Cambium
PTP 650 Series
User Guide

System Release 650-01-00

Cambium Networks

Accuracy

While reasonable efforts have been made to assure the accuracy of this document, Cambium Networks assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. Cambium reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Cambium does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others. It is possible that this publication may contain references to, or information about Cambium products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Cambium intends to announce such Cambium products, programming, or services in your country.

Copyrights

This document, Cambium products, and 3rd Party software products described in this document may include or describe copyrighted Cambium and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Cambium, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Cambium, its licensors, or the 3rd Party software supplied material contained in the Cambium products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Cambium. Furthermore, the purchase of Cambium products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Cambium or other 3rd Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Cambium.

License Agreements

The software described in this document is the property of Cambium and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

High Risk Materials

Cambium and its supplier(s) specifically disclaim any express or implied warranty of fitness for any high risk activities or uses of its products including, but not limited to, the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, life support, or weapons systems ("High Risk Use"). Any High Risk is unauthorized, is made at your own risk and you shall be responsible for any and all losses, damage or claims arising out of any High Risk Use.

Contents

About This User Guide

This guide describes the planning, installation, configuration and operation of the Cambium PTP 650 Series of point-to-point wireless Ethernet bridges. It is intended for use by the system designer, system installer and system administrator.

For radio network design, refer to the following chapters:

- Chapter 1: Product description
- Chapter 2: System hardware
- Chapter 3: System planning
- Chapter 4: Legal and regulatory information

For radio equipment installation, refer to the following chapter:

- Chapter 5: Installation

For system configuration, monitoring and fault-finding, refer to the following chapters:

- Chapter 6: Configuration and alignment
- Chapter 7: Operation
- Chapter 8: Troubleshooting

Contacting Cambium Networks

Support website:	http://www.cambiumnetworks.com/support
Main website:	http://www.cambiumnetworks.com
Sales enquiries:	solutions@cambiumnetworks.com
Support enquiries:	support@cambiumnetworks.com
Telephone number list:	http://www.cambiumnetworks.com/contact
Address:	Cambium Networks Limited, Linhay Business Park, Eastern Road, Ashburton, Devon, UK, TQ13 7UP

Purpose

Cambium Networks Point-To-Point (PTP) documents are intended to instruct and assist personnel in the operation, installation and maintenance of the Cambium PTP equipment and ancillary devices. It is recommended that all personnel engaged in such activities be properly trained.

Cambium disclaims all liability whatsoever, implied or express, for any risk of damage, loss or reduction in system performance arising directly or indirectly out of the failure of the customer, or anyone acting on the customer's behalf, to abide by the instructions, system parameters, or recommendations made in this document.

Cross references

References to external publications are shown in italics. Other cross references, emphasized in blue text in electronic versions, are active links to the references.

This document is divided into numbered chapters that are divided into sections. Sections are not numbered, but are individually named at the top of each page, and are listed in the table of contents.

Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents. Send feedback to support@cambiumnetworks.com.

Important regulatory information

The PTP 650 product is certified as an unlicensed device in frequency bands where it is not allowed to cause interference to licensed services (called primary users of the bands).

Radar avoidance

In countries where radar systems are the primary band users, the regulators have mandated special requirements to protect these systems from interference caused by unlicensed devices. Unlicensed devices must detect and avoid co-channel operation with radar systems.

The PTP 650 provides detect and avoid functionality for countries and frequency bands requiring protection for radar systems.

Installers and users must meet all local regulatory requirements for radar detection. To meet these requirements, users must install a license key for the correct country during commissioning of the PTP 650. If this is not done, installers and users may be liable to civil and criminal penalties.

Contact the Cambium helpdesk if more guidance is required.

USA and Canada specific information

The USA Federal Communications Commission (FCC) has asked manufacturers to implement special features to prevent interference to weather radar systems that operate in the band 5600 MHz to 5650 MHz. These features must be implemented in all products able to operate outdoors in the band 5470 MHz to 5725 MHz.

Manufacturers must ensure that such radio products cannot be configured to operate outside of FCC rules; specifically it must not be possible to disable or modify the radar protection functions that have been demonstrated to the FCC.

In order to comply with these FCC requirements, Cambium supplies variants of the PTP 650 for operation in the USA or Canada. These variants are only allowed to operate with license keys that comply with FCC/IC rules. In particular, operation of radio channels overlapping the band 5600-5650 MHz is not allowed and these channels are permanently barred.

In addition, other channels may also need to be barred when operating close to weather radar installations.

Note

To ensure compliance with FCC rules (KDB 443999: Interim Plans to Approve UNII Devices Operating in the 5470 - 5725 MHz Band with Radar Detection and DFS Capabilities), follow Avoidance of weather radars (USA only) on page 3-20.

Other variants of the PTP 650 are available for use in the rest of the world, but these variants are not supplied to the USA or Canada except under strict controls, when they are needed for export and deployment outside the USA or Canada.

Specific expertise and training required for professional installers

To ensure that the PTP 650 is installed and configured in compliance with the requirements of Industry Canada and the FCC, installers must have the radio engineering skills and training described in this section. This is particularly important when installing and configuring a PTP 650 system for operation in the 5.4 GHz UNII band.

Avoidance of weather radars

The installer must be familiar with the requirements in FCC KDB 443999. Essentially, the installer must be able to:

- Access the FCC data base of weather radar location and channel frequencies.
- Use this information to correctly configure the product (using the GUI) to avoid operation on channels that should be barred according to the guidelines that are contained in the KDB and explained in detail in this user guide.

External antennas

When using a connectorized version of the product (as compared to the version with an integrated antenna), the conducted transmit power may need to be reduced to ensure the regulatory limit on transmitter EIRP is not exceeded. The installer must have an understanding of how to compute the effective antenna gain from the actual antenna gain and the feeder cable losses.

The range of permissible values for maximum antenna gain and feeder cable losses are included in this user guide together with a sample calculation. The product GUI automatically applies the correct conducted power limit to ensure that it is not possible for the installation to exceed the EIRP limit, when the appropriate values for antenna gain and feeder cable losses are entered into the GUI.

Ethernet networking skills

The installer must have the ability to configure IP addressing on a PC and to set up and control products using a web browser interface.

Lightning protection

To protect outdoor radio installations from the impact of lightning strikes, the installer must be familiar with the normal procedures for site selection, bonding and grounding. Installation guidelines for the PTP 650 can be found in Chapter 2: System hardware and Chapter 5: Installation.

Training

The installer needs to have basic competence in radio and IP network installation. The specific requirements applicable to the PTP 650 should be gained by reading Chapter 5: Installation and Chapter 6: Configuration and alignment and by performing sample set ups at base workshop before live deployments.

Problems and warranty

Reporting problems

If any problems are encountered when installing or operating this equipment, follow this procedure to investigate and report:

1. Search this document and the software release notes of supported releases.
2. Visit the support website.
3. Ask for assistance from the Cambium product supplier.
4. Gather information from affected units, such as any available diagnostic downloads.
5. Escalate the problem by emailing or telephoning support.

Repair and service

If unit failure is suspected, obtain details of the Return Material Authorization (RMA) process from the support website.

Hardware warranty

Cambium's standard hardware warranty is for one (1) year from date of shipment from Cambium Networks or a Cambium distributor. Cambium Networks warrants that hardware will conform to the relevant published specifications and will be free from material defects in material and workmanship under normal use and service. Cambium shall within this time, at its own option, either repair or replace the defective product within thirty (30) days of receipt of the defective product. Repaired or replaced product will be subject to the original warranty period but not less than thirty (30) days.

To register PTP products or activate warranties, visit the support website. For warranty assistance, contact the reseller or distributor.

⚠ **Caution**

Using non-Cambium parts for repair could damage the equipment or void warranty. Contact Cambium for service and repair instructions.

Portions of Cambium equipment may be damaged from exposure to electrostatic discharge. Use precautions to prevent damage.

Security advice

Cambium Networks systems and equipment provide security parameters that can be configured by the operator based on their particular operating environment. Cambium recommends setting and using these parameters following industry recognized security practices. Security aspects to be considered are protecting the confidentiality, integrity, and availability of information and assets. Assets include the ability to communicate, information about the nature of the communications, and information about the parties involved.

In certain instances Cambium makes specific recommendations regarding security practices, however the implementation of these recommendations and final responsibility for the security of the system lies with the operator of the system.

Warnings, cautions, and notes

The following describes how warnings and cautions are used in this document and in all documents of the Cambium Networks document set.

Warnings

Warnings precede instructions that contain potentially hazardous situations. Warnings are used to alert the reader to possible hazards that could cause loss of life or physical injury. A warning has the following format:

Warning

Warning text and consequence for not following the instructions in the warning.

Cautions

Cautions precede instructions and are used when there is a possibility of damage to systems, software, or individual items of equipment within a system. However, this damage presents no danger to personnel. A caution has the following format:

Caution

Caution text and consequence for not following the instructions in the caution.

Notes

A note means that there is a possibility of an undesirable situation or provides additional information to help the reader understand a topic or concept. A note has the following format:

Note

Note text.

Caring for the environment

The following information describes national or regional requirements for the disposal of Cambium Networks supplied equipment and for the approved disposal of surplus packaging.

In EU countries

The following information is provided to enable regulatory compliance with the European Union (EU) directives identified and any amendments made to these directives when using Cambium equipment in EU countries.

Disposal of Cambium equipment

European Union (EU) Directive 2002/96/EC Waste Electrical and Electronic Equipment (WEEE)

Do not dispose of Cambium equipment in landfill sites. For disposal instructions, refer to http://www.cambiumnetworks.com/support

Disposal of surplus packaging

Do not dispose of surplus packaging in landfill sites. In the EU, it is the individual recipient’s responsibility to ensure that packaging materials are collected and recycled according to the requirements of EU environmental law.

In non-EU countries

In non-EU countries, dispose of Cambium equipment and all surplus packaging in accordance with national and regional regulations.

Chapter 1: Product description

This chapter provides a high level description of the PTP 650 product. It describes in general terms the function of the product, the main product variants and the main hardware components. The following topics are described in this chapter:

- Overview of the PTP 650 on page 1-2 introduces the key features, typical uses, product variants and components of the PTP 650.
- Wireless operation on page 1-6 describes how the PTP 650 wireless link is operated, including modulation modes, power control and spectrum management.
- Ethernet bridging on page 1-15 describes how the PTP 650 controls Ethernet data, in both the customer data and system management networks.
- System management on page 1-23 introduces the PTP 650 management system, including the web interface, installation, configuration, security, alerts and upgrades.

Overview of the PTP 650

This section introduces the key features, typical uses, product variants and components of the PTP 650.

Purpose

Cambium PTP 650 Series Bridge products are designed for Ethernet bridging over point-to-point microwave links in unlicensed and lightly-licensed frequency bands between 4.9 GHz and 5.8 GHz. Users must ensure that the PTP 650 Series complies with local operating regulations.

The PTP 650 Series acts as a transparent bridge between two segments of the operator's network. In this sense, it can be treated as a virtual wired connection between two points. The PTP 650 Series forwards 802.3 Ethernet frames destined for the other part of the network and filters frames it does not need to forward. The system is transparent to higher-level protocols such as VLANs and Spanning Tree.

Key features

The PTP 650 is a high performance wireless bridge for Ethernet traffic with a maximum throughput of 450 Mbps. It is capable of operating in line-of-sight (LOS), near-LOS and non-LOS propagation condition. Its maximum LOS range is 200 km.

The PTP 650 operates in unlicensed and lightly-licensed frequency bands between 4.9 and 5.8 GHz. It has a very high spectral efficiency of 10 bps/Hz and supports a channel bandwidth of up to 45 MHz. The integrated ODU has its own flat plate antenna. The connectorized ODU is designed for use with an external antenna.

The wireless link is TDD based and supports both symmetric and asymmetric configurations.

From a network point-of-view, the PTP 650 wireless link is a transparent Layer 2 bridge. It supports up to three Gigabit Ethernet ports. Two ports support twisted pair Gigabit Ethernet. One of them is capable of providing power via standard 802.3at PoE to an external device such as a video surveillance camera or a wireless access point. The third port accepts either a twisted pair or fibre GE SFP module.

PTP 650 has extensive quality of service (QoS) classification capability and supports up to eight levels of queues. Management of the unit may be via the same interface as the bridged traffic (in-band management) or on a separate port (out-of-band local management).

Table 1 gives a summary of the main PTP 650 characteristics.

Table 1 Main characteristics of the PTP 650 Series

Characteristic	Value
Topology	PTP
Wireless link condition	LOS, near LOS or non-LOS
Range	Up to 200 km
Duplexing	TDD (symmetric and asymmetric)
Connectivity	Ethernet
Operating frequencies	4.9 to 5.8 GHz
Channel bandwidth	10, 20, 40 or 45 MHz
High spectral efficiency	Up to 10 bps/Hz
Data rate	Up to 450 Mbps (45 MHz channel BW)

Frequency bands

The PTP 650 ODU can be configured by the user to operate in the following bands:

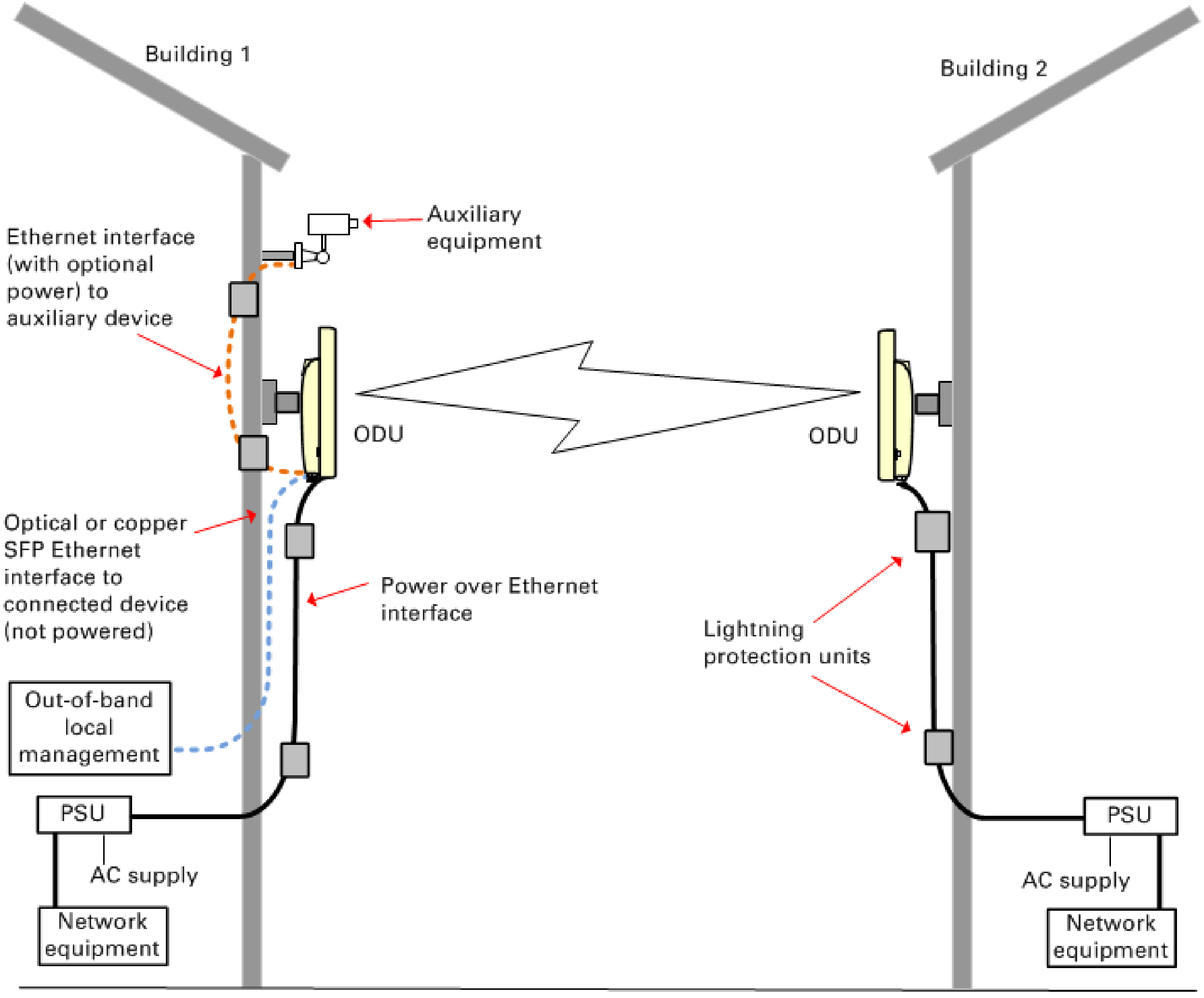
- 4900 to 4990 MHz
- 5470 to 5725 MHz
- 5725 to 5875 MHz

Typical bridge deployment

The PTP 650 is an “all outdoor” solution consisting of a wireless bridge between two sites. Each site installation consists of an integrated or connectorized outdoor unit (ODU) and a power injector (PSU) (Figure 1). The ODU provides the following interfaces:

- PSU port: This provides proprietary power over Ethernet and connection to the management and/or data networks via 100BASE-TX or 1000BASE-T Ethernet. In the basic configuration, this is the only Ethernet connection to the ODU.
- SFP port: This provides an optical or copper Gigabit Ethernet interface for out-of-band local management, user data or user data with in-band management.
- Aux port: This provides an optional power and 100BASE-TX or 1000BASE-T Ethernet connection to an IEEE803.2at device such as a video camera or wireless access point.

Figure 1 PTP 650 typical bridge deployment


Building 1
Building 2
Auxiliary equipment
Ethernet interface (with optional power) to auxiliary device
ODU
ODU
Optical or copper SFP Ethernet interface to connected device (not powered)
Power over Ethernet interface
Lightning protection units
Out-of-band local management
PSU
AC supply
Network equipment
PSU
AC supply
Network equipment

Hardware overview

The main hardware components of the PTP 650 are as follows:

- Outdoor unit (ODU): The ODU is a self-contained transceiver unit that houses both radio and networking electronics. The ODU is supplied in the following product variants:
  - Integrated or Connectorized: The ODU may be either Integrated (attached to its own flat plate antenna) or connectorized (without an antenna).
  - FCC/IC, EU or RoW: These variants are for deployment in the USA and Canada, the EU and the rest of the world respectively.
- Power supply unit (PSU): There is a choice of two PSUs:
  - The AC Power Injector is suitable for installations without an auxiliary device.
  - The AC+DC power injector is required when powering from a DC supply or when the PSU is needed to operate at extreme temperatures.
- Antennas and antenna cabling: Connectorized ODUs require external antennas connected using RF cable.
- Ethernet cabling: All configurations require a copper Ethernet Cat5e connection from the ODU (PSU port) to the PSU. Advanced configurations may also require one or both of the following:
  - A copper or optical Ethernet connection from the ODU (SFP port) to network terminating equipment or another device.
  - A copper Ethernet Cat5e connection from the ODU (Aux port) to an auxiliary device.
- Lightning protection unit (LPU): LPUs are installed in the PSU and Aux copper drop cables to provide transient voltage surge suppression.
- Ground cables: ODU, LPUs and outdoor copper Ethernet cables are bonded to the site grounding system using ground cables.

For more information about these components, including interfaces, specifications and Cambium part numbers, refer to Chapter 2: System hardware.

Wireless operation

This section describes how the PTP 650 wireless link is operated, including modulation modes, power control and security.

Time division duplexing

TDD cycle

PTP 650 links operate using Time Division Duplexing (TDD). They use a TDD cycle in which the ODUs alternately transmit and receive TDD bursts. The TDD cycle is illustrated in Figure 2. The steps in the cycle are as follows:

1. The TDD master transmits a burst to the TDD slave.
2. A delay occurs as the master-slave burst propagates over the link.
3. The slave receives the burst from the master.
4. The slave processes the master-slave burst.
5. The slave transmits a burst to the master.
6. A delay occurs as the slave-master burst propagates over the link.
7. The master receives the burst from the slave.
8. The master transmits the next burst to the slave.

TDD frame parameters

The TDD burst duration varies depending on the following:

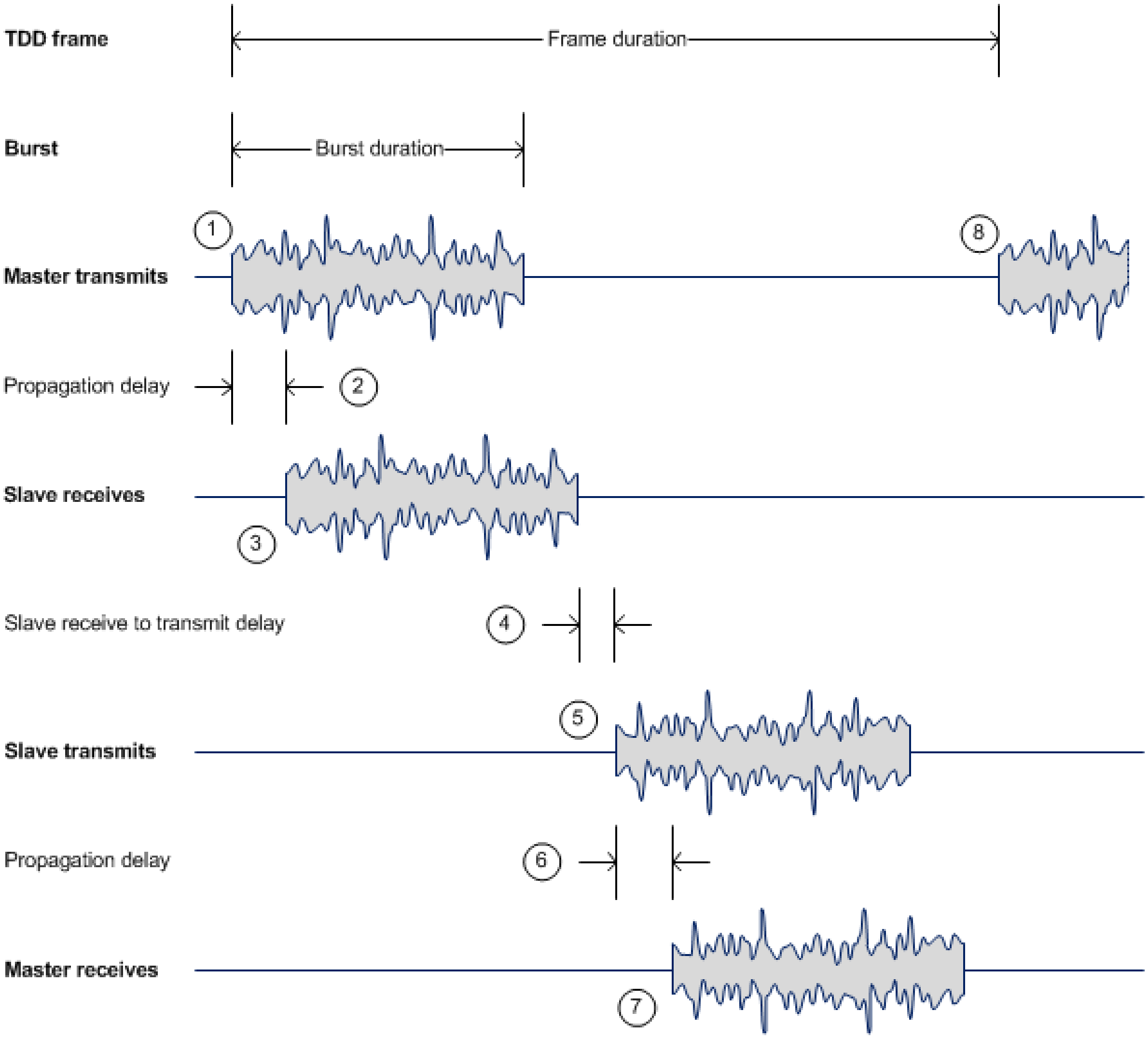
- Channel bandwidth
- Link range
- Link optimization mode
- Link symmetry
- Offered traffic loading.

The TDD frame duration varies depending on the following:

- TDD burst duration master-slave.
- TDD burst duration slave-master.
- Link range.

The propagation delay in Step 2 is necessarily equal to the propagation delay in Step 6, and is determined solely by the link range. There may be added delays between rx and tx on the master and slave to minimize interference, as set up by the link planner or installer.

Figure 2 TDD cycle



Channel selection

The PTP 650 series links are capable of transmitting and receiving on the same channel or on different channels. In other words, the slave-master direction may use a different channel from the master-slave direction. Independent selection of transmit and receive frequencies can be useful in planned networks or for countering interference.

When links operate in radar avoidance regions, each unit monitors its transmit channel for the presence of radar signals. Therefore, the transmit and receive channels are always identical.

Link mode optimization

Link mode optimization allows the PTP 650 link to be optimized according to the type of traffic that will be bridged. The link supports two modes, IP Traffic and TDM Traffic.

IP traffic

IP Traffic mode is optimized to provide the maximum possible link capacity. IP Traffic mode is an appropriate choice where applications in the bridged networks provide some measure of reliable transmission, and where very low latency is not critical. IP mode supports both fixed and adaptive link symmetry (see Link symmetry on page 1-8).

TDM traffic

TDM Traffic mode is optimized to provide the lowest possible latency. TDM Traffic mode additionally implements a more conservative approach to adaptive modulation, leading to lower error rates in fading channels at the expense of slightly lower link capacity. TDM Traffic mode is an appropriate choice for delay intolerant data without reliable transmission (for example voice over IP data).

Link symmetry

The PTP 650 series provides four configuration options for apportioning the available capacity between the two link directions.

- **Symmetric –** The Master and Slave have equal capacity. The PTP 650 series achieves this by allocating an equal Burst Duration for the Master and the Slave.
- **2:1 –** The capacity in the direction Master to Slave is twice that of the direction Slave to Master. The PTP 650 series achieves this by setting the Burst Duration of the Master to twice that of the Slave.
- **1:2 –** The capacity in the direction Slave to Master is twice that of the direction Master to Slave. The PTP 650 series achieves this by setting the Burst Duration of the Slave to twice that of the Master.
- **Adaptive –** This is only available on the Full variant. The capacity allocated to a given link direction is dependent on the offered level of network traffic in both link directions. If the level of offered traffic in both directions is equally high or equally low, the PTP 650 will allocate equal capacity to both directions. If however the offered level of traffic is greater in one direction, it is allocated a greater proportion of the overall link capacity. The PTP 650 series achieves this by increasing (or decreasing) the duration of the Transmit Burst in a given link direction as the offered level of network traffic increases (or decreases) in this same direction. This is done independently for the two directions.

Adaptive mode is not available in the following configurations:

- When link mode optimization is set to TDM Traffic (see Link mode optimization on page 1-8).
- In regions where radar avoidance is operational (see Radar avoidance on page 1-12).
- When the ODU is not a Full variant.

OFDM and channel bandwidth

The PTP 650 series transmits using Orthogonal Frequency Division Multiplexing (OFDM). This wideband signal consists of many equally spaced sub-carriers. Although each sub carrier is modulated at a low rate using conventional modulation schemes, the resultant data rate from the sub-carriers is high. OFDM works exceptionally over a Non-Line-of-Sight (NLoS) channel.

The channel bandwidth of the OFDM signal is configurable to one of the following values: 10, 20, 40 and 45 MHz. Higher bandwidths provide greater link capacity at the expense of using more spectrum. Systems configured for a narrower channel bandwidth provide better receiver sensitivity and can also be an appropriate choice in deployments where the amount of free spectrum is limited.

Each channel is offset in center frequency from its neighboring channel by 10 or 5 MHz.

Note

The Channel Bandwidth must be configured to the same value at both ends of the link. Not all channel bandwidths are available in all regulatory bands.

Spectrum management

The spectrum management feature of the PTP 650 Series monitors the available wireless spectrum and directs both ends of the wireless link to operate on a channel with a minimum level of co-channel and adjacent channel interference.

Spectrum management measurements

The PTP 650 Series performs two mean signal measurements per TDD cycle, per channel. This mean measurement represents the mean received signal power for the 40 microsecond measurement period.

The Spectrum Management algorithm collects measurements equally from all channels in the operating band. This process is called the Channel Availability Check (CAC). The CAC uses a round-robin channel selection process to collect an equal amount of measurements from each channel. The CAC measurement process is not altered by the channel barring process. Measurements are still collected for all channels irrespective of the number of barred channels.

Measurement analysis

Spectrum Management uses statistical analysis to process the received peak and mean measurement. The statistical analysis is based on a fixed, one minute, measurement quantization period. Spectrum Management collects data for the specified quantization period and only at the end of the period is the statistical analysis performed.

Statistical summary

The display of statistical measurement on the spectrum management page always shows a statistical summary of all channel measurement. The statistical summary is controlled by the Statistics Window attribute. This attribute defaults to a value of twenty minutes, which means that the mean and percentile values displayed for each channel are calculated over the 20 minute period. All channel decisions are made using the values computed over the statistics window period.

Spectrum management in fixed frequency mode

The transmit and receive frequencies can be fixed in a PTP 650 wireless link. Once fixed frequency mode is configured, the spectrum management software will not attempt to move the wireless link to a channel with lower co-channel and adjacent-channel interference. Therefore this mode of operation is only recommended for deployments where the installer has a good understanding of the prevailing interference environment. Care must also be taken to ensure that the frequency allocations at each end of the link are compatible.

Fixed frequency mode is not available in regions where radar detection is required by the regulations.

Adaptive modulation

The PTP 650 series can transport data over the wireless link using a number of different modulation modes ranging from 256QAM 0.81 to BPSK 0.63. For a given channel bandwidth and TDD frame structure, each modulation mode transports data at a fixed rate. Also, the receiver requires a minimum signal to noise ratio in order to successfully demodulate a given modulation mode. Although the more complex modulations such as 256QAM 0.81 will transport data at a much higher rate than the less complex modulation modes, the receiver requires a much higher signal to noise ratio.

The PTP 650 series provides an adaptive modulation scheme where the receiver constantly monitors the quality of the received signal and notifies the far end of the link of the optimum modulation mode with which to transmit. In this way, optimum capacity is achieved at all times. This is one of a number of features which allows the PTP 650 to operate in challenging non-line of sight radio channels.

Note

PTP LINKPlanner includes an estimate of mean data rate, the data rate provided by each modulation and the percentage of time spent in each modulation mode.

MIMO

Multiple-Input Multiple-Output (MIMO) techniques provide protection against fading and increase the probability that the receiver will decode a usable signal. When the effects of MIMO are combined with those of OFDM techniques and a high link budget, there is a high probability of a robust connection over a non-line-of-sight path.

The PTP 650 transmits two signals on the same radio frequency, one of which is vertically polarized and the other horizontally polarized. Depending on the channel conditions, the PTP 650 will adapt between two modes of operation:

- **Dual Payload**: When the radio channel conditions allow, the PTP 650 will transmit two different and parallel data streams, one on the vertical channel and one on the horizontal channel. This doubles the capacity of the PTP 650.
- **Single Payload**: As the radio channel becomes more challenging, the PTP 650 has the ability to detect this and switch to a mode which transmits the same data stream on both vertical and horizontal channels. This provides polar diversity and is another key feature which allows the PTP 650 to operate in challenging non- line of sight radio channels.

Lower order modulations (BPSK 0.63 up to QPSK 0.87) only operate in single payload mode. Higher order modulations (16QAM 0.63 to 256QAM 0.81) are available in single payload mode and dual payload mode. The switching between modes is automatically controlled by the adaptive modulation feature described in Adaptive modulation on page 1-10.

Note

The system automatically chooses between dual and single payload to try to increase the capacity of a link. However the user can disable the dual payload mode, forcing the more robust option of single payload.

Dynamic spectrum optimization

The PTP 650 series uses an interference mitigation technique known as Dynamic Spectrum Optimization (DSO). Both the Master and Slave continually monitor for interference on all channels and then select the best frequency of operation. This is a dynamic process where the PTP 650 can continually move channels in response to changes in interference. Two modes of operation are available:

- First mode: the two link directions are forced to select the same frequency, determined by the Master.
- Second mode: the frequency of operation can be determined independently for each direction. This mode is not permitted in radar regions.

Radar avoidance

In regions where protection of radars is part of the local regulations, the PTP 650 must detect interference from radar-like systems and avoid co-channel operation with these systems.

To meet this requirement, the PTP 650 implements the following features:

- The radar detection algorithm will always scan a usable channel for 60 seconds for radar interference before making the channel an available channel.
- This compulsory channel scan will mean that there is at least 60 seconds service outage every time radar is detected and that the installation time is extended by at least 60 seconds even if no radar is found.
- When operating on a channel, the spectrum management algorithm implements a radar detection function which looks for impulsive interference on the operating channel. If impulsive interference is detected, spectrum management will mark the current operating channel as having detected radar (unavailable channel) and initiate a channel hop to an available channel. The previous operating channel will remain in the unavailable state for thirty minutes after the impulsive interference pulse was detected.
- After the thirty minutes have expired the channel will be returned to the usable channel pool.

There is a secondary requirement for bands requiring radar avoidance. Regulators have mandated that products provide a uniform loading of the spectrum across all devices. In general, this prevents operation with fixed frequency allocations. However:

- ETSI regulations do allow frequency planning of networks (as that has the same effect of spreading the load across the spectrum).
- The FCC does allow channels to be barred if there is actually interference on them.

Note

Fixed frequency allocation is not recommended in radar avoidance regions, as any radar detection would cause a system outage of at least 30 minutes.

Encryption

The PTP 650 supports optional encryption for data transmitted over the wireless link. The encryption algorithm used is the Advanced Encryption Standard (AES) with 128-bit and 256-bit key size. AES is a symmetric encryption algorithm approved by U.S. Government organizations (and others) to protect sensitive information. The AES implementation in PTP 650 is approved to FIPS-197. Encryption is enabled through the purchase of an upgrade.

License keys and regulatory bands

The PTP 650 license key specifies the country of operation for the ODU, and lists the regulatory bands that are licensed by regulators in that country. If a license key provides access to more than one regulatory band, PTP 650 provides a choice between the available bands. In each regulatory band, PTP 650 sets the following aspects of wireless operation to comply with the applicable regulations:

- Maximum transmit power
- Radar avoidance
- Transmit power reduction in edge channels
- Frequency range
- Channel plan

The country of operation (and thus the supported regulatory bands) can be changed by generating a new license key at the License Key Generator page of the Cambium web-site, and entering the new license key using the Installation Wizard.

Caution

To avoid possible enforcement action by the country regulator, always operate links in accordance with local regulations.

PTP networks

Using Dynamic Spectrum Optimization

The Dynamic Spectrum Optimization (DSO) feature allows a PTP 650 unit to select wireless channels for a lower level of radio frequency (RF) interference. This approach is appropriate where the network consists of a small number of PTP links, or where the RF interference is predominantly from equipment belonging to other operators.

Using frequency planning

Networks will benefit from the use of fixed channel allocations if (a) the network consists of multiple PTP links, and (b) RF interference predominantly arises from equipment in the same network.

Frequency planning is the exercise of assigning operating channels to PTP units so as to minimize RF interference between links. Frequency planning must consider interference from any PTP unit to any other PTP unit in the network. Low levels of interference normally allow for stable operation and high link capacity.

The frequency planning task is made more straightforward by use of the following techniques:

- Using several different channels
- Separating units located on the same mast
- Using high performance (directional) external antennas

For help with planning networks, refer to Chapter 3: System planning, or contact your Cambium distributor or re-seller.

Ethernet bridging

This section describes how the PTP 650 processes Ethernet data, in both the customer and system management networks.

Ethernet ports

The PTP 650 Series ODU has three Ethernet ports:

- **Main PSU**: The Main PSU port provides a copper Ethernet interface for 100BASE-TX and 1000BASE-T, and accepts power from the AC+DC Enhanced Power Injector or the AC Power Injector to the ODU using a proprietary power over Ethernet (PoE) method.
- **Aux:** The Aux port provides a copper Ethernet interface for 100BASE-TX and 1000BASE-T, and supplies power from the ODU to external equipment using standards-based power over Ethernet (PoE) complying with IEEE 802.3at.
- **SFP:** The SFP port is a small format pluggable receptacle accepting copper or optical plug-in modules supplied as part of the SFP module kits on page 2-27.

Each of the three Ethernet ports can be allocated for customer data or network management in the following ways:

- **Disabled:** The port is not in use for customer data or network management.
- **Data Only**: The port is connected to the customer data network only.
- **Data and In-Band Management**: The port is connected to the customer data network and to the management agent of the local ODU
- **Out-of-Band Local Management**: The port is connected directly to the management agent of the local ODU.

Port allocation is subject to the following rules:

- One port should be allocated to Data Only or Data and In-Band Management
- The remaining ports should be allocated to Disabled or Out-of-Band Local Management

Further examples of port allocation are provided in Chapter 3: System planning.

Note

The PTP 650 provides flexible interconnection of customer data and network management using several Ethernet ports, but it does not contain a general-purpose Ethernet switch, and it is not possible to forward traffic between the Ethernet ports of the same ODU.

Customer data network

Transparent Ethernet service

The PTP 650 Series provides an Ethernet service between one of the Ethernet ports at a local ODU and one of the Ethernet ports at an associated remote ODU. The Ethernet service is based on conventional layer two transparent bridging, and is equivalent to the Ethernet Private Line (EPL) service defined by the Metro Ethernet Forum (MEF).

The service is transparent to untagged frames, standard VLAN frames, priority-tagged frames, provider bridged frames, Q-in-Q frames and provider backbone bridged frames. In each case, the service preserves MAC addresses, VLAN ID, Ethernet priority and Ethernet payload in the forwarded frame. The maximum frame size for bridged frames in the customer network is 9600 bytes.

Note

There is no requirement for the customer data network to be connected to the same Ethernet port at both ends of a wireless link. For example, it is possible to connect the Main PSU port to the customer data network at one end of the link and to connect the Aux port to the customer data network at the other end of the link.

Layer two control protocols

The PTP 650 Series is transparent to layer two control protocols (L2CP) including:

- Spanning tree protocol (STP), rapid spanning tree protocol (RSTP)
- Multiple spanning tree protocol (MSTP)
- Link aggregation control protocol (LACP)
- Link OAM, IEEE 802.3ah
- Port authentication, IEEE 802.1X
- Ethernet local management interface (E-LMI), ITU-T Q.933.
- Link layer discovery protocol (LLDP)
- Multiple registration protocol (MRP)
- Generic attribute registration protocol (GARP)

The PTP 650 Series does not generate or respond to any L2CP traffic.

Quality of service for bridged Ethernet traffic

The PTP 650 Series supports eight traffic queues for Ethernet frames waiting for transmission over the wireless link. Ethernet frames are classified by inspection of the Ethernet priority code point in the outermost VLAN tag, the Differentiated Services Code Point (DSCP) in an IPv4 or IPv6 header, or the Traffic Class in an MPLS header.

PTP 650 provides a configurable mapping between Ethernet, IP or MPLS priority and transmission queue, together with a simple way to restore a default mapping based on the recommended default in IEEE 802.1Q-2005. Untagged frames, or frames with an unknown network layer protocol, can be separately classified.

Scheduling for transmission over the wireless link is by strict priority. In other words, a frame at the head of a given queue is transmitted only when all higher priority queues are empty.

Fragmentation

The PTP 650 Series minimizes latency and jitter for high-priority Ethernet traffic by fragmenting Ethernet frames before transmission over the wireless link. The fragment size is selected automatically according to channel bandwidth and modulation mode of the wireless link. Fragments are reassembled on reception, and incomplete Ethernet frames are discarded.

Wireless link down alert

The PTP 650 Series provides an optional indication of failure of the wireless link by means of a brief disconnection of the copper data port or the optical data port allocated to the customer data network. The Wireless link down alert can be used to trigger protection switching by Spanning Tree Protocol (STP) or Ethernet Automatic Protection Switching (EAPS) and other higher layer protocols in a redundant network.

Lowest Ethernet Modulation Mode

The PTP 650 ODU can be configured to discard Ethernet frames when the modulation mode is lower than the configured Lowest Ethernet Modulation Mode.

This feature is likely to be useful in networks that have alternate routes, for example in a ring or mesh topology where EAPS or RSTP is used to resolve loops. In this application, Lowest Ethernet Modulation Mode should be set to ensure that an active link will provide at least the minimum necessary capacity for high-priority constant bit rate traffic such as voice over IP or TDM pseudo wire. An active link will be blocked when the capacity falls below the minimum required, triggering a routing change in associated Ethernet switches to bring alternate links into use.

Lowest Ethernet Modulation Mode should normally be set to BPSK 0.63 Single in simply connected tree networks or other topologies that do not have alternative routes.

Network management

IPv4 and IPv6 interfaces

The PTP 650 ODU contains an embedded management agent with IPv4 and IPv6 interfaces. Network management communication is exclusively based on IP and associated higher layer transport and application protocols. The default IPv4 address of the management agent is 169.254.1.1. There is no default IPv6 address. The PTP 650 does not require use of supplementary serial interfaces.

MAC address

The management agent end-station MAC address is recorded on the enclosure and is displayed on the Status web page. The MAC address is not configurable by the user.

VLAN membership

The management agent can be configured to transmit and receive either untagged, priority-tagged, C-tagged (IEEE 802.1Q) or S-tagged (IEEE 802.1ad) frames. C-tagged and S-tagged frames must be single tagged. The VLAN ID can be 0 (priority tagged) or in the range 1 to 4094.

Ethernet and DHCP priority

The management agent transmits IPv4 and IPv6 management packets with a configurable DHCP value in the range 0 to 63. If the management agent is configured to operate in a management VLAN, the Ethernet frames will be transmitted with a configurable Ethernet priority in the range 0 to 7. The same DHCP and Ethernet priorities are assigned to all management packets generated by the agent. Management frames are multiplexed with customer data frames of the same priority for transmission at the wireless port.

Access to the management agent

The management agent can be reached from any Ethernet port at the local ODU that is allocated to either Data and In-Band Management or Out-of-Band Local Management.

If the wireless link is established, the management agent can also be reached from the remote ODU via an Ethernet port that is allocated to Data and In-Band Management.

Management frames are processed by the management agent if (a) the destination MAC address in the frame matches the ODU MAC address, and (b) the VLAN ID in the frame matches the VLAN configuration of the management agent.

If Local Packet Filtering is enabled, unicast frames forwarded to the management agent as in-band management are filtered, that is, not forwarded in the customer data network.

The Port Allocation options described in Ethernet ports on page 1-15 allow for several combinations of in-band and out-of-band local management as shown in Figure 3, Figure 4 and Figure 5.

Figure 3 shows a single port allocated to Data and In-Band Management. The in-band management might be connected to a network management center or to a management terminal of an installer or technician.

Figure 3 In-band management

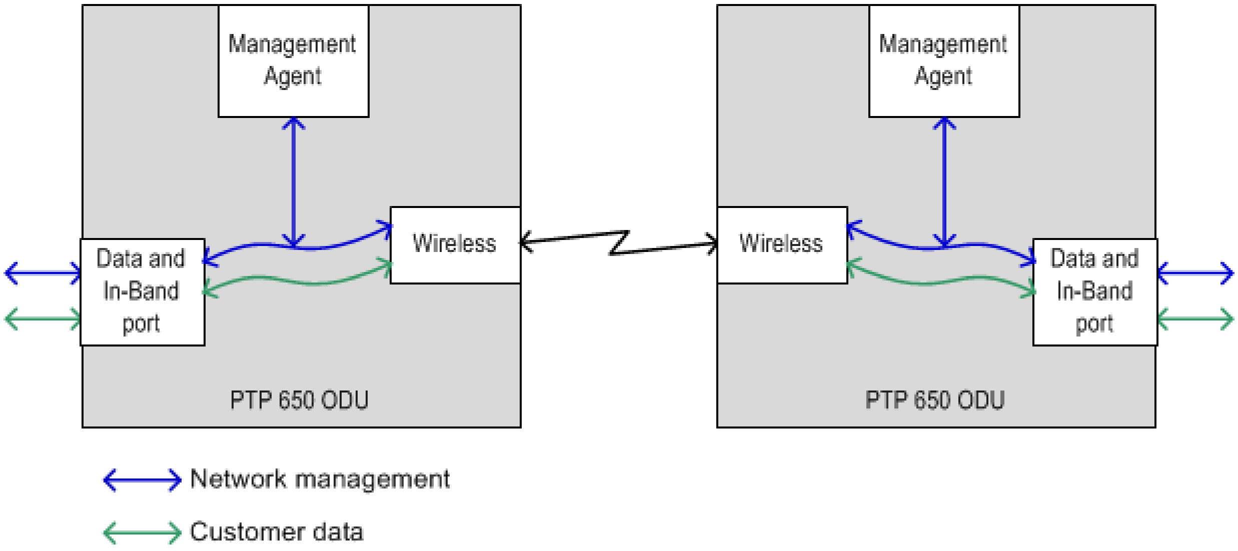


Figure 4 shows one port allocated to Data Only and one allocated to Out-of-Band Local Management. The local management network (shown in red) is isolated from the customer data network (shown in green). Management frames are not forwarded over the wireless link. The connection to the management agent is solely through the management port of the local ODU.

Figure 4 Out-of-band local management

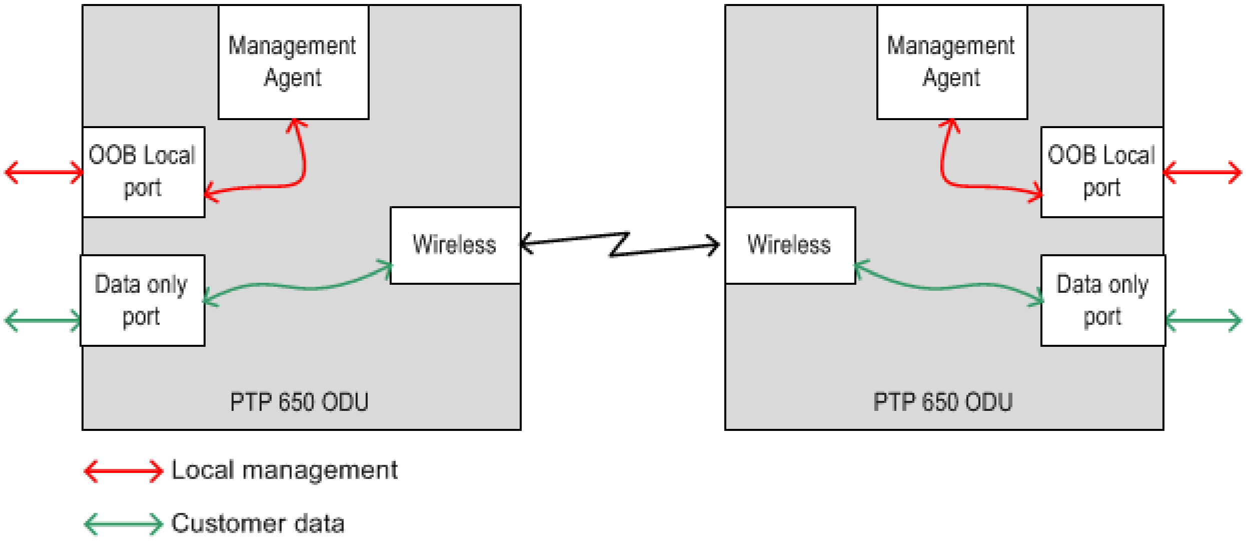
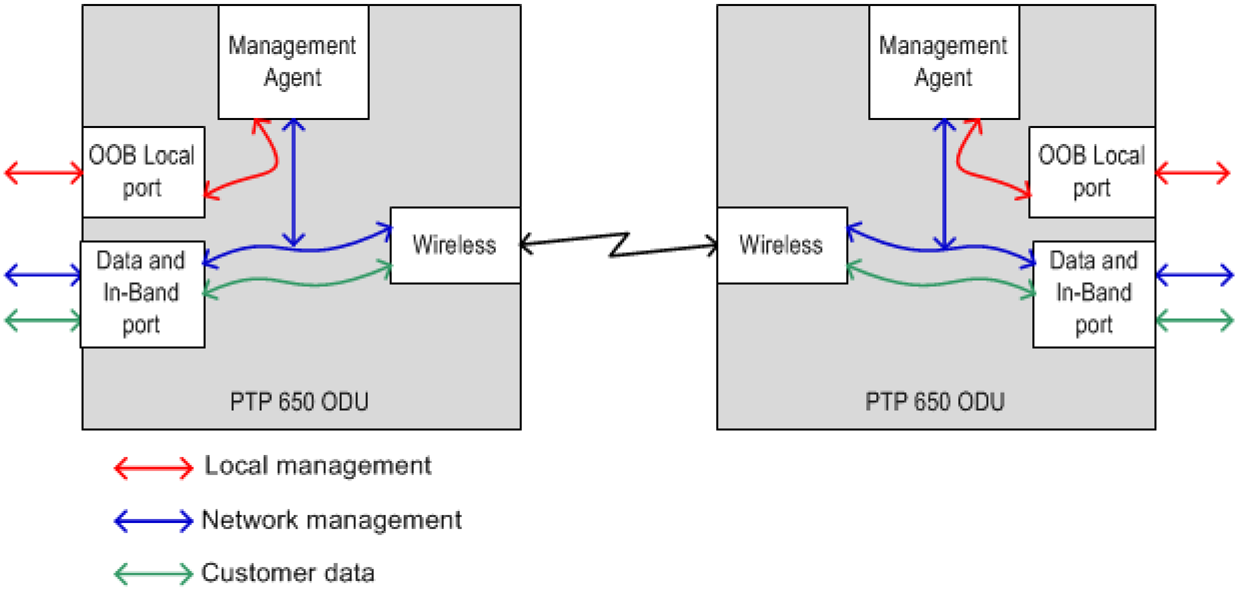


Figure 5 shows a combination of in-band and out-of-band local management. Here, the out-of-band local port might be used to connect a management terminal of an installer or technician, whilst the in-band management is connected to a network management center.

Figure 5 IB and OOB local management



MAC address and IP address of the management agent

The MAC address and IP address used by the management agent will be the same at each port that is allocated to In-Band Management or Out-Of-Band Local Management. The management agent does not provide the function of a dual-homed or multi-homed host. Network designers should take care to ensure that the ODU will not be connected to more than one IP network.

Further examples of useful port allocation schemes are provided in Chapter 3: System planning.

Source address learning

If Local Packet Filtering is enabled, the PTP 650 learns the location of end stations from the source addresses in received management frames. The agent filters transmitted management frames to ensure that the frame is transmitted at the appropriate Ethernet port, or over the wireless link as required to reach the reach the correct end station. If the end station address is unknown, then management traffic is transmitted at each of Ethernet port enabled for management and over the wireless link.

Ethernet loopback mode

PTP 650 provides a local Ethernet loopback function that can be used to loop traffic between the Aux Port and one of the other Ethernet ports.

Loopback is intended to assist in the commissioning of a camera or other auxiliary device collocated with the PTP 650 ODU. For example, when setting up a camera which will ultimately be connected to the wireless bridge, it may be useful to loop the data back to a second local interface, to assist in the positioning and alignment of the camera.

When ports are configured for Ethernet local loopback, they are temporarily disconnected from their allocated function and connected together internally within the PTP 650 ODU. Out-of-band local management is disconnected from the management agent, and the In-band management path will also be un-available if one of the loopback ports has been allocated for Data and in-band management. In this case, it will not be possible to manage the ODU from a local Ethernet port. For this reason the Ethernet loopback is always disabled when the ODU is rebooted or power-cycled, restoring the previous port configuration and any associated management paths.

During loopback operation, the same frame size restrictions that apply to management traffic are present, jumbo frames are not supported and the maximum frame size is restricted to 1536 bytes.

Loopback is able to loop between Ethernet ports operating at different line rates if required, and it is possible to configure a Loopback between ports operating at 1000BASE-T/LX/SX and 100BASE-TX if needed.

Protocol model

Ethernet bridging behavior at each end of the wireless link is equivalent to a two-port, managed, transparent MAC bridge where the two ports are Ethernet Port and Wireless Port.

Frames are transmitted at the Wireless port over a proprietary point-to-point circuit-mode link layer between ends of the PTP 650 link. Ethernet frames received at the Ethernet port, or generated internally within the management agent, are encapsulated within a lightweight MAC layer for transmission over the wireless link.

Protocol layers involved in bridging between Ethernet and wireless interfaces are shown in Figure 6. Protocol layers involved in bridging between external interfaces and the management agent are shown in Figure 7. In these figures, the layers have the meanings defined in IEEE 802.1Q-2005.

Figure 6 Protocol layers between Ethernet and wireless interfaces

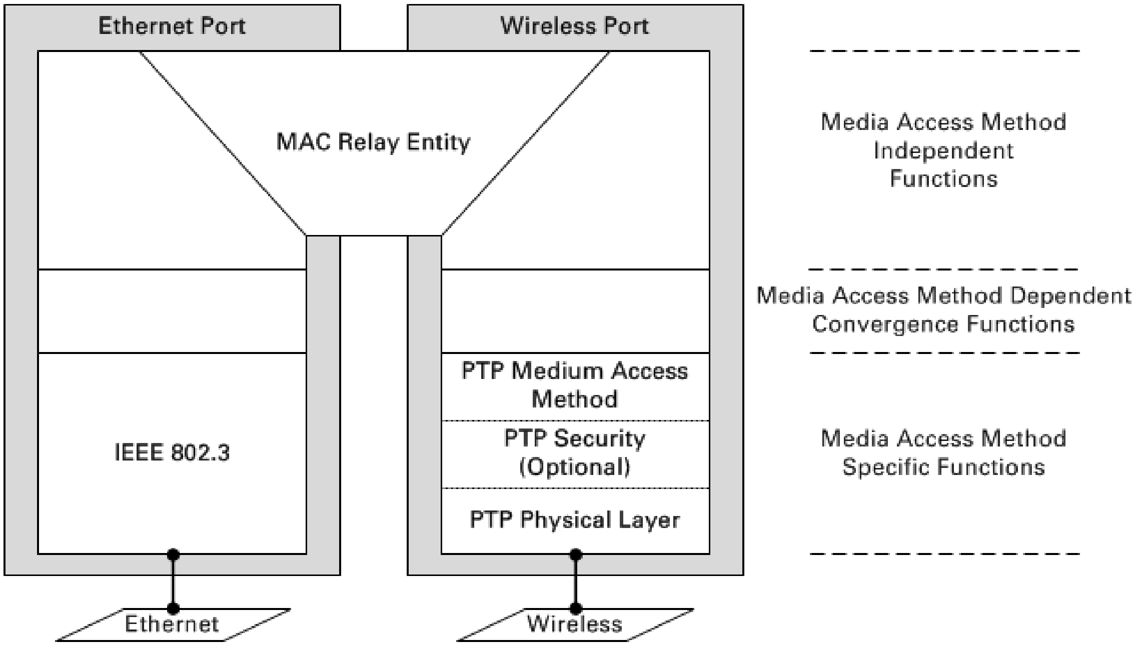
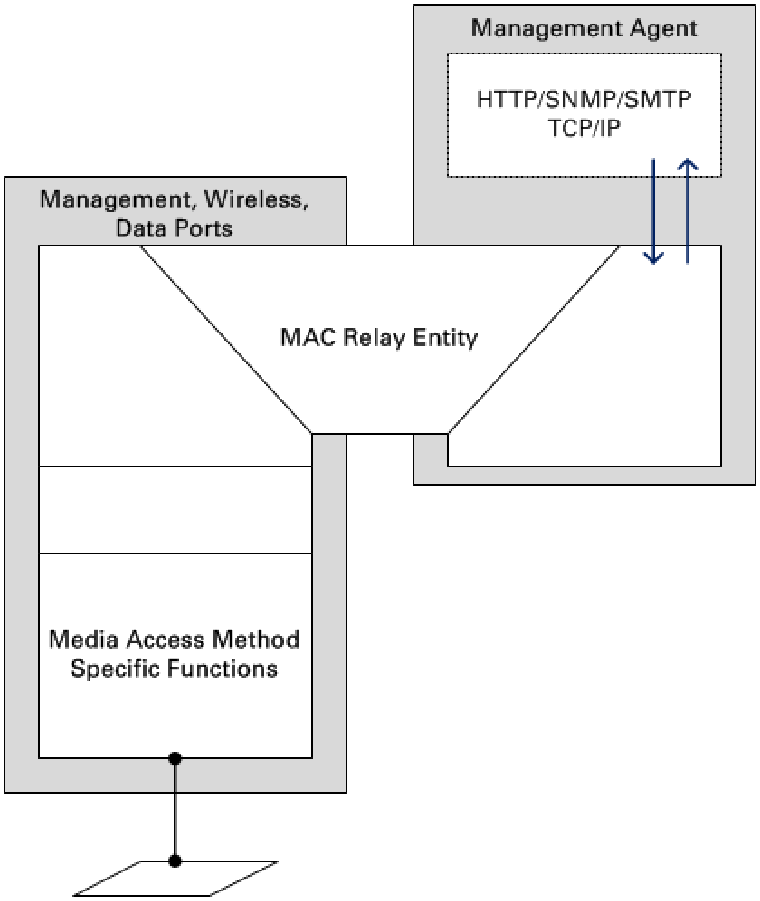


Figure 7 Protocol layers between external interfaces and the management agent


Management Agent
HTTP/SNMP/SMTP
TCP/IP
Management, Wireless, Data Ports
MAC Relay Entity
Media Access Method Specific Functions

System management

This section introduces the PTP 650 management system, including the web interface, installation, configuration, alerts and upgrades.

Management agent

PTP 650 equipment is managed through an embedded management agent. Management workstations, network management systems or PCs can be connected to this agent using a choice of in-band or out-of-band local modes. These modes are described in detail in Network management on page 1-18.

The management agent includes a dual IPv4/IPv6 interface at the management agent. The IP interface operates in the following modes:

- IPv4 only (default)
- IPv6 only
- Dual IPv4/IPv6

In the dual IPv4/IPv6 mode, the IP interface is configured with an IPv4 address and an IPv6 address and can operate using both IP versions concurrently. This dual mode of operation is useful when a network is evolving from IPv4 to IPv6.

The management agent supports the following application layer protocols (regardless of the management agent IP mode):

- Hypertext transfer protocol (HTTP)
- HTTP over transport layer security (HTTPS/TLS)
- RADIUS authentication
- TELNET
- Simple network management protocol (SNMP)
- Simple mail transfer protocol (SMTP)
- Simple network time protocol (SNTP)
- System logging (syslog)

Note

PTP 650 supports a single public key certificate for HTTPS. This certificate must be based on an IPv4 or IPv6 address as the Common Name. The Dual IPv4/IPv6 interface should not normally be used when HTTPS is required.

IPv6

The PTP 650 management agent supports the following IPv6 features:

Neighbor discovery

PTP 650 supports neighbor discovery for IPv6 as specified in RFC 4861 including:

- Neighbor un-reachability detection (NUD),
- Sending and receiving of neighbor solicitation (NS) and neighbor advertisement (NA) messages,
- Processing of redirect functionality.

PTP 650 sends router solicitations, but does not process router advertisements.

Path MTU discovery and packet size

PTP 650 supports path MTU discovery as specified in RFC 1981, and packet fragmentation and reassembly as specified in RFC 2460 and RFC 5722.

ICMP for IPv6

PTP 650 supports ICMPv6 as specified in RFC 4443. PTP 650 does not support RFC 4884 (multi-part messages).

Addressing

The PTP 650 management agent is compatible with the IPv6 addressing architecture specified in RFC 4291. PTP 650 allows static configuration of the following:

- Global unicast address
- IPv6 prefix length
- IPv6 default router.

PTP 650 additionally assigns an automatically configured Link Local address using stateless address auto-configuration (SLAAC) as specified in RFC 4862. PTP 650 does not assign a global unicast IP address using SLAAC.

PTP 650 responds on the standard management agent interfaces (HTTP, HTTPS, syslog, Telnet, SNMP, SMTP, SNTP) using the global unicast address.

Privacy extensions

PTP 650 does not support the privacy extensions specified in RFC 4941.

DHCPv6

PTP 650 does not support address assignment using DHCPv6. The address of the management agent must be configured statically.

Multicast listener discovery for IPv6

The PTP 650 management agent supports Multicast Listener Discovery version 1 (MLDv1) as specified in RFC 2710.

PTP 650 does not support Multicast Listener Discovery version 2 (MLDv2).

Textual representation of IPv6 addresses

PTP 650 allows users to input text-based IP addresses in any valid format defined in RFC 5952. IPv6 addresses are automatically converted by PTP 650 to the preferred compressed form, apart from those using the prefix length on the same line as the address, such as **2000::1/64**.

Security

PTP 650 does not support IP security (IPsec).

Web server

The PTP 650 management agent contains a web server. The web server supports the HTTP and HTTPS/TLS interfaces.

Web-based management offers a convenient way to manage the PTP 650 equipment from a locally connected computer or from a network management workstation connected through a management network, without requiring any special management software. The web-based interfaces are the only interfaces supported for installation of PTP 650.

Web pages

The web-based management interfaces provide comprehensive web-based fault, configuration, performance and security management functions organized into the following web-pages and groups:

- **Home:** The Home web-page reports Wireless Link Status and basic information needed to identify the link. The Home page additionally lists all active alarm conditions.
- **Status:** The Status web-page reports the detailed status of the PTP 650.
- **System:** These web-pages are used for configuration management, including IP and Ethernet, AES encryption keys, quality of service and software upgrade. The System pages additionally provide detailed counters and diagnostic measurements used for performance management.

- **Installation:** The Installation Wizard is used to install license keys, configure the PTP 650 wireless interface and to arm the unit ready for alignment.
- **Management:** These web-pages are used to configure the network management interfaces.
- **Security:** The Security Wizard is used to configure the HTTPS/TLS interface and other security parameters such as the AES wireless link encryption key and the key of keys for encrypting CSPs on the ODU. The Security Wizard is disabled until AES encryption is enabled by license key.
- **Change Password**: The Change Password web page changes the web interface password of the active user. The User Accounts page is also used to change passwords.
- **Logout:** Allows a user to log out from the web-based interface.

Transport layer security

The HTTPS/TLS interface provides the same set of web-pages as the HTTP interface, but allows HTTP traffic to be encrypted using Transport Layer Security (TLS). PTP 650 uses AES encryption for HTTPS/TLS. Operation of HTTPS/TLS is enabled by purchase of an optional AES upgrade.

HTTPS/TLS requires installation of a private key and a public key certificate where the common name of the subject in the public key certificate is the IP address or host name of the PTP 650 unit. PTP 650 supports certificates with 2048-bit key size.

HTTPS/TLS operation is configured through the web-based interfaces using the Security Wizard.

Details of the security material needed for HTTPS/TLS are provided in Security planning on page 3-33.

Note

The PTP 650 has no default public key certificate, and Cambium Networks is not able to generate private keys or public key certificates for specific network applications.

Note

PTP 650 supports a single public key certificate for HTTPS. This certificate must be based on an IPv4 or IPv6 address as the Common Name. Any attempt to use HTTPS without a certificate for the associated IP address will not be secure, and will trigger browser security warnings. It follows from this that the Dual IPv4/IPv6 interface should not normally be used when HTTPS is required.

User account management

PTP 650 allows a network operator to configure a policy for login attempts, the period of validity of passwords and the action taken on expiry of passwords.

Identity-based user accounts

The PTP 650 web-based interface provides two methods of authenticating users:

- Role-based user authentication allows the user, on entry of a valid password, to access all configuration capabilities and controls. This is the default method.
- Identity-based user authentication supports up to 10 users with individual usernames and passwords.

When identity-based user accounts are enabled, a security officer can define from one to ten user accounts, each of which may have one of the three possible roles:

- Security officer.
- System administrator.
- Read only.

Identity-based user accounts are enabled in the Local User Accounts page of the web-based interface.

Password complexity

PTP 650 allows a network operator to enforce a configurable policy for password complexity. Password complexity configuration additionally allows a pre-determined best practice configuration to be set.

SNMP control of passwords

PTP 650 allows the role-based and identity-based passwords for the web-based interface to be updated using the proprietary SNMP MIB. This capability is controlled by the SNMP Control of Passwords, and is disabled by default.

SNMP Control of Passwords can be used together with SNMPv3 to provide a secure means to update passwords from a central network manager. However, password complexity rules are not applied.

RADIUS authentication

PTP 650 supports remote authentication for users of the web interface using the Remote Authentication Dial-In User Service (RADIUS) with one of the following authentication methods:

- Challenge Handshake Authentication Protocol (CHAP)
- Microsoft CHAP Version 2 (MS-CHAPv2)

PTP 650 supports connections to primary and secondary RADIUS servers. The RADIUS interface is configured through the RADIUS Authentication page of the web-based interfaces.

PTP 650 RADIUS supports the standard Service Type attribute to indicate authentication roles of System Administrator and Read Only together with a vendor specific attribute to indicate authentication roles of Security Officer, System Administrator, and Read Only.

Remote authentication can be used in addition to local authentication, or can be used as a replacement for local authentication. If remote and local authentications are used together, PTP 650 checks log in attempts against locally stored user credentials before submitting a challenge and response for remote authentication. Remote authentication is not attempted if the username and password match locally stored credentials, or fails against the local database.

RADIUS is only available when PTP 650 is configured for Identity-based User Accounts. For more information, refer to Planning for RADIUS operation on page 3-39.

SNMP

The management agent supports fault and performance management by means of an SNMP interface. The management agent is compatible with SNMP v1, SNMP v2c, and SNMPv3 using the following Management Information Bases (MIBs):

- RFC-1493. BRIDGE-MIB. dot1dBase group.
- RFC-2233. IF-MIB. Interfaces group, and ifXTable table.
- RFC-3411. SNMP-FRAMEWORK-MIB. snmpEngine group.
- RFC-3412. SNMP-MPD-MIB. snmpMPDStats group.
- RFC-3413. SNMP-TARGET-MIB. snmpTargetObjects group and SNMP-NOTIFICATION-MIB snmpNotifyTable table.
- RFC-3414. SNMP-USER-BASED-SM-MIB. usmStats group and usmUser group.
- RFC-3415. SNMP-VIEW-BASED-ACM-MIB vacmMIBObjects group.
- RFC-3418. SNMPv2-MIB. System group, SNMP group, and set group.
- RFC-3826. SNMP-USM-AES-MIB. usmAesCfb128Protocol OID.
- RFC-4293 IP-MIB, ipForwarding, ipAdEntAddr, ipAdEntIfIndex, ipAdEntNetMask
- PTP 650 Series proprietary MIB.

Simple Network Time Protocol (SNTP)

The clock supplies accurate date and time information to the system. It can be set to run with or without a connection to a network time server (SNTP). It can be configured to display local time by setting the time zone and daylight saving in the Time web page.

If an SNTP server connection is available, the clock can be set to synchronize with the server time at regular intervals. For secure applications, the PTP 650 can be configured to authenticate received NTP messages using an MD5 signature.

SNMPv3 security

SNMP Engine ID

PTP 650 supports four different formats for SNMP Engine ID:

- MAC address
- IPv4 address
- Configurable text string
- IPv6 address

SNMPv3 security configuration is re-initialized when the SNMP Engine ID is changed.

User-based security model

PTP 650 supports the SNMPv3 user-based security model (USM) for up to 10 users, with MD5, SHA-1, DES and (subject to the license key) AES protocols in the following combinations:

- No authentication, no privacy,
- MD5, no privacy,
- SHA-1, no privacy,
- MD5, DES,
- SHA-1, DES,
- MD5, AES,
- SHA-1, AES.

Use of AES privacy requires the PTP 650 AES upgrade described in AES license on page 1-32.

View-based access control model

PTP 650 supports the SNMPv3 view-based access control model (VACM) with a single context. The context name is the empty string. The context table is read-only, and cannot be modified by users.

Access to critical security parameters

The SNMPv3 management interface does not provide access to critical security parameters (CSPs) of PTP 650. It is not possible to read or modify AES keys used to encrypt data transmitted at the wireless interface. Neither is it possible to read or modify security parameters associated with TLS protection of the web-based management interface. The recovery mode option to zeroize CSPs does not affect SNMPv3 configuration.

MIB-based management of SNMPv3 security

PTP 650 supports a standards-based approach to configuring SNMPv3 users and views through the SNMP MIB. This approach provides maximum flexibility in terms of defining views and security levels appropriate for different types of user.

PTP 650 provides a default SNMPv3 configuration. This initial configuration is not secure, but it provides the means by which a secure configuration can be created using SNMPv3.

The secure configuration should be configured in a controlled environment to prevent disclosure of the initial security keys necessarily sent as plaintext, or sent as encrypted data using a predictable key. The initial security information should not be configured over an insecure network.

The default configuration is restored when any of the following occurs:

- All ODU configuration data is erased.
- All SNMP users are deleted using the SNMP management interface.
- The SNMP Engine ID Format has been changed.
- The SNMP Engine ID Format is Internet Address AND the Internet Address has been changed.
- The SNMP Engine ID Format is Text String AND the text string has been changed.
- The SNMP Engine ID Format is MAC Address AND configuration has been restored using a file saved from a different unit.
- SNMPv3 Security Management is changed from web-based to MIB-based.

The default user configuration is specified in SNMPv3 default configuration (MIB-based) on page 3-37.

PTP 650 creates the `initial` user and template users with localized authentication and privacy keys derived from the passphrase string `123456789`. Authentication keys for the templates users are fixed and cannot be changed. Any or all of the template users can be deleted.

The default user `initial` is created with a view of the entire MIB, requiring authentication for SET operations. There is no access for template users.

Note

VACM grants access for requests sent with more than the configured security level.

The default user `initial` will have read/write access to the whole of the MIB. This is described in further detail in View-based access control model on page 1-29. The template users have no access to the MIB in the default configuration. User `initial` will normally be used to create one or more additional users with secret authentication and privacy keys, and with appropriate access to the whole of the MIB or to particular views of the MIB according to the operator's security policy. New users must be created by cloning template users. The user `initial` may then be deleted to prevent access using the well-known user name and keys. Alternatively, the keys associated with `initial` may be set to some new secret value.

Web-based management of SNMPv3 security

PTP 650 supports an alternative, web-based approach for configuring SNMPv3 security. In this case, the web-based interface allows users to specify SNMPv3 users, security levels, privacy and authentication protocols, and passphrases. Web-based management will be effective for many network applications, but the capabilities supported are somewhat less flexible than those supported using the MIB-based security management.

Selection of web-based management for SNMPv3 security disables the MIB-based security management.

Web-based management of SNMPv3 security allows for two security roles:

- Read Only
- System Administrator

Read Only and System Administrator users are associated with fixed views allowing access to the whole of the MIB, excluding the objects associated with SNMPv3 security. System Administrators have read/write access as defined in the standard and proprietary MIBs.

Web-based management of SNMPv3 security allows an operator to define the security levels and protocols for each of the security roles; all users with the same role share a common selection of security level and protocols.

Web-based security configuration is re-initialized when any of the following occurs:

- All ODU configuration data is erased.
- The SNMP Engine ID Format has been changed.
- The SNMP Engine ID Format is Internet Address and the Internet Address has been changed.
- The SNMP Engine ID Format is Text String and the text string has been changed.
- The SNMP Engine ID Format is MAC Address and configuration has been restored using a file saved from a different unit.
- SNMPv3 Security Management is changed from MIB-based to web-based.

Additionally, all SNMP user accounts are disabled when the authentication protocol, the privacy protocol, or the security level is changed.

Downgrade of the license key

A possible lockout condition exists if a user downgrades the PTP 650 license key so as to disable the AES capability when SNMPv3 users are configured with AES privacy and VACM is configured to require privacy. In this case, recovery is by either (a) restoring the correct license key, or (b) using recovery mode to erase all configuration and entering new configuration.

Option (b) will cause default users and access configuration to be re-created.

System logging (syslog)

PTP 650 supports the standard syslog protocol to log important configuration changes, status changes and events. The protocol complies with RFC 3164.

PTP 650 creates syslog messages for configuration changes to any attribute that is accessible via the web-based interface, or via the enterprise MIB at the SNMP interface.

PTP 650 additionally creates syslog messages for changes in any status variable displayed in the web-based interface.

PTP 650 creates syslog messages on a number of events (for example successful and unsuccessful attempts to log in to the web-based interface).

PTP 650 can be configured to send syslog messages to one or two standard syslog servers.

Additionally, PTP 650 logs event notification messages locally. Locally-stored event messages survive reboot of the unit, and are overwritten only when the storage capacity is exhausted (approximately 2000 messages). The locally stored events can be reviewed using the web-based user interface.

Only users with Security Officer role are permitted to configure the syslog client. Users with Security Officer, System Administrator or Read Only roles are permitted to review the locally logged event messages.

AES license

PTP 650 provides optional encryption using the Advanced Encryption Standard (AES). Encryption is not available in the standard PTP 650 system.

AES upgrades are supplied as an access key purchased from your Cambium Point-to-Point distributor or solutions provider. The access key authorizes AES operation for one ODU. Two access keys are needed to operate AES on a link. The upgrade is applied by entering an access key together with the MAC address of the target ODU into the PTP License Key Generator web page, which may be accessed from the support website.

The License Key Generator creates a new license key that is delivered by email. The license key must be installed on the ODU. When the license key is installed, the ODU must be rebooted before AES can be enabled. Once applied, the AES upgrade is bound to a single ODU and is not transferrable.

AES encryption may be used in the following ways:

- At the wireless port to encrypt data transmitted over the wireless link.
- At the SNMP management interface in the SNMPv3 mode.
- At the HTTPS/TLS management interface.
- At the RADIUS interface when PEAP (MS-CHAPv2) is used as the authentication method.

Two levels of encryption are available to purchase:

- 128-bit: This allows an operator to encrypt all traffic sent over the wireless link using 128-bit encryption.
- 256-bit: This allows an operator to encrypt traffic using either 128-bit or 256-bit encryption.

Encryption must be configured with the same size key in each direction.

AES encryption at the PTP 650 wireless port is based on pre-shared keys. An identical key must be entered at each end of the link.

AES encryption for SNMPv3 or TLS is always based on a 128-bit key, regardless of level enabled in the PTP 650 license key.

Critical security parameters

Critical security parameters (CSPs) are as follows:

- Key of keys.
- AES encryption keys for the wireless interface.
- Private key for the HTTPS/TLS interface.
- Entropy value for the HTTPS/TLS interface.
- User account passwords for the web-based interface.

CSPs can be erased (zeroized) using the Zeroize CSPs page of the web-based interface or by selecting the Zeroize CSPs option in Recovery mode.

Login information

PTP 650 optionally provides details of the most recent successful login, and the most recent unsuccessful login attempt, for each user of the web-based interface.

Capability upgrades

ODUs are shipped with “Lite” data throughput capability, that is, up to 125 Mbps. Cambium Networks supply capability upgrades to upgrade ODUs to “Mid” (up to 250 Mbps) or “Full” (up to 450 Mbps) capability. ODUs are shipped without AES encryption capability. Cambium Networks supply capability upgrades to upgrade ODUs to128-bit or 256-bit AES Encryption.

Capability upgrades are purchased from Cambium and supplied as access keys. The user then enters the access key into the PTP License Key Generator web page on the support website.

The License Key Generator creates a new license key and delivers it by email. The user then installs the license key using the ODU web interface. License keys are bound to a single ODU and are not transferrable.

Full capability trial period

A full capability trial period is available for units that are licensed for “Lite” (up to 125 Mbps) or “Mid” (up to 250 Mbps) data throughput capability. This trial allows the ODU to operate with “Full” capability (up to 450 Mbps) during a 60 day period, reverting to the Lite or Mid capability afterwards. The trial period can be started, paused and resumed from the web interface.

Software upgrade

The management agent supports application software upgrade using either the web-based interface or the SNMP interface.

PTP 650 software images are digitally signed, and the ODU will accept only images that contain a valid Cambium Networks PTP digital signature. The ODU always requires a reboot to complete a software upgrade.

Note

Obtain the application software and this user guide from the support website BEFORE warranty expires.

Caution

ODU software version must be the same at both ends of the link. Limited operation may sometimes be possible with dissimilar software versions, but such operation is not supported by Cambium Networks.

Recovery mode

The PTP 650 recovery mode provides a means to recover from serious configuration errors including lost or forgotten passwords and unknown IP addresses.

Recovery mode also allows new main application software to be loaded even when the integrity of the existing main application software image has been compromised. The most likely cause of an integrity problem with the installed main application software is where the power supply has been interrupted during an earlier software upgrade.

The ODU operates in recovery mode in the following circumstances:

- When a checksum error occurs for the main application software image.
- When a power on, power off, power on cycle is applied to the ODU with the power off period being around 5sec.

Recovery mode supports a single IPv4 interface, with IP address 169.254.1.1. Recovery mode does not support IPv6.

Note

When Recovery has been entered through a power on/off/on cycle, the ODU will revert to normal operation if no web access has been made to the unit within 30 seconds. This prevents the unit remaining inadvertently in recovery following a power outage.

Recovery mode options

Options in recovery mode (IPv4 only) are as follows:

- Load new main application software.
- Reset all configuration data. This option resets IP and Ethernet configuration, and erases (zeroizes) critical security parameters.
- Reset IP and Ethernet configuration.
- Erase (zeroize) critical security parameters.
- Reboot with existing software and configuration.

Note

If recovery mode has been entered because of a checksum error, after a 30 second wait the ODU will attempt to reboot with existing software and configuration.

The recovery software image is installed during manufacture of the ODU and cannot be upgraded by operators.

Chapter 2: System hardware

This chapter describes the hardware components of a PTP 650 link.

The following topics are described in this chapter:

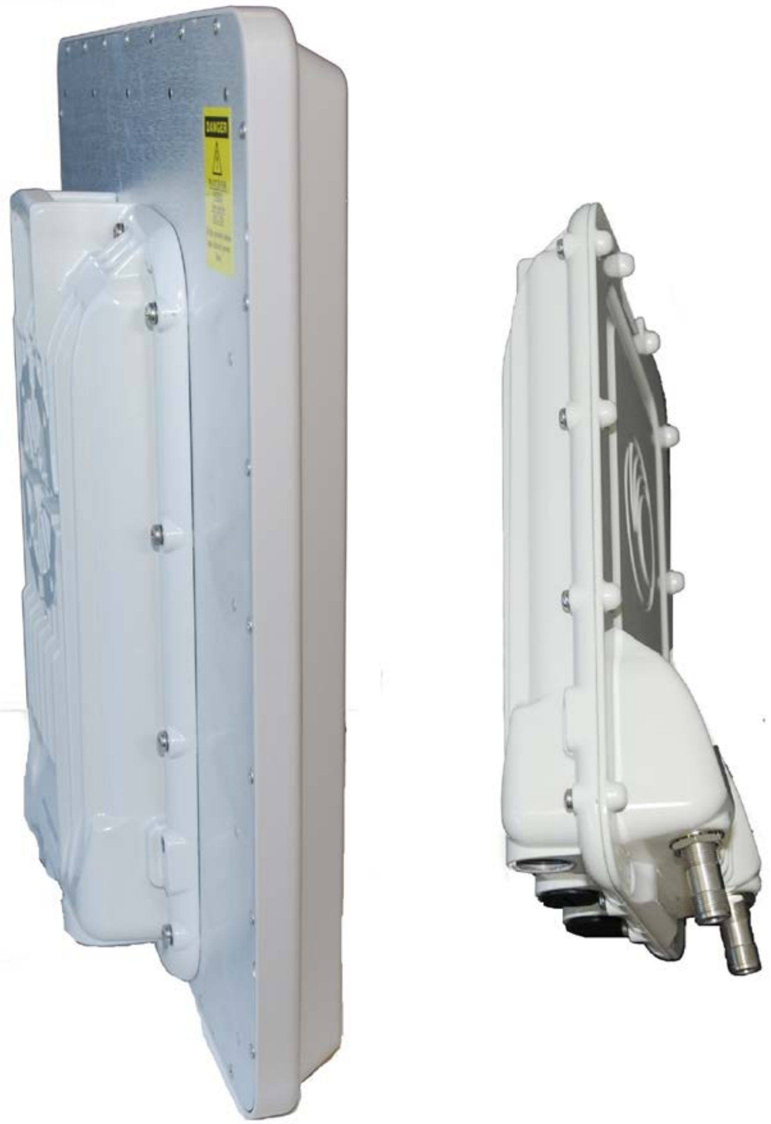
- Outdoor unit (ODU) on page 2-2
- Power supply units (PSU) on page 2-8
- Antennas and antenna cabling on page 2-13
- Ethernet cabling on page 2-20

Outdoor unit (ODU)

ODU description

The ODU is a self-contained transceiver unit that houses both radio and networking electronics. The ODU is supplied in two configurations: integrated (attached to its own flat plate antenna) () or connectorized (without an antenna) (Figure 8). The connectorized ODU is designed to work with externally mounted antennas that have higher gains than the integrated antenna. Connectorized units can cope with more difficult radio conditions.

Figure 8 PTP 650 Series ODUs (integrated and connectorized)



ODU part numbers

One ODU is required for each link end. Order ODUs and ODU kits from Cambium Networks (Table 2 and Table 3).

Note

To determine when to install connectorized units and to calculate their impact on link performance and regulatory limits, see Planning for connectorized units on page 3-25.

To select antennas, RF cables and connectors for connectorized units, see Antennas and antenna cabling on page 2-13.

Choose the correct regional variant: one is for use in regions where FCC or IC licensing restrictions apply (FCC/IC), one is for use in ETSI countries (EU), and the other is for the rest of the world (RoW).

Individual ODUs

Each of the parts listed in Table 2 includes the following items:

- One integrated or connectorized ODU.
- With connectorized ODUs only: one connectorized ODU mounting bracket (Figure 9). Integrated ODUs, when sold individually, are supplied without mounting brackets.

Table 2 ODU part numbers

Cambium description	Cambium part number
PTP 650 (4.9 to 6.05 GHz) Integrated ODU (FCC/IC)	C050065B001
PTP 650 (4.9 to 6.05 GHz) Connectorized ODU (FCC/IC)	C050065B002
PTP 650 (4.9 to 6.05 GHz) Integrated ODU (RoW)	C050065B003
PTP 650 (4.9 to 6.05 GHz) Connectorized ODU (RoW)	C050065B004
PTP 650 (4.9 to 6.05 GHz) Integrated ODU (EU)	C050065B005
PTP 650 (4.9 to 6.05 GHz) Connectorized ODU (EU)	C050065B006

ODU kits

Each of the parts listed in Table 3 includes the following additional items:

- One integrated or connectorized ODU.
- One integrated or connectorized ODU mounting bracket (Figure 9), as appropriate.
- One PSU of the type stated in the Cambium description.
- One line cord, either US (FCC/IC) or EU (EU and RoW).

Table 3 ODU kit part numbers

Cambium description	Cambium part number
PTP 650 Connectorized END with AC Supply (FCC/IC)	C050065H007
PTP 650 Connectorized END with AC+DC Enhanced Supply (FCC/IC)	C050065H008
PTP 650 Integrated END with AC Supply (FCC/IC)	C050065H009
PTP 650 Integrated END with AC+DC Enhanced Supply (FCC/IC)	C050065H010
PTP 650 Connectorized END with AC Supply (RoW)	C050065H011
PTP 650 Connectorized END with AC+DC Enhanced Supply (RoW)	C050065H012
PTP 650 Integrated END with AC Supply (RoW)	C050065H013
PTP 650 Integrated END with AC+DC Enhanced Supply (RoW)	C050065H014
PTP 650 Connectorized END with AC Supply (EU)	C050065H017
PTP 650 Connectorized END with AC+DC Enhanced Supply (EU)	C050065H018
PTP 650 Integrated END with AC Supply (EU)	C050065H019
PTP 650 Integrated END with AC+DC Enhanced Supply (EU)	C050065H020

Accessories

Spare ODU port blanking plugs are available from Cambium Networks (Table 4).

Table 4 ODU accessory part numbers

Cambium description	Cambium part number
PTP 650 Series Blanking Plug Pack (Qty 10)	N000065L036

ODU mounting brackets

The integrated and connectorized mounting brackets (Figure 9) are used to mount the ODU on poles with diameters in the range 50 to 75 mm (2 to 3 inches). The extended mounting bracket (Figure 9) is used for mounting an integrated or connectorized ODU on poles with a diameter of either 90 mm (3.5 inches) or 115 mm (4.5 inches).

Before ordering ODU mounting brackets, be aware of the following:

- Individual integrated ODUs are supplied without a mounting bracket (Table 2).
- Individual connectorized ODUs are supplied with a connectorized mounting bracket (Table 2).
- ODUs in kits are supplied with an integrated or connectorized bracket, as appropriate (Table 3).

If separate ODU mounting brackets are required, order them from Cambium Networks (Table 5).

Figure 9 ODU mounting brackets (integrated, connectorized and extended)

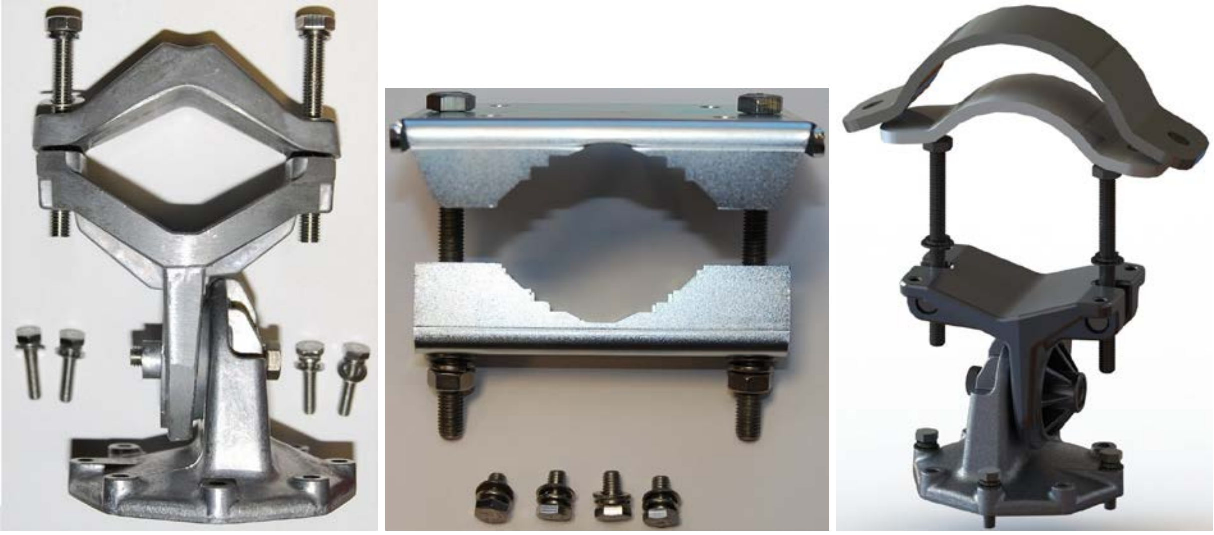


Table 5 ODU mounting bracket part numbers

Pole diameter	ODU type	Cambium description	Cambium part number
From 50 to 75 mm (2 to 3 inches)	Integrated	PTP 650 Mounting Bracket (integrated)	N000065L031
	Connectorized	PTP 650 Mounting Bracket (connectorized)	N000065L032
Either 90 mm (3.5 inches) or 115 mm (4.5 inches)	Integrated and connectorized	Extended Diameter Mast mounting kit 3.5″ and 4.5″	N000065L030

ODU interfaces

The PSU, AUX and SFP ports are on the rear of the integrated and connectorized ODUs (Figure 10). These interfaces are described in Table 6. Each of the PSU, AUX and SFP ports can be configured to disable Ethernet traffic or to carry the following Ethernet traffic:

- Wireless bridge data
- Wireless bridge data and in-band management
- Out-of-band local management
- Local loop-back between any two ports

Figure 10 ODU rear interfaces

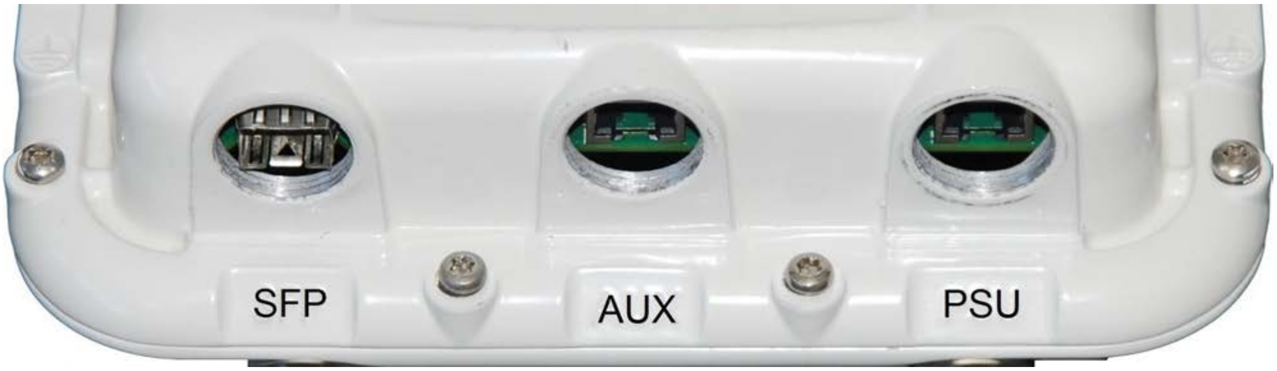
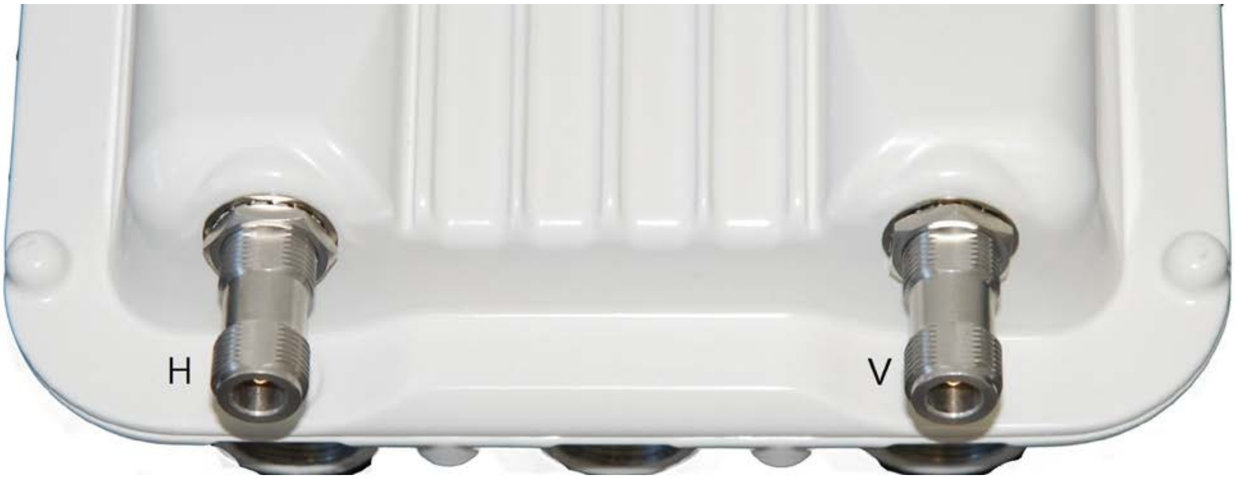


Table 6 ODU rear interfaces

Port name	Connector	Interface	Description
PSU	RJ45	POE input	Proprietary power over Ethernet (POE).
		100/1000BASE-T Ethernet	Management and/or data.
AUX	RJ45	100/1000BASE-T Ethernet with 802.3at compliant POE out capability	Auxiliary Ethernet port which can be used, for example, to connect and power a video camera or wireless access point.
SFP	SFP	Optical or Copper Gigabit Ethernet	OOB management, user data, user data with IB management, ODU-to-ODU. Plug-in SFP module must be purchased separately.

