,SINGLE PACK KIT
AO-0228-0	SFP-GE-COPER-EXT-TMP-LOS-DIS	XCVR,SFP,COOPER 1000BASE-T,RX_LOS DISABLE,INDUSTRIAL TEMP

The following table lists recommended SFP+ modules that can be used with the IP-50E.

Table 49: Approved 10 GbE SFP+ Modules

Part Number	Marketing Model	Marketing Description	Item Description
AO-0264-0	SFP+10GBASE-LR10-EXT-TEMP	SFP+ 10GE OPT 10GBASELR, 10km,EXT-TEMP	XCVR,SFP+,1310nm,SM,10 Gbit/s,10km,INDUSTRIAL GRADE,SINGLE P
AO-0283-0	SFP+10GBASE-SR10-EXT-TEMP	XCVR,SFP+,850nm,MM,10 Gbit/s, INDUSTRIAL GRADE	SFP+10GBASE-SR10-EXT-TEMP

Table 50: Approved QSFP Modules

Part Number	Marketing Model	Marketing Description	Item Description
AO-0280-0	QSFP+40GE-OPT-EXT-TEMP	QSFP+ MPO MALE 40GE EXT-TEMP	XCVR,QSFP+,850nm,MM,40Gbit/s,100m,MPO MALE,W.DDM,IND

Note: Ceragon recommends the use of SFP and SFP+ modules certified by Ceragon, as listed above.

8.9 Carrier Ethernet Functionality

"Jumbo" Frame Support	Up to 9600 Bytes
General	Enhanced link state propagation Header De-Duplication
Integrated Carrier Ethernet Switch	Maximum number of Ethernet services: 1024 plus one pre-defined management service MAC address learning with 64K 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/Hierarchical) Per interface and per queue traffic shaping Hierarchical-QoS (H-QoS) – 2K service level queues 2 Gbit packet buffer
Network resiliency[18]	MSTP ERP (G.8032)
OAM	CFM (802.1ag)
Performance Monitoring	Per port Ethernet counters (RMON/RMON2) Radio ACMB statistics Enhanced radio Ethernet statistics (Throughput, Capacity, Utilization)

[18] MSTP and G.8032 are planned for future release.

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

8.10 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)
- Precision Time Protocol (version 2, IEEE1588-2008)

8.11 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-50E[19], and NMS
Performance Monitoring	Integral with onboard memory per ITU-T G.826/G.828

[19] 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).

8.12 Mechanical Specifications

	Direct Mount HW (For parabolic antennas)	43dBi Integrated Antenna
Module Dimensions	322mm(H), 227/270mm(W), 86mm(D) 12.67”(H), 8.93”/10.62”(W), 3.38”(D)	341mm(H), 270/276mm(W), 103mm(D) 13.42”(H), 10.62/10.86”(W), 4.05”(D)
Module Weight	5.5 kg/12.12 lbs.	7 kg/15.43 lbs.
Pole Diameter Range (for Remote Mount Installation)	8.89 cm – 11.43 cm 3.5” – 4.5”	

8.13 Standards Compliance

Specification	Standard
Radio Spectral Efficiency	ETSI: EN 302 217-2 Certification ordinance Article 2-1-31-5 (Japan)
EMC	EN 301 489-1, EN 301 489-4, Class A (Europe) FCC 47 CFR, part 15, subpart B, class A (US) ICES-003, Class A (Canada) TEC/SD/DD/EMC-221/05/OCT-16, Class A (India) IEC 61000-4-29
Surge	EN61000-4-5, Class 4 (for PoE port)
Safety	EN 60950-1, EN 62368-1 IEC 60950-1, IEC 62368-1 UL 60950-1, UL 62368-1 CAN/CSA C22.2 NO 60950-1, CAN/CSA C22.2 NO 62368-1 EN 60950-22 IEC 60950-22 UL 60950-22 CAN/CSA C22.2 NO 60950-22

8.14 Environmental Specifications

- 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

    Temperature range for exceptional temperatures; tested successfully, with limited margins:
    -45°C to +60°C/-49°F to +140°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

8.15 Antenna Specifications

Direct Mount:

MTI, CommScope (VHLP)

Remote Mount:

Waveguide Standard	Antenna Flange
WR12	UG387/U

8.16 Integrated Antenna

The following table describes the electrical parameters of the integrated antenna:

Frequency coverage	71-86 GHz
Gain	43dBi
VSWR	1.6
3dB beam width (azimuth and elevation)	1°
Polarization	Single Linear: 45° (diamond)
Co/cross-polar ratio	>35dB
Front to back ratio	>60dB
Side lobe suppression	ETSI EN 3020217-42 V1 5.1 CLASS 2 CLASS 3 FCC 47CFR101.115

8.17 Power Input Specifications

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

8.18 Power Consumption Specifications

Unit Configuration	Power Consumption
Active	58W
Standby	47W

8.19 Power Connection Options

Power Source and Range	Data Connection Type	Connection Length	DC Cable Type / Gage
Ext DC -(40.5 ÷ 60)VDC (Using an RJ-45 to DC cable adaptor)	Optical	≤ 75m (247ft)	18AWG
		76m ÷ 150m (248ft ÷ 493ft)	14AWG
		151m ÷ 300m (494ft ÷ 984ft)	12AWG
Active PoE Injector	Electrical	≤ 100m (328ft)	CAT5e (24AWG)
Passive PoE Injector for Power Redundancy Only for use in non-XPIC configurations (≤ 57W)	Electrical	≤ 100m (328ft)	CAT5e (24AWG)

Note: For details and marketing models of the recommended PoE options and when they are used, see *PoE Injector* on page 35.

8.20 PoE Injector Specifications – Standard PoE

The specifications in this section are for the standard PoE Injector units with the following marketing models:

- PoE_Inj_AO_2DC_24V_48V
- PoE_Inj_AO

8.20.1 Power Input

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

8.20.2 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**
  - Temperature range for exceptional temperatures; tested successfully, with limited margins: **-45°C to +60°C/-49°F to +140°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

8.20.3 Standards Requirements

Specification	Standard
EMC	EN 301 489-1, EN 301 489-4, Class A (Europe) FCC 47 CFR, part 15, class B (US) ICES-003, Class B (Canada) TEC/EMI/TEL-001/01, Class A (India)
Safety	EN 60950-1 IEC 60950-1 UL 60950-1 CSA-C22.2 No.60950-1 EN 60950-22 UL 60950-22 CSA C22.2.60950-22

8.20.4 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

8.21 PoE Injector Specifications – Passive PoE

The specifications in this section are for the passive PoE Injector for use with power redundancy, with the following marketing model:

- AC_POE_STD_PWR_INDOOR

8.21.1 Power Input

AC Input range	90VAC to 264VAC

8.21.2 Environmental

- Operating Temperature Range: -10°C to +40°C/+14°F to +104°F
- Non-Operating Temperature Range: -20°C to +65°C/-4°F to +149°F
- 5%RH to 90%RH

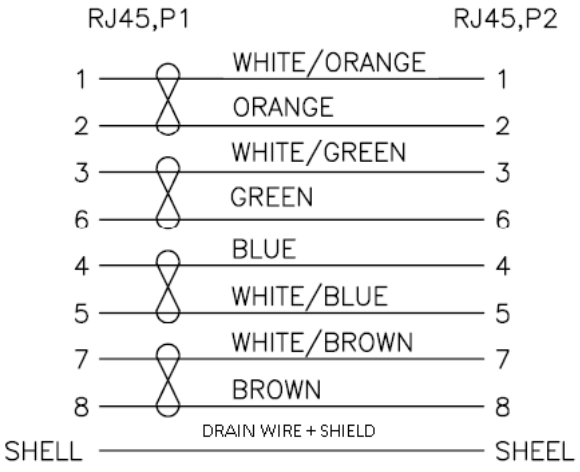
8.21.3 Mechanical

Module Dimensions	(H)44mm x (W)80mm x (L)166mm (H)1.7inch x (W)3.1inch(D)6.5inch
Module Weight	0.5kg/1.1lbs

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
Wire gage	24 AWG
Stranding	Solid
Voltage rating	70V
Shielding	Braid + Foil
Pinout	

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
Wire gage	18 AWG (for ≤150m (492ft) installations, optical connections) 14 AWG (for 150m ÷ 300m (492ft ÷ 984ft) installations, electrical connections)
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

9. Appendix A – Marketing Models

The following IP-50E hardware models are available.

Table 51: IP-50E Marketing Model Examples

Marketing Model	Explanation
IP-50E-DX0H-H-ESSQ	TX High, external antenna
IP-50E-DX0H-L-ESSQ	TX Low, external antenna
IP-50E-DX0H-H-ESSQ-43IA	TX High, 43 dBi integrated antenna
IP-50E-DX0H-L-ESSQ-43IA	TX Low, 43 dBi integrated antenna