The front of the connectorized ODU (Figure 11) provides N type female connectors for RF cable interfaces to antennas with horizontal (H) and vertical (V) polarization.

Figure 11 Connectorized ODU antenna interfaces



ODU specifications

The PTP 650 ODU conforms to the specifications listed in Table 7.

Table 7 ODU specifications

Category	Specification
Dimensions	Integrated: 370 mm (14.5 in) x 370 mm (14.5 in) x 95 mm (3.75 in) Connectorized: 305 mm (12 in) x 305 mm (12 in) x 105 mm (4.01 in)
Weight	Integrated: 5.5 Kg (12.1 lbs) including bracket Connectorized: 4.3 Kg (9.1 lbs) including bracket
Temperature	-40°C (-40°F) to +60°C (140°F)
Wind loading	200 mph (323 kph) maximum. See ODU wind loading on page 3-11.
Humidity	100% condensing
Waterproofing	IP66, IP67
UV exposure	10 year operational life (UL746C test evidence)
Static discharge	See Electromagnetic compatibility (EMC) compliance on page 4-23

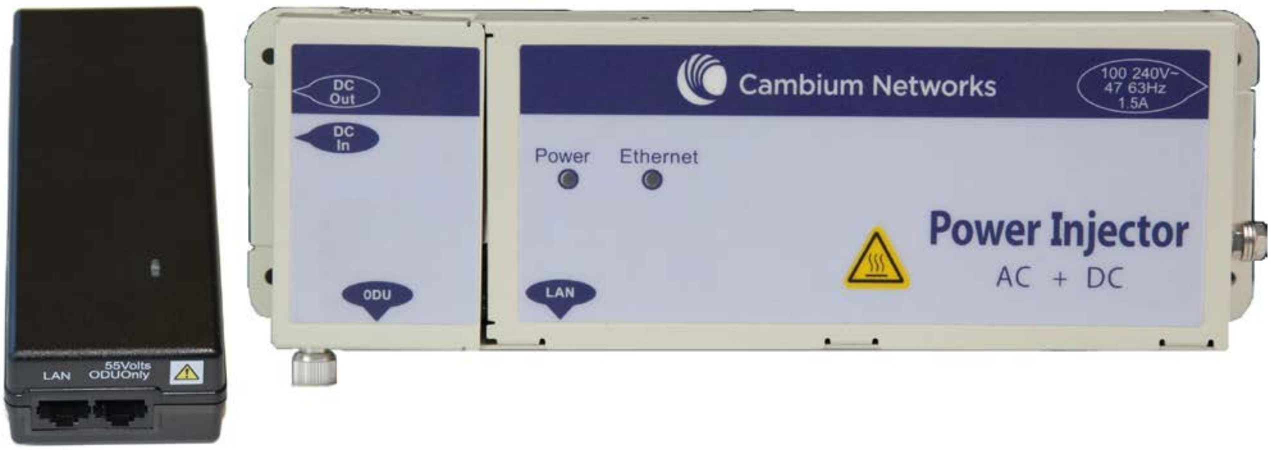
Power supply units (PSU)

PSU description

The PSU is an indoor unit that is connected to the ODU and network terminating equipment using Cat5e cable with RJ45 connectors. It is also plugged into an AC or DC power supply so that it can inject Power over Ethernet (POE) into the ODU. Choose one of the following PSUs (Figure 12):

- The AC Power Injector (left) accepts an AC input supply only.
- The AC+DC Enhanced Power Injector (right) accepts both AC and DC input, tolerates a greater temperature range, and allows the ODU to support a device on the Aux port, such as a video camera or wireless access point. It also allows the ODU to provide DC power output.

Figure 12 PSU 650 PSUs



Caution

The PSU ODU ports are designed to connect only to PTP 650 ODUs or LPUs. Do not connect any other equipment, as damage may occur.

Do not connect the PIDU Plus PTP 300/500/600 Series to the PTP 650 ODU or LPU.

Note

Each of the ODU kits listed in Table 3 includes one PSU and one US or EU line cord as stated in the Cambium description.

PSU part numbers

Order PSUs and (for AC power) line cords from Cambium Networks (Table 8).

Table 8 Power supply component part numbers

Cambium description	Cambium part number
PTP 650 AC Power Injector	N000065L001
PTP 650 AC+DC Enhanced Power Injector	C000065L002
US Line Cord Fig 8	N000065L003
UK Line Cord Fig 8	N000065L004
EU Line Cord Fig 8	N000065L005
Australia Line Cord Fig 8	N000065L006

AC Power Injector interfaces

The AC Power Injector interfaces are shown in Figure 13 and described in Table 9.

Figure 13 AC Power Injector interfaces

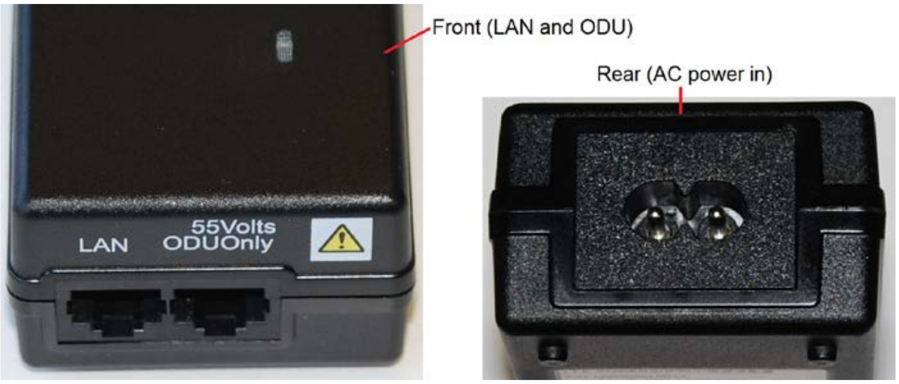


Table 9 AC Power Injector interface functions

Interface	Function
AC power in	AC power input (main supply).
ODU	RJ45 socket for connecting Cat5e cable to ODU.
LAN	RJ45 socket for connecting Cat5e cable to network.
Power (green) LED	Power supply detection

AC+DC Enhanced Power Injector interfaces

The AC+DC Enhanced Power Injector interfaces are shown in Figure 14 and described in Table 10.

Figure 14 AC+DC Enhanced Power Injector interfaces

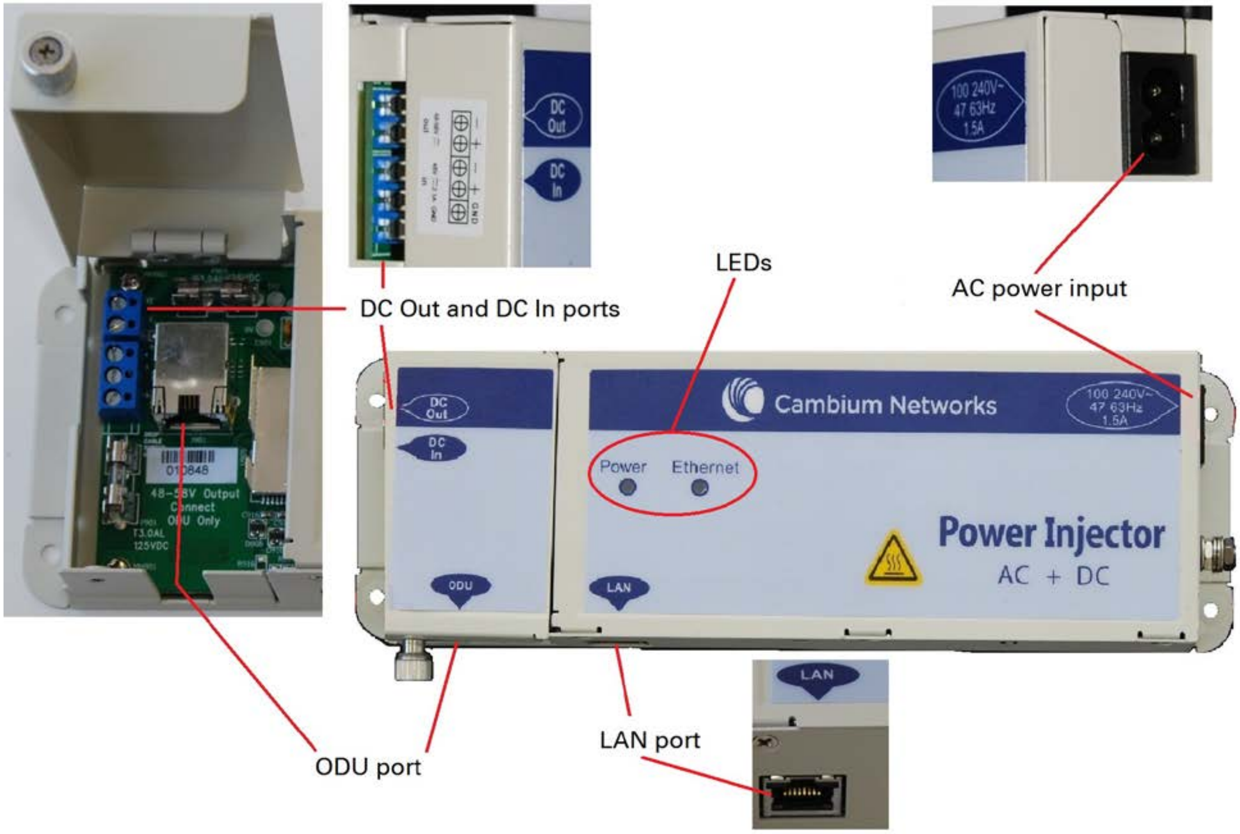


Table 10 AC+DC Enhanced Power Injector interface functions

Interface	Function
100-240V 47-63Hz 1.5A	AC power input (main supply).
DC In	Alternative DC power supply input.
DC Out	DC power output to a second PSU (for power supply redundancy).
ODU	RJ45 socket for connecting Cat5e cable to ODU.
LAN	RJ45 socket for connecting Cat5e cable to network.
Power (green) LED	Power supply detection
Ethernet (yellow) LED	Ethernet traffic detection

PSU specifications

The PTP 650 AC Power Injector conforms to the specifications listed in Table 11.

The PTP 650 AC+DC Enhanced Power Injector conforms to the specifications listed in Table 12.

Table 11 AC Power Injector specifications

Category	Specification
Dimensions	137 mm (5.4 in) x 56 mm (2.2 in) x 38 mm (1.5 in)
Weight	0.240 Kg (0.5 lbs)
Temperature	0°C to +40°C
Humidity	90% non-condensing
Waterproofing	Not waterproof
Altitude	Sea level to 5000 meters (16000 ft)
AC Input	Min 90 V AC, 57 – 63 Hz, max 264 V AC, 47 – 53 Hz.
DC output voltage to the ODU	55V +/- 5%
AC connector	IEC-320-C8
Efficiency	Better than 85%, efficiency level ‘V’
Over Current Protection	Hiccup current limiting, trip point set between 120% to 150% of full load current
Hold up time	At least 10 milliseconds

Table 12 AC+DC Enhanced Power Injector specifications

Category	Specification
Dimensions	250 mm (9.75 in) x 40 mm (1.5 in) x 80 mm (3 in)
Weight	0.864 Kg (1.9 lbs)
Temperature	-40°C (-40°F) to +60°C (140°F)
Humidity	0 to 90% non-condensing
Waterproofing	Not waterproof
AC Input	90-264 V AC, 47-60 Hz
Alternative DC Input	37-60 V DC
DC Output Voltage	For mains input: 58 V, +2V, -0V For DC input: Output voltage at maximum rated output current, not more than 1.5 V below the DC input voltage. Maximum length of DC output cable: 3 meters.
AC Input connector	IEC-320-C8
DC Output current	1.7A
Efficiency	Better than 84%
Over Current Protection	Hiccup current limiting, trip point set between 120% to 150% of full load current
Hold up time	At least 20 milliseconds
Power factor	Better than 0.9

Antennas and antenna cabling

Antenna requirements

Each connectorized ODU requires one external antenna (normally dual-polar), or if spatial diversity is required, each ODU requires two antennas. These antennas are not supplied by Cambium Networks.

For connectorized units operating in the USA or Canada 5.4 GHz or 5.8 GHz bands, choose external antennas from those listed in FCC and IC approved antennas on page 2-14. Do not install any other antennas. For links in other countries, the listed antennas are advisory, not mandatory.

Note

To determine when to install connectorized units and to calculate their impact on link performance and regulatory limits, see Planning for connectorized units on page 3-25.

RF cable and connectors

RF cable of type CNT-400 is required for connecting the ODU to the antenna. N type male connectors are required for connecting the RF cables to the connectorized ODU. Two connectors are required per ODU. Use weatherproof connectors, preferably ones that are supplied with adhesive lined heat shrink sleeves that are fitted over the interface between the cable and connector. Order RF cable and N type male connectors from Cambium Networks (Table 13).

Table 13 RF cable and connector part numbers

Cambium description	Cambium part number
50 Ohm Braided Coaxial Cable - 75 meter	30010194001
50 Ohm Braided Coaxial Cable - 500 meter	30010195001
RF CONNECTOR,N,MALE,STRAIGHT FOR CNT-400 CABLE	09010091001

Note

To select the correct connectors for the antenna end of the RF cable, refer to the antenna manufacturer's instructions.

Antenna accessories

Connectorized ODUs require the following additional components:

- Cable grounding kits: Order one cable grounding kit for each grounding point on the antenna cables. Refer to Cable grounding kit on page 2-22 for specifications and part numbers.
- Self-amalgamating and PVC tape: Order these items to weatherproof the RF connectors.
- Lightning arrestors: When the connectorized ODU is mounted indoors, lightning arrestors (not PTP 650 LPUs) are required for protecting the antenna RF cables at building entry. One arrestor is required per antenna cable. One example of a compatible lightning arrestor is the Polyphaser LSXL-ME or LSXL (not supplied by Cambium Networks).

FCC and IC approved antennas

For connectorized units operating in the USA or Canada, choose external antennas from Table 14 (5.4 GHz) or Table 15 (5.8 GHz). These are approved by the FCC for use with the product and are constrained by the following limits for single- or dual-polarization parabolic dish antennas:

- 5.4 GHz - 34.9 dBi per polarization or antenna.
- 5.8 GHz - up to 37.7 dBi per polarization or antenna.

Caution

Antennas not included in these tables are strictly prohibited for use with the PTP 650 in the specified bands.

Caution

This radio transmitter (IC certification number 109AO-50650) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Le présent émetteur radio (Numéro de certification IC 109AO-50650) a été approuvé par Industrie Canada pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Table 14 Antennas permitted for deployment in USA/Canada – 5.4 GHz

Manufacturer	Antenna Type	Nom gain (dBi)	Parabolic dish
RFS	RFS 2-foot Parabolic, SPF2-52AN	27.9	Y
Gabriel	Gabriel 2-foot High Performance Dual QuickFire Parabolic, HQFD2-52-N	28.1	Y
RadioWaves	Radio Waves 2-foot Dual-Pol Parabolic, SPD2-5.2	28.1	Y
Cambium	5.25-5.85 GHZ, 2-FT (0.6M), RDH4503B	28.1	Y
Gabriel	Gabriel 2-foot High Performance QuickFire Parabolic, HQF2-52-N	28.2	Y
RadioWaves	Radio Waves 2-foot Parabolic, SP2-2/5	28.3	Y
Gabriel	Gabriel 2-foot Standard Dual QuickFire Parabolic, QFD2-52-N	28.4	Y
Gabriel	Gabriel 2-foot Standard Dual QuickFire Parabolic, QFD2-52-N-RK	28.4	Y
Gabriel	Gabriel 2-foot Standard QuickFire Parabolic, QF2-52-N	28.5	Y
Gabriel	Gabriel 2-foot Standard QuickFire Parabolic, QF2-52-N-RK	28.5	Y
RadioWaves	Radio Waves 2-foot Parabolic, SP2-5.2	29	Y
Andrew	Andrew 2-foot Dual-Pol Parabolic, PX2F-52	29.4	Y
Andrew	Andrew 2-foot Parabolic, P2F-52	29.4	Y
Gabriel	Gabriel 2.5-foot Standard Dual QuickFire Parabolic, QFD2.5-52-N	31.1	Y
RadioWaves	Radio Waves 3-foot Dual-Pol Parabolic, SPD3-5.2	31.1	Y
Cambium	5.25-5.85 GHz, 3-FT (0.9M), DUAL-POL, H-POL & V-POL, RDH4504B	31.1	Y
Gabriel	Gabriel 2.5-foot Standard QuickFire Parabolic, QF2.5-52-N	31.2	Y
RadioWaves	Radio Waves 3-foot Parabolic, SP3-2/5	31.4	Y
RadioWaves	Radio Waves 3-foot Parabolic, SP3-5.2	31.4	Y
Cambium	5.25-5.85 GHZ, 3-FT (0.9M), SINGLE-POL, RDH4513B	31.4	Y
Andrew	Andrew 3-foot Dual-Pol Parabolic, PX3F-52	33.4	Y

Manufacturer	Antenna Type	Nom gain (dBi)	Parabolic dish
Andrew	Andrew 3-foot Parabolic, P3F-52	33.4	Y
RFS	RFS 4-foot HP Parabolic, SDF4-52AN	33.9	Y
RFS	RFS 4-foot Parabolic, SPF4-52AN	33.9	Y
Gabriel	Gabriel 4-foot High Performance Dual QuickFire Parabolic, HQFD4-52-N	34.3	Y
Gabriel	Gabriel 4-foot High Performance QuickFire Parabolic, HQF4-52-N	34.4	Y
RadioWaves	Radio Waves 4-foot Dual-Pol Parabolic, SPD4-5.2	34.4	Y
Cambium	5.25-5.85 GHZ, 4-FT (1.2M), DUAL-POL, H-POL & V-POL, RDH4505B	34.4	Y
RadioWaves	Radio Waves 4-foot Parabolic, SP4-2/5	34.6	Y
Gabriel	Gabriel 4-foot Standard Dual QuickFire Parabolic, QFD4-52-N	34.7	Y
Gabriel	Gabriel 4-foot Standard Dual QuickFire Parabolic, QFD4-52-N-RK	34.7	Y
Gabriel	Gabriel 4-foot Standard QuickFire Parabolic, QF4-52-N	34.8	Y
Gabriel	Gabriel 4-foot Standard QuickFire Parabolic, QF4-52-N-RK	34.8	Y
RadioWaves	Radio Waves 4-foot Parabolic, SP4-5.2	34.8	Y
Andrew	Andrew 4-foot Dual-Pol Parabolic, PX4F-52	34.9	Y
Cambium	5.25-5.85 GHZ, 4-FT (1.2M), DUAL-POL PARABOLIC DISH, RDG4453B	34.9	Y
Andrew	Andrew 4-foot Parabolic, P4F-52	34.9	Y
Cambium	5.25-5.85 GHZ, 4-FT (1.2M), HIGH PERFORMANCE SINGLE-POL, RDH4524A	34.9	Y
MARS	Flat Plate (Dual-Pol)	23	N
Laird	90 Sectorized (Dual-Pol)	17	N
Laird	60 Sectorized (Dual-Pol)	17	N
KPPA	OMNI (Dual-Pol)	13	N
MARS	Small Form Factor Flat Plate Antenna Part # MA-EM56-DP19CM.	19	N
MTI	MTI 15 inch Dual-Pol Flat Panel, MT-485025/NVH	23	N

Manufacturer	Antenna Type	Nom gain (dBi)	Parabolic dish
Andrew	Andrew 1-foot Flat Panel Single, UBP300-4-1	21	N
Andrew	Andrew 1.25-foot Flat Panel Dual, UBXP375-4-1	21	N

Table 15 Antennas permitted for deployment in USA/Canada – 5.8 GHz

Manufacturer	Antenna Type	Nom Gain (dBi)	Parabolic Dish
RFS	RFS 2-foot Parabolic, SPF2-52AN	27.9	Y
Gabriel	Gabriel 2-foot High Performance Dual QuickFire Parabolic, HQFD2-52-N	28.1	Y
RadioWaves	Radio Waves 2-foot Dual-Pol Parabolic, SPD2-5.2	28.1	Y
Cambium	5.25-5.85 GHZ, 2-FT (0.6M), RDH4503B	28.1	Y
Gabriel	Gabriel 2-foot High Performance QuickFire Parabolic, HQF2-52-N	28.2	Y
RadioWaves	Radio Waves 2-foot Parabolic, SP2-2/5	28.3	Y
Gabriel	Gabriel 2-foot Standard Dual QuickFire Parabolic, QFD2-52-N	28.4	Y
Gabriel	Gabriel 2-foot Standard Dual QuickFire Parabolic, QFD2-52-N-RK	28.4	Y
Gabriel	Gabriel 2-foot Standard QuickFire Parabolic, QF2-52-N	28.5	Y
Gabriel	Gabriel 2-foot Standard QuickFire Parabolic, QF2-52-N-RK	28.5	Y
RadioWaves	Radio Waves 2-foot Parabolic, SP2-5.2	29	Y
Andrew	Andrew 2-foot Dual-Pol Parabolic, PX2F-52	29.4	Y
Andrew	Andrew 2-foot Parabolic, P2F-52	29.4	Y
Gabriel	Gabriel 2.5-foot Standard Dual QuickFire Parabolic, QFD2.5-52-N	31.1	Y
RadioWaves	Radio Waves 3-foot Dual-Pol Parabolic, SPD3-5.2	31.1	Y
Cambium	5.25-5.85 GHz, 3-FT (0.9M), DUAL-POL, H-POL & V-POL, RDH4504B	31.1	Y
Gabriel	Gabriel 2.5-foot Standard QuickFire Parabolic, QF2.5-52-N	31.2	Y

Manufacturer	Antenna Type	Nom Gain (dBi)	Parabolic Dish
RadioWaves	Radio Waves 3-foot Parabolic, SP3-2/5	31.4	Y
RadioWaves	Radio Waves 3-foot Parabolic, SP3-5.2	31.4	Y
Cambium	5.25-5.85 GHZ, 3-FT (0.9M), SINGLE-POL, RDH4513B	31.4	Y
Andrew	Andrew 3-foot Dual-Pol Parabolic, PX3F-52	33.4	Y
Andrew	Andrew 3-foot Parabolic, P3F-52	33.4	Y
StellaDoradus	StellaDoradus 45 inch Parabolic Antenna, 58PSD113	33.8	Y
RFS	RFS 4-foot HP Parabolic, SDF4-52AN	33.9	Y
RFS	RFS 4-foot Parabolic, SPF4-52AN	33.9	Y
Gabriel	Gabriel 4-foot High Performance Dual QuickFire Parabolic, HQFD4-52-N	34.3	Y
Gabriel	Gabriel 4-foot High Performance QuickFire Parabolic, HQF4-52-N	34.4	Y
RadioWaves	Radio Waves 4-foot Dual-Pol Parabolic, SPD4-5.2	34.4	Y
Cambium	5.25-5.85 GHZ, 4-FT (1.2M), DUAL-POL, H-POL & V-POL, RDH4505B	34.4	Y
RadioWaves	Radio Waves 4-foot Parabolic, SP4-2/5	34.6	Y
Gabriel	Gabriel 4-foot Standard Dual QuickFire Parabolic, QFD4-52-N	34.7	Y
Gabriel	Gabriel 4-foot Standard Dual QuickFire Parabolic, QFD4-52-N-RK	34.7	Y
Gabriel	Gabriel 4-foot Standard QuickFire Parabolic, QF4-52-N	34.8	Y
Gabriel	Gabriel 4-foot Standard QuickFire Parabolic, QF4-52-N-RK	34.8	Y
RadioWaves	Radio Waves 4-foot Parabolic, SP4-5.2	34.8	Y
Andrew	Andrew 4-foot Dual-Pol Parabolic, PX4F-52	34.9	Y
Cambium	5.25-5.85 GHZ, 4-FT (1.2M), DUAL-POL PARABOLIC DISH, RDG4453B	34.9	Y
Andrew	Andrew 4-foot Parabolic, P4F-52	34.9	Y
Cambium	5.25-5.85 GHZ, 4-FT (1.2M), HIGH PERFORMANCE SINGLE-POL, RDH4524A	34.9	Y
Gabriel	Gabriel 6-foot High Performance Dual QuickFire Parabolic, HQFD6-52-N	37.3	Y

Manufacturer	Antenna Type	Nom Gain (dBi)	Parabolic Dish
Gabriel	Gabriel 6-foot High Performance QuickFire Parabolic, HQF6-52-N	37.4	Y
RFS	RFS 6-foot HP Parabolic, SDF6-52AN	37.4	Y
RFS	RFS 6-foot Parabolic, SPF6-52AN	37.4	Y
RadioWaves	Radio Waves 6-foot Dual-Pol Parabolic, SPD6-5.2	37.5	Y
Andrew	Andrew 6-foot Dual-Pol Parabolic, PX6F-52	37.6	Y
Andrew	Andrew 6-foot Parabolic, P6F-52	37.6	Y
Cambium	5.25-5.85 GHZ, 6-FT (1.8M), HIGH PERFORMANCE SINGLE-POL, RDH4525A	37.6	Y
Gabriel	Gabriel 6-foot Standard Dual QuickFire Parabolic, QFD6-52-N	37.7	Y
Gabriel	Gabriel 6-foot Standard QuickFire Parabolic, QF6-52-N	37.7	Y
RadioWaves	Radio Waves 6-foot Parabolic, SP6-2/5	37.7	Y
RadioWaves	Radio Waves 6-foot Parabolic, SP6-5.2	37.7	Y
MARS	Flat Plate (Dual-Pol)	23	N
Laird	90 Sectorized (Dual-Pol)	17	N
Laird	60 Sectorized (Dual-Pol)	17	N
KPPA	OMNI (Dual-Pol)	13	N
MARS	Small Form Factor Flat Plate Antenna Part # MA-EM56-DP19CM.	19	N
MTI	MTI 15 inch Dual-Pol Flat Panel, MT-485025/NVH	23	N
RFS	RFS 1-foot Flat Panel, MA0528-23AN	23	N
Andrew	Andrew 1-foot Flat Panel Single, UBP300-4-1	21	N
Andrew	Andrew 1.25-foot Flat Panel Dual, UBXP375-4-1	21	N

Ethernet cabling

Ethernet standards and cable lengths

All configurations require a copper Ethernet connection from the ODU (PSU port) to the PSU. Advanced configurations may also require one or both of the following:

- A copper Ethernet connection from the ODU (Aux port) to an auxiliary device.
- An optical or copper Ethernet connection from the ODU (SFP port) to network terminating equipment or a linked ODU.

Table 16 specifies, for each type of PSU and power supply, the maximum permitted PSU drop cable length.

Table 17 specifies, for Aux and copper SFP interfaces, the Ethernet standards supported and the maximum permitted drop cable lengths.

Note

For optical SFP interfaces, the Ethernet standards supported and maximum permitted cable lengths are specified in SFP module kits on page 2-27.

Table 16 PSU drop cable length restrictions

Type of PSU installed	Power supply to PSU	Ethernet supported (*1)	Power output to auxiliary device	Maximum cable length (*2)
AC Power Injector	AC mains	100BASE-TX 1000BASE-T	No	100 m (330 ft)
AC+DC Enhanced power injector	AC mains	No (*3)	No	300 m (990 ft)
	48 V dc	No (*3)	No	300 m (990 ft)
	AC mains	100BASE-TX 1000BASE-T	Yes	100 m (330 ft)
	48 V dc	100BASE-TX 1000BASE-T	Yes	100 m (330 ft)

(*1) 10BASE-T is not supported by PTP 650.

(*2) Maximum length of Ethernet cable from ODU to network terminating equipment via PSU.

(*3) Ethernet is provided via optical SFP interface.

Table 17 Aux and copper SFP Ethernet standards and cable length restrictions

ODU drop cable	Power over Ethernet	Ethernet supported (*1)	Maximum cable length (*2)
Aux – auxiliary device	POE to auxiliary device	100BASE-TX 1000BASE-T	100 m (330 ft)
	None	100BASE-TX	100 m (330 ft)
SFP (copper) – linked device	None	100BASE-TX	100 m (330 ft)

(*1) 10BASE-T is not supported by PTP 650.

(*2) Maximum length of Ethernet cable from the ODU to the linked device.

Outdoor copper Cat5e Ethernet cable

For copper Cat5e Ethernet connections from the ODU to the PSU, LPUs and other devices, use Cat5e cable that is gel-filled and shielded with copper-plated steel, for example Superior Essex type BBDGe. This is known as “drop cable” (Figure 15).

Caution

Always use Cat5e cable that is gel-filled and shielded with copper-plated steel. Alternative types of drop cable are not supported by Cambium Networks.

Order Superior Essex type BBDGe cable from Cambium Networks (Table 18). Other lengths of this cable are available from Superior Essex.

Figure 15 Outdoor drop cable

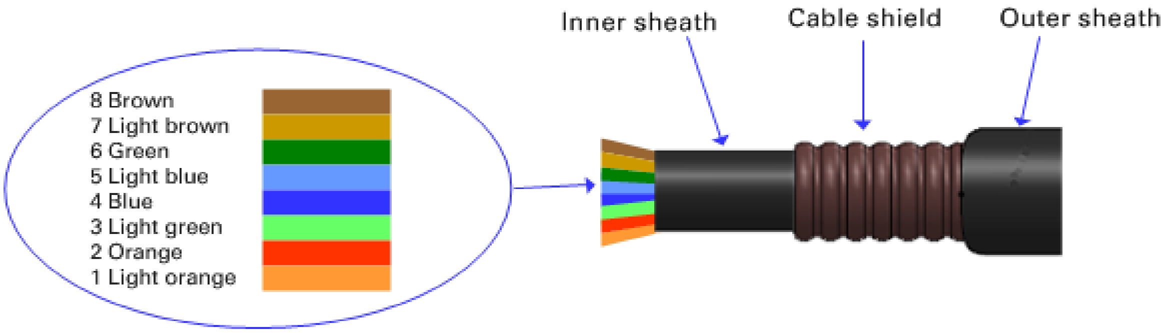


Table 18 Drop cable part numbers

Cambium description	Cambium part number
1000 ft Reel Outdoor Copper Clad CAT5E	WB3175
328 ft (100 m) Reel Outdoor Copper Clad CAT5E	WB3176

Cable grounding kit

Copper drop cable shields must be bonded to the grounding system in order to prevent lightning creating a potential difference between the structure and cable, which could cause arcing, resulting in fire risk and damage to equipment. Optical cables do not require grounding.

One grounding kit (Figure 16) is required for each grounding point on the PSU, Aux and copper SFP drop cables. Order cable grounding kits from Cambium Networks (Table 19).

Caution

To provide adequate protection, all grounding cables must be a minimum size of 10 mm^2 csa (8AWG), preferably 16 mm^2 csa (6AWG), or 25 mm^2 csa (4AWG).

Figure 16 Cable grounding kit

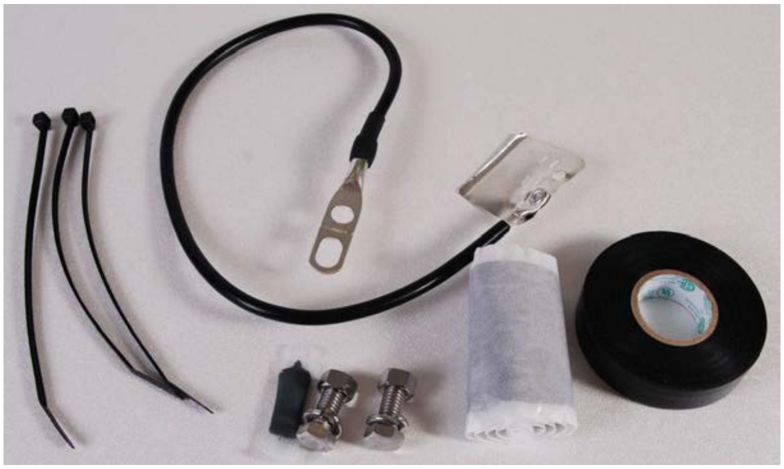


Table 19 Cable grounding kit part numbers

Cambium description	Cambium part number
Cable Grounding Kits For 1/4" And 3/8" Cable	01010419001

Lightning protection unit (LPU) and grounding kit

PTP 650 LPUs provide transient voltage surge suppression for PTP 650 installations. Each PSU or Aux drop cable requires two LPUs, one near the ODU and the other near the linked device, usually at the building entry point (Table 20).

Table 20 LPU and grounding kit contents

Lightning protection units (LPUs) LPU grounding point nuts and washers 	ODU to top LPU drop cable (600 mm) EMC strain relief cable glands
U-bolts, nuts and washers for mounting LPUs 	ODU to top LPU ground cable (M6-M6)
Bottom LPU ground cable (M6-M10) 	ODU to ground cable (M6-M10

One LPU and grounding kit (Table 20) is required for the PSU drop cable connection to the ODU. If the ODU is to be connected to an auxiliary device, one additional LPU and grounding kit is required for the Aux drop cable. Order the kits from Cambium Networks (Table 21).

Table 21 LPU and grounding kit part number

Cambium description	Cambium part number
PTP 650 LPU and Grounding Kit	C000065L007

Note

PTP 650 LPUs are not suitable for installation on SFP copper Cat5e Ethernet interfaces. For SFP drop cables, obtain suitable surge protectors from a specialist supplier.

SFP optical Ethernet interfaces do not require surge protectors.

RJ45 connectors and spare glands

RJ45 connectors are required for plugging Cat5e cables into ODUs, LPUs, PSUs and other devices. Order RJ45 connectors and crimp tool from Cambium Networks (Table 22).

Note

The RJ45 connectors and crimp tool listed in Table 22 work with Superior Essex type BBDGe cable (as supplied by Cambium Networks). They may not work with other types of cable.

The ODU is supplied with one environmental sealing gland for the drop cable. However, this is not suitable when surge protection is required: EMC glands must be used instead. EMC strain relief cable glands (quantity 5) are included in the LPU and grounding kit (Figure 17). These are identified with a black sealing nut. If extra glands are required, order them from Cambium Networks (in packs of 10) (Table 22).

One long EMC strain relief gland (Figure 21) is included in each SFP module kit. This is longer than the standard cable gland as it must house an SFP module plugged into the ODU.

Figure 17 Cable gland

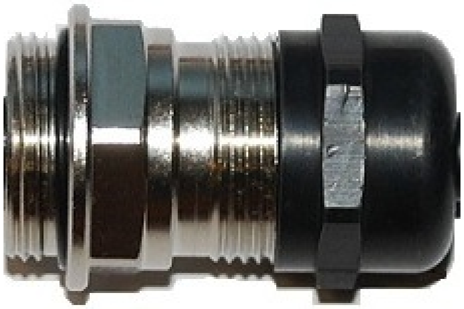


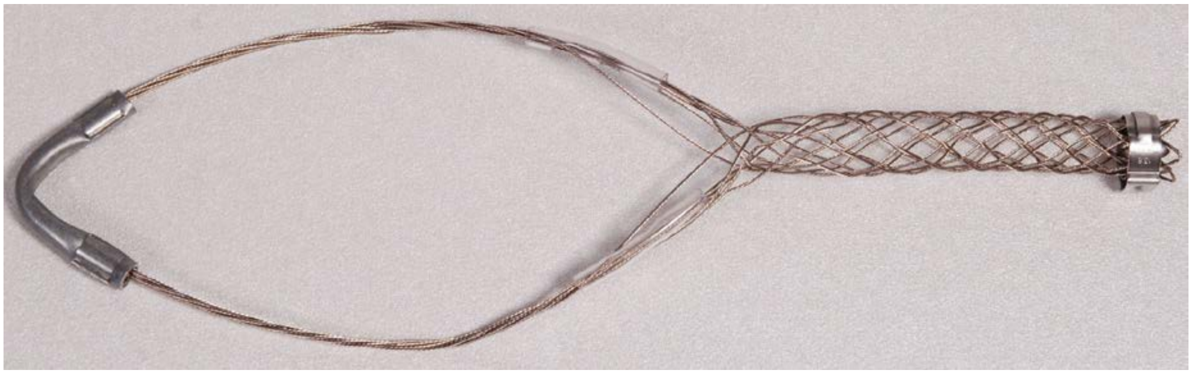
Table 22 RJ45 connector and spare gland part numbers

Cambium description	Cambium part number
Tyco/AMP, Mod Plug RJ45, 100 pack	WB3177
Tyco/AMP Crimp Tool	WB3211
RJ-45 Spare Grounding Gland - PG16 size (Qty. 10)	N000065L033

Cable hoisting grip

One or more grips are required for hoisting the drop cable up to the ODU without damaging the gland or RJ45 plug (Figure 18). They are not supplied by Cambium Networks.

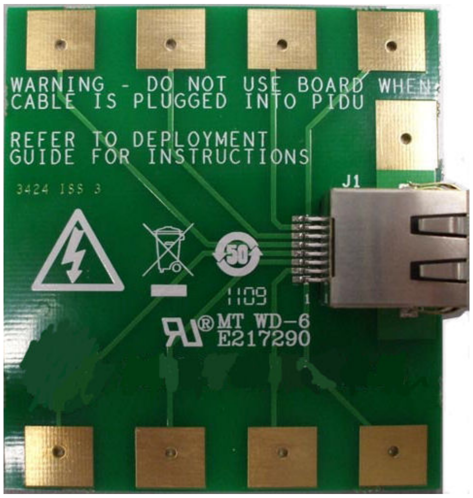
Figure 18 Cable hoisting grip



Drop cable tester

The drop cable tester is an optional item for testing the resistances between the RJ45 pins of the drop cable (Figure 19). Order it by completing the order form on the support website (see Contacting Cambium Networks on page 1).

Figure 19 Drop cable tester



Indoor Cat5e cable

To connect the PSU to network terminating equipment, use indoor Cat5e cable. The ODU network connection implements automatic MDI/MDI-X sensing and pair swapping, allowing connection to networking equipment that requires cross-over cables (MDI-X networks) or straight-through cables (MDI Networks).

SFP module kits

SFP module kits allow connection of a PTP 650 Series ODU to a network over a Gigabit Ethernet interface in one of the following full-duplex modes:

- Optical Gigabit Ethernet: 1000BaseLX or 1000BaseSX
- Copper Gigabit Ethernet: 100BASE-TX or 1000BASE-T

Order SFP module kits from Cambium Networks (Table 23).

Table 23 SFP module kit part numbers

Cambium description	Cambium part number
PTP 650 Optical 1000BaseLX Ethernet SFP Module	C000065L008
PTP 650 Optical 1000BaseSX Ethernet SFP Module	C000065L009
PTP 650 Twisted Pair 1000BASE-T Ethernet SFP Module	C000065L010

To compare the capabilities of the two optical SFP modules, refer to Table 24 and Table 25.

Table 24 Optical 1000BaseLX Ethernet SFP Module (part number C000065L008)

Core/ cladding (microns)	Mode	Bandwidth at 1310 nm (MHz/km)	Maximum length of optical interface	Insertion loss (dB)
62.5/125	Multi	500	550 m (1800 ft)	1.67
50/125	Multi	400	550 m (1800 ft)	0.07
50/125	Multi	500	550 m (1800 ft)	1.19
10/125	Single	N/A	5000 m (16400 ft)	0.16

Table 25 Optical 1000BaseSX Ethernet SFP Module (part number C000065L009)

Core/ cladding (microns)	Mode	Bandwidth at 850 nm (MHz/km)	Maximum length of optical interface	Insertion loss (dB)
62.5/125	Multi	160	220 m (720 ft)	2.38
62.5/125	Multi	200	275 m (900 ft)	2.6
50/125	Multi	400	500 m (1640 ft)	3.37
50/125	Multi	500	550 m (1800 ft)	3.56

The upgrade kits contain the following components:

- Optical or copper SFP transceiver module (Figure 20)
- Long EMC strain relief cable gland (Figure 21)
- The *PTP 650 Series SFP Interface Upgrade Guide*
- License key instructions and unique Access Key

Figure 20 Optical or copper SFP transceiver module

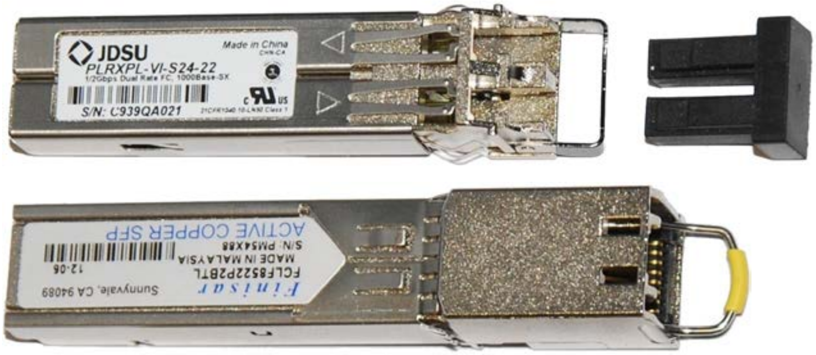
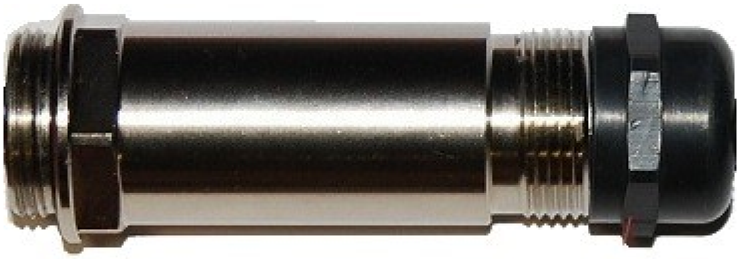


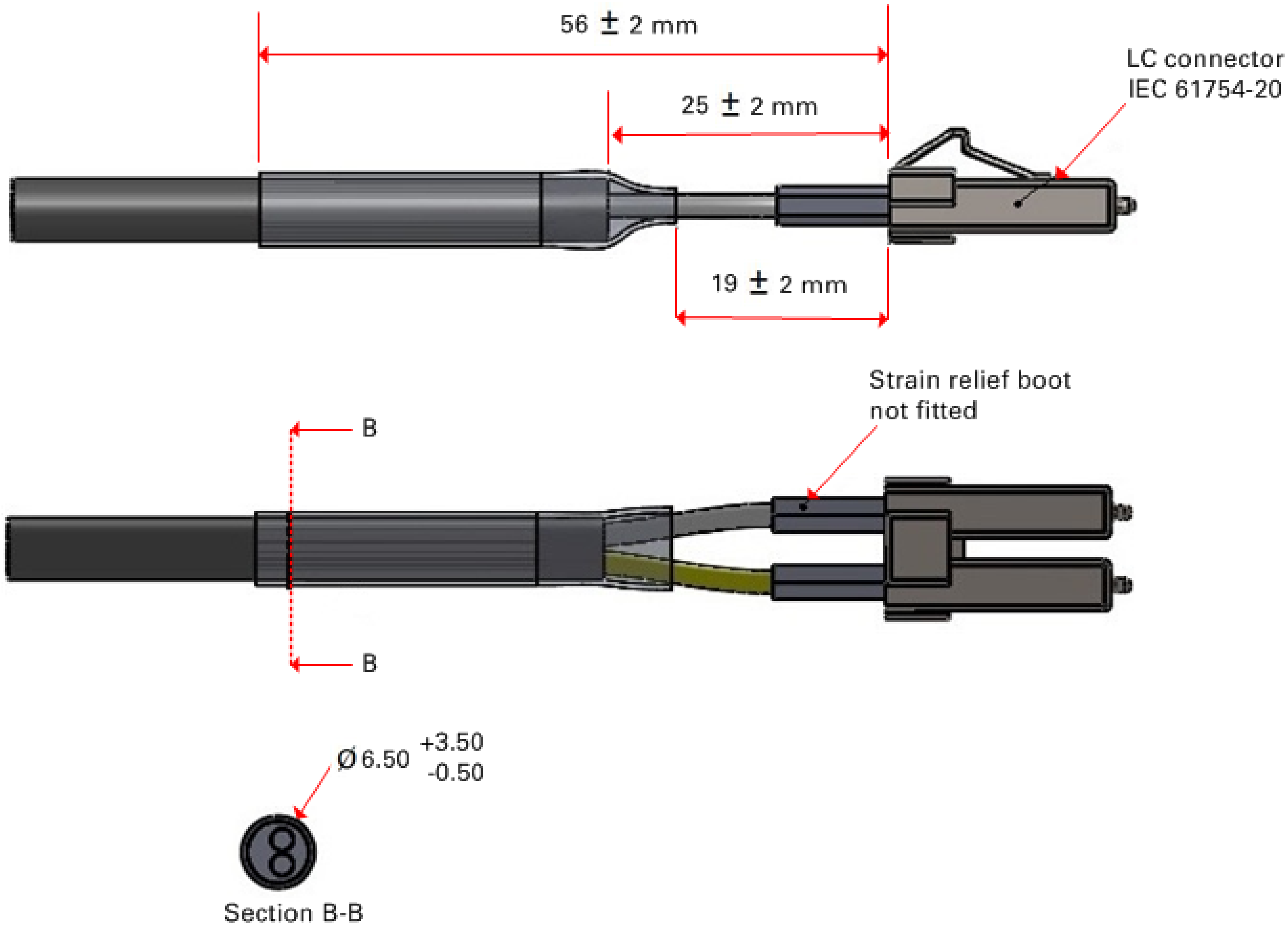
Figure 21 Long cable gland



Optical cable and connectors

Order an optical cable with LC connectors from a specialist fabricator, quoting the specification shown in Figure 22. It must be the correct length to connect the ODU to the other device. LC connectors should be supplied with dust caps to prevent dust build up.

Figure 22 Optical optic cable and connector specification



Chapter 3: System planning

This chapter provides information to help the user to plan a PTP 650 link.

The following topics are described in this chapter:

- Typical deployment on page 3-2 contains diagrams illustrating typical PTP 650 site deployments.
- Site planning on page 3-8 describes factors to be considered when planning the proposed link end sites, including grounding, lightning protection and equipment location.
- Radio spectrum planning on page 3-16 describes how to plan PTP 650 links to conform to the regulatory restrictions that apply in the country of operation.
- Link planning on page 3-21 describes factors to be taken into account when planning links, such as range, path loss and throughput.
- Planning for connectorized units on page 3-25 describes factors to be taken into account when planning to use connectorized ODUs with external antennas in PTP 650 links.
- Data network planning on page 3-27 describes factors to be considered when planning PTP 650 data networks.
- Network management planning on page 3-31 describes how to plan for PTP 650 links to be managed remotely using SNMP.
- Security planning on page 3-33 describes how to plan for PTP 650 links to operate in secure mode.
- System threshold, output power and link loss on page 3-41 contains tables that specify the system threshold (dBm), output power (dBm) and maximum link loss (dB) per channel bandwidth and modulation mode.
- Data throughput capacity tables on page 3-47 contains tables and graphs to support calculation of the data rate capacity that can be provided by PTP 650 configurations.

Typical deployment

This section contains diagrams illustrating typical PTP 650 site deployments.

ODU with POE interface to PSU

In the basic configuration, there is only one Ethernet interface, a copper Cat5e power over Ethernet (POE) from the PSU to the ODU (PSU port), as shown in the following diagrams: mast or tower installation (Figure 23), wall installation (Figure 24) and roof installation (Figure 25).

Figure 23 Mast or tower installation

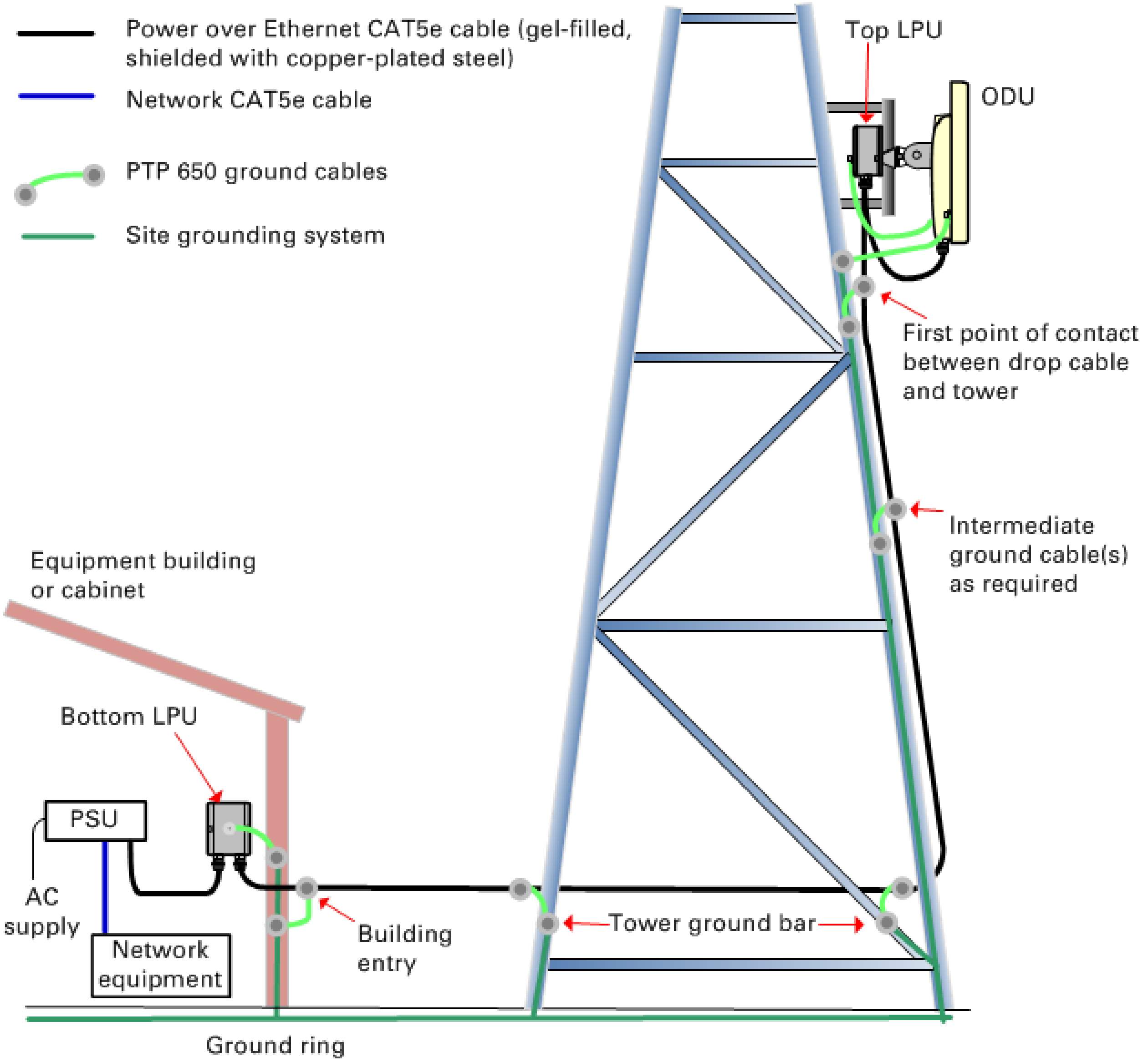

Power over Ethernet CAT5e cable (gel-filled, shielded with copper-plated steel)
Network CAT5e cable
PTP 650 ground cables
Site grounding system
Top LPU
ODU
First point of contact between drop cable and tower
Intermediate ground cable(s) as required
Equipment building or cabinet
Bottom LPU
PSU
AC supply
Network equipment
Building entry
Tower ground bar
Ground ring

Figure 24 Wall installation

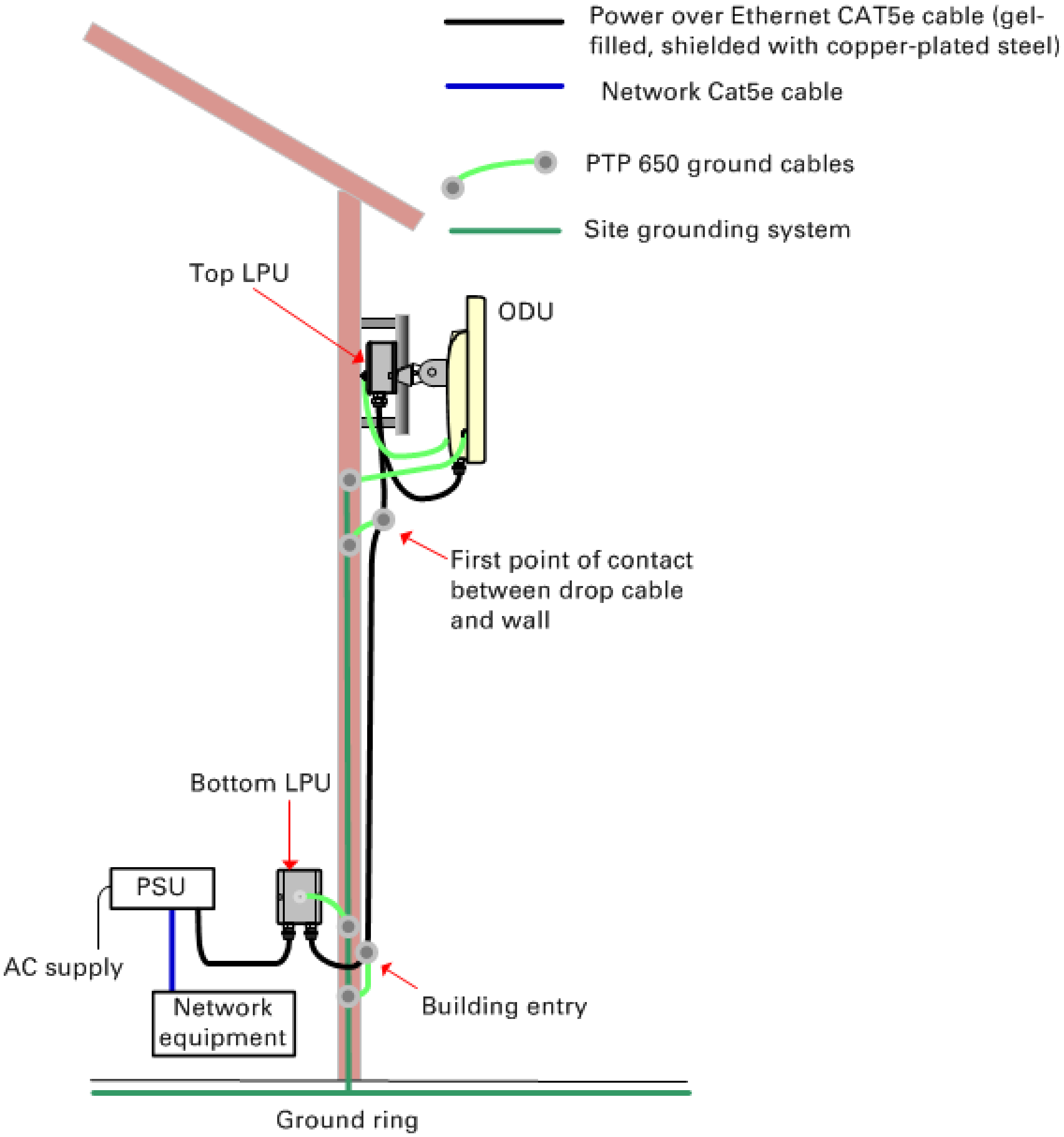
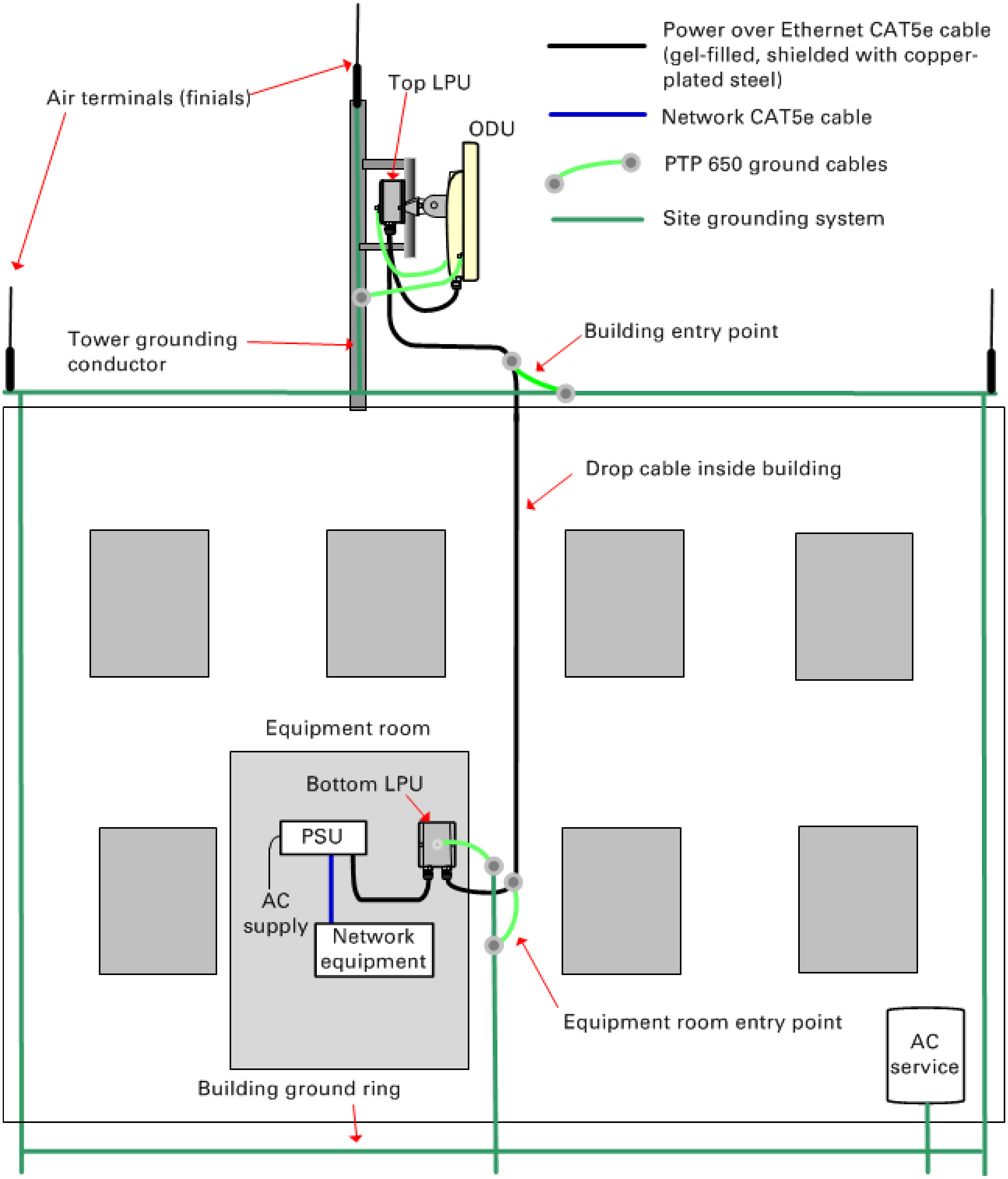


Figure 25 Roof installation



SFP and Aux Ethernet interfaces

There may be one or two additional Ethernet interfaces connected to the ODU: one to the SFP port (copper or optical) and one to the Aux port, as shown in the following diagrams:

- ODU with copper SFP and PSU interfaces – Figure 26
- ODU with optical SFP and PSU interfaces – Figure 27
- ODU with Aux and PSU interfaces – Figure 28

Figure 26 ODU with copper SFP and PSU interfaces

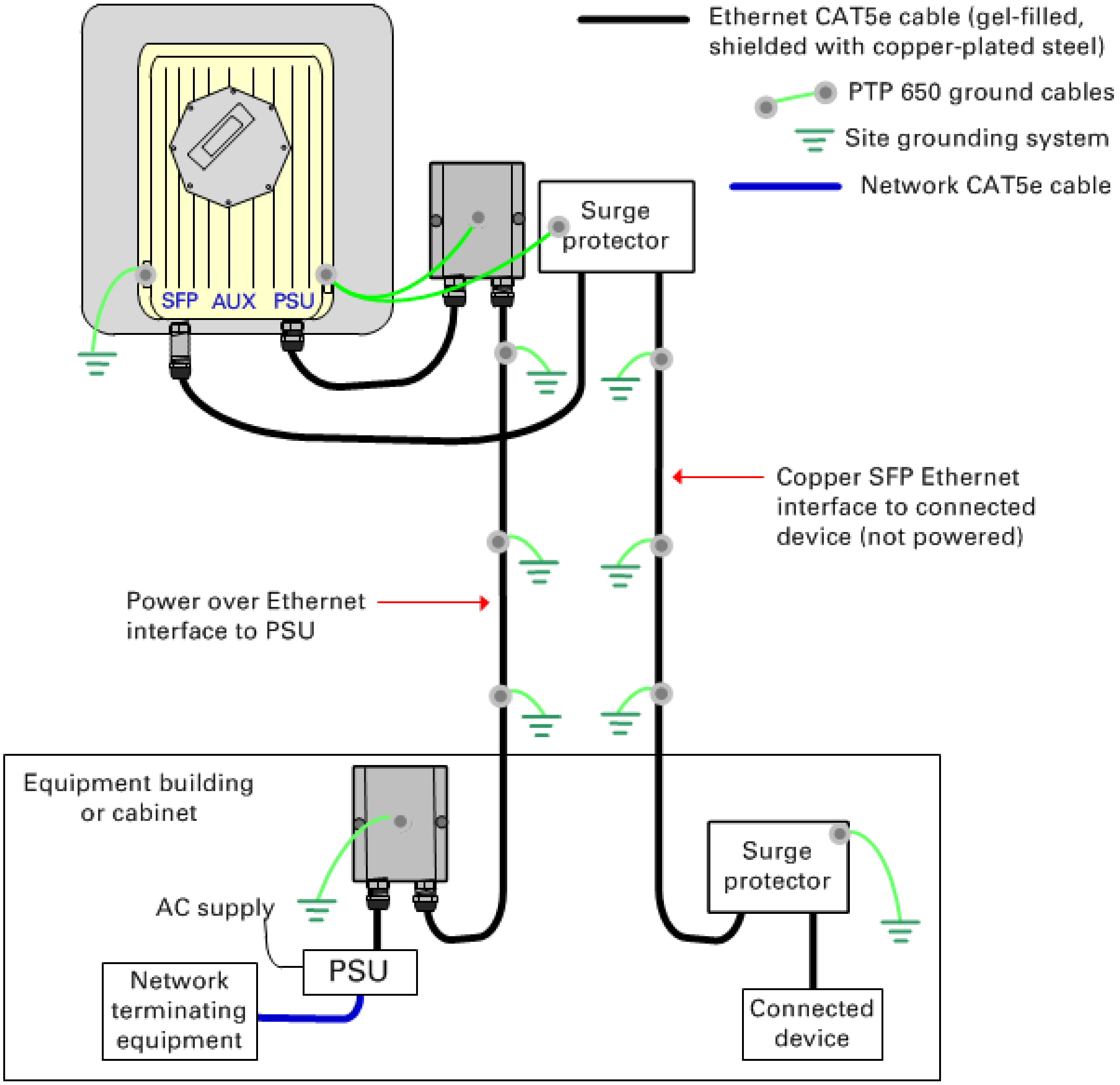

Ethernet CAT5e cable (gel-filled, shielded with copper-plated steel)
PTP 650 ground cables
Site grounding system
Network CAT5e cable
SFP
AUX
PSU
Surge protector
Copper SFP Ethernet interface to connected device (not powered)
Power over Ethernet interface to PSU
Equipment building or cabinet
AC supply
PSU
Network terminating equipment
Surge protector
Connected device

Figure 27 ODU with optical SFP and PSU interfaces

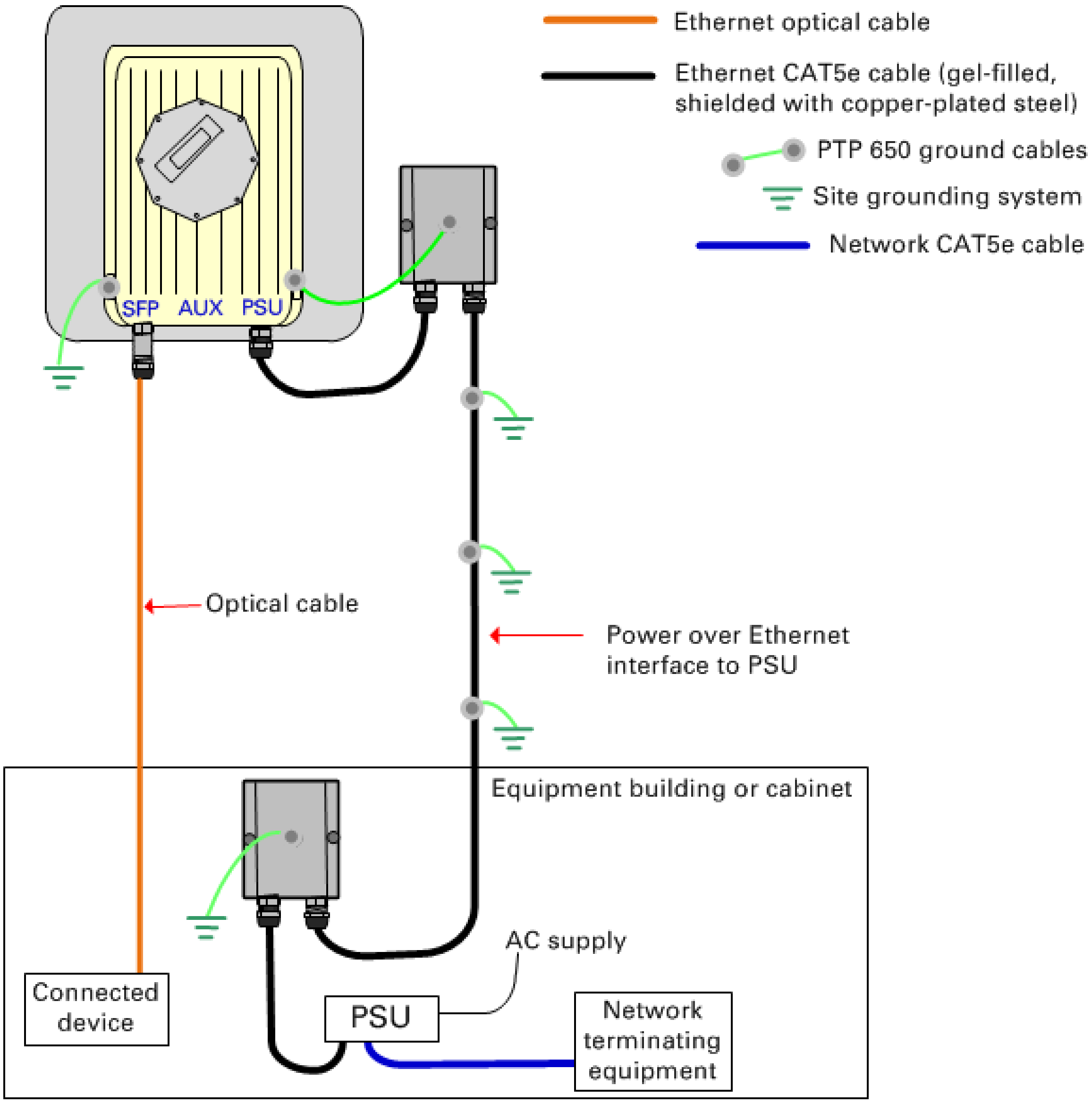
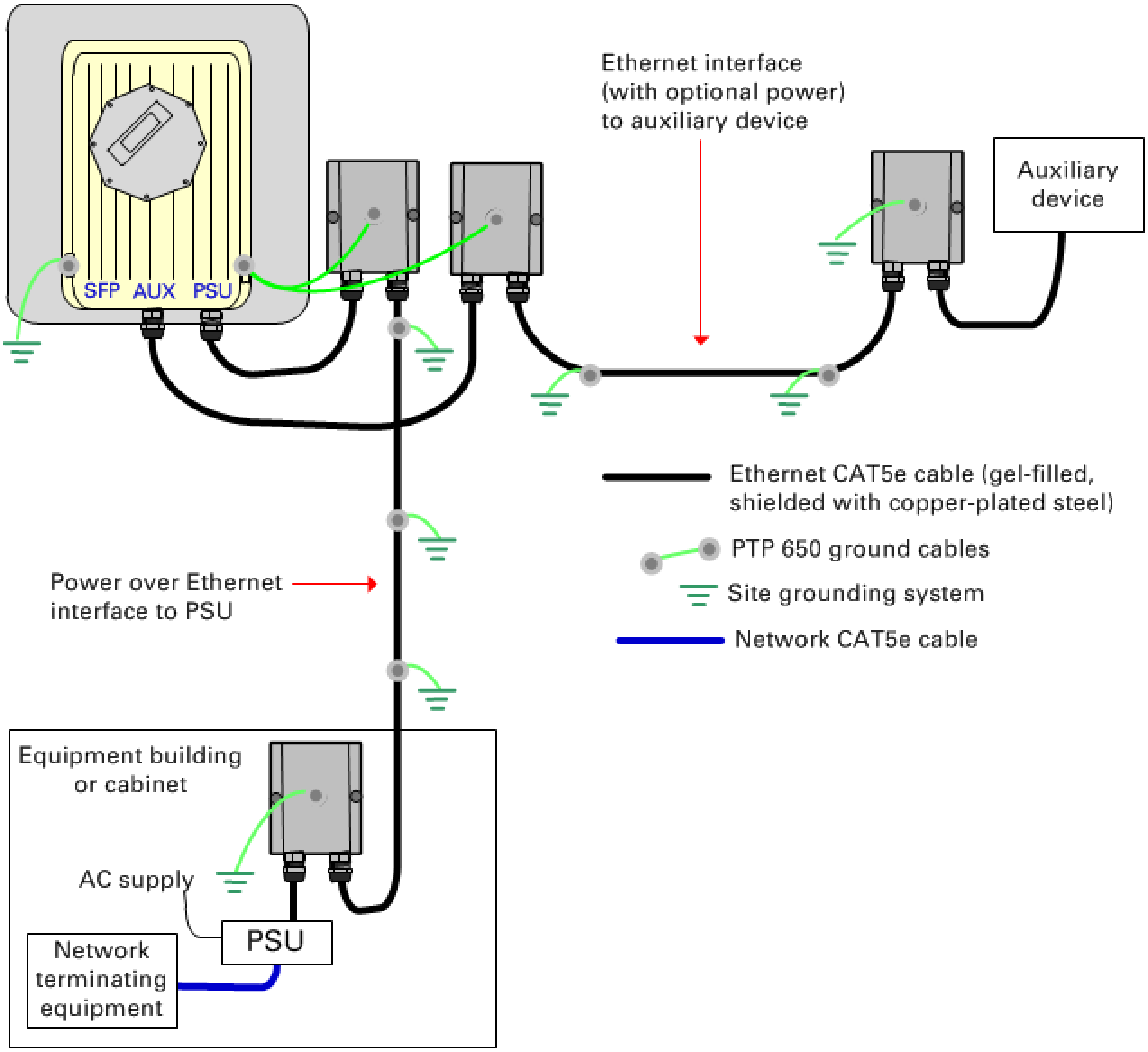

Ethernet optical cable
Ethernet CAT5e cable (gel-filled, shielded with copper-plated steel)
PTP 650 ground cables
Site grounding system
Network CAT5e cable
SFP
AUX
PSU
Optical cable
Power over Ethernet interface to PSU
Equipment building or cabinet
AC supply
Connected device
PSU
Network terminating equipment

Figure 28 ODU with Aux and PSU interfaces


Ethernet interface
(with optional power)
to auxiliary device
Auxiliary device
SFP
AUX
PSU
Ethernet CAT5e cable (gel-filled, shielded with copper-plated steel)
PTP 650 ground cables
Site grounding system
Network CAT5e cable
Power over Ethernet interface to PSU
Equipment building or cabinet
AC supply
PSU
Network terminating equipment

Site planning

This section describes factors to be considered when planning the proposed link end sites, including grounding, lightning protection and equipment location.

Grounding and lightning protection

Warning

Electro-magnetic discharge (lightning) damage is not covered under warranty. The recommendations in this guide, when followed correctly, give the user the best protection from the harmful effects of EMD. However 100% protection is neither implied nor possible.

Structures, equipment and people must be protected against power surges (typically caused by lightning) by conducting the surge current to ground via a separate preferential solid path. The actual degree of protection required depends on local conditions and applicable local regulations. To adequately protect a PTP 650 installation, both ground bonding and transient voltage surge suppression are required.

Full details of lightning protection methods and requirements can be found in the international standards IEC 61024-1 and IEC 61312-1, the U.S. National Electric Code ANSI/NFPA No. 70-1984 or section 54 of the Canadian Electric Code.

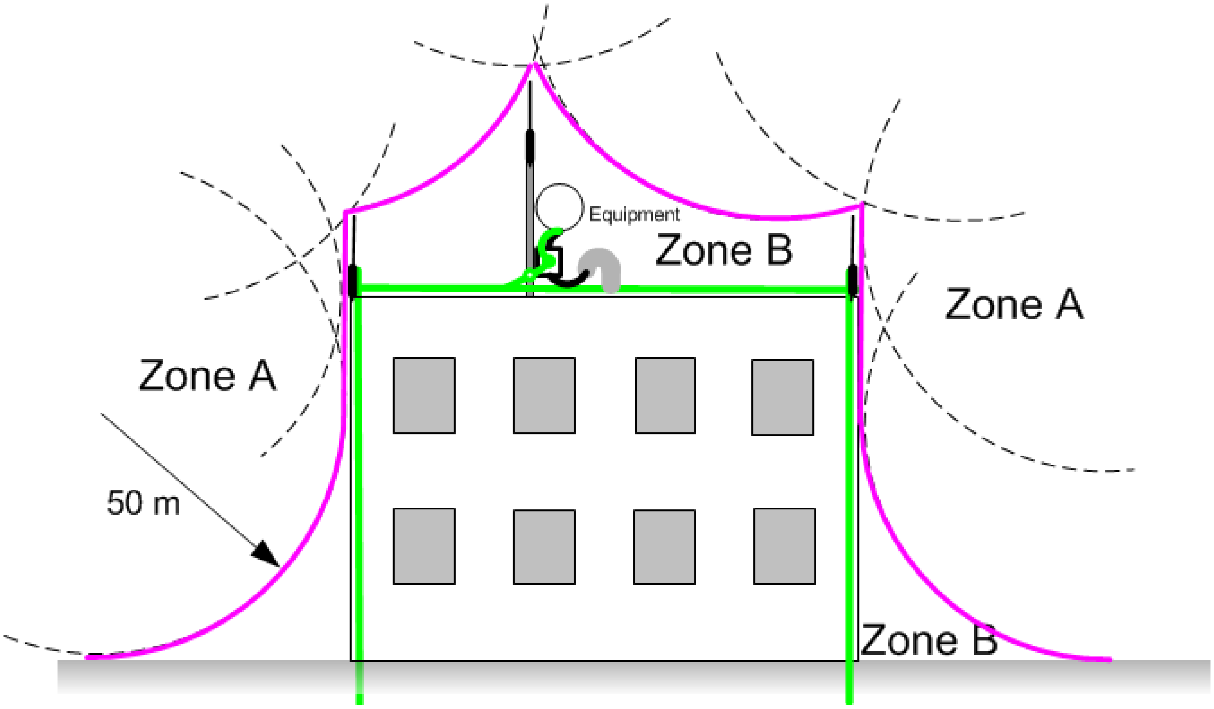
Note

International and national standards take precedence over the requirements in this guide.

Lightning protection zones

Use the rolling sphere method (Figure 29) to determine where it is safe to mount equipment. An imaginary sphere, typically 50 meters in radius, is rolled over the structure. Where the sphere rests against the ground and a strike termination device (such as a finial or ground bar), all the space under the sphere is considered to be in the zone of protection (Zone B). Similarly, where the sphere rests on two finials, the space under the sphere is considered to be in the zone of protection.

Figure 29 Rolling sphere method to determine the lightning protection zones



Assess locations on masts, towers and buildings to determine if the location is in Zone A or Zone B:

- Zone A: In this zone a direct lightning strike is possible. Do not mount equipment in this zone.
- Zone B: In this zone, direct EMD (lightning) effects are still possible, but mounting in this zone significantly reduces the possibility of a direct strike. Mount equipment in this zone.

⚠ **Warning**

Never mount equipment in Zone A. Mounting in Zone A may put equipment, structures and life at risk.

Site grounding system

Confirm that the site has a correctly installed grounding system on a common ground ring with access points for grounding PTP 650 equipment.

If the outdoor equipment is to be installed on the roof of a high building (Figure 25), confirm that the following additional requirements are met:

- A grounding conductor is installed around the roof perimeter to form the main roof perimeter lightning protection ring.
- Air terminals are installed along the length of the main roof perimeter lightning protection ring, typically every 6.1m (20ft).
- The main roof perimeter lightning protection ring contains at least two down conductors connected to the grounding electrode system. The down conductors should be physically separated from one another, as far as practical.

ODU and external antenna location

Find a location for the ODU (and external antenna for connectorized units) that meets the following requirements:

- The equipment is high enough to achieve the best radio path.
- People can be kept a safe distance away from the equipment when it is radiating. The safe separation distances are defined in Calculated distances and power compliance margins on page 4-25.
- The equipment is lower than the top of the supporting structure (tower, mast or building) or its lightning air terminal.
- If the ODU is connectorized, select a mounting position that gives it maximum protection from the elements, but still allows easy access for connecting and weatherproofing the cables. To minimize cable losses, select a position where the antenna cable lengths can be minimized. If diverse or two external antennas are being deployed, it is not necessary to mount the ODU at the midpoint of the antennas.

ODU wind loading

Ensure that the ODU and the structure on which it is mounted are capable of withstanding the prevalent wind speeds at a proposed PTP 650 site. Wind speed statistics should be available from national meteorological offices.

The ODU and its mounting bracket are capable of withstanding wind speeds of up to 323 kph (200 mph).

Wind blowing on the ODU will subject the mounting structure to significant lateral force. The magnitude of the force depends on both wind strength and surface area of the ODU. Wind loading is estimated using the following formulae:

Force (in kilogrammes) = $0.1045aV^2$

Where:	**Is:**
a	surface area in square meters
V	wind speed in meters per second

Force (in pounds) = $0.0042Av^2$

Where:	**Is:**
A	surface area in square feet
v	wind speed in miles per hour

Applying these formulae to the PTP 650 ODU at different wind speeds, the resulting wind loadings are shown in Table 26 and Table 27.

Table 26 ODU wind loading (Kg)

Type of ODU	Max surface area (square meters)	Wind speed (meters per second)				
		30	40	50	60	70
Integrated	0.130	12 Kg	22 Kg	34 Kg	49 Kg	66 Kg
Connectorized	0.093	9 Kg	16 Kg	24 Kg	35 Kg	48 Kg

Table 27 ODU wind loading (lb)

Type of ODU	Max surface area (square feet)	Wind speed (miles per hour)				
		80	100	120	140	150
Integrated	1.36	37 lb	57 lb	82 lb	146 lb	229 lb
Connectorized	1.00	27 lb	42 lb	61 lb	108 lb	168 lb

Note

For a connectorized ODU, add the wind loading of the external antenna to that of the ODU. The antenna manufacturer should be able to quote wind loading.

PSU DC power supply

If using the DC input on the AC+DC power injector, ensure that the DC power supply meets the following requirements:

- The voltage and polarity must be correct and must be applied to the correct PSU terminals.
- The power source must be rated as Safety Extra Low Voltage (SELV).
- The power source must be rated to supply at least 1.5A continuously.
- The power source cannot provide more than the Energy Hazard Limit as defined by IEC/EN/UL60950-1, Clause 2.5, Limited Power (The Energy Hazard Limit is 240VA).

PSU location

Find a location for the PSU (AC Power Injector or AC+DC Enhanced Power Injector) that meets the following requirements:

- The AC+DC Enhanced Power Injector can be mounted on a wall or other flat surface. The AC Power Injector can be mounted on a flat surface.
- The PSU is kept dry, with no possibility of condensation, flooding or rising damp.
- The PSU is located in an environment where it is not likely to exceed its operational temperature rating, allowing for natural convection cooling.
- The PSU can be connected to the ODU drop cable and network terminating equipment.

Find a location for the AC+DC Enhanced power injector where it can be connected to a mains or DC power supply. The use of DC supplies of less than 55V will reduce the usable distance between the PSU and ODU.

Drop cable grounding points

To estimate how many grounding kits are required for each drop cable, refer to the site installation diagrams (Figure 23 , Figure 24 and Figure 25) and use the following criteria:

- The drop cable shield must be grounded near the ODU at the first point of contact between the drop cable and the mast, tower or building.
- The drop cable shield must be grounded at the building entry point.

For mast or tower installations (Figure 23), use the following additional criteria:

- The drop cable shield must be grounded at the bottom of the tower, near the vertical to horizontal transition point. This ground cable must be bonded to the tower or tower ground bus bar (TGB), if installed.
- If the tower is greater than 61 m (200 ft) in height, the drop cable shield must be grounded at the tower midpoint, and at additional points as necessary to reduce the distance between ground cables to 61 m (200 ft) or less.
- In high lightning-prone geographical areas, the drop cable shield must be grounded at spacing between 15 to 22 m (50 to 75 ft). This is especially important on towers taller than 45 m (150 ft).

For roof installations (Figure 25), use the following additional criteria:

- The drop cable shield must be bonded to the building grounding system at its top entry point (usually on the roof).
- The drop cable shield must be bonded to the building grounding system at the entry point to the equipment room.

LPU location

Find a location for the top LPU that meets the following requirements:

- There is room to mount the LPU, either on the ODU mounting bracket or on the mounting pole below the ODU.
- The drop cable length between the ODU and top LPU must not exceed 600 mm.
- There is access to a metal grounding point to allow the ODU and top LPU to be bonded in the following ways: top LPU to ODU; ODU to grounding system.

Find a location for the bottom LPU that meets the following requirements:

- The bottom LPU can be connected to the drop cable from the ODU.
- The bottom LPU is within 600 mm (24 in) of the point at which the drop cable enters the building, enclosure or equipment room within a larger building.
- The bottom LPU can be bonded to the grounding system.

Multiple LPUs

If two or three drop cables are connected to the ODU, the PSU and Aux drop cables each require their own top LPU, and the copper SFP drop cable requires a top surge protector, not a PTP 650 LPU (Figure 30). Optical cables do not require LPUs or ground cables (Figure 31).

The copper SFP drop cable requires a bottom surge protector, not a PTP 650 LPU (Figure 32).

The Aux drop cable may require an LPU near the auxiliary device.

Figure 30 ODU with PSU, Aux and copper SFP interfaces

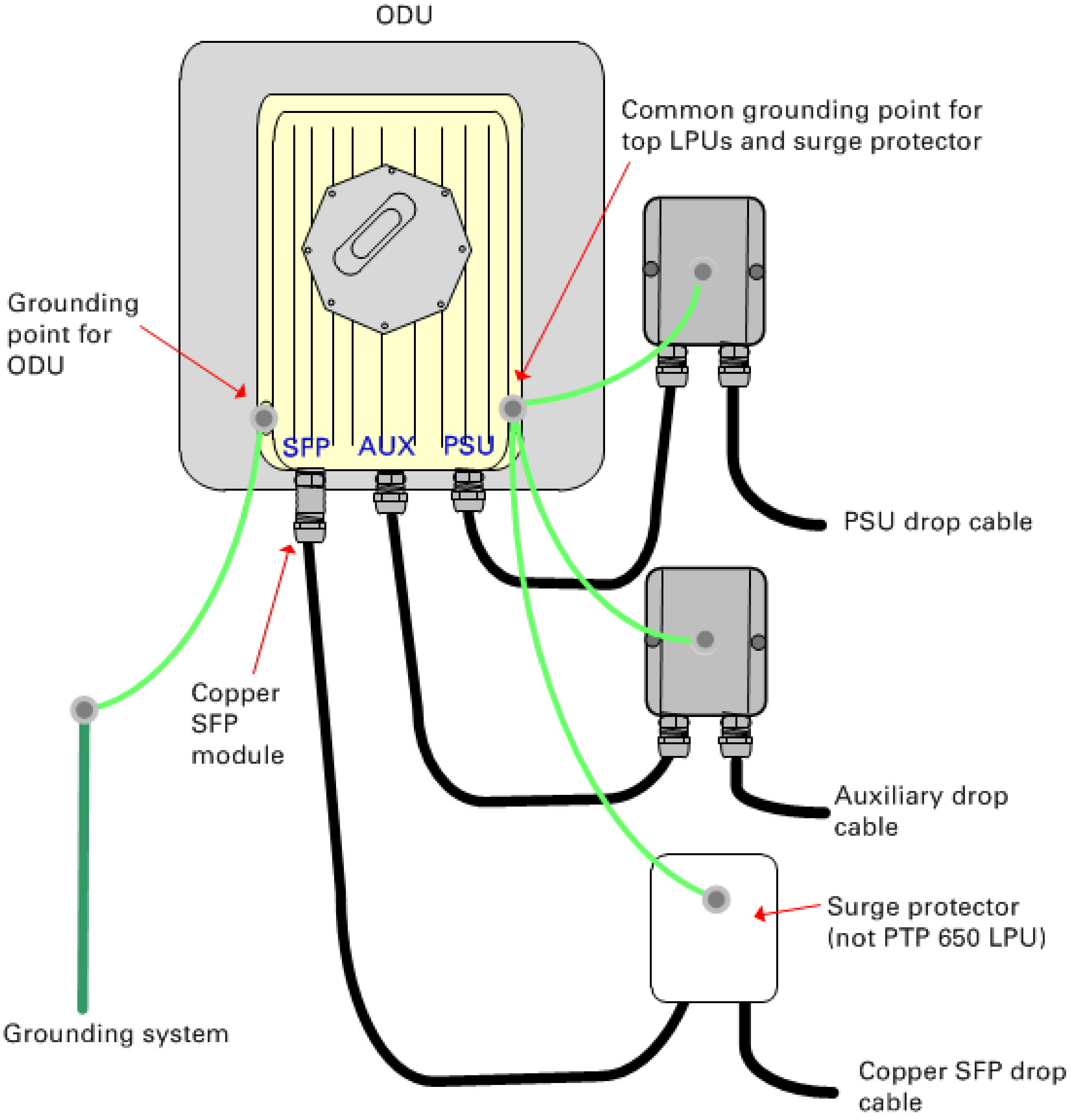


Figure 31 ODU with PSU, Aux and optical SFP interfaces

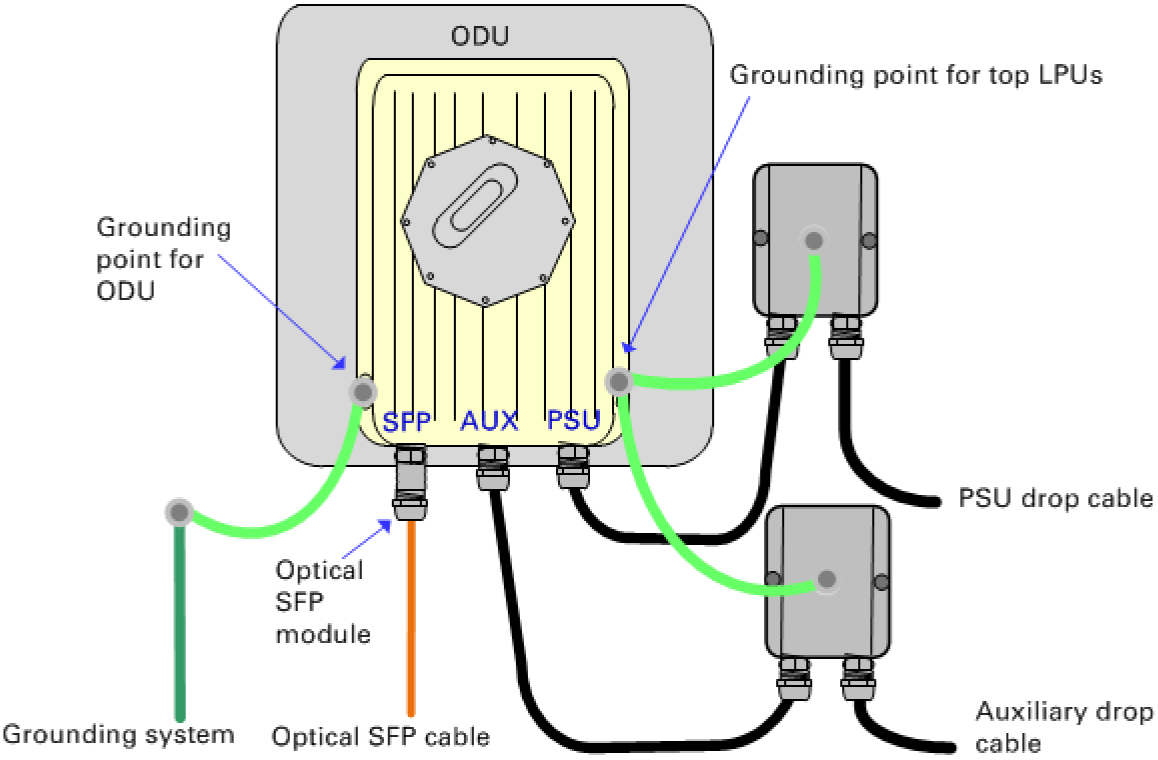
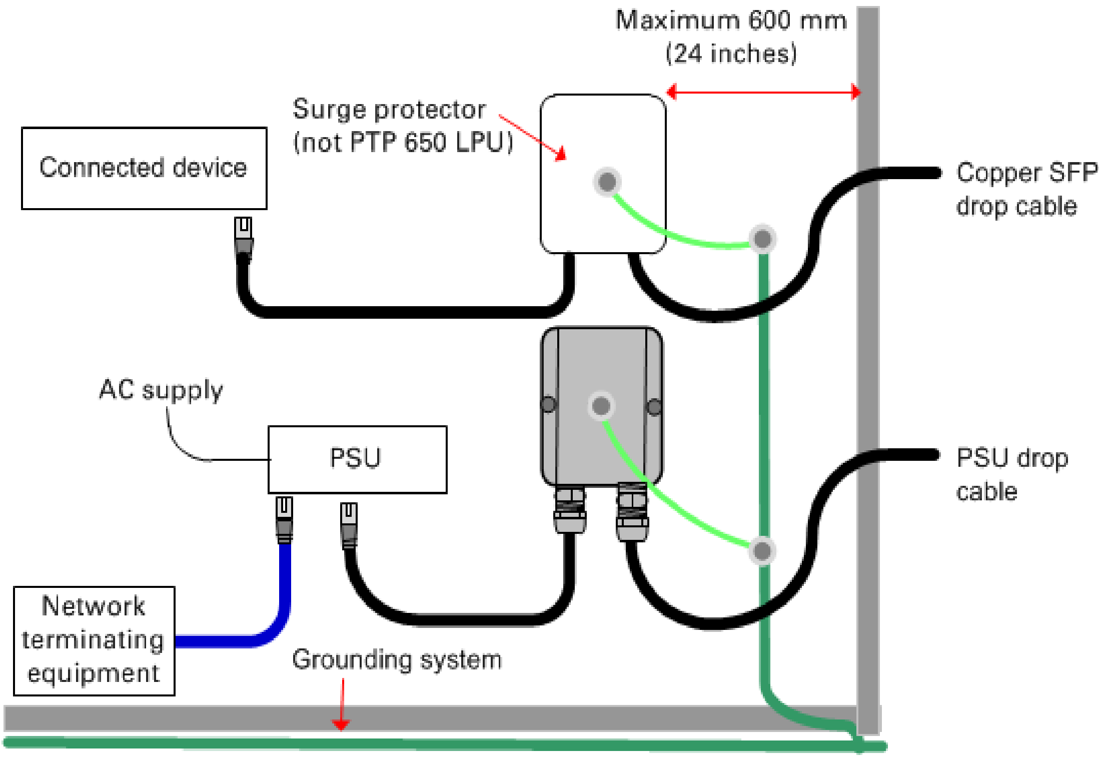


Figure 32 Bottom LPU and surge protector


Maximum 600 mm (24 inches)
Surge protector (not PTP 650 LPU)
Connected device
Copper SFP drop cable
AC supply
PSU
PSU drop cable
Network terminating equipment
Grounding system

Radio spectrum planning

This section describes how to plan PTP 650 links to conform to the regulatory restrictions that apply in the country of operation.

Caution

It is the responsibility of the user to ensure that the PTP product is operated in accordance with local regulatory limits.

Note

Contact the applicable radio regulator to find out whether or not registration of the PTP 650 link is required.

General wireless specifications

Table 28 lists the wireless specifications that apply to all PTP 650 frequency bands. Table 29 lists the wireless specifications that are specific to a single frequency band.

Table 28 PTP 650 wireless specifications (all variants)

Item	Specification
Channel selection	Manual selection (fixed frequency). Dynamic frequency selection (DFS or DFS with DSO) is available in radar avoidance regions.
Manual power control	To avoid interference to other users of the band, maximum power can be set lower than the default power limit.
Integrated antenna type	Flat plate antenna
Duplex schemes	Symmetric fixed, asymmetric fixed and, for the Full variant only, adaptive TDD.
Range	Optical Line-of-Sight: 200 km (125 miles). Non-Line-of-Sight: 10 km (6 miles).
Over-the-air encryption	AES 128-bit or 256-bit.
Weather sensitivity	Sensitivity at higher modes may be reduced by adjusting the Adaptive Modulation Threshold.
Error Correction	FEC

Table 29 PTP 650 wireless specifications (per frequency band)

Item	4.9 GHz	5.4 GHz	5.8 GHz
RF band (GHz)	4.900 -4.990	5.470 -5.725	5.725 -5.875
Channel bandwidth	10, 20 MHz	10, 20, 40, 45 MHz	10, 20, 40, 45 MHz
Typical receiver noise	6 dB	6 dB	6 dB
Typical antenna gain (integrated)	23 dBi	23 dBi	23 dBi
Antenna beamwidth (integrated)	8°	8°	8°

Regulatory limits

Many countries impose EIRP limits (Allowed EIRP) on products operating in the bands used by the PTP 650 Series. For example, in the 5.4 GHz and 5.8 GHz bands, these limits are calculated as follows:

- In the 5.4 GHz band (5470 MHz to 5725 MHz), the EIRP must not exceed the lesser of 30 dBm or (17 + 10 x Log Channel width in MHz) dBm.
- In the 5.8 GHz band (5725 MHz to 5875 MHz), the EIRP must not exceed the lesser of 36 dBm or (23 + 10 x Log Channel width in MHz) dBm.

Some countries (for example the USA) impose conducted power limits on products operating in the 5.8 GHz band.

Conforming to the limits

Ensure the link is configured to conform to local regulatory requirements by installing license keys for the correct country. In the following situations, the license key does not prevent operation outside the regulations:

- When using connectorized ODUs with external antennas, the regulations may require the maximum transmit power to be reduced.
- When installing 5.4 GHz links in the USA, it may be necessary to avoid frequencies used by Terminal Doppler Weather Radar (TDWR) systems. For more information, refer to Avoidance of weather radars (USA only) on page 3-20.

Available spectrum

The available spectrum for operation depends on the regulatory band. When configured with the appropriate license key, the unit will only allow operation on those channels which are permitted by the regulations.

Note

In Italy, there is a regulation which requires a general authorization of any 5.4 GHz radio link which is used outside the operator's own premises. It is the responsibility of the installer or operator to have the link authorized. Details may be found at:

http://www.sviluppoeconomico.gov.it/index.php?option=com_content&view=article&idmenu=672&idarea1=593&andor=AND&idarea2=1052&id=68433&sectionid=1,16&viewType=1&showMenu=1&showCat=1&idarea3=0&andorcat=AND&partebassaType=0&idareaCalendario1=0&MvediT=1&idarea4=0&showArchiveNewsBotton=0&directionidUser=0

The form to be used for general authorization may be found at:

http://www.sviluppoeconomico.gov.it/images/stories/mise_extra/Allegato%20n19.doc

Certain regulations have allocated certain channels as unavailable for use:

- ETSI has allocated part of the 5.4 GHz band to weather radar.
- UK and some other European countries have allocated part of the 5.8 GHz band to Road Transport and Traffic Telematics (RTTT) systems.

The number and identity of channels barred by the license key and regulatory band is dependent on the channel bandwidth and channel raster selected.

Barred channels are indicated by a "No Entry" symbol displayed on the Spectrum Management web page (Spectrum management in radar avoidance mode on page 7-27).

Channel bandwidth

Select the required channel bandwidth for the link. The selection depends upon the regulatory band selected.

The wider the channel bandwidth, the greater the capacity. As narrower channel bandwidths take up less spectrum, selecting a narrow channel bandwidth may be a better choice when operating in locations where the spectrum is very busy.

Both ends of the link must be configured to operate on the same channel bandwidth.

Frequency selection

Regions without mandatory radar detection

In regions that do not mandate DFS, choose **DSO** or **Fixed Frequency**:

- **Dynamic Spectrum Optimization (DSO)**: In this mode, the unit monitors the spectrum looking for the channel with the lowest level of interference. Statistical techniques are used to select the most appropriate transmit and receive channels. The unit can be configured such that it operates in DSO mode, but does not operate on selected channels. This allows a frequency plan to be implemented in cases where multiple links are installed in close proximity.
- **Fixed Frequency**: In this mode, the unit must be configured with a single fixed transmit frequency and a single fixed receive frequency. These may set to the same value or to different values. This mode should only be considered in exceptional circumstances, for example where it is known that are no sources of interference on the selected channels.

Regions with mandatory radar detection

In regions that mandate DFS, the unit first ensures that there is no radar activity on a given channel for a period of 60 seconds before radiating on that channel. Once a channel has been selected for operation, the unit will continually monitor for radar activity on the operating channel. If detected, it will immediately cease radiating and attempt to find a new channel.

In DFS regions, choose **DFS** or **DFS with DSO**:

- **Dynamic Frequency Selection (DFS)**: Once a channel is selected, the unit will only attempt to find an alternative channel if radar activity has been detected on the operating channel.
- **DFS with DSO**: In addition to switching channels on detection of radar, the unit will also switch to a channel which has a significantly lower level of interference than the current channel of operation. Before radiating on the newly selected channel, the unit must again ensure that there is no radar activity on the new channel for a period of 60 seconds. This mode therefore provides the benefit of switching to a channel with lower interference but at the expense of an outage of approximately 60 to 120 seconds. For this reason, the threshold for switching channels is greater than when DSO is operating in a non-radar region.

Radar avoidance requirements in the 5.4 GHz band are defined as follows:

- For the EU: in specification EN 301-893 V1.6.1.
- For the US: in the specification FCC part 15.407 plus the later requirements covered in **Important Regulatory Information** in this User Guide.
- For Canada: in the specification RSS210 Annex 9 (Issue 8).

Radar avoidance at 5.8 GHz is applicable to EU operation (not FCC/IC) and the requirements are defined in EN 302 502 V1.1.1.

Avoidance of weather radars (USA only)

To comply with FCC rules (KDB 443999: Interim Plans to Approve UNII Devices Operating in the 5470 - 5725 MHz Band with Radar Detection and DFS Capabilities), units which are installed within 35 km (22 miles) of a Terminal Doppler Weather Radar (TDWR) system (or have a line of sight propagation path to such a system) must be configured to avoid any frequency within +30 MHz or –30 MHz of the frequency of the TDWR device. This requirement applies even if the master is outside the 35 km (22 miles) radius but communicates with outdoor clients which may be within the 35 km (22 miles) radius of the TDWRs.

If interference is not eliminated, a distance limitation based on line-of-sight from TDWR will need to be used. Devices with bandwidths greater than 20 MHz may require greater frequency separation.

When planning a link in the USA, visit http://spectrumbridge.com/udia/home.aspx, enter the location of the planned link and search for TDWR radars. If a TDWR system is located within 35 km (22 miles) or has line of sight propagation to the PTP device, perform the following tasks:

- Register the installation on http://spectrumbridge.com/udia/home.aspx.
- Make a list of channel center frequencies that must be barred, that is, those falling within +30 MHz or –30 MHz of the frequency of the TDWR radars.

The affected channels must be barred as described in Barring channels on page 7-31.

Edge channel power reduction

Operation at or near the 5.8 GHz band edges can result in a lower maximum transmit power. The amount of reduction, if any, is dependent on the regulatory band. This currently only affects systems configured with regulatory band 1 (Table 30).

Table 30 Edge channel power reduction in regulatory band 1

Channel Bandwidth	Channel Frequency	Maximum power
10 MHz	Below 5737.0 MHz	25 dB
	Above 5837.0 MHz	25 dB
20 MHz	Below 5742.0 MHz	25 dB
	Above 5832.0 MHz	25 dB
40 MHz	Below 5765.0 MHz	24 dB
	Above 5810.0 MHz	24 dB
45 MHz	Below 5778.0 MHz	23 dB
	Above 5795.0 MHz	23 dB

Link planning

This section describes factors to be taken into account when planning links, such as range, obstacles path loss and throughput. PTP LINKPlanner is recommended.

PTP LINKPlanner

The Cambium PTP LINKPlanner software and user guide may be downloaded from the support website (see Contacting Cambium Networks on page 1).

PTP LINKPlanner imports path profiles and predicts data rates and reliability over the path. It allows the system designer to try different antenna heights and RF power settings. It outputs an installation report that defines the parameters to be used for configuration, alignment and operation. The installation report can be used to compare the predicted and actual performance of the link.

Range and obstacles

Calculate the range of the link and identify any obstacles that may affect radio performance.

Perform a survey to identify all the obstructions (such as trees or buildings) in the path and to assess the risk of interference. This information is necessary in order to achieve an accurate link feasibility assessment.

The PTP 650 Series is designed to operate in Non-Line-of-Sight (NLoS) and Line-of-Sight (LoS) environments. An NLOS environment is one in which there is no optical line-of-sight, that is, there are obstructions between the antennas.

The PTP 650 Series will operate at ranges from 100 m (330 ft) to 200 km (125 miles), within 3 modes: 0-40 km (0-25 miles), 0-100 km (0-62 miles) and 0-200 km (0-124 miles). Operation of the system will depend on obstacles in the path between the units. Operation at 40 km (25 miles) or above will require a near line-of-sight path. Operation at 100 m (330 ft) could be achieved with one unit totally obscured from the other unit, but with the penalty of transmitting at higher power in a non-optimal direction, thereby increasing interference in the band.

LoS links in radar regions

When planning an LoS link to operate in a radar detection region, ensure that receiver signal level is low enough to allow the PTP 650 to detect radar signals:

- With integrated antennas, the recommended minimum LoS operating range is 110 meters (360 ft) for 5.4 GHz or 185 meters (610 ft) for 5.8 GHz. Shorter operating ranges will lead to excessive receiver signal levels.
- With higher gain connectorized antennas, ensure the predicted receiver signal level (from LINKPlanner) is below -53 dBm (for 5.4 GHz) or below -58 dBm (for 5.8 GHz).

Path loss

Path loss is the amount of attenuation the radio signal undergoes between the two ends of the link. The path loss is the sum of the attenuation of the path if there were no obstacles in the way (Free Space Path Loss), the attenuation caused by obstacles (Excess Path Loss) and a margin to allow for possible fading of the radio signal (Fade Margin). The following calculation needs to be performed to judge whether a particular link can be installed:

$$L_{free\_space} + L_{excess} + L_{fade} + L_{seasonal} < L_{capability}$$

Where:	Is:
L_{free_space}	Free Space Path Loss (dB)
L_{excess}	Excess Path Loss (dB)
L_{fade}	Fade Margin Required (dB)
$L_{seasonal}$	Seasonal Fading (dB)
$L_{capability}$	Equipment Capability (dB)

Adaptive modulation

Adaptive modulation ensures that the highest throughput that can be achieved instantaneously will be obtained, taking account of propagation and interference. When the link has been installed, web pages provide information about the link loss currently measured by the equipment, both instantaneously and averaged. The averaged value will require maximum seasonal fading to be added, and then the radio reliability of the link can be computed. For minimum error rates on TDM links, the maximum modulation mode should be limited to 64QAM 0.75.

For details of the system threshold, output power and link loss for each frequency band in all modulation modes for all available channel bandwidths, refer to System threshold, output power and link loss on page 3-41.

Calculating data rate capacity

The data rate capacity of a PTP link is defined as the maximum end-to-end Ethernet throughput (including Ethernet headers) that it can support. It is assumed that Ethernet frames are 1500 octet. Data rate capacity is determined by the following factors:

- Licensed data throughput capability (ODU variant: Lite, Mid or Full)
- Link Symmetry
- Link Mode Optimization (IP or TDM)
- Modulation Mode
- Channel Bandwidth
- Link Range

Calculation procedure

To calculate the data rate capacity of a PTP 650 link, proceed as follows:

1. Use the tables in Data throughput capacity tables on page 3-47 to look up the data throughput capacity rates (Tx, Rx and Both) for the required combination of:

    - Link Symmetry
    - Link Mode Optimization
    - Modulation Mode
    - Channel Bandwidth

    The tables contain data rates for PTP 650 Full only.

2. The tables contain data rates for links of zero range. Use the range adjustment graphs in Data throughput capacity tables on page 3-47 to look up the Throughput Factor that must be applied to adjust the data rates for the actual range of the link.

3. Multiply the data rates by the Throughput Factor to give the throughput capacity of the link.

Note

The data rates for adaptive symmetry apply to the most asymmetric case where the link has significant offered traffic in one direction only. The data rates for adaptive symmetry with bidirectional offered traffic are the same as those for link symmetry 1:1 with link optimization IP.

Calculation example

Suppose that the link characteristics are:

- PTP 650 variant = Mid
- Link Symmetry = 1:1
- Link Mode Optimization = TDM
- Modulation Mode = 64QAM 0.92 Dual
- Channel Bandwidth = 10 MHz
- Link Range = 60 km

The calculation procedure for this example is as follows:

1. Use Table 52 to look up the data throughput capacity rates:

   Tx = 23 Mbits/s

   Rx = 23 Mbits/s

   Aggregated = 46 Mbits/s

2. Use Figure 40 to look up the Throughput Factor for 1:1, TDM, 10 MHz, Mid and Link Range 60 km. The factor is 0.86.

3. Multiply the rates from Step 1 by the Throughput Factor from Step 2 to give the throughput capacity of the link:

   Tx = 19.8 Mbits/s

   Rx = 19.8 Mbits/s

   Aggregated = 39.6 Mbits/s

Planning for connectorized units

This section describes factors to be taken into account when planning to use connectorized ODUs with external antennas in PTP 650 links.

When to install connectorized units

The majority of radio links can be successfully deployed with the integrated ODU. However the integrated units may not be sufficient in some areas, for example:

- Where the path is heavily obscured by dense woodland on an NLOS link.
- Where long LOS links (>23 km or >14 miles) are required.
- Where there are known to be high levels of interference.

PTP LINKPlanner can be used to identify these areas of marginal performance.

In these areas, connectorized ODUs and external antennas should be used.

Choosing external antennas

When selecting external antennas, consider the following factors:

- The required antenna gain.
- Ease of mounting and alignment.
- Antenna polarization:
  - For a simple installation process, select one dual-polarization antenna (as the integrated antenna) at each end.
  - To achieve spatial diversity, select two single-polarization antennas at each end. Spatial diversity provides additional fade margin on very long LOS links where there is evidence of correlation of the fading characteristics on Vertical and Horizontal polarizations.

Note

Enter the antenna gain and cable loss into the Installation Wizard, if the country selected has an EIRP limit, the corresponding maximum transmit power will be calculated automatically by the unit.

Note

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that necessary for successful communication.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

Calculating RF cable length (5.8 GHz FCC only)

The 5.8 GHz band FCC approval for the product is based on tests with a cable loss between the ODU and antenna of not less than 1.2 dB. If cable loss is below 1.2 dB with a 1.3 m (6 ft) diameter external antenna, the connectorized PTP 650 may exceed the maximum radiated spurious emissions allowed under FCC 5.8 GHz rules.

Cable loss depends mainly upon cable type and length. To meet or exceed the minimum loss of 1.2 dB, use cables of the type and length specified in Table 31 (source: Times Microwave). This data excludes connector losses.

Table 31 RF cable lengths required to achieve 1.2 dB loss at 5.8 GHz

RF cable type	Minimum cable length
LMR100	0.6 m (1.9 ft)
LMR200	1.4 m (4.6 ft)
LMR300	2.2 m (7.3 ft)
LMR400	3.4 m (11.1 ft)
LMR600	5.0 m (16.5 ft)

Data network planning

This section describes factors to be considered when planning PTP 650 data networks.

Ethernet interfaces

The PTP 650 Ethernet ports conform to the specifications listed in Table 32.

Table 32 PTP 650 Ethernet bridging specifications

Ethernet Bridging	Specification
Protocol	IEEE802.1; IEEE802.1p; IEEE802.3 compatible
QoS	Eight wireless interface priority queues based on these standards: IEEE 802.1p, IEEE 802.1Q, IEEE 802.1ah, IEEE 802.1ad, DSCP IPv4, DSCP IPv6, MPLS TC
Interfaces	100BASE-TX, 1000BASE-T, 1000BASE-SX, 1000BASE-LX MDI/MDIX auto crossover supported
Max Ethernet frame size	9600 bytes
Service classes for traffic	8 classes

Practical Ethernet rates depend on network configuration and higher layer protocols. Over the air throughput is capped to the rate of the Ethernet interface at the receiving end of the link.

Layer 2 control protocols

PTP 650 identifies L2 control protocols from the Ethernet destination address of bridged frames:

Table 33 Destination address in layer 2 control protocols

Destination address	Protocol
01-80-c2-00-00-00 to 01-80-c2-00-00-0f	IEEE 802.1 bridge protocols
01-80-c2-00-00-20 to 01-80-c2-00-00-2f	IEEE 802.1 Multiple Registration Protocol (MRP)
01-80-c2-00-00-30 to 01-80-c2-00-00-3f	IEEE 802.1ag, Connectivity Fault Management (CFM)
01-19-a7-00-00-00 to 01-19-a7-00-00-ff	Ring Automatic Protection Switching (R-APS)
00-e0-2b-00-00-04	Ethernet Automatic Protection Switching (EAPS)

Ethernet port allocation

Decide how the three Ethernet ports will be allocated to the customer data network, in-band management and out-of-band local management, based on the following rules:

- Ensure that one port is allocated to Data Only or Data and In-Band Management. This port should be associated with the customer data network.
- Ensure that the remaining ports are set to Disabled or Out-of-Band Local Management.
- Ensure that at least one port is allocated for in-band or out-of-band network management. This port should be associated with the management network.

Note

The Main PSU port is always used to supply power to the ODU, even when it is Disabled for the purpose of Ethernet port allocation.

VLAN membership

Decide if the IP interface of the ODU management agent will be connected in a VLAN. If so, decide if this is a standard (IEEE 802.1Q) VLAN or provider bridged (IEEE 802.1ad) VLAN, and select the VLAN ID for this VLAN.

Use of a separate management VLAN is strongly recommended. Use of the management VLAN helps to ensure that the ODU management agent cannot be accessed by customers.

Priority for management traffic

Choose the Ethernet and IP (DSCP) priority for management traffic generated within the ODU management agent. The priority should be selected so as to be consistent with existing policy on priority of management traffic in the network. Use of a high priority is strongly recommended to ensure that management traffic is not discarded if the link is overloaded.

Ensure that the priority assigned to management traffic is consistent with the quality of service scheme configured for bridged Ethernet traffic. If QoS for bridged traffic is based on the IP/MPLS scheme, set the DSCP management priority to map to a high priority queue. If QoS for bridged traffic is based on the Ethernet scheme, set the VLAN management priority to map to a high priority queue.

IP interface

Select the IP version for the IP interface of the ODU management agent. PTP 650 can operate in IPv4 mode, IPv6 mode, or in a dual IPv4/IPv6 mode. Choose one IPv4 address and/or one IPv6 address for the IP interface of the ODU management agent. The IP address or addresses must be unique and valid for the connected network segment and VLAN.

Find out the correct subnet mask (IPv4) or prefix length (IPv6) and gateway IP address for this network segment and VLAN.

Ensure that the design of the data network permits bidirectional routing of IP datagrams between network management systems and the ODUs. For example, ensure that the gateway IP address identifies a router or other gateway that provides access to the rest of the data network.

Quality of service for bridged Ethernet traffic

Decide how quality of service will be configured in PTP 650 to minimize frame loss and latency for high priority traffic. Wireless links often have lower data capacity than wired links or network equipment like switches and routers, and quality of service configuration is most critical at network bottlenecks.

PTP 650 provides eight queues for traffic waiting for transmission over the wireless link. Q0 is the lowest priority queue and Q7 is the highest priority queue. Traffic is scheduled using strict priority; in other words, traffic in a given queue is transmitted when all higher-priority queues are empty.

Layer 2 control protocols

Select the transmission queue for each of the recognised layer 2 control protocols (L2CP). These protocols are essential to correct operation of the Ethernet network, and are normally mapped to a high priority queue. Ethernet frames that match one of the recognized L2CPs are not subject to the Ethernet and IP/MPLS classification described below.

Priority schemes

Select the priority scheme based on Ethernet priority or IP/MPLS priority to match QoS policy in the rest of the data network. Ethernet priority is also known as Layer 2 or link layer priority. IP/MPLS priority is also known as Layer 3 or network layer priority.

Ethernet priority scheme

Ethernet priority is encoded in a VLAN tag. Use the Ethernet priority scheme if the network carries traffic in customer or service provider VLANs, and the priority in the VLAN tag has been set to indicate the priority of each type of traffic. Select a suitable mapping from the Ethernet priority to the eight PTP 650 queues.

An advantage of Ethernet priority is that any VLAN-tagged frame can be marked with a priority, regardless of the higher-layer protocols contained within the frame. A disadvantage of Ethernet priority is that the priority in the frame must be regenerated whenever traffic passes through a router.

IP/MPLS priority scheme

IP priority is encoded in the DSCP value encoded in the ToS field in IPv4 and Traffic Class in IPv6. The DSCP field provides 64 levels of priority. Determine the DSCP values used in the network and select a suitable mapping from these DSCP values to the eight PTP 650 queues.

The advantages of IP priority are that priority in the IP header is normally propagated transparently through a router, also the DSCP field supports a large number of distinct priority code points. A disadvantage of DSCP is that frames receive a single default classification if they contain a network layer protocol other than IPv4 or IPv6. This is controlled by the user setting the Unknown Network Layer Protocol queue value in the same QoS Configuration page under IP/MPLS QoS.

MPLS priority is encoded in the traffic class (TC) field in the outermost MPLS label. Select a suitable mapping from MPLS TC to the eight PTP 650 queues.

“Daisy-chaining” PTP 650 links

When connecting two or more PTP 650 links together in a network (daisy-chaining), do not install direct copper Cat5e connections between the PSUs. Each PSU must be connected to the network terminating equipment using the LAN port. To daisy-chain PTP 650 links, install each ODU-to-ODU link using one of the following solutions:

- A copper Cat5e connection between the Aux ports of two ODUs. For details of the Ethernet standards supported and maximum permitted cable lengths, see Ethernet standards and cable lengths on page 2-20.
- A copper Cat5e connection between the Aux port of one ODU and the SFP port of the next ODU (using a copper SFP module). For details of the Ethernet standards supported and maximum permitted cable lengths, see Ethernet standards and cable lengths on page 2-20.
- Optical connections between the ODUs (SFP ports) using optical SFP modules at each ODU. For details of the Ethernet standards supported and maximum permitted cable lengths, see SFP module kits on page 2-27.

Green Ethernet switches

Do not connect PTP 650 units to Ethernet networking products that control the level of the transmitted Ethernet signal based on the measured length of the Ethernet link, for example Green Ethernet products manufactured by D-Link Corporation. The Ethernet interfaces in these networking products do not work correctly when connected directly to the PTP 650 PSU.

Network management planning

This section describes how to plan for PTP 650 links to be managed remotely using SNMP.

Planning for SNMP operation

The supported notifications are as follows:

- Cold start
- Wireless Link Up/Down
- Channel Change
- DFS Impulse Interference
- Authentication Failure
- Main PSU Port Up Down
- Aux Port Up Down
- SFP Port Up Down

Ensure that the following MIBs are loaded on the network management system.

- RFC-1493. BRIDGE-MIB
- RFC-2233. IF-MIB
- RFC-3411. SNMP-FRAMEWORK-MIB
- RFC-3412. SNMP-MPD-MIB
- RFC-3413. SNMP-TARGET-MIB
- RFC-3414. SNMP-USER-BASED-SM-MIB
- RFC-3415. SNMP-VIEW-BASED-ACM-MIB
- RFC-3418. SNMPv2-MIB
- RFC-3826. SNMP-USM-AES-MIB
- RFC-4293 IP-MIB
- PTP 650 Series proprietary MIB

Note

The proprietary MIBs are provided in the PTP 650 Series software download files in the support website (see Contacting Cambium Networks on page 1).

Supported diagnostic alarms

PTP 650 supports the diagnostic alarms listed in Table 101.

The web-based interface may be used to enable or disable generation of each supported SNMP notification or diagnostic alarm.

Enabling SNMP

Enable the SNMP interface for use by configuring the following attributes in the SNMP Configuration page:

- SNMP State (default disabled)
- SNMP Version (default SNMPv1/2c)
- SNMP Port Number (default 161)

Security planning

This section describes how to plan for PTP 650 links to operate in secure mode.

Planning for SNTP operation

Note

PTP 650 does not have a battery-powered clock, so the set time is lost each time the ODU is powered down. To avoid the need to manually set the time after each reboot, use SNTP server synchronization.

Before starting to configure Simple Network Time Protocol (SNTP):

- Identify the time zone and daylight saving requirements that apply to the system.
- If SNTP server synchronization is required, identify the details of one or two SNTP servers: IP address, port number and server key.
- Decide whether or not to authenticate received NTP messages using an MD5 signature.

Planning for HTTPS/TLS operation

Before starting to configure HTTPS/TLS operation, ensure that the cryptographic material listed in Table 34 is available.

Table 34 HTTPS/TLS security material

Item	Description	Quantity required
Key of Keys	An encryption key generated using a cryptographic key generator. The key length is dictated by the installed license key. License keys with AES-128 will require a key of keys of 128-bits. License keys with AES-256 will require a key of keys of 256-bits. The key output should be in ASCII hexadecimal characters.	Two per link. For greater security, each link end should be allocated a unique Key of Keys.

Item	Description	Quantity required
TLS Private Key and Public Certificates	An RSA private key of size 2048 bytes, generated in either PKCS#1 or PKCS#5 format, unencrypted, and encoded in the ASN.1 DER format. An X.509 certificate containing an RSA public key, generated in either PKCS#1 or PKCS#5 format, unencrypted, and encoded in the ASN.1 DER format. The public key certificate must have Common Name equal to the IPv4 or IPv6 address of the ODU. The public key certificate must form a valid pair with the private key.	Two pairs per link. These items are unique to IP address.
User Defined Security Banner	The banner provides warnings and notices to be read by the user before logging in to the ODU. Use text that is appropriate to the network security policy.	Normally one per link. This depends upon network policy.
Entropy Input	This must be of size 512 bits (128 hexadecimal characters), output from a random number generator.	Two per link. For greater security, each link end should be allocated a unique Entropy Input.
Wireless Link Encryption Key for AES	An encryption key generated using a cryptographic key generator. The key length is dictated by the selected AES encryption algorithm (128 or 256 bits).	One per link. The same encryption key is required at each link end.
Port numbers for HTTP, HTTPS and Telnet	Port numbers allocated by the network.	As allocated by network.

Planning for SNMPv3 operation

SNMP security mode

Decide how SNMPv3 security will be configured.

MIB-based security management uses standard SNMPv3 MIBs to configure the user-based security model and the view-based access control model. This approach provides considerable flexibility, allowing a network operator to tailor views and security levels appropriate for different types of user. MIB-based security management may allow a network operator to take advantage of built-in security management capabilities of existing network managers.

Web-based security management allows an operator to configure users, security levels, privacy and authentication protocols, and passphrases using the PTP 650 web-based management interface. The capabilities supported are somewhat less flexible than those supported using the MIB-based security management, but will be sufficient in many applications. Selection of web-based management for SNMPv3 security disables the MIB-based security management. PTP 650 does not support concurrent use of MIB-based and web-based management of SNMPv3 security.

Web-based management of SNMPv3 security

Initial configuration of SNMPv3 security is available only to HTTP or HTTPS/TLS user accounts with security role of Security Officer.

Identify the minimum security role of HTTP or HTTPS/TLS user accounts that will be permitted access for web-based management of SNMPv3 security. The following roles are available:

- System Administrator
- Security Officer

Identify the format used for SNMP Engine ID. The following formats are available:

- MAC address (default)
- IPv4 address
- Text string
- IPv6 address

If SNMP Engine ID will be based on a text string, identify the text string required by the network management system. This is often based on some identifier that survives replacement of the PTP hardware.

Identify the user names and security roles of initial SNMPv3 users. Two security roles are available:

- Read Only
- System Administrator

Identify the security level for each of the security roles. Three security levels are available: (a) No authentication, no privacy; (b) Authentication, no privacy; (c) Authentication, privacy.

If authentication is required, identify the protocol. Two authentication protocols are available: MD5 or SHA.

If privacy will be used, identify the protocol. Two privacy protocols are available: DES or AES (an AES 128-bit or 256-bit capability upgrade must be purchased).

If authentication or authentication and privacy protocols are required, identify passphrases for each protocol for each SNMP user. It is considered good practice to use different passphrases for authentication and privacy. Passphrases must have length between 8 and 32 characters, and may contain any of the characters listed in Table 35.

Table 35 Permitted character set for SNMPv3 passphrases

Character	Code	Character	Code
<space>	32	;	59
!	33	<	60
“	34	=	61
#	35	>	62
$	36	?	63
%	37	@	64
&	38	A..Z	65..90
'	39	[	91
(	40	\	92
)	41	]	93
*	42	^	94
+	43	_	95
,	44	`	96
-	45	a..z	97..122
.	46	{	123
/	47	|	124
0..9	48..57	}	125
:	58	~	126

Identify up to two SNMP users that will be configured to receive notifications (traps). Identify the Internet address (IPv4 or IPv6) and UDP port number of the associated SNMP manager.

SNMPv3 default configuration (MIB-based)

When SNMPv3 MIB-based Security Mode is enabled, the default configuration for the `usmUserTable` table is based on one initial user and four template users as listed in Table 36.

Table 36 Default SNMPv3 users

Object	Entry 1
Name	initial
SecurityName	initial
AuthProtocol	usmHMACMD5AuthProtocol
PrivProtocol	usmDESPrivProtocol
StorageType	nonVolatile

Object	Entry 2	Entry 3
Name	templateMD5_DES	templateSHA_DES
SecurityName	templateMD5_DES	templateSHA_DES
AuthProtocol	usmHMACMD5AuthProtocol	usmHMACSAHAuthProtocol
PrivProtocol	usmDESPrivProtocol	usmDESPrivProtocol
StorageType	nonVolatile	nonVolatile

Object	Entry 4	Entry 5
Name	templateMD5_AES	templateSHA_AES
SecurityName	templateMD5_AES	templateSHA_AES
AuthProtocol	usmHMACMD5AuthProtocol	usmHMACSHAAuthProtocol
PrivProtocol	usmAESPrivProtocol	usmAESPrivProtocol
StorageType	nonVolatile	nonVolatile

VACM default configuration

The default user `initial` is assigned to VACM group `initial` in the `vacmSecurityToGroupTable` table. The template users are not assigned to a group.

PTP 650 creates default view trees and access as shown in Table 37 and Table 38.

Table 37 Default VACM view trees

Object	Entry 1	Entry 2
ViewName	internet	restricted
Subtree	1.3.6.1	1.3.6.1
Mask	“”	“”
Type	included	included
StorageType	nonVolatile	nonvolatile

Table 38 Default data fill for access table

Object	Entry 1	Entry 2
GroupName	initial	initial
ContextPrefix	“”	“”
SecurityLevel	authNoPriv	noAuthNoPriv
ContextMatch	exact	exact
ReadViewName	internet	restricted
WriteViewName	internet	“”
NotifyViewName	internet	restricted
StorageType	nonVolatile	nonVolatile

Planning for RADIUS operation

Configure RADIUS where remote authentication is required for users of the web-based interface. Remote authentication has the following advantages:

- Control of passwords can be centralized.
- Management of user accounts can be more sophisticated. For example; users can be prompted by a network manager to change passwords at regular intervals. As another example, passwords can be checked for inclusion of dictionary words and phrases.
- Passwords can be updated without reconfiguring multiple network elements.
- User accounts can be disabled without reconfiguring multiple network elements.

Remote authentication has one significant disadvantage in a wireless link product such as PTP 650. If the wireless link is down, a unit on the remote side of the broken link may be prevented from contacting a RADIUS Server, with the result that users are unable to access the web-based interface.

One useful strategy would be to combine RADIUS authentication for normal operation with a single locally-authenticated user account for emergency use.

PTP 650 provides a choice of the following authentication methods:

- CHAP
- MS-CHAPv2

Ensure that the authentication method selected in PTP 650 is supported by the RADIUS server.

RADIUS attributes

If the standard RADIUS attribute session-timeout (Type 27) is present in a RADIUS response, PTP 650 sets a maximum session length for the authenticated user. If the attribute is absent, the maximum session length is infinite.

If the standard RADIUS attribute idle-timeout (Type 28) is present in a RADIUS response, PTP 650 overrides the Auto Logout Timer with this value in the authenticated session.

If the vendor-specific RADIUS attribute auth-role is present in a RADIUS response, PTP 650 selects the role for the authenticated user according to auth-role. The supported values of auth-role are as follows:

- 0: Invalid role. The user is not admitted.
- 1: Read Only
- 2: System Administrator
- 3: Security Officer

If the vendor-specific auth-role attribute is absent, but the standard service-type (Type 6) attribute is present, PTP 650 selects the role for the authenticated user according to service-type. The supported values of service-type are as follows:

- Login(1): Read Only
- Administrative(6): System Administrator
- NAS Prompt(7): Read Only

If the auth-role and service-type attributes are absent, PTP 650 selects the Read Only role.

The auth-role vendor-specific attribute is defined in Table 39.

Table 39 Definition of auth-role vendor-specific attribute

Field	Length	Value	Notes
Type	1	26	Vendor-specific attribute.
Length	1	12	Overall length of the attribute.
Vendor ID	4	17713	The same IANA code used for the SNMP enterprise MIB.
Vendor Type	1	1	auth-role
Vendor Length	1	4	Length of the attribute specific part.
Attribute-Specific	4	0..3	Integer type (32-bit unsigned). Supported values: invalid-role(0), readonly-role(1), system-admin-role(2), security-officer-role(3).

System threshold, output power and link loss

The following tables specify the system threshold (dBm), output power (dBm) and maximum link loss (dB) per channel bandwidth and modulation mode:

- Table 40 - 4.9 GHz - IP mode
- Table 41 - 4.9 GHz - TDM mode
- Table 42 - 5.4 GHz - IP mode
- Table 43 - 5.4 GHz - TDM mode
- Table 44 - 5.8 GHz - IP mode
- Table 45 - 5.8 GHz - TDM mode

Table 40 4.9 GHz - IP mode - threshold, power and link loss

Modulation mode	System threshold (dBm) per channel bandwidth		Output power (dBm)	Maximum link loss (dB) per channel bandwidth	
	10 MHz	20 MHz	All bands	10 MHz	20 MHz
BPSK 0.63 single	-95.7	-92.5	+27	168.7	165.5
QPSK 0.63 single	-90.0	-88.4	+26	163.0	161.4
QPSK 0.87 single	-86.9	-84.8	+26	159.9	157.8
16QAM 0.63 single	-84.7	-82.8	+25	156.7	154.8
16QAM 0.63 dual	-81.8	-79.1	+25	153.8	151.1
16QAM 0.87 single	-80.5	-78.1	+25	152.5	150.1
16QAM 0.87 dual	-77.6	-75.1	+25	149.6	147.1
64QAM 0.75 single	-77.3	-75.0	+24	148.3	146.0
64QAM 0.75 dual	-74.7	-72.1	+24	145.7	143.1
64QAM 0.92 single	-73.2	-70.7	+24	144.2	141.7
64QAM 0.92 dual	-70.2	-67.6	+24	141.2	138.6
256QAM 0.81 single	-69.9	-67.5	+23	138.9	136.5
256QAM 0.81 dual	-66.8	-64.1	+23	135.8	133.1

Table 41 4.9 GHz - TDM mode - threshold, power and link loss

Modulation mode	System threshold (dBm) per channel bandwidth		Output power (dBm)	Maximum link loss (dB) per channel bandwidth	
	10 MHz	20 MHz	All bands	10 MHz	20 MHz
BPSK 0.63 single	-92.5	-93.4	27	165.5	166.4
QPSK 0.63 single	-87.6	-86.1	26	160.6	159.1
QPSK 0.87 single	-84.2	-82.0	26	157.2	155.0
16QAM 0.63 single	-81.6	-79.7	25	153.6	151.7
16QAM 0.63 dual	-78.4	-76.2	25	150.4	148.2
16QAM 0.87 single	-77.4	-75.0	25	149.4	147.0
16QAM 0.87 dual	-74.4	-71.7	25	146.4	143.7
64QAM 0.75 single	-73.5	-71.3	24	144.5	142.3
64QAM 0.75 dual	-71.1	-68.3	24	142.1	139.3
64QAM 0.92 single	-69.6	-67.0	24	140.6	138.0
64QAM 0.92 dual	-66.9	-64.3	24	137.9	135.3
256QAM 0.81 single	-69.4	-67.2	23	138.4	136.2
256QAM 0.81 dual	-64.3	-63.2	23	133.3	132.2

Table 42 5.4 GHz - IP mode - threshold, power and link loss

Modulation mode	System threshold (dBm) per channel bandwidth				Output power (dBm)	Maximum link loss (dB) per channel bandwidth			
	10 MHz	20 MHz	40 MHz	45 MHz	All bands	10 MHz	20 MHz	40 MHz	45 MHz
BPSK 0.63 single	-96.3	-93.4	-90.7	-90.1	27	169.3	166.4	163.7	163.1
QPSK 0.63 single	-90.8	-88.8	-85.7	-85.2	26	163.8	161.8	158.7	158.2
QPSK 0.87 single	-87.2	-85.3	-82.0	-81.2	26	160.2	158.3	155.0	154.2
16QAM 0.63 single	-85.2	-83.2	-79.9	-79.3	25	157.2	155.2	151.9	151.3
16QAM 0.63 dual	-81.9	-79.6	-76.4	-76.2	25	153.9	151.6	148.4	148.2
16QAM 0.87 single	-81.0	-78.7	-75.4	-74.8	25	153.0	150.7	147.4	146.8
16QAM 0.87 dual	-77.9	-75.1	-72.0	-72.1	25	149.9	147.1	144.0	144.1
64QAM 0.75 single	-77.7	-75.7	-72.4	-71.7	24	148.7	146.7	143.4	142.7
64QAM 0.75 dual	-75.1	-72.1	-69.1	-69.1	24	146.1	143.1	140.1	140.1
64QAM 0.92 single	-73.7	-71.5	-68.3	-67.4	24	144.7	142.5	139.3	138.4
64 QAM 0.92 dual	-70.7	-67.9	-64.9	-64.5	24	141.7	138.9	135.9	135.5
256QAM 0.81 single	-70.5	-68.6	-65.4	-64.9	23	139.5	137.6	134.4	133.9
256QAM 0.81 dual	-67.7	-64.9	-61.8	-62.0	23	136.7	133.9	130.8	131.0

Table 43 5.4 GHz - TDM mode - threshold, power and link loss

Modulation mode	System threshold (dBm) per channel bandwidth				Output power (dBm)	Maximum link loss (dB) per channel bandwidth			
	10 MHz	20 MHz	40 MHz	45 MHz	All bands	10 MHz	20 MHz	40 MHz	45 MHz
BPSK 0.63 single	-96.4	-93.5	-90.3	-90.0	27	169.4	166.5	163.3	163.0
QPSK 0.63 single	-87.9	-86.4	-83.2	-82.8	26	160.9	159.4	156.2	155.8
QPSK 0.87 single	-84.8	-82.4	-79.1	-78.7	26	157.8	155.4	152.1	151.7
16QAM 0.63 single	-82.6	-80.0	-76.9	-76.4	25	154.6	152.0	148.9	148.4
16QAM 0.63 dual	-78.7	-76.3	-73.4	-73.0	25	150.7	148.3	145.4	145.0
16QAM 0.87 single	-78.2	-75.6	-72.3	-71.9	25	150.2	147.6	144.3	143.9
16QAM 0.87 dual	-74.8	-72.0	-69.0	-68.9	25	146.8	144.0	141.0	140.9
64QAM 0.75 single	-74.3	-72.0	-68.9	-68.5	24	145.3	143.0	139.9	139.5
64QAM 0.75 dual	-71.3	-68.6	-65.7	-65.6	24	142.3	139.6	136.7	136.6
64QAM 0.92 single	-70.1	-68.0	-65.0	-64.5	24	141.1	139.0	136.0	135.5
64 QAM 0.92 dual	-67.3	-64.6	-61.1	-61.6	24	138.3	135.6	132.1	132.6
256QAM 0.81 single	-70.5	-68.2	-65.0	-64.7	23	139.5	137.2	134.0	133.7
256QAM 0.81 dual	-66.9	-64.1	-61.3	-61.2	23	135.9	133.1	130.3	130.2

Table 44 5.8 GHz - IP mode - threshold, power and link loss

Modulation mode	System threshold (dBm) per channel bandwidth				Output power (dBm)	Maximum link loss (dB) per channel bandwidth			
	10 MHz	20 MHz	40 MHz	45 MHz	All bands	10 MHz	20 MHz	40 MHz	45 MHz
BPSK 0.63 single	-95.8	-92.9	-89.6	-89.4	27	168.8	165.9	162.6	162.4
QPSK 0.63 single	-90.3	-87.9	-85.3	-85.0	26	163.3	160.9	158.3	158.0
QPSK 0.87 single	-87.3	-84.5	-81.4	-81.0	26	160.3	157.5	154.4	154.0
16QAM 0.63 single	-85.2	-82.5	-79.2	-78.9	25	157.2	154.5	151.2	150.9
16QAM 0.63 dual	-81.4	-79.0	-75.7	-75.3	25	153.4	151.0	147.7	147.3
16QAM 0.87 single	-80.6	-77.8	-74.8	-74.6	25	152.6	149.8	146.8	146.6
16QAM 0.87 dual	-77.3	-74.4	-71.4	-71.1	25	149.3	146.4	143.4	143.1
64QAM 0.75 single	-77.3	-74.8	-71.7	-71.4	24	148.3	145.8	142.7	142.4
64QAM 0.75 dual	-74.5	-71.5	-68.5	-68.2	24	145.5	142.5	139.5	139.2
64QAM 0.92 single	-73.4	-70.7	-67.7	-67.5	24	144.4	141.7	138.7	138.5
64 QAM 0.92 dual	-70.0	-67.1	-64.2	-64.0	24	141.0	138.1	135.2	135.0
256QAM 0.81 single	-70.1	-67.4	-64.8	-64.4	23	139.1	136.4	133.8	133.4
256QAM 0.81 dual	-67.0	-64.0	-61.2	-60.8	23	136.0	133.0	130.2	129.8

Table 45 5.8 GHz - TDM mode - threshold, power and link loss

Modulation mode	System threshold (dBm) per channel bandwidth				Output power (dBm)	Maximum link loss (dB) per channel bandwidth			
	10 MHz	20 MHz	40 MHz	45 MHz	All bands	10 MHz	20 MHz	40 MHz	45 MHz
BPSK 0.63 single	-96.4	-92.7	-90.2	-89.6	27	169.4	165.7	163.2	162.6
QPSK 0.63 single	-87.5	-86.0	-83.2	-82.7	26	160.5	159.0	156.2	155.7
QPSK 0.87 single	-84.3	-81.9	-79.0	-78.4	26	157.3	154.9	152.0	151.4
16QAM 0.63 single	-81.9	-79.6	-76.6	-76.2	25	153.9	151.6	148.6	148.2
16QAM 0.63 dual	-78.2	-76.0	-73.0	-72.6	25	150.2	148.0	145.0	144.6
16QAM 0.87 single	-77.7	-75.0	-72.1	-71.6	25	149.7	147.0	144.1	143.6
16QAM 0.87 dual	-74.0	-71.4	-69.0	-68.2	25	146.0	143.4	141.0	140.2
64QAM 0.75 single	-73.8	-71.4	-68.8	-68.2	24	144.8	142.4	139.8	139.2
64QAM 0.75 dual	-70.7	-68.0	-65.7	-64.9	24	141.7	139.0	136.7	135.9
64QAM 0.92 single	-69.8	-67.2	-64.8	-64.2	24	140.8	138.2	135.8	135.2
64 QAM 0.92 dual	-66.7	-63.8	-61.2	-60.3	24	137.7	134.8	132.2	131.3
256QAM 0.81 single	-70.0	-67.3	-64.7	-64.3	23	139.0	136.3	133.7	133.3
256QAM 0.81 dual	-66.2	-63.5	-61.1	-60.3	23	135.2	132.5	130.1	129.3

Data throughput capacity tables

Use the following tables to look up the data throughput rates (Mbits/s) that are achieved when two PTP 650 ODUs are linked and the link distance (range) is 0 km:

PTP 650 variant	Link symmetry	Link optimization	Table
Full	1:1	IP	Table 46
		TDM	Table 47
	2:1	IP	Table 48
		TDM	Table 49
	Adaptive	IP	Table 50
Mid	1:1	IP	Table 51
		TDM	Table 52
	2:1	IP	Table 53
		TDM	Table 54
	Adaptive	IP	Table 55
Lite	1:1	IP	Table 56
		TDM	Table 57
	2:1	IP	Table 58
		TDM	Table 59
	Adaptive	IP	Table 60

Use the following range adjustment graphs to look up the link range and find the throughput factor that must be applied to adjust the 0 km data throughput rates:

Link symmetry	Link optimization	Bandwidth			
		45 MHz	40 MHz	20 MHz	10 MHz
1:1	IP	Figure 33	Figure 34	Figure 35	Figure 36
	TDM	Figure 37	Figure 38	Figure 39	Figure 40
2:1	IP	Figure 41	Figure 42	Figure 43	Figure 44
	TDM	Figure 45	Figure 46	Figure 47	Figure 48
Adaptive	IP	Figure 49	Figure 50	Figure 51	Figure 52

Throughput for link symmetry 2:1 is the same as 1:2, but the Tx and Rx data rates are swapped.

Table 46 Throughput at zero link range (Mbit/s), Full, symmetry 1:1, optimization IP

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	226.1	226.1	452.2	206.3	206.3	412.6
64QAM 0.92 dual	190.5	190.5	381.0	173.8	173.8	347.6
64QAM 0.75 dual	155.7	155.7	311.3	142.0	142.0	284.1
16QAM 0.87 dual	121.1	121.1	242.2	110.5	110.5	221.0
16QAM 0.63 dual	87.1	87.1	174.1	79.4	79.4	158.9
256QAM 0.81 single	113.0	113.0	226.1	103.1	103.1	206.3
64QAM 0.92 single	95.2	95.2	190.5	86.9	86.9	173.8
64QAM 0.75 single	77.8	77.8	155.7	71.0	71.0	142.0
16QAM 0.87 single	60.5	60.5	121.1	55.2	55.2	110.5
16QAM 0.63 single	43.5	43.5	87.0	39.7	39.7	79.4
QPSK 0.87 single	30.3	30.3	60.5	27.6	27.6	55.2
QPSK 0.63 single	21.8	21.8	43.5	19.9	19.9	39.7
BPSK 0.63 single	10.9	10.9	21.8	9.9	9.9	19.9
Modulation mode	**20 MHz (Tx/Rx/Aggregate)**			**10 MHz (Tx/Rx/Aggregate)**		
256QAM 0.81 dual	100.0	100.0	200.1	50.1	50.1	100.2
64QAM 0.92 dual	84.3	84.3	168.6	42.2	42.2	84.4
64QAM 0.75 dual	68.9	68.9	137.8	34.5	34.5	69.0
16QAM 0.87 dual	53.6	53.6	107.2	26.8	26.8	53.7
16QAM 0.63 dual	38.5	38.5	77.0	19.3	19.3	38.6
256QAM 0.81 single	50.0	50.0	100.0	25.0	25.0	50.1
64QAM 0.92 single	42.1	42.1	84.3	21.1	21.1	42.2
64QAM 0.75 single	34.4	34.4	68.9	17.2	17.2	34.5
16QAM 0.87 single	26.8	26.8	53.6	13.4	13.4	26.8
16QAM 0.63 single	19.3	19.3	38.5	9.6	9.6	19.3
QPSK 0.87 single	13.4	13.4	26.8	6.7	6.7	13.4
QPSK 0.63 single	9.6	9.6	19.3	4.8	4.8	9.6
BPSK 0.63 single	4.8	4.8	9.6	2.4	2.4	4.8

Tx/Rx/Aggregate columns contain the transmit, receive and aggregate data rates per bandwidth.

Table 47 Throughput at zero link range (Mbit/s), Full, symmetry 1:1, optimization TDM

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	202.1	202.1	404.1	186.1	186.1	372.1
64QAM 0.92 dual	170.2	170.2	340.5	156.8	156.8	313.5
64QAM 0.75 dual	139.1	139.1	278.2	128.1	128.1	256.2
16QAM 0.87 dual	108.2	108.2	216.5	99.7	99.7	199.3
16QAM 0.63 dual	77.8	77.8	155.6	71.6	71.6	143.3
256QAM 0.81 single	101.0	101.0	202.1	93.0	93.0	186.1
64QAM 0.92 single	85.1	85.1	170.2	78.4	78.4	156.8
64QAM 0.75 single	69.6	69.6	139.1	64.0	64.0	128.1
16QAM 0.87 single	54.1	54.1	108.2	49.8	49.8	99.7
16QAM 0.63 single	38.9	38.9	77.8	35.8	35.8	71.6
QPSK 0.87 single	27.1	27.1	54.1	24.9	24.9	49.8
QPSK 0.63 single	19.4	19.4	38.9	17.9	17.9	35.8
BPSK 0.63 single	9.7	9.7	19.4	9.0	9.0	17.9
Modulation mode	**20 MHz (Tx/Rx/Aggregate)**			**10 MHz (Tx/Rx/Aggregate)**		
256QAM 0.81 dual	96.0	96.0	192.0	49.1	49.1	98.2
64QAM 0.92 dual	80.9	80.9	161.7	41.4	41.4	82.8
64QAM 0.75 dual	66.1	66.1	132.2	33.8	33.8	67.6
16QAM 0.87 dual	51.4	51.4	102.8	26.3	26.3	52.6
16QAM 0.63 dual	37.0	37.0	73.9	18.9	18.9	37.8
256QAM 0.81 single	48.0	48.0	96.0	24.6	24.6	49.1
64QAM 0.92 single	40.4	40.4	80.9	20.7	20.7	41.4
64QAM 0.75 single	33.0	33.0	66.1	16.9	16.9	33.8
16QAM 0.87 single	25.7	25.7	51.4	13.2	13.2	26.3
16QAM 0.63 single	18.5	18.5	37.0	9.5	9.5	18.9
QPSK 0.87 single	12.8	12.8	25.7	6.6	6.6	13.1
QPSK 0.63 single	9.2	9.2	18.5	4.7	4.7	9.5
BPSK 0.63 single	4.6	4.6	9.2	2.4	2.4	4.7

Tx/Rx/Aggregate columns contain the transmit, receive and aggregate data rates per bandwidth.

Table 48 Throughput at zero link range (Mbit/s), Full, symmetry 2:1, optimization IP

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	299.7	149.9	449.6	273.6	136.8	410.5
64QAM 0.92 dual	252.5	126.3	378.8	230.5	115.3	345.8
64QAM 0.75 dual	206.4	103.2	309.6	188.4	94.2	282.6
16QAM 0.87 dual	160.6	80.3	240.8	146.6	73.3	219.8
16QAM 0.63 dual	115.4	57.7	173.1	105.4	52.7	158.0
256QAM 0.81 single	149.9	74.9	224.8	136.8	68.4	205.2
64QAM 0.92 single	126.3	63.1	189.4	115.3	57.6	172.9
64QAM 0.75 single	103.2	51.6	154.8	94.2	47.1	141.3
16QAM 0.87 single	80.3	40.1	120.4	73.3	36.6	109.9
16QAM 0.63 single	57.7	28.9	86.6	52.7	26.3	79.0
QPSK 0.87 single	40.1	20.1	60.2	36.6	18.3	55.0
QPSK 0.63 single	28.9	14.4	43.3	26.3	13.2	39.5
BPSK 0.63 single	14.4	7.2	21.6	13.2	6.6	19.7
Modulation mode	**20 MHz (Tx/Rx/Aggregate)**			**10 MHz (Tx/Rx/Aggregate)**		
256QAM 0.81 dual	133.4	66.7	200.1	66.3	33.2	99.5
64QAM 0.92 dual	112.4	56.2	168.6	55.9	27.9	83.8
64QAM 0.75 dual	91.8	45.9	137.8	45.7	22.8	68.5
16QAM 0.87 dual	71.5	35.7	107.2	35.5	17.8	53.3
16QAM 0.63 dual	51.4	25.7	77.0	25.5	12.8	38.3
256QAM 0.81 single	66.7	33.3	100.0	33.2	16.6	49.8
64QAM 0.92 single	56.2	28.1	84.3	27.9	14.0	41.9
64QAM 0.75 single	45.9	23.0	68.9	22.8	11.4	34.3
16QAM 0.87 single	35.7	17.9	53.6	17.8	8.9	26.6
16QAM 0.63 single	25.7	12.8	38.5	12.8	6.4	19.2
QPSK 0.87 single	17.9	8.9	26.8	8.9	4.4	13.3
QPSK 0.63 single	12.8	6.4	19.3	6.4	3.2	9.6
BPSK 0.63 single	6.4	3.2	9.6	3.2	1.6	4.8

Tx/Rx/Aggregate columns contain the transmit, receive and aggregate data rates per bandwidth.

Table 49 Throughput at zero link range (Mbit/s), Full, symmetry 2:1, optimization TDM

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	280.8	140.4	421.2	257.7	128.9	386.6
64QAM 0.92 dual	236.6	118.3	354.8	217.1	108.6	325.7
64QAM 0.75 dual	193.3	96.7	290.0	177.4	88.7	266.1
16QAM 0.87 dual	150.4	75.2	225.6	138.0	69.0	207.1
16QAM 0.63 dual	108.1	54.1	162.2	99.2	49.6	148.8
256QAM 0.81 single	140.4	70.2	210.6	128.9	64.4	193.3
64QAM 0.92 single	118.3	59.1	177.4	108.6	54.3	162.8
64QAM 0.75 single	96.7	48.3	145.0	88.7	44.4	133.1
16QAM 0.87 single	75.2	37.6	112.8	69.0	34.5	103.5
16QAM 0.63 single	54.1	27.0	81.1	49.6	24.8	74.4
QPSK 0.87 single	37.6	18.8	56.4	34.5	17.3	51.8
QPSK 0.63 single	27.0	13.5	40.5	24.8	12.4	37.2
BPSK 0.63 single	13.5	6.8	20.3	12.4	6.2	18.6
Modulation mode	**20 MHz (Tx/Rx/Aggregate)**			**10 MHz (Tx/Rx/Aggregate)**		
256QAM 0.81 dual	130.6	65.3	195.9	66.3	33.2	99.5
64QAM 0.92 dual	110.1	55.0	165.1	55.9	27.9	83.8
64QAM 0.75 dual	89.9	45.0	134.9	45.7	22.8	68.5
16QAM 0.87 dual	70.0	35.0	104.9	35.5	17.8	53.3
16QAM 0.63 dual	50.3	25.1	75.4	25.5	12.8	38.3
256QAM 0.81 single	65.3	32.7	98.0	33.2	16.6	49.8
64QAM 0.92 single	55.0	27.5	82.5	27.9	14.0	41.9
64QAM 0.75 single	45.0	22.5	67.4	22.8	11.4	34.3
16QAM 0.87 single	35.0	17.5	52.5	17.8	8.9	26.6
16QAM 0.63 single	25.1	12.6	37.7	12.8	6.4	19.2
QPSK 0.87 single	17.5	8.7	26.2	8.9	4.4	13.3
QPSK 0.63 single	12.6	6.3	18.9	6.4	3.2	9.6
BPSK 0.63 single	6.3	3.1	9.4	3.2	1.6	4.8

Tx/Rx/Aggregate columns contain the transmit, receive and aggregate data rates per bandwidth.

Table 50 Throughput at zero link range (Mbit/s), Full, symmetry adaptive, optimization IP

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	407.9	40.8	448.7	367.9	40.9	408.8
64QAM 0.92 dual	343.7	34.4	378.0	310.0	34.4	344.4
64QAM 0.75 dual	280.8	28.1	308.9	253.3	28.1	281.4
16QAM 0.87 dual	218.5	21.8	240.3	197.1	21.9	218.9
16QAM 0.63 dual	157.1	15.7	172.8	141.7	15.7	157.4
256QAM 0.81 single	204.0	20.4	224.3	183.9	20.4	204.4
64QAM 0.92 single	171.8	17.2	189.0	155.0	17.2	172.2
64QAM 0.75 single	140.4	14.0	154.5	126.6	14.1	140.7
16QAM 0.87 single	109.2	10.9	120.2	98.5	10.9	109.5
16QAM 0.63 single	78.5	7.9	86.4	70.8	7.9	78.7
QPSK 0.87 single	54.6	5.5	60.1	49.3	5.5	54.7
QPSK 0.63 single	39.3	3.9	43.2	35.4	3.9	39.3
BPSK 0.63 single	19.6	2.0	21.6	17.7	2.0	19.7
Modulation mode	**20 MHz (Tx/Rx/Aggregate)**			**10 MHz (Tx/Rx/Aggregate)**		
256QAM 0.81 dual	159.4	39.8	199.2	66.3	33.2	99.5
64QAM 0.92 dual	134.3	33.6	167.9	55.9	27.9	83.8
64QAM 0.75 dual	109.7	27.4	137.2	45.7	22.8	68.5
16QAM 0.87 dual	85.4	21.3	106.7	35.5	17.8	53.3
16QAM 0.63 dual	61.4	15.3	76.7	25.5	12.8	38.3
256QAM 0.81 single	79.7	19.9	99.6	33.2	16.6	49.8
64QAM 0.92 single	67.1	16.8	83.9	27.9	14.0	41.9
64QAM 0.75 single	54.9	13.7	68.6	22.8	11.4	34.3
16QAM 0.87 single	42.7	10.7	53.4	17.8	8.9	26.6
16QAM 0.63 single	30.7	7.7	38.4	12.8	6.4	19.2
QPSK 0.87 single	21.3	5.3	26.7	8.9	4.4	13.3
QPSK 0.63 single	15.3	3.8	19.2	6.4	3.2	9.6
BPSK 0.63 single	7.7	1.9	9.6	3.2	1.6	4.8

Tx/Rx/Aggregate columns contain the transmit, receive and aggregate data rates per bandwidth.

Table 51 Throughput at zero link range (Mbit/s), Mid, symmetry 1:1, optimization IP

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	127.0	127.0	254.0	116.0	116.0	232.0
64QAM 0.92 dual	107.0	107.0	214.0	97.0	97.0	194.0
64QAM 0.75 dual	87.0	87.0	174.0	80.0	80.0	160.0
16QAM 0.87 dual	68.0	68.0	136.0	62.0	62.0	124.0
16QAM 0.63 dual	49.0	49.0	98.0	44.0	44.0	88.0
256QAM 0.81 single	63.0	63.0	126.0	58.0	58.0	116.0
64QAM 0.92 single	53.0	53.0	106.0	49.0	49.0	98.0
64QAM 0.75 single	44.0	44.0	88.0	40.0	40.0	80.0
16QAM 0.87 single	34.0	34.0	68.0	31.0	31.0	62.0
16QAM 0.63 single	24.0	24.0	48.0	22.0	22.0	44.0
QPSK 0.87 single	17.0	17.0	34.0	15.0	15.0	30.0
QPSK 0.63 single	12.0	12.0	24.0	11.0	11.0	22.0
BPSK 0.63 single	6.0	6.0	12.0	6.0	6.0	12.0
Modulation mode	**20 MHz (Tx/Rx/Aggregate)**			**10 MHz (Tx/Rx/Aggregate)**		
256QAM 0.81 dual	56.0	56.0	112.0	28.0	28.0	56.0
64QAM 0.92 dual	47.0	47.0	94.0	24.0	24.0	48.0
64QAM 0.75 dual	39.0	39.0	78.0	19.0	19.0	38.0
16QAM 0.87 dual	30.0	30.0	60.0	15.0	15.0	30.0
16QAM 0.63 dual	22.0	22.0	44.0	11.0	11.0	22.0
256QAM 0.81 single	28.0	28.0	56.0	14.0	14.0	28.0
64QAM 0.92 single	24.0	24.0	48.0	12.0	12.0	24.0
64QAM 0.75 single	19.0	19.0	38.0	10.0	10.0	20.0
16QAM 0.87 single	15.0	15.0	30.0	8.0	8.0	16.0
16QAM 0.63 single	11.0	11.0	22.0	5.0	5.0	10.0
QPSK 0.87 single	8.0	8.0	16.0	5.0	5.0	10.0
QPSK 0.63 single	5.0	5.0	10.0	4.8	4.8	9.6
BPSK 0.63 single	4.8	4.8	9.6	2.4	2.4	4.8

Tx/Rx/Aggregate columns contain the transmit, receive and aggregate data rates per bandwidth.

Table 52 Throughput at zero link range (Mbit/s), Mid, symmetry 1:1, optimization TDM

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	113.0	113.0	226.0	104.0	104.0	208.0
64QAM 0.92 dual	95.0	95.0	190.0	88.0	88.0	176.0
64QAM 0.75 dual	78.0	78.0	156.0	72.0	72.0	144.0
16QAM 0.87 dual	61.0	61.0	122.0	56.0	56.0	112.0
16QAM 0.63 dual	44.0	44.0	88.0	40.0	40.0	80.0
256QAM 0.81 single	57.0	57.0	114.0	52.0	52.0	104.0
64QAM 0.92 single	48.0	48.0	96.0	44.0	44.0	88.0
64QAM 0.75 single	39.0	39.0	78.0	36.0	36.0	72.0
16QAM 0.87 single	30.0	30.0	60.0	28.0	28.0	56.0
16QAM 0.63 single	22.0	22.0	44.0	20.0	20.0	40.0
QPSK 0.87 single	15.0	15.0	30.0	14.0	14.0	28.0
QPSK 0.63 single	11.0	11.0	22.0	10.0	10.0	20.0
BPSK 0.63 single	5.0	5.0	10.0	5.0	5.0	10.0
Modulation mode	**20 MHz (Tx/Rx/Aggregate)**			**10 MHz (Tx/Rx/Aggregate)**		
256QAM 0.81 dual	54.0	54.0	108.0	28.0	28.0	56.0
64QAM 0.92 dual	45.0	45.0	90.0	23.0	23.0	46.0
64QAM 0.75 dual	37.0	37.0	74.0	19.0	19.0	38.0
16QAM 0.87 dual	29.0	29.0	58.0	15.0	15.0	30.0
16QAM 0.63 dual	21.0	21.0	42.0	11.0	11.0	22.0
256QAM 0.81 single	27.0	27.0	54.0	14.0	14.0	28.0
64QAM 0.92 single	23.0	23.0	46.0	12.0	12.0	24.0
64QAM 0.75 single	19.0	19.0	38.0	9.0	9.0	18.0
16QAM 0.87 single	14.0	14.0	28.0	7.0	7.0	14.0
16QAM 0.63 single	10.0	10.0	20.0	5.0	5.0	10.0
QPSK 0.87 single	7.0	7.0	14.0	5.0	5.0	10.0
QPSK 0.63 single	5.0	5.0	10.0	4.7	4.7	9.5
BPSK 0.63 single	4.6	4.6	9.2	2.4	2.4	4.7

Tx/Rx/Aggregate columns contain the transmit, receive and aggregate data rates per bandwidth.

Table 53 Throughput at zero link range (Mbit/s), Mid, symmetry 2:1, optimization IP

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	168.0	84.0	252.0	153.0	77.0	230.0
64QAM 0.92 dual	141.0	71.0	212.0	129.0	65.0	194.0
64QAM 0.75 dual	116.0	58.0	174.0	106.0	53.0	159.0
16QAM 0.87 dual	90.0	45.0	135.0	82.0	41.0	123.0
16QAM 0.63 dual	65.0	32.0	97.0	59.0	30.0	89.0
256QAM 0.81 single	84.0	42.0	126.0	77.0	38.0	115.0
64QAM 0.92 single	71.0	35.0	106.0	65.0	32.0	97.0
64QAM 0.75 single	58.0	29.0	87.0	53.0	26.0	79.0
16QAM 0.87 single	45.0	22.0	67.0	41.0	21.0	62.0
16QAM 0.63 single	32.0	16.0	48.0	30.0	15.0	45.0
QPSK 0.87 single	22.0	11.0	33.0	21.0	10.0	31.0
QPSK 0.63 single	16.0	8.0	24.0	15.0	7.0	22.0
BPSK 0.63 single	8.0	5.0	13.0	7.0	5.0	12.0
Modulation mode	**20 MHz (Tx/Rx/Aggregate)**			**10 MHz (Tx/Rx/Aggregate)**		
256QAM 0.81 dual	75.0	37.0	112.0	37.0	19.0	56.0
64QAM 0.92 dual	63.0	31.0	94.0	31.0	16.0	47.0
64QAM 0.75 dual	51.0	26.0	77.0	26.0	13.0	39.0
16QAM 0.87 dual	40.0	20.0	60.0	20.0	10.0	30.0
16QAM 0.63 dual	29.0	14.0	43.0	14.0	7.0	21.0
256QAM 0.81 single	37.0	19.0	56.0	19.0	9.0	28.0
64QAM 0.92 single	31.0	16.0	47.0	16.0	8.0	24.0
64QAM 0.75 single	26.0	13.0	39.0	13.0	6.0	19.0
16QAM 0.87 single	20.0	10.0	30.0	10.0	5.0	15.0
16QAM 0.63 single	14.0	7.0	21.0	7.0	5.0	12.0
QPSK 0.87 single	10.0	5.0	15.0	5.0	4.4	9.4
QPSK 0.63 single	7.0	5.0	12.0	5.0	3.2	8.2
BPSK 0.63 single	5.0	3.2	8.2	3.2	1.6	4.8

Tx/Rx/Aggregate columns contain the transmit, receive and aggregate data rates per bandwidth.

Table 54 Throughput at zero link range (Mbit/s), Mid, symmetry 2:1, optimization TDM

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	157.0	79.0	236.0	144.0	72.0	216.0
64QAM 0.92 dual	132.0	66.0	198.0	122.0	61.0	183.0
64QAM 0.75 dual	108.0	54.0	162.0	99.0	50.0	149.0
16QAM 0.87 dual	84.0	42.0	126.0	77.0	39.0	116.0
16QAM 0.63 dual	61.0	30.0	91.0	56.0	28.0	84.0
256QAM 0.81 single	79.0	39.0	118.0	72.0	36.0	108.0
64QAM 0.92 single	66.0	33.0	99.0	61.0	30.0	91.0
64QAM 0.75 single	54.0	27.0	81.0	50.0	25.0	75.0
16QAM 0.87 single	42.0	21.0	63.0	39.0	19.0	58.0
16QAM 0.63 single	30.0	15.0	45.0	28.0	14.0	42.0
QPSK 0.87 single	21.0	11.0	32.0	19.0	10.0	29.0
QPSK 0.63 single	15.0	8.0	23.0	14.0	7.0	21.0
BPSK 0.63 single	8.0	5.0	13.0	7.0	5.0	12.0
Modulation mode	**20 MHz (Tx/Rx/Aggregate)**			**10 MHz (Tx/Rx/Aggregate)**		
256QAM 0.81 dual	73.0	37.0	110.0	37.0	19.0	56.0
64QAM 0.92 dual	62.0	31.0	93.0	31.0	16.0	47.0
64QAM 0.75 dual	50.0	25.0	75.0	26.0	13.0	39.0
16QAM 0.87 dual	39.0	20.0	59.0	20.0	10.0	30.0
16QAM 0.63 dual	28.0	14.0	42.0	14.0	7.0	21.0
256QAM 0.81 single	37.0	18.0	55.0	19.0	9.0	28.0
64QAM 0.92 single	31.0	15.0	46.0	16.0	8.0	24.0
64QAM 0.75 single	25.0	13.0	38.0	13.0	6.0	19.0
16QAM 0.87 single	20.0	10.0	30.0	10.0	5.0	15.0
16QAM 0.63 single	14.0	7.0	21.0	7.0	5.0	12.0
QPSK 0.87 single	10.0	5.0	15.0	5.0	4.4	9.4
QPSK 0.63 single	7.0	5.0	12.0	5.0	3.2	8.2
BPSK 0.63 single	5.0	3.1	8.1	3.2	1.6	4.8

Tx/Rx/Aggregate columns contain the transmit, receive and aggregate data rates per bandwidth.

Table 55 Throughput at zero link range (Mbit/s), Mid, symmetry adaptive, optimization IP

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	228.0	23.0	251.0	206.0	23.0	229.0
64QAM 0.92 dual	192.0	19.0	211.0	174.0	19.0	193.0
64QAM 0.75 dual	157.0	16.0	173.0	142.0	16.0	158.0
16QAM 0.87 dual	122.0	12.0	134.0	110.0	12.0	122.0
16QAM 0.63 dual	88.0	9.0	97.0	79.0	9.0	88.0
256QAM 0.81 single	114.0	11.0	125.0	103.0	11.0	114.0
64QAM 0.92 single	96.0	10.0	106.0	87.0	10.0	97.0
64QAM 0.75 single	79.0	8.0	87.0	71.0	8.0	79.0
16QAM 0.87 single	61.0	6.0	67.0	55.0	6.0	61.0
16QAM 0.63 single	44.0	5.0	49.0	40.0	5.0	45.0
QPSK 0.87 single	31.0	5.0	36.0	28.0	5.0	33.0
QPSK 0.63 single	22.0	3.9	25.9	20.0	3.9	23.9
BPSK 0.63 single	11.0	2.0	13.0	10.0	2.0	12.0
Modulation mode	**20 MHz (Tx/Rx/Aggregate)**			**10 MHz (Tx/Rx/Aggregate)**		
256QAM 0.81 dual	89.0	22.0	111.0	37.0	19.0	56.0
64QAM 0.92 dual	75.0	19.0	94.0	31.0	16.0	47.0
64QAM 0.75 dual	61.0	15.0	76.0	26.0	13.0	39.0
16QAM 0.87 dual	48.0	12.0	60.0	20.0	10.0	30.0
16QAM 0.63 dual	34.0	9.0	43.0	14.0	7.0	21.0
256QAM 0.81 single	45.0	11.0	56.0	19.0	9.0	28.0
64QAM 0.92 single	38.0	9.0	47.0	16.0	8.0	24.0
64QAM 0.75 single	31.0	8.0	39.0	13.0	6.0	19.0
16QAM 0.87 single	24.0	6.0	30.0	10.0	5.0	15.0
16QAM 0.63 single	17.0	5.0	22.0	7.0	5.0	12.0
QPSK 0.87 single	12.0	5.0	17.0	5.0	4.4	9.4
QPSK 0.63 single	9.0	3.8	12.8	5.0	3.2	8.2
BPSK 0.63 single	5.0	1.9	6.9	3.2	1.6	4.8

Tx/Rx/Aggregate columns contain the transmit, receive and aggregate data rates per bandwidth.

Table 56 Throughput at zero link range (Mbit/s), Lite, symmetry 1:1, optimization IP

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	63.0	63.0	126.0	58.0	58.0	116.0
64QAM 0.92 dual	53.0	53.0	106.0	49.0	49.0	98.0
64QAM 0.75 dual	44.0	44.0	88.0	40.0	40.0	80.0
16QAM 0.87 dual	34.0	34.0	68.0	31.0	31.0	62.0
16QAM 0.63 dual	24.0	24.0	48.0	22.0	22.0	44.0
256QAM 0.81 single	32.0	32.0	64.0	29.0	29.0	58.0
64QAM 0.92 single	27.0	27.0	54.0	24.0	24.0	48.0
64QAM 0.75 single	22.0	22.0	44.0	20.0	20.0	40.0
16QAM 0.87 single	17.0	17.0	34.0	15.0	15.0	30.0
16QAM 0.63 single	12.0	12.0	24.0	11.0	11.0	22.0
QPSK 0.87 single	8.0	8.0	16.0	8.0	8.0	16.0
QPSK 0.63 single	6.0	6.0	12.0	6.0	6.0	12.0
BPSK 0.63 single	5.0	5.0	10.0	5.0	5.0	10.0
Modulation mode	**20 MHz (Tx/Rx/Aggregate)**			**10 MHz (Tx/Rx/Aggregate)**		
256QAM 0.81 dual	28.0	28.0	56.0	14.0	14.0	28.0
64QAM 0.92 dual	24.0	24.0	48.0	12.0	12.0	24.0
64QAM 0.75 dual	19.0	19.0	38.0	10.0	10.0	20.0
16QAM 0.87 dual	15.0	15.0	30.0	8.0	8.0	16.0
16QAM 0.63 dual	11.0	11.0	22.0	5.0	5.0	10.0
256QAM 0.81 single	14.0	14.0	28.0	7.0	7.0	14.0
64QAM 0.92 single	12.0	12.0	24.0	6.0	6.0	12.0
64QAM 0.75 single	10.0	10.0	20.0	5.0	5.0	10.0
16QAM 0.87 single	8.0	8.0	16.0	5.0	5.0	10.0
16QAM 0.63 single	5.0	5.0	10.0	5.0	5.0	10.0
QPSK 0.87 single	5.0	5.0	10.0	5.0	5.0	10.0
QPSK 0.63 single	5.0	5.0	10.0	4.8	4.8	9.6
BPSK 0.63 single	4.8	4.8	9.6	2.4	2.4	4.8

Tx/Rx/Aggregate columns contain the transmit, receive and aggregate data rates per bandwidth.

Table 57 Throughput at zero link range (Mbit/s), Lite, symmetry 1:1, optimization TDM

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	57.0	57.0	114.0	52.0	52.0	104.0
64QAM 0.92 dual	48.0	48.0	96.0	44.0	44.0	88.0
64QAM 0.75 dual	39.0	39.0	78.0	36.0	36.0	72.0
16QAM 0.87 dual	30.0	30.0	60.0	28.0	28.0	56.0
16QAM 0.63 dual	22.0	22.0	44.0	20.0	20.0	40.0
256QAM 0.81 single	28.0	28.0	56.0	26.0	26.0	52.0
64QAM 0.92 single	24.0	24.0	48.0	22.0	22.0	44.0
64QAM 0.75 single	19.0	19.0	38.0	18.0	18.0	36.0
16QAM 0.87 single	15.0	15.0	30.0	14.0	14.0	28.0
16QAM 0.63 single	11.0	11.0	22.0	10.0	10.0	20.0
QPSK 0.87 single	8.0	8.0	16.0	7.0	7.0	14.0
QPSK 0.63 single	5.0	5.0	10.0	5.0	5.0	10.0
BPSK 0.63 single	5.0	5.0	10.0	5.0	5.0	10.0
Modulation mode	**20 MHz (Tx/Rx/Aggregate)**			**10 MHz (Tx/Rx/Aggregate)**		
256QAM 0.81 dual	27.0	27.0	54.0	14.0	14.0	28.0
64QAM 0.92 dual	23.0	23.0	46.0	12.0	12.0	24.0
64QAM 0.75 dual	19.0	19.0	38.0	9.0	9.0	18.0
16QAM 0.87 dual	14.0	14.0	28.0	7.0	7.0	14.0
16QAM 0.63 dual	10.0	10.0	20.0	5.0	5.0	10.0
256QAM 0.81 single	13.0	13.0	26.0	7.0	7.0	14.0
64QAM 0.92 single	11.0	11.0	22.0	6.0	6.0	12.0
64QAM 0.75 single	9.0	9.0	18.0	5.0	5.0	10.0
16QAM 0.87 single	7.0	7.0	14.0	5.0	5.0	10.0
16QAM 0.63 single	5.0	5.0	10.0	5.0	5.0	10.0
QPSK 0.87 single	5.0	5.0	10.0	5.0	5.0	10.0
QPSK 0.63 single	5.0	5.0	10.0	4.7	4.7	9.5
BPSK 0.63 single	4.6	4.6	9.2	2.4	2.4	4.7

Tx/Rx/Aggregate columns contain the transmit, receive and aggregate data rates per bandwidth.

Table 58 Throughput at zero link range (Mbit/s), Lite, symmetry 2:1, optimization IP

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	84.0	42.0	126.0	77.0	38.0	115.0
64QAM 0.92 dual	71.0	35.0	106.0	65.0	32.0	97.0
64QAM 0.75 dual	58.0	29.0	87.0	53.0	26.0	79.0
16QAM 0.87 dual	45.0	22.0	67.0	41.0	21.0	62.0
16QAM 0.63 dual	32.0	16.0	48.0	30.0	15.0	45.0
256QAM 0.81 single	42.0	21.0	63.0	38.0	19.0	57.0
64QAM 0.92 single	35.0	18.0	53.0	32.0	16.0	48.0
64QAM 0.75 single	29.0	14.0	43.0	26.0	13.0	39.0
16QAM 0.87 single	22.0	11.0	33.0	21.0	10.0	31.0
16QAM 0.63 single	16.0	8.0	24.0	15.0	7.0	22.0
QPSK 0.87 single	11.0	6.0	17.0	10.0	5.0	15.0
QPSK 0.63 single	8.0	5.0	13.0	7.0	5.0	12.0
BPSK 0.63 single	5.0	5.0	10.0	5.0	5.0	10.0
Modulation mode	**20 MHz (Tx/Rx/Aggregate)**			**10 MHz (Tx/Rx/Aggregate)**		
256QAM 0.81 dual	37.0	19.0	56.0	19.0	9.0	28.0
64QAM 0.92 dual	31.0	16.0	47.0	16.0	8.0	24.0
64QAM 0.75 dual	26.0	13.0	39.0	13.0	6.0	19.0
16QAM 0.87 dual	20.0	10.0	30.0	10.0	5.0	15.0
16QAM 0.63 dual	14.0	7.0	21.0	7.0	5.0	12.0
256QAM 0.81 single	19.0	9.0	28.0	9.0	5.0	14.0
64QAM 0.92 single	16.0	8.0	24.0	8.0	5.0	13.0
64QAM 0.75 single	13.0	6.0	19.0	6.0	5.0	11.0
16QAM 0.87 single	10.0	5.0	15.0	5.0	5.0	10.0
16QAM 0.63 single	7.0	5.0	12.0	5.0	5.0	10.0
QPSK 0.87 single	5.0	5.0	10.0	5.0	4.4	9.4
QPSK 0.63 single	5.0	5.0	10.0	5.0	3.2	8.2
BPSK 0.63 single	5.0	3.2	8.2	3.2	1.6	4.8

Tx/Rx/Aggregate columns contain the transmit, receive and aggregate data rates per bandwidth.

Table 59 Throughput at zero link range (Mbit/s), Lite, symmetry 2:1, optimization TDM

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	79.0	39.0	118.0	72.0	36.0	108.0
64QAM 0.92 dual	66.0	33.0	99.0	61.0	30.0	91.0
64QAM 0.75 dual	54.0	27.0	81.0	50.0	25.0	75.0
16QAM 0.87 dual	42.0	21.0	63.0	39.0	19.0	58.0
16QAM 0.63 dual	30.0	15.0	45.0	28.0	14.0	42.0
256QAM 0.81 single	39.0	20.0	59.0	36.0	18.0	54.0
64QAM 0.92 single	33.0	17.0	50.0	30.0	15.0	45.0
64QAM 0.75 single	27.0	14.0	41.0	25.0	12.0	37.0
16QAM 0.87 single	21.0	11.0	32.0	19.0	10.0	29.0
16QAM 0.63 single	15.0	8.0	23.0	14.0	7.0	21.0
QPSK 0.87 single	11.0	5.0	16.0	10.0	5.0	15.0
QPSK 0.63 single	8.0	5.0	13.0	7.0	5.0	12.0
BPSK 0.63 single	5.0	5.0	10.0	5.0	5.0	10.0
Modulation mode	**20 MHz (Tx/Rx/Aggregate)**			**10 MHz (Tx/Rx/Aggregate)**		
256QAM 0.81 dual	37.0	18.0	55.0	19.0	9.0	28.0
64QAM 0.92 dual	31.0	15.0	46.0	16.0	8.0	24.0
64QAM 0.75 dual	25.0	13.0	38.0	13.0	6.0	19.0
16QAM 0.87 dual	20.0	10.0	30.0	10.0	5.0	15.0
16QAM 0.63 dual	14.0	7.0	21.0	7.0	5.0	12.0
256QAM 0.81 single	18.0	9.0	27.0	9.0	5.0	14.0
64QAM 0.92 single	15.0	8.0	23.0	8.0	5.0	13.0
64QAM 0.75 single	13.0	6.0	19.0	6.0	5.0	11.0
16QAM 0.87 single	10.0	5.0	15.0	5.0	5.0	10.0
16QAM 0.63 single	7.0	5.0	12.0	5.0	5.0	10.0
QPSK 0.87 single	5.0	5.0	10.0	5.0	4.4	9.4
QPSK 0.63 single	5.0	5.0	10.0	5.0	3.2	8.2
BPSK 0.63 single	5.0	3.1	8.1	3.2	1.6	4.8

Tx/Rx/Aggregate columns contain the transmit, receive and aggregate data rates per bandwidth.

Table 60 Throughput at zero link range (Mbit/s), Lite, symmetry adaptive, optimization IP

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	114.0	11.0	125.0	103.0	11.0	114.0
64QAM 0.92 dual	96.0	10.0	106.0	87.0	10.0	97.0
64QAM 0.75 dual	79.0	8.0	87.0	71.0	8.0	79.0
16QAM 0.87 dual	61.0	6.0	67.0	55.0	6.0	61.0
16QAM 0.63 dual	44.0	5.0	49.0	40.0	5.0	45.0
256QAM 0.81 single	57.0	6.0	63.0	52.0	6.0	58.0
64QAM 0.92 single	48.0	5.0	53.0	43.0	5.0	48.0
64QAM 0.75 single	39.0	5.0	44.0	35.0	5.0	40.0
16QAM 0.87 single	31.0	5.0	36.0	28.0	5.0	33.0
16QAM 0.63 single	22.0	5.0	27.0	20.0	5.0	25.0
QPSK 0.87 single	15.0	5.0	20.0	14.0	5.0	19.0
QPSK 0.63 single	11.0	3.9	14.9	10.0	3.9	13.9
BPSK 0.63 single	5.0	2.0	7.0	5.0	2.0	7.0
Modulation mode	**20 MHz (Tx/Rx/Aggregate)**			**10 MHz (Tx/Rx/Aggregate)**		
256QAM 0.81 dual	45.0	11.0	56.0	19.0	9.0	28.0
64QAM 0.92 dual	38.0	9.0	47.0	16.0	8.0	24.0
64QAM 0.75 dual	31.0	8.0	39.0	13.0	6.0	19.0
16QAM 0.87 dual	24.0	6.0	30.0	10.0	5.0	15.0
16QAM 0.63 dual	17.0	5.0	22.0	7.0	5.0	12.0
256QAM 0.81 single	22.0	6.0	28.0	9.0	5.0	14.0
64QAM 0.92 single	19.0	5.0	24.0	8.0	5.0	13.0
64QAM 0.75 single	15.0	5.0	20.0	6.0	5.0	11.0
16QAM 0.87 single	12.0	5.0	17.0	5.0	5.0	10.0
16QAM 0.63 single	9.0	5.0	14.0	5.0	5.0	10.0
QPSK 0.87 single	6.0	5.0	11.0	5.0	4.4	9.4
QPSK 0.63 single	5.0	3.8	8.8	5.0	3.2	8.2
BPSK 0.63 single	5.0	1.9	6.9	3.2	1.6	4.8

Tx/Rx/Aggregate columns contain the transmit, receive and aggregate data rates per bandwidth.

Figure 33 Range adjustment for PTP 650, symmetry 1:1, optimization IP, bandwidth 45 MHz

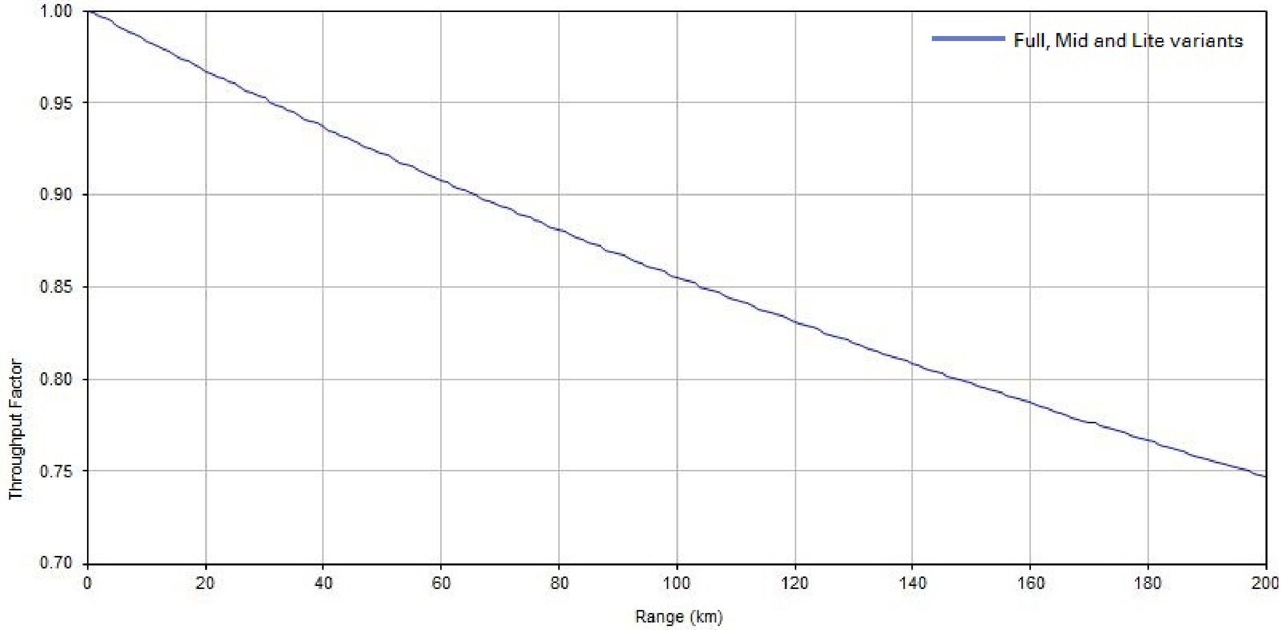


Figure 34 Range adjustment for PTP 650, symmetry 1:1, optimization IP, bandwidth 40 MHz

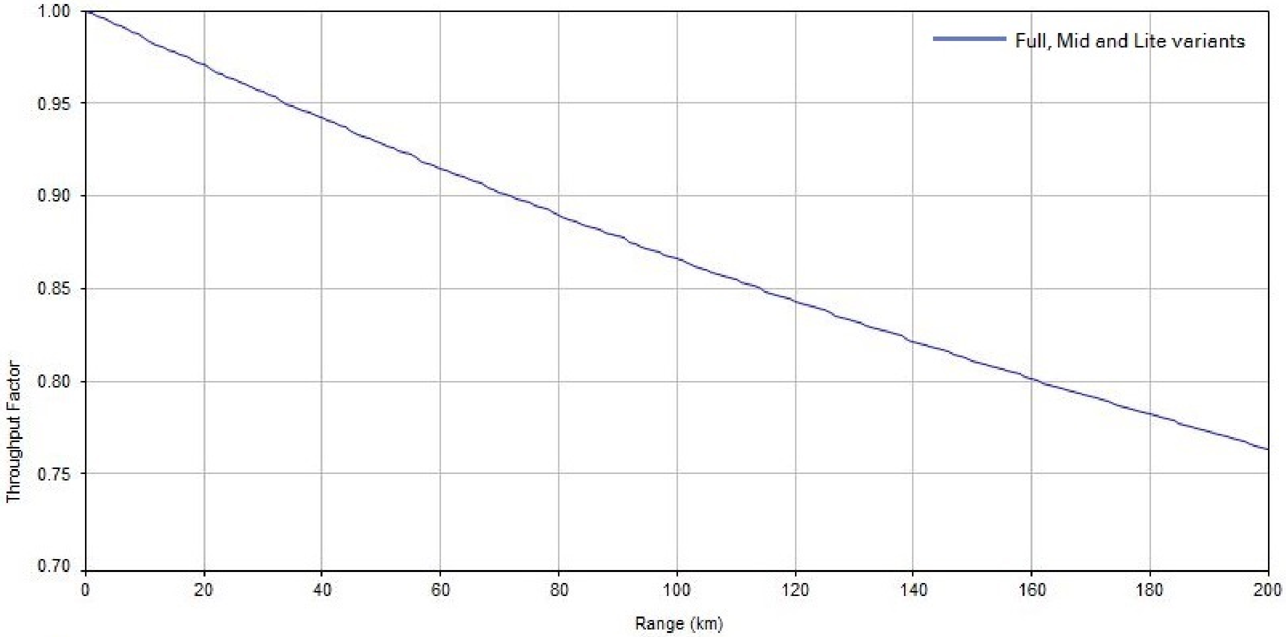


Figure 35 Range adjustment for PTP 650, symmetry 1:1, optimization IP, bandwidth 20 MHz

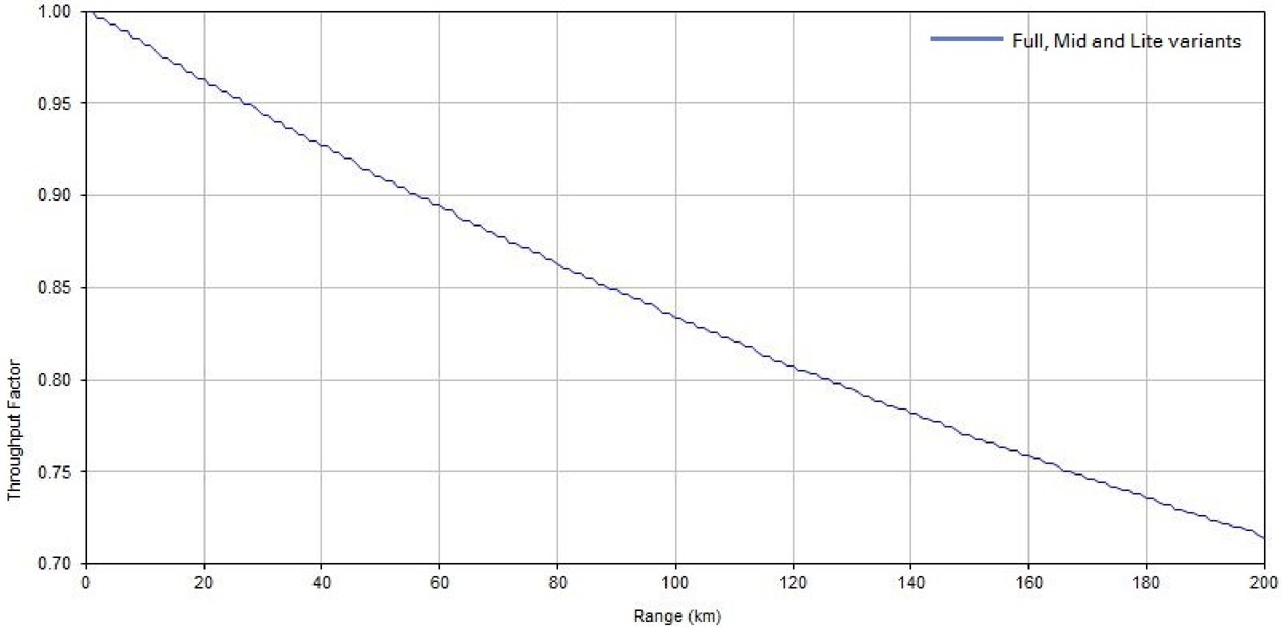


Figure 36 Range adjustment for PTP 650, symmetry 1:1, optimization IP, bandwidth 10 MHz

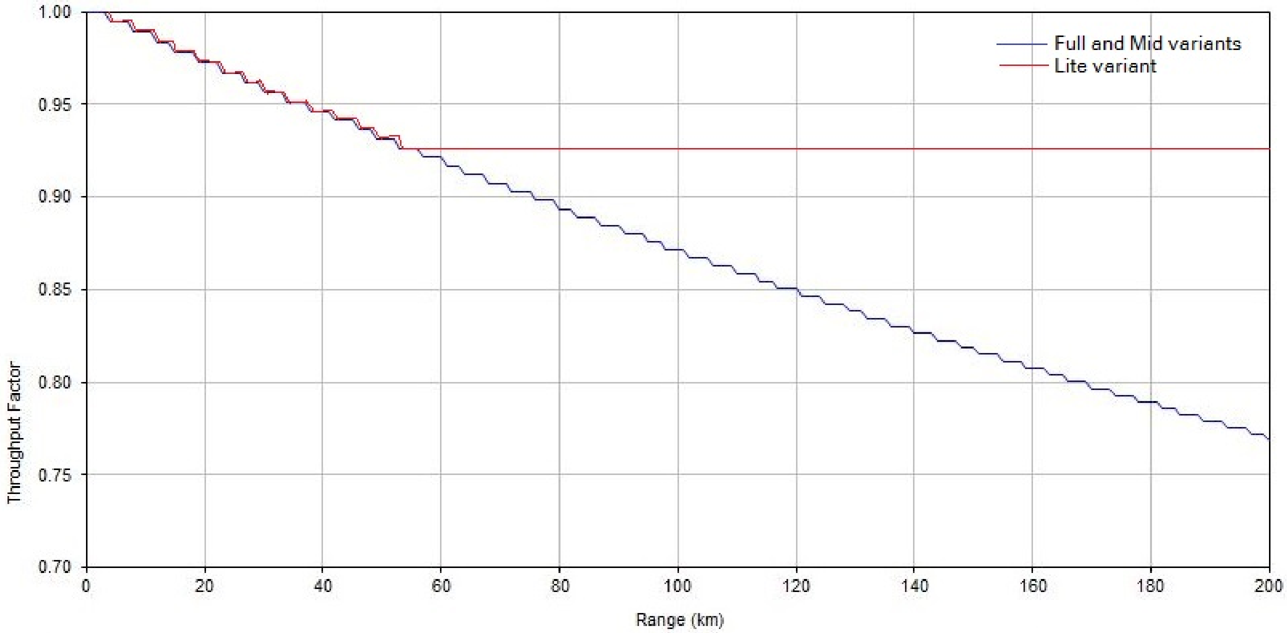


Figure 37 Range adjustment for PTP 650, symmetry 1:1, optimization TDM, bandwidth 45 MHz

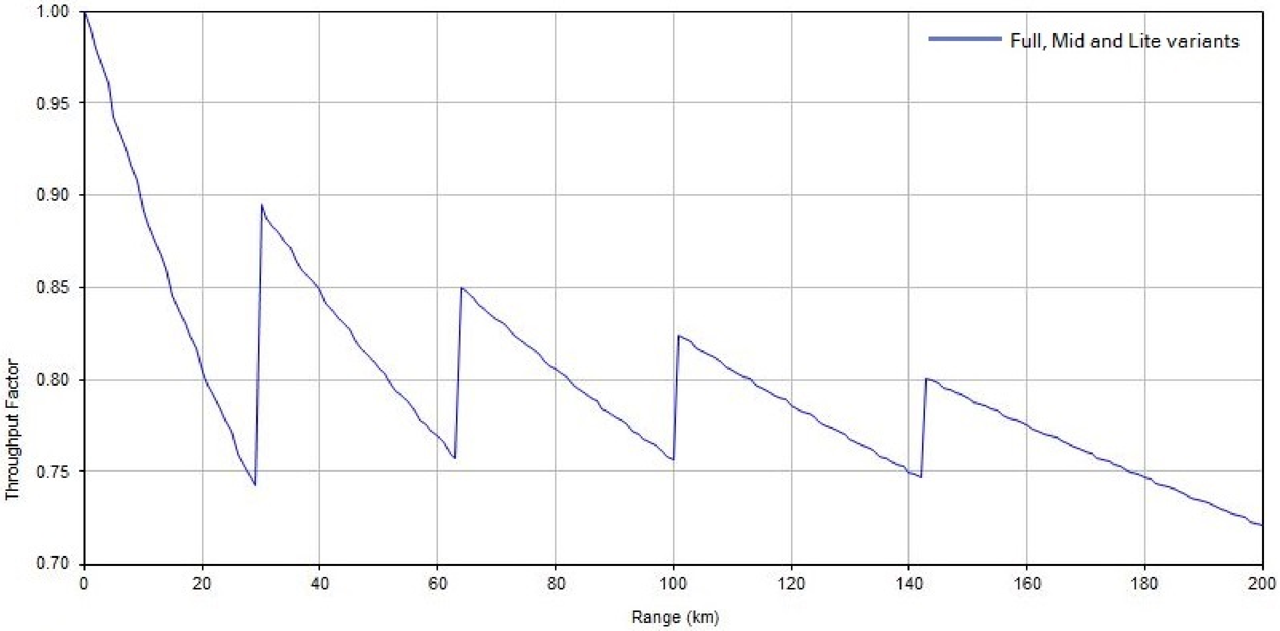


Figure 38 Range adjustment for PTP 650, symmetry 1:1, optimization TDM, bandwidth 40 MHz

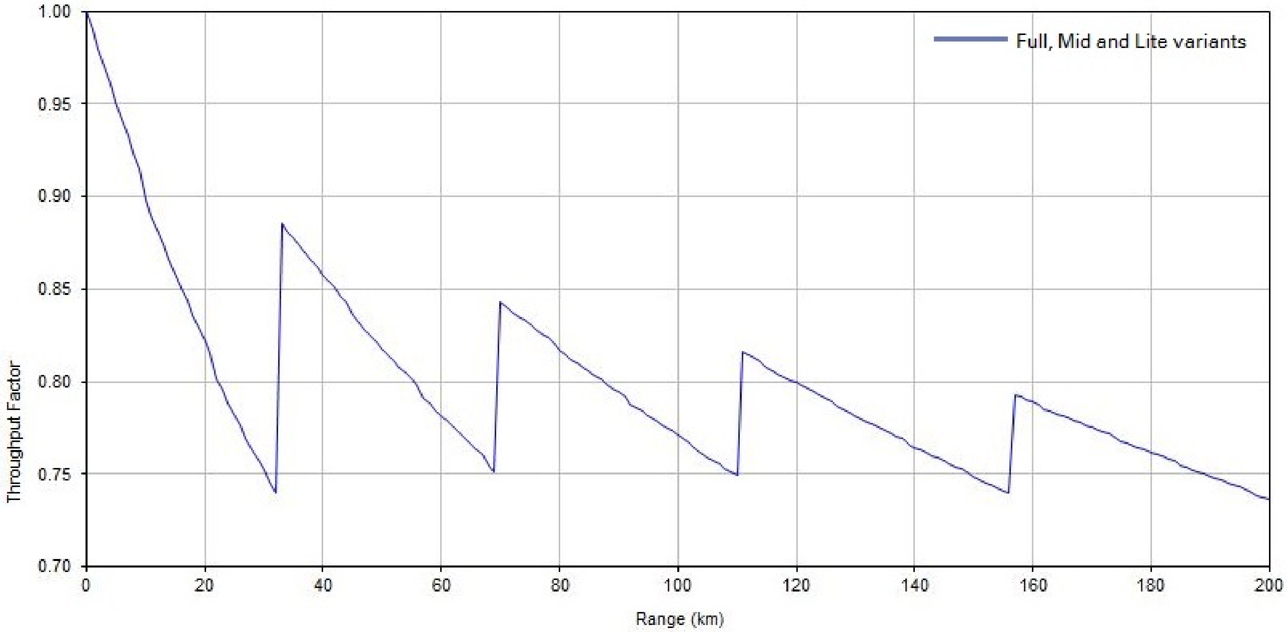


Figure 39 Range adjustment for PTP 650, symmetry 1:1, optimization TDM, bandwidth 20 MHz

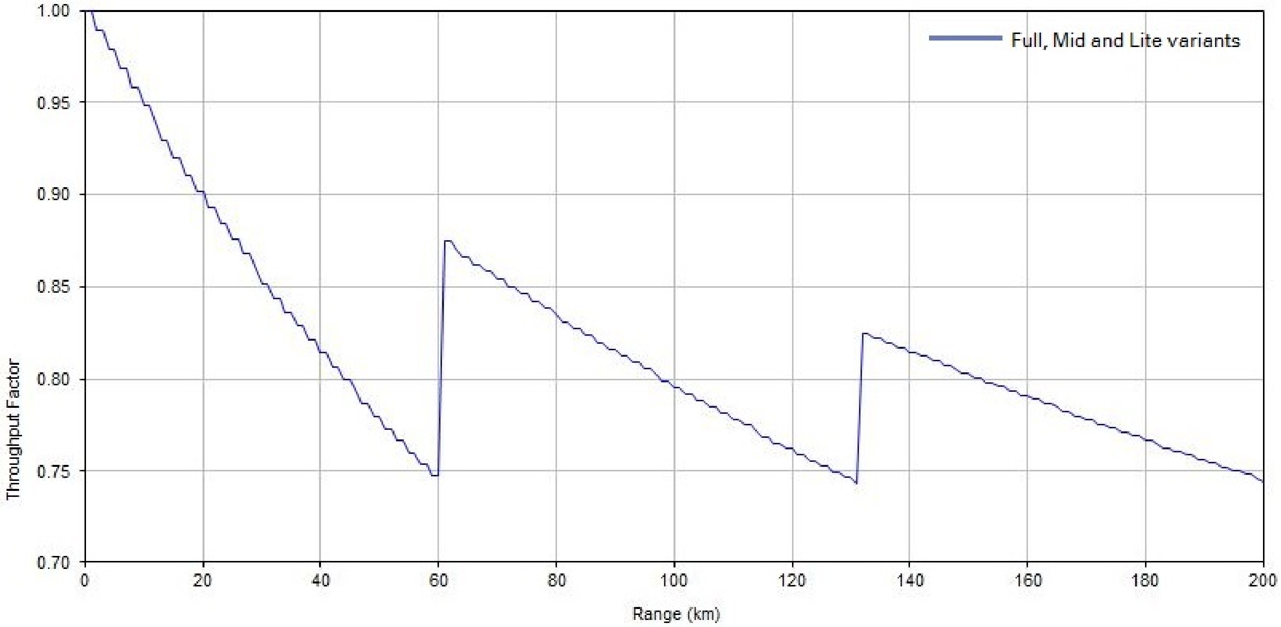


Figure 40 Range adjustment for PTP 650, symmetry 1:1, optimization TDM, bandwidth 10 MHz

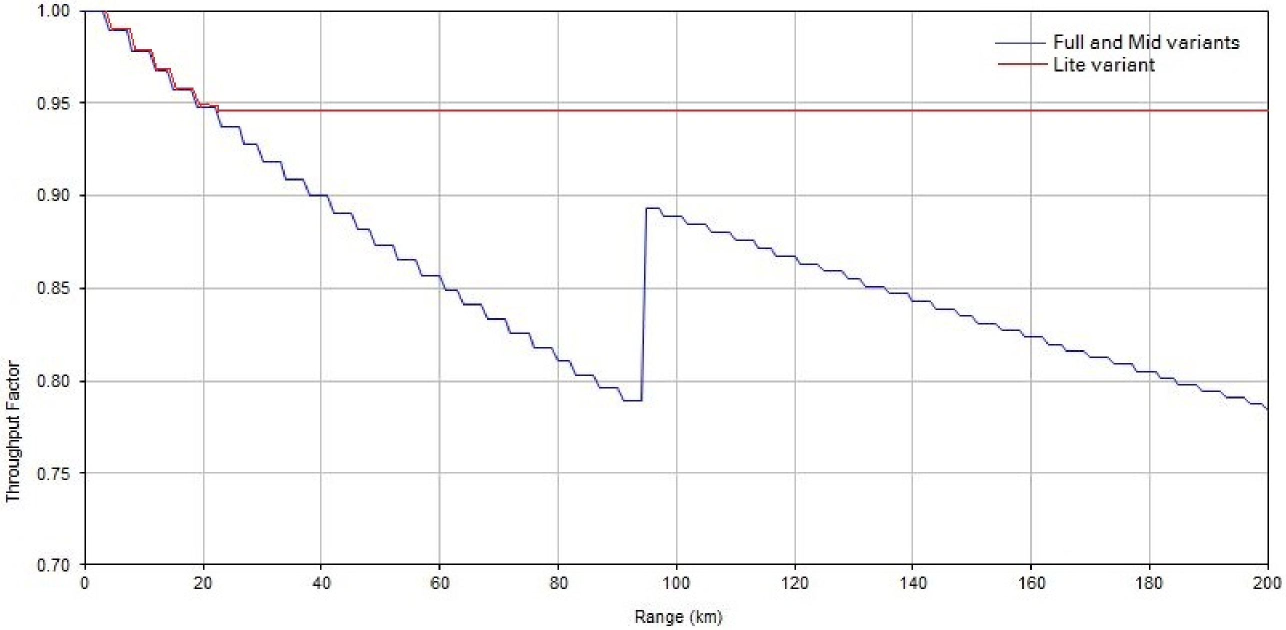


Figure 41 Range adjustment for PTP 650, symmetry 2:1, optimization IP, bandwidth 45 MHz

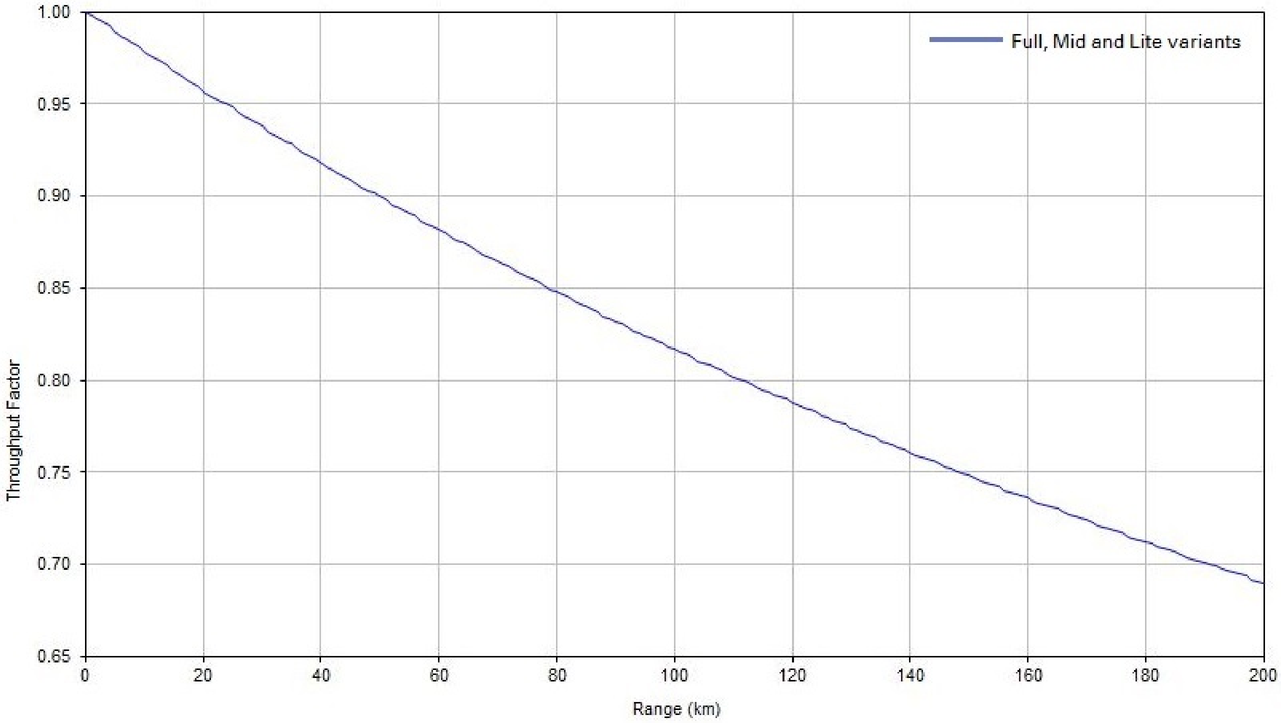


Figure 42 Range adjustment for PTP 650, symmetry 2:1, optimization IP, bandwidth 40 MHz

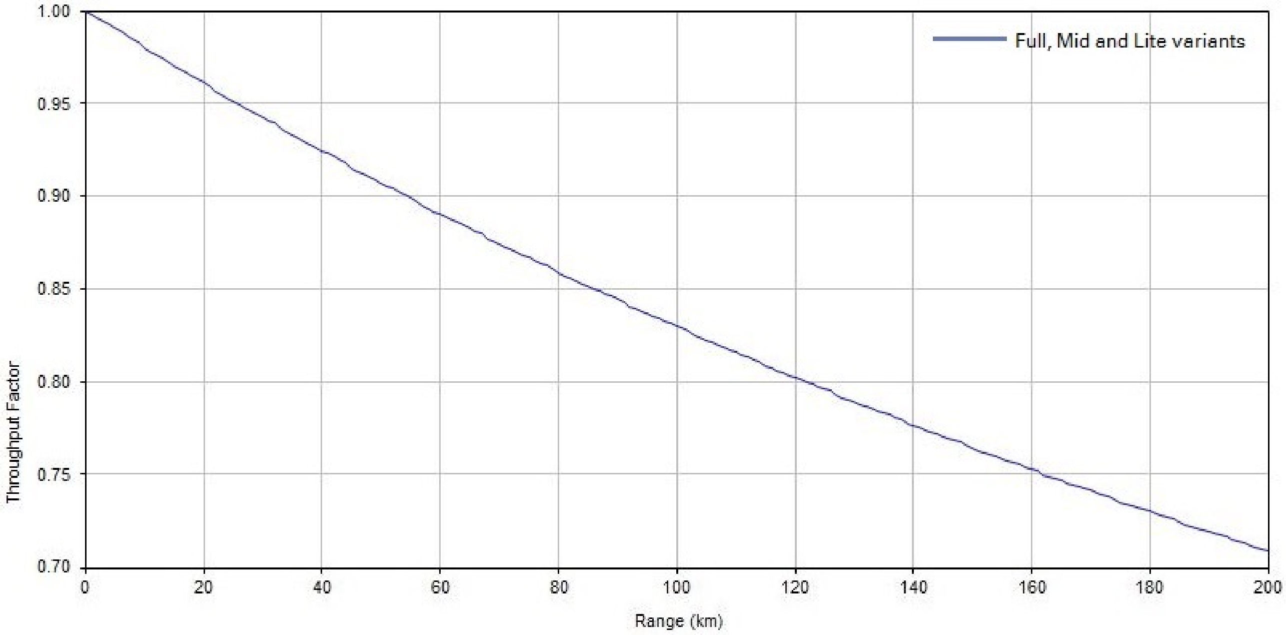


Figure 43 Range adjustment for PTP 650, symmetry 2:1, optimization IP, bandwidth 20 MHz

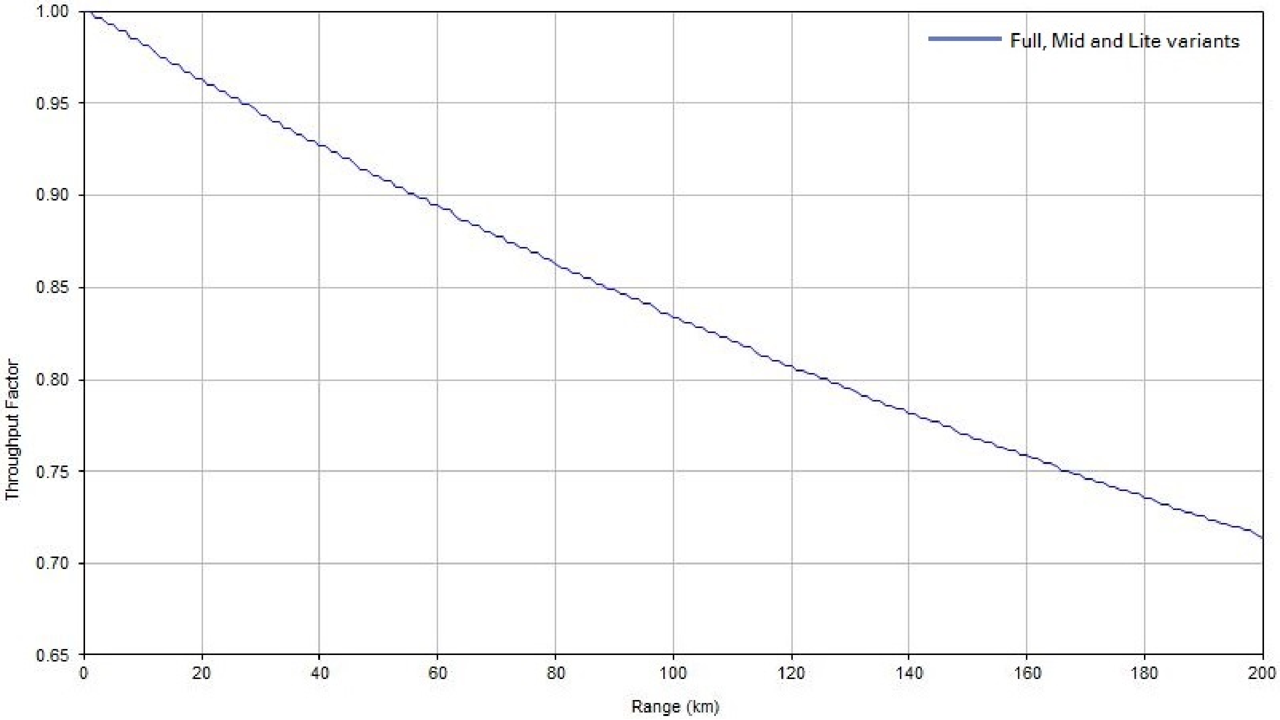


Figure 44 Range adjustment for PTP 650, symmetry 2:1, optimization IP, bandwidth 10 MHz

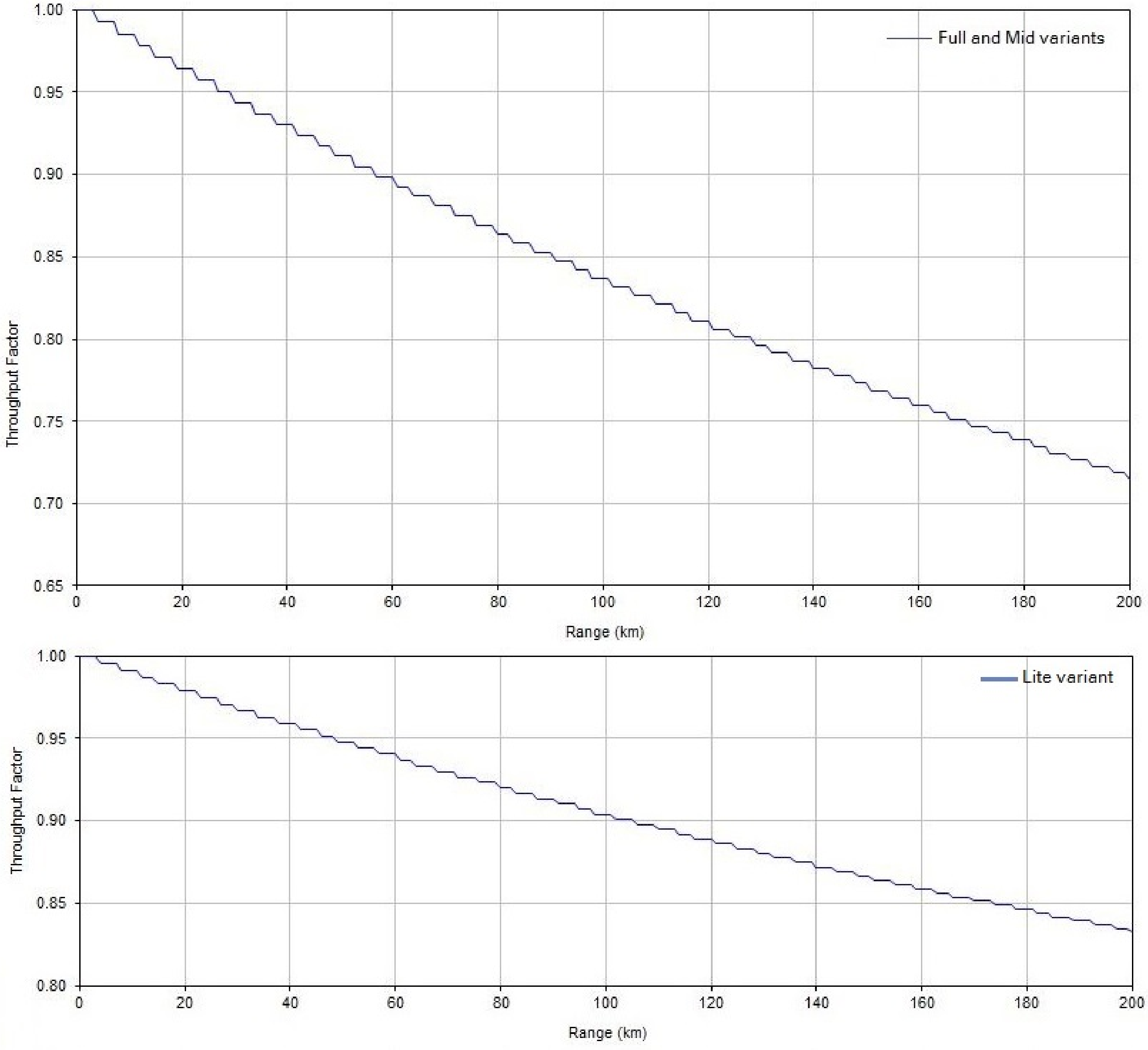


Figure 45 Range adjustment for PTP 650, symmetry 2:1, optimization TDM, bandwidth 45 MHz

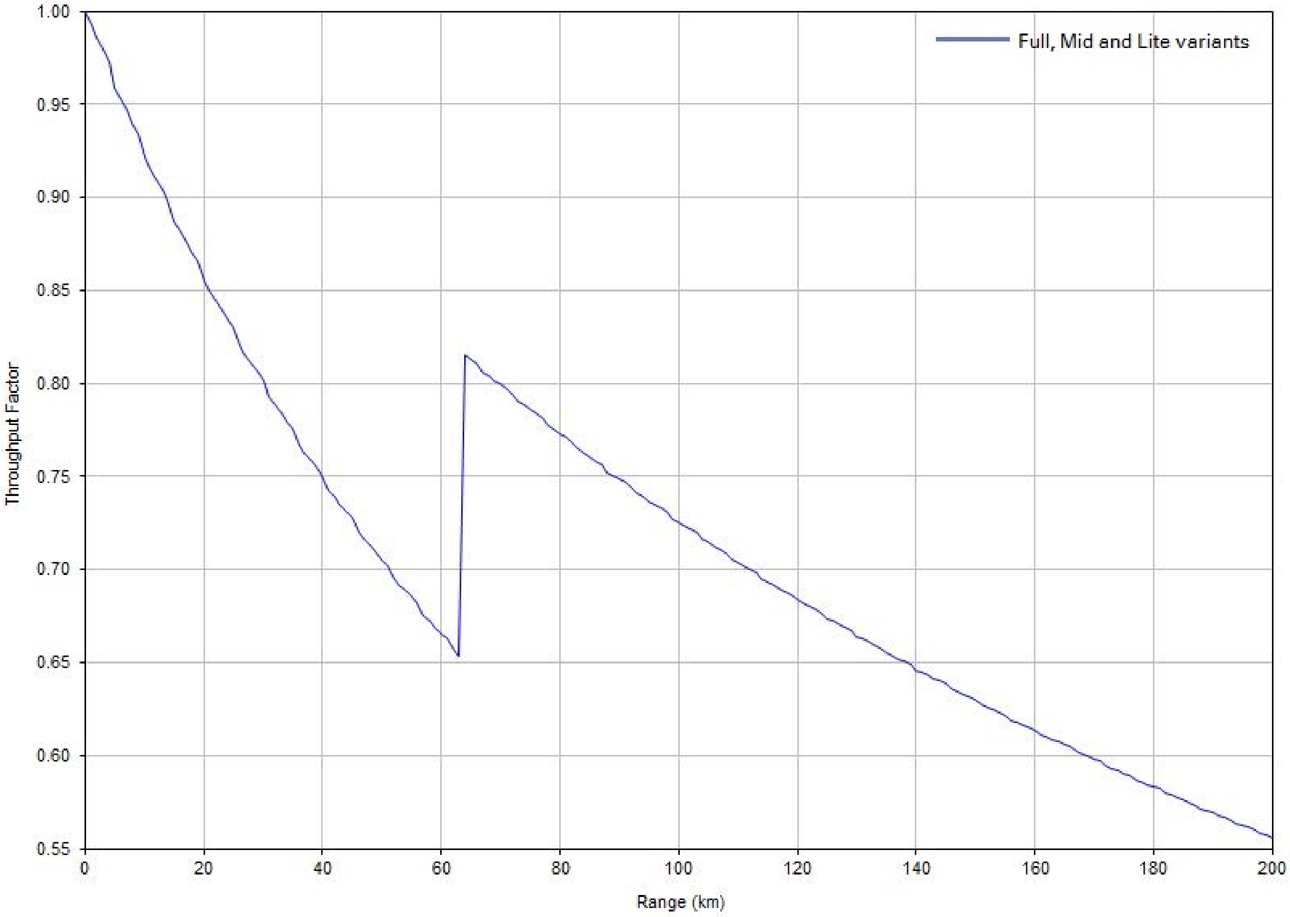


Figure 46 Range adjustment for PTP 650, symmetry 2:1, optimization TDM, bandwidth 40 MHz

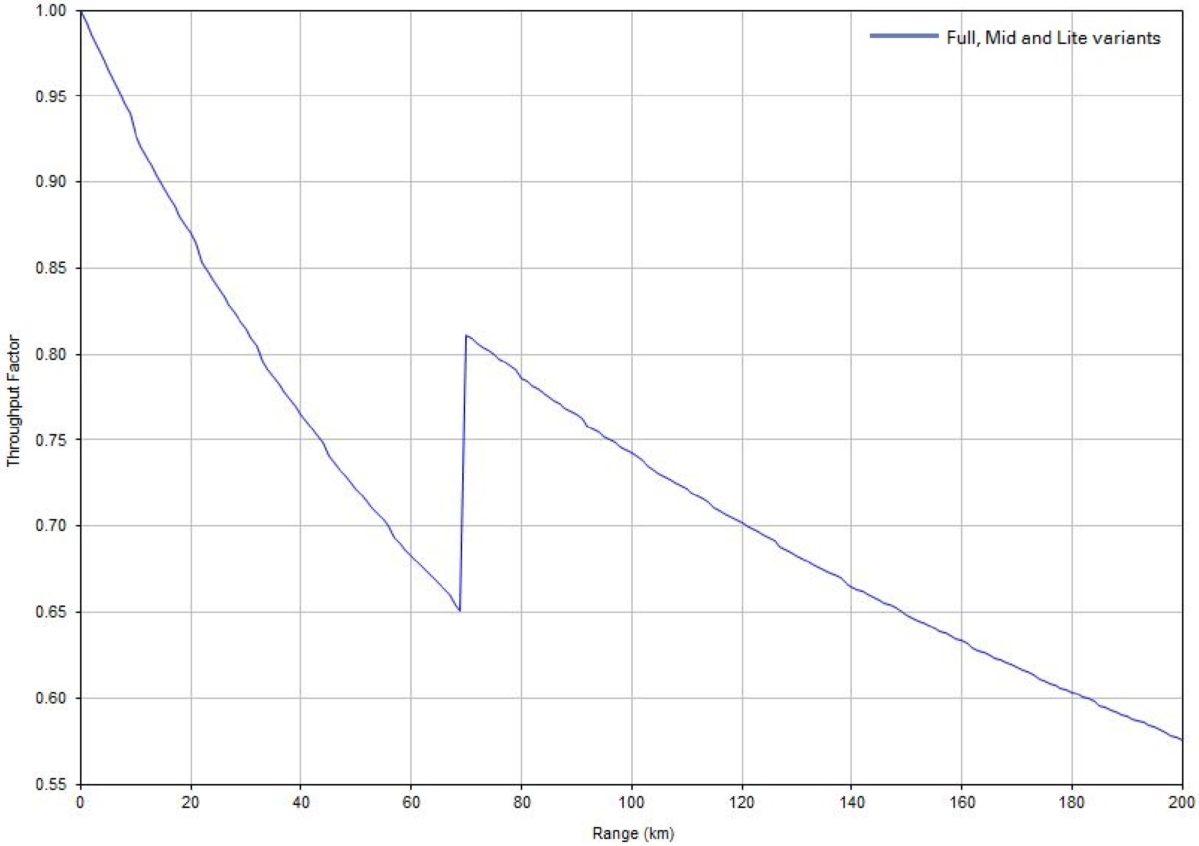


Figure 47 Range adjustment for PTP 650, symmetry 2:1, optimization TDM, bandwidth 20 MHz

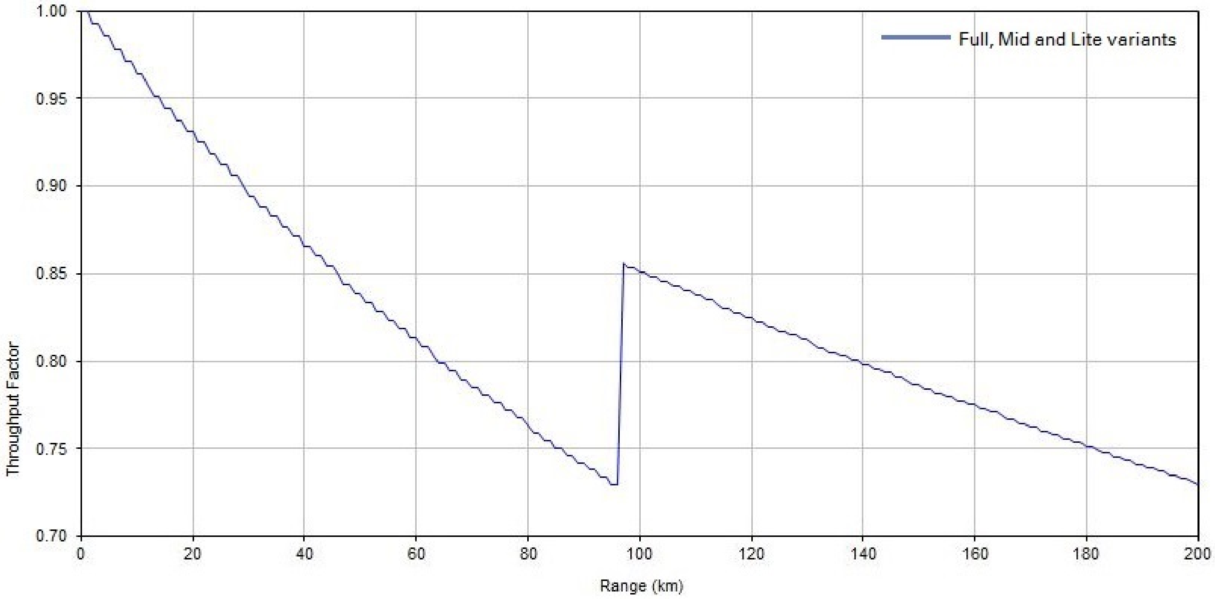


Figure 48 Range adjustment for PTP 650, symmetry 2:1, optimization TDM, bandwidth 10 MHz

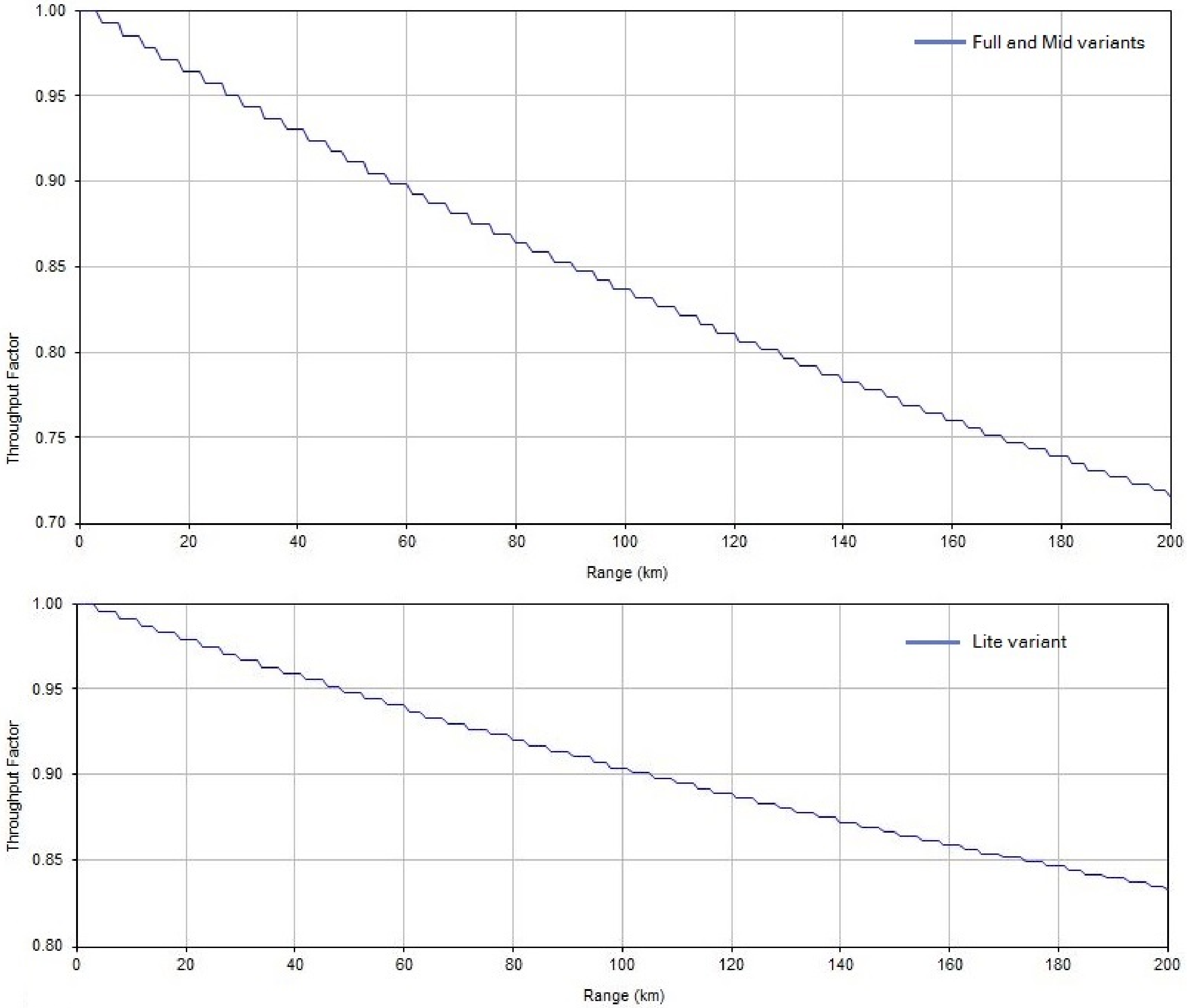


Figure 49 Range adjustment for PTP 650, adaptive, optimization IP, bandwidth 45 MHz

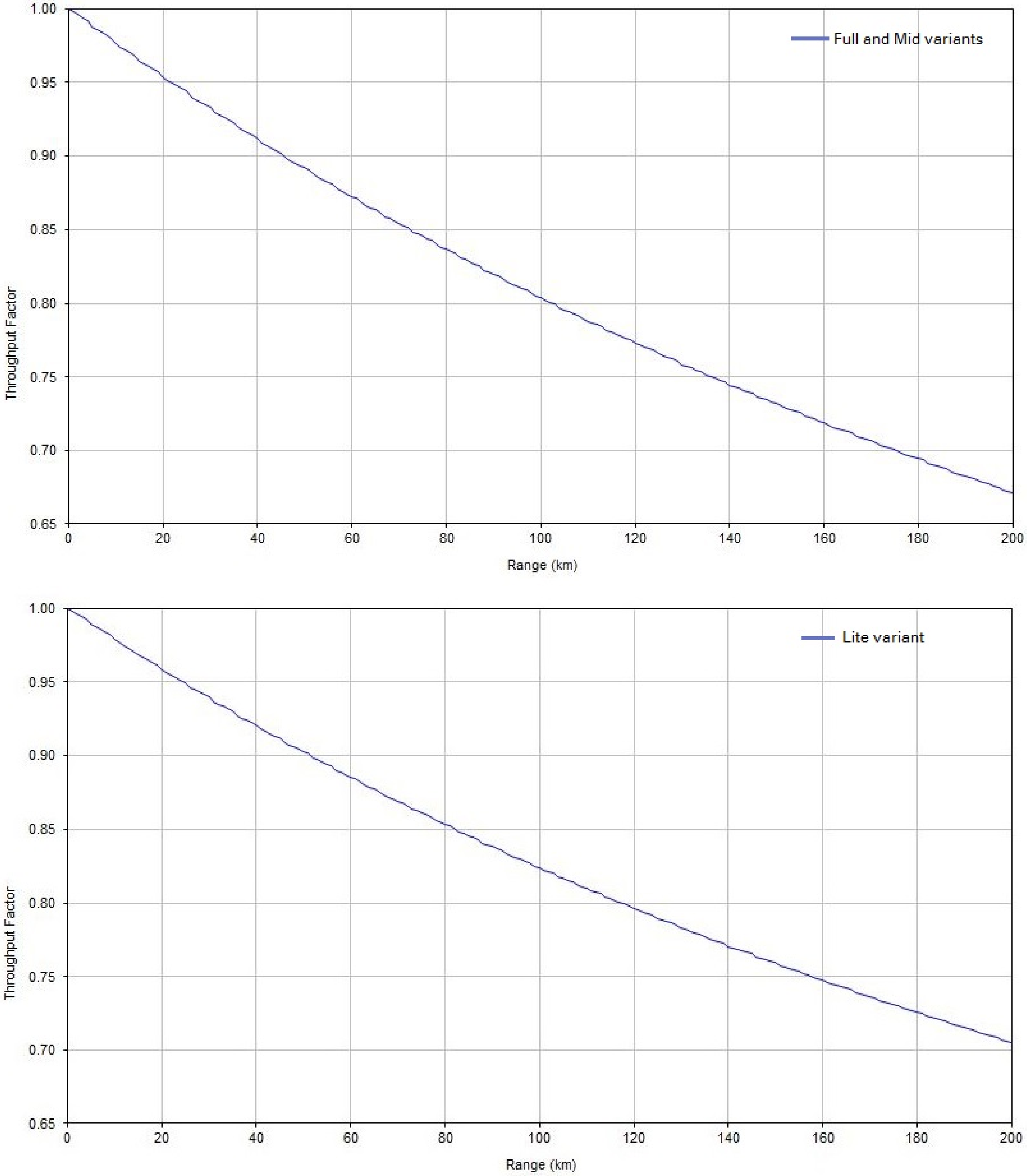


Figure 50 Range adjustment for PTP 650, adaptive, optimization IP, bandwidth 40 MHz

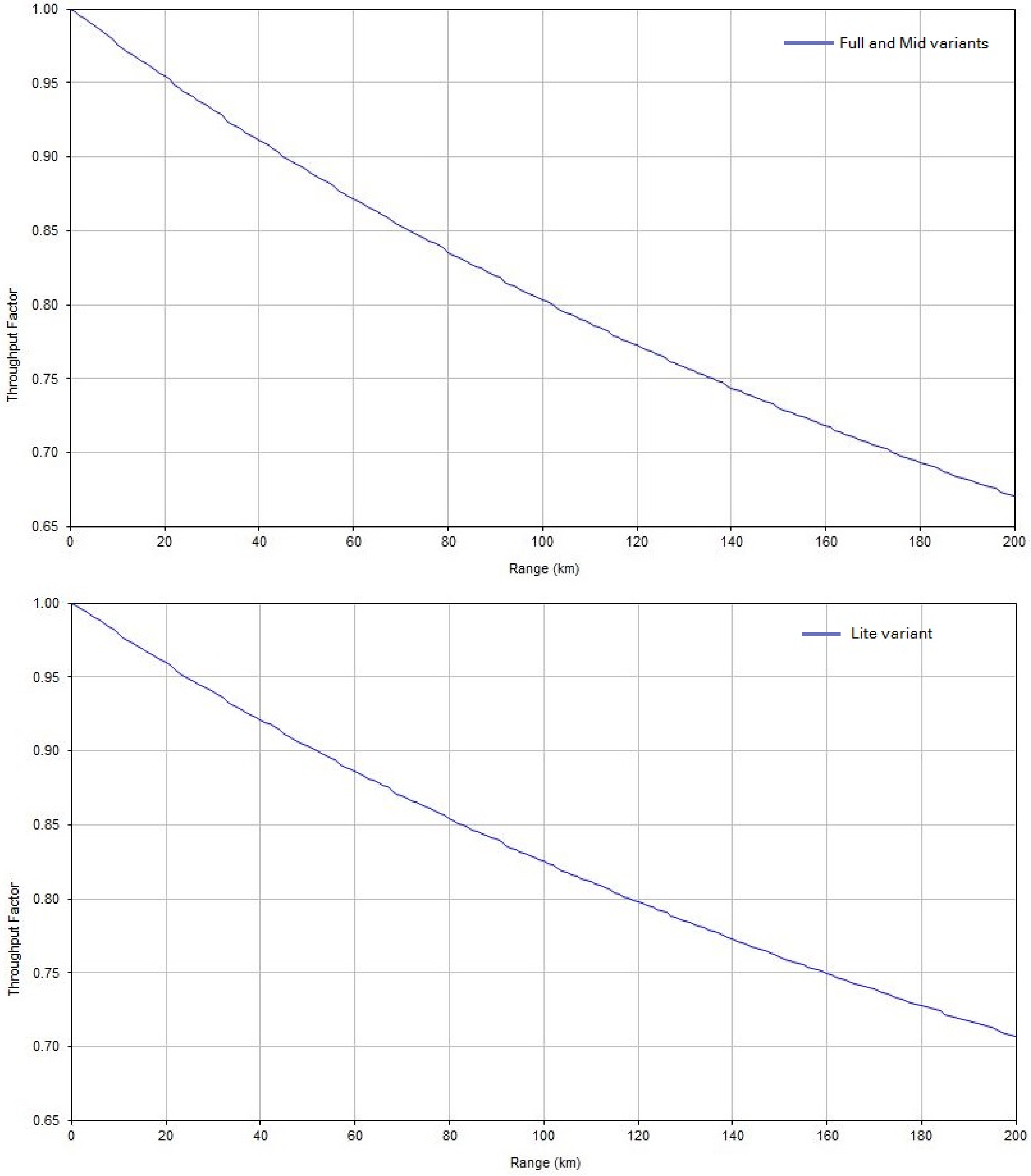


Figure 51 Range adjustment for PTP 650, adaptive, optimization IP, bandwidth 20 MHz

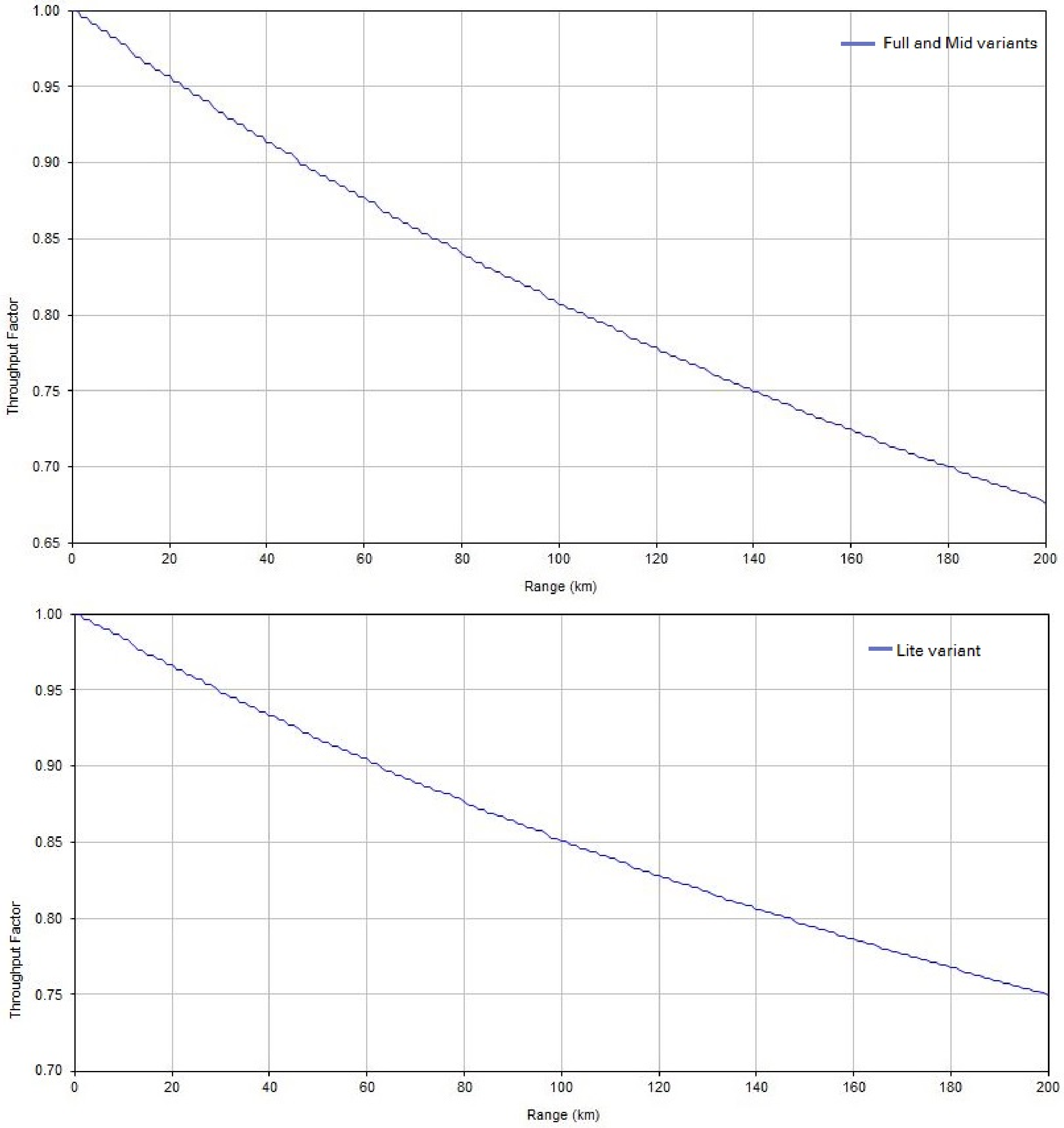
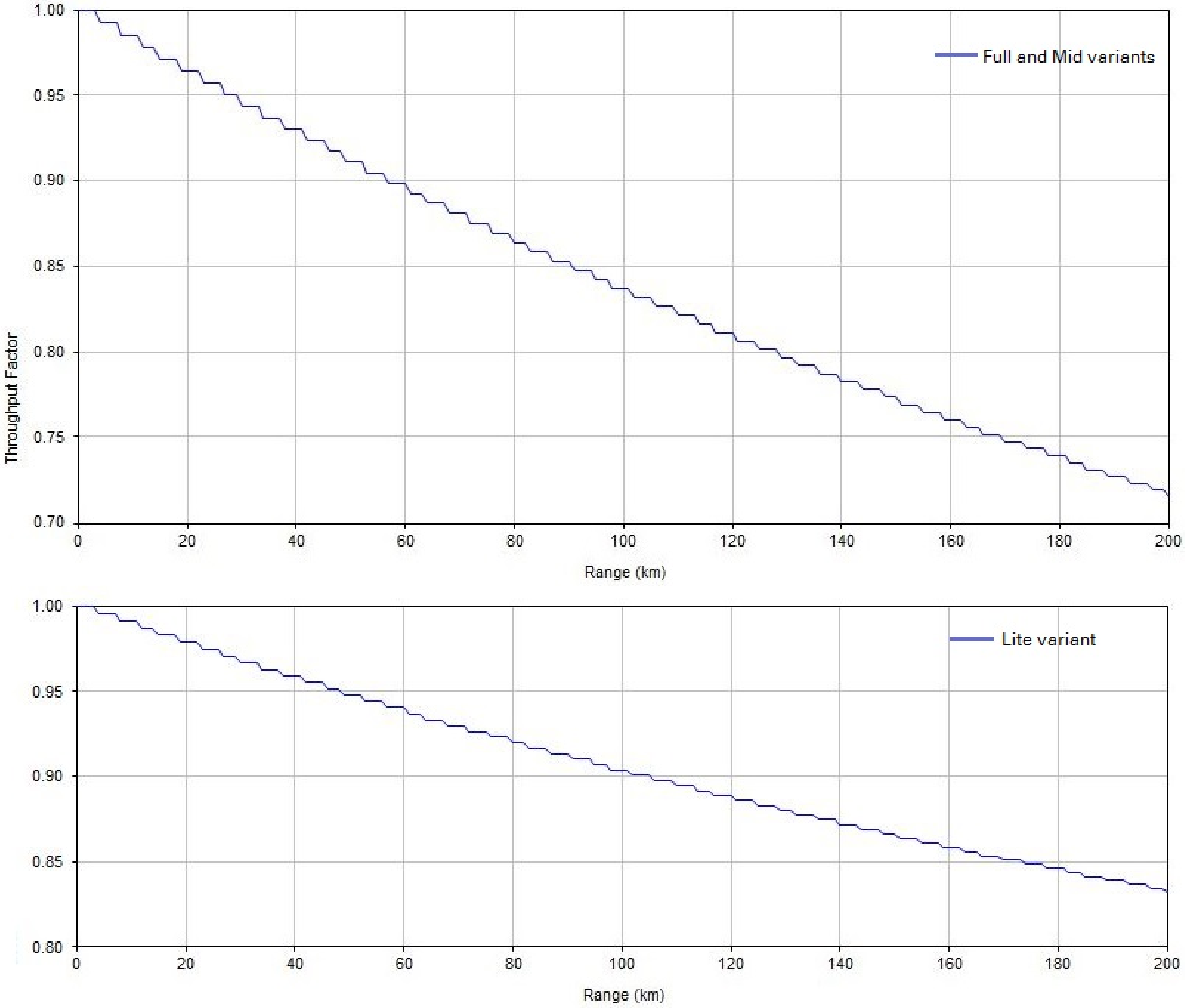


Figure 52 Range adjustment for PTP 650, adaptive, optimization IP, bandwidth 10 MHz



Chapter 4: Legal and regulatory information

This chapter provides end user license agreements and regulatory notifications.

⚠ **Caution**

Intentional or unintentional changes or modifications to the equipment must not be made unless under the express consent of the party responsible for compliance. Any such modifications could void the user's authority to operate the equipment and will void the manufacturer's warranty.

The following topics are described in this chapter:

- Cambium Networks end user license agreement on page 4-2 contains the Cambium and third party license agreements for the PTP 650 Series products.
- Compliance with safety standards on page 4-23 lists the safety specifications against which the PTP 650 has been tested and certified. It also describes how to keep RF exposure within safe limits.
- Compliance with radio regulations on page 4-27 describes how the PTP 650 complies with the radio regulations that are in force in various countries, and contains notifications made to regulatory bodies for the PTP 650.

Cambium Networks end user license agreement

Acceptance of this agreement

In connection with Cambium Networks' delivery of certain proprietary software or products containing embedded or pre-loaded proprietary software, or both, Cambium Networks is willing to license this certain proprietary software and the accompanying documentation to you only on the condition that you accept all the terms in this End User License Agreement ("Agreement").

IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT USE THE PRODUCT OR INSTALL THE SOFTWARE. INSTEAD, YOU MAY, FOR A FULL REFUND, RETURN THIS PRODUCT TO THE LOCATION WHERE YOU ACQUIRED IT OR PROVIDE WRITTEN VERIFICATION OF DELETION OF ALL COPIES OF THE SOFTWARE. ANY USE OF THE SOFTWARE, INCLUDING BUT NOT LIMITED TO USE ON THE PRODUCT, WILL CONSTITUTE YOUR ACCEPTANCE TO THE TERMS OF THIS AGREEMENT.

Definitions

In this Agreement, the word "Software" refers to the set of instructions for computers, in executable form and in any media, (which may include diskette, CD-ROM, downloadable internet, hardware, or firmware) licensed to you. The word "Documentation" refers to electronic or printed manuals and accompanying instructional aids licensed to you. The word "Product" refers to Cambium Networks' fixed wireless broadband devices for which the Software and Documentation is licensed for use.

Grant of license

Cambium Networks Limited ("Cambium") grants you ("Licensee" or "you") a personal, nonexclusive, non-transferable license to use the Software and Documentation subject to the Conditions of Use set forth in "**Conditions of use**" and the terms and conditions of this Agreement. Any terms or conditions relating to the Software and Documentation appearing on the face or reverse side of any purchase order, purchase order acknowledgment or other order document that are different from, or in addition to, the terms of this Agreement will not be binding on the parties, even if payment is accepted.

Conditions of use

Any use of the Software and Documentation outside of the conditions set forth in this Agreement is strictly prohibited and will be deemed a breach of this Agreement.

1. Only you, your employees or agents may use the Software and Documentation. You will take all necessary steps to insure that your employees and agents abide by the terms of this Agreement.

2. You will use the Software and Documentation (i) only for your internal business purposes; (ii) only as described in the Software and Documentation; and (iii) in strict accordance with this Agreement.

3. You may use the Software and Documentation, provided that the use is in conformance with the terms set forth in this Agreement.

4. Portions of the Software and Documentation are protected by United States copyright laws, international treaty provisions, and other applicable laws. Therefore, you must treat the Software like any other copyrighted material (for example, a book or musical recording) except that you may either: (i) make 1 copy of the transportable part of the Software (which typically is supplied on diskette, CD-ROM, or downloadable internet), solely for back-up purposes; or (ii) copy the transportable part of the Software to a PC hard disk, provided you keep the original solely for back-up purposes. If the Documentation is in printed form, it may not be copied. If the Documentation is in electronic form, you may print out 1 copy, which then may not be copied. With regard to the copy made for backup or archival purposes, you agree to reproduce any Cambium Networks copyright notice, and other proprietary legends appearing thereon. Such copyright notice(s) may appear in any of several forms, including machine-readable form, and you agree to reproduce such notice in each form in which it appears, to the extent it is physically possible to do so. Unauthorized duplication of the Software or Documentation constitutes copyright infringement, and in the United States is punishable in federal court by fine and imprisonment.

5. You will not transfer, directly or indirectly, any product, technical data or software to any country for which the United States Government requires an export license or other governmental approval without first obtaining such license or approval.

Title and restrictions

If you transfer possession of any copy of the Software and Documentation to another party outside of the terms of this agreement, your license is automatically terminated. Title and copyrights to the Software and Documentation and any copies made by you remain with Cambium Networks and its licensors. You will not, and will not permit others to: (i) modify, translate, decompile, bootleg, reverse engineer, disassemble, or extract the inner workings of the Software or Documentation, (ii) copy the look-and-feel or functionality of the Software or Documentation; (iii) remove any proprietary notices, marks, labels, or logos from the Software or Documentation; (iv) rent or transfer all or some of the Software or Documentation to any other party without Cambium's prior written consent; or (v) utilize any computer software or hardware which is designed to defeat any copy protection device, should the Software and Documentation be equipped with such a protection device. If the Software and Documentation is provided on multiple types of media (such as diskette, CD-ROM, downloadable internet), then you will only use the medium which best meets your specific needs, and will not loan, rent, lease, or transfer the other media contained in the package without Cambium's written consent. Unauthorized copying of the Software or Documentation, or failure to comply with any of the provisions of this Agreement, will result in automatic termination of this license.

Confidentiality

You acknowledge that all Software and Documentation contain valuable proprietary information and trade secrets and that unauthorized or improper use of the Software and Documentation will result in irreparable harm to Cambium Networks for which monetary damages would be inadequate and for which Cambium Networks will be entitled to immediate injunctive relief. If applicable, you will limit access to the Software and Documentation to those of your employees and agents who need to use the Software and Documentation for your internal business purposes, and you will take appropriate action with those employees and agents to preserve the confidentiality of the Software and Documentation, using the same degree of care to avoid unauthorized or improper disclosure as you use for the protection of your own proprietary software, but in no event less than reasonable care.

You have no obligation to preserve the confidentiality of any proprietary information that: (i) was in the public domain at the time of disclosure; (ii) entered the public domain through no fault of yours; (iii) was given to you free of any obligation to keep it confidential; (iv) is independently developed by you; or (v) is disclosed as required by law provided that you notify Cambium Networks prior to such disclosure and provide Cambium Networks with a reasonable opportunity to respond.

Right to use Cambium's name

Except as required in "**Conditions of use**", you will not, during the term of this Agreement or thereafter, use any trademark of Cambium Networks, or any word or symbol likely to be confused with any Cambium Networks trademark, either alone or in any combination with another word or words.

Transfer

The Software and Documentation may not be transferred to another party without the express written consent of Cambium Networks, regardless of whether or not such transfer is accomplished by physical or electronic means. Cambium's consent may be withheld at its discretion and may be conditioned upon transferee paying all applicable license fees and agreeing to be bound by this Agreement.

Updates

During the first 12 months after purchase of a Product, or during the term of any executed Maintenance and Support Agreement for the Product, you are entitled to receive Updates. An "Update" means any code in any form which is a bug fix, patch, error correction, or minor enhancement, but excludes any major feature added to the Software. Updates are available for download at the support website.

Major features may be available from time to time for an additional license fee. If Cambium Networks makes available to you major features and no other end user license agreement is provided, then the terms of this Agreement will apply.

Maintenance

Except as provided above, Cambium Networks is not responsible for maintenance or field service of the Software under this Agreement.

Disclaimer

CAMBIUM NETWORKS DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR IN ANY COMMUNICATION WITH YOU. CAMBIUM NETWORKS SPECIFICALLY DISCLAIMS ANY WARRANTY INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILTY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS." CAMBIUM NETWORKS DOES NOT WARRANT THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS, OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE, OR THAT DEFECTS IN THE SOFTWARE WILL BE CORRECTED. CAMBIUM NETWORKS MAKES NO WARRANTY WITH RESPECT TO THE CORRECTNESS, ACCURACY, OR RELIABILITY OF THE SOFTWARE AND DOCUMENTATION. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Limitation of liability

IN NO EVENT SHALL CAMBIUM NETWORKS BE LIABLE TO YOU OR ANY OTHER PARTY FOR ANY DIRECT, INDIRECT, GENERAL, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR OTHER DAMAGE ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR ANY OTHER PECUNIARY LOSS, OR FROM ANY BREACH OF WARRANTY, EVEN IF CAMBIUM NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. (Some states do not allow the exclusion or limitation of incidental or consequential damages, so the above exclusion or limitation may not apply to you.) IN NO CASE SHALL CAMBIUM'S LIABILITY EXCEED THE AMOUNT YOU PAID FOR THE PRODUCT.

U.S. government

If you are acquiring the Product on behalf of any unit or agency of the U.S. Government, the following applies. Use, duplication, or disclosure of the Software and Documentation is subject to the restrictions set forth in subparagraphs (c) (1) and (2) of the Commercial Computer Software – Restricted Rights clause at FAR 52.227-19 (JUNE 1987), if applicable, unless being provided to the Department of Defense. If being provided to the Department of Defense, use, duplication, or disclosure of the Products is subject to the restricted rights set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 (OCT 1988), if applicable. Software and Documentation may or may not include a Restricted Rights notice, or other notice referring specifically to the terms and conditions of this Agreement. The terms and conditions of this Agreement will each continue to apply, but only to the extent that such terms and conditions are not inconsistent with the rights provided to you under the aforementioned provisions of the FAR and DFARS, as applicable to the particular procuring agency and procurement transaction.

Term of license

Your right to use the Software will continue in perpetuity unless terminated as follows. Your right to use the Software will terminate immediately without notice upon a breach of this Agreement by you. Within 30 days after termination of this Agreement, you will certify to Cambium Networks in writing that through your best efforts, and to the best of your knowledge, the original and all copies, in whole or in part, in any form, of the Software and all related material and Documentation, have been destroyed, except that, with prior written consent from Cambium Networks, you may retain one copy for archival or backup purposes. You may not sublicense, assign or transfer the license or the Product, except as expressly provided in this Agreement. Any attempt to otherwise sublicense, assign or transfer any of the rights, duties or obligations hereunder is null and void.

Governing law

This Agreement is governed by the laws of the United States of America to the extent that they apply and otherwise by the laws of the State of Illinois.

Assignment

This agreement may not be assigned by you without Cambium's prior written consent.

Survival of provisions

The parties agree that where the context of any provision indicates an intent that it survives the term of this Agreement, then it will survive.

Entire agreement

This agreement contains the parties' entire agreement regarding your use of the Software and may be amended only in writing signed by both parties, except that Cambium Networks may modify this Agreement as necessary to comply with applicable laws.

Third party software

The software may contain one or more items of Third-Party Software supplied by other third-party suppliers. The terms of this Agreement govern your use of any Third-Party Software UNLESS A SEPARATE THIRD-PARTY SOFTWARE LICENSE IS INCLUDED, IN WHICH CASE YOUR USE OF THE THIRD-PARTY SOFTWARE WILL THEN BE GOVERNED BY THE SEPARATE THIRD-PARTY LICENSE.

Trademarks

Java™ Technology and/or J2ME™ : Java and all other Java-based marks are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

UNIX® : UNIX is a registered trademark of The Open Group in the United States and other countries.

Net SNMP

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright © 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright © 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright © 2003-2008, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Sparta, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 6: Cisco/BUPTNIC copyright notice (BSD) -----

Copyright © 2004, Cisco, Inc and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Cisco, Inc, Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD) -----

Copyright © Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenSSL

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

“This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptographic related.

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

“This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

Zlib

Copyright © 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided ‘as-is’, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu

Libpng

libpng versions 1.2.6, August 15, 2004, through 1.2.35, February 14, 2009, are Copyright © 2004, 2006-2008 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.2.5 with the following individual added to the list of Contributing Authors

Cosmin Truta

libpng versions 1.0.7, July 1, 2000, through 1.2.5 - October 3, 2002, are Copyright © 2000-2002 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-1.0.6 with the following individuals added to the list of Contributing Authors

Simon-Pierre Cadieux

Eric S. Raymond

Gilles Vollant

and with the following additions to the disclaimer:

There is no warranty against interference with your enjoyment of the library or against infringement. There is no warranty that our efforts or the library will fulfil any of your particular purposes or needs. This library is provided with all faults, and the entire risk of satisfactory quality, performance, accuracy, and effort is with the user.

libpng versions 0.97, January 1998, through 1.0.6, March 20, 2000, are Copyright © 1998, 1999 Glenn Randers-Pehrson, and are distributed according to the same disclaimer and license as libpng-0.96, with the following individuals added to the list of Contributing Authors:

Tom Lane

Glenn Randers-Pehrson

Willem van Schaik

libpng versions 0.89, June 1996, through 0.96, May 1997, are Copyright © 1996, 1997 Andreas Dilger

Distributed according to the same disclaimer and license as libpng-0.88, with the following individuals added to the list of Contributing Authors:

John Bowler

Kevin Bracey

Sam Bushell

Magnus Holmgren

Greg Roelofs

Tom Tanner

libpng versions 0.5, May 1995, through 0.88, January 1996, are Copyright © 1995, 1996 Guy Eric Schalnat, Group 42, Inc.

For the purposes of this copyright and license, “Contributing Authors” is defined as the following set of individuals:

Andreas Dilger

Dave Martindale

Guy Eric Schalnat

Paul Schmidt

Tim Wegner

The PNG Reference Library is supplied “AS IS”. The Contributing Authors and Group 42, Inc. disclaim all warranties, expressed or implied, including, without limitation, the warranties of merchantability and of fitness for any purpose. The Contributing Authors and Group 42, Inc. assume no liability for direct, indirect, incidental, special, exemplary, or consequential damages, which may result from the use of the PNG Reference Library, even if advised of the possibility of such damage.

Permission is hereby granted to use, copy, modify, and distribute this source code, or portions hereof, for any purpose, without fee, subject to the following restrictions:

1. The origin of this source code must not be misrepresented.

2. Altered versions must be plainly marked as such and must not be misrepresented as being the original source.

3. This Copyright notice may not be removed or altered from any source or altered source distribution.

The Contributing Authors and Group 42, Inc. specifically permit, without fee, and encourage the use of this source code as a component to supporting the PNG file format in commercial products. If you use this source code in a product, acknowledgment is not required but would be appreciated.

A “png_get_copyright” function is available, for convenient use in “about” boxes and the like:

printf("%s",png_get_copyright(NULL));

Also, the PNG logo (in PNG format, of course) is supplied in the files "pngbar.png" and "pngbar.jpg (88x31) and "pngnow.png" (98x31).

Libpng is OSI Certified Open Source Software. OSI Certified Open Source is a certification mark of the Open Source Initiative.

Glenn Randers-Pehrson

glennrp at users.sourceforge.net

February 14, 2009

Bzip2

This program, "bzip2", the associated library "libbzip2", and all documentation, are copyright (C) 1996-2007 Julian R Seward. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, jseward@bzip.org

USB library functions

Atmel Corporation

2325 Orchard Parkway
San Jose, Ca 95131

Copyright (c) 2004 Atmel

Apache

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer,

and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

D3 JS library

Compliance with safety standards

This section lists the safety specifications against which the PTP 650 has been tested and certified. It also describes how to keep RF exposure within safe limits.

Electrical safety compliance

The PTP 650 hardware has been tested for compliance to the electrical safety specifications listed in Table 61.

Table 61 PTP 650 safety compliance specifications

Region	Standard
USA	UL 60950-1, 2nd Edition; UL60950-22
Canada	CAN/CSA C22.2 No.60950-1-07, 2nd Edition; CAN/CSA C22.2 No.60950-22-07
EU	EN 60950-1:2006 + Amendment 12:2011, EN 60950-22
International	CB certified to IEC 60950-1: 2005 (modified); IEC 60950-22: 2005 (modified)

Electromagnetic compatibility (EMC) compliance

The PTP 650 complies with European EMC Specification EN301 489-1 with testing carried out to the detailed requirements of EN301 489-4.

Note

For EN 61000-4-2: 1995 to 2009 Electro Static Discharge (ESD), Class 2, 8 kV air, 4 kV contact discharge, the PTP 650 has been tested to ensure immunity to 15 kV air and 8 kV contact.

Table 62 lists the EMC specification type approvals that have been granted for PTP 650 products.

Table 62 EMC emissions compliance

Region	Specification (Type Approvals)
Europe	ETSI EN301 489-4

Human exposure to radio frequency energy

Relevant standards (USA and EC) applicable when working with RF equipment are:

- ANSI IEEE C95.1-1991, IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz.
- Council recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz) (1999/519/EC) and respective national regulations.
- *Directive 2004/40/EC of the European Parliament and of the Council of 29 April 2004* on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) (18th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC).
- US FCC limits for the general population. See the FCC web site at http://www.fcc.gov, and the policies, guidelines, and requirements in Part 1 of Title 47 of the Code of Federal Regulations, as well as the guidelines and suggestions for evaluating compliance in FCC OET Bulletin 65.
- Health Canada limits for the general population. See the Health Canada web site at http://www.hc-sc.gc.ca/ewh-semt/pubs/radiation/99ehd-dhm237/limits-limites_e.html and Safety Code 6.
- EN 50383:2002 to 2010 Basic standard for the calculation and measurement of electromagnetic field strength and SAR related to human exposure from radio base stations and fixed terminal stations for wireless telecommunication systems (110 MHz - 40 GHz).
- BS EN 50385:2002 Product standard to demonstrate the compliances of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110 MHz – 40 GHz) – general public.
- ICNIRP (International Commission on Non-Ionizing Radiation Protection) guidelines for the general public. See the ICNIRP web site at http://www.icnirp.de/ and Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields.

Power density exposure limit

Install the radios for the PTP 650 family of PTP wireless solutions so as to provide and maintain the minimum separation distances from all persons.

The applicable power density exposure limit for RF energy in the 4.9, 5.4 and 5.8 GHz frequency bands is **10 W/m^2**. For more information, see Human exposure to radio frequency energy on page 4-24.

Calculation of power density

The following calculation is based on the ANSI IEEE C95.1-1991 method, as that provides a worst case analysis. Details of the assessment to EN50383:2002 can be provided, if required.

Peak power density in the far field of a radio frequency point source is calculated as follows:

$$S = \frac{P.G}{4\pi d^2}$$

Where:	**Is:**
S	power density in W/m^2
P	maximum average transmit power capability of the radio, in W
G	total Tx gain as a factor, converted from dB
d	distance from point source, in m

Rearranging terms to solve for distance yields:

$$d = \sqrt{\frac{P.G}{4\pi.S}}$$

Calculated distances and power compliance margins

Table 63 shows calculated minimum separation distances, recommended distances and resulting margins for each frequency band and antenna combination. These are conservative distances that include compliance margins. At these and greater separation distances, the power density from the RF field is below generally accepted limits for the general population.

Explanation of terms used in Table 63:

Tx burst – maximum average transmit power in burst (Watt)

P – maximum average transmit power capability of the radio (Watt)

G – total transmit gain as a factor, converted from dB

S – power density (W/m^2)

d – minimum distance from point source (meters)

R – recommended distances (meters)

C – compliance factor

Table 63 Power compliance margins

Band	Antenna	Tx burst (W)	P (W)	G	S (W/m^2)	d (m)	R (m)	C
4.9 GHz	Integrated	0.25	0.2	158	10	0.5	2	4.0
	Connectorized	0.25	0.2	398	10	0.8	5	6.25
5.4 GHz	Integrated	0.005	0.004	200	10	0.08	1	12.5
	External 4ft Dish	0.00035	0.00028	2884	10	0.08		
5.8 GHz	Integrated	0.5	0.41	200	10	0.79	2.5	3.2
	External 2ft Flat Plate	0.5	0.41	631	10	1.26	6.3	5.0
	External 6ft Dish	0.5	0.41	6310	10	3.86	12.6	3.25

Note

Gain of antenna in dBi = 10*log(G).

The regulations require that the power used for the calculations is the maximum power in the transmit burst subject to allowance for source-based time-averaging.

At 5.4 GHz and EU 5.8 GHz, the products are generally limited to a fixed EIRP which can be achieved with the Integrated Antenna. The calculations above assume that the maximum EIRP allowed by the regulations is being transmitted.

Note

If there are no EIRP limits in the country of deployment, use the distance calculations for FCC 5.8 GHz for all frequency bands.

At FCC 5.8 GHz, for antennas between 0.6m (2ft) and 1.8m (6ft), alter the distance proportionally to the antenna gain.

Compliance with radio regulations

This section describes how the PTP 650 complies with the radio regulations that are in force in various countries.

Caution

Where necessary, the end user is responsible for obtaining any National licenses required to operate this product and these must be obtained before using the product in any particular country. Contact the appropriate national administrations for details of the conditions of use for the bands in question and any exceptions that might apply.

Caution

Changes or modifications not expressly approved by Cambium Networks could void the user's authority to operate the system.

Caution

For the connectorized version of the product and in order to reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the Effective Isotropically Radiated Power (EIRP) is not more than that permitted for successful communication.

Type approvals

The system has been tested against various local technical regulations and found to comply. The frequency band in which the system operates is "license exempt" and the system is allowed to be used provided it does not cause interference. The licensing authority does not guarantee protection against interference from other products and installations. Table 64, Table 65 and Table 66 list the radio specification type approvals that have been granted for PTP 650 products.

Table 64 Radio certifications (4.9 GHz)

Region	Regulatory approvals
USA	FCC 47 CFR Part 90
Canada	IC RSS-211, Issue 4
Europe	Europe EN302 625; V1.1.1 Broadband Disaster Relief (BBDR)

Table 65 Radio certifications (5.4 GHz)

Region	Regulatory approvals
USA	FCC 47 CFR Part 15 E
Canada	IC RSS-210 Issue 8, Annex 9 (or latest)
Europe	ETSI EN301 893 v1.6.1

Table 66 Radio certifications (5.8 GHz)

Region	Regulatory approvals
USA	FCC 47 CFR Part 15 C
Canada	IC RSS-210 Issue 8, Annex 8 (or latest)
Denmark	Radio Interface 00 007
Eire	ComReg 02/71R4
Germany	Order No 47/2007
Iceland	ETSI EN302 502 v1.2.1
Finland	ETSI EN302 502 v1.2.1
Greece	ETSI EN302 502 v1.2.1
Liechtenstein	ETSI EN302 502 v1.2.1
Norway	REG 2009-06-02 no. 580
Portugal	ETSI EN302 502 v1.2.1
Serbia	ETSI EN302 502 v1.2.1
Spain	CNAF 2010
Switzerland	ETSI EN302 502 v1.2.1
UK	UK IR 2007

FCC/IC compliance

The PTP 650 complies with the regulations that are in force in the USA and Canada.

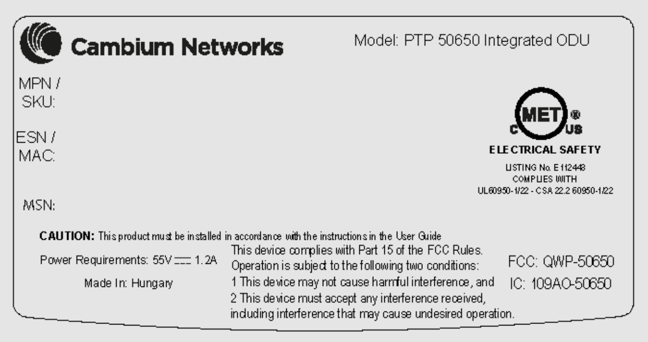
Caution

If this equipment does cause interference to radio or television reception, refer to Radio and television interference on page 8-10 for corrective actions.

FCC/IC product labels

FCC IDs and Industry Canada Certification Numbers are reproduced on the product labels (Figure 53 and Figure 54).

Figure 53 FCC and IC certifications on integrated ODU product label



Cambium Networks

Model: PTP 50650 Integrated ODU

MPN / SKU:

ESN / MAC:

MSN:

MET ® C US
ELECTRICAL SAFETY
LISTING No. E112448
COMPLIES WITH
UL60950-1/22 - CSA 22.2 60950-1/22

CAUTION: This product must be installed in accordance with the instructions in the User Guide

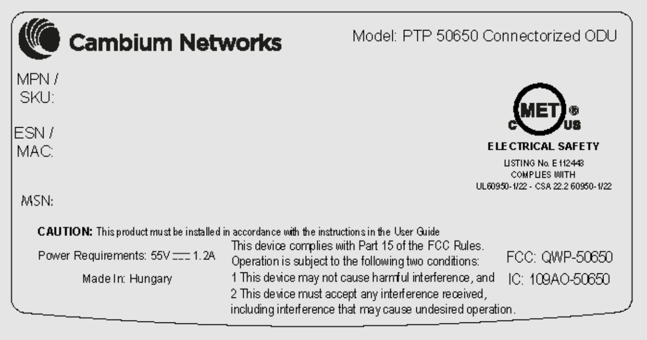
Power Requirements: 55V ⎓ 1.2A

Made In: Hungary

This device complies with Part 15 of the FCC Rules.
Operation is subject to the following two conditions:
1 This device may not cause harmful interference, and
2 This device must accept any interference received,
including interference that may cause undesired operation.

FCC: QWP-50650
IC: 109AO-50650

Figure 54 FCC and IC certifications on connectorized ODU product label



Cambium Networks

Model: PTP 50650 Connectorized ODU

MPN / SKU:

ESN / MAC:

MSN:

MET ® C US
ELECTRICAL SAFETY
LISTING No. E112448
COMPLIES WITH
UL60950-1/22 - CSA 22.2 60950-1/22

CAUTION: This product must be installed in accordance with the instructions in the User Guide

Power Requirements: 55V ⎓ 1.2A

Made In: Hungary

This device complies with Part 15 of the FCC Rules.
Operation is subject to the following two conditions:
1 This device may not cause harmful interference, and
2 This device must accept any interference received,
including interference that may cause undesired operation.

FCC: QWP-50650
IC: 109AO-50650

4.9 GHz FCC and IC notification

The system has been approved under FCC Part 90 and Industry Canada RSS-111 for Public Safety Agency usage. The installer or operator is responsible for obtaining the appropriate site licenses before installing or using the system.

5.4 GHz FCC and IC notification

This device complies with part 15.407 of the US FCC Rules and Regulations and with Industry Canada RSS-210 Annex 9. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation. In Canada, users should be cautioned to take note that high power radars are allocated as primary users (meaning they have priority) of 5250 – 5350 MHz and 5470 – 5725 MHz and these radars could cause interference and/or damage to license-exempt local area networks (LELAN).

For the connectorized version of the product and in order to reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that permitted by the regulations. The transmitted power must be reduced to achieve this requirement.

5.8 GHz FCC notification

This device complies with part 15 of the US FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

5.8 GHz IC notification

RSS-GEN issue 3 (7.1.3) Licence-Exempt Radio Apparatus:

> This device complies with Industry Canada license-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.
>
> *Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.*

In Canada, high power radars are allocated as primary users (meaning they have priority) of the 5650 – 5850 MHz spectrum. These radars could cause interference or damage to license-exempt local area network (LE-LAN) devices.

European Union compliance

The PTP 650 complies with the regulations that are in force in the European Union.

Caution

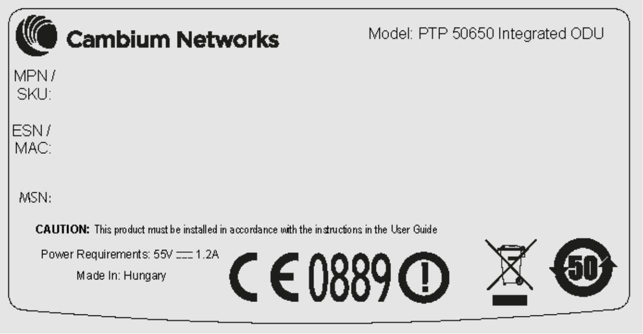
This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

If this equipment does cause interference to radio or television reception, refer to Radio and television interference on page 8-10 for corrective actions.

EU product labels

The European R&TTE directive 1999/5/EC Certification Number is reproduced on the product labels (Figure 55 and Figure 56).

Figure 55 European Union certification on integrated product label



Cambium Networks

Model: PTP 50650 Integrated ODU

MPN / SKU:

ESN / MAC:

MSN:

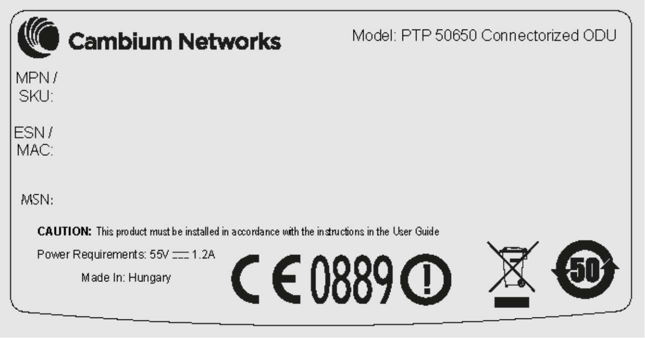
CAUTION: This product must be installed in accordance with the instructions in the User Guide

Power Requirements: 55V ⎓ 1.2A

Made In: Hungary

CE 0889 ⓘ

Figure 56 European Union certification on connectorized product label



Cambium Networks

Model: PTP 50650 Connectorized ODU

MPN / SKU:

ESN / MAC:

MSN:

CAUTION: This product must be installed in accordance with the instructions in the User Guide

Power Requirements: 55V ⎓ 1.2A

Made In: Hungary

CE 0889 ⓘ

5.4 GHz European Union notification

The PTP 650 product is a two-way radio transceiver suitable for use in Broadband Wireless Access System (WAS), Radio Local Area Network (RLAN), or Fixed Wireless Access (FWA) systems. It is a Class 1 device and uses operating frequencies that are harmonized throughout the EU member states. The operator is responsible for obtaining any national licenses required to operate this product and these must be obtained before using the product in any particular country.

Hereby, Cambium Networks declares that the PTP 650 product complies with the essential requirements and other relevant provisions of Directive 1999/5/EC. The declaration of conformity may be consulted at the support website (see Contacting Cambium Networks on page 1).

5.8 GHz European Union notification

The PTP 650 is a Class 2 device as it operates on frequencies that are not harmonized across the EU. Currently the product may only be operated in the countries listed in Table 66. However, the regulatory situation in Europe is changing and the radio spectrum may become available in other countries in future. See www.ero.dk for further information. The operator is responsible for obtaining any national licenses required to operate this product and these must be obtained before using the product in any particular country.

⚠ **Caution**

This equipment operates as a secondary application, so it has no rights against harmful interference, even if generated by similar equipment, and must not cause harmful interference on systems operating as primary applications.

Hereby, Cambium Networks declares that the PTP 650 product complies with the essential requirements and other relevant provisions of Directive 1999/5/EC. The declaration of conformity may be consulted at the support website (see Contacting Cambium Networks on page 1).

5.8 GHz operation in the UK

The PTP 650 connectorized product has been notified for operation in the UK, and when operated in accordance with instructions for use it is compliant with UK Interface Requirement IR2007. For UK use, installations must conform to the requirements of IR2007 in terms of EIRP spectral density against elevation profile above the local horizon in order to protect Fixed Satellite Services. The frequency range 5795-5815 MHz is assigned to Road Transport & Traffic Telematics (RTTT) in the U.K. and shall not be used by FWA systems in order to protect RTTT devices. UK Interface Requirement IR2007 specifies that radiolocation services shall be protected by a Dynamic Frequency Selection (DFS) mechanism to prevent co-channel operation in the presence of radar signals.

Chapter 5: Installation

This chapter describes how to install and test the hardware for a PTP 650 link. It contains the following topics:

- Safety on page 5-2 contains important safety guidelines that must be observed by personnel installing or operating PTP 650 equipment.
- Installing the ODU and top LPU on page 5-5 describes how to mount and ground an integrated or connectorized ODU, how to mount and ground the top LPU, and how to mount and connect an external antenna for the connectorized ODU.
- Installing the copper Cat5e Ethernet interface on page 5-13 describes how to install the copper Cat5e power over Ethernet interface from the ODU (PSU port) to the PSU.
- Installing the PSU on page 5-21 describes how to install a power supply unit for the PTP 650, either the AC Power Injector or the AC+DC Enhanced Power Injector.
- Installing an SFP Ethernet interface on page 5-23 describes how to install an optical or copper Cat5e Ethernet interface from the ODU (SFP port) to a connected device.
- Installing an Aux Ethernet interface on page 5-32 describes how to install a copper Cat5e Ethernet interface from the ODU (Aux port) to a connected device.
- Supplemental installation information on page 5-33 contains detailed installation procedures that are not included in the above topics, such as how to strip cables, create grounding points and weatherproof connectors.

Note

These instructions assume that LPUs are being installed from the PTP 650 LPU and grounding kit (Cambium part number C000065L007). If the installation does not require LPUs, adapt these instructions as appropriate.

If LPUs are being installed, only use the five black-capped EMC cable glands supplied in the LPU and grounding kit. The silver-capped cable glands supplied in the ODU kits must only be used in PTP 650 installations which do not require LPUs.

Safety

Warning

To prevent loss of life or physical injury, observe the following safety guidelines. In no event shall Cambium Networks be liable for any injury or damage caused during the installation of the Cambium PTP 650. Ensure that only qualified personnel install a PTP 650 link.

Power lines

Exercise extreme care when working near power lines.

Working at heights

Exercise extreme care when working at heights.

PSU

Always use one of the Cambium PTP 650 Series power supply units (PSU) to power the ODU. Failure to use a Cambium supplied PSU could result in equipment damage and will invalidate the safety certification and may cause a safety hazard.

Grounding and protective earth

The Outdoor Unit (ODU) must be properly grounded to protect against lightning. It is the user's responsibility to install the equipment in accordance with national regulations. In the USA follow the requirements of the National Electrical code NFPA 70-2005 and 780-2004 *Installation of Lightning Protection Systems*. In Canada, follow Section 54 of the *Canadian Electrical Code*. These codes describe correct installation procedures for grounding the outdoor unit, mast, lead-in wire and discharge unit, size of grounding conductors and connection requirements for grounding electrodes. Other regulations may apply in different countries and therefore it is recommended that installation of the outdoor unit be contracted to a professional installer.

DC supply

To power the ODU from a DC supply, use the AC+DC Enhanced Power Injector (PSU) (Cambium part number C000065L002). Ensure that the DC power supply meets the requirements specified in PSU DC power supply on page 3-12.

Powering down before servicing

Before servicing PTP 650 equipment, always switch off the power supply and unplug it from the PSU.

Do not disconnect the RJ45 drop cable connectors from the ODU while the PSU is connected to the power supply. Always remove the AC or DC input power from the PSU.

Primary disconnect device

The main power supply is the primary disconnect device. The AC+DC Enhanced power injector is fused on the DC input. Some installations will also require an additional circuit breaker or isolation switch to be fitted in the DC supply.

External cables

Safety may be compromised if outdoor rated cables are not used for connections that will be exposed to the outdoor environment. For outdoor copper Cat5e Ethernet interfaces, always use Cat5e cable that is gel-filled and shielded with copper-plated steel. Alternative types of drop cable are not supported by Cambium Networks.

Drop cable tester

The PSU output voltage may be hazardous in some conditions, for example in wet weather. Do NOT connect the drop cable tester to the PSU, either directly or via LPUs.

RF exposure near the antenna

Strong radio frequency (RF) fields will be present close to the antenna when the transmitter is on. Always turn off the power to the ODU before undertaking maintenance activities in front of the antenna.

Minimum separation distances

Ensure that personnel are not exposed to unsafe levels of RF energy. The units start to radiate RF energy as soon as they are powered up. Never work in front of the antenna when the ODU is powered. Install the ODUs so as to provide and maintain the minimum separation distances from all persons. For minimum separation distances, see Calculated distances and power compliance margins on page 4-25.

Grounding and lightning protection requirements

Ensure that the installation meets the requirements defined in Grounding and lightning protection on page 3-8.

Grounding cable installation methods

To provide effective protection against lightning induced surges, observe these requirements:

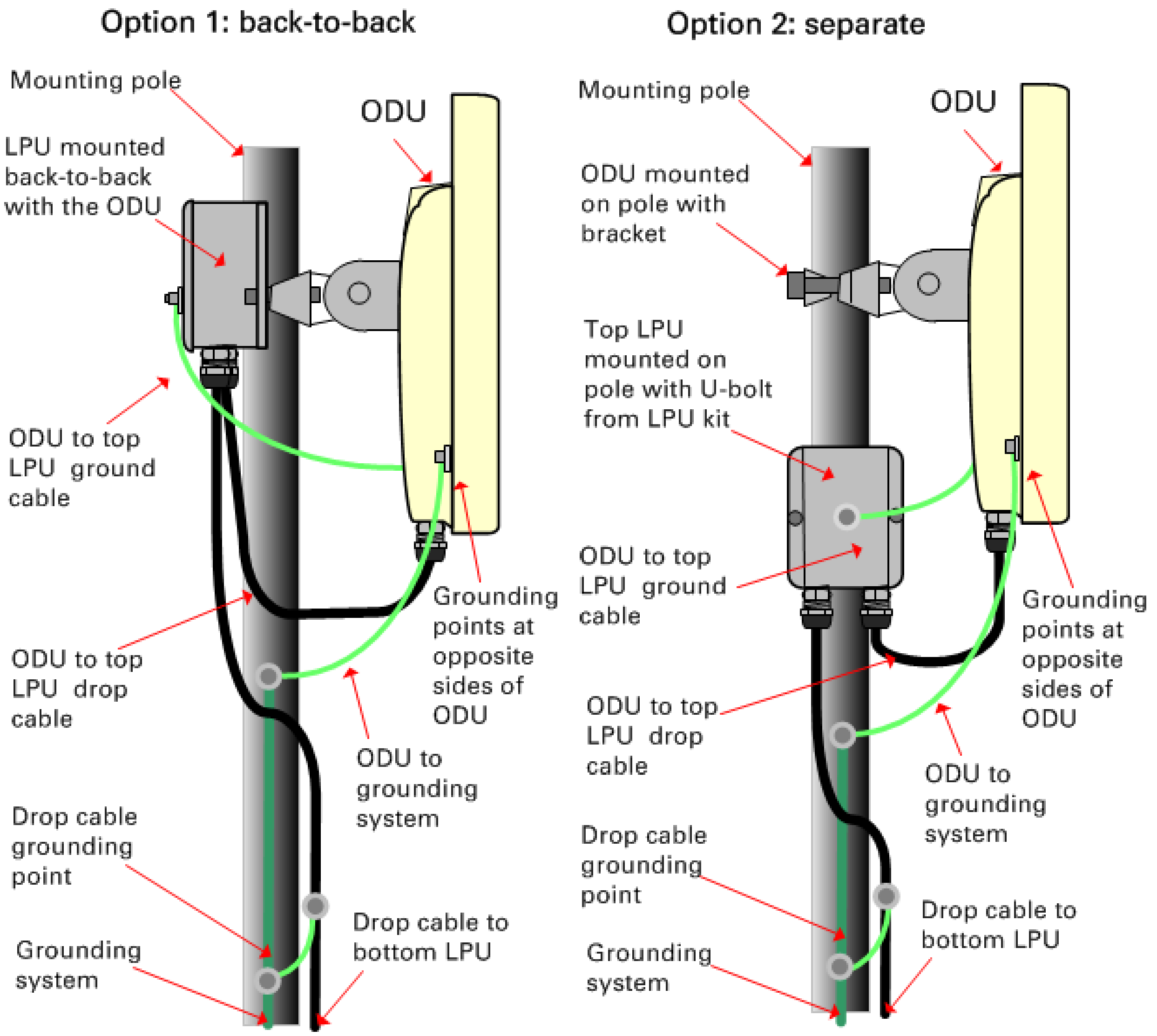
- Grounding conductor runs are as short, straight and smooth as possible, with bends and curves kept to a minimum.
- Grounding cables must not be installed with drip loops.
- All bends must have a minimum radius of 203 mm (8 in) and a minimum angle of 90°. A diagonal run is preferable to a bend, even though it does not follow the contour or run parallel to the supporting structure.
- All bends, curves and connections must be routed towards the grounding electrode system, ground rod, or ground bar.
- Grounding conductors must be securely fastened.
- Braided grounding conductors must not be used.
- Approved bonding techniques must be used for the connection of dissimilar metals.

Siting ODUs and antennas

ODUs and external antennas are not designed to survive direct lightning strikes. For this reason they must be installed in Zone B as defined in Lightning protection zones on page 3-8. Mounting in Zone A may put equipment, structures and life at risk.

Installing the ODU and top LPU

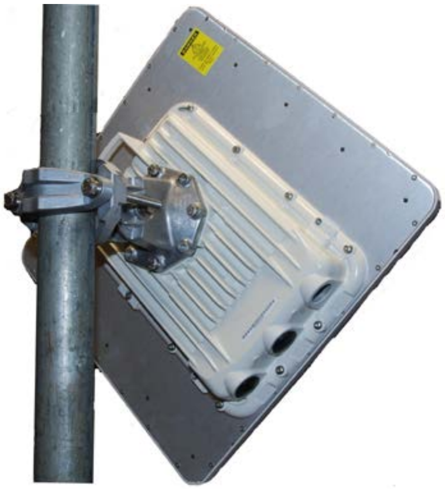
Decide how to mount the ODU and top LPU


Option 1: back-to-back
Mounting pole
ODU
LPU mounted back-to-back with the ODU
ODU to top LPU ground cable
Grounding points at opposite sides of ODU
ODU to top LPU drop cable
ODU to grounding system
Drop cable grounding point
Drop cable to bottom LPU
Grounding system
Option 2: separate
Mounting pole
ODU
ODU mounted on pole with bracket
Top LPU mounted on pole with U-bolt from LPU kit
ODU to top LPU ground cable
Grounding points at opposite sides of ODU
ODU to top LPU drop cable
ODU to grounding system
Drop cable grounding point
Drop cable to bottom LPU
Grounding system

Note

For improved radio performance, mount the integrated ODU at 45 degrees to the vertical.

The mounting pole may be vertical or horizontal.



Prepare ODU for mounting

1 Use the correct mounting bracket for the pole diameter and ODU type:

- If pole diameter is between 50 and 75 mm (2 and 3 inches):

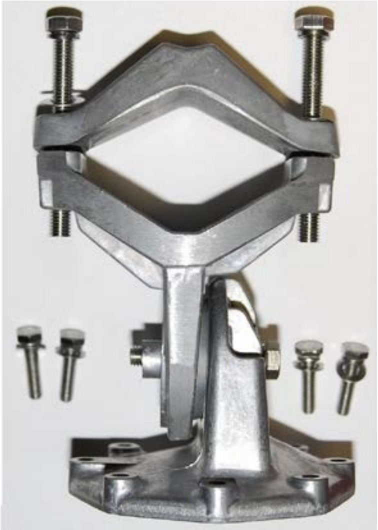
  (a) For an integrated ODU, use the integrated mounting bracket, Cambium part number N000065L031.

  (b) For a connectorized ODU, use the connectorized mounting bracket supplied with the ODU (alternatively, use the integrated ODU bracket).

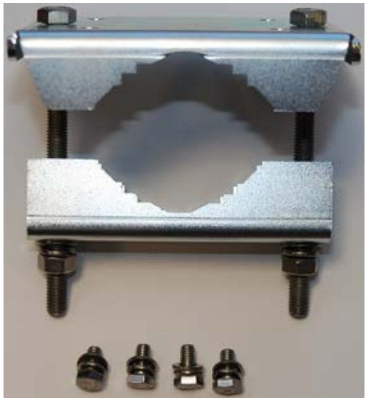
- If pole diameter is **either** 90 mm (3.5 inches) **or** 115 mm (4.5 inches):

  (c) For both integrated and connectorized ODUs, use the extended mounting bracket, Cambium part number N000065L030.

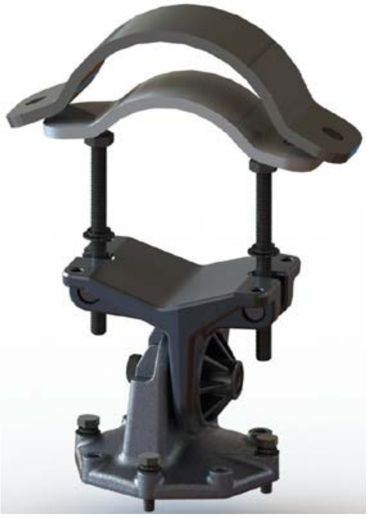
(a) Integrated bracket:



(b) Connectorized bracket:

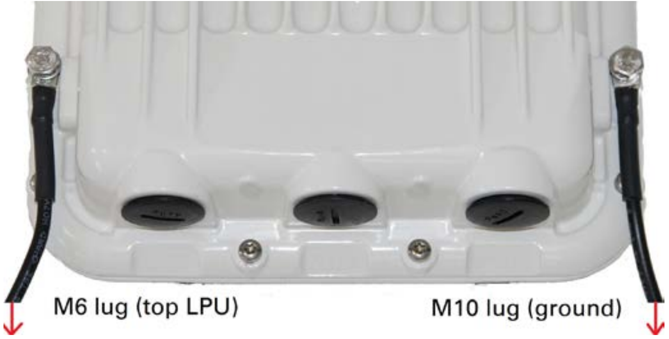


(c) Extended bracket:

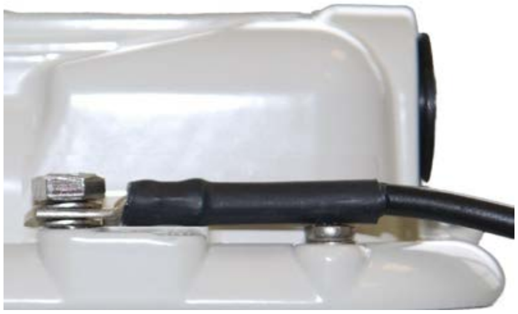


2 (a) Fasten one ground cable to each ODU grounding point using the M6 (small) lugs: one is for the top LPU (M6 lug at other end) and the other is for the tower or building (M10 lug at other end). It does not matter which cable goes on which ODU grounding point. (b) Tighten both ODU grounding bolts to a torque of 5 Nm (3.9 lb ft).

(a) ODU ground cables:



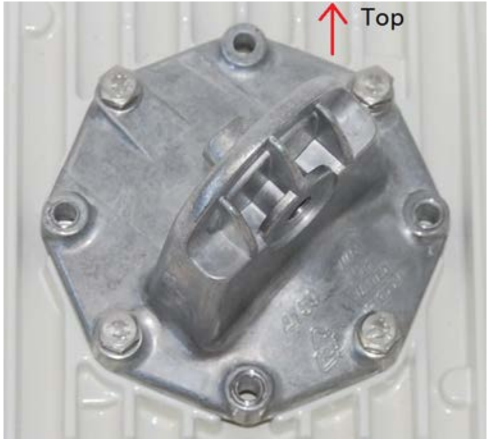
(b) ODU ground cable tightened:



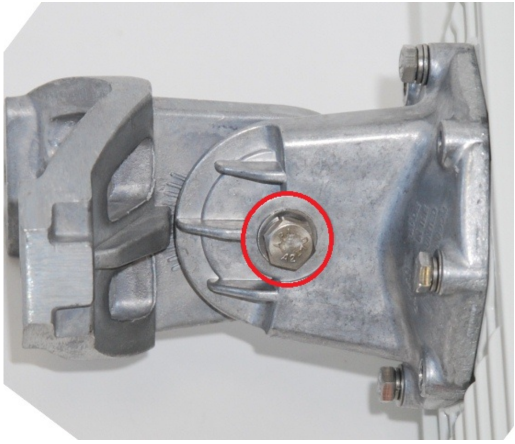
Integrated ODU

1 (a) Fix the mounting plate to the back of the ODU at an angle of 45 degrees to the vertical using the bolts and washers provided. Tighten the four bolts to a torque setting of 5 Nm (4 lb ft). (b) Fix the bracket body to the mounting plate using the M8 bolt.

(a) Fix the mounting plate:



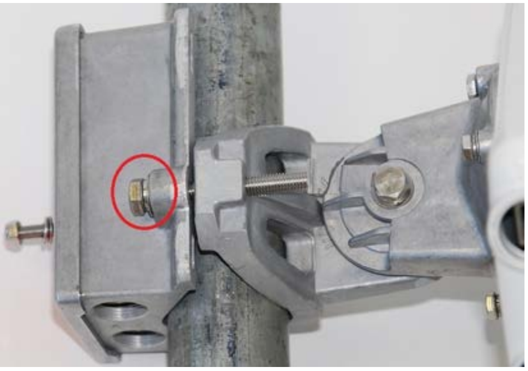
(b) Fix the bracket body:



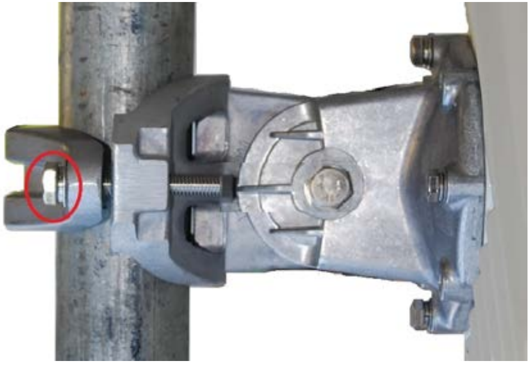
2 Hoist the ODU up to its position on the mounting pole.

3 (a) For back-to-back LPU mounting, fix the ODU to the pole using the LPU.
(b) For separate LPU mounting, fix the ODU to the pole using the bracket strap.

(a) Back-to-back LPU:

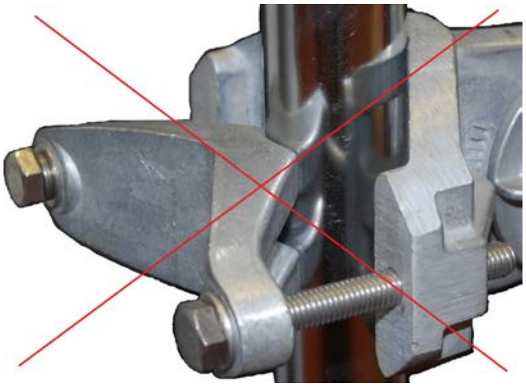


(b) Separate LPU:

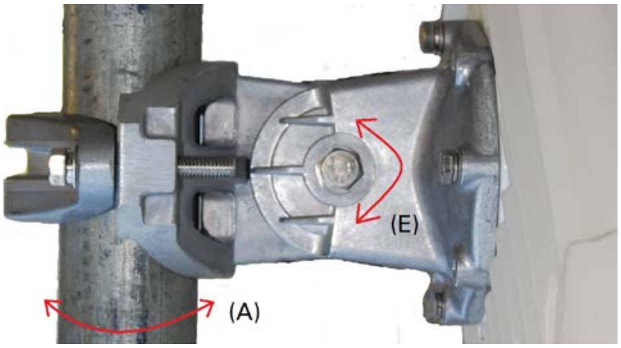


Caution

Do not reverse the ODU bracket strap, as this arrangement may lead to failure of the assembly:



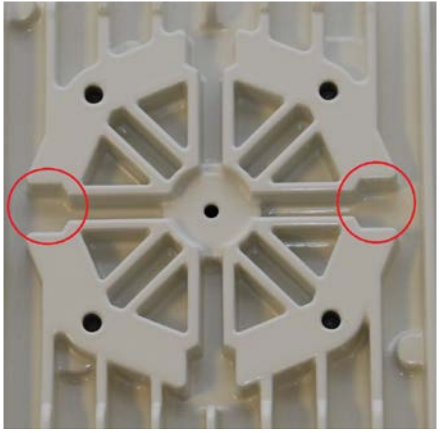
4 Adjust the elevation (E) and azimuth (A) of the unit to achieve initial alignment. Tighten all three M8 ODU bracket bolts to a torque setting of 14 Nm (11 lb ft). Do not over-tighten the bolts, as this may lead to failure of the assembly:



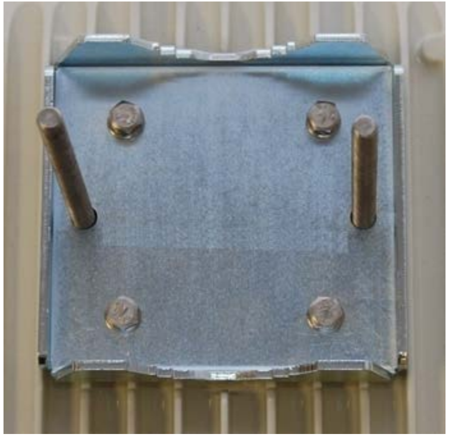
Connectorized ODU

1 (a) Line up the bolt heads with receptacles in the ODU. (b) Fix the mounting plate and bracket bolts to the back of the ODU using the bolts and washers. Tighten to a torque setting of 5 Nm (4 lb ft).

(a) Receptacles for bracket bolts:



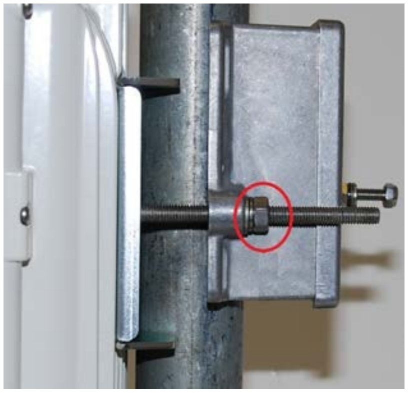
(b) Mounting plate fixed:



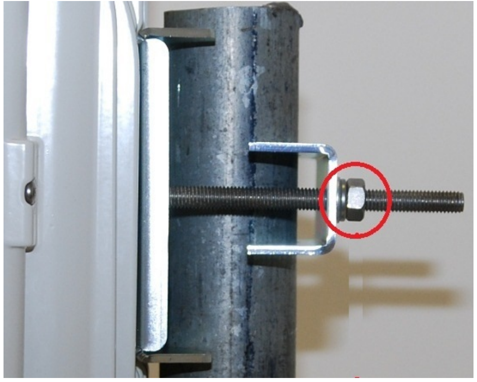
2 Hoist the ODU up to its position on the mounting pole.

3 (a) For back-to-back LPU mounting, fix the ODU to the pole using the LPU.
(b) For separate LPU mounting, fix the ODU to the pole using the bracket strap.

(c) Back-to-back LPU:



(d) Separate LPU:



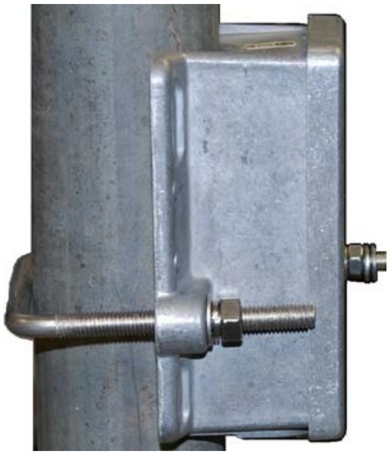
4 Tighten the mounting bolts to a torque setting of 7 Nm (5.5 lb ft). Do not over-tighten the bolts, as this may lead to failure of the assembly.

Ground the ODU and top LPU

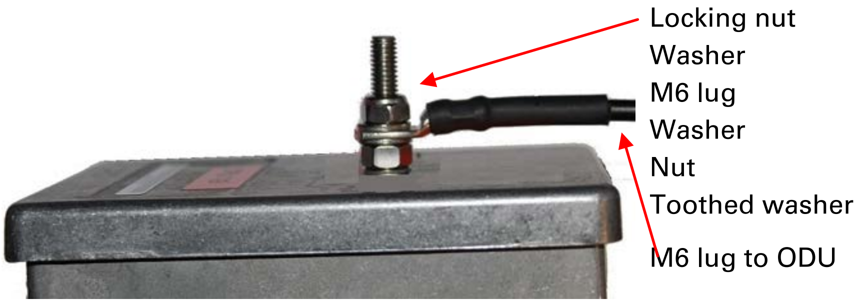
Caution

Do not attach grounding cables to the ODU mounting bracket bolts, as this arrangement will not provide full protection.

1 For separate LPU mounting, use the U-bolt bracket from the LPU kit to mount the top LPU on the pole below the ODU. Tighten to a torque setting of 7 Nm (5.5 lb ft):



2 Fasten the ODU grounding cable to the top LPU using the M6 (small) lug. Tighten both nuts to a torque of 5 Nm (3.9 lb ft):



3 Select a tower or building grounding point within 0.3 meters (1 ft) of the ODU bracket. Remove paint from the surface and apply anti-oxidant compound. Fasten the ODU grounding cable to this point using the M10 (large) lug.

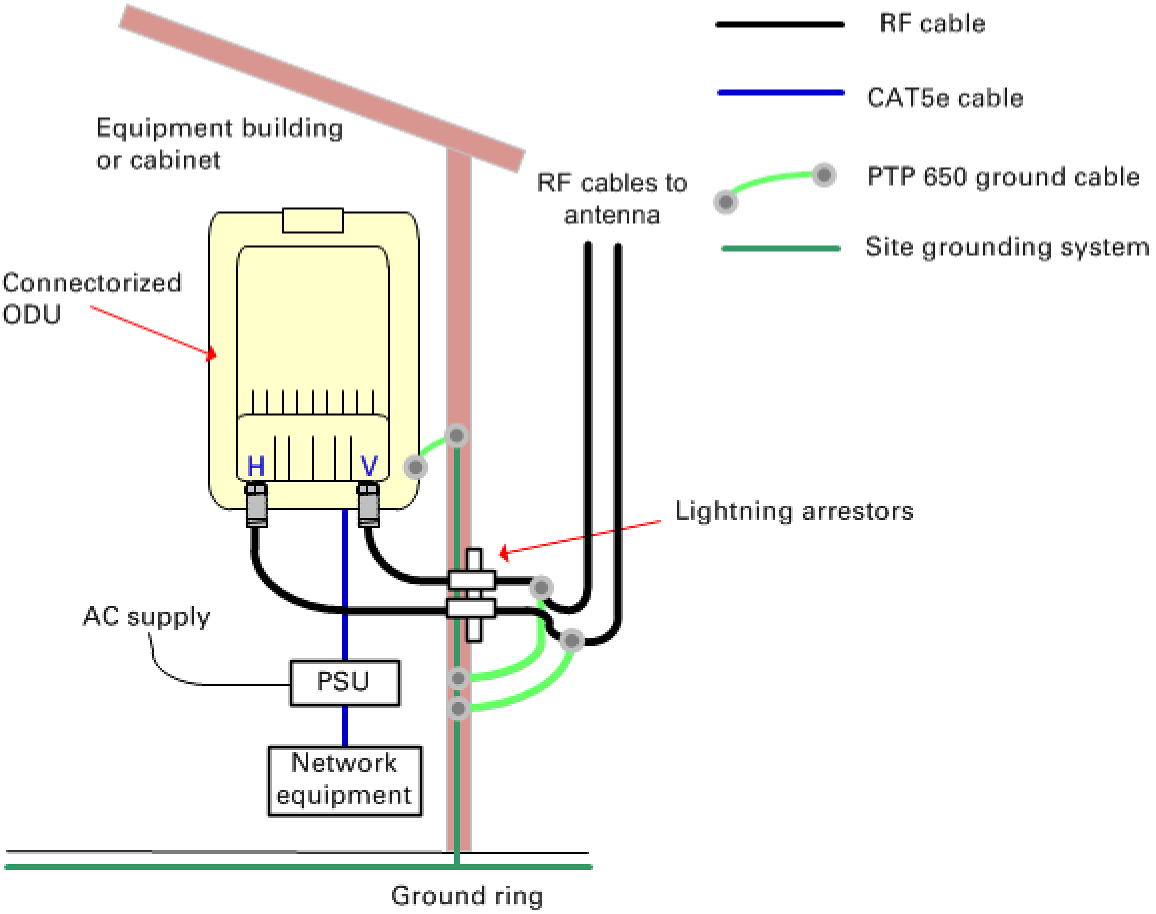
4 If local regulations mandate the independent grounding of all devices, add a third ground cable to connect the top LPU directly to the grounding system.

Install external antennas for a connectorized ODU

1 Mount the antenna(s) according to manufacturer's instructions. When using separate antennas to achieve spatial diversity, mount one with Horizontal polarization and the other with Vertical polarization.

2 Connect the ODU V and H interfaces to the antenna(s) with RF cable of type CNT-400 (Cambium part numbers 30010194001 and 30010195001) and N type connectors (Cambium part number 09010091001). Tighten the N type connectors to a torque setting of 1.7 Nm (1.3 lb ft).

3 If the ODU is mounted indoors, install lightning arrestors at the building entry point:

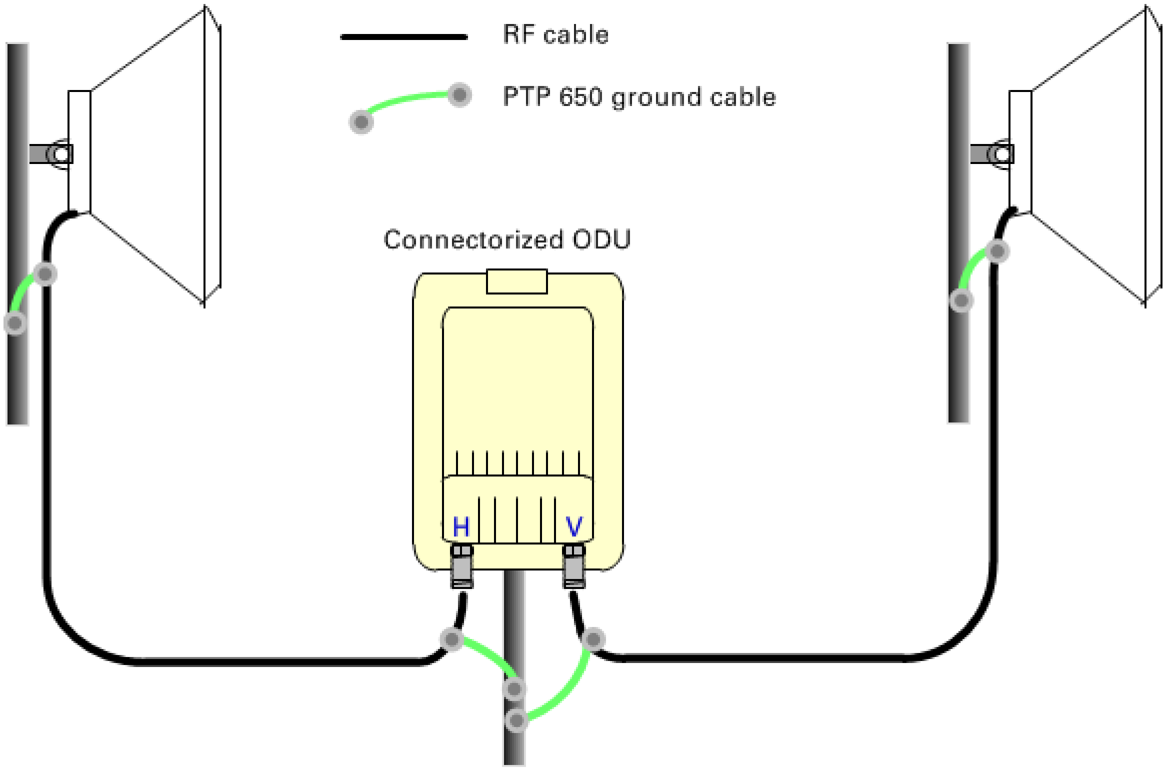


4 Form drip loops near the lower ends of the antenna cables. These ensure that water is not channeled towards the connectors.

5 If the ODU is mounted outdoors, weatherproof the N type connectors (when antenna alignment is complete) using PVC tape and self-amalgamating rubber tape.

6 Weatherproof the antenna connectors in the same way (unless the antenna manufacturer specifies a different method).

7 Ground the antenna cables to the supporting structure within 0.3 meters (1 foot) of the ODU and antennas using the Cambium grounding kit (part number 01010419001):



8 Fix the antenna cables to the supporting structure using site approved methods. Ensure that no undue strain is placed on the ODU or antenna connectors.

Caution

Ensure that the cables do not flap in the wind, as flapping cables are prone to damage and induce unwanted vibrations in the supporting structure.

Installing the copper Cat5e Ethernet interface

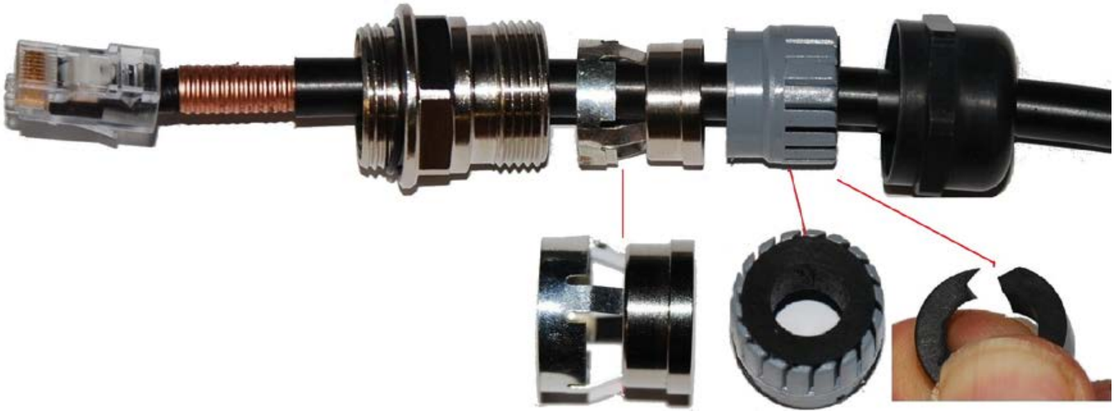
⚠	**Caution** To avoid damage to the installation, do not connect or disconnect the drop cable when power is applied to the PSU or network terminating equipment.
⚠	**Caution** Do not connect the SFP or Aux drop cables to the PSU, as this may damage equipment.
⚠	**Caution** Always use Cat5e cable that is gel-filled and shielded with copper-plated steel. Alternative types of Cat5e cable are not supported by Cambium Networks. Cambium Networks supply this cable (Cambium part numbers WB3175 and WB3176), RJ45 connectors (Cambium part number WB3177) and a crimp tool (Cambium part number WB3211). The LPU and grounding kit contains a 600 mm length of this cable.

Install the ODU to top LPU drop cable

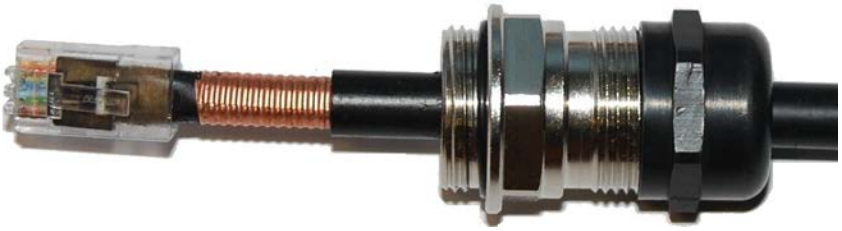
Fit glands to the ODU to top LPU drop cable

Fit EMC strain relief cable glands (with black caps) to both ends of the 600 mm length of pre-terminated cable. These parts are supplied in the LPU and grounding kit.

1 Disassemble the gland and thread each part onto the cable (the rubber bung is split). Assemble the spring clip and the rubber bung:



2 Fit the parts into the body and lightly screw on the gland nut (do not tighten it):

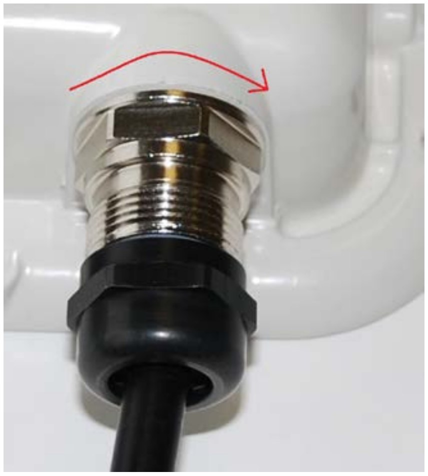


Connect the drop cable to the ODU (PSU port) and LPU

1 (a) Plug the RJ45 connector into the socket in the unit, ensuring that it snaps home.
(b) Fit the gland body to the RJ45 port and tighten it to a torque of 5.5 Nm (4.3 lb ft):

(a)

(b)

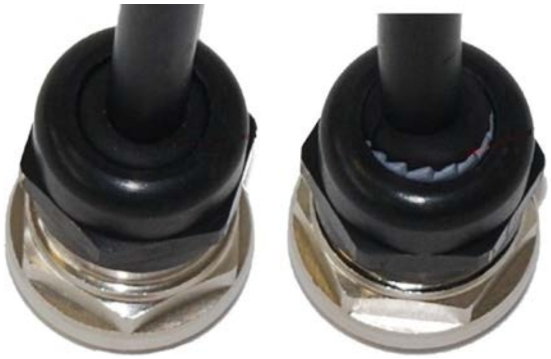


2 (a) Fit the gland nut and tighten until the rubber seal closes on the cable. (b) Do not over-tighten the gland nut, as there is a risk of damage to its internal components:

(a)

(b)

Correct Incorrect

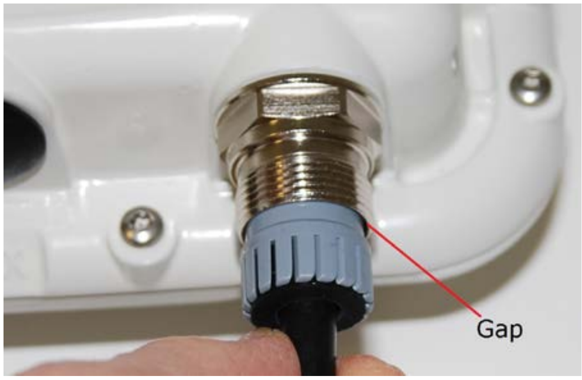


Disconnect the drop cable from the LPU or ODU

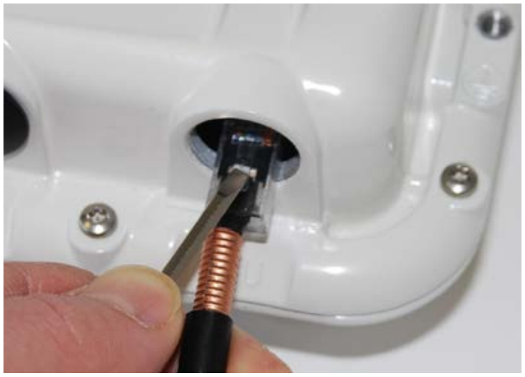
Use this procedure if it is necessary to remove an EMC strain relief cable gland and RJ45 connector from the ODU (as illustrated) or LPU.

1 (a) Remove the gland nut. Wiggle the drop cable to release the tension of the gland body. When the tension in the gland body is released, a gap opens at the point show. Unscrew the gland body.
(b) Use a small screwdriver to press the RJ45 locking tab, then remove the RJ45 connector.

(a)



(b)



Install the main drop cable

Warning

The metal screen of the drop cable is very sharp and may cause personal injury.

- ALWAYS wear cut-resistant gloves (check the label to ensure they are cut resistant).
- ALWAYS wear protective eyewear.
- ALWAYS use a rotary blade tool to strip the cable (DO NOT use a bladed knife).

Warning

Failure to obey the following precautions may result in injury or death:

- Use the proper hoisting grip for the cable being installed. If the wrong hoisting grip is used, slippage or insufficient gripping strength will result.
- Do not reuse hoisting grips. Used grips may have lost elasticity, stretched, or become weakened. Reusing a grip can cause the cable to slip, break, or fall.
- The minimum requirement is one hoisting grip for each 60 m (200 ft) of cable.

Cut to length and fit hoisting grips

1. Cut the main drop cable to length from the top LPU to the bottom LPU.
2. Slide one or more hoisting grips onto the top end of the drop cable.
3. Secure the hoisting grip to the cable using a special tool, as recommended by the manufacturer.

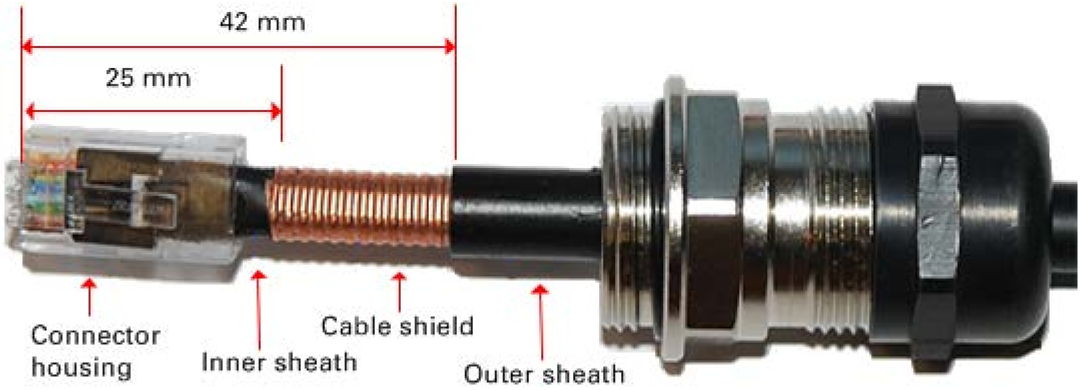
Terminate with RJ45 connectors and glands

Caution

Check that the crimp tool matches the RJ45 connector, otherwise the cable or connector may be damaged.

1. Thread the cable gland (with black cap) onto the main drop cable.
2. Strip the cable outer sheath and fit the RJ45 connector load bar.

3 Fit the RJ45 connector housing as shown. To ensure there is effective strain relief, locate the cable inner sheath under the connector housing tang. Do not tighten the gland nut:



Hoist and fix the main drop cable

Warning

Failure to obey the following precautions may result in injury or death:

- Use the hoisting grip to hoist one cable only. Attempting to hoist more than one cable may cause the hoisting grip to break or the cables to fall.
- Do not use the hoisting grip for lowering cable unless the clamp is securely in place.
- Maintain tension on the hoisting grip during hoisting. Loss of tension can cause dangerous movement of the cable and result in injury or death to personnel.
- Do not release tension on the grip until after the grip handle has been fastened to the supporting structure.
- Do not apply any strain to the RJ45 connectors.

Caution

Do not lay the drop cable alongside a lightning air terminal.

1 Hoist the top end of the main drop cable up to the top LPU, following the hoist manufacturer's instructions. When the cable is in position, fasten the grip handle to the supporting structure and remove the hoist line.

2 Connect the main drop cable to the top LPU by following the procedure Connect the drop cable to the ODU (PSU port) and LPU on page 5-14.

3 Run the main drop cable to the site of the bottom LPU.

4 Attach the main drop cable to the supporting structure using site approved methods.

Ground the main drop cable

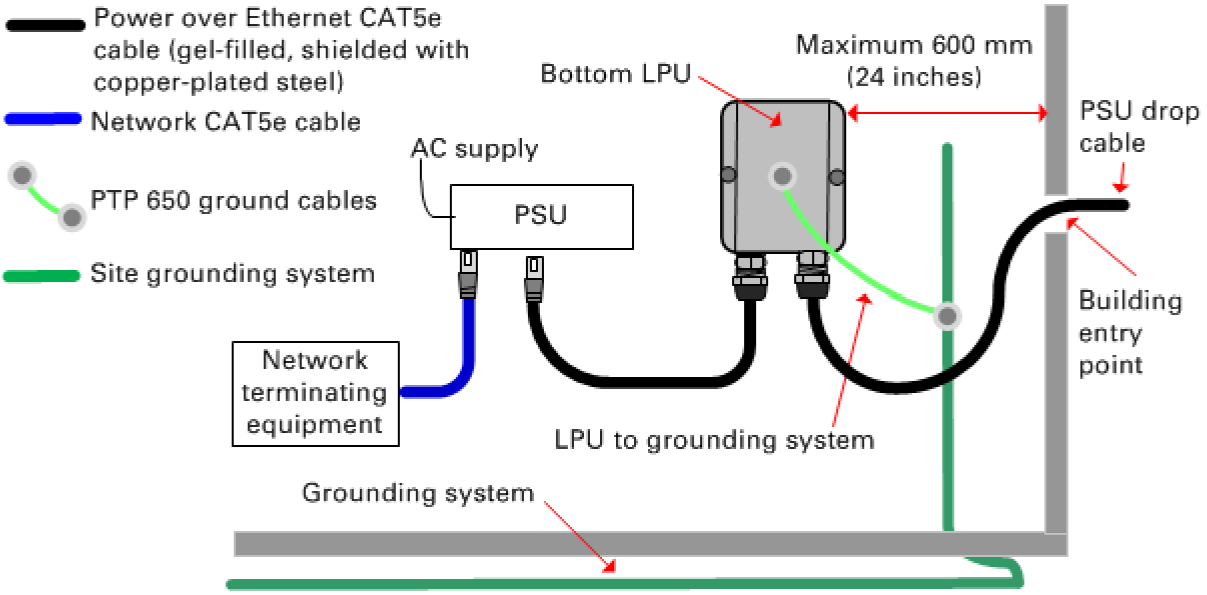
At all required grounding points, connect the screen of the main drop cable to the metal of the supporting structure using the cable grounding kit (Cambium part number 01010419001).

Install the bottom LPU to PSU drop cable

Install the bottom LPU

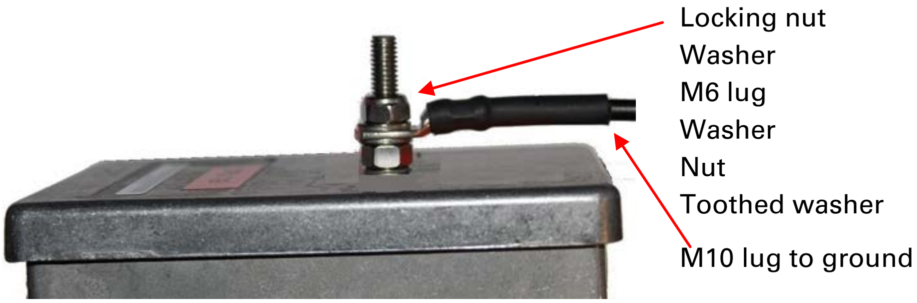
Install the bottom LPU, ground it, and connect it to the main drop cable.

1 Select a mounting point for the bottom LPU within 600 mm (24 in) of the building entry point. Mount the LPU vertically with cable glands facing downwards.



2 Connect the main drop cable to the bottom LPU by following the procedure Connect the drop cable to the ODU (PSU port) and LPU on page 5-14.

3 Fasten one ground cable to the bottom LPU using the M6 (small) lug. Tighten both nuts to a torque of 5 Nm (3.9 lb ft):



4 Select a building grounding point near the LPU bracket. Remove paint from the surface and apply anti-oxidant compound. Fasten the LPU ground cable using the M10 (large) lug.

Install the LPU to PSU drop cable

Use this procedure to terminate the bottom LPU to PSU drop cable with RJ45 connectors at both ends, and with a cable gland at the LPU end.

⚠ **Warning**

The metal screen of the drop cable is very sharp and may cause personal injury. ALWAYS wear cut-resistant gloves (check the label to ensure they are cut resistant). ALWAYS wear protective eyewear. ALWAYS use a rotary blade tool to strip the cable, not a bladed knife.

⚠ **Caution**

Check that the crimp tool matches the RJ45 connector, otherwise the cable or connector may be damaged.

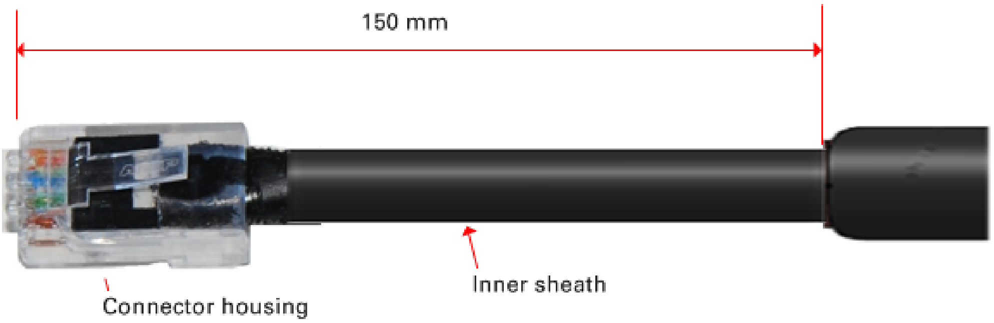
1 Cut the drop cable to the length required from bottom LPU to PSU.

2 **At the LPU end only**:

- Fit one cable gland and one RJ45 connector by following the procedure Terminate with RJ45 connectors and glands on page 5-16.

- Connect this cable and gland to the bottom LPU by following the procedure Connect the drop cable to the ODU (PSU port) and LPU on page 5-14.

4 **At the PSU end only**: Do not fit a cable gland. Strip the cable outer sheath and fit the RJ45 connector load bar. Fit the RJ45 connector housing. To ensure there is effective strain relief, locate the cable inner sheath under the connector housing tang:



Test resistance in the drop cable

Connect the bottom end of the copper Cat5e drop cable to a PTP drop cable tester and test that the resistances between pins are within the correct limits, as specified in the table below. If any of the tests fail, examine the drop cable for wiring faults. Order the PTP drop cable tester from the support website (http://www.cambiumnetworks.com/support).

Measure the resistance between...	Enter measured resistance	To pass test, resistance must be...	Circle “Pass” or “Fail”	Additional tests and notes
Pins 1 and 2	Ohms	<20 Ohms (60 Ohms) (*1)	Pass Fail	Resistances must be within 10% of each other (*2). Circle “Pass” or “Fail”: Pass Fail
Pins 3 and 6	Ohms	<20 Ohms (60 Ohms) (*1)	Pass Fail	
Pins 4 and 5	Ohms	<20 Ohms (60 Ohms) (*1)	Pass Fail	
Pins 7 and 8	Ohms	<20 Ohms (60 Ohms) (*1)	Pass Fail	
Pin 1 and screen (ODU ground)	K Ohms	>100K Ohms	Pass Fail	These limits apply regardless of cable length.
Pin 8 and screen (ODU ground)	K Ohms	>100K Ohms	Pass Fail	

(*1) A resistance of 20 Ohms is the maximum allowed when the cable is carrying Ethernet.
A resistance of 60 Ohms is the maximum allowed when the cable is carrying only power to the ODU (when Ethernet is carried by one of the other ODU interfaces).

(*2) Ensure that these resistances are within 10% of each other by multiplying the lowest resistance by 1.1 – if any of the other resistances are greater than this, the test has failed.

Installing the PSU

Install one of the following types of PSU (as specified in the installation plan):

- PTP 650 AC Power Injector (Cambium part number N000065L001).
- PTP 650 AC+DC Enhanced Power Injector (Cambium part number C000065L002).

Caution

As the PSU is not waterproof, locate it away from sources of moisture, either in the equipment building or in a ventilated moisture-proof enclosure. Do not locate the PSU in a position where it may exceed its temperature rating.

Caution

Do not plug any device other than a PTP 650 ODU into the ODU port of the PSU. Other devices may be damaged due to the non-standard techniques employed to inject DC power into the Ethernet connection between the PSU and the ODU.

Do not plug any device other than a Cambium PTP 650 PSU into the PSU port of the ODU. Plugging any other device into the PSU port of the ODU may damage the ODU and device.

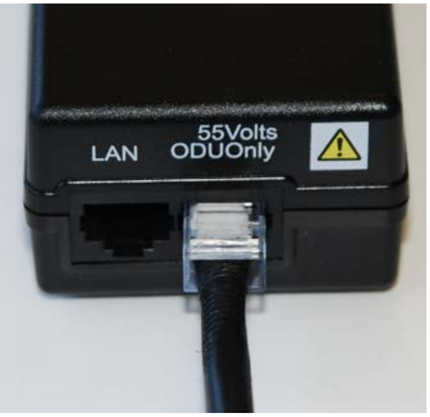
Installing the AC Power Injector

Follow this procedure to install the AC Power Injector (Cambium part number N000065L001):

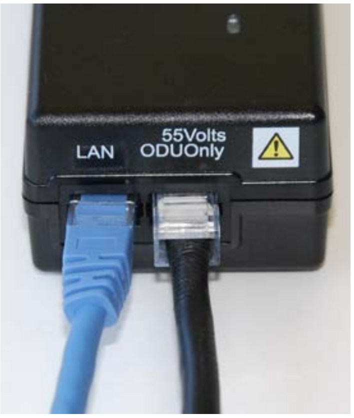
1 Form a drip loop on the PSU end of the LPU to PSU drop cable. The drip loop ensures that any moisture that runs down the cable cannot enter the PSU.

2 (a) Place the AC Power Injector on a horizontal surface. Plug the LPU to PSU drop cable into the PSU port labeled ODU. (b) When the system is ready for network connection, connect the network Cat5e cable to the LAN port of the PSU:

(a)



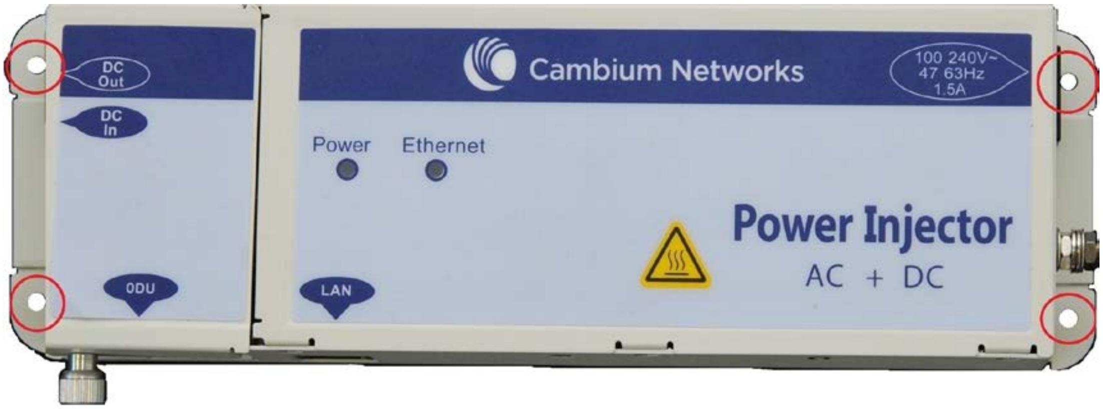
(b)



Installing the AC+DC Enhanced Power Injector

Follow this procedure to install the AC+DC Enhanced Power Injector (Cambium part number C000065L002):

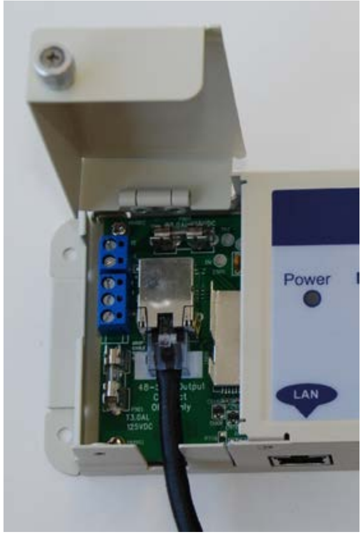
1 Mount the AC+DC power injector by screwing it to a vertical or horizontal surface using the four screw holes (circled):



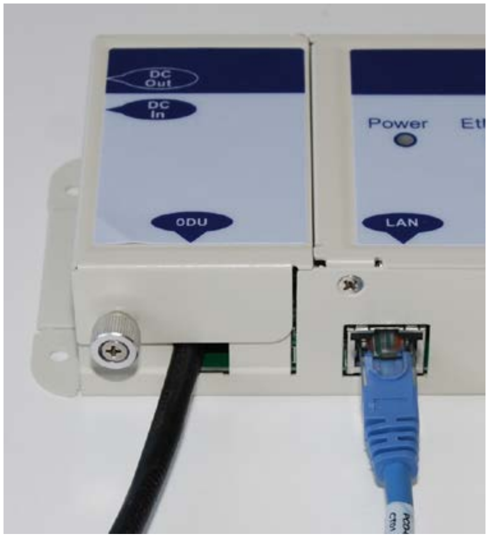
2 Form a drip loop on the PSU end of the LPU to PSU drop cable. The drip loop ensures that any moisture that runs down the cable into the cabinet or enclosure cannot enter the PSU.

3 (a) Undo the retaining screw, hinge back the cover and plug the drop cable into the port. (b) Close the cover and secure with the screw. (c) When the system is ready for network connection, connect the network Cat5e cable to the LAN port of the PSU:

(a)



(b) and (c)



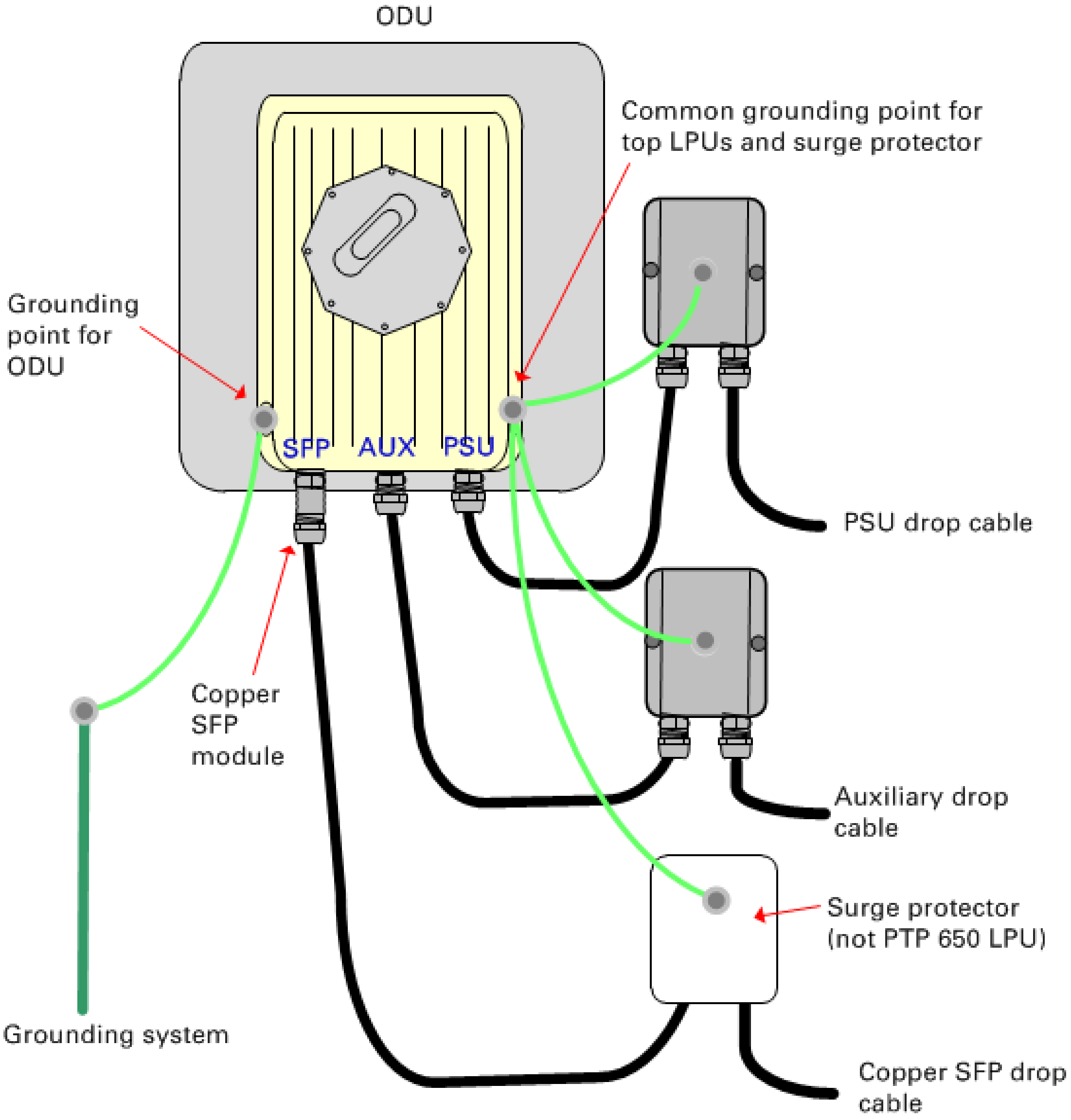
Installing an SFP Ethernet interface

In more advanced configurations, there may be an optical or copper Cat5e Ethernet interface connected to the SFP port of the ODU. Refer to Typical deployment on page 3-2 for diagrams of these configurations.

Adapt the installation procedures in this chapter as appropriate for SFP interfaces, noting the following differences from a PSU interface:

- Install an optical or copper SFP module in the ODU (SFP port) and connect the SFP optical or copper cable into this module using the long cable gland from the SFP module kit. This is described in the following procedures:
  - Fitting the long cable gland on page 5-25
  - Inserting the SFP module on page 5-26
  - Connecting the cable on page 5-29
  - Fitting the gland on page 5-30
  - Removing the cable and SFP module on page 5-31
- Optical cables do not require LPUs or ground cables.
- At the remote end of an SFP drop cable, use an appropriate termination for the connected device.
- If the connected device is outdoors, not in the equipment building or cabinet, adapt the grounding instructions as appropriate.
- PTP 650 LPUs are not suitable for installation on SFP copper Cat5e interfaces. For SFP drop cables, obtain suitable surge protectors from a specialist supplier.
- Ground the top LPUs and surge protector to the same point on the ODU (Figure 57).

Figure 57 ODU with copper Cat5e connections to all three Ethernet ports

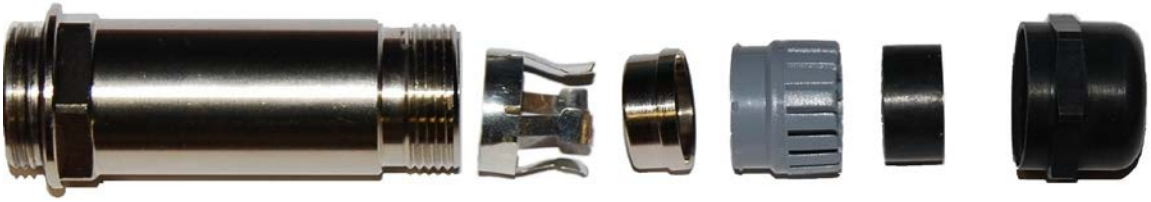


Fitting the long cable gland

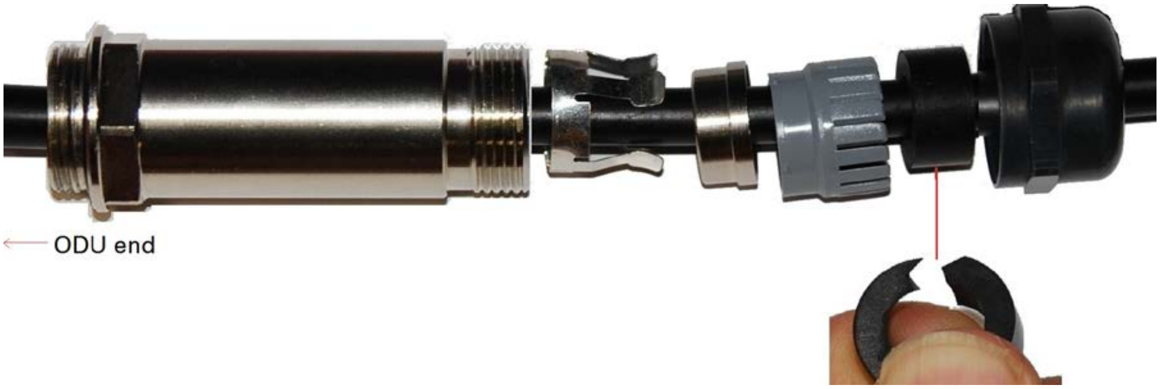
Optical SFP interface: Disassemble the long cable gland and thread its components over the LC connector at the ODU end as shown below.

Copper Cat5e SFP interface: Disassemble the long cable gland and thread its components over the RJ45 connector at the ODU end as shown below.

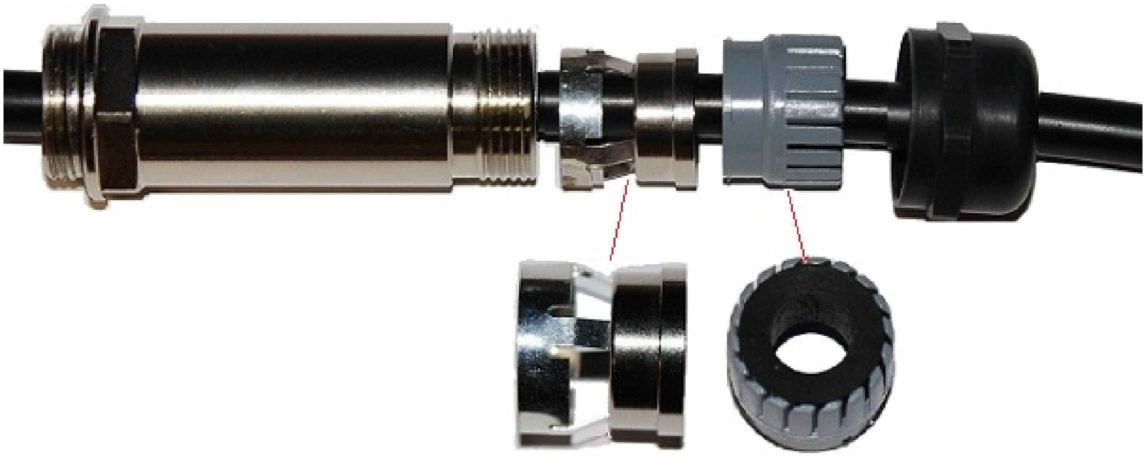
1 Disassemble the gland:



2 Thread each part onto the cable (the rubber bung is split):

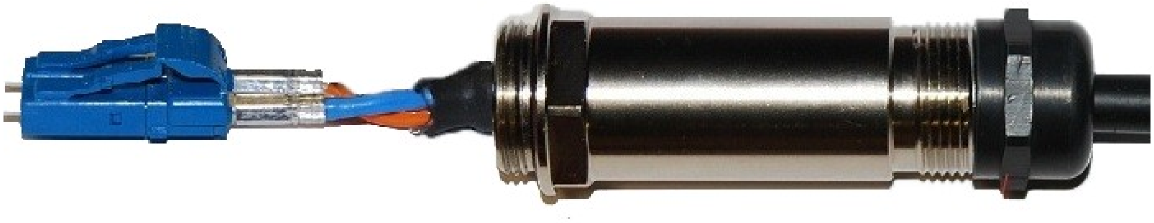


3 Assemble the spring clip and the rubber bung (the clips go inside the ring):

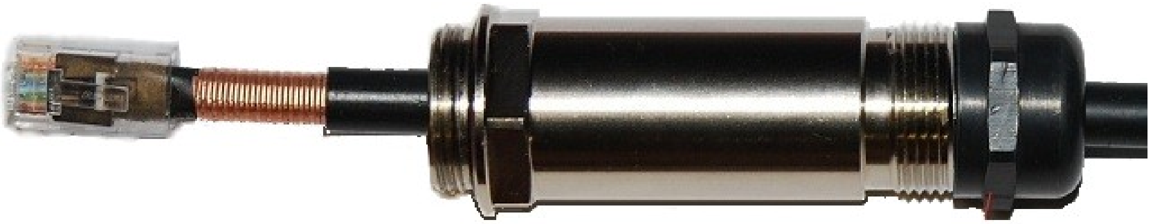


4 Fit the parts into the body and lightly screw on the gland nut (do not tighten it):

Optical



Copper



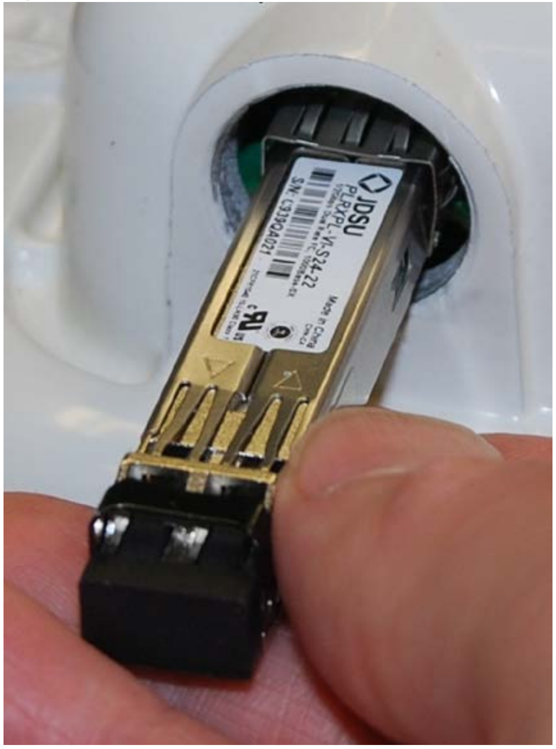
Inserting the SFP module

To insert the SFP module into the ODU, proceed as follows:

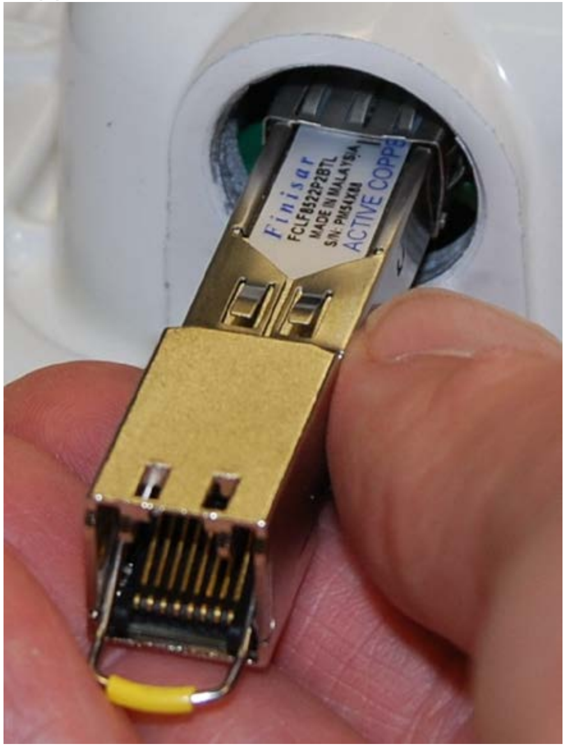
1 Remove the blanking plug from the SFP port of the ODU:

2 Insert the SFP module into the SFP receptacle with the label up:

Optical

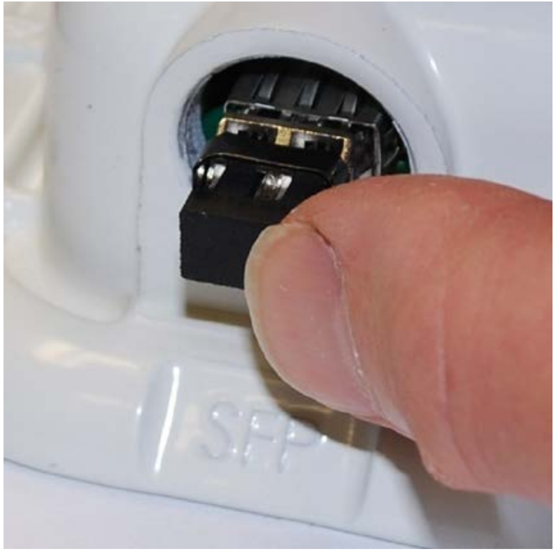


Copper

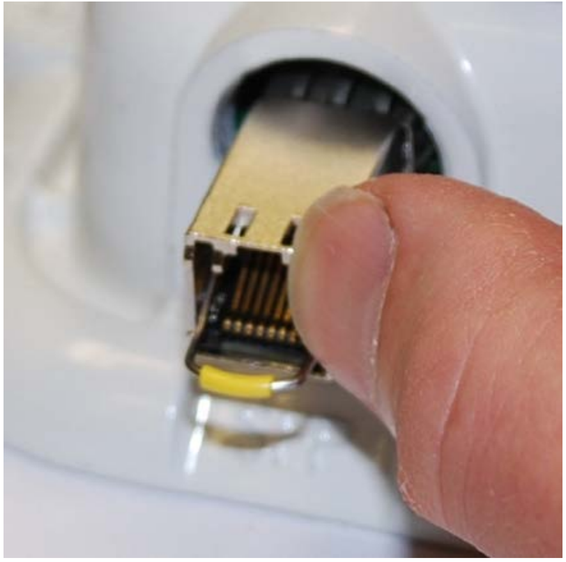


3 Push the module home until it clicks into place:

Optical

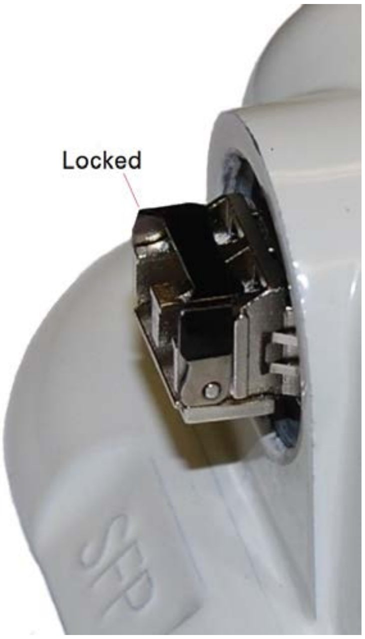


Copper

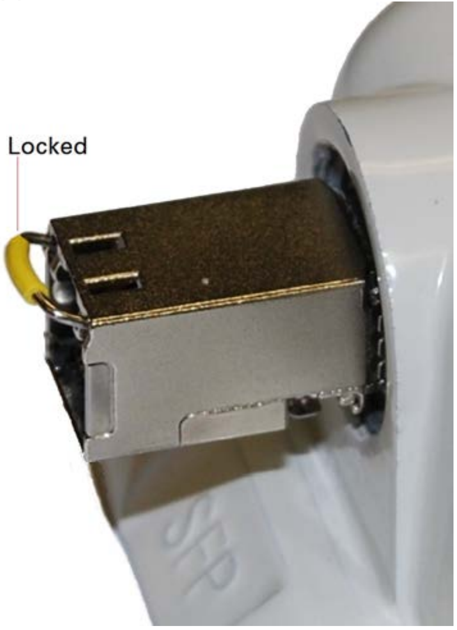


4 Rotate the latch to the locked position:

Optical



Copper



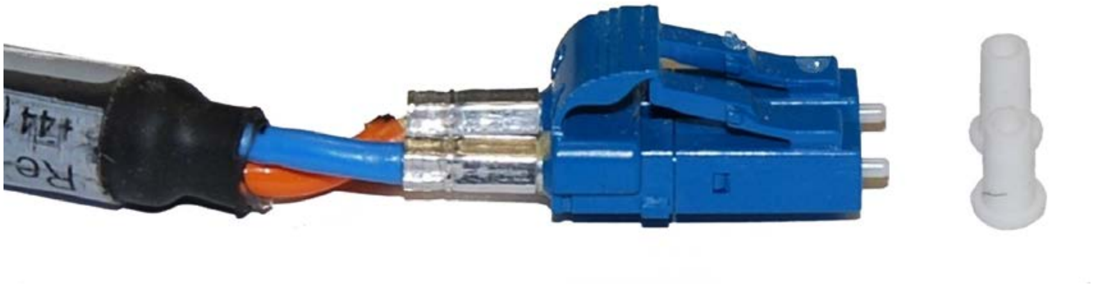
Connecting the cable

Caution

The fiber optic cable assembly is very delicate. To avoid damage, handle it with extreme care. Ensure that the fiber optic cable does not twist during assembly, especially when fitting and tightening the weatherproofing gland.

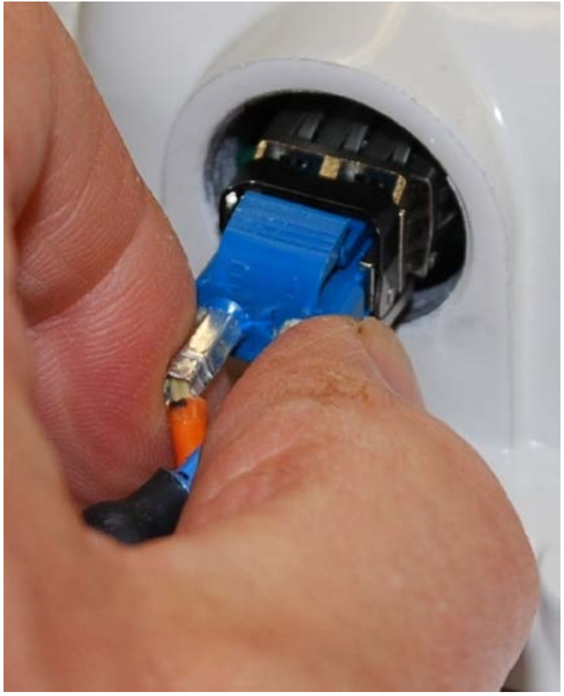
Do not insert the power over Ethernet drop cable from the PSU into the SFP module, as this will damage the module.

1 Remove the LC connector dust caps from the ODU end (optical cable only):

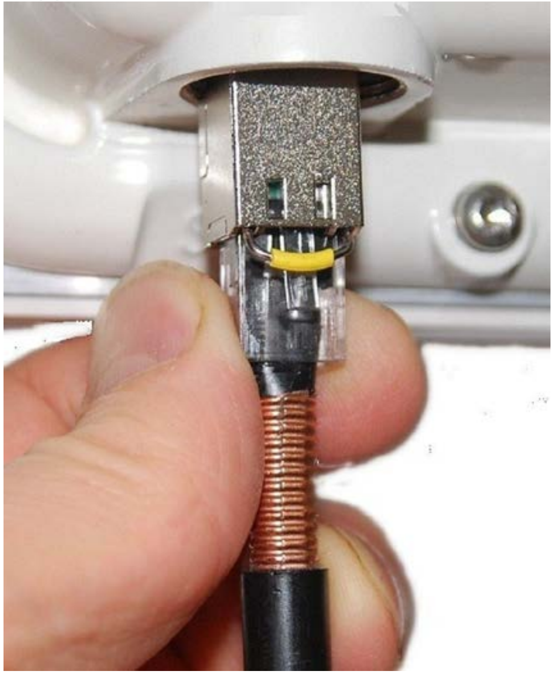


2 Plug the connector into the SFP module, ensuring that it snaps home:

Optical

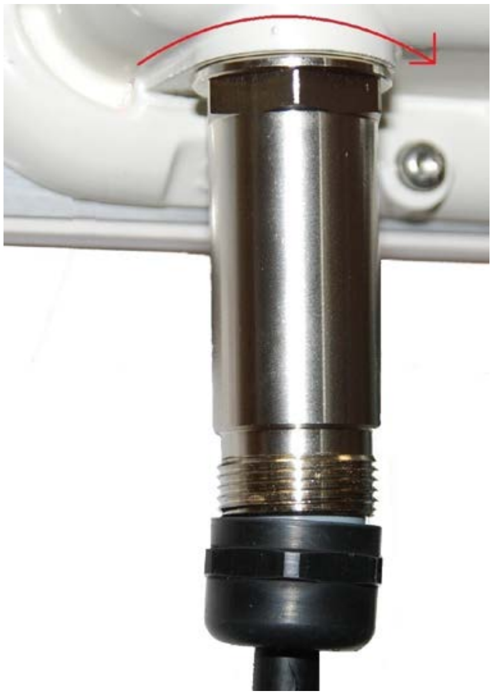


Copper

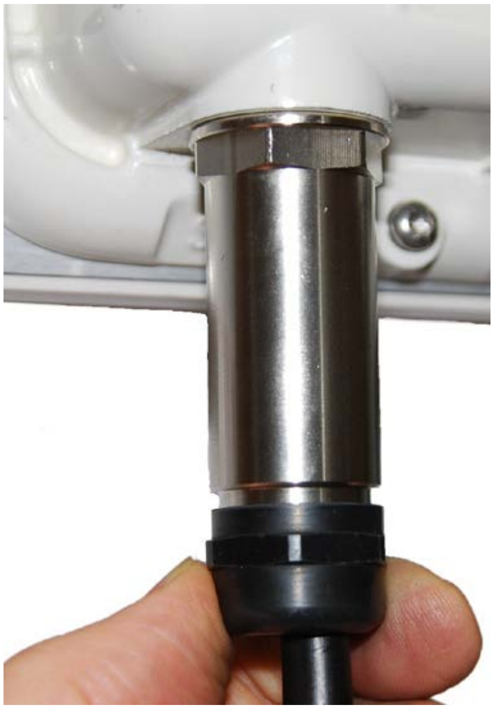


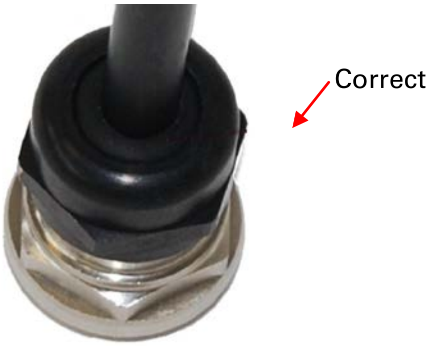
Fitting the gland

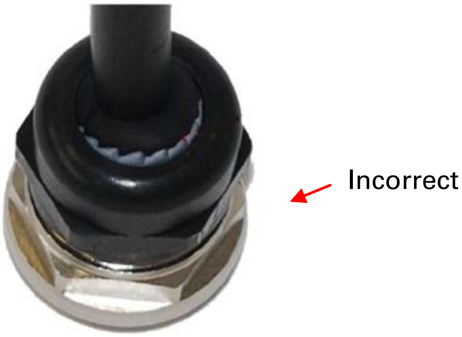
1 Fit the gland body to the SFP port and tighten it to a torque of 5.5 Nm (4.3 lb ft)



2 Fit the gland nut and tighten until the rubber seal closes on the cable. Do not over-tighten the gland nut, as there is a risk of damage to its internal components:





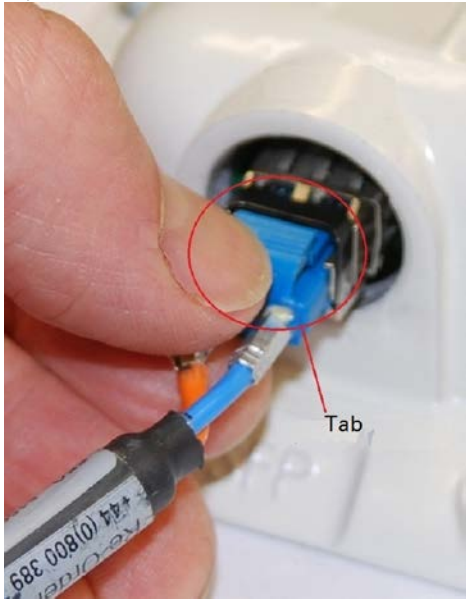


Removing the cable and SFP module

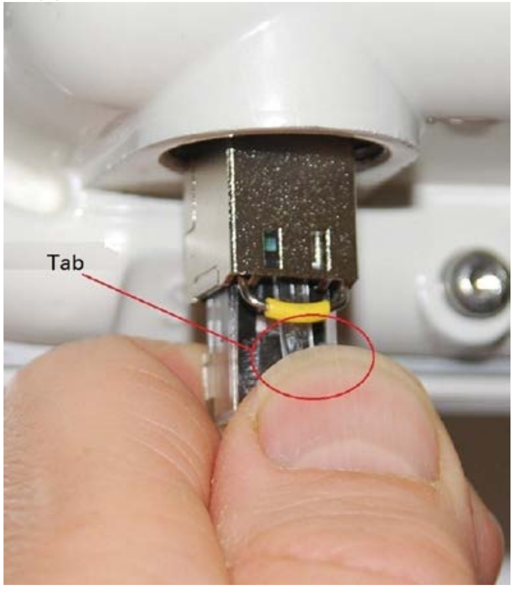
Do not attempt to remove the module without disconnecting the cable, otherwise the locking mechanism in the ODU will be damaged.

1 Remove the cable connector by pressing its release tab before pulling it out:

Optical

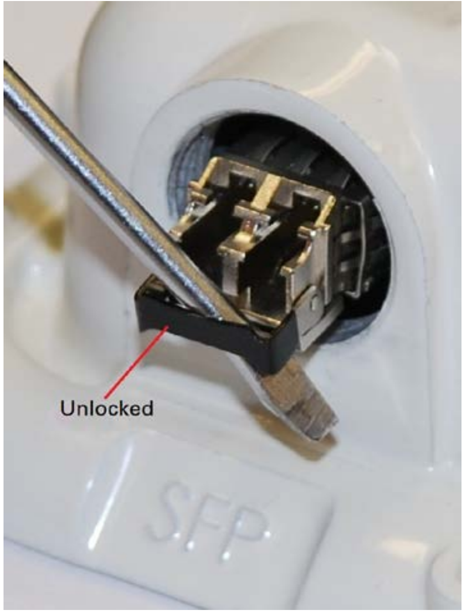


Copper

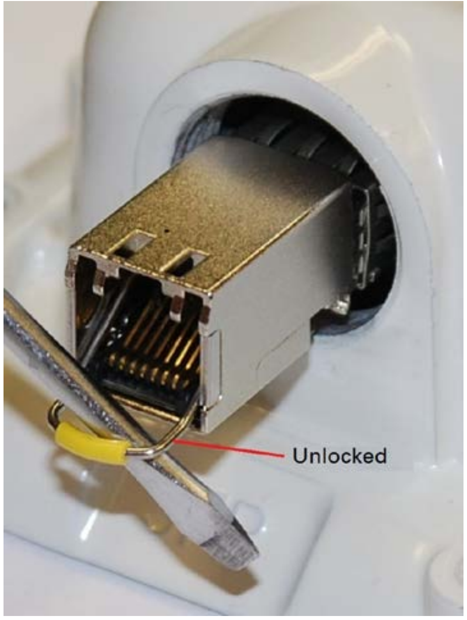


2 Rotate the latch to the unlocked position. Extract the module by using a screwdriver:

Optical



Copper



Installing an Aux Ethernet interface

In more advanced configurations, there may be a copper Cat5e Ethernet interface connected to the Aux port of the ODU. Refer to Typical deployment on page 3-2 for a diagram of this configuration.

Adapt the installation procedures in this chapter as appropriate for the Aux interface, noting the following differences:

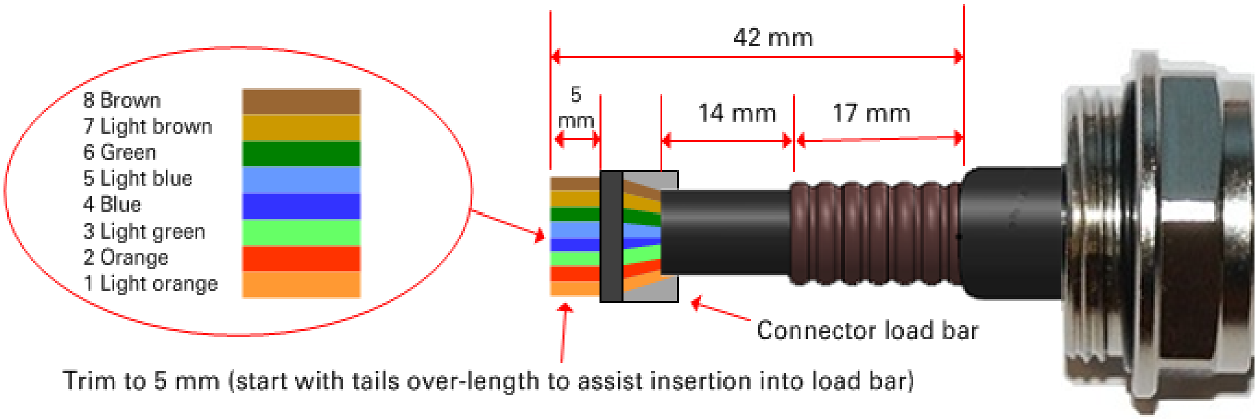
- At the remote end of the Aux drop cable, use an appropriate termination for the connected device (for example, a video camera or wireless access point).
- If the connected device is outdoors, not in the equipment building or cabinet, adapt the grounding instructions as appropriate.
- Ground the top LPUs and surge protector to the same point on the ODU (Figure 57).

Supplemental installation information

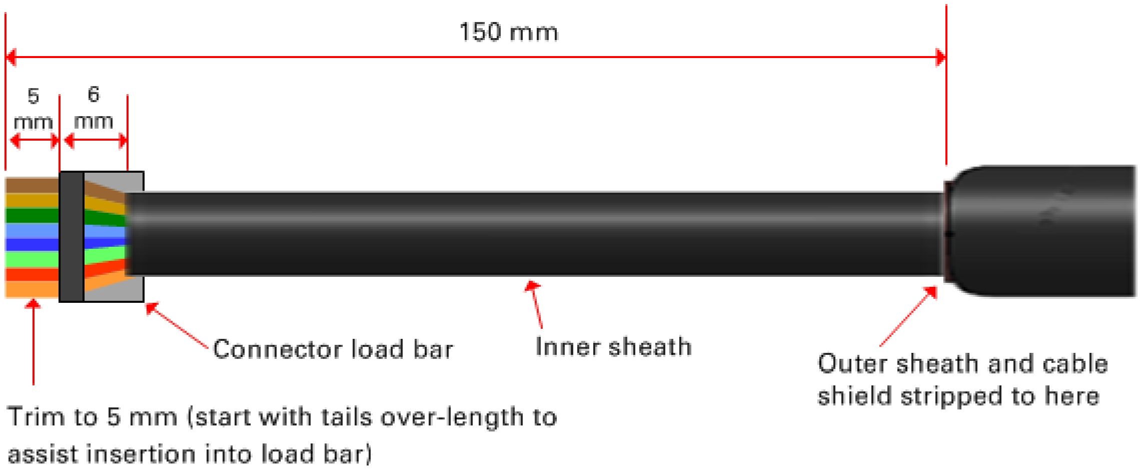
This section contains detailed installation procedures that are not included in the above topics, such as how to strip cables, create grounding points and weatherproof connectors.

Stripping drop cable

When preparing drop cable for connection to the PTP 650 ODU or LPU, use the following measurements:



When preparing drop cable for connection to the PTP 650 PSU (without a cable gland), use the following measurements:

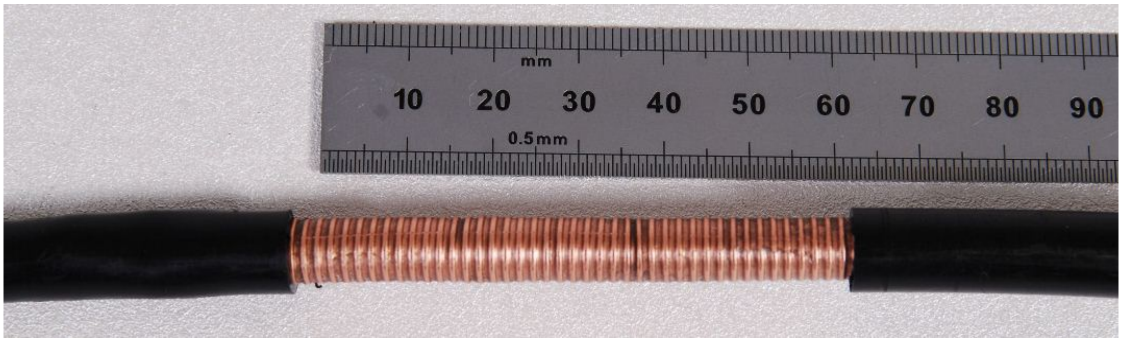

150 mm
5 mm
6 mm
Connector load bar
Inner sheath
Outer sheath and cable shield stripped to here
Trim to 5 mm (start with tails over-length to assist insertion into load bar)

Creating a drop cable grounding point

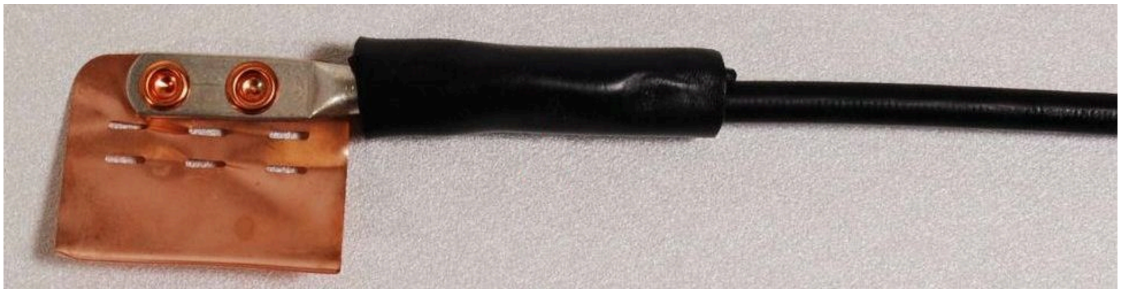
Use this procedure to connect the screen of the main drop cable to the metal of the supporting structure using the cable grounding kit (Cambium part number 01010419001).

To identify suitable grounding points, refer to Drop cable grounding points on page 3-13.

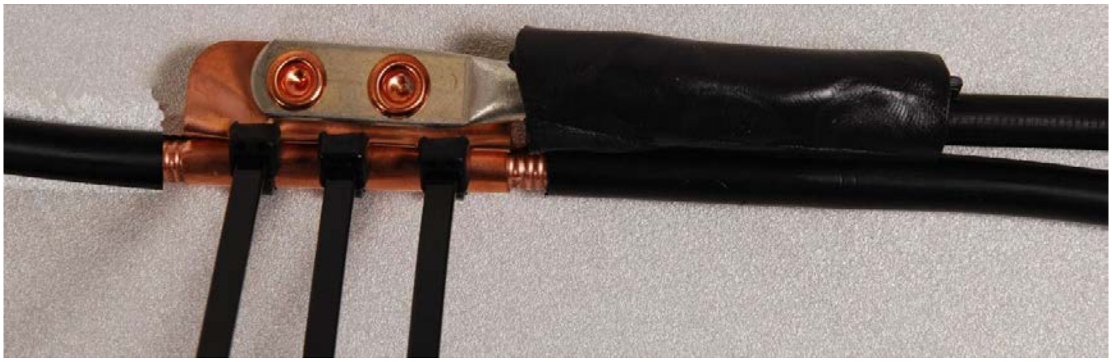
1 Remove 60 mm (2.5 inches) of the drop cable outer sheath.



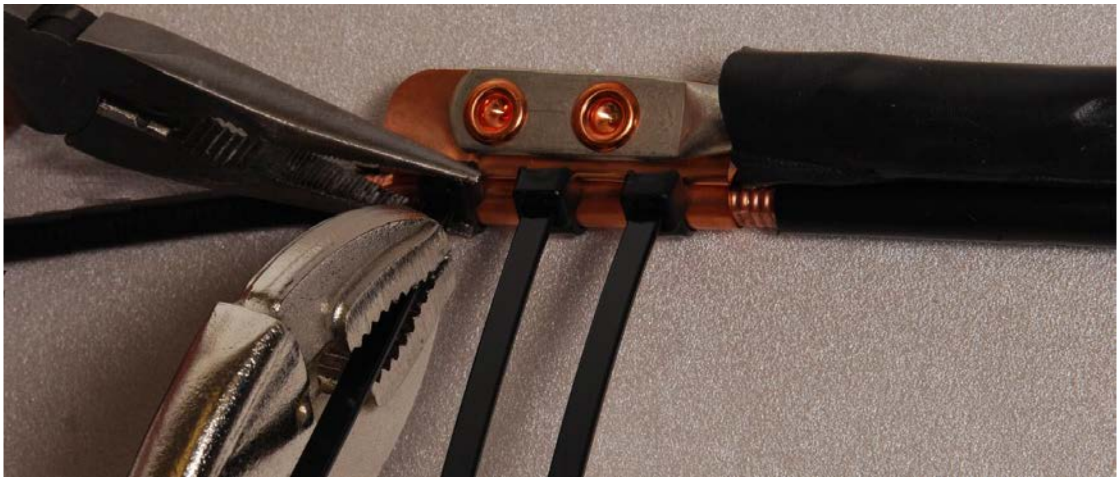
2 Cut 38mm (1.5 inches) of rubber tape (self-amalgamating) and fit to the ground cable lug. Wrap the tape completely around the lug and cable.



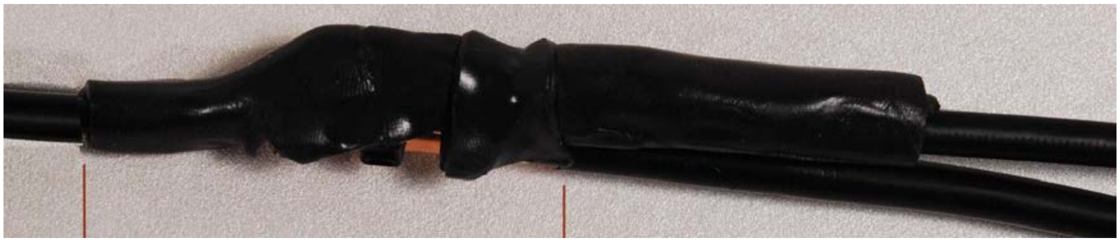
3 Fold the ground wire strap around the drop cable screen and fit cable ties.



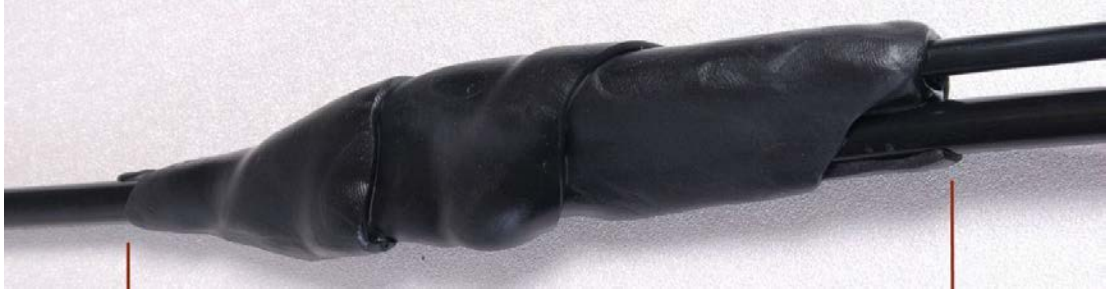
4 Tighten the cable ties with pliers. Cut the surplus from the cable ties.



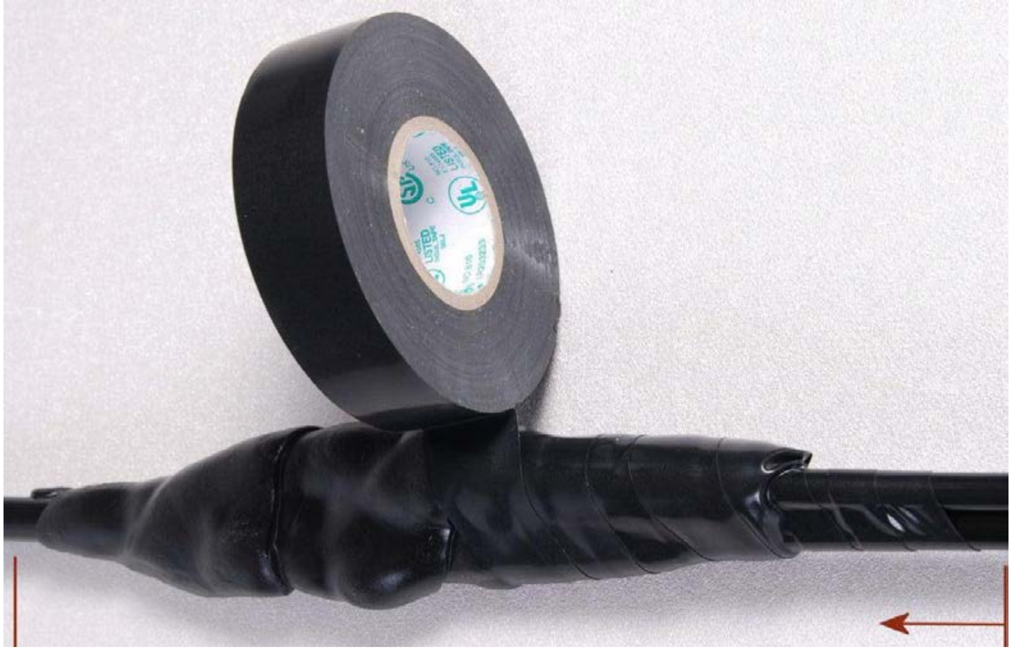
5 Cut a 38mm (1.5 inches) section of self-amalgamating tape and wrap it completely around the joint between the drop and ground cables.



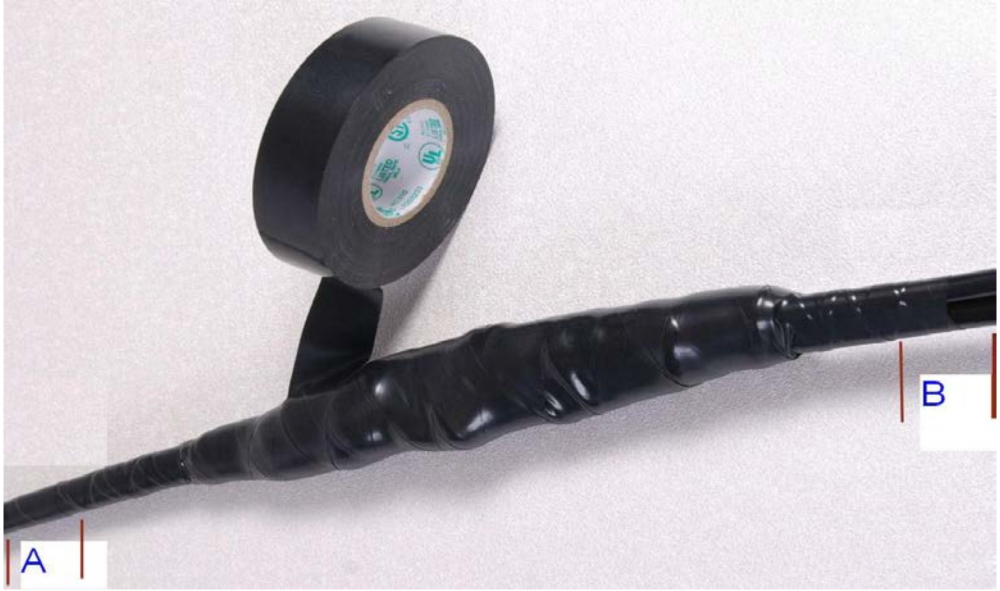
6 Use the remainder of the self-amalgamating tape to wrap the complete assembly. Press the tape edges together so that there are no gaps.



7 Wrap a layer of PVC tape from bottom to top, starting from 25 mm (1 inch) below and finishing 25 mm (1 inch) above the edge of the self-amalgamating tape, over lapping at half width.



8 Repeat with a further four layers of PVC tape, always overlapping at half width. Wrap the layers in alternate directions (top to bottom, then bottom to top). The edges of each layer should be 25mm (1 inch) above (A) and 25 mm (1 inch) below (B) the previous layer.



9 Prepare the metal grounding point of the supporting structure to provide a good electrical contact with the grounding cable clamp. Remove paint, grease or dirt, if present. Apply anti-oxidant compound liberally between the two metals.

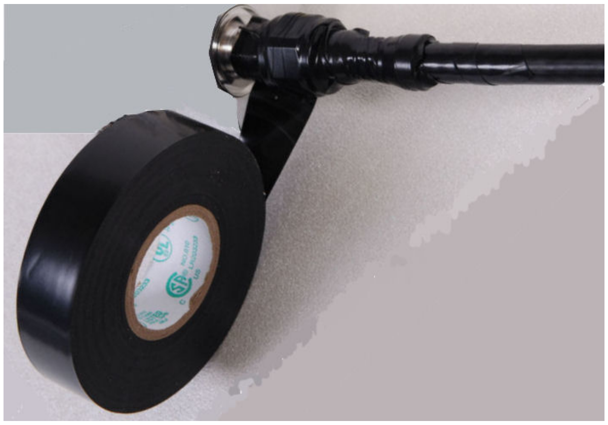
10 Clamp the bottom lug of the grounding cable to the supporting structure using site approved methods. Use a two-hole lug secured with fasteners in both holes. This provides better protection than a single-hole lug.

Weatherproofing an N type connector

Use this procedure to weatherproof the N type connectors fitted to the connectorized ODU and external antenna (if recommended by the antenna manufacturer).

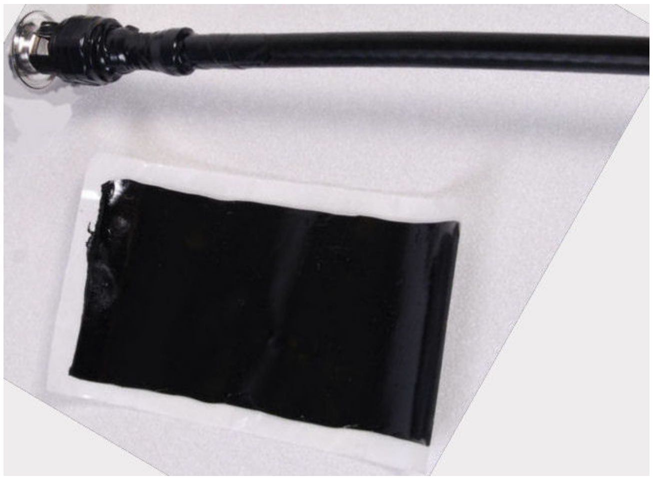
1 Ensure the connection is tight. A torque wrench should be used if available:

2 Wrap the connection with a layer of 19 mm (0.75 inch) PVC tape, starting 25 mm (1 inch) below the connector body. Overlap the tape to half-width and extend the wrapping to the body of the LPU. Avoid making creases or wrinkles:

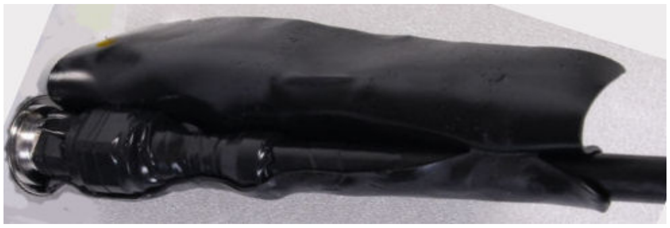


3 Smooth the tape edges:

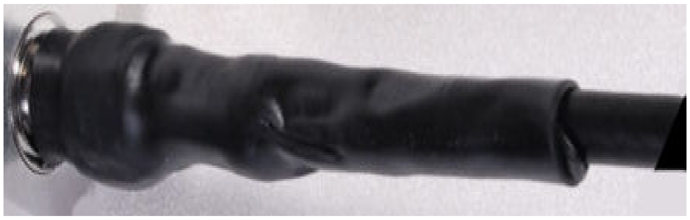
4 Cut a 125mm (5 inches) length of rubber tape (self-amalgamating):



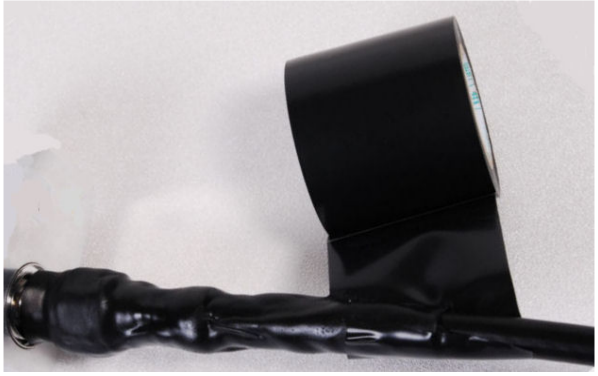
5 Expand the width of the tape by stretching it so that it will wrap completely around the connector and cable:



6 Press the tape edges together so that there are no gaps. The tape should extend 25 mm (1 inch) beyond the PVC tape:



7 Wrap a layer of 50 mm (2 inch) PVC tape from bottom to top, starting from 25 mm (1 inch) below the edge of the self-amalgamating tape, overlapping at half width.



8 Repeat with a further four layers of 19 mm (0.75 inch) PVC tape, always overlapping at half width. Wrap the layers in alternate directions:

- Second layer: top to bottom.
- Third layer: bottom to top.
- Fourth layer: top to bottom.
- Fifth layer: bottom to top.

The bottom edge of each layer should be 25 mm (1 inch) below the previous layer.

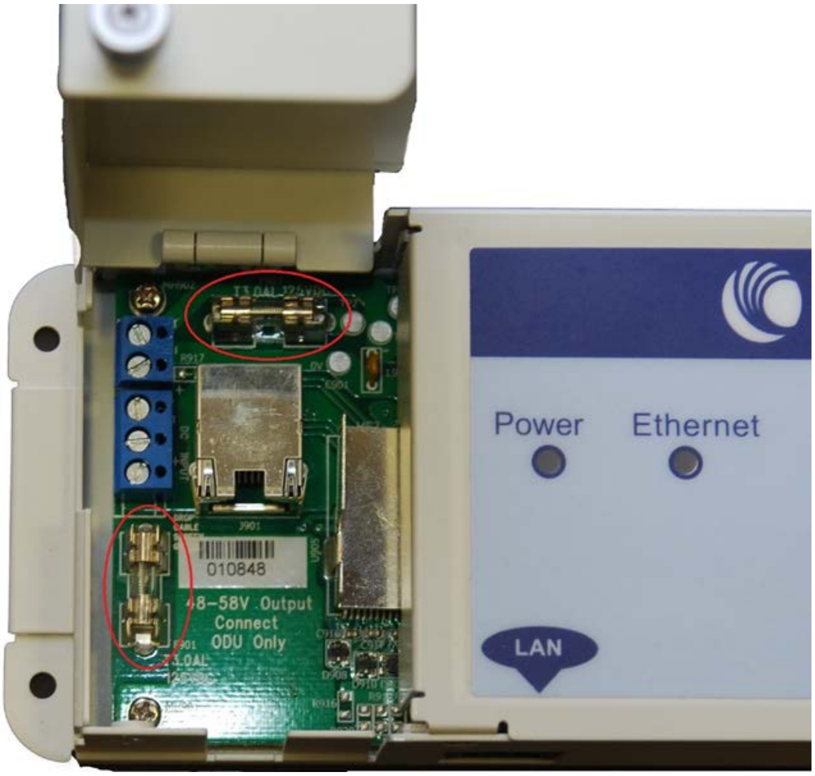
9 Check the completed weatherproof connection:

Replacing PSU fuses

The AC+ DC Enhanced Power Injector contains two replaceable fuses. These fuses protect the positive and negative grounded DC input voltages. If an incorrect power supply (that is, not in the range 37V to 60V DC) is connected to the DC input terminals, one or both fuses may blow.

Both fuses are 3 Amp slow-blow, for example Littlefuse part number 0229003.

To replace these fuses, undo the retaining screw and hinge back the cover as indicated:



Note

No other fuses are replaceable in the AC+DC Enhanced Power Injector.

Note

The AC Power Injector does not contain replaceable fuses.

Chapter 6: Configuration and alignment

This chapter describes how to use the web interface to configure the PTP 650 link. It also describes how to align antennas. This chapter contains the following topics:

Preparing for configuration and alignment

This section describes the checks to be performed before proceeding with unit configuration and antenna alignment.

Safety precautions

All national and local safety standards must be followed while configuring the units and aligning the antennas.

⚠ **Warning**

Ensure that personnel are not exposed to unsafe levels of RF energy. The units start to radiate RF energy as soon as they are powered up. Respect the safety standards defined in Compliance with safety standards on page 4-23, in particular the minimum separation distances.

Observe the following guidelines:

- Never work in front of the antenna when the ODU is powered.
- Always power down the PSU before connecting or disconnecting the drop cable from the PSU, ODU or LPU.

Regulatory compliance

All applicable radio regulations must be followed while configuring the units and aligning the antennas. For more information, refer to Compliance with radio regulations on page 4-27.

⚠ **Caution**

If the system designer has provided a list of channels to be barred for TDWR radar avoidance, the affected channels must be barred before the units are allowed to radiate on site, otherwise the regulations will be infringed. To bar these channels, follow the procedure Barring channels on page 7-31.

Selecting configuration options

Use the installation report to determine which configuration options are required. Refer to PTP LINKPlanner on page 3-21.

Generating a License Key

ODUs are shipped with a default License Key factory installed. The default license key enables a limited set of capabilities as follows:

- Operation in selected regulatory bands (these are restricted by the ODU regional variant):
  - FCC/IC variants: 5.8 GHz USA (regulatory band 1).
  - RoW variants: 5.4 GHz unrestricted (regulatory band 8) and 5.8 GHz unrestricted (regulatory band 35).
  - EU variants: 5.4 GHz ETSI (regulatory band 26)
- “Lite” throughput capability (up to 125 Mbps).

A license key is required to upgrade the ODU to the following capabilities:

- To allow the ODU to operate in other regulatory bands (these are restricted by the ODU regional variant). This capability is free of charge.
- To enable the SFP port. An Access Key for this capability is provided in the SFP module kits (SFP module kits on page 2-27).
- To allow “Med” (up to 250 Mbps) or “Full” (up to 450 Mbps) throughput capability. Purchase an access key from Cambium Networks (Table 67). Cambium will email one Access Key for each upgrade purchased.
- To allow 128-bit or 256-bit AES encryption. Purchase an access key from Cambium Networks (Table 67). Cambium will email one Access Key for each upgrade purchased.

Table 67 Capability upgrades

Cambium description (*1)	Cambium part number
PTP 650 128-bit AES Encryption – per ODU (*2)	C000065K018
PTP 650 256-bit AES Encryption – per ODU (*2)	C000065K019
PTP 650 Lite (Up to 125Mbps) to Mid (Up to 250Mbps) Link Capacity upgrade license per ODU	C000065K021
PTP 650 Lite (Up to 125Mbps) to Full (Up to 450Mbps) Link Capacity upgrade license per ODU	C000065K022
PTP 650 Mid (Up to 250Mbps) to Full (Up to 450Mbps) Link Capacity upgrade license per ODU	C000065K023

(*1) If the Cambium description contains the words “per ODU”, then order two upgrades per link.

(*2) Cambium Networks will supply these upgrades only if there is official permission to export AES encryption to the country of operation.

To obtain the License Key, proceed as follows:

- Obtain the MAC Address of the unit (it is on the System Status page).
- Go to the Cambium Support web page (see Contacting Cambium Networks on page 1) and navigate to the **Cambium Networks License Key Generator**.
- Complete the required fields, including MAC Address and Country. For SFP capability, AES encryption and data throughput upgrades only, enter the Access Key.
- Submit the web form. Cambium will send the License Key by email.

Connecting to the unit

This section describes how to connect the unit to a management PC and power it up.

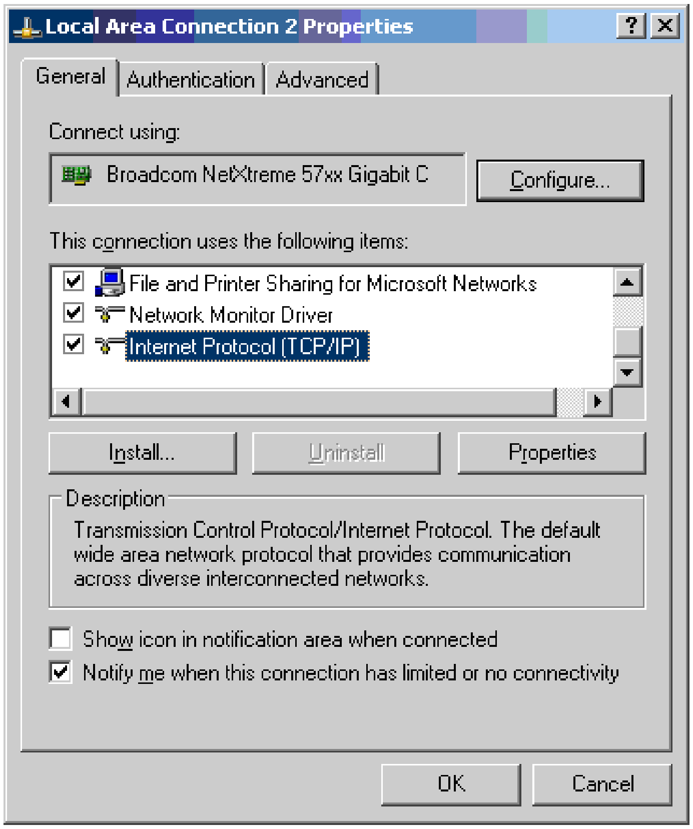
Configuring the management PC

Use this procedure to configure the local management PC to communicate with the PTP 650.

Procedure:

1 Select **Properties** for the Ethernet port. In Windows 7 this is found in **Control Panel > Network and Internet > Network Connections > Local Area Connection**.

2 Select **Internet Protocol (TCP/IP)**:



Local Area Connection 2 Properties

Connect using:

Broadcom NetXtreme 57xx Gigabit C

This connection uses the following items:

☑ File and Printer Sharing for Microsoft Networks
☑ Network Monitor Driver
☑ Internet Protocol (TCP/IP)

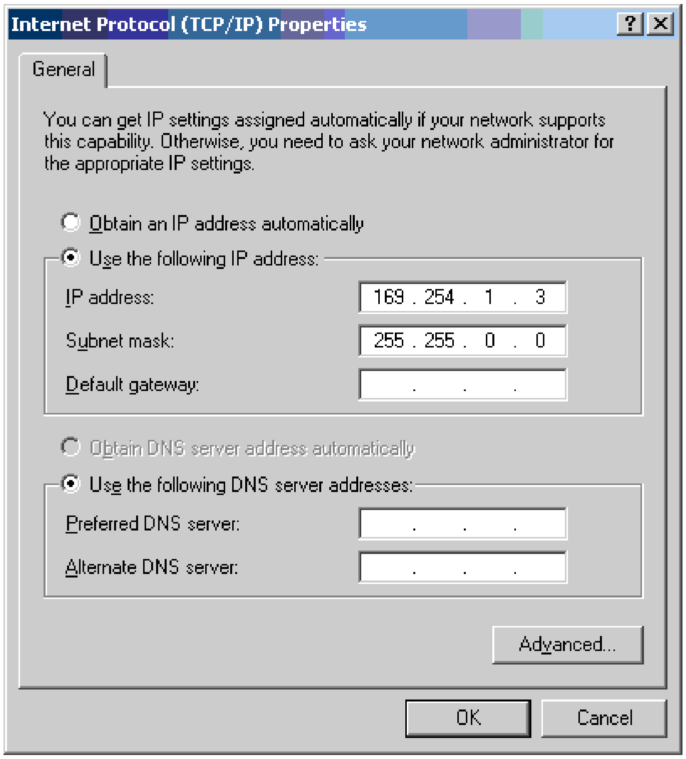
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

3 Click **Properties**.

4 Enter an IP address that is valid for the 169.254.X.X network, avoiding 169.254.0.0 and 169.254.1.1. A good example is 169.254.1.3:



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 169 . 254 . 1 . 3

Subnet mask: 255 . 255 . 0 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

5 Enter a subnet mask of 255.255.0.0. Leave the default gateway blank.

Connecting to the PC and powering up

Use this procedure to connect a management PC and power up the PTP 650.

Procedure:

1 Check that the ODU and PSU are correctly connected.

2 Connect the PC Ethernet port to the LAN port of the PSU using a standard (not crossed) Ethernet cable.

3 Apply mains or battery power to the PSU. The green Power LED should illuminate continuously.

4 After about 45 seconds, check that the orange Ethernet LED starts with 10 slow flashes.

5 Check that the Ethernet LED then illuminates continuously. If the Power and Ethernet LEDs do not illuminate correctly, refer to Testing link end hardware on page 8-2.

Using the web interface

This section describes how to log into the PTP 650 web interface and use its menus.

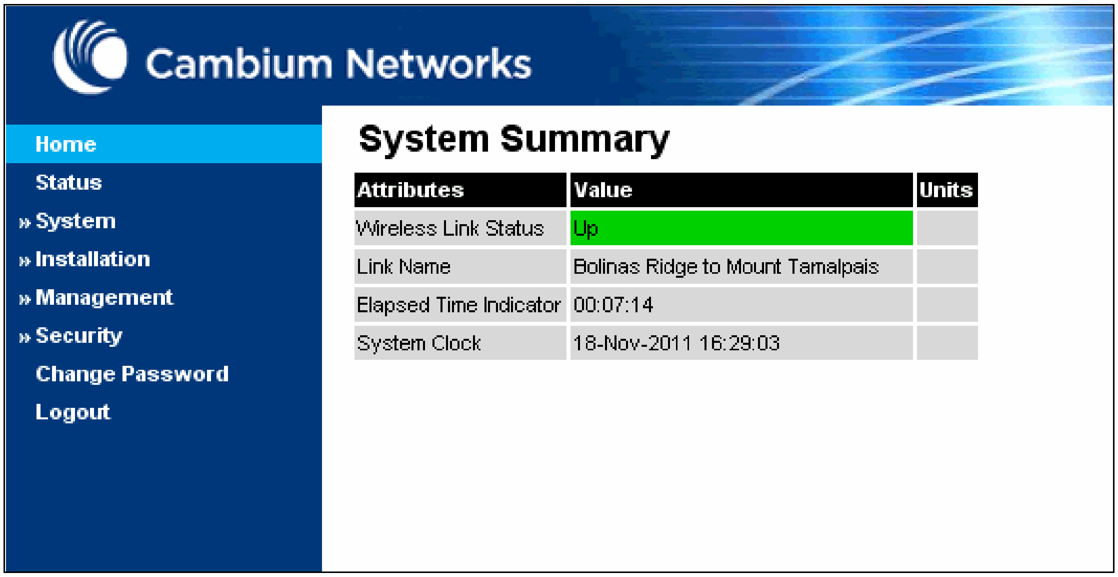
Logging into the web interface

Use this procedure to log into the web interface as a system administrator.

Procedure:

1 Start the web browser from the management PC.

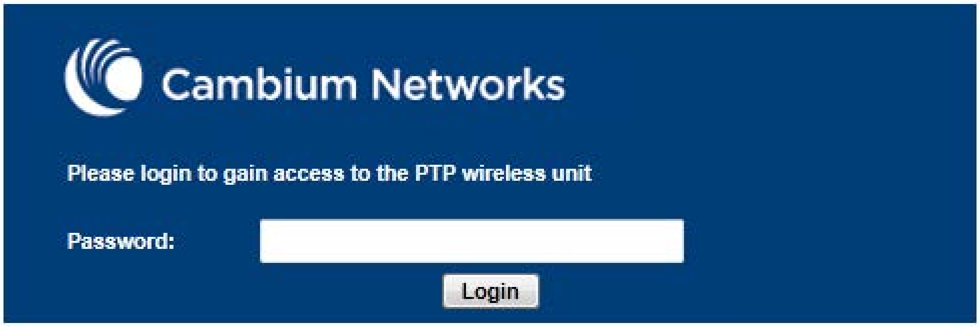
2 Type the IP address of the unit into the address bar. The factory default IP address is **169.254.1.1**. Press ENTER. The web interface menu and System Summary page are displayed:



System Summary

Attributes	Value	Units
Wireless Link Status	Up	
Link Name	Bolinas Ridge to Mount Tamalpais	
Elapsed Time Indicator	00:07:14	
System Clock	18-Nov-2011 16:29:03	

3 On the menu, click **System**. The login page is displayed with Password only (the default) or with Username and Password (if identity-based user accounts have been enabled):



Please login to gain access to the PTP wireless unit

Password:

4 Enter Username (if requested) and Password (the default is blank) and click **Login**.

Using the menu options

Use the menu navigation bar in the left panel to navigate to each web page. Some of the menu options are only displayed for specific system configurations. Use Table 68 to locate information about using each web page.

Table 68 Menu options and web pages

Main menu	Menu option	Web page information
Home		System Summary page on page 7-2
Status		System Status page on page 7-3
System		
	Configuration	System Configuration page on page 6-21
	LAN Configuration	LAN Configuration page on page 6-24
	QoS Configuration	QoS Configuration page on page 6-30
	SFP Configuration	SFP Configuration page on page 6-33
	Save and Restore	Save & Restore Configuration page on page 6-34
	Spectrum Management	Spectrum Management page on page 7-20 Barring channels on page 7-31
	Statistics	System Statistics page on page 7-32 Comparing actual to predicted performance on page 6-94
	Wireless Port Counters	Wireless Port Counters page on page 7-37 Test Ethernet packet errors reported by ODU on page 8-7
	Main Port Counters	Main Port Counters page on page 7-38
	Aux Port Counters	Aux Port Counters page on page 7-40
	SFP Port Counters	SFP Port Counters page on page 7-41
	Diagnostics Plotter	Diagnostics Plotter page on page 7-42
	CSV Download	Generate Downloadable Diagnostics page on page 7-43
	Software Upgrade	Software Upgrade page on page 6-37
	Reboot	Reboot Wireless Unit page on page 7-9

Main menu	Menu option	Web page information
Installation		Installation menu on page 6-10
	Graphical Install	Graphical Install page on page 6-92
Management		
	Web	Web-Based Management page on page 6-39
	Local User Accounts	Local User Accounts page on page 6-42
	RADIUS Configuration	RADIUS Configuration page on page 6-47
	Login Information	Login Information page on page 7-9
	Web Properties	Webpage Properties page on page 6-49
	SNMP	SNMP pages (for SNMPv3) on page 6-61 SNMP pages (for SNMPv1/2c) on page 6-71
	Email	Email Configuration page on page 6-52
	Diagnostic Alarms	Diagnostic Alarms page on page 6-54
	Time	Time Configuration page on page 6-55
	Syslog	Syslog page on page 7-16
	Syslog Configuration	Syslog Configuration page on page 6-59
Security		Security menu on page 6-75
	Zeroize CSPs	Zeroize CSPs page on page 6-86
Change Password		Change Password page on page 7-10
Logout		Logging out on page 7-11

Installation menu

This section describes how to use the Installation Wizard to complete the essential system configuration tasks that must be performed on a new link.

Caution

If the system designer has provided a list of channels to be barred for TDWR radar avoidance, the affected channels must be barred before the units are allowed to radiate on site, otherwise the regulations will be infringed. To bar these channels, follow the procedure Barring channels on page 7-31.

Starting the Installation Wizard

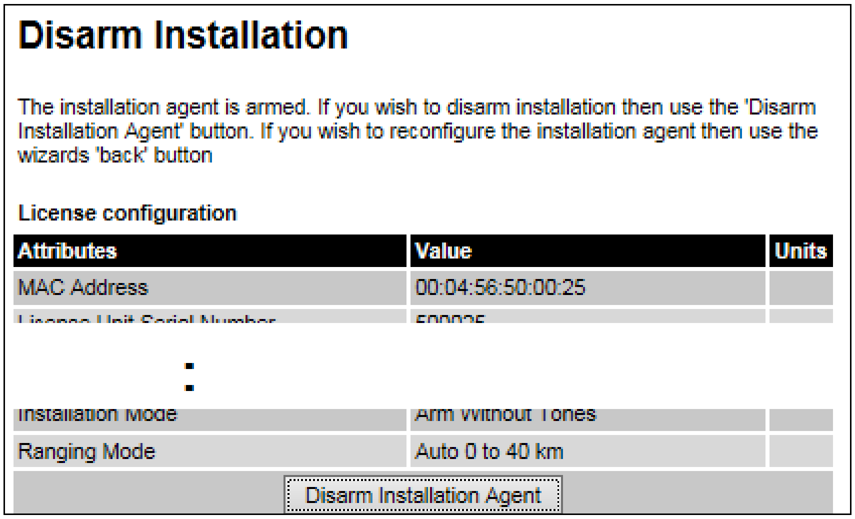
To start the Installation Wizard: on the menu, click **Installation**. The response depends upon the state of the unit:

- If the unit is newly installed, the Software License Key page is displayed. Continue at Software License Key page on page 6-12.
- If the unit is armed for alignment, the Disarm Installation page is displayed. Continue at Disarm Installation page on page 6-11.
- If the unit is not armed, the Current Installation Summary page is displayed. Continue at Current Installation Summary page on page 6-11.

Disarm Installation page

Menu option: **Installation** (Figure 58). This page is displayed only when unit is armed.

Figure 58 Disarm Installation page (top and bottom of page shown)



Disarm Installation

The installation agent is armed. If you wish to disarm installation then use the 'Disarm Installation Agent' button. If you wish to reconfigure the installation agent then use the wizards 'back' button

License configuration

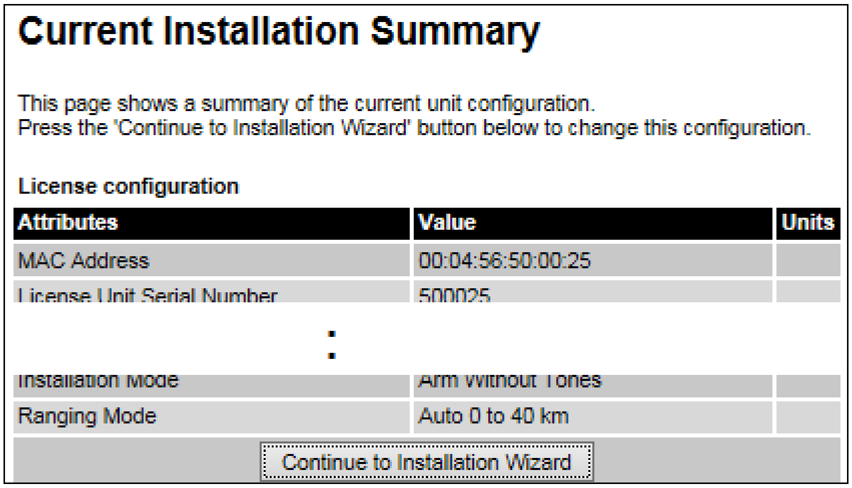
Attributes	Value	Units
MAC Address	00:04:56:50:00:25	
License Unit Serial Number	500025	
:		
Installation Mode	Arm Without Tones	
Ranging Mode	Auto 0 to 40 km	

To disarm the unit, click **Disarm Installation Agent.**

Current Installation Summary page

Menu option: **Installation** (Figure 59). This page is displayed only when unit is not armed.

Figure 59 Current Installation Summary page (top and bottom of page shown)



Current Installation Summary

This page shows a summary of the current unit configuration.
Press the 'Continue to Installation Wizard' button below to change this configuration.

License configuration

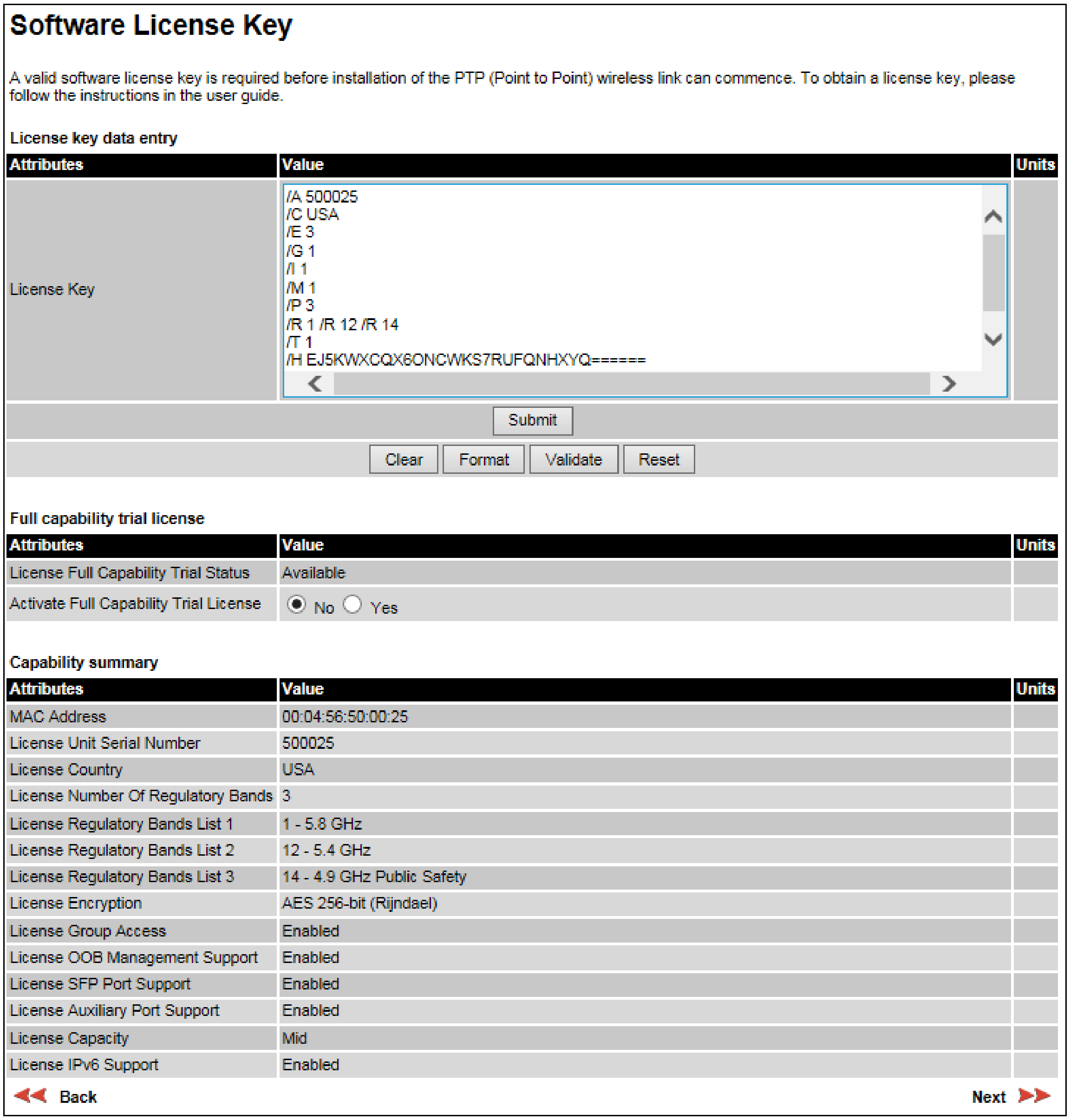
Attributes	Value	Units
MAC Address	00:04:56:50:00:25	
License Unit Serial Number	500025	
:		
Installation Mode	Arm Without Tones	
Ranging Mode	Auto 0 to 40 km	

Click **Continue to Installation Wizard.**

Software License Key page

Menu option: **Installation** (Figure 60). Use this page to configure the unit with a new License Key and to review the capabilities of an installed License Key. The Capability Summary section is not displayed until a License Key is submitted and accepted. Ensure that Licenses Keys are available (Generating a License Key on page 6-3).

Figure 60 Software License Key page (showing a Mid license)



Software License Key

A valid software license key is required before installation of the PTP (Point to Point) wireless link can commence. To obtain a license key, please follow the instructions in the user guide.

License key data entry

Attributes	Value	Units
License Key	/A 500025 /C USA /E 3 /G 1 /I 1 /M 1 /P 3 /R 1 /R 12 /R 14 /T 1 /H EJ5KWXCQX6ONCWKS7RUFQNHXYQ======	

Full capability trial license

Attributes	Value	Units
License Full Capability Trial Status	Available	
Activate Full Capability Trial License	● No ○ Yes	

Capability summary

Attributes	Value	Units
MAC Address	00:04:56:50:00:25	
License Unit Serial Number	500025	
License Country	USA	
License Number Of Regulatory Bands	3	
License Regulatory Bands List 1	1 - 5.8 GHz	
License Regulatory Bands List 2	12 - 5.4 GHz	
License Regulatory Bands List 3	14 - 4.9 GHz Public Safety	
License Encryption	AES 256-bit (Rijndael)	
License Group Access	Enabled	
License OOB Management Support	Enabled	
License SFP Port Support	Enabled	
License Auxiliary Port Support	Enabled	
License Capacity	Mid	
License IPv6 Support	Enabled	

Note

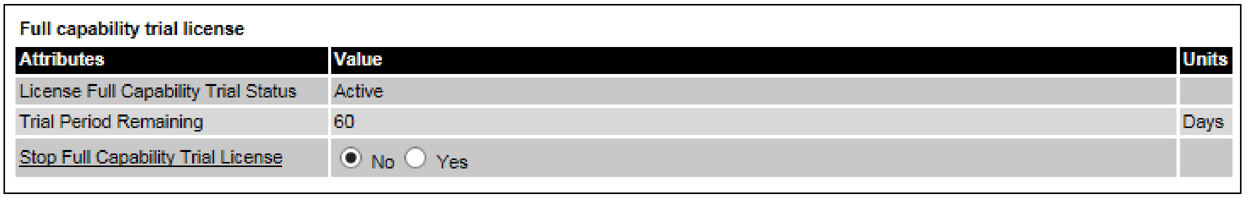
Full capability is available only when both ODUs have the trial active or are already licensed to operate with that capacity.

When the trial has started, the Software License Key page displays the Trial Period Remaining attribute (Figure 61). This shows the number of days remaining before the full capacity trial period expires.

Procedure:

- To clear the existing License Key (if present), click **Clear**.
- To format the new License Key: copy it from the Cambium notification email, paste it into the License Key box and click **Format**. The page is redisplayed with the License Key formatted.
- For Lite and Mid licenses only, select one of the following options:
  - o If License Full Capability Trial Status is **Available** (Figure 60): to start the full capability trial period, set Activate Full Capability Trial License to **Yes**.
  - o If License Full Capability Trial Status is **Active** (Figure 61): to suspend the full capability trial period, set Stop Full Capability Trial License to **Yes**.
  - o If License Full Capability Trial Status is **Inactive** (Figure 62): to resume the full capability trial period, set Start Full Capability Trial License to **Yes**.
- To enter the new License Key, click **Submit**. The page is redisplayed with the Capability Summary.
- To continue with the Installation Wizard, click **Next**.

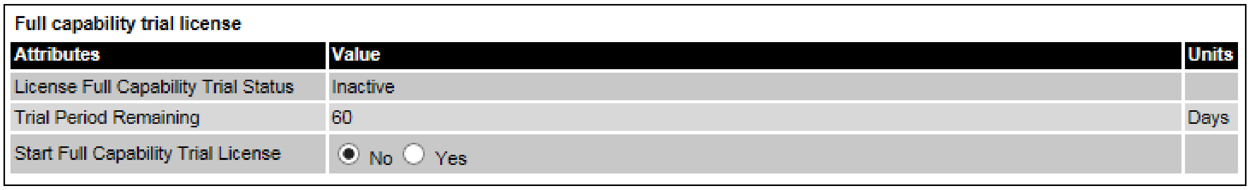
Figure 61 Software License Key page (extract) with full capability trial active



Full capability trial license

Attributes	Value	Units
License Full Capability Trial Status	Active	
Trial Period Remaining	60	Days
Stop Full Capability Trial License	● No ○ Yes	

Figure 62 Software License Key page (extract) with full capability trial inactive



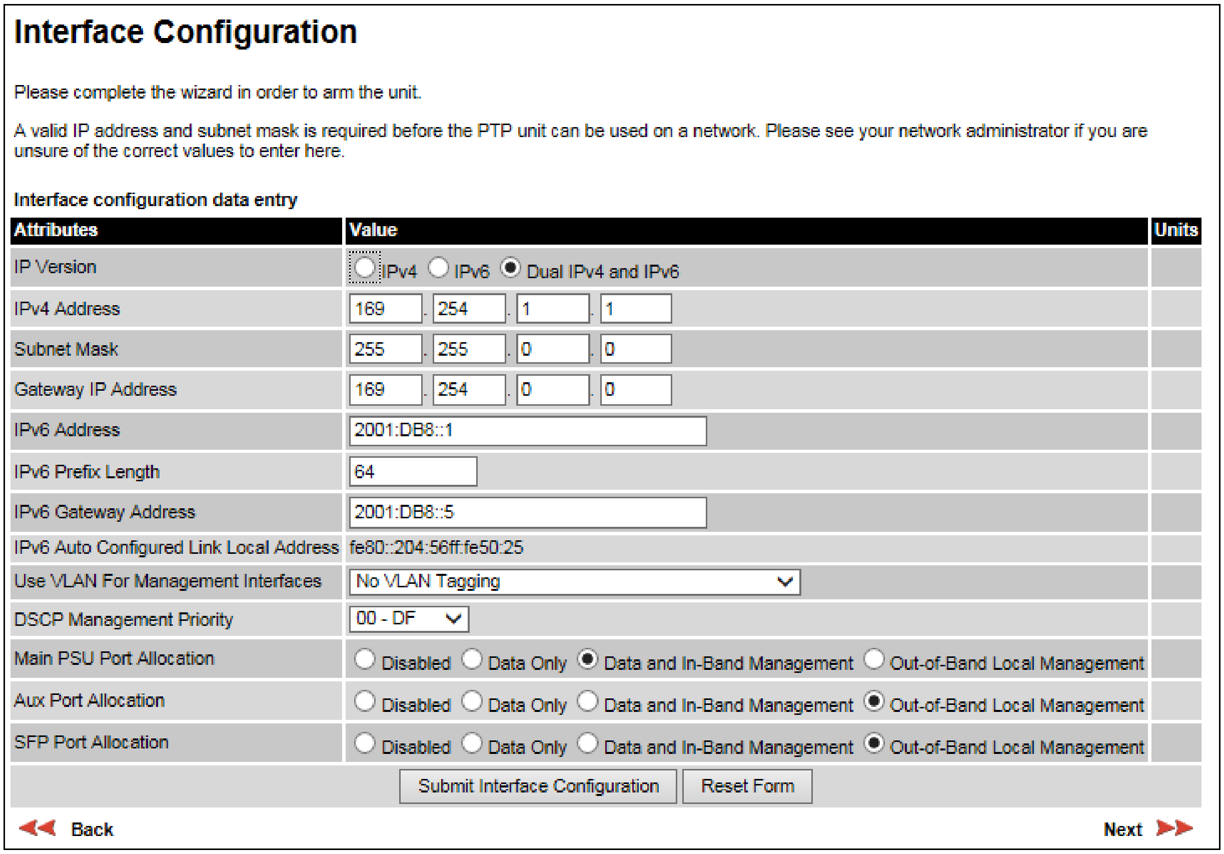
Full capability trial license

Attributes	Value	Units
License Full Capability Trial Status	Inactive	
Trial Period Remaining	60	Days
Start Full Capability Trial License	● No ○ Yes	

Interface Configuration page

Menu option: **Installation** (Figure 63). Use this page to update the IP interface attributes.

Figure 63 Interface Configuration page (showing Dual IPv4 and IPv6)



Interface Configuration

Please complete the wizard in order to arm the unit.

A valid IP address and subnet mask is required before the PTP unit can be used on a network. Please see your network administrator if you are unsure of the correct values to enter here.

Interface configuration data entry

Attributes	Value	Units
IP Version	○ IPv4 ○ IPv6 ● Dual IPv4 and IPv6	
IPv4 Address	169 . 254 . 1 . 1	
Subnet Mask	255 . 255 . 0 . 0	
Gateway IP Address	169 . 254 . 0 . 0	
IPv6 Address	2001:DB8::1	
IPv6 Prefix Length	64	
IPv6 Gateway Address	2001:DB8::5	
IPv6 Auto Configured Link Local Address	fe80::204:56ff:fe50:25	
Use VLAN For Management Interfaces	No VLAN Tagging	
DSCP Management Priority	00 - DF	
Main PSU Port Allocation	○ Disabled ○ Data Only ● Data and In-Band Management ○ Out-of-Band Local Management	
Aux Port Allocation	○ Disabled ○ Data Only ○ Data and In-Band Management ● Out-of-Band Local Management	
SFP Port Allocation	○ Disabled ○ Data Only ○ Data and In-Band Management ● Out-of-Band Local Management	

Review and update the attributes: they are repeated in the LAN Configuration page (Table 71).

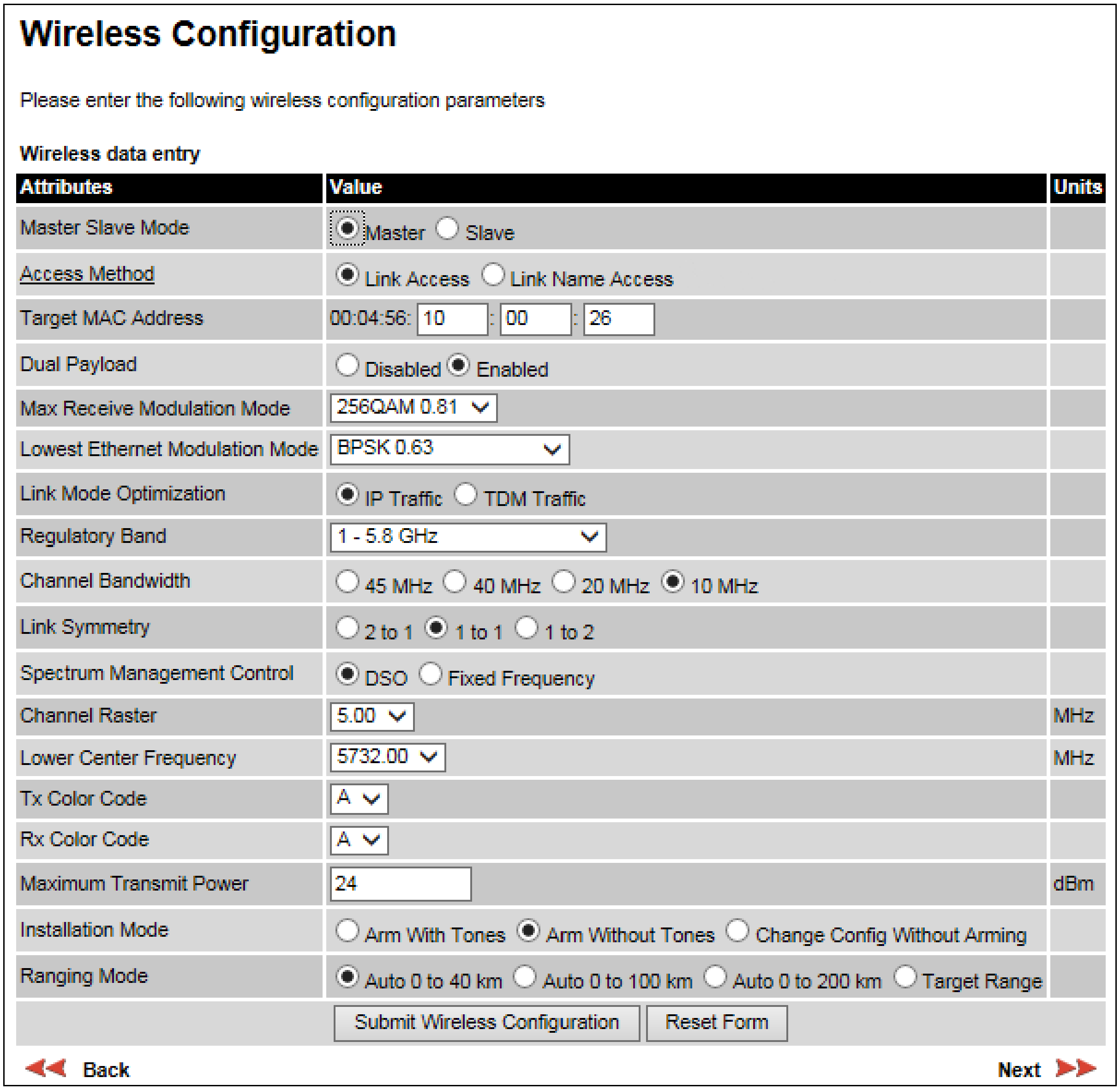
To continue with the Installation Wizard, click **Next** or **Submit Interface Configuration**.

Wireless Configuration page

Menu option: **Installation** (Figure 64).

This page is part of the Installation Wizard. Use it to update the wireless attributes.

Figure 64 Wireless Configuration page



Wireless Configuration

Please enter the following wireless configuration parameters

Wireless data entry

Attributes	Value	Units
Master Slave Mode	● Master ○ Slave	
Access Method	● Link Access ○ Link Name Access	
Target MAC Address	00:04:56: 10 : 00 : 26	
Dual Payload	○ Disabled ● Enabled	
Max Receive Modulation Mode	256QAM 0.81	
Lowest Ethernet Modulation Mode	BPSK 0.63	
Link Mode Optimization	● IP Traffic ○ TDM Traffic	
Regulatory Band	1 - 5.8 GHz	
Channel Bandwidth	○ 45 MHz ○ 40 MHz ○ 20 MHz ● 10 MHz	
Link Symmetry	○ 2 to 1 ● 1 to 1 ○ 1 to 2	
Spectrum Management Control	● DSO ○ Fixed Frequency	
Channel Raster	5.00	MHz
Lower Center Frequency	5732.00	MHz
Tx Color Code	A	
Rx Color Code	A	
Maximum Transmit Power	24	dBm
Installation Mode	○ Arm With Tones ● Arm Without Tones ○ Change Config Without Arming	
Ranging Mode	● Auto 0 to 40 km ○ Auto 0 to 100 km ○ Auto 0 to 200 km ○ Target Range	
	Submit Wireless Configuration Reset Form	

Procedure:

- Update the attributes (Table 69).
- To save any changes and continue with the Installation Wizard, click **Next** or click **Submit Wireless Configuration**.

Caution

The lower center frequency attribute must be configured to the same value for both the Master and Slave, otherwise the wireless link will fail to establish. The only way to recover from this situation is to modify the Lower Center Frequency attributes so that they are identical on both the master and slave units.

Note

When configuring a linked pair of units, use the Master Slave Mode to ensure that one unit is **Master** and the other is **Slave**.

Table 69 Wireless Configuration attributes

Attribute	Meaning
Master Slave Mode	**Master:** The unit controls the point-to-point link and its maintenance. On startup, the Master transmits until a link with the Slave is made. **Slave:** The unit listens for its peer and only transmits when the peer has been identified.
Access Method	ODUs must be configured in pairs before a link can be established. Access Method determines how paired ODUs will recognize each other. **Link Access:** Each ODU must be configured with Target MAC Address equal to the MAC Address of the other unit. **Link Name Access:** Both ODUs must be configured with the same Link Name.
Target MAC Address	Only displayed when Access Method is set to **Link Access**. This is the MAC Address of the peer unit that will be at the other end of the wireless link. This is used by the system to ensure the unit establishes a wireless link to the correct peer. The MAC Address can be found embedded within the serial number of the unit. The last six characters of the serial number are the last three bytes of the unit's MAC address.
Link Name	Only displayed when Access Method is set to **Link Name Access**. Link Name may consist of letters (A-Z and a-z), numbers (0-9), spaces, and the following special characters: (),-.,:<=>[]_{} Link Name must be same at both ends and different to site name.
Dual Payload	**Disabled:** The link maximizes robustness against fading and interference. **Enabled:** The link attempts to reach maximum throughput at the expense of robustness against fading and interference.

Attribute	Meaning
Max Receive Modulation Mode	The maximum mode the unit will use as its adaptive modulation. By default the Max Receive Modulation Mode is the highest mode available. For minimum error rates, set the maximum modulation mode to the minimum necessary to carry the required traffic.
Lowest Ethernet Modulation Mode	The lowest modulation mode that must be achieved before the link is allowed to bridge Ethernet frames.
Link Mode Optimization	**IP Traffic:** The link is optimized for IP traffic to provide the maximum possible link capacity. **TDM Traffic:** The link is optimized for TDM traffic to provide the lowest possible latency.
Regulatory Band	The regulatory band selected from the list in the license key.
Channel Bandwidth	Bandwidth of the transmit and receive radio channels.
Link Symmetry	Only displayed when Master Slave Mode is set to **Master**. **Adaptive**: Allows link symmetry to vary dynamically in response to offered traffic load. This is not supported in the following cases: • Where radar avoidance is mandated in the region. • Link Mode Optimization is set to **TDM Traffic**. **"2 to 1"**, "**1 to 1"** or "**1 to 2"**: There is a fixed division between transmit and receive time in the TDD frame of the master ODU. The first number in the ratio represents the time allowed for the transmit direction and the second number represents the time allowed for the receive direction. The appropriate matching Link Symmetry is set at the slave ODU automatically. For example, if Link Symmetry is set to "**2 to 1"** at the master ODU, then the slave ODU will be set automatically as "**1 to 2"**. In this example, the master-slave direction has double the capacity of the slave-master direction.
Spectrum Management Control	In regions that do not mandate DFS (radar detection), the options are: **DSO** **Fixed Frequency** In regions that mandate DFS (radar detection), the options are: **DFS** **DFS with DSO** This attribute is disabled if the regulatory requirement is fixed frequency only.

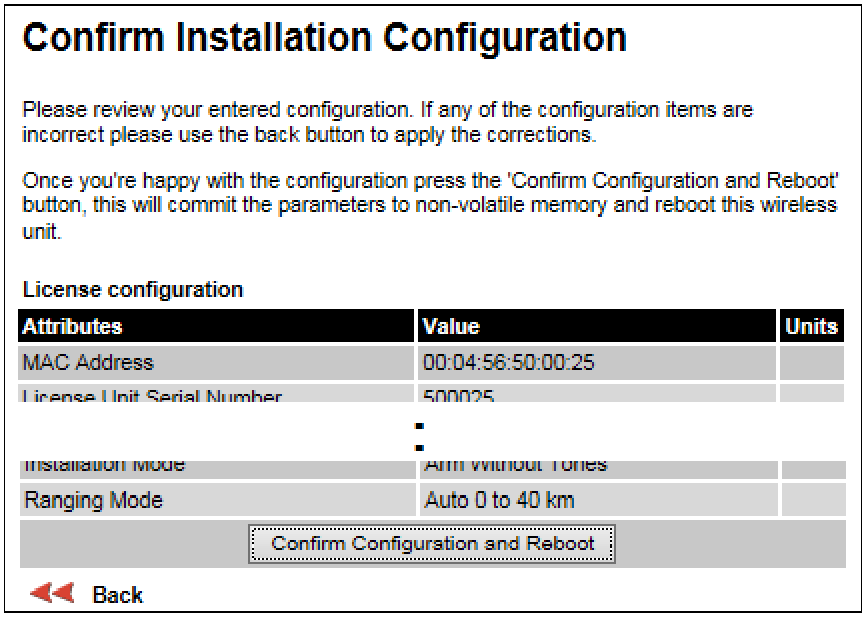
Attribute	Meaning
Lower Center Frequency	The center frequency (MHz) of the lowest channel that may be used by this link. Not displayed when Spectrum Management Control is set to **Fixed Frequency**. Use this attribute to slide the available channels up and down the band.
Default Raster	This is only displayed when Spectrum Management Control is set to **Fixed Frequency**. Limits frequency selection to the unit's default raster setting.
Fixed Tx Frequency, Fixed Rx Frequency	This is only displayed when Spectrum Management Control is set to **Fixed Frequency**. The settings must be compatible at each end of the link. Once configured, the spectrum management software will not attempt to move the wireless link to a channel with lower co-channel or adjacent channel interference. Therefore this mode of operation is only recommended for deployments where the installer has a good understanding of the prevailing interference environment.
Tx Color Code, Rx Color Code	Tx Color Code and Rx Color Code may be used to minimize interference in a dense network of synchronized PTP 650 units where some of the units are operating on the same frequency. When this type of network is designed, the Color Code values are normally specified in the link planning report. In all other cases, Cambium Networks recommend that Tx Color Code and Rx Color Code are left at the default value of **A**. The value of Tx Color Code MUST always match the value of Rx Color Code at the other end of the link.
Antenna Gain	Only displayed when the ODU is connectorized. Gain of the remote antenna.
Cable Loss	Only displayed when the ODU is connectorized. Loss in the ODU-antenna RF cable. If there is a significant difference in length of the RF cables for the two antenna ports, then the average value should be entered.
Maximum Transmit Power	The maximum power (dBm) at which the unit will transmit, configurable in steps of 1 dB. Its maximum value is controlled by the selected combination of Regulatory Band, Bandwidth and (for connectorized units) Antenna Gain and Cable Loss. To prepare for antenna alignment, set this attribute to the alignment value specified in the installation report (PTP LINKPlanner). To prepare for link operation, set this attribute to the operational value specified in the installation report (PTP LINKPlanner). This may be higher than the alignment value.

Attribute	Meaning
Installation Mode	**Arm With Tones**: Audio tones will be emitted during antenna alignment (the recommended option). **Arm Without Tones**: Audio tones will not be emitted during antenna alignment. **Change Config Without Arming**: Configuration changes will be made without arming the ODU for alignment.
Ranging Mode	This can only be modified if Installation Mode is **Arm With Tones** or **Arm Without Tones**. **Auto..**: During alignment, the wireless units use algorithms to calculate link range. To implement automatic ranging, select a value that corresponds to the estimated maximum range of the link: **Auto 0 to 40 km** (0 to 25 miles). **Auto 0 to 100km** (0 to 62 miles). **Auto 0 to 200km** (0 to 125 miles). **Target Range**: During alignment, the wireless units use the approximate link distance (entered in Target Range) to calculate link range. The main advantage of Target Range mode is that it reduces the time taken by the units to range. If preferred, range functions can be configured to operate in miles, as described in Webpage Properties page on page 6-49.
Target Range	Only available when Ranging Mode is set to **Target Range**. The approximate distance between the two wireless units to within ± 1 km. Enter the same value at both ends of the link.

Confirm Installation Configuration page

Menu option: **Installation** (Figure 65). Use this page to review and confirm the updated wireless configuration of the unit.

Figure 65 Confirm Installation Configuration page (top and bottom of page shown)



Confirm Installation Configuration

Please review your entered configuration. If any of the configuration items are incorrect please use the back button to apply the corrections.

Once you're happy with the configuration press the 'Confirm Configuration and Reboot' button, this will commit the parameters to non-volatile memory and reboot this wireless unit.

License configuration

Attributes	Value	Units
MAC Address	00:04:56:50:00:25	
License Unit Serial Number	500025	
	:	
Installation Mode	Arm Without Tones	
Ranging Mode	Auto 0 to 40 km	

Procedure:

- To undo or correct any updates, click **Back**.
- To confirm the updates and arm the installation, click **Confirm Configuration and Reboot** and click **OK** to reboot the unit.
- If IP Address, Subnet Mask or Gateway IP Address have been changed: reconfigure the local management PC to use an IP address that is valid for the network. Refer to Configuring the management PC on page 6-5.
- If IP Address has been changed, use the new IP address to log into the unit.

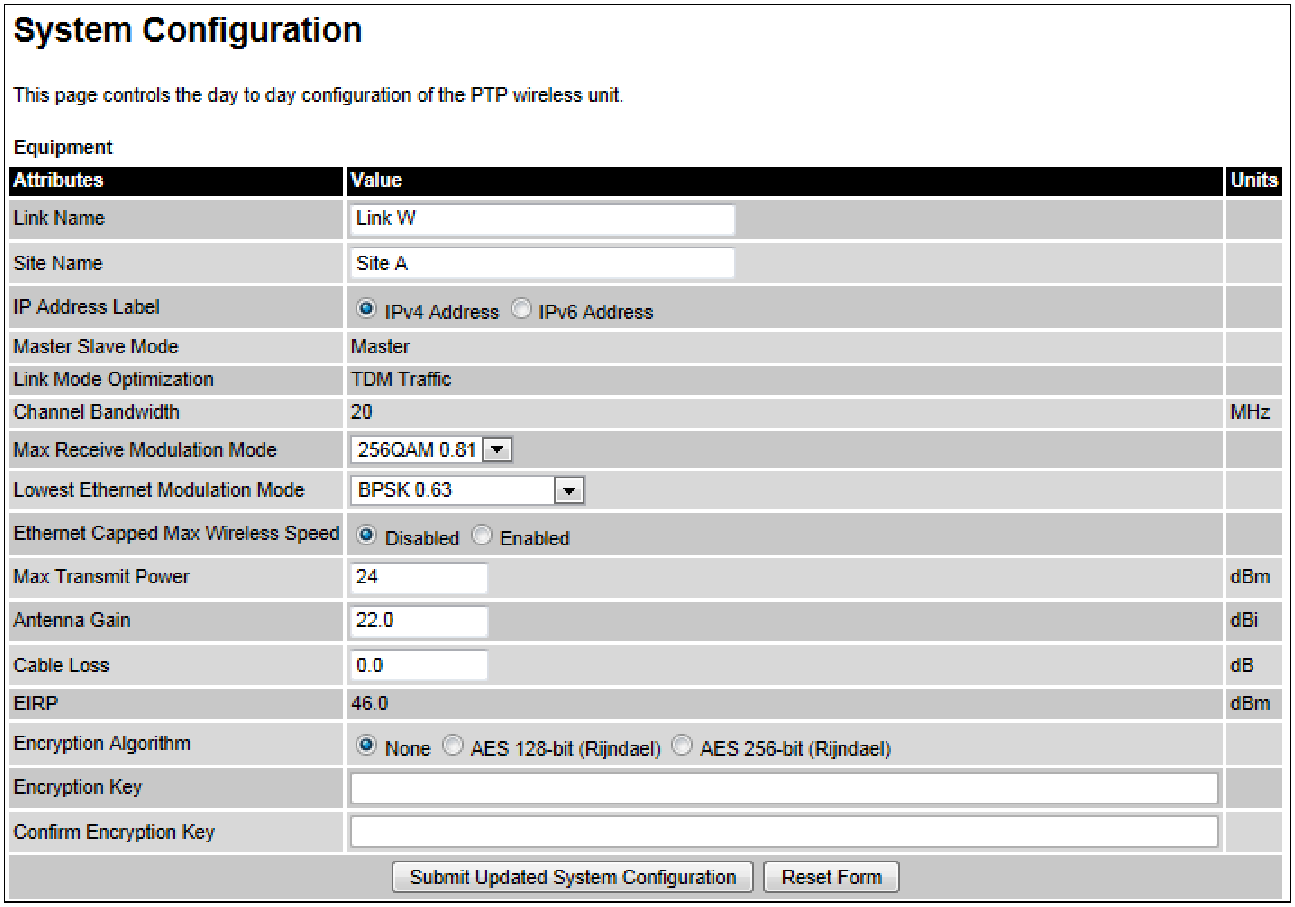
System menu

This section describes how to configure the IP and Ethernet interfaces of the PTP 650 unit.

System Configuration page

Menu option: **System > Configuration** (Figure 66). Use this page to enable AES encryption and to review and update key wireless attributes of the unit.

Figure 66 System Configuration page



System Configuration

This page controls the day to day configuration of the PTP wireless unit.

Equipment

Attributes	Value	Units
Link Name	Link W	
Site Name	Site A	
IP Address Label	● IPv4 Address ○ IPv6 Address	
Master Slave Mode	Master	
Link Mode Optimization	TDM Traffic	
Channel Bandwidth	20	MHz
Max Receive Modulation Mode	256QAM 0.81	
Lowest Ethernet Modulation Mode	BPSK 0.63	
Ethernet Capped Max Wireless Speed	● Disabled ○ Enabled	
Max Transmit Power	24	dBm
Antenna Gain	22.0	dBi
Cable Loss	0.0	dB
EIRP	46.0	dBm
Encryption Algorithm	● None ○ AES 128-bit (Rijndael) ○ AES 256-bit (Rijndael)	
Encryption Key		
Confirm Encryption Key		

Caution

Configuring link encryption over an operational link will necessitate a service outage. Therefore, the configuration process should be scheduled during a period of low link utilization.

Procedure:

- If AES encryption is required but the System Configuration page does not contain the Encryption Algorithm or Encryption Key attributes, then order the necessary AES capability upgrade, generate a license key and enter it on the Software License Key page (Software License Key page on page 6-12).
- Update the attributes (Table 70).
- To save changes, click **Submit Updated System Configuration**.
- If a reboot request is displayed, click **Reboot Wireless Unit** and **OK** to confirm.

Table 70 System Configuration attributes

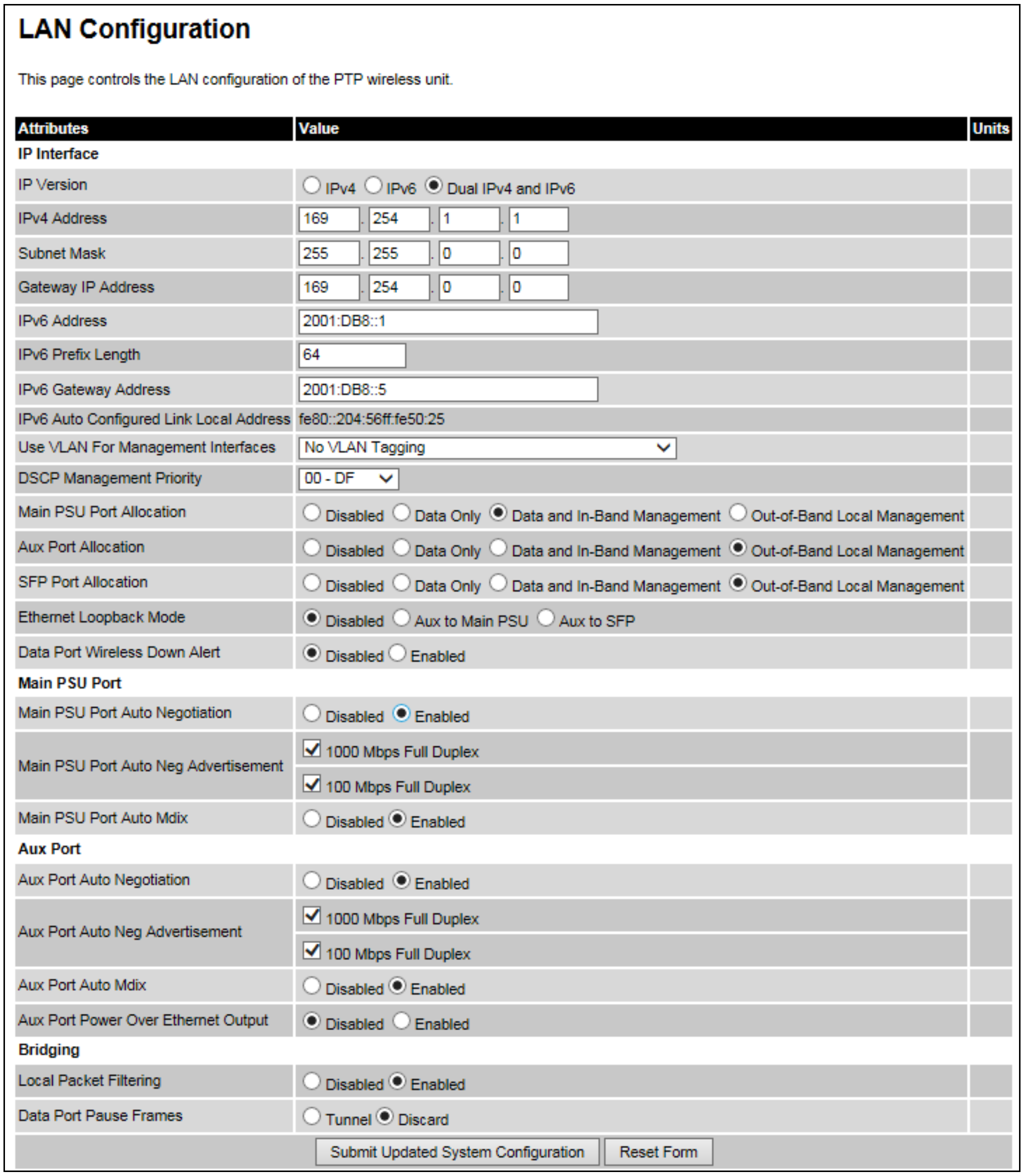
Attribute	Meaning
Link Name	Link Name may consist of letters (A-Z and a-z), numbers (0-9), spaces, and the following special characters: (),-.,:<=>[]_{}. Link Name must be same at both ends and different to site name.
Site Name	User defined name for the site, with additional notes (if required).
IP Address Label	Read only. The IP Address version used to identify the unit in SMTP messages, fault logs and other system outputs. **IPv4** or **IPv6**: The unit is identified using its IPv4 or IPv6 Address. These options are only available when IP Version is set to **Dual IPv4 and IPv6** in the in the LAN Configuration page (Table 71).
Master Slave Mode	**Master:** The unit is a Master, that is, it controls the point-to-point link and its maintenance. On startup, the Master transmits until a link with the Slave is made. **Slave:** The unit is a Slave, that is, it listens for its peer and only transmits when the peer has been identified. Read only.
Link Mode Optimization	**IP Traffic:** The link is optimized for IP traffic to provide the maximum possible link capacity. **TDM Traffic:** The link is optimized for TDM traffic to provide the lowest possible latency. Read only.
Channel Bandwidth	Bandwidth of the transmit and receive radio channels. Read only.
Max Receive Modulation Mode	The maximum mode the unit will use as its adaptive modulation. By default the Max Receive Modulation Mode is the highest mode available. For minimum error rates, set the maximum modulation mode to the minimum necessary to carry the required traffic.

Attribute	Meaning
Lowest Ethernet Modulation Mode	The lowest modulation mode that must be achieved before the link is allowed to bridge Ethernet frames.
Ethernet Capped Max Wireless Speed	**Disabled**: Wireless speed is not limited by the connected Ethernet link. **Enabled:** Wireless speed is limited to a mode that the connected Ethernet link can sustain. If either ODU is connected to an Ethernet link operating at less than 1000 Mbps, set this attribute to **Enabled**.
Max Transmit Power	The maximum power (dBm) at which the unit will transmit, configurable in steps of 1 dB. Its maximum value is controlled by the combination of the selected Regulatory Band, Bandwidth and (for connectorized units) Antenna Gain and Cable Loss. To prepare for antenna alignment, set this attribute to the alignment value specified in the installation report (PTP LINKPlanner). To prepare for link operation, set this attribute to the operational value specified in the installation report (PTP LINKPlanner). This may be higher than the alignment value.
Antenna Gain	Only displayed when the ODU is connectorized. Gain of the remote antenna.
Cable Loss	Only displayed when the ODU is connectorized. Loss in the ODU-antenna RF cable. If there is a significant difference in length of the RF cables for the two antenna ports, then the average value should be entered.
EIRP	Only displayed when the ODU is connectorized. Effective Isotropic Radiated Power (EIRP) describes the strength of the radio signal leaving the wireless unit. Use it to verify that the link configuration (Max Transmit Power, Antenna Gain and Cable Loss) does not exceed any applicable regulatory limit. Read only.
Encryption Algorithm	Only displayed when AES encryption is enabled by license key. Values are: **None**, **AES 128-bit** or **AES 256-bit**. Use the same setting at both link ends.
Encryption Key	Only displayed when AES encryption is enabled by license key. The key consists of 32 or 64 case-insensitive hexadecimal characters. Use the same key at both link ends.
Confirm Encryption Key	Only displayed when AES encryption is enabled by license key. Retype the Encryption Key.

LAN Configuration page

Menu option: **System > Configuration > LAN Configuration** (Figure 67). Use this page to control how users connect to the PTP 650 web interface, either from a locally connected computer or from a management network.

Figure 67 LAN Configuration page (showing Dual IPv4 and IPv6)



LAN Configuration

This page controls the LAN configuration of the PTP wireless unit.

Attributes	Value	Units
IP Interface		
IP Version	○ IPv4 ○ IPv6 ● Dual IPv4 and IPv6	
IPv4 Address	169 . 254 . 1 . 1	
Subnet Mask	255 . 255 . 0 . 0	
Gateway IP Address	169 . 254 . 0 . 0	
IPv6 Address	2001:DB8::1	
IPv6 Prefix Length	64	
IPv6 Gateway Address	2001:DB8::5	
IPv6 Auto Configured Link Local Address	fe80::204:56ff:fe50:25	
Use VLAN For Management Interfaces	No VLAN Tagging	
DSCP Management Priority	00 - DF	
Main PSU Port Allocation	○ Disabled ○ Data Only ● Data and In-Band Management ○ Out-of-Band Local Management	
Aux Port Allocation	○ Disabled ○ Data Only ○ Data and In-Band Management ● Out-of-Band Local Management	
SFP Port Allocation	○ Disabled ○ Data Only ○ Data and In-Band Management ● Out-of-Band Local Management	
Ethernet Loopback Mode	● Disabled ○ Aux to Main PSU ○ Aux to SFP	
Data Port Wireless Down Alert	● Disabled ○ Enabled	
Main PSU Port		
Main PSU Port Auto Negotiation	○ Disabled ● Enabled	
Main PSU Port Auto Neg Advertisement	☑ 1000 Mbps Full Duplex ☑ 100 Mbps Full Duplex	
Main PSU Port Auto Mdix	○ Disabled ● Enabled	
Aux Port		
Aux Port Auto Negotiation	○ Disabled ● Enabled	
Aux Port Auto Neg Advertisement	☑ 1000 Mbps Full Duplex ☑ 100 Mbps Full Duplex	
Aux Port Auto Mdix	○ Disabled ● Enabled	
Aux Port Power Over Ethernet Output	● Disabled ○ Enabled	
Bridging		
Local Packet Filtering	○ Disabled ● Enabled	
Data Port Pause Frames	○ Tunnel ● Discard	

Caution

Before configuring a VLAN for management interfaces, ensure that the VLAN is accessible, otherwise the unit will be inaccessible after the next reboot.

Caution

Before configuring in-band management, ensure that the Master and Slave units are configured with different IP addresses, otherwise the management agent will not be able to distinguish the two units.

Caution

Auto-negotiation and forced Ethernet configuration:

- To operate an Ethernet link at a fixed speed, set Auto Negotiation to **Enabled** and limit Auto Neg Advertisement to the desired speed. If constrained auto-negotiation fails, set Auto Negotiation to **Disabled** (forced Ethernet configuration), but only as a last resort.
- Both ends of an Ethernet link must be configured identically, because forced and auto-negotiation are not compatible: a mixed configuration will cause a duplex mismatch, resulting in greatly reduced data capacity.
- The Auto Neg Advertisement or Forced Configuration data rates must be within the capability of the Ethernet link partner, otherwise loss of service will occur.

Procedure:

1 Review and update the attributes: IP Interface (Table 71); Main PSU or Aux Port (Table 72); Bridging (Table 73).

2 To save changes, click **Submit Updated System Configuration**. Some updates will cause the system to reboot.

3 If Main PSU Port Allocation has been changed to **Disabled** or **Data Only**, connect the management PC to whichever port (Aux or SFP) has been set to **Data and In-Band Management** or **Out-of-Band Local Management**.

4 If IP Address, Subnet Mask or Gateway IP Address have been changed, reconfigure the local management PC to use an IP address that is valid for the network. Refer to Configuring the management PC on page 6-5.

5 If IP Address has been changed, use the new IP address to log into the unit.

Table 71 IP interface attributes

Attribute	Meaning
IP Version	The internet protocols to be supported by this ODU: **IPv4:** IPv4 protocols only. IPv4 attributes are displayed. **IPv6:** IPv6 protocols only. IPv6 attributes are displayed. **Dual IPv4 and IPv6:** Both IPv4 and IPv6 protocols. IPv4 and IPv6 attributes are displayed.
IPv4 Address	The IPv4 internet protocol address. This address is used by the family of Internet protocols to uniquely identify this unit on a network.
Subnet Mask	The address range of the connected IPv4 network.
Gateway IP Address	The IPv4 address of a computer on the current network that acts as an IPv4 gateway. A gateway acts as an entrance and exit to frames from and to other networks.
IPv6 Address	The IPv6 internet protocol address. This address is used by the family of Internet protocols to uniquely identify this unit on a network.
IPv6 Prefix Length	Length of the IPv6 subnet prefix (default 64 bits).
IPv6 Gateway Address	The IPv6 address of a computer on the current network that acts as an IPv6 gateway. A gateway acts as an entrance and exit to frames from and to other networks. It is usual to use the link-local address of the gateway.
IPv6 Auto Configured Link Local Address	The link-local address of the IPv6 gateway (displayed only, not updateable).
Use VLAN For Management Interfaces	VLAN tagging options for the management interfaces: **No VLAN Tagging** **IEEE 802.1Q Tagged (C-Tag, Type 8100)** **IEEE 802.1ad Tagged (S-Tag or B-Tag, Type 88a8)** Ensure that the configured VLAN is accessible, otherwise it will not be possible to access the unit following the next reboot. The PTP 650 management function is only compatible with single VLAN tagged frames. Any management frame with two or more tags will be ignored.

Attribute	Meaning
VLAN Management VID	Only displayed when Use VLAN for Management Interfaces is not set to **No VLAN Tagging**. The VLAN VID (range 0 to 4094) that will be included in Ethernet frames generated by the management interfaces.
VLAN Management Priority	Only displayed when Use VLAN for Management Interfaces is not set to **No VLAN Tagging**. The VLAN priority (range 0 to 7) that will be included in Ethernet frames generated by the management interfaces.
DSCP Management Priority	Differentiated Services Code Point (DSCP) value to be inserted in the IP header of all IP datagrams transmitted by the management interface.
Main PSU Port Allocation Aux Port Allocation SFP Port Allocation	**Disabled**: The port is not used. **Data Only**: The port handles customer data only. **Data and In-Band Management**: The port handles both customer data and network management data. It can be used to access the web interface of the local unit, and if the wireless link is established, the remote unit. Ensure that the local and remote units have different IP addresses. **Out-of-band Local Management**: The port handles local management data only. It can be used to access the web interface of the local unit. Only one port can be allocated to customer data. At least one port must be allocated to management data.
Ethernet Loopback Mode	Sets a temporary loopback between the selected ports. The loopback is disabled on a reboot. This mode is provided to allow access to a device connected to the local ODU Aux port via either the main PSU or SFP port. Loopback does not work with jumbo frames: the maximum frame size is 1536 bytes in loopback.
Data Port Wireless Down Alert	**Disabled:** The data Ethernet link will not be dropped when the wireless link drops. **Enabled:** The data Ethernet link will be dropped briefly when the wireless link drops. This signals to the connected network equipment that this link is no longer available. Connected Ethernet switches can be configured to forward Ethernet frames on an alternative path identified using the Spanning Tree Protocol (STP).

Table 72 Main PSU Port and Aux Port attributes

Attribute	Meaning
Auto Negotiation	**Disabled:** Configuration of the Ethernet interface is forced. **Enabled:** Configuration of the Ethernet interface is automatically negotiated (default). This is the preferred setting. See the caution at the start of this section about auto-negotiation versus forced Ethernet configuration. Use the same setting for the Ethernet link partner.
Auto Neg Advertisement	Only displayed when Auto Negotiation is set to **Enabled**. The data rate that the auto-negotiation mechanism will advertise as available on the Ethernet interface (1000 Mbps or 100 Mbps Full Duplex). Select a data rate that is within the capability of the Ethernet link partner. Use the same setting for the Ethernet link partner.
Forced Configuration	Only displayed when Auto Negotiation is set to **Disabled**. This forces the speed and duplex setting of the Ethernet interface. Over-the-air throughput will be capped to the rate of the Ethernet interface at the receiving end of the link. Select a data rate that is within the capability of the Ethernet link partner. Use the same setting for the Ethernet link partner.
Auto Mdix	**Disabled:** The Auto Medium Dependent Interface (MDI)/Medium Dependent Interface Crossover (MDIX) capability is disabled. **Enabled:** The Auto Medium Dependent Interface (MDI)/Medium Dependent Interface Crossover (MDIX) capability is enabled.
Power Over Ethernet Output	Aux port only. **Disabled:** The ODU does not supply power to the auxiliary device. **Enabled:** The ODU supplies power to the auxiliary device.

Table 73 Bridging attributes

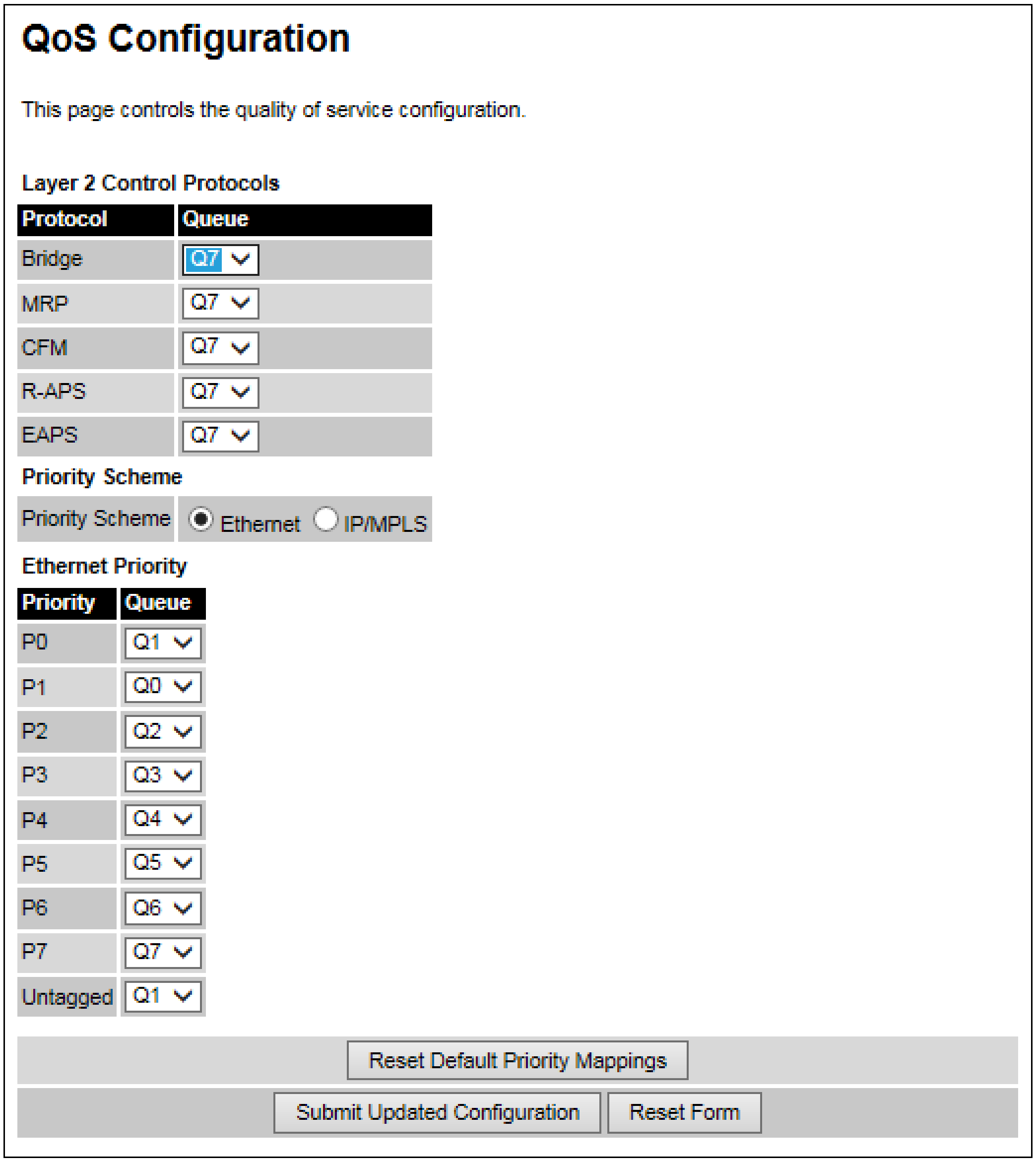
Attribute	Meaning
Local Packet Filtering	**Enabled:** The management agent learns the location of end stations from the source addresses in received management frames. The agent filters transmitted management frames to ensure that the frame is transmitted at the Ethernet (data or management) port, or over the wireless link as appropriate. If the end station address is unknown, then management traffic is transmitted at the Ethernet port and over the wireless link. In out-of-band local management mode, management frames are not transmitted over the wireless link, and so address learning is not active.
Data Port Pause Frames	Controls whether the bridge tunnels or discards Layer 2 pause frames arriving at the data port. Such frames are identified by the destination MAC Address being equal to 01-80-C2-00-00-01.

QoS Configuration page

Menu option: **System > Configuration > QoS Configuration** (Figure 68 or Figure 69).

Use this page to control the quality of service configuration. Classification may be based on fields in the Ethernet header (Layer 2) or in the network header (Layer 3). The unit recognizes two network layer protocols: IP and MPLS.

Figure 68 QoS Configuration page (Ethernet)



QoS Configuration

This page controls the quality of service configuration.

Layer 2 Control Protocols

Protocol	Queue
Bridge	Q7
MRP	Q7
CFM	Q7
R-APS	Q7
EAPS	Q7

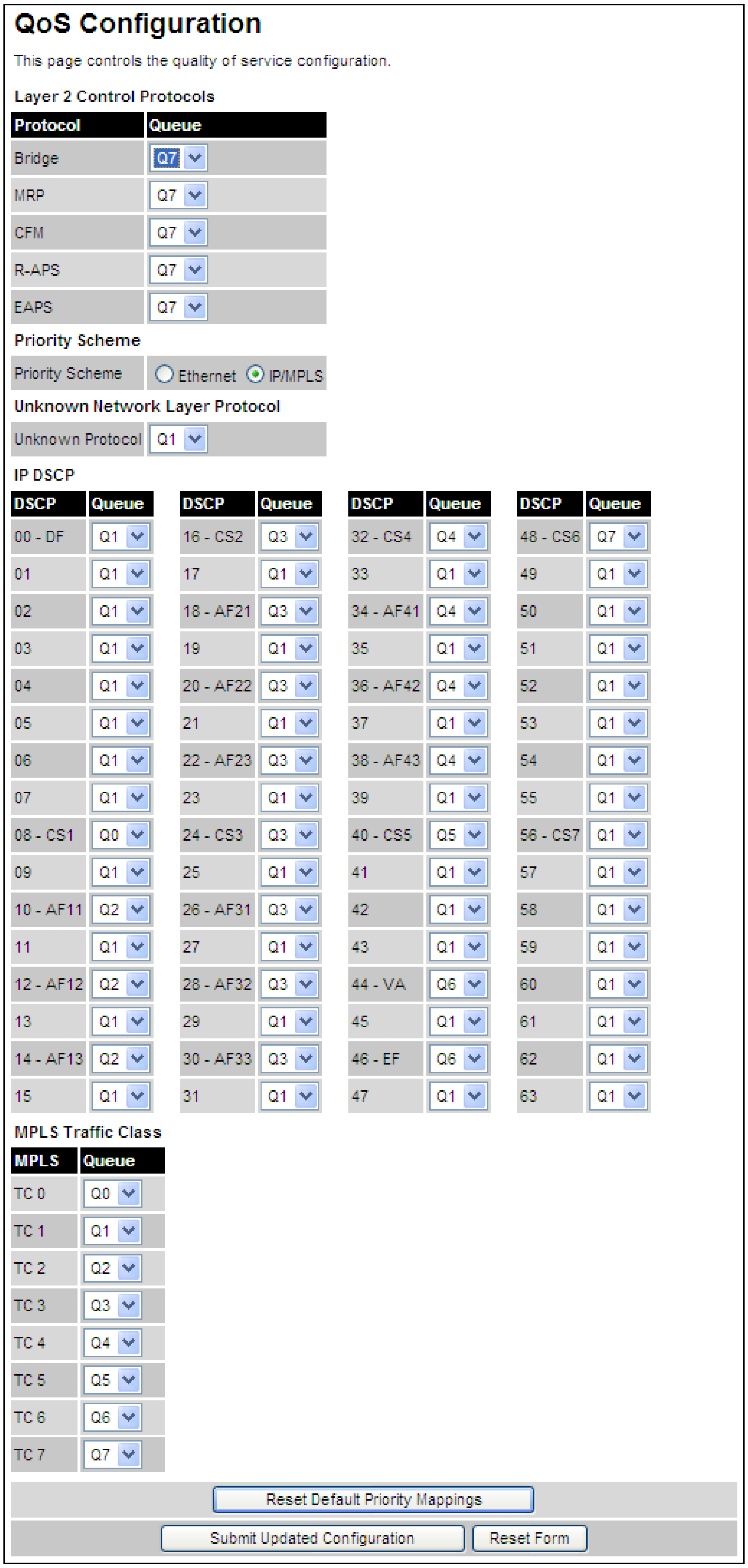
Priority Scheme

Priority Scheme ● Ethernet ○ IP/MPLS

Ethernet Priority

Priority	Queue
P0	Q1
P1	Q0
P2	Q2
P3	Q3
P4	Q4
P5	Q5
P6	Q6
P7	Q7
Untagged	Q1

Figure 69 QoS Configuration page (IP/MPLS)



QoS Configuration

This page controls the quality of service configuration.

Layer 2 Control Protocols

Protocol	Queue
Bridge	Q7
MRP	Q7
CFM	Q7
R-APS	Q7
EAPS	Q7

Priority Scheme

Priority Scheme	○ Ethernet ● IP/MPLS

Unknown Network Layer Protocol

Unknown Protocol	Q1

IP DSCP

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
00 - DF	Q1	16 - CS2	Q3	32 - CS4	Q4	48 - CS6	Q7
01	Q1	17	Q1	33	Q1	49	Q1
02	Q1	18 - AF21	Q3	34 - AF41	Q4	50	Q1
03	Q1	19	Q1	35	Q1	51	Q1
04	Q1	20 - AF22	Q3	36 - AF42	Q4	52	Q1
05	Q1	21	Q1	37	Q1	53	Q1
06	Q1	22 - AF23	Q3	38 - AF43	Q4	54	Q1
07	Q1	23	Q1	39	Q1	55	Q1
08 - CS1	Q0	24 - CS3	Q3	40 - CS5	Q5	56 - CS7	Q1
09	Q1	25	Q1	41	Q1	57	Q1
10 - AF11	Q2	26 - AF31	Q3	42	Q1	58	Q1
11	Q1	27	Q1	43	Q1	59	Q1
12 - AF12	Q2	28 - AF32	Q3	44 - VA	Q6	60	Q1
13	Q1	29	Q1	45	Q1	61	Q1
14 - AF13	Q2	30 - AF33	Q3	46 - EF	Q6	62	Q1
15	Q1	31	Q1	47	Q1	63	Q1

MPLS Traffic Class

MPLS	Queue
TC 0	Q0
TC 1	Q1
TC 2	Q2
TC 3	Q3
TC 4	Q4
TC 5	Q5
TC 6	Q6
TC 7	Q7

Procedures:

- Review and update the attributes: Layer 2 and Priority Scheme (Table 74).
- To use IEEE 802.1Q classification rules, click **Reset Default Priority Mappings**.
- To save changes, click: **Submit Updated Configuration**.

Note

Priority mapping must be configured the same at both Master and Slave units on the wireless link.

Table 74 QoS Configuration attributes

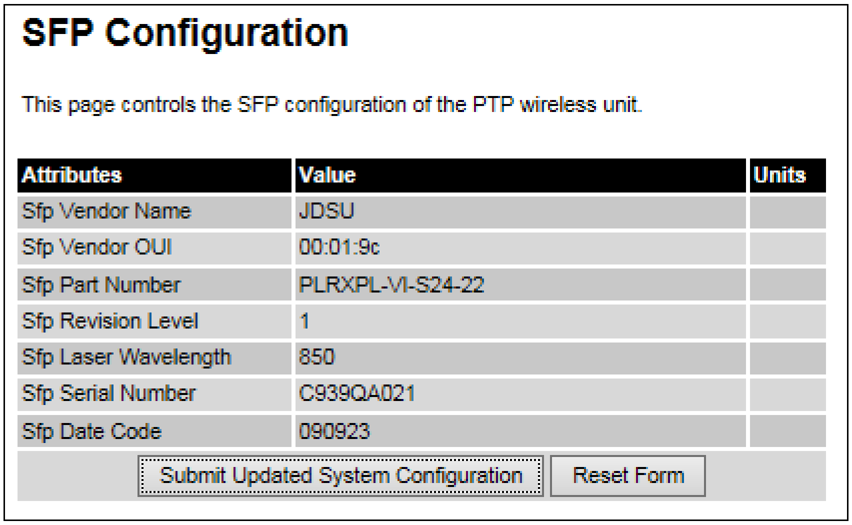
Attribute	Meaning
Bridge	The classification of each layer 2 control protocol (L2CP) to an egress queue at the wireless port.
MRP	
CFM	
R-APS	
EAPS	
Priority Scheme	**Ethernet**: Classification is based on fields in the Ethernet header (Layer 2). **IP/MPLS**: Classification is based on fields in the network header (Layer 3). IP includes IPv4 and IPv6.
Unknown Protocol	Only displayed when Priority Scheme is **IP/MPLS**. The classification of unknown network protocols (that is, not IP or MPLS) to an egress queue at the wireless port.

SFP Configuration page

Menu option: **System > Configuration > SFP Configuration**.

This page is only available when the ODU detects an optical (Figure 70) or copper (Figure 71) SFP module in the SFP port. Use it to configure the way in which the unit connects to the network via the SFP interface.

Figure 70 SFP Configuration page (optical SFP module)

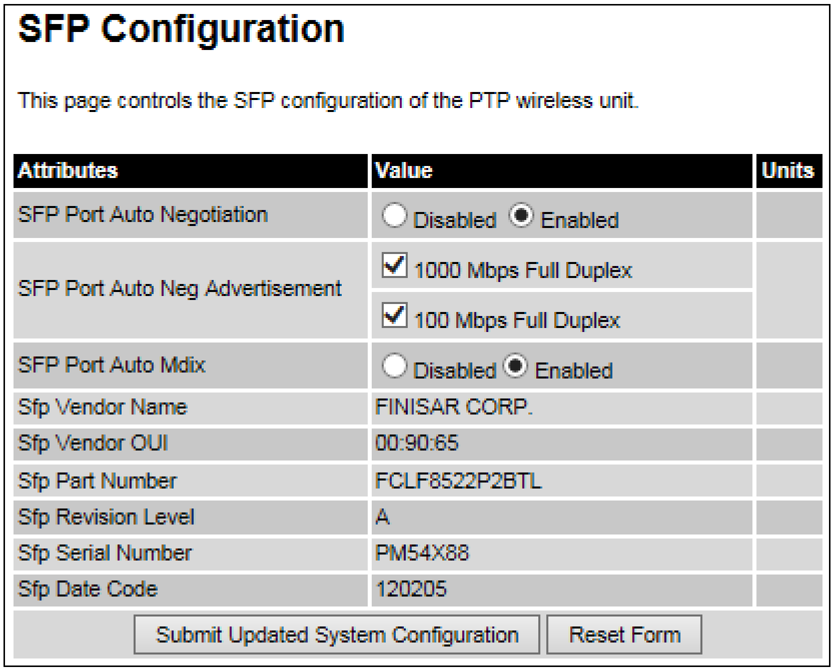


SFP Configuration

This page controls the SFP configuration of the PTP wireless unit.

Attributes	Value	Units
Sfp Vendor Name	JDSU	
Sfp Vendor OUI	00:01:9c	
Sfp Part Number	PLRXPL-VI-S24-22	
Sfp Revision Level	1	
Sfp Laser Wavelength	850	
Sfp Serial Number	C939QA021	
Sfp Date Code	090923	

Figure 71 SFP Configuration page (copper SFP module)



SFP Configuration

This page controls the SFP configuration of the PTP wireless unit.

Attributes	Value	Units
SFP Port Auto Negotiation	○ Disabled ● Enabled	
SFP Port Auto Neg Advertisement	☑ 1000 Mbps Full Duplex ☑ 100 Mbps Full Duplex	
SFP Port Auto Mdix	○ Disabled ● Enabled	
Sfp Vendor Name	FINISAR CORP.	
Sfp Vendor OUI	00:90:65	
Sfp Part Number	FCLF8522P2BTL	
Sfp Revision Level	A	
Sfp Serial Number	PM54X88	
Sfp Date Code	120205	

Procedure (only applies when copper SFP module is installed)**:**

- Update the attributes (Table 75).
- To save changes, click **Submit Updated System Configuration**.

Table 75 SFP Configuration (copper SFP module) attributes

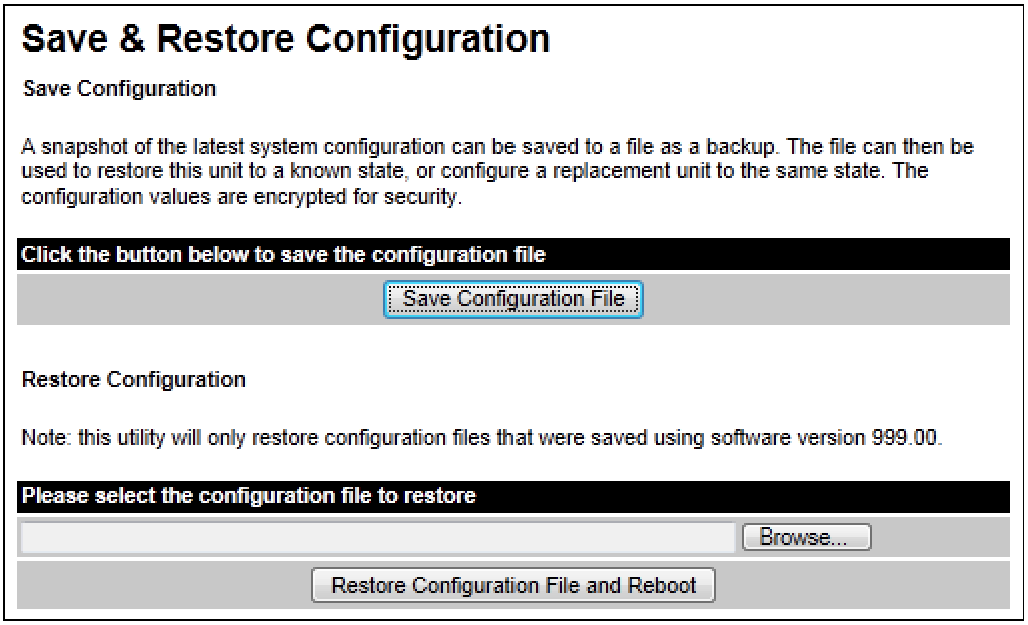
Attribute	Meaning
SFP Port Auto Negotiation	**Disabled:** Configuration of the Ethernet interface is forced. This is to be used as a last resort only if auto-negotiation fails. **Enabled:** Configuration of the Ethernet interface is automatically negotiated (default). This is the preferred setting.
SFP Port Auto Neg Advertisement	Only displayed when SFP Port Auto Negotiation is set to **Enabled**. The data rate that the auto-negotiation mechanism will advertise as available on the Ethernet interface (1000 Mbps or 100 Mbps Full Duplex). Select a data rate that is within the capability of the Ethernet link partner. Use the same setting for the Ethernet link partner.
Forced Configuration	Only displayed when SFP Port Auto Negotiation is set to **Disabled**. This forces the speed and duplex setting of the Ethernet interface. Over-the-air throughput will be capped to the rate of the Ethernet interface at the receiving end of the link. Select a data rate that is within the capability of the Ethernet link partner. Use the same setting for the Ethernet link partner.
Auto Mdix	**Disabled:** The Auto Medium Dependent Interface (MDI)/Medium Dependent Interface Crossover (MDIX) capability is disabled. **Enabled:** The Auto Medium Dependent Interface (MDI)/Medium Dependent Interface Crossover (MDIX) capability is enabled.

Save & Restore Configuration page

Menu option: **System > Configuration > Save And Restore** (Figure 72).

Use the Save & Restore Configuration page to take a snapshot of the latest system configuration as a backup. The file can then be used to restore this unit to a known state, or to configure a replacement unit to the same state. The configuration values are encrypted for security.

Figure 72 Save & Restore Configuration page



Save & Restore Configuration

Save Configuration

A snapshot of the latest system configuration can be saved to a file as a backup. The file can then be used to restore this unit to a known state, or configure a replacement unit to the same state. The configuration values are encrypted for security.

Click the button below to save the configuration file

Restore Configuration

Note: this utility will only restore configuration files that were saved using software version 999.00.

Please select the configuration file to restore

Save the system configuration in the following situations:

- After a new unit has been fully configured as described in this chapter.
- After any change has been made to the configuration.
- Before upgrading the unit to a new software version.
- After upgrading the unit to a new software version.

Note

The restore is only guaranteed to work if the installed software version has not been changed since the configuration file was saved. This is why the configuration should always be saved immediately after upgrading the software version.

Note

The license key is restored automatically if the configuration file is saved and then loaded on the same unit. However, the license key is not restored if the configuration file is loaded on a different unit. Before restoring configuration to a different PTP 650 unit, ensure that a valid license key is installed (with optional capabilities enabled where appropriate).

Most of the configuration can be restored from the backup. However, certain attributes that were part of the configuration are not saved or restored automatically. Use the web interface to reconfigure the following attributes:

- Usernames, passwords and roles for the web-based interface.
- Key of Keys
- HTTPS Entropy
- HTTPS Private Key
- HTTPS Public Key Certificate
- HTTP Access Enabled
- HTTPS Access Enabled
- Telnet Access Enabled
- HTTP Port Number
- HTTPS Port Number
- Telnet Port Number
- Encryption Algorithm
- Encryption Key
- SNMP Control Of HTTP And Telnet
- SNMP Control of Passwords

Procedures:

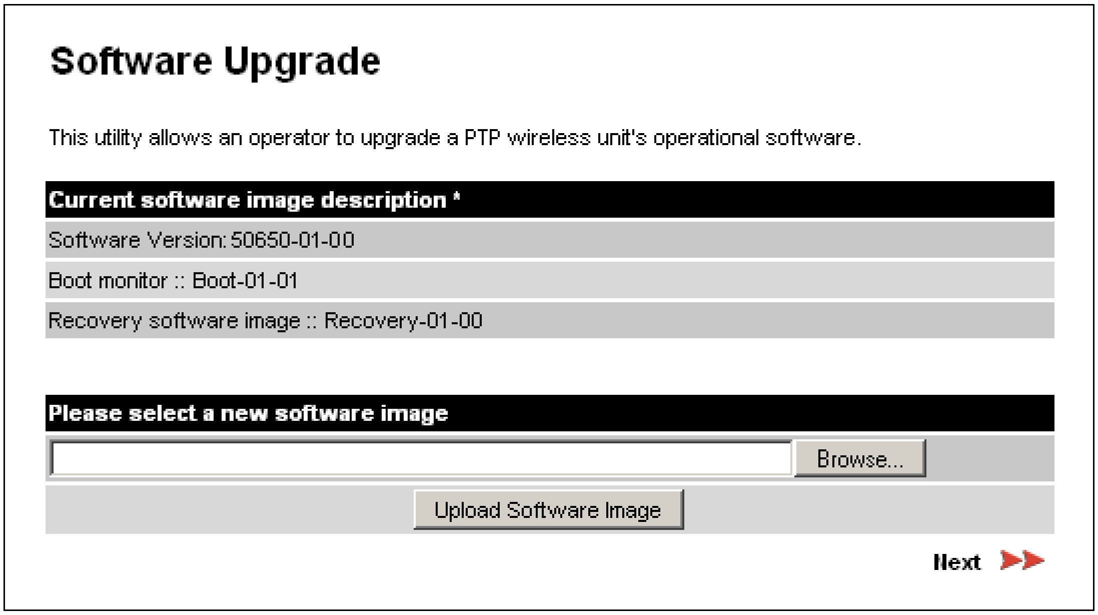
- To save the configuration:
  - Click Save Configuration File.
  - Save the file using the format **MAC-mm-mm-mm_IP-iii-iii-iii-iii.cfg**, where **mm-mm-mm** is MAC address of unit and **iii-iii-iii-iii** is Internet address of unit (IPv4 or IPv6, depending on IP address label).
- To restore the configuration:
  - Click **Browse** and navigate to the PC folder containing the saved configuration file (.cfg).
  - Click **Restore Configuration File and Reboot**.
  - Click **OK** to confirm the restore. The configuration file is uploaded and used to reconfigure the new unit to the same state as the old unit. On completion, the unit reboots.

Software Upgrade page

Menu option: **System > Software Upgrade** (Figure 73).

Use this page to upgrade the unit to a new version of PTP 650 operational software.

Figure 73 Software Upgrade page



Software Upgrade

This utility allows an operator to upgrade a PTP wireless unit's operational software.

Current software image description *
Software Version: 50650-01-00
Boot monitor :: Boot-01-01
Recovery software image :: Recovery-01-00

Please select a new software image

Caution

Ensure that the correct units are upgraded, as units cannot easily be downgraded afterwards.

Caution

Software version must be the same at both ends of the link. Limited operation may sometimes be possible with dissimilar software versions, but such operation is not supported by Cambium Networks.

Caution

If the link is operational, upgrade the remote end of the link first, then upgrade the local end. Otherwise, the remote end may not be accessible.

Preparation:

- Go to the Cambium Support web page (see Contacting Cambium Networks on page 1) and navigate to **Point-to-Point Software and Documentation**, **PTP 650 Series**.
- If the support web page contains a later Software Version than that installed on the PTP 650 unit, perform the procedure below.

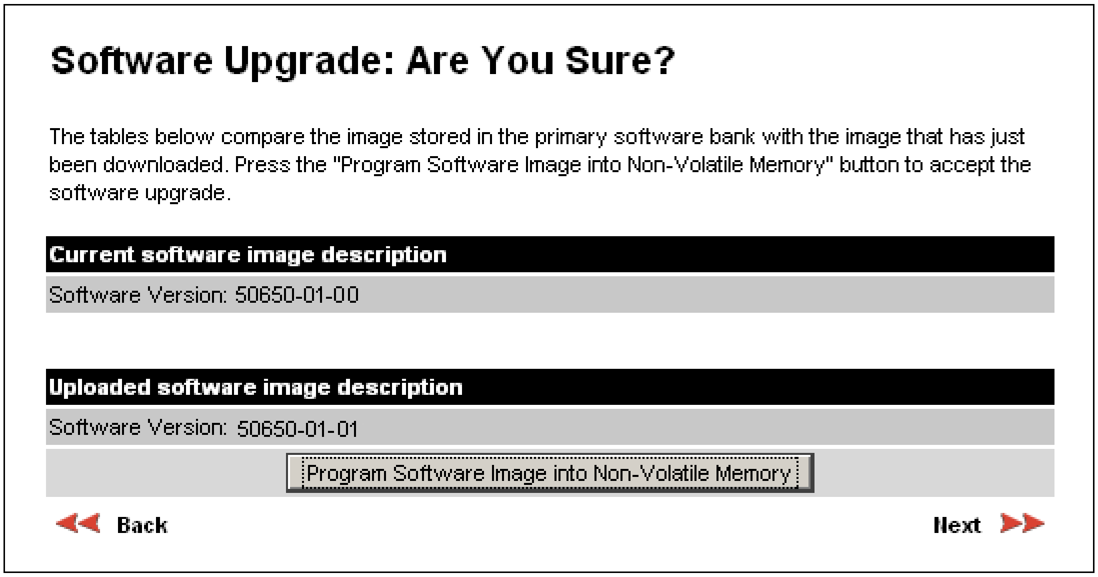
Procedure:

1 Save the system configuration; see Save & Restore Configuration page on page 6-34.

2 On the Cambium Support web page, select the latest PTP 650 software image (dld2 file) and save it to the local management PC.

3 On the Software Upgrade page, click **Browse**. Navigate to the folder containing the downloaded software image and click **Open**.

4 Click **Upload Software Image**. The Software Upgrade Confirmation page is displayed:



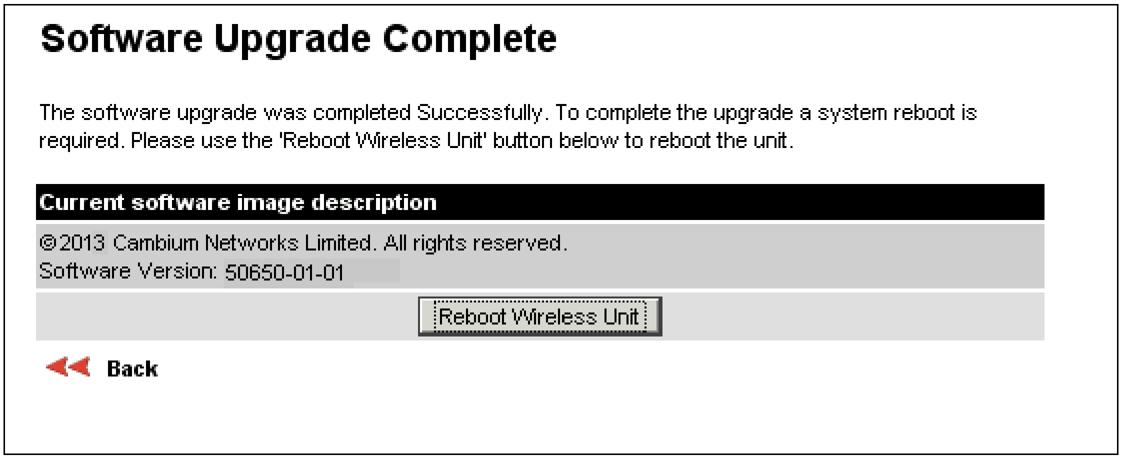
Software Upgrade: Are You Sure?

The tables below compare the image stored in the primary software bank with the image that has just been downloaded. Press the "Program Software Image into Non-Volatile Memory" button to accept the software upgrade.

Current software image description
Software Version: 50650-01-00

Uploaded software image description
Software Version: 50650-01-01

5 Click **Program Software Image into Non-Volatile Memory**. The Progress Tracker page is displayed. On completion, the Software Upgrade Complete page is displayed:



Software Upgrade Complete

The software upgrade was completed Successfully. To complete the upgrade a system reboot is required. Please use the 'Reboot Wireless Unit' button below to reboot the unit.

Current software image description
©2013 Cambium Networks Limited. All rights reserved. Software Version: 50650-01-01

6 Click **Reboot Wireless Unit**, then click **OK** to confirm. The unit reboots with the new software installed.

7 Save the post-upgrade system configuration; see Save & Restore Configuration page on page 6-34.

Management menu

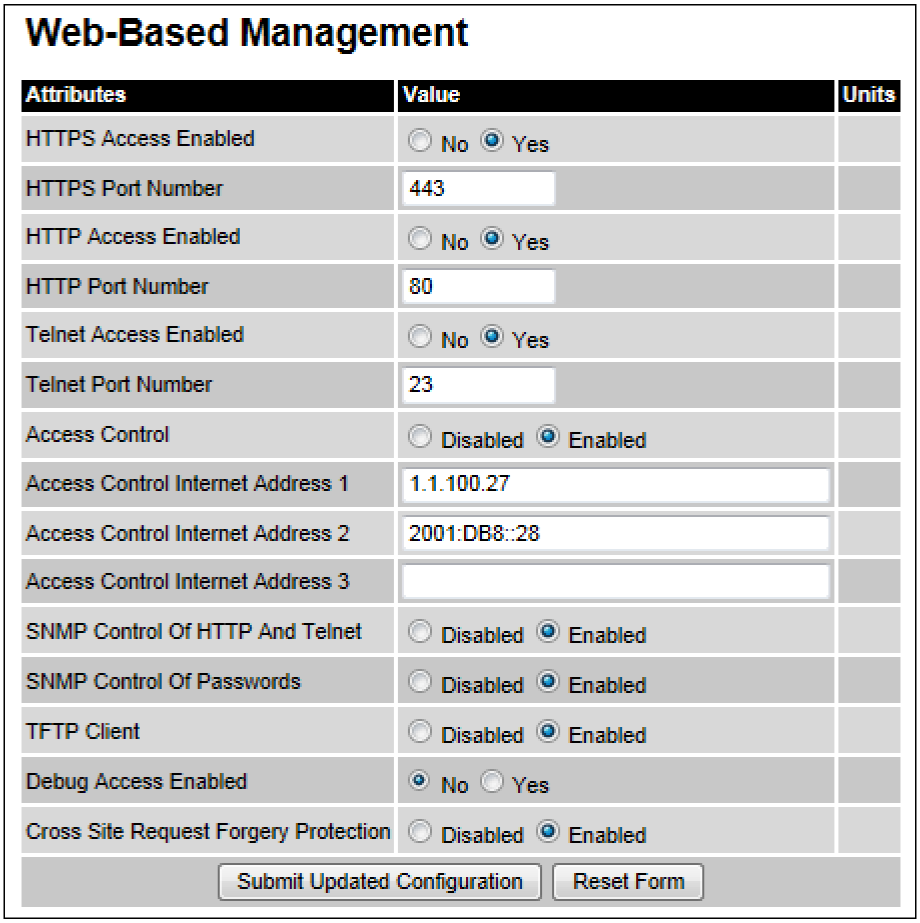
This section describes how to configure web-based management of the PTP 650 unit.

Web-Based Management page

Menu option: **Management > Web** (Figure 74).

Use this page to configure web-based management of the unit.

Figure 74 Web-Based Management page



Web-Based Management

Attributes	Value	Units
HTTPS Access Enabled	○ No ● Yes	
HTTPS Port Number	443	
HTTP Access Enabled	○ No ● Yes	
HTTP Port Number	80	
Telnet Access Enabled	○ No ● Yes	
Telnet Port Number	23	
Access Control	○ Disabled ● Enabled	
Access Control Internet Address 1	1.1.100.27	
Access Control Internet Address 2	2001:DB8::28	
Access Control Internet Address 3		
SNMP Control Of HTTP And Telnet	○ Disabled ● Enabled	
SNMP Control Of Passwords	○ Disabled ● Enabled	
TFTP Client	○ Disabled ● Enabled	
Debug Access Enabled	● No ○ Yes	
Cross Site Request Forgery Protection	○ Disabled ● Enabled	

Caution

If the HTTP, HTTPS, Telnet and SNMP interfaces are all disabled, then it will be necessary to use the Recovery image to reset IP & Ethernet Configuration back to defaults to re-enable the interfaces.

Note

The HTTP and Telnet interfaces should be disabled if the HTTPS interface is configured. (Preparing for HTTPS/TLS page 6-75).

Procedure:

- Review and update the attributes (Table 76).
- To save changes, click **Submit Updated Configuration**.

Table 76 Web-Based Management attributes

Attribute	Meaning
HTTPS Access Enabled	Only displayed when HTTPS is configured. **No:** The unit will not respond to any requests on the HTTPS port. **Yes:** The unit will respond to requests on the HTTPS port.
HTTPS Port Number	Only displayed when HTTPS is configured. The port number for HTTPS access. A value of zero means the wireless unit uses the default port.
HTTP Access Enabled	**No:** The unit will not respond to any requests on the HTTP port. **Yes:** The unit will respond to requests on the HTTP port. Remote management via HTTPS is not affected by this setting.
HTTP Port Number	The port number for HTTP access. A value of zero means the wireless unit uses the default port.
Telnet Access Enabled	**No:** The unit will not respond to any requests on the Telnet port. **Yes:** The unit will respond to requests on the Telnet port.
Telnet Port Number	The port number for Telnet access. A value of zero means the wireless unit uses the default port.
Access Control	Enables or disables access control to web-based management by Internet Address.
Access Control Internet Address 1/2/3	A list of up to three IPv4 or IPv6 Addresses permitted to perform web-based management. Only displayed when Access Control is set to **Enabled**.

Attribute	Meaning
SNMP Control of HTTP And Telnet	**Disabled:** Neither HTTP nor Telnet can be controlled remotely via SNMP. **Enabled:** Both HTTP and Telnet can be controlled remotely via SNMP.
SNMP Control of Passwords	**Enabled:** Passwords for identity-based user accounts in the web-based interface can be updated via SNMP. This option can be used together with SNMPv3 to provide a secure means to update passwords from a central network manager. **Disabled**: Passwords for identity-based user accounts can be updated only via the web-based interface (default).
TFTP Client	**Disabled:** The unit will not respond to any TFTP software download requests. **Enabled:** Software can be downloaded via TFTP, as described in Upgrading software using TFTP on page 6-96.
Debug Access Enabled	**Yes:** Cambium Technical Support is allowed to access the system to investigate faults.
Cross Site Request Forgery Protection	**Enabled:** The system is protected against cross-site request forgery attacks at the web-based interface.

Local User Accounts page

Menu option: **Management > Web > Local User Accounts**.

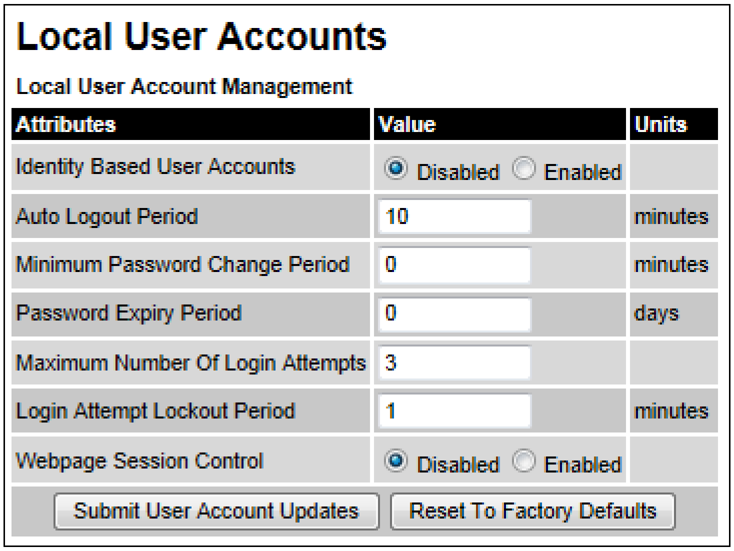
The contents of this page depend upon the setting of Identity Based User Accounts: **Disabled** (Figure 75) or **Enabled** (Figure 76).

Use this page to ensure that user access to the web-based management interface is controlled in accordance with the network operator's security policy. The Identity Based User Accounts option allows multiple users (from one to ten) to access the unit with one of three levels of access: Security Officer, System Administrator and Read Only. If Identity Based User Accounts are **Enabled**, this procedure may only be performed by a Security Officer.

Note

Local User Account Names, Roles and Passwords are critical security parameters that can be rest from the Zeroize CSPs page (Zeroize CSPs page on page 6-86**).**

Figure 75 Local User Accounts page (Identity Based User Accounts disabled)

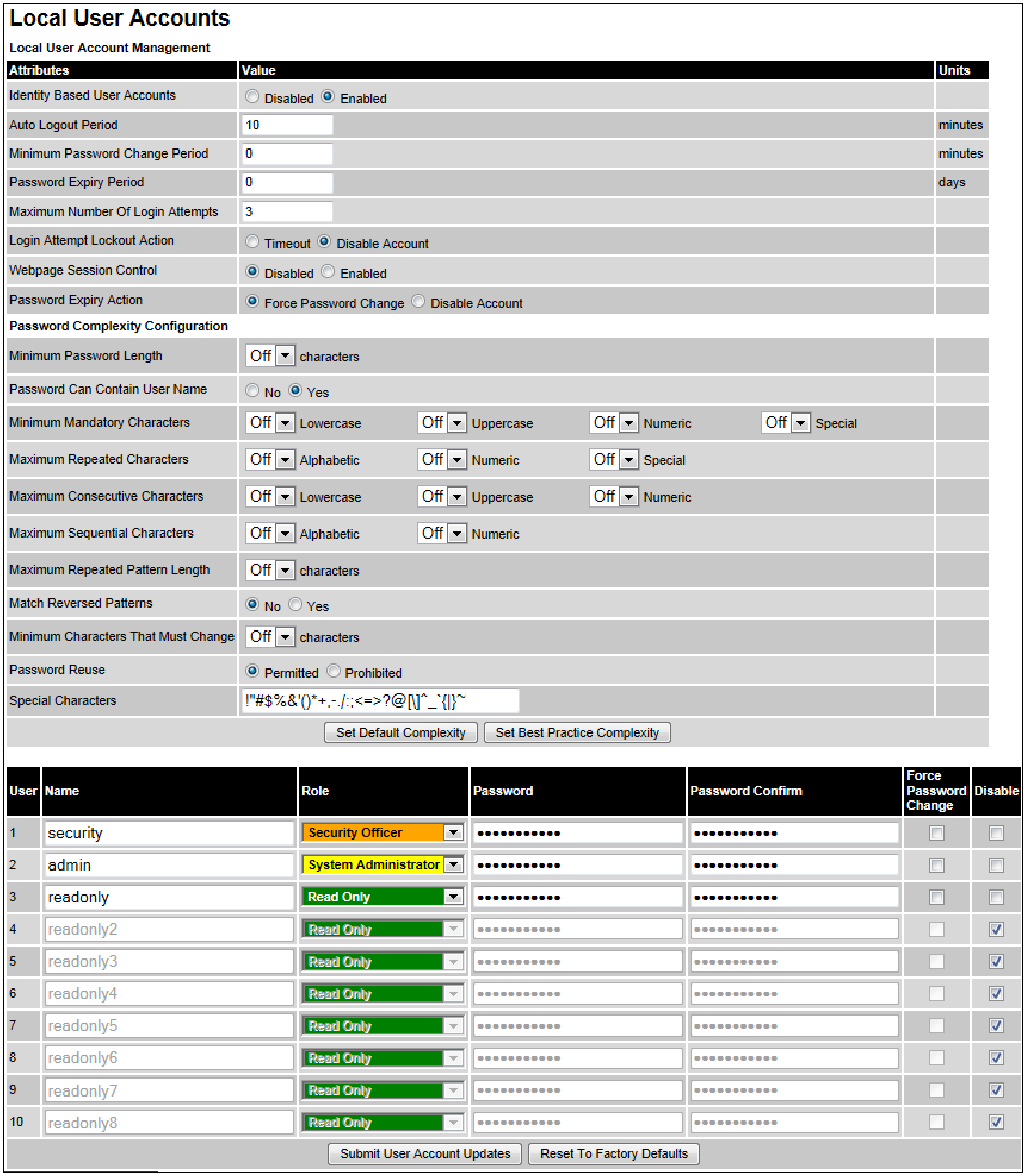


Local User Accounts

Local User Account Management

Attributes	Value	Units
Identity Based User Accounts	● Disabled ○ Enabled	
Auto Logout Period	10	minutes
Minimum Password Change Period	0	minutes
Password Expiry Period	0	days
Maximum Number Of Login Attempts	3	
Login Attempt Lockout Period	1	minutes
Webpage Session Control	● Disabled ○ Enabled	

Figure 76 Local User Accounts page (Identity Based User Accounts enabled)



Local User Accounts

Local User Account Management

Attributes	Value	Units
Identity Based User Accounts	○ Disabled ● Enabled	
Auto Logout Period	10	minutes
Minimum Password Change Period	0	minutes
Password Expiry Period	0	days
Maximum Number Of Login Attempts	3	
Login Attempt Lockout Action	○ Timeout ● Disable Account	
Webpage Session Control	● Disabled ○ Enabled	
Password Expiry Action	● Force Password Change ○ Disable Account	
Password Complexity Configuration		
Minimum Password Length	Off characters	
Password Can Contain User Name	○ No ● Yes	
Minimum Mandatory Characters	Off Lowercase Off Uppercase Off Numeric Off Special	
Maximum Repeated Characters	Off Alphabetic Off Numeric Off Special	
Maximum Consecutive Characters	Off Lowercase Off Uppercase Off Numeric	
Maximum Sequential Characters	Off Alphabetic Off Numeric	
Maximum Repeated Pattern Length	Off characters	
Match Reversed Patterns	● No ○ Yes	
Minimum Characters That Must Change	Off characters	
Password Reuse	● Permitted ○ Prohibited	
Special Characters	!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~	

User	Name	Role	Password	Password Confirm	Force Password Change	Disable
1	security	Security Officer	●●●●●●●●●●●	●●●●●●●●●●●	☐	☐
2	admin	System Administrator	●●●●●●●●●●●	●●●●●●●●●●●	☐	☐
3	readonly	Read Only	●●●●●●●●●●●	●●●●●●●●●●●	☐	☐
4	readonly2	Read Only	●●●●●●●●●●●	●●●●●●●●●●●	☐	☑
5	readonly3	Read Only	●●●●●●●●●●●	●●●●●●●●●●●	☐	☑
6	readonly4	Read Only	●●●●●●●●●●●	●●●●●●●●●●●	☐	☑
7	readonly5	Read Only	●●●●●●●●●●●	●●●●●●●●●●●	☐	☑
8	readonly6	Read Only	●●●●●●●●●●●	●●●●●●●●●●●	☐	☑
9	readonly7	Read Only	●●●●●●●●●●●	●●●●●●●●●●●	☐	☑
10	readonly8	Read Only	●●●●●●●●●●●	●●●●●●●●●●●	☐	☑

Procedure:

- Choose whether to set Identity Based User Accounts to **Disabled** or **Enabled**.
- Review and update the Local User Account Management attributes (Table 77).
- If Identity Based User Accounts is set to **Enabled:**
  - Review and update the Password Complexity Configuration attributes (Table 78). To reset all attributes to the best practice values, click **Set Best Practice Complexity**. To return to default values, click **Set Default Complexity.**
  - Review and update up to 10 identity-based user accounts (Table 79).
- If any attributes have been updated, click **Submit User Account Updates**.

Table 77 Local User Account Management attributes

Attribute	Meaning
Identity Based User Accounts	**Disabled**: Access to the web interface is controlled by a single system administration password. **Enabled**: Up to 10 users may access the unit.
Auto Logout Period	The time without user activity that elapses before a user is automatically logged out (minutes). A value of zero disables this feature.
Minimum Password Change Period	The minimum time that elapses before a user is allowed to change a password (minutes). A value of zero disables this feature.
Password Expiry Period	The time that elapses before a password expires (days). A value of zero disables this feature.
Maximum Number of Login Attempts	The maximum number of login attempts (with incorrect password) that are allowed before a user is locked out. Also, the maximum number of password change attempts before a user is locked out.
Login Attempt Lockout Action	Only displayed when Identity Based User Accounts is **Enabled**. **Timeout**: When a user is locked out, the user is allowed to log in again after a specified period. **Disabled**: When a user is locked out, the user is disabled.
Login Attempt Lockout Period	Only displayed when Identity Based User Accounts is **Disabled.** The time that elapses before a locked out user is allowed to log in again (minutes). Only displayed when Login Attempt Lockout Action is set to **Timeout**.
Webpage Session Control	When this is enabled, any attempt to open a new tab or browser instance will force the user to re-enter password.

Attribute	Meaning
Password Expiry Action	Only displayed when Identity Based User Accounts is **Enabled**. The action to be taken by the PTP 650 when a password expires.

Table 78 Password Complexity Configuration attributes

Attribute	Meaning	Best practice
Minimum Password Length	The minimum number of characters required in passwords.	10
Password Can Contain User Name	**No**: Passwords must not contain the user name. **Yes**: Passwords may contain the user name.	No
Minimum Mandatory Characters	The minimum number of lowercase, uppercase, numeric and special characters required in passwords. For example, if all values are set to **2**, then **FredBloggs** will be rejected, but **FredBloggs(25)** will be accepted.	2
Maximum Repeated Characters	The maximum number of consecutive repeated alphabetic, numeric and special characters permitted in passwords. For example, if all values are set to **2**, then **aaa**, **XXX**, **999** and **$$$** will be rejected, but **aa**, **XX**, **99** or **$$** will be accepted.	2
Maximum Consecutive Characters	The maximum number of consecutive lowercase, uppercase and numeric characters permitted in passwords. For example, if all values are set to **5**, then **ALFRED**, **neuman** and **834030** will be rejected.	5
Maximum Sequential Characters	The maximum number of alphabetic and numeric characters permitted in passwords. For example, if set to **3**, then **abcd**, **WXYZ** and **0123** will be rejected, but **abc**, **xyz** and **123** will be accepted.	3
Maximum Repeated Pattern Length	The maximum sequence of characters that can be repeated consecutively in passwords. For example, if set to **3**, then **BlahBlah** and **31st31st** will be rejected, but **TicTicTock** and **GeeGee** will be accepted. **Blah-Blah** will be accepted because the two sequences are not consecutive.	3

Attribute	Meaning	Best practice
Match Reversed Patterns	**No**: Reversed patterns are not checked. **Yes**: Reversed patterns are checked. For example, if Maximum Repeated Pattern Length is set to **3** and Match Reversed Patterns is set to **Yes**, then **AB1221BA** will be rejected.	Yes
Minimum Characters That Must Change	The minimum number of password characters that must change every time a password is updated.	4
Password Reuse	**Permitted**: A user may reuse a previous password. **Prohibited**: A user must not reuse a previous password.	Prohibited
Special Characters	User defined set of special characters used in password construction. The only characters permitted in a password are: (a-z), (A-Z), (0-9) and any of the special characters entered here.	!"%&'()*+,-./:;<=>?

Table 79 Identity-based user accounts attributes

Attribute	Meaning
Name	Enter a user name.
Role	Select a role from the list: **Security Officer, System Administrator** or **Read Only**.
Password	Enter a password for the user. Passwords must comply with the complexity rules (Table 78).
Password Confirm	Retype the password to confirm.
Force Password Change	Force this user to change their password when they next log on.
Disable	Tick the box to disable a user account.

Note

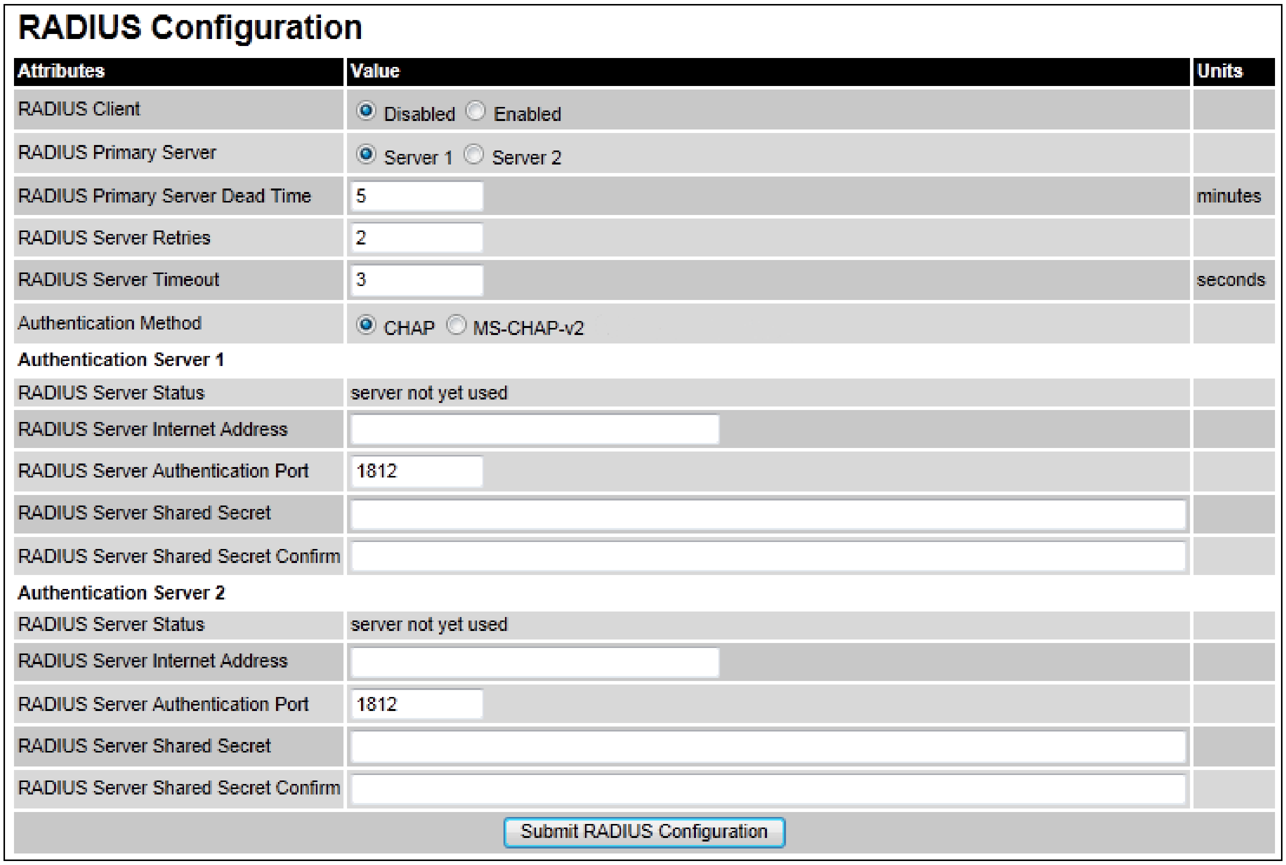
At least one user must be assigned the Security Officer role. If RADIUS is enabled, then this rule is relaxed, in which case the RADIUS server(s) SHOULD be configured with at least one user with **Security Officer** privileges.

RADIUS Configuration page

Menu option: **Management > Web > Radius Configuration** (Figure 77).

Use this page to configure RADIUS authentication. RADIUS authentication is only available when PTP 650 is configured for Identity-based User Accounts and when RADIUS servers are connected to the network.

Figure 77 RADIUS Configuration page



RADIUS Configuration

Attributes	Value	Units
RADIUS Client	● Disabled ○ Enabled	
RADIUS Primary Server	● Server 1 ○ Server 2	
RADIUS Primary Server Dead Time	5	minutes
RADIUS Server Retries	2	
RADIUS Server Timeout	3	seconds
Authentication Method	● CHAP ○ MS-CHAP-v2	
Authentication Server 1		
RADIUS Server Status	server not yet used	
RADIUS Server Internet Address		
RADIUS Server Authentication Port	1812	
RADIUS Server Shared Secret		
RADIUS Server Shared Secret Confirm		
Authentication Server 2		
RADIUS Server Status	server not yet used	
RADIUS Server Internet Address		
RADIUS Server Authentication Port	1812	
RADIUS Server Shared Secret		
RADIUS Server Shared Secret Confirm		

Note

Only users with **Security Officer** role are permitted to configure RADIUS authentication.

Note

When RADIUS is enabled, the Security Officer may disable all user accounts.

Note

At least one user with Security Officer privileges must exist and be enabled, in order to disable the RADIUS client.

Procedure:

- Update the attributes (Table 80).
- Click **Submit RADIUS Configuration**.

Table 80 RADIUS Authentication attributes

Attribute	Meaning
RADIUS Client Enabled	**Enabled:** PTP 650 users may be authenticated via the RADIUS servers. **Disabled**: RADIUS authentication is not used. This may only be selected if at least one user with Security Officer privileges exists.
RADIUS Primary Server	Specifies the primary server, determining the order in which the servers are tried.
RADIUS Primary Server Dead Time	Time (in minutes) to hold off trying to communicate with a previously unavailable RADIUS server. Setting the value to zero disables the timer.
RADIUS Server Retries	Number of times the PTP 650 will retry after a RADIUS server fails to respond to an initial request.
RADIUS Server Timeout	Time (in seconds) the PTP 650 will wait for a response from a RADIUS server.
Authentication Method	Method used by RADIUS to authenticate users.
Authentication Server 1 and 2:	
RADIUS Server Status	The status of the RADIUS server. This contains the time of the last test and an indication of success or failure. If the Authentication Server attributes are incorrect, the displayed status is "`server config not valid`".
RADIUS Server Internet Address	IPv4 or IPv6 address of the RADIUS server.
RADIUS Server Authentication Port	Network port used by RADIUS server for authentication services.
RADIUS Server Shared Secret	Shared secret used in RADIUS server communications. May contain alphabetic, numeric, special characters or spaces, but not extended unicode characters. The maximum length is 127 characters.

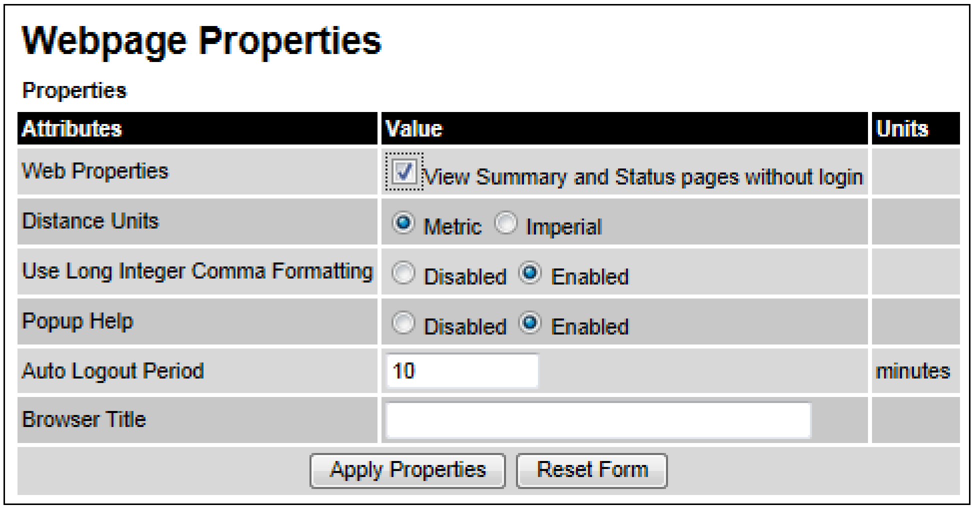
Attribute	Meaning
RADIUS Server Shared Secret Confirm	Shared secret confirmation.

Webpage Properties page

Menu option: **Management > Web > Web Properties** (Figure 78).

Use this page to control the display of the web interface.

Figure 78 Webpage Properties page



Webpage Properties

Properties

Attributes	Value	Units
Web Properties	☑ View Summary and Status pages without login	
Distance Units	● Metric ○ Imperial	
Use Long Integer Comma Formatting	○ Disabled ● Enabled	
Popup Help	○ Disabled ● Enabled	
Auto Logout Period	10	minutes
Browser Title		

Procedure:

- Update the attributes (Table 81).
- Click Apply Properties.

Table 81 Webpage Properties attributes

Attribute	Meaning
Web Properties	**View Summary and Status pages without login**: • If ticked (the default setting), users can view the Summary and Status web pages without entering a password. • If not ticked, users must enter a password before viewing the Summary and Status pages. This is only effective if the System Administration Password has been set, see Change Password page on page 7-10.
Distance Units	**Metric:** Distances are displayed in kilometers or meters. **Imperial:** Distances are displayed in miles or feet.
Use Long Integer Comma Formatting	**Disabled:** Long integers are displayed thus: 1234567. **Enabled:** Long integers are displayed thus: 1,234,567.
Popup Help	**Disabled:** Web page popup help is not displayed. **Enabled:** Web page popup help is displayed.
Send HTTPS Close Notify Alerts	Only displayed when HTTPS is configured. Controls whether or not the HTTPS server sends TLS Close Notify Alerts before it shuts down each socket. **Disabled**: TLS Close Notify Alerts are not sent before closing each socket. This is the default because these alerts can cause problems with some browsers (e.g. Internet Explorer) **Enabled**: TLS Close Notify Alerts are sent before closing each socket.
Auto Logout Period	Only displayed if role-based user accounts are in use. Automatic logout period in minutes. If there is no user activity within this time, the user is required to log in again. Think this is only displayed when not using identity based user accounts.
Browser Title	By default, the PTP 650 web interface displays the following text in web browser tab titles: **`Cambium PTP 50650 - <current page> (IP=<ipAddress>)`** To change the default text, enter simple text and optional variables (prefixed with a $ character). The full list of variables is in Table 82.

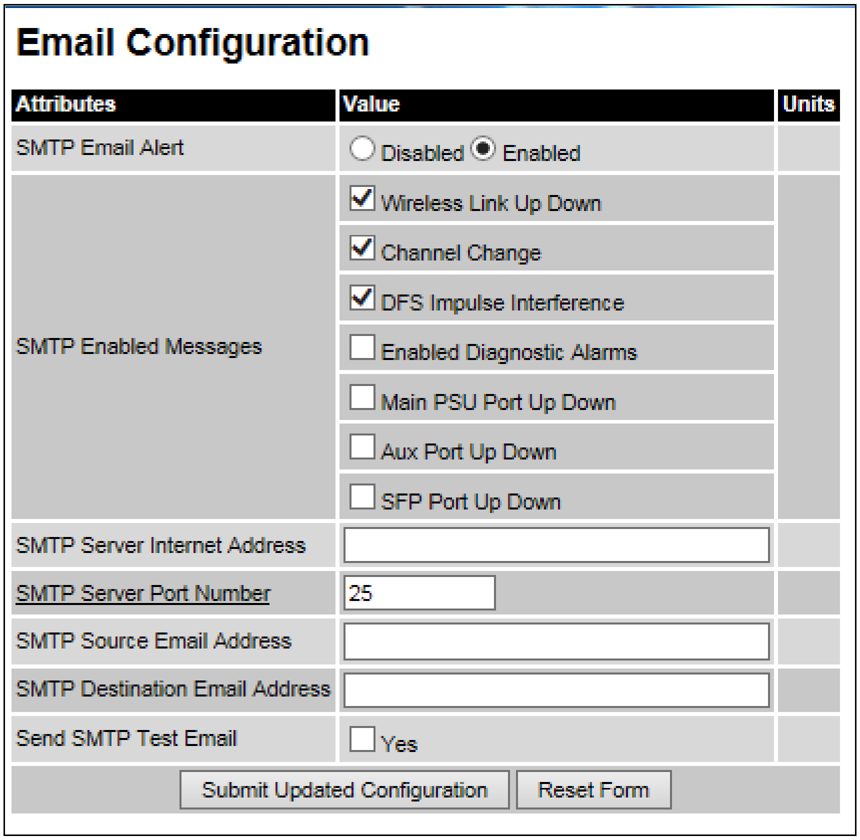
Table 82 Browser Title attribute variables

Variable	Meaning
$siteName	Site Name, as set in the System Configuration page (Table 70).
$linkName	Link Name, as set in the System Configuration page (Table 70).
$masterSlaveMode	Master Slave Mode, as set in the Step 2: Wireless Configuration page (Table 69).
$ipAddress	IP Address currently used to identify the ODU, either IPv4 or IPv6 Address, depending upon the setting of IP Address Label in the System Configuration page (Table 70): • **IPv4**: $ipAddress = $ipv4Address • **IPv6**: $ipAddress = $ipv6Address (if not blank) or $ipv6LinkLocalAddress
$ipv4Address	IPv4 Address of the ODU, as set in the LAN Configuration page (Table 71).
$ipv6Address	IPv6 Address of the ODU, as set in the LAN Configuration page (Table 71).
$ipv6LinkLocalAddress	IPv6 Auto Configured Link Local Address of the ODU. This cannot be updated, but it can be viewed in the LAN Configuration page (Table 71).
$sysName	Sys Name for this SNMP managed node, as set in the Step 2: SNMP MIB-II System Objects page (Table 88).
$productName	The product variant, for example **Cambium PTP50650**. Not updateable.
$pageName	Name of the page currently being browsed.

Email Configuration page

Menu option: **Management** > **Email** (Figure 79). Use this page to enable the PTP 650 to generate Simple Mail Transfer Protocol (SMTP) email messages to notify the system administrator when certain events occur.

Figure 79 Email Configuration page



Email Configuration

Attributes	Value	Units
SMTP Email Alert	○ Disabled ● Enabled	
SMTP Enabled Messages	☑ Wireless Link Up Down ☑ Channel Change ☑ DFS Impulse Interference □ Enabled Diagnostic Alarms □ Main PSU Port Up Down □ Aux Port Up Down □ SFP Port Up Down	
SMTP Server Internet Address		
SMTP Server Port Number	25	
SMTP Source Email Address		
SMTP Destination Email Address		
Send SMTP Test Email	□ Yes	

Procedure:

- Update the attributes (Table 83).
- Click **Submit Updated Configuration**. The Configuration Change Reboot dialog is displayed.
- Click **Reboot Wireless Unit** and click **OK**. The reboot progress message is displayed. On completion, the unit restarts.

Table 83 Email Configuration attributes

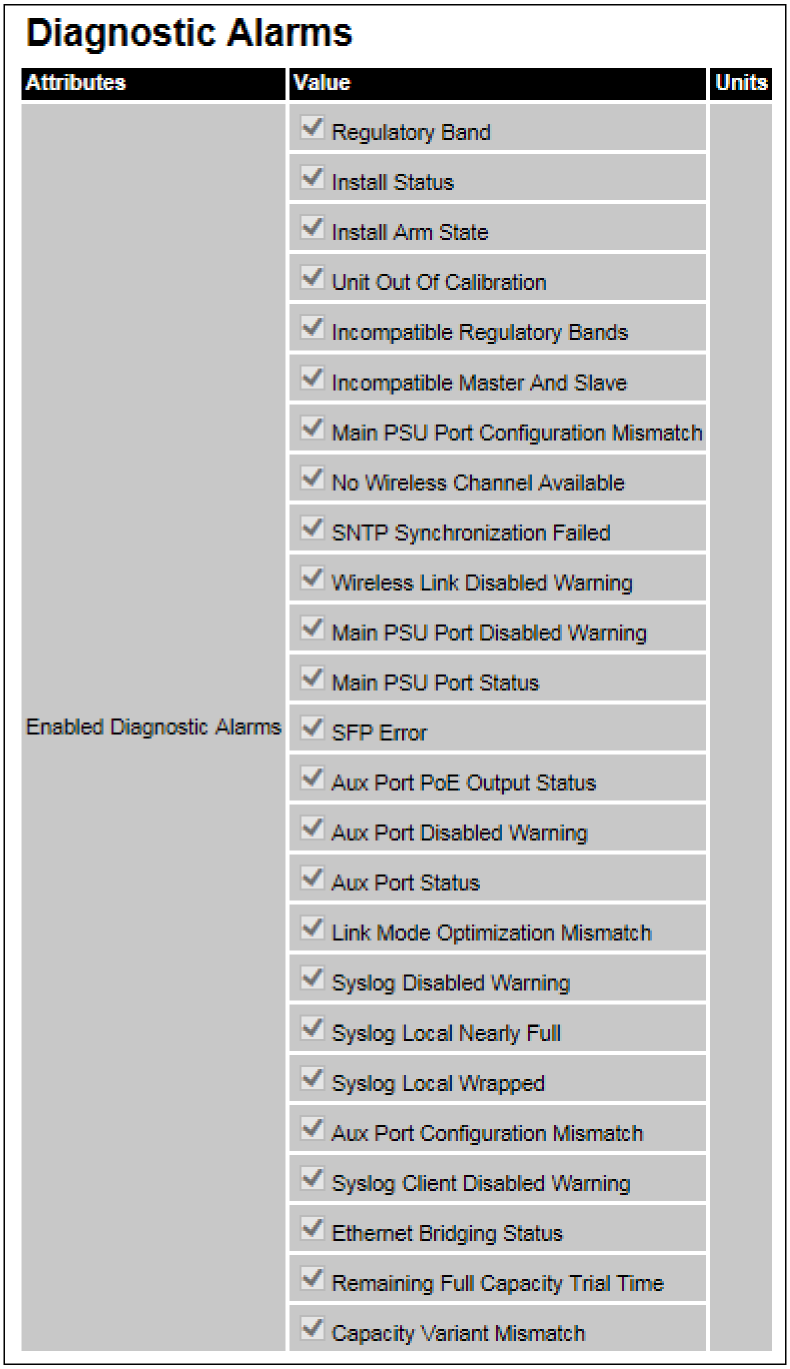
Attribute	Meaning
SMTP Email Alert	Controls the activation of the SMTP client.
SMTP Enabled Messages	The SMTP Enabled Messages attribute controls which email alerts the unit will send.
SMTP Server Internet Address	The IPv4 or IPv6 Address of the networked SMTP server.
SMTP Server Port Number	The SMTP Port Number is the port number used by the networked SMTP server. By convention the default value for the port number is 25.
SMTP Source Email Address	The email address used by the PTP 650 Series to log into the SMTP server. This must be a valid email address that will be accepted by your SMTP Server.
SMTP Destination Email Address	The email address to which the PTP 650 Series will send the alert messages.
Send SMTP Test Email	Generate and send an email in order to test the SMTP settings. The tick box will self-clear when **Submit** is clicked.

Diagnostic Alarms page

Menu option: **Management** > **Diagnostic Alarms** (Figure 80).

Use this page to select which diagnostic alarms will be notified to the system administrator.

Figure 80 Diagnostic Alarms page



Diagnostic Alarms

Attributes	Value	Units
Enabled Diagnostic Alarms	☑ Regulatory Band	
	☑ Install Status	
	☑ Install Arm State	
	☑ Unit Out Of Calibration	
	☑ Incompatible Regulatory Bands	
	☑ Incompatible Master And Slave	
	☑ Main PSU Port Configuration Mismatch	
	☑ No Wireless Channel Available	
	☑ SNTP Synchronization Failed	
	☑ Wireless Link Disabled Warning	
	☑ Main PSU Port Disabled Warning	
	☑ Main PSU Port Status	
	☑ SFP Error	
	☑ Aux Port PoE Output Status	
	☑ Aux Port Disabled Warning	
	☑ Aux Port Status	
	☑ Link Mode Optimization Mismatch	
	☑ Syslog Disabled Warning	
	☑ Syslog Local Nearly Full	
	☑ Syslog Local Wrapped	
	☑ Aux Port Configuration Mismatch	
	☑ Syslog Client Disabled Warning	
	☑ Ethernet Bridging Status	
	☑ Remaining Full Capacity Trial Time	
	☑ Capacity Variant Mismatch	

Procedure:

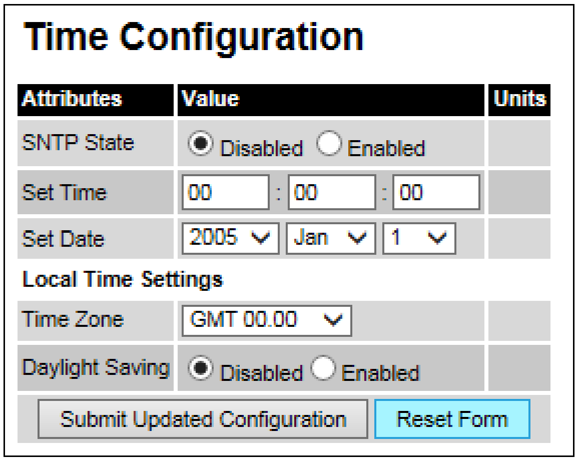
- Tick the required alarms. These alarms are described in Alarms on page 7-12.
- Click **Submit Updated Configuration**.

Time Configuration page

Menu option: **Management > Time** (Figure 81 and Figure 82)

Use this page to set the real-time clock of the PTP 650.

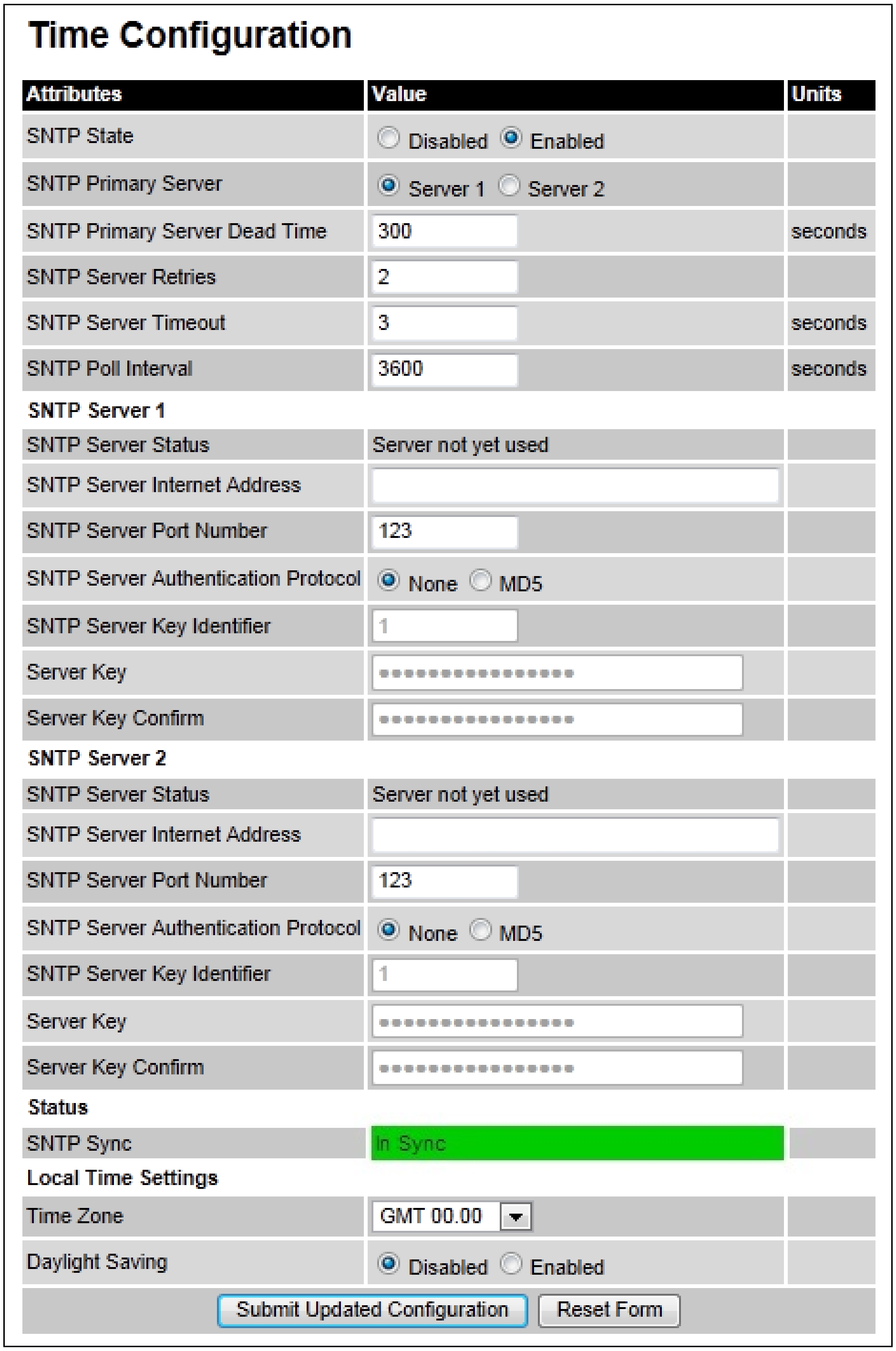
Figure 81 Time Configuration page (SNTP disabled)



Time Configuration

Attributes	Value	Units
SNTP State	● Disabled ○ Enabled	
Set Time	00 : 00 : 00	
Set Date	2005 Jan 1	
Local Time Settings		
Time Zone	GMT 00.00	
Daylight Saving	● Disabled ○ Enabled	

Figure 82 Time Configuration page (SNTP enabled)



Time Configuration

Attributes	Value	Units
SNTP State	○ Disabled ● Enabled	
SNTP Primary Server	● Server 1 ○ Server 2	
SNTP Primary Server Dead Time	300	seconds
SNTP Server Retries	2	
SNTP Server Timeout	3	seconds
SNTP Poll Interval	3600	seconds
SNTP Server 1		
SNTP Server Status	Server not yet used	
SNTP Server Internet Address		
SNTP Server Port Number	123	
SNTP Server Authentication Protocol	● None ○ MD5	
SNTP Server Key Identifier	1	
Server Key	••••••••••••••••	
Server Key Confirm	••••••••••••••••	
SNTP Server 2		
SNTP Server Status	Server not yet used	
SNTP Server Internet Address		
SNTP Server Port Number	123	
SNTP Server Authentication Protocol	● None ○ MD5	
SNTP Server Key Identifier	1	
Server Key	••••••••••••••••	
Server Key Confirm	••••••••••••••••	
Status		
SNTP Sync	In Sync	
Local Time Settings		
Time Zone	GMT 00.00	
Daylight Saving	● Disabled ○ Enabled	

Setting the real-time clock manually

Use this procedure to keep time without connecting to a networked time server.

Note

If SNTP is disabled, it will be necessary to reset the time manually after each system reboot.

Procedure:

- Set SNTP State to **Disabled**.
- Review and update the manual clock attributes (Table 84).
- Click **Submit Updated Configuration**.

Table 84 Manual clock attributes

Attribute	Meaning
SNTP State	**Disabled:** the PTP 650 will keep time without connecting to a networked time server.
Set Time	Set hours, minutes and seconds.
Set Date	Set year, month and day.
Time Zone	Set the time zone offset from Greenwich Mean Time (GMT). To set the clock to UTC time, set Time Zone to **GMT 00.00**.
Daylight Saving	**Disabled:** There is no offset for daylight saving time. **Enabled:** System clock is moved forward one hour to adjust for daylight saving time. To set the clock to UTC time, set Daylight Saving to **Disabled**.

Setting the real-time clock to synchronize using SNTP

Use this procedure to synchronize the unit with a networked time server:

Procedure:

- Set the SNTP State attribute to **Enabled**.
- Review and update the SNTP clock attributes (Table 85).
- Click **Submit Updated Configuration**.

Table 85 SNTP clock attributes

Attribute	Meaning
SNTP State	**Enabled:** the ODU will obtain accurate date and time updates from a networked time server.
SNTP Primary Server	Specifies the primary SNTP server, determining the order in which the servers are tried.
SNTP Primary Server Dead Time	Time (in seconds) to wait before retrying communications with an unresponsive primary SNTP server. Setting the value to zero disables the timer.
SNTP Server Retries	Number of times the PTP will retry after an SNTP server fails to respond.
SNTP Server Timeout	Time (in seconds) the PTP will wait for a response from an SNTP server.
SNTP Poll Interval	The SNTP server polling interval.
SNTP Server 1 and 2:	
SNTP Server Status	Status message reflecting the state of communications with the SNTP server.
SNTP Server Internet Address	The IPv4 or IPv6 Address of the networked SNTP server.
SNTP Server Port Number	The port number of the networked SNTP server. By convention the default value for the port number is 123.
SNTP Server Authentication Protocol	Authentication protocol to be used with this SNTP server (**None** or **MD5**).
SNTP Server Key Identifier	SNTP key identifier. A key of zeros is reserved for testing.
Server Key	Key used to authenticate SNTP communications.
Server Key Confirm	Must match the Server Key.
Status:	
SNTP Sync	This shows the current status of SNTP synchronization. If **No Sync** is displayed, then review the SNTP Server Internet Address and Port Number. A change of state may generate an SNMP trap or SMTP email alert.
SNTP Last Sync	This shows the date and time of the last SNTP synchronization.

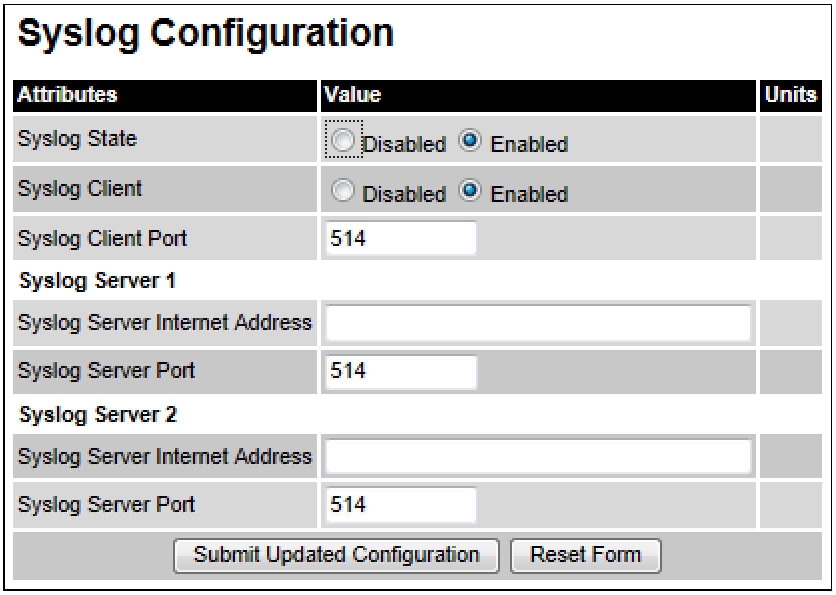
Attribute	Meaning
System Clock	This displays the local time, allowing for the Time Zone and Daylight Saving settings.
Local Time Settings:	
Time Zone	Set the time zone offset from Greenwich Mean Time (GMT). To set the clock to UTC time, set Time Zone to **GMT 00.00**.
Daylight Saving	**Disabled:** Daylight saving adjustments will not be applied to the time. **Enabled:** Daylight saving adjustments will be applied to the time, according to local rules. To set the clock to UTC time, set Daylight Saving to **Disabled**.

Syslog Configuration page

Menu option: **Management** > **Syslog** > **Syslog configuration** (Figure 83).

Use this page to configure system logging. Only users with **Security Officer** role are permitted to configure the syslog client.

Figure 83 Syslog Configuration page



Syslog Configuration

Attributes	Value	Units
Syslog State	○ Disabled ● Enabled	
Syslog Client	○ Disabled ● Enabled	
Syslog Client Port	514	
Syslog Server 1		
Syslog Server Internet Address		
Syslog Server Port	514	
Syslog Server 2		
Syslog Server Internet Address		
Syslog Server Port	514	

Note

To record Coordinated Universal Time (UTC time) in syslog messages, use the Time Configuration page to set Time Zone to **GMT 00.00** and Daylight Saving to **Disabled** (Time Configuration page on page 6-55).

Procedure:

- Update the attributes (Table 86).
- Click **Submit Updated Configuration**.

Table 86 Syslog Configuration attributes

Attribute	Meaning
Syslog State	When system logging is enabled, log entries are added to the internal log and (optionally) transmitted as UDP messages to one or two syslog servers.
Syslog Client	**Enabled:** Event messages are logged. **Disabled:** Event messages are not logged.
Syslog Client Port	The client port from which syslog messages are sent.
Syslog Server 1 and 2:	
Syslog Server Internet Address	The IPv4 or IPv6 Address of the syslog server. Delete the IP address to disable logging on the syslog server.
Syslog Server Port	The server port at which syslog messages are received.

SNMP pages (for SNMPv3)

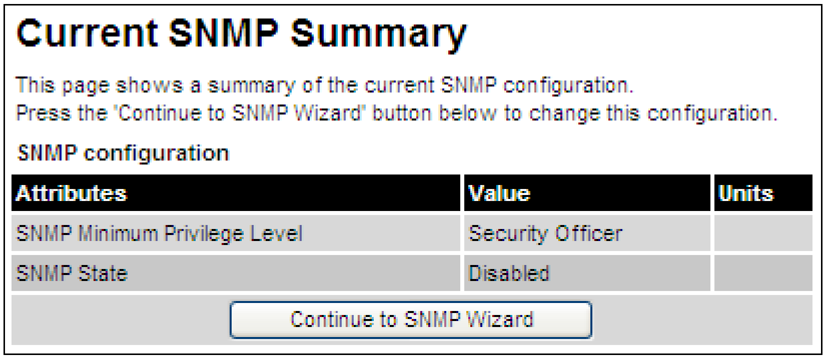
This section describes how to configure Simple Network Management Protocol version 3 (SNMPv3) traps using the SNMP Wizard.

Current SNMP Summary (for SNMPv3)

Menu option: **Management > SNMP** (Figure 84).

Use this page to review the current SNMP configuration and start the SNMP Wizard.

Figure 84 Current SNMP Summary page (when SNMP is disabled)



Current SNMP Summary

This page shows a summary of the current SNMP configuration.
Press the 'Continue to SNMP Wizard' button below to change this configuration.

SNMP configuration

Attributes	Value	Units
SNMP Minimum Privilege Level	Security Officer	
SNMP State	Disabled	

Procedure:

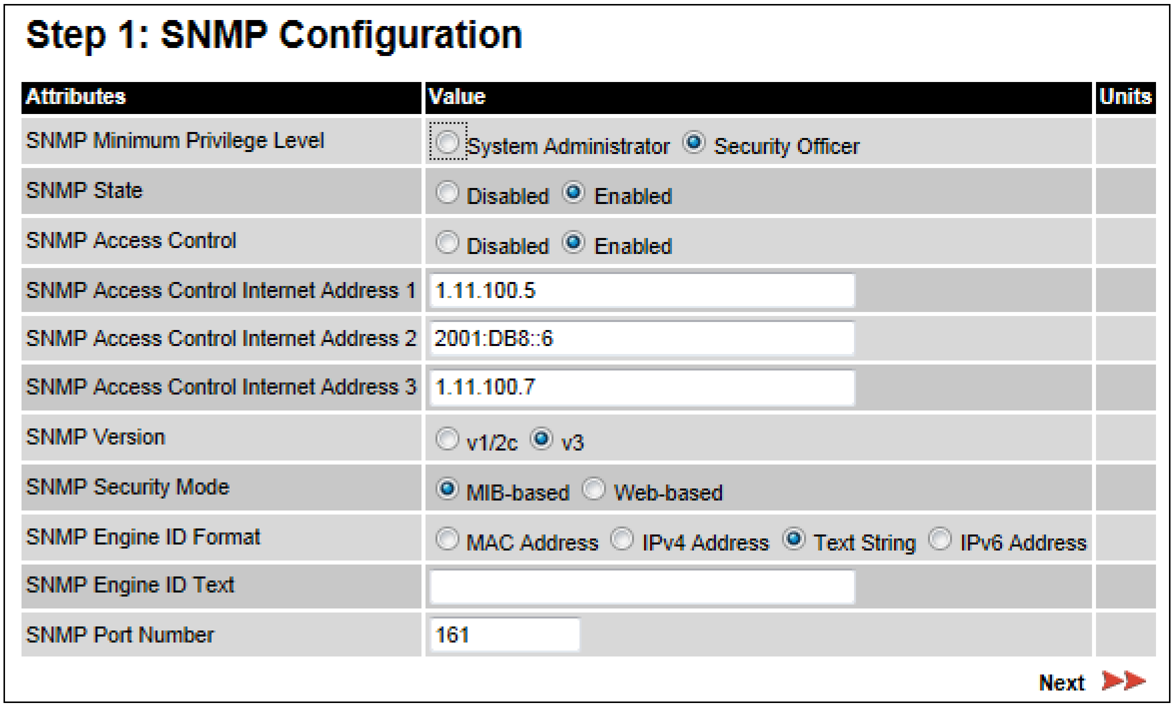
- Review the summary.
- If any updates are required, click **Continue to SNMP Wizard**.

Step 1: SNMP Configuration (for SNMPv3)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 85).

Use this page to enable SNMP, select SNMPv3 and configure access to the SNMP server.

Figure 85 Step 1: SNMP Configuration page (for SNMPv3)



Step 1: SNMP Configuration

Attributes	Value	Units
SNMP Minimum Privilege Level	○ System Administrator ● Security Officer	
SNMP State	○ Disabled ● Enabled	
SNMP Access Control	○ Disabled ● Enabled	
SNMP Access Control Internet Address 1	1.11.100.5	
SNMP Access Control Internet Address 2	2001:DB8::6	
SNMP Access Control Internet Address 3	1.11.100.7	
SNMP Version	○ v1/2c ● v3	
SNMP Security Mode	● MIB-based ○ Web-based	
SNMP Engine ID Format	○ MAC Address ○ IPv4 Address ● Text String ○ IPv6 Address	
SNMP Engine ID Text		
SNMP Port Number	161	

Procedure:

- Set SNMP State to **Enabled**.
- Set SNMP Version to **v3**. The page is redisplayed with SNMPv3 attributes.
- Update the attributes (Table 87).
- Click **Next**.

Table 87 Step 1: SNMP Configuration attributes (for SNMPv3)

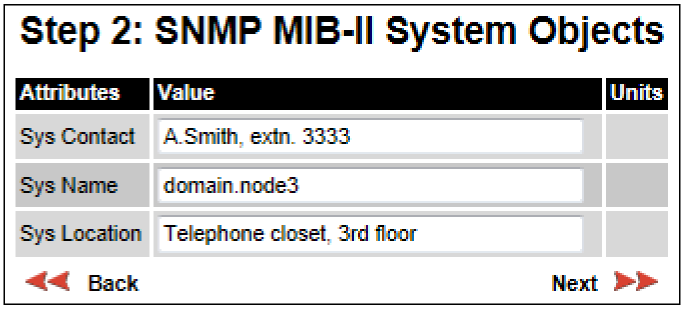
Attribute	Meaning
SNMP Minimum Privilege Level	Minimum security level which is permitted to administer SNMP security settings. Only displayed when Identity Based User Accounts are **Enabled** on the User Accounts page (Table 77).
SNMP State	Enables or disables SNMP.
SNMP Access Control	Enables or disables access control to SNMP management by IP address.
SNMP Access Control Internet Address 1/2/3	A list of up to three IPv4 or IPv6 Addresses permitted to perform SNMP management. Only displayed when SNMP Access Control is set to **Enabled**.
SNMP Version	SNMP protocol version: **v1/2c** or **v3**.
SNMP Security Mode	**MIB-based**: SNMPv3 security parameters are managed via SNMP MIBs. **Web-based**: SNMPv3 security parameters are not available over SNMP, but instead are configured using the SNMP Accounts page, as described in Step 3: SNMP User Policy Configuration (for SNMPv3) on page 6-65.
SNMP Engine ID Format	Specifies whether the Engine ID is generated from the **MAC Address**, **IP4 Address**, **Text String** or **IPv6 Address**.
SNMP Engine ID Text	Only enabled when SNMP Engine ID Format is set to **Text String**. Text used to generate the SNMP Engine ID.
SNMP Port Number	The port that the SNMP agent is listening to for commands from a management system.

Step 2: SNMP MIB-II System Objects (for SNMPv3)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 86).

Use this page to enter details of the SNMP managed node.

Figure 86 Step 2: SNMP MIB-II System Objects page (for SNMPv3)



Step 2: SNMP MIB-II System Objects

Attributes	Value	Units
Sys Contact	A.Smith, extn. 3333	
Sys Name	domain.node3	
Sys Location	Telephone closet, 3rd floor	

Procedure:

- Update the attributes (Table 88).
- Click **Next.**
- The next step depends upon which SNMP Security Mode was selected in the Step 1: SNMP Configuration page:
  - If **Web-based**, go to Step 3: SNMP User Policy Configuration (for SNMPv3) on page 6-65.
  - If **MIB-based**, go to Confirm SNMP Configuration (for SNMPv3) on page 6-70.

Table 88 Step 2: SNMP MIB-II System Objects attributes (for SNMPv3)

Attribute	Meaning
Sys Contact	The name of the contact person for this managed node, together with information on how to contact this person.
Sys Name	An administratively-assigned name for this managed node. By convention, this is the fully qualified domain name of the node.
Sys Location	The physical location of this node, for example **Telephone closet, 3rd floor**.

Step 3: SNMP User Policy Configuration (for SNMPv3)

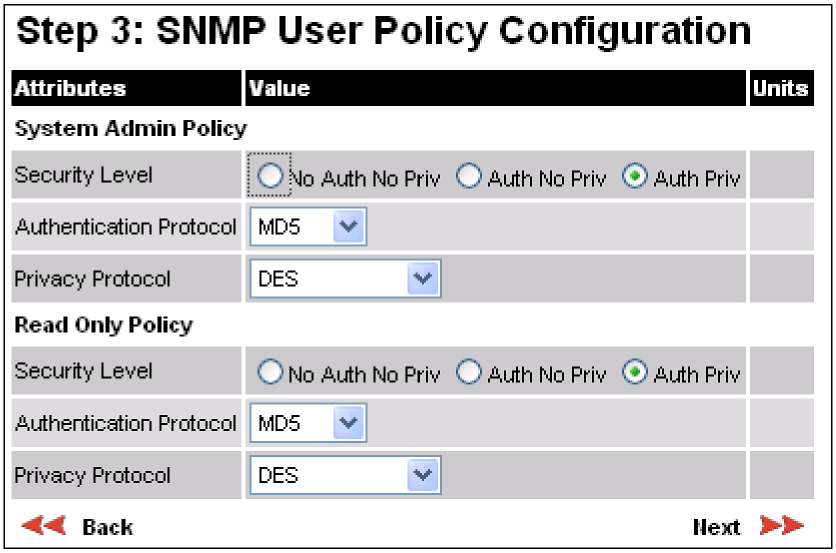
Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 87).

This page is only displayed when SNMP Security Mode is set to **Web-based** in the Step 1: SNMP Configuration page. Use this page to configure which authentication and privacy protocols are required for SNMP users with roles **System administrator** and **Read only**.

Procedure:

- Update the attributes (Table 89).
- Click **Next**.

Figure 87 Step 3: SNMP User Policy Configuration page (for SNMPv3)



Step 3: SNMP User Policy Configuration

Attributes	Value	Units
System Admin Policy		
Security Level	○ No Auth No Priv ○ Auth No Priv ● Auth Priv	
Authentication Protocol	MD5	
Privacy Protocol	DES	
Read Only Policy		
Security Level	○ No Auth No Priv ○ Auth No Priv ● Auth Priv	
Authentication Protocol	MD5	
Privacy Protocol	DES	

Table 89 Step 3: SNMP User Policy Configuration attributes (for SNMPv3)

Attribute	Meaning
Security Level	Defines the security level and associated protocols that are required to allow SNMP users to access the PTP 650. **No Auth No Priv**: Users are not required to use authentication or privacy protocols. **Auth No Priv**: Users are required to use only authentication protocols. **Auth Priv**: Users are required to use both authentication and privacy protocols.

Attribute	Meaning
Authentication Protocol	The authentication protocol to be used to access the PTP 650 via SNMP. This is disabled when Security Level is set to **Auth No Priv**. **MD5**: Message Digest Algorithm is used. **SHA**: NIST FIPS 180-1, Secure Hash Algorithm SHA-1 is used.
Privacy Protocol	The privacy protocol to be used to access the PTP 650 via SNMP. This is disabled when Security Level is set to **No Auth No Priv** or **Auth No Priv**. **DES**: Data Encryption Standard (DES) symmetric encryption protocol. **AES**: Advanced Encryption Standard (AES) cipher algorithm.

Note

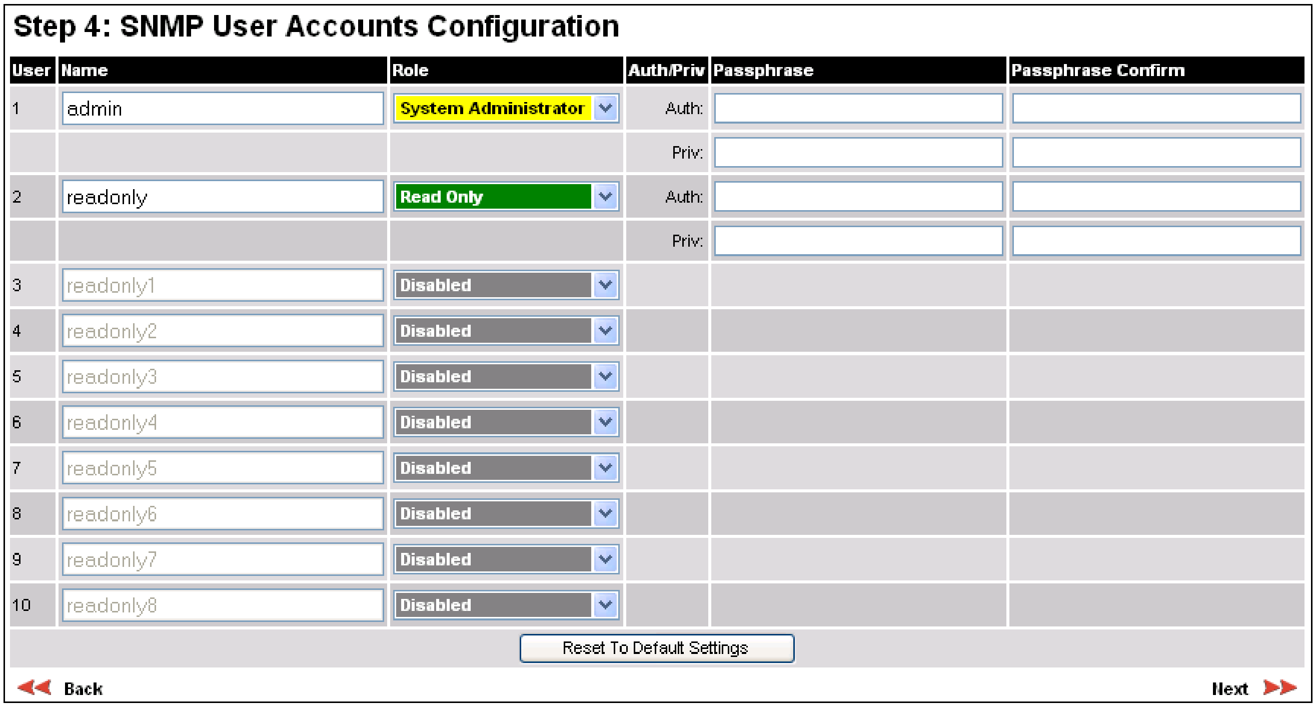
A user configured to use AES privacy protocol will not be able to transmit and receive encrypted messages unless the license key enables the AES capability.

Step 4: SNMP User Accounts Configuration (for SNMPv3)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 88).

This page is only displayed when SNMP Security Mode is set to **Web-based** in the Step 1: SNMP Configuration page. Use this page to update the SNMP user accounts.

Figure 88 Step 4: SNMP User Accounts Configuration page (for SNMPv3)



Step 4: SNMP User Accounts Configuration

User	Name	Role	Auth/Priv	Passphrase	Passphrase Confirm
1	admin	System Administrator	Auth:		
			Priv:		
2	readonly	Read Only	Auth:		
			Priv:		
3	readonly1	Disabled			
4	readonly2	Disabled			
5	readonly3	Disabled			
6	readonly4	Disabled			
7	readonly5	Disabled			
8	readonly6	Disabled			
9	readonly7	Disabled			
10	readonly8	Disabled			

Procedure:

- Update the individual user attributes (Table 90) for up to 10 SNMP users.
- Click **Next.**

Table 90 Step 4: SNMP User Accounts Configuration attributes (for SNMPv3)

Attribute	Meaning
Name	Name to be used by the SNMP user to access the system.
Role	Selects which of the two web-based security profiles are applied to this user: **System administrator** or **Read only**. Select **Disabled** to disable the SNMP account.
Auth/Priv	Indicates whether the Passphrase applies to authentication or privacy protocols.

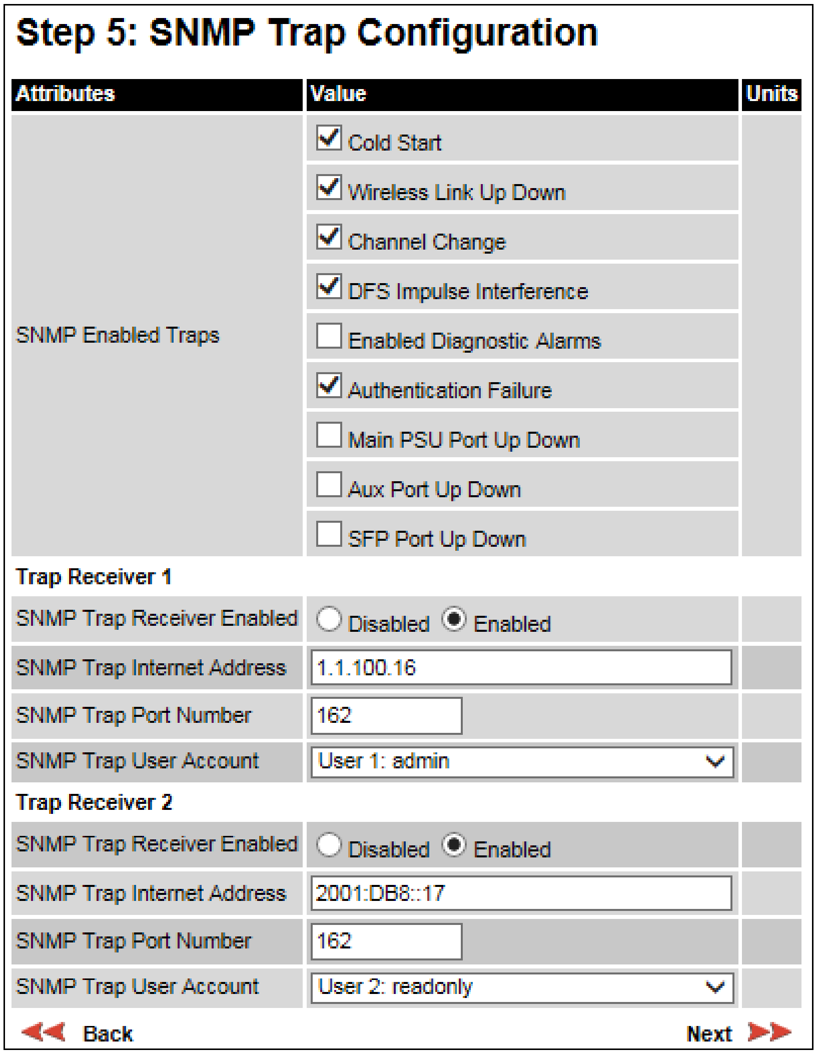
Attribute	Meaning
Passphrase	The phrase to be entered by this SNMP user to access the system using an authentication or privacy protocol. Length must be between 8 and 32 characters. May contain spaces. The Auth Passphrase is hidden when Security Level for this user's Role is set to **No Auth No Priv**. The Priv Passphrase is hidden when Security Level for this user's Role is set to **No Auth No Priv** or **Auth No Priv**.
Passphrase Confirm	Passphrase must be reentered to confirm it has been correctly typed.

Step 5: SNMP Trap Configuration (for SNMPv3)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 89).

This page is only displayed when SNMP Security Mode is set to **Web-based** in the Step 1: SNMP Configuration page. Use this page to configure the events that will generate SNMP traps and to set up trap receivers.

Figure 89 Step 5: SNMP Trap Configuration page (for SNMPv3)



Step 5: SNMP Trap Configuration

Attributes	Value	Units
SNMP Enabled Traps	☑ Cold Start ☑ Wireless Link Up Down ☑ Channel Change ☑ DFS Impulse Interference □ Enabled Diagnostic Alarms ☑ Authentication Failure □ Main PSU Port Up Down □ Aux Port Up Down □ SFP Port Up Down	
Trap Receiver 1		
SNMP Trap Receiver Enabled	○ Disabled ● Enabled	
SNMP Trap Internet Address	1.1.100.16	
SNMP Trap Port Number	162	
SNMP Trap User Account	User 1: admin	
Trap Receiver 2		
SNMP Trap Receiver Enabled	○ Disabled ● Enabled	
SNMP Trap Internet Address	2001:DB8::17	
SNMP Trap Port Number	162	
SNMP Trap User Account	User 2: readonly	

Procedure:

- Update the attributes (Table 91).
- Click **Next**.

Table 91 Step 5: SNMP Trap Configuration attributes (for SNMPv3)

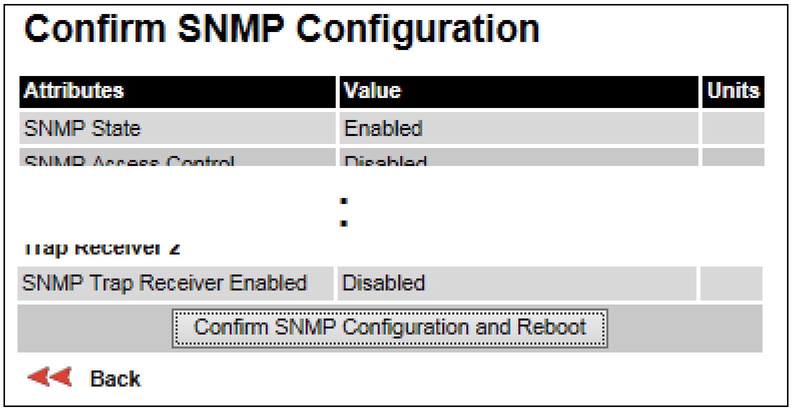
Attribute	Meaning
SNMP Enabled Traps	Select the events that will generate SNMP traps.
SNMP Trap Receiver 1 and SNMP Trap Receiver 2:	
SNMP Trap Receiver Enabled	**Disabled**: SNMP traps are not sent to the corresponding SNMP Trap Receiver (1 or 2). **Enabled**: SNMP traps are sent to the corresponding SNMP Trap Receiver (1 or 2).
SNMP Trap Internet Address	The IPv4 or IPv6 Address of the SNMP server (trap receiver). This is normally the network management system, but it may be a separate trap receiver.
SNMP Trap Port Number	The server port at which SNMP traps are received.
SNMP Trap User Account	The user name (and associated protocols) to use when sending SNMP traps to the server.

Confirm SNMP Configuration (for SNMPv3)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 90).

Use this page to review and confirm the updated SNMPv3 configuration of the unit.

Figure 90 Confirm SNMP Configuration page (for SNMPv3) (top and bottom of page shown)



Confirm SNMP Configuration

Attributes	Value	Units
SNMP State	Enabled	
SNMP Access Control	Disabled	
:		
Trap Receiver 2		
SNMP Trap Receiver Enabled	Disabled	

Procedure:

- To ensure that the changes take effect, click **Confirm SNMP Configuration and Reboot**. The unit reboots and the changes take effect.

SNMP pages (for SNMPv1/2c)

This section describes how to configure Simple Network Management Protocol version 1 or 2c (SNMPv1 or SNMPv2c) traps using the SNMP Wizard.

Current SNMP Summary (for SNMPv1/2c)

Menu option: **Management > SNMP** (Figure 84).

Use this page to review the current SNMP configuration and start the SNMP Wizard.

Procedure:

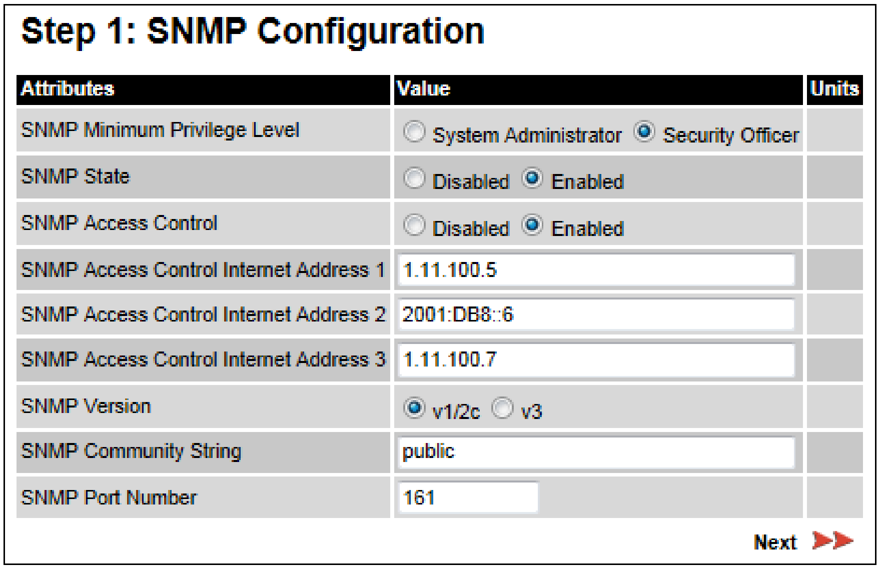
- Review the summary.
- If any updates are required, click **Continue to SNMP Wizard**.

Step 1: SNMP Configuration (for SNMPv1/2c)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 91).

Use this page to enable SNMP, select SNMPv1/2c and configure access to the SNMP server.

Figure 91 Step 1: SNMP Configuration page (for SNMPv1/2c)



Step 1: SNMP Configuration

Attributes	Value	Units
SNMP Minimum Privilege Level	○ System Administrator ● Security Officer	
SNMP State	○ Disabled ● Enabled	
SNMP Access Control	○ Disabled ● Enabled	
SNMP Access Control Internet Address 1	1.11.100.5	
SNMP Access Control Internet Address 2	2001:DB8::6	
SNMP Access Control Internet Address 3	1.11.100.7	
SNMP Version	● v1/2c ○ v3	
SNMP Community String	public	
SNMP Port Number	161	

Procedure:

- Set SNMP State to **Enabled**.
- Set SNMP Version to **v1/2c**. The page is redisplayed with SNMPv1/2c attributes.
- Update the attributes (Table 92).
- Click **Next**.

Table 92 Step 1: SNMP Configuration attributes (for SNMPv1/2c)

Attribute	Meaning
SNMP Minimum Privilege Level	Minimum security level which is permitted to administer SNMP security settings. Only displayed when Identity Based User Accounts are **Enabled** on the User Accounts page (Table 77).
SNMP State	Enables or disables SNMP.
SNMP Access Control	Enables or disables access control to SNMP management by IP address.
SNMP Access Control Internet Address 1/2/3	A list of up to three IPv4 or IPv6 Addresses permitted to perform SNMP management. Only displayed when SNMP Access Control is set to **Enabled**.
SNMP Version	SNMP protocol version: **v1/2c** or **v3**.
SNMP Community String	The SNMP community string acts like a password between the network management system and the distributed SNMP clients (PTP 650 ODUs). Only if the community string is configured correctly on all SNMP entities can the flow of management information take place. By convention the default value is set to **public**.
SNMP Port Number	Enter the port that the SNMP agent is listening to for commands from a management system.

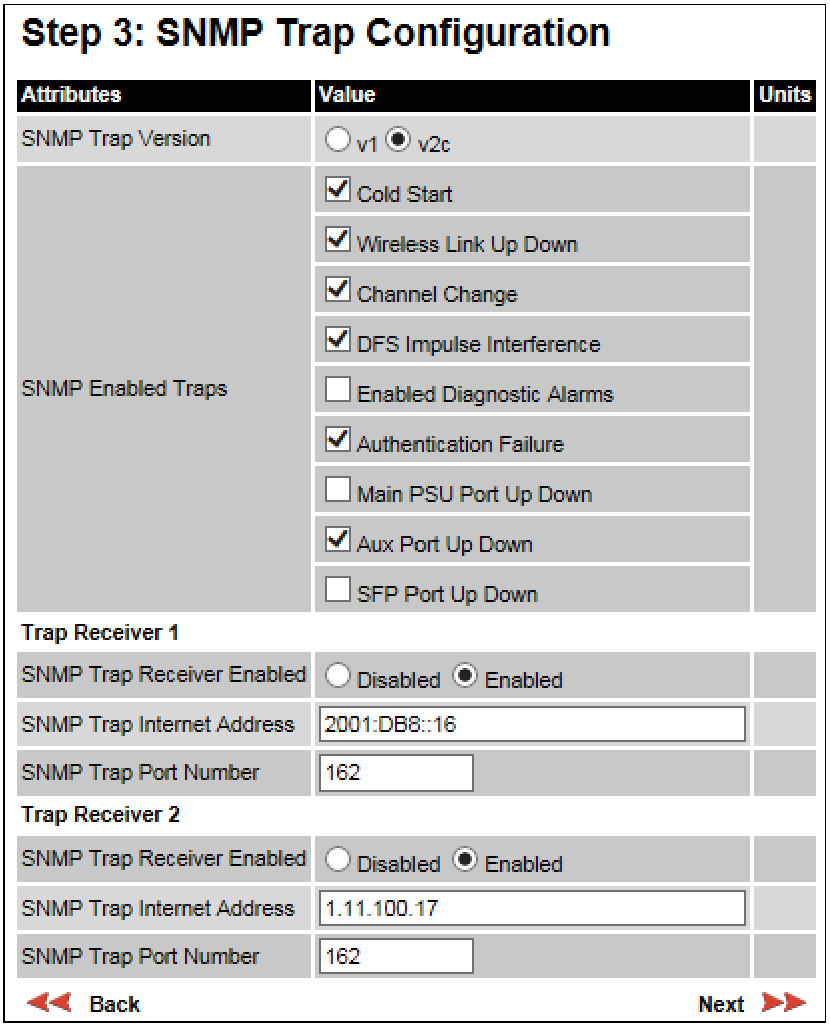
Step 2: SNMP MIB-II System Objects (for SNMPv1/2c)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 86). Use this page to enter details of the SNMP managed node. Update the attributes (Table 88) and click **Next**.

Step 3: SNMP Trap Configuration (for SNMPv1/2c)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 92).

Figure 92 Step 3: SNMP Trap Configuration page (for SNMPv1/2c)



Step 3: SNMP Trap Configuration

Attributes	Value	Units
SNMP Trap Version	○ v1 ● v2c	
SNMP Enabled Traps	☑ Cold Start ☑ Wireless Link Up Down ☑ Channel Change ☑ DFS Impulse Interference □ Enabled Diagnostic Alarms ☑ Authentication Failure □ Main PSU Port Up Down ☑ Aux Port Up Down □ SFP Port Up Down	
Trap Receiver 1		
SNMP Trap Receiver Enabled	○ Disabled ● Enabled	
SNMP Trap Internet Address	2001:DB8::16	
SNMP Trap Port Number	162	
Trap Receiver 2		
SNMP Trap Receiver Enabled	○ Disabled ● Enabled	
SNMP Trap Internet Address	1.11.100.17	
SNMP Trap Port Number	162	

Procedure:

- Update the attributes (Table 93).
- Click **Next.**

Table 93 Step 3: SNMP Trap Configuration attributes (for SNMPv1/2c)

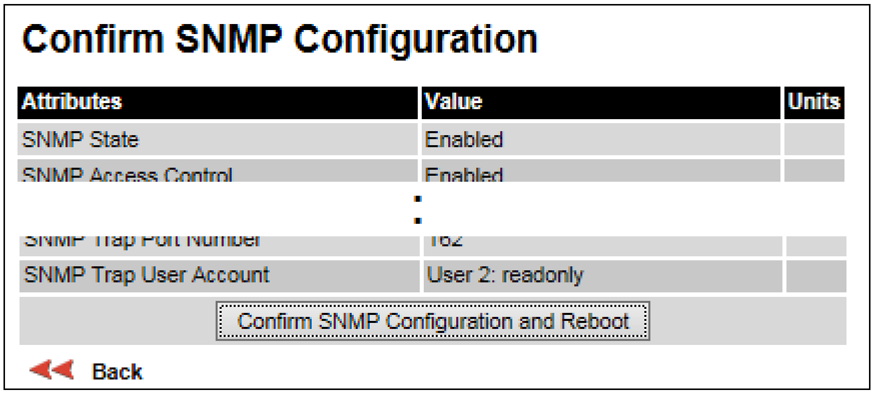
Attribute	Meaning
SNMP Trap Version	Select the SNMP protocol version to use for SNMP traps: **v1** or **v2c**.
SNMP Enabled Traps	Select the events that will generate SNMP traps.
SNMP Trap Receiver Enabled	**Disabled**: SNMP traps are not sent to the corresponding SNMP Trap Receiver (1 or 2). **Enabled**: SNMP traps are sent to the corresponding SNMP Trap Receiver (1 or 2).
SNMP Trap Internet Address	The IPv4 or IPv6 Address of the SNMP server (trap receiver). This is normally the network management system, but it may be a separate trap receiver.
SNMP Trap Port Number	The server port at which SNMP traps are received.

Confirm SNMP Configuration (for SNMPv1/2c)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 93).

Use this page to review and confirm the updated SNMPv1/2c configuration of the unit.

Figure 93 Confirm SNMP Configuration page (for SNMPv1/2c) (top and bottom of page shown)



Confirm SNMP Configuration

Attributes	Value	Units
SNMP State	Enabled	
SNMP Access Control	Enabled	
:		
SNMP Trap Port Number	162	
SNMP Trap User Account	User 2: readonly	

Procedure:

- To ensure that the changes take effect, click **Confirm SNMP Configuration and Reboot**. The unit reboots and the changes take effect.

Security menu

This section describes how to configure HTTPS/TLS security using the Security Wizard.

Caution

Ensure that the operator's security requirements are configured before connecting the PTP 650 to the network. Otherwise, security may be compromised.

Preparing for HTTPS/TLS

Before running the Security Configuration Wizard, obtain the necessary cryptographic material and ensure that the unit has AES capability. For more information, refer to Planning for HTTPS/TLS operation on page 3-33.

Procedure:

1 Ensure that the following cryptographic material has been generated:

- Key Of Keys
- TLS Private Key and Public Certificates (for the correct IP address)
- User Defined Security Banner
- Random Number Entropy Input

2 Order the necessary AES capability upgrade, generate a license key and enter it on the Software License Key page (Software License Key page on page 6-12).

3 Identify the Port numbers for HTTPS, HTTP and Telnet.

4 Ensure that the web browsers used are enabled for HTTPS/TLS operation.

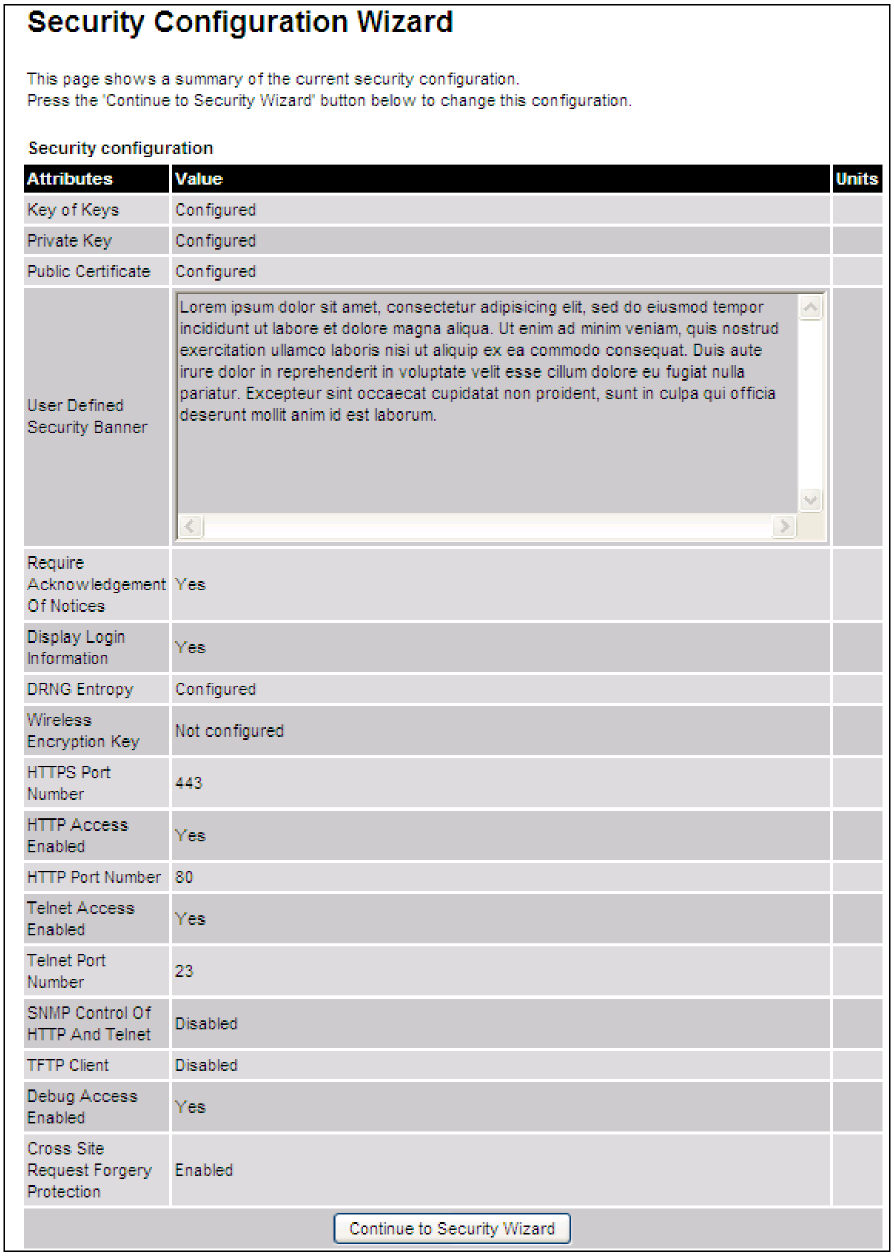
5 On the Local User Accounts page (Local User Accounts page on page 6-42), check that:

- Either: Identity Based User Accounts are set to **Disabled**,
- Or: Identity Based User Accounts are set to **Enabled** and the current user's role is **Security Officer**.

Security Configuration Wizard page

Menu option: **Security**. Displayed only when AES encryption is enabled by license key (Figure 94). Use this page to review the current security configuration of the unit.

Figure 94 Security Configuration Wizard page



Security Configuration Wizard

This page shows a summary of the current security configuration.
Press the 'Continue to Security Wizard' button below to change this configuration.

Security configuration

Attributes	Value	Units
Key of Keys	Configured	
Private Key	Configured	
Public Certificate	Configured	
User Defined Security Banner	Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.	
Require Acknowledgement Of Notices	Yes	
Display Login Information	Yes	
DRNG Entropy	Configured	
Wireless Encryption Key	Not configured	
HTTPS Port Number	443	
HTTP Access Enabled	Yes	
HTTP Port Number	80	
Telnet Access Enabled	Yes	
Telnet Port Number	23	
SNMP Control Of HTTP And Telnet	Disabled	
TFTP Client	Disabled	
Debug Access Enabled	Yes	
Cross Site Request Forgery Protection	Enabled	

Procedure:

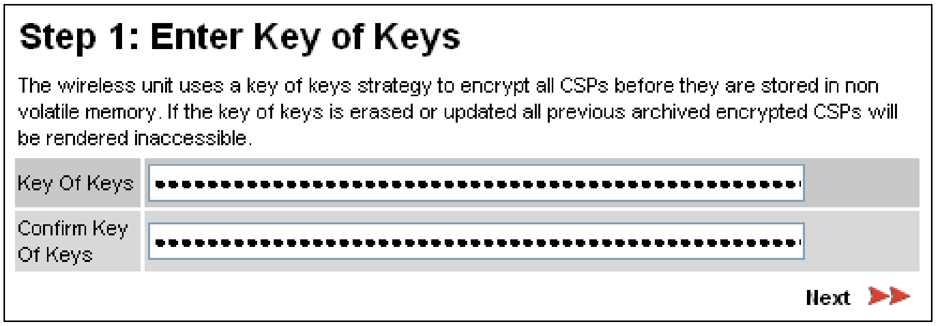
- To continue with the Security Wizard, click **Continue to Security Wizard**.

Step 1: Enter Key of Keys

Menu option: **Security**. Part of the Security Wizard (Figure 95).

Use this page to enter a Key of Keys to encrypt all critical security parameters (CSPs) before they are stored in non-volatile memory.

Figure 95 Step 1: Enter Key of Keys page



Step 1: Enter Key of Keys

The wireless unit uses a key of keys strategy to encrypt all CSPs before they are stored in non volatile memory. If the key of keys is erased or updated all previous archived encrypted CSPs will be rendered inaccessible.

Key Of Keys	••
Confirm Key Of Keys	••

Caution

Erasing or changing the key of keys erases all CSPs.

Procedure:

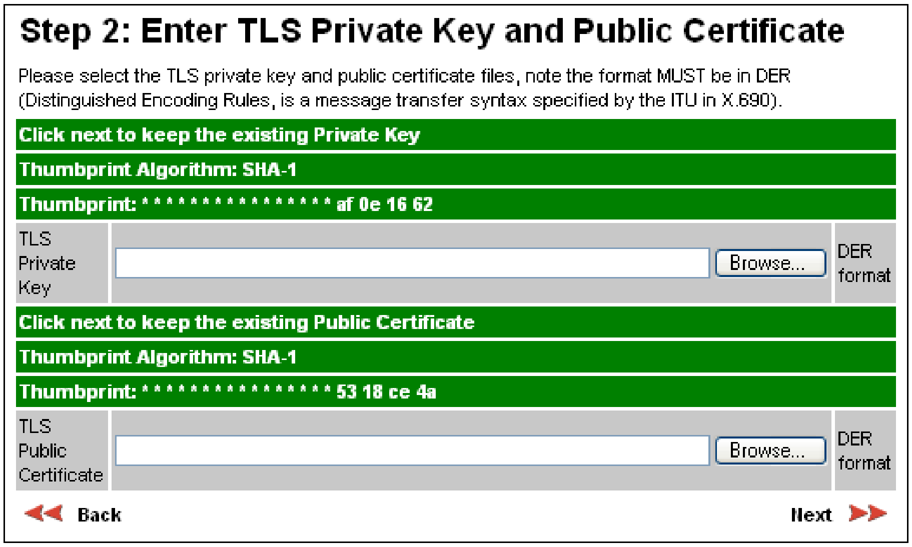
- Enter and confirm the generated Key of Keys.
- Click **Next**.

Step 2: Enter TLS Private Key and Public Certificate

Menu option: **Security.** Part of the Security Wizard (Figure 96).

Use this page to select and upload the TLS Private Key and Public Certificate files.

Figure 96 Step 2: Enter TLS Private Key and Public Certificate page



Step 2: Enter TLS Private Key and Public Certificate

Please select the TLS private key and public certificate files, note the format MUST be in DER (Distinguished Encoding Rules, is a message transfer syntax specified by the ITU in X.690).

Click next to keep the existing Private Key

Thumbprint Algorithm: SHA-1

Thumbprint: * * * * * * * * * * * * * * * * af 0e 16 62

TLS Private Key	Browse...	DER format

Click next to keep the existing Public Certificate

Thumbprint Algorithm: SHA-1

Thumbprint: * * * * * * * * * * * * * * * * 53 18 ce 4a

TLS Public Certificate	Browse...	DER format

Caution

If the certificates expire, the unit will be unreachable. If this occurs, put the unit into recovery mode and erase all configuration settings. For more information, refer to Recovery mode on page 7-44.

Procedure:

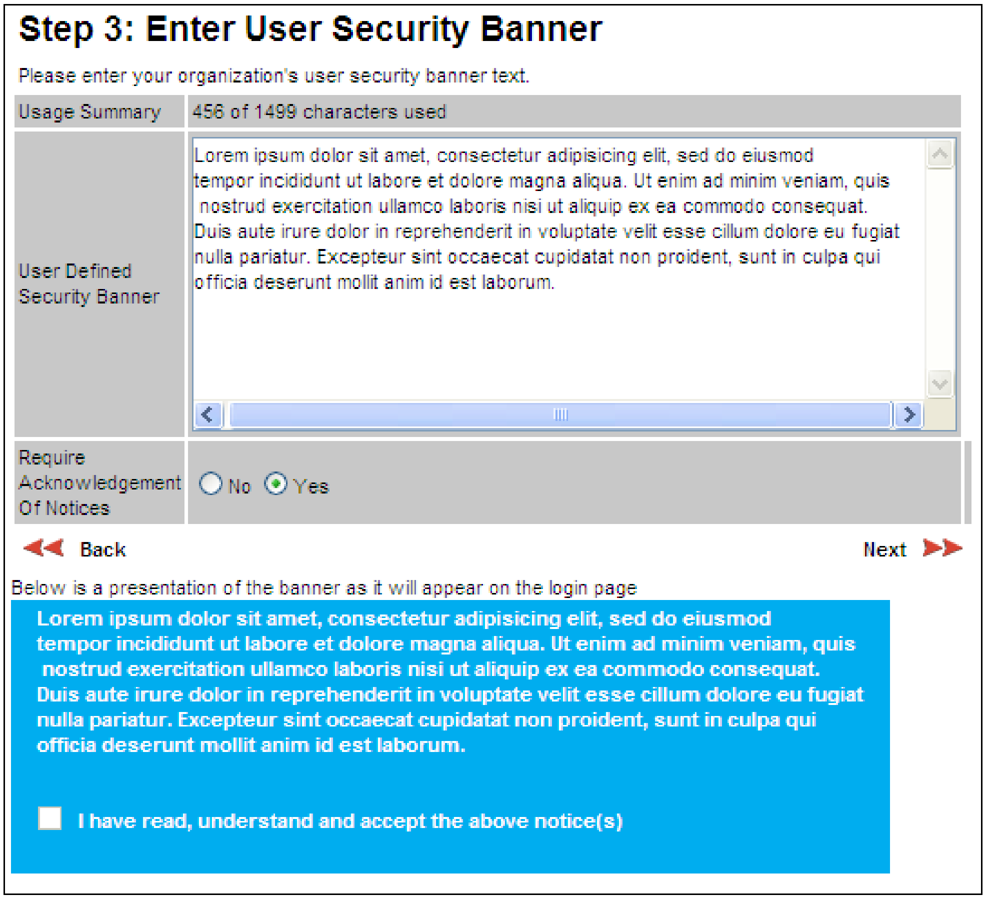
- If a valid TLS private key exists, then an SHA-1 thumbprint of the key is displayed. If this key is correct, then take no action. Otherwise, click **Browse** and select the generated private key file (.der).
- If a valid TLS public certificate exists, then an SHA-1 thumbprint of the certificate is displayed. If this certificate is correct, then take no action. Otherwise, click **Browse** and select the generated certificate file (.der).
- Click **Next.**

Step 3: Enter User Security Banner

Menu option: **Security**. Part of the Security Wizard (Figure 97).

Use this page to enter a banner that will be displayed every time a user attempts to login to the wireless unit.

Figure 97 Step 3: Enter User Security Banner page



Step 3: Enter User Security Banner

Please enter your organization's user security banner text.

Usage Summary	456 of 1499 characters used
User Defined Security Banner	Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.
Require Acknowledgement Of Notices	○ No ● Yes

Below is a presentation of the banner as it will appear on the login page

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

□ **I have read, understand and accept the above notice(s)**

Procedure:

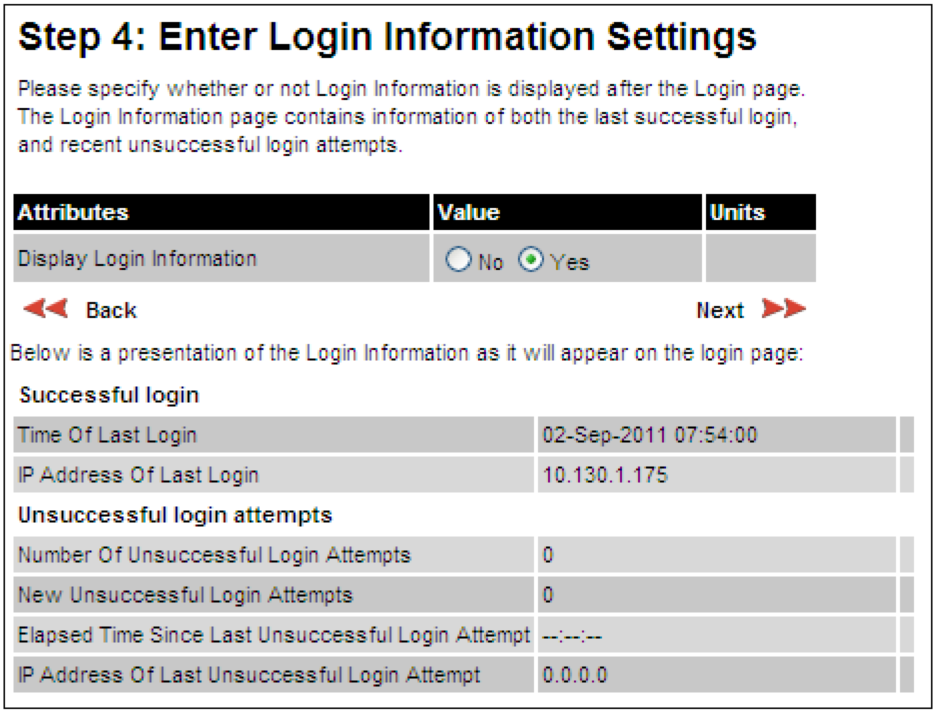
- Update the User Defined Security Banner (optional).
- Set the Acknowledgement to **No** or **Yes**.
- Click **Next**.

Step 4: Enter Login Information Settings

Menu option: **Security**. Part of the Security Wizard (Figure 98).

Use this page to choose whether or not to display information about previous login attempts when the user logs into the web interface.

Figure 98 Step 4: Enter Login Information Settings page



Step 4: Enter Login Information Settings

Please specify whether or not Login Information is displayed after the Login page. The Login Information page contains information of both the last successful login, and recent unsuccessful login attempts.

Attributes	Value	Units
Display Login Information	○ No ● Yes	

Below is a presentation of the Login Information as it will appear on the login page:

Successful login

Time Of Last Login	02-Sep-2011 07:54:00
IP Address Of Last Login	10.130.1.175

Unsuccessful login attempts

Number Of Unsuccessful Login Attempts	0
New Unsuccessful Login Attempts	0
Elapsed Time Since Last Unsuccessful Login Attempt	--:--:--
IP Address Of Last Unsuccessful Login Attempt	0.0.0.0

Procedure:

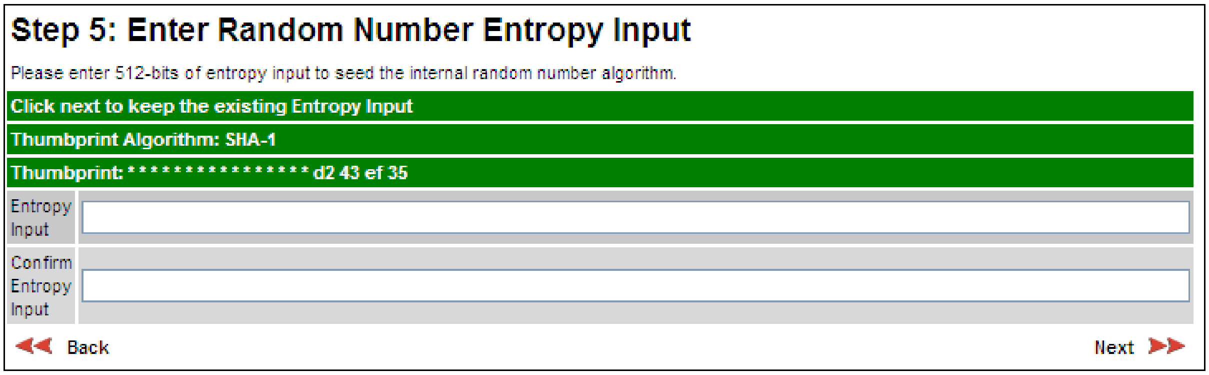
- Set Display Login Information to **No** or **Yes**.
- Click **Next**.

Step 5: Enter Random Number Entropy Input

Menu option: **Security**. Part of the Security Wizard (Figure 99).

Use this page to enter entropy input to seed the internal random number algorithm.

Figure 99 Step 5: Random Number Entropy Input page



Step 5: Enter Random Number Entropy Input

Please enter 512-bits of entropy input to seed the internal random number algorithm.

Click next to keep the existing Entropy Input

Thumbprint Algorithm: SHA-1

Thumbprint: * * * * * * * * * * * * * * * * d2 43 ef 35

Entropy Input

Confirm Entropy Input

Procedure:

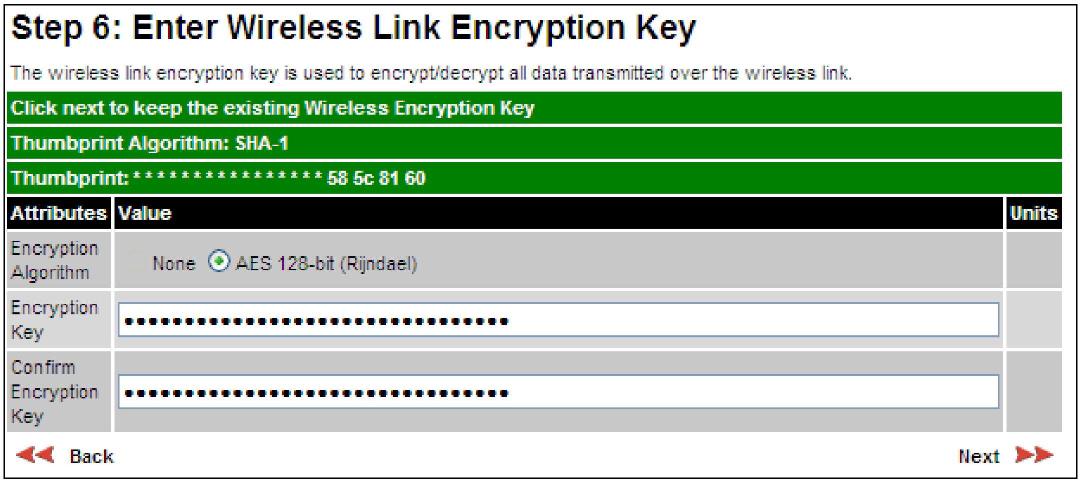
- If valid entropy input exists, then an SHA-1 thumbprint of the input is displayed. If this input is correct, then take no action. Otherwise, enter the generated input in the Entropy Input and Confirm Entropy Input fields.
- Click **Next.**

Step 6: Enter Wireless Link Encryption Key

Menu option: **Security**. Part of the Security Wizard (Figure 100).

Use this page to enable AES encryption and enter the encryption key. The wireless link encryption key is used to encrypt all traffic over the PTP 650 wireless link.

Figure 100 Step 6: Enter Wireless Link Encryption Key page



Step 6: Enter Wireless Link Encryption Key

The wireless link encryption key is used to encrypt/decrypt all data transmitted over the wireless link.

Click next to keep the existing Wireless Encryption Key

Thumbprint Algorithm: SHA-1

Thumbprint: ************** 58 5c 81 60**

Attributes	Value	Units
Encryption Algorithm	None ● AES 128-bit (Rijndael)	
Encryption Key	•••••••••••••••••••••••••••••••••	
Confirm Encryption Key	•••••••••••••••••••••••••••••••••	

Procedure:

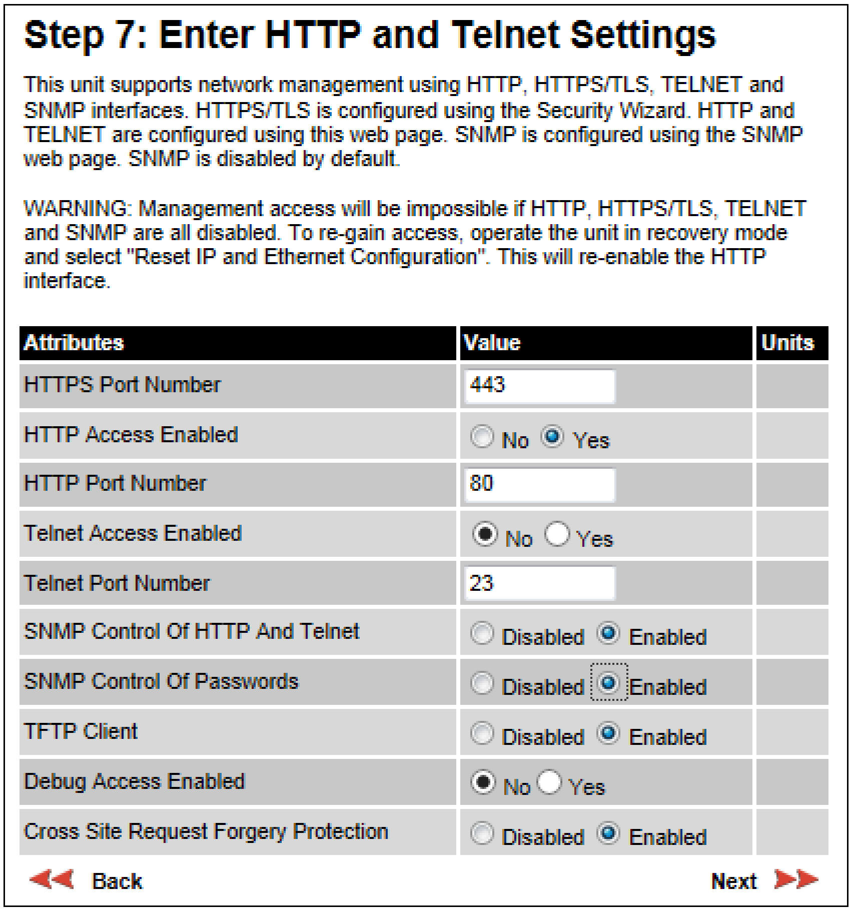
- Select the applicable value in the Encryption Algorithm field. If a valid encryption key exists, then an SHA-1 thumbprint of the key is displayed. If this key is correct, then take no action. Otherwise, enter the generated key in the Wireless Link Encryption Key and Confirm Wireless Link Encryption Key fields.
- Click **Next**.

Step 7: Enter HTTP and Telnet Settings

Menu option: **Security.** Part of the Security Wizard (Figure 101).

Use this page to configure network management of the PTP 650 using one or more of the following methods: HTTPS, HTTP, Telnet or SNMP.

Figure 101 Step 7: Enter HTTP and Telnet Settings page



Step 7: Enter HTTP and Telnet Settings

This unit supports network management using HTTP, HTTPS/TLS, TELNET and SNMP interfaces. HTTPS/TLS is configured using the Security Wizard. HTTP and TELNET are configured using this web page. SNMP is configured using the SNMP web page. SNMP is disabled by default.

WARNING: Management access will be impossible if HTTP, HTTPS/TLS, TELNET and SNMP are all disabled. To re-gain access, operate the unit in recovery mode and select "Reset IP and Ethernet Configuration". This will re-enable the HTTP interface.

Attributes	Value	Units
HTTPS Port Number	443	
HTTP Access Enabled	○ No ● Yes	
HTTP Port Number	80	
Telnet Access Enabled	● No ○ Yes	
Telnet Port Number	23	
SNMP Control Of HTTP And Telnet	○ Disabled ● Enabled	
SNMP Control Of Passwords	○ Disabled ● Enabled	
TFTP Client	○ Disabled ● Enabled	
Debug Access Enabled	● No ○ Yes	
Cross Site Request Forgery Protection	○ Disabled ● Enabled	

Caution

If HTTPS, HTTP, Telnet and SNMP are all disabled, management access will be impossible until the unit is placed in recovery mode.

Note

If HTTP, Telnet and SNMP are all disabled, the secure web server becomes the only management tool for the ODU web interface. To reenter the web interface after Step 7 of the Security Wizard, use the URL **https://aa.bb.cc.dd** (where aa.bb.cc.dd is the IP address of the unit). Enclose the IPv6 address in the URL in square brackets.

Procedure:

- Review and update the HTTP and Telnet attributes (Table 94) and click **Next**.

Table 94 HTTP and Telnet attributes

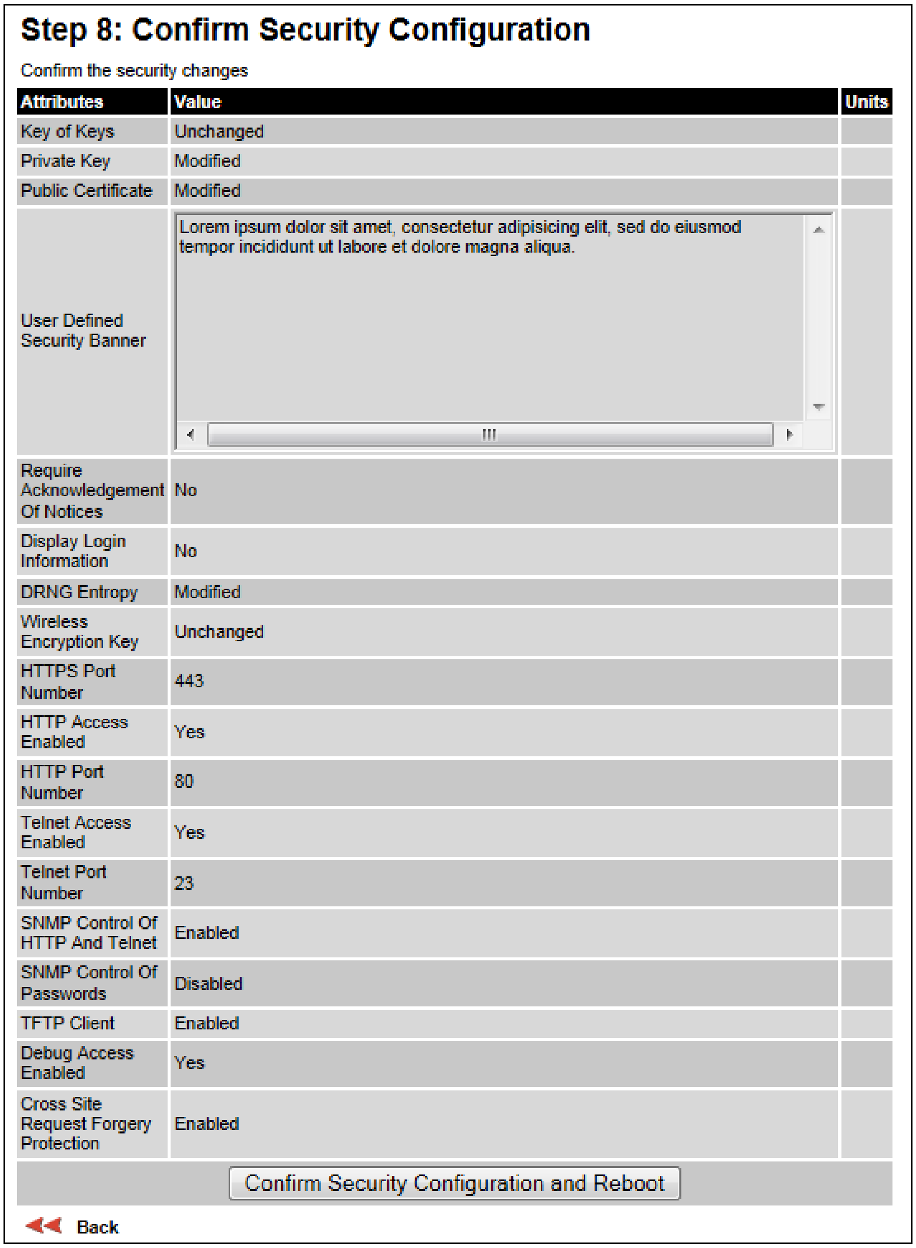
Attribute	Meaning
HTTPS Port Number	The port number for HTTPS access. Zero means use the default port.
HTTP Access Enabled	**No**: The unit will not respond to any requests on the HTTP port. **Yes**: The unit will respond to requests on the HTTP port. Remote management via HTTPS is not affected by this setting.
HTTP Port Number	The port number for HTTP access. Zero means use the default port.
Telnet Access Enabled	**No**: The unit will not respond to any requests on the Telnet port. **Yes**: The unit will respond to requests on the Telnet port.
Telnet Port Number	The port number for Telnet access. Zero means use the default port.
SNMP Control of HTTP And Telnet	**Disabled**: Neither HTTP nor Telnet can be controlled remotely via SNMP. **Enabled**: Both HTTP and Telnet can be controlled remotely via SNMP.
SNMP Control of Passwords	**Enabled:** Passwords for identity-based user accounts in the web-based interface can be updated via SNMP. Use this with SNMPv3 to provide secure password updating from a central network manager. **Disabled**: Passwords for identity-based user accounts can be updated only via the web-based interface (default).
TFTP Client	**Enabled**: The unit will respond to TFTP software download requests.
Debug Access Enabled	**Yes**: Cambium Technical Support is allowed to access the system to investigate faults.
Cross Site Request Forgery Protection	**Enabled**: The system is protected against cross-site request forgery attacks at the web-based interface.

Step 8: Commit Security Configuration

Menu option: **Security**. Part of the Security Wizard (Figure 102).

Use this page to review and confirm the updated security configuration of the unit.

Figure 102 Step 8: Commit Security Configuration page



Step 8: Confirm Security Configuration

Confirm the security changes

Attributes	Value	Units
Key of Keys	Unchanged	
Private Key	Modified	
Public Certificate	Modified	
User Defined Security Banner	Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.	
Require Acknowledgement Of Notices	No	
Display Login Information	No	
DRNG Entropy	Modified	
Wireless Encryption Key	Unchanged	
HTTPS Port Number	443	
HTTP Access Enabled	Yes	
HTTP Port Number	80	
Telnet Access Enabled	Yes	
Telnet Port Number	23	
SNMP Control Of HTTP And Telnet	Enabled	
SNMP Control Of Passwords	Disabled	
TFTP Client	Enabled	
Debug Access Enabled	Yes	
Cross Site Request Forgery Protection	Enabled	

Procedure:

- Review all changes that have been made in the Security Wizard.
- To ensure that the changes take effect, click **Commit Security Configuration and Reboot**. The unit reboots and the changes take effect.

Note

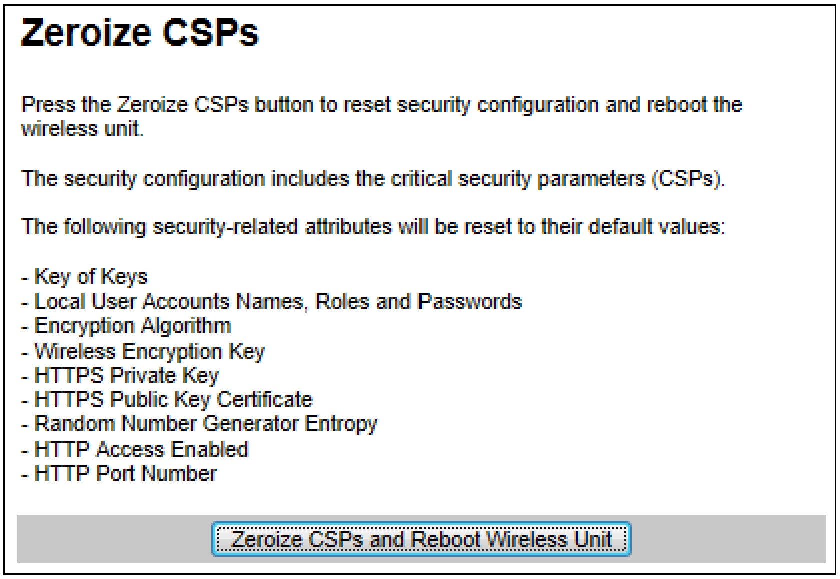
If the Key of keys is entered or modified in the Security Wizard, user accounts are reset when **Commit Security Configuration and Reboot** is clicked. It is then necessary to reconfigure them.

Zeroize CSPs page

Menu option: **Security** > **Zeroize CSPs** (Figure 103).

Use this page if it is necessary to zeroize Critical security parameters (CSPs).

Figure 103 Zeroize CSPs page



Zeroize CSPs

Press the Zeroize CSPs button to reset security configuration and reboot the wireless unit.

The security configuration includes the critical security parameters (CSPs).

The following security-related attributes will be reset to their default values:

- Key of Keys
- Local User Accounts Names, Roles and Passwords
- Encryption Algorithm
- Wireless Encryption Key
- HTTPS Private Key
- HTTPS Public Key Certificate
- Random Number Generator Entropy
- HTTP Access Enabled
- HTTP Port Number

Procedure:

- Click **Zeroize CSPs and Reboot Wireless Unit**.
- Confirm the reboot.

Aligning antennas

This section describes how to align the antennas in a PTP 650 link, use the web interface to assist with alignment, and check wireless performance after alignment.

Before performing this task, check that hardware installation is complete (apart from the network connections) at both the Master and Slave sites.

Starting up the units

Use this procedure to connect one of the units to a management PC and start up both units.

Procedure:

1 Select the unit from which this process is to be controlled; either Master or Slave. This is the “local” unit.

2 Check that the management PC is connected to the local unit, powered up and logged on as described in Connecting to the unit on page 6-5.

4 Power up the remote unit.

5 Log into the local unit as described in Logging into the web interface on page 6-7.

Checking that the units are armed

Use this procedure to confirm that the units are in the armed state, ready for alignment.

In the armed state, the modulation mode is fixed at BPSK 0.63 Single, the TDD frame duration is extended to allow the link to acquire at unknown range, and the transmit power is automatically adjusted for optimum operation.

Procedure:

- Select menu option **Home**. The System Summary page is displayed.
- Check that the Install Arm State is set to **Armed**.
- If the units are not armed, execute the installation wizard as described in Installation menu on page 6-10.

Aligning antennas

Use this procedure to align linked antennas (master and slave), whether integrated or connectorized. The goal of antenna alignment is to find the center of the main beam. This is done by adjusting the antennas while monitoring the receive signal level.

Preparation:

Ensure that the following parameters are available:

- Location of both sites (latitude and longitude).
- Bearing to the other end of the link for both sites.
- Prediction of receive signal level for both ends of the link.
- Prediction of link loss.

PTP LINKPlanner provides all of these parameters in the form of an installation report.

If a connectorized ODU is installed at either site with two separate antennas for spatial diversity, refer to Aligning separate antennas for spatial diversity on page 6-89 before starting alignment.

Note

For improved radio performance, mount the integrated ODU at 45 degrees to the vertical, as shown in Installing the ODU and top LPU on page 5-5.

To achieve best results, make small incremental changes to elevation and azimuth.

Caution

The action of tightening the mounting bolts can alter antenna alignment. This can be helpful when fine-tuning alignment, but it can also lead to misalignment. To prevent misalignment, continue to monitor receive signal level during final tightening of the bolts.

Procedure:

1 At each end of the link, adjust the antenna to point at the other end of the link. This should be done with the aid of a compass.

2 Without moving the master antenna, adjust the elevation and azimuth of the slave antenna to achieve the highest receive signal level using one of the following methods:

- ODU installation tones on page 6-90
- Graphical Install page on page 6-92

3 Without moving the Slave antenna, adjust the elevation and azimuth of the Master antenna to achieve the highest receive signal level (using one of the above methods).

4 Repeat steps 2 and 3 as necessary to fine-tune the alignment to find the center of the beam.

5 When the antennas have been aligned on the center of the beam, verify that the receive level is within the predicted range (from the installation report). If this is not the case, go back to step 2.

The current value of receive level can be verified by using the graphical installation method (see Graphical Install page on page 6-92) or by selecting menu option **Status** and monitoring the Receive Power attribute on the System Status page.

6 If after repeated attempts to align, the receive level still does not lie within the predicted range, this may be because the data provided to the prediction tool (such as PTP LINKPlanner) is inaccurate. For example estimates of path obstructions, antenna heights or site locations may be inaccurate. Check this data and update the prediction as necessary.

7 Once the antennas have been aligned correctly, tighten the integrated ODU (or connectorized antenna) mountings. To ensure that the action of tightening does not alter antenna alignment, continue to monitor received signal level.

Aligning separate antennas for spatial diversity

Use this procedure if a connectorized ODU is installed at either site with two separate antennas for spatial diversity.

Procedure:

1 Connect the horizontal polarization antenna to the ODU, disconnect the vertical polarization antenna, then perform Aligning antennas on page 6-88.

2 Connect the vertical polarization antenna to the ODU, disconnect the horizontal polarization antenna, then perform Aligning antennas on page 6-88.

3 Re-connect the horizontal polarization antennas. The received signal level should increase.

4 Weatherproof the antenna connections at the “H” and “V” interfaces of the ODUs, as described in Weatherproofing an N type connector on page 5-37.

ODU installation tones

This is the first of two methods that may be used to monitor receive signal level during antenna alignment.

The ODU emits audible tones during installation to assist with alignment. The pitch of the alignment tone is proportional to the received power of the wireless signals. Adjust the alignment of the unit in both azimuth and elevation until the highest pitch tone is achieved.

Note

When using ODU installation tones to align connectorized antennas, it may not be possible to hear the tones. To overcome this problem, either use an assistant, or use a stethoscope to give a longer reach.

The tones and their meanings are described in Table 95. In each of the states detailed in the table, align the unit to give the highest pitch tone. The term "wanted signal" refers to that of the peer unit being installed.

Table 95 ODU installation tones

State Name	Tone Description	State Description	Pitch Indication
Free Channel Search	Regular beep	Executing band scan	N/A
Scanning	Slow broken tone	Not demodulating the wanted signal	Rx Power
Synchronized	Fast broken tone	Demodulating the wanted signal	Rx Power
Registered	Solid tone	Both Master and Slave units exchanging Radio layer MAC management messages	Rx Power

Caution

If, when in the Synchronized or Registered state, the tone varies wildly, there may be interference or a fast fading link. Installing in this situation may not give a reliable link. Investigate the cause of the problem.

During alignment, the installation tones should exhibit the following behavior:

- **Band scan:** When first started up and from time to time, the Master unit will carry out a band scan to determine which channels are not in use. During this time, between 10 and 15 seconds, the Master unit will not transmit and as a consequence of this neither will the Slave unit. During this time the installation tone on the master unit will drop back to the band scan state, and the Slave unit will drop back to the Scanning state with the pitch of the tone set to the background noise level. Alignment of the unit should cease during this time.
- **Radar detection:** If the unit is operating where mandatory radar avoidance algorithms are implemented, the ranging behavior may be affected. The Master has to monitor the initially chosen channel for 60 seconds to make sure it is clear of radar signals before transmitting. If a radar signal is detected during any of the installation phases, a further compulsory 60 seconds channel scan will take place as the master unit attempts to locate a new channel that is free of radar interference.
- **Ranging:** The PTP 650 Series does not require the user to enter the link range. The Master unit typically takes less than 60 seconds to determine the length of the link being installed. The Master unit will remain in the Scanning state until the range of the link has been established. The Master unit will only move to the Synchronized state when the range of the link has been established.

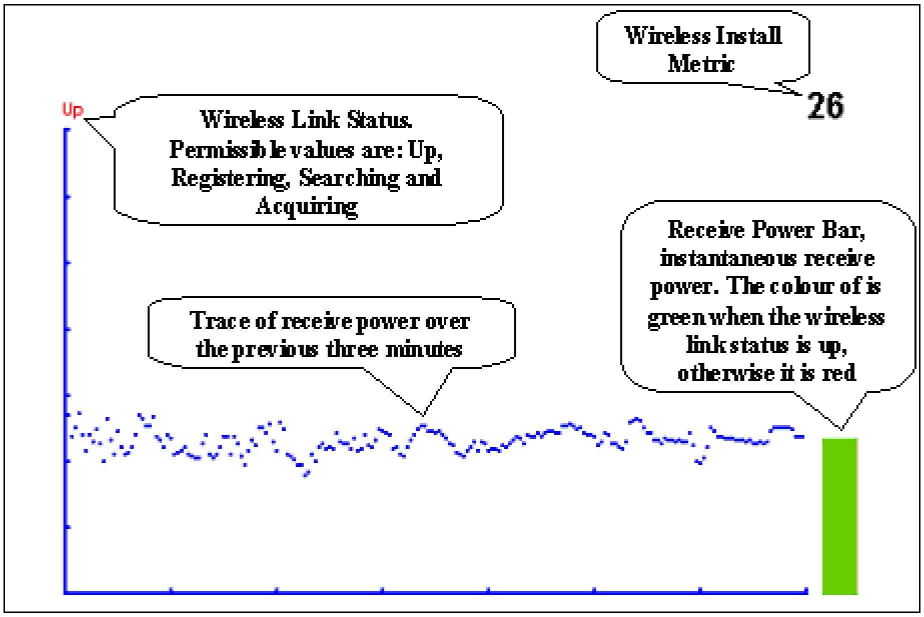
  The Slave unit does not have a ranging process. The slave unit will change to the Synchronized state as soon as the wanted signal is demodulated.
- **Retrying same channel:** If, at the end of the ranging period, the Registered state is not achieved due to interference or other reasons, the Master unit will retry twice more on the same channel before moving to another available channel. Should this occur it may take a number of minutes to establish a link in the Registered state.

Graphical Install page

Menu option: **Installation > Graphical Install** (Figure 104).

This is the second of two methods that may be used to monitor receive signal level during antenna alignment.

Figure 104 Graphical Install page


Wireless Install Metric
26
Up
Wireless Link Status. Permissible values are: Up, Registering, Searching and Acquiring
Receive Power Bar, instantaneous receive power. The colour of is green when the wireless link status is up, otherwise it is red
Trace of receive power over the previous three minutes

Procedure:

- Check that Wireless Link Status (top left) is “Up”, “Registering”, “Searching” or “Acquiring”.
- While slowly sweeping the antenna, monitor the trace of receive power over the last three minutes.
- Monitor the Receiver Power Bar (bottom right). Green signifies that the wireless link is up and red signifies all other states.
- Monitor the Wireless Install Metric (top right). This is the instantaneous receive power in dBm + 110.

Note

To access the PDA version of the graphical installation tool, use this URL - **http://<ip-address>/pda.cgi**. This link is only available to system administrators.

Disarming the units

When antenna alignment is complete, use this procedure to disarm both units in the link in order to:

- Turn off the audible alignment aid.
- Enable adaptive modulation.
- Fully enable spectrum management features (such as DSO, if configured).
- Clear unwanted installation information from the various systems statistics.
- Store the link range for fast link acquisition on link drop.
- Enable higher data rates.

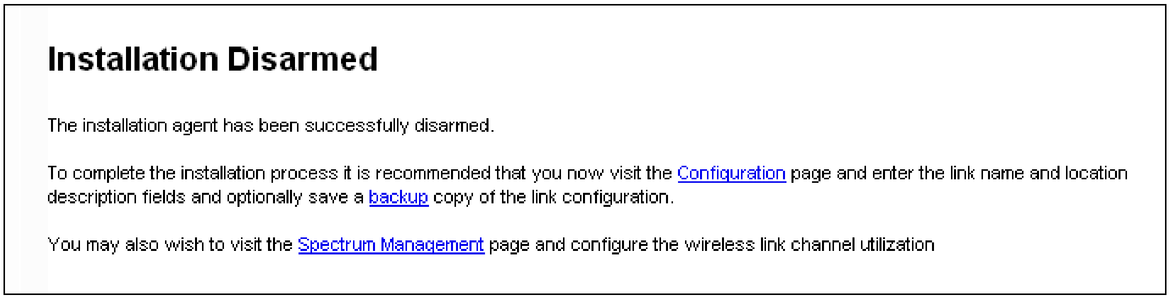
Note

After 24 hours, the units will be disarmed automatically, provided that they are armed and that the link is up.

Procedure:

- Select menu option **Installation.** The Disarm Installation page is displayed (Figure 58).
- Click **Disarm Installation Agent**. The confirmation page is displayed (Figure 105).

Figure 105 Optional post-disarm configuration



Installation Disarmed

The installation agent has been successfully disarmed.

To complete the installation process it is recommended that you now visit the Configuration page and enter the link name and location description fields and optionally save a backup copy of the link configuration.

You may also wish to visit the Spectrum Management page and configure the wireless link channel utilization

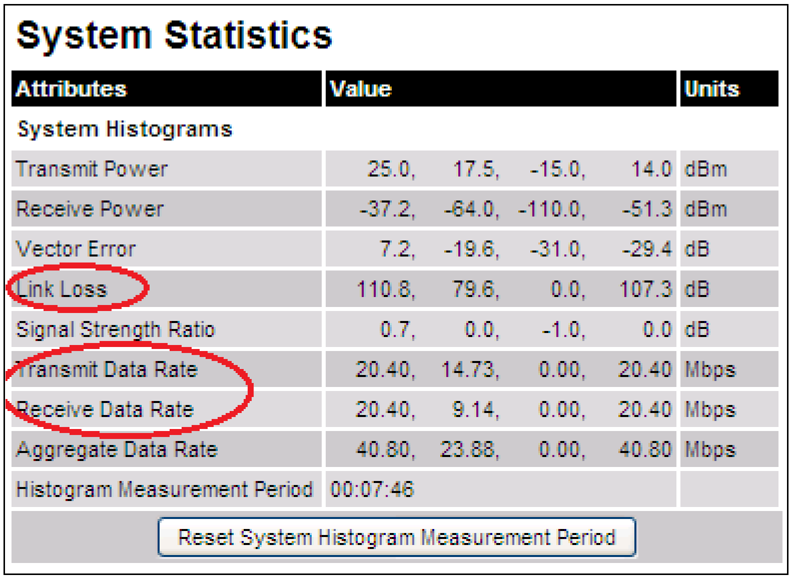
Comparing actual to predicted performance

For at least one hour of operation after disarming, use this procedure to monitor the link to check that it is achieving predicted levels of performance. PTP LINKPlanner provides the prediction in the form of an installation report.

Procedure:

- Select menu option **System > Statistics**. The System Statistic page is displayed (Figure 106).
- Monitor the following attributes:
  - o Link Loss
  - o Transmit Data Rate
  - o Receive Data Rate

Figure 106 Statistics to be monitored after alignment



System Statistics

Attributes	Value	Units
System Histograms		
Transmit Power	25.0, 17.5, -15.0, 14.0	dBm
Receive Power	-37.2, -64.0, -110.0, -51.3	dBm
Vector Error	7.2, -19.6, -31.0, -29.4	dB
Link Loss	110.8, 79.6, 0.0, 107.3	dB
Signal Strength Ratio	0.7, 0.0, -1.0, 0.0	dB
Transmit Data Rate	20.40, 14.73, 0.00, 20.40	Mbps
Receive Data Rate	20.40, 9.14, 0.00, 20.40	Mbps
Aggregate Data Rate	40.80, 23.88, 0.00, 40.80	Mbps
Histogram Measurement Period	00:07:46	

For more information on the System Statistics page, refer to System Statistics page on page 7-32.

Other configuration tasks

This section describes other configuration tasks.

Connecting to the network

Use this procedure to complete and test network connections.

Procedure:

1 If a management PC is connected directly to the PTP 650, disconnect it.

2 Confirm that all ODU Ethernet interface cables (PSU, SFP and Aux) are connected to the correct network terminating equipment or devices.

If Main PSU Port Allocation is set to **Disabled** in the LAN Configuration page), it is not necessary to connect the PSU LAN port to network terminating equipment.

3 Test that the unit is reachable from the network management system by opening the web interface to the management agent, or by requesting ICMP echo response packets using the Ping application. For in-band management, test that both units are reachable from one PC.

If the network management system is remote from the sites, either ask co-workers at the management center to perform this test, or use remote login to the management system.

4 Test the data network for correct operation across the wireless link. This may be by requesting ICMP echo response packets between hosts in the connected network segments, or by some more structured use of network testing tools.

5 Monitor the Ethernet ports and wireless link to confirm that they are running normally. For instructions, see System Summary page on page 7-2 and System Status page on page 7-3.

Upgrading software using TFTP

Use this procedure to upgrade software remotely using Trivial FTP (TFTP) triggered by SNMP.

Procedure:

1 Check that the TFTP client is enabled. Refer to Web-Based Management page on page 6-39.

2 Set tFTP attributes as described in Table 96.

3 Monitor tFTP attributes as described in Table 97.

4 Reboot the ODU as described in Rebooting the unit on page 7-51.

Table 96 Setting tFTP attributes

Attribute	Meaning
tFTPServerInternetAddress	The IPv4 or IPv6 address of the TFTP server from which the TFTP software upgrade file Name will be retrieved. For example, to set the TFTP server IP address for the unit at 10.10.10.10 to the IPv4 address 10.10.10.1, enter this command: **`snmpset_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.7.9.19.0 a 10.10.10.1`**
tFTPServerPortNumber	This setting is optional. The port number of the TFTP server from which the TFTP software upgrade file name will be retrieved (default=69).
tFTPSoftwareUpgrade FileName	The filename of the software upgrade to be loaded from the TFTP server. For example, to set the TFTP software upgrade filename on 10.10.10.10 to "B1095.dld", enter this command: **`snmpset_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.7.9.7.0 s B1095.dld`**
tFTPStartSoftware Upgrade	Write “1” to this attribute to start the TFTP software upgrade process. The attribute will be reset to 0 when the upgrade process has finished. For example, enter this command: **`snmpset_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.7.9.8.0 i 1`**

Table 97 Monitoring tFTP attributes

Attribute	Meaning

tFTPSoftwareUpgradeStatus	This is the current status of the TFTP software upgrade process. Values:
	idle(0)
	uploadinprogress(1)
	uploadsuccessfulprogrammingFLASH(2)
	upgradesuccessfulreboottorunthenewsoftwareimage(3)
	upgradefailed(4).
	For example, enter this command:
	snmpget_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.7.9.9.0

tFTPSoftwareUpgradeStatusText	This describes the status of the TFTP software upgrade process, including any error details. For example, enter this command: **snmpget_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.7.9.10.0**
tFTPSoftwareUpgradeStatusAdditionalText	This is used if tFTPSoftwareUpgradeStatusText is full and there are more than 255 characters to report. It contains additional text describing the status of the TFTP software upgrade process, including any error details. For example, enter this command: **snmpget_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.7.9.11.0**

Chapter 7: Operation

This chapter provides instructions for operators of the PTP 650 wireless Ethernet bridge.

The following topics are described in this chapter:

System summary and status

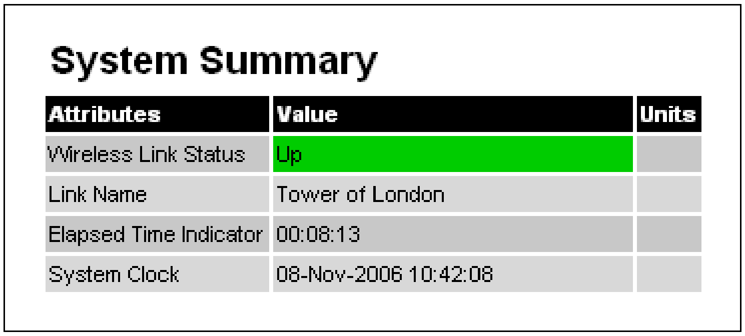
This section describes how to use the summary and status pages to monitor the status of the Ethernet ports and wireless link.

System Summary page

Menu option: **Home** (Figure 107).

This page contains a high level summary of the status of the wireless link and associated equipment.

Figure 107 System Summary page



System Summary

Attributes	Value	Units
Wireless Link Status	Up	
Link Name	Tower of London	
Elapsed Time Indicator	00:08:13	
System Clock	08-Nov-2006 10:42:08	

Procedure:

- Review the attributes (Table 98).
- Check that the Wireless Link Status is "Up" on both units. If it is not "Up", review any uncleared system alarms: these are displayed below the System Clock attribute. Whenever system alarms are outstanding, a yellow warning triangle is displayed on the navigation bar. For more information, refer to Alarms on page 7-12.

Table 98 System Summary attributes

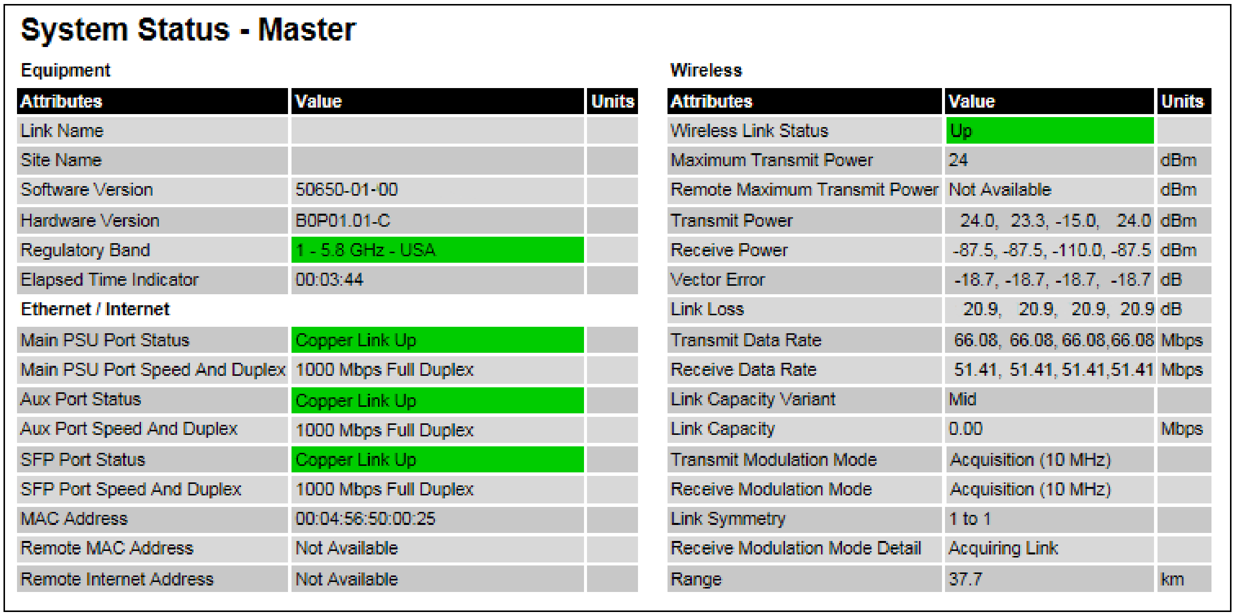
Attribute	Meaning
Wireless Link Status	Current status of the wireless link. A green background with status text "Up" means that the point-to-point link is established. A red background with suitable status text (for example "`Searching`") indicates that the link is not established.

Attribute	Meaning
Link Name	The name of the PTP link, as set in the System Configuration page.
Elapsed Time Indicator	The time (hh:mm:ss) that has elapsed since the last system reboot. The system can reboot for several reasons, for example, commanded reboot from the system reboot webpage, or a power cycle of the equipment.
System Clock	The system clock presented as local time, allowing for zone and daylight saving (if set).

System Status page

Menu option: **Status** (Figure 108). This page provides a detailed view of the operation of the PTP 650 link from both the wireless and network perspectives.

Figure 108 System Status page



System Status - Master

Equipment

Attributes	Value	Units
Link Name		
Site Name		
Software Version	50650-01-00	
Hardware Version	B0P01.01-C	
Regulatory Band	1 - 5.8 GHz - USA	
Elapsed Time Indicator	00:03:44	
Ethernet / Internet		
Main PSU Port Status	Copper Link Up	
Main PSU Port Speed And Duplex	1000 Mbps Full Duplex	
Aux Port Status	Copper Link Up	
Aux Port Speed And Duplex	1000 Mbps Full Duplex	
SFP Port Status	Copper Link Up	
SFP Port Speed And Duplex	1000 Mbps Full Duplex	
MAC Address	00:04:56:50:00:25	
Remote MAC Address	Not Available	
Remote Internet Address	Not Available	

Wireless

Attributes	Value	Units
Wireless Link Status	Up	
Maximum Transmit Power	24	dBm
Remote Maximum Transmit Power	Not Available	dBm
Transmit Power	24.0, 23.3, -15.0, 24.0	dBm
Receive Power	-87.5, -87.5, -110.0, -87.5	dBm
Vector Error	-18.7, -18.7, -18.7, -18.7	dB
Link Loss	20.9, 20.9, 20.9, 20.9	dB
Transmit Data Rate	66.08, 66.08, 66.08,66.08	Mbps
Receive Data Rate	51.41, 51.41, 51.41,51.41	Mbps
Link Capacity Variant	Mid	
Link Capacity	0.00	Mbps
Transmit Modulation Mode	Acquisition (10 MHz)	
Receive Modulation Mode	Acquisition (10 MHz)	
Link Symmetry	1 to 1	
Receive Modulation Mode Detail	Acquiring Link	
Range	37.7	km

The two PTP 650 Series units are arranged in a master and slave relationship. The roles of the units in this relationship are displayed in the page title. The master unit will always have the title "`- Master`", and the slave will always have "`- Slave`" appended to the "`Systems Status`" page title.

Note

Link Symmetry is configured at the master ODU only. The appropriate matching Link Symmetry is set at the slave ODU automatically. For example, if Link Symmetry is configured as **2 to 1** at the master ODU, then the slave ODU will be set automatically as **1 to 2**. In this example, the master-slave direction has double the capacity of the slave-master direction.

Procedures:

- Review the attributes (Table 99).
- Confirm that the Ethernet Link Status attributes are green and set to **Copper Link Up** or **Fiber Link Up**.

Table 99 System Status attributes

Attribute	Meaning
Link Name	The link name is allocated by the system administrator and is used to identify the equipment on the network. The link name attribute is limited to a maximum size of 63 ASCII characters.
Site Name	The site name is allocated by the system administrator and can be used as a generic scratch pad to describe the location of the equipment or any other equipment related notes. The site name attribute is limited to a maximum size of 63 ASCII characters.
Software Version	The version of PTP 650 software installed on the equipment.
Hardware Version	The PTP 650 hardware version. Formatted as "vvvv" where vvvv is the version of the printed circuit card
Regulatory Band	This is used by the system to constrain the wireless to operate within regulatory regime of a particular band and country. The license key provides the capability to operate in one or more regulatory bands. The Installation Wizard is used to choose one of those bands.
Elapsed Time Indicator	The elapsed time indicator attribute presents the total time in years, days, hours, minutes and seconds since the last system restart. The system can restart for several reasons, for example commanded reboot from the system reboot web page, or a power cycle of the equipment.
Main PSU Port Status	This indicates the current status of the Ethernet link to the PSU port. A state of "`Copper Link Up`" with a green background indicates that an Ethernet link is established. A state of "`Down`" with a red background indicates that the Ethernet link is not established.
Main PSU Port Speed and Duplex	The negotiated speed and duplex setting of the Ethernet link to the PSU port. The speed setting is specified in Mbps.

Attribute	Meaning
Aux Port Status	This indicates the current status of the Ethernet link to the Aux port. A state of "Copper Link Up" with a green background indicates that an Ethernet link is established. A state of "Down" with a red background indicates that the Ethernet link is not established.
Aux Port Speed and Duplex	The negotiated speed and duplex setting of the Ethernet link to the Aux port. The speed setting is specified in Mbps.
SFP Port Status	This indicates the current status of the Ethernet link to the SFP port. A state of "Copper Link Up" or "Fiber Link Up" with a green background indicates that an Ethernet link is established. A state of "Down" with a red background indicates that the Ethernet link is not established.
SFP Port Speed and Duplex	The negotiated speed and duplex setting of the Ethernet link to the PSU port. The speed setting is specified in Mbps.
MAC Address	The MAC Address of this unit.
Remote MAC Address	The MAC Address of the peer unit. If the link is down, this is set to "Not available".
Remote Internet Address	The Internet Address of the peer unit. To open the web interface of the peer unit, click on the hyperlink. If the link is down, this is set to "Not available". Depending on the settings of IP Version (Table 71) and IP Address Label (Table 70), this may be either an IPv4 or an IPv6 address.
Wireless Link Status	As the attribute name suggests it displays the current status of the wireless link. A state of "Up" on a green background indicates that a point-to-point link is established. A state of "Down" on a red background indicates that the wireless link is not established.
Maximum Transmit Power	The maximum transmit power that the local wireless unit is permitted to use to sustain a link.
Remote Maximum Transmit Power	The maximum transmit power that the remote wireless unit is permitted to use to sustain a link.
Transmit Power	The maximum, mean, minimum and latest measurements of Transmit Power (dBm). See System histograms on page 7-32.
Receive Power	The maximum, mean, minimum and latest measurements of Receive Power (dBm). See System histograms on page 7-32.

Attribute	Meaning
Vector Error	The maximum, mean, minimum and latest measurements of Vector Error (dB). See System histograms on page 7-32. Vector Error compares the received signals In phase / Quadrature (IQ) modulation characteristics to an ideal signal to determine the composite error vector magnitude. The expected range for Vector Error is approximately -2 dB (NLOS link operating at sensitivity limit on BPSK 0.67) to -33 dB (short LOS link running 256 QAM 0.83).
Link Loss	The maximum, mean, minimum and latest measurements of Link Loss (dB). See System histograms on page 7-32. The link loss is the total attenuation of the wireless signal between the two point-to-point units. The link loss calculation is presented below: $P_{ll} = P_{T_x} - P_{R_x} + g_{T_x} + g_{R_x}$ Where: P_{ll} = Link Loss (dB) P_{T_x} = Transmit power of the remote wireless unit (dBm) P_{R_x} = Received signal power at the local unit (dBm) g_{T_x}, g_{R_x} = Antenna gain at the remote and local units respectively (dBi). The antenna gain of the PTP 650 Series (23.5 dBi) is used unless one or both of the units is a Connectorized version. For connectorized ODUs, the link loss calculation is modified to allow for the increased antenna gains at each end of the link.
Transmit Data Rate	The maximum, mean, minimum and latest measurements of Transmit Data Rate (Mbps). See System histograms on page 7-32.
Receive Data Rate	The maximum, mean, minimum and latest measurements of Receive Data Rate (Mbps). See System histograms on page 7-32.
Link Capacity Variant	Indicates whether the installed license key is Lite, Mid or Full. When a link is established, this attribute shows the lower of the license keys at each end. For example, if this end is Full and the other end is Lite, it shows “Lite”. To see the installed key, go to the Installation Wizard.

Attribute	Meaning
Link Capacity	The maximum aggregate data rate capacity available for user traffic, assuming the units have been connected using Gigabit Ethernet. The link capacity is variable and depends on the prevailing wireless conditions as well as the distance (range) between the two wireless units.
Transmit Modulation Mode	The modulation mode currently being used on the transmit channel.
Receive Modulation Mode	The modulation mode currently being used on the receive channel.
Link Symmetry	A ratio that expresses the division between transmit and receive time in the TDD frame. The first number in the ratio represents the time allowed for the transmit direction and the second number represents the time allowed for the receive direction.
Receive Modulation Mode Detail	The receive modulation mode in use. For a list of values and their meanings, see Table 100.
Range	The range between the PTP 650 Series ODUs. This is displayed in kilometers by default, but can be changed to miles by updating the Distance Units attribute to imperial, as described in Webpage Properties page on page 6-49.

Table 100 Receive Modulation Mode Detail values and meanings

Value	Meaning
Running At Maximum Receive Mode	The link is operating at maximum modulation mode in this channel and maximum throughput has been obtained.
Running At User-Configured Max Modulation Mode	The maximum modulation mode has been capped by the user and the link is operating at this cap.
Restricted Because Installation Is Armed	The Installation Wizard has been run and the unit is armed, forcing the link to operate in the lowest modulation mode. To remove this restriction, re-run the Installation Wizard to disarm the unit.
Restricted Because Of Byte Errors On The Wireless Link	The receiver has detected data errors on the radio and reduced the modulation mode accordingly. The radio may achieve a higher modulation mode as shown by the vector error, but there is some other error source, probably RF interference.
Restricted Because Channel Change Is In Progress	This is a transient event where the modulation mode is temporarily reduced during a channel change.

Value	Meaning
Limited By The Wireless Conditions	The radio is running at the maximum achievable modulation mode given the current wireless conditions shown by the vector error. The radio is capable of reaching a higher modulation mode if wireless conditions (vector error) improve.

Rebooting and logging out

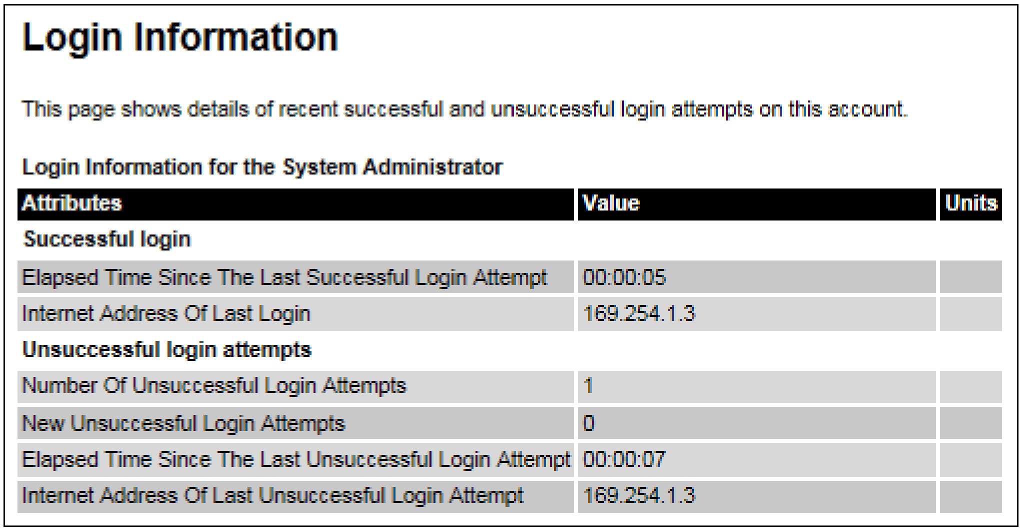
This section describes how to reboot the unit and log out of the web interface.

Login Information page

Menu option: **Management > Web > Login Information** (Figure 109).

Use this page to show recent successful and unsuccessful login attempts on this account.

Figure 109 Login Information page



Login Information

This page shows details of recent successful and unsuccessful login attempts on this account.

Login Information for the System Administrator

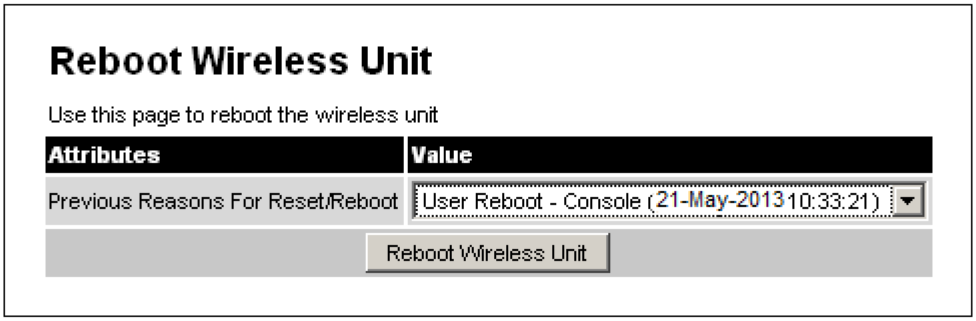
Attributes	Value	Units
Successful login		
Elapsed Time Since The Last Successful Login Attempt	00:00:05	
Internet Address Of Last Login	169.254.1.3	
Unsuccessful login attempts		
Number Of Unsuccessful Login Attempts	1	
New Unsuccessful Login Attempts	0	
Elapsed Time Since The Last Unsuccessful Login Attempt	00:00:07	
Internet Address Of Last Unsuccessful Login Attempt	169.254.1.3	

Reboot Wireless Unit page

Menu option: **System > Reboot** (Figure 110).

Use this page to reboot the ODU or view a list of previous reboot reasons.

Figure 110 Reboot Wireless Unit page



Reboot Wireless Unit

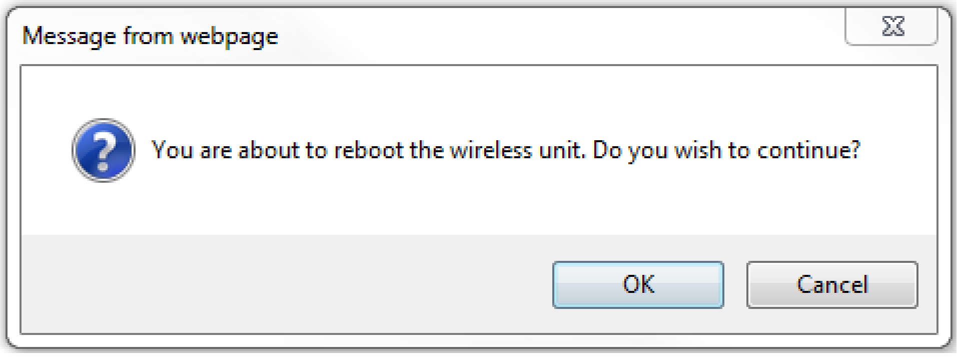
Use this page to reboot the wireless unit

Attributes	Value
Previous Reasons For Reset/Reboot	User Reboot - Console (21-May-2013 10:33:21)

Procedure:

- Use the drop-down list to view the Previous Reasons For Reset/Reboot.
- If a reboot is required:
  - o Click **Reboot Wireless Unit**. The Reboot Confirmation dialog is displayed (Figure 111).
  - o Click **OK**. The reboot progress message is displayed. On completion, the unit restarts.

Figure 111 Reboot confirmation pop up



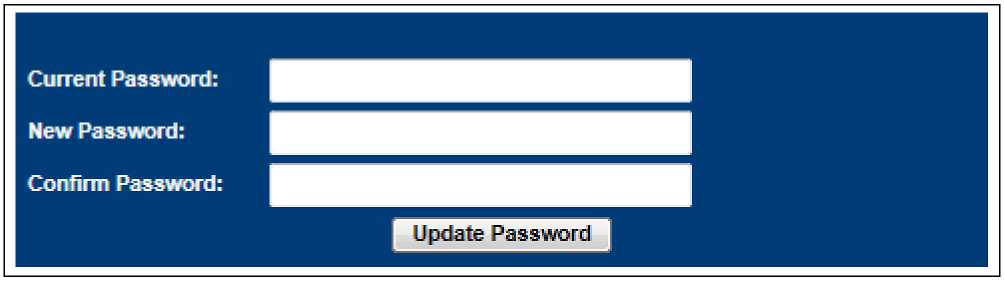
Message from webpage

You are about to reboot the wireless unit. Do you wish to continue?

Change Password page

Menu option: **Change Password** (Figure 112). Use this page to change a personal password.

Figure 112 Change Password page (System Administration example)



Current Password:

New Password:

Confirm Password:

Note

A security officer can change the passwords of other users using the User Accounts page, as described in Local User Accounts page on page 6-42.

Procedure:

- Enter and confirm the new password (the default is blank). The new password must comply with the complexity rules (Table 78).

Logging out

To maintain security, always log out at the end of a session: on the menu, click **Logout**.

The unit will log out automatically if there is no user activity for a set time, but this depends upon Auto Logout Period in the Webpage Properties page (Figure 78).

Alarms, alerts and messages

This section describes how to use alarms, alerts and syslog messages to monitor the status of a PTP 650 link.

Alarms

Whenever system alarms are outstanding, a yellow warning triangle is displayed on the navigation bar. The warning triangle is visible from all web pages.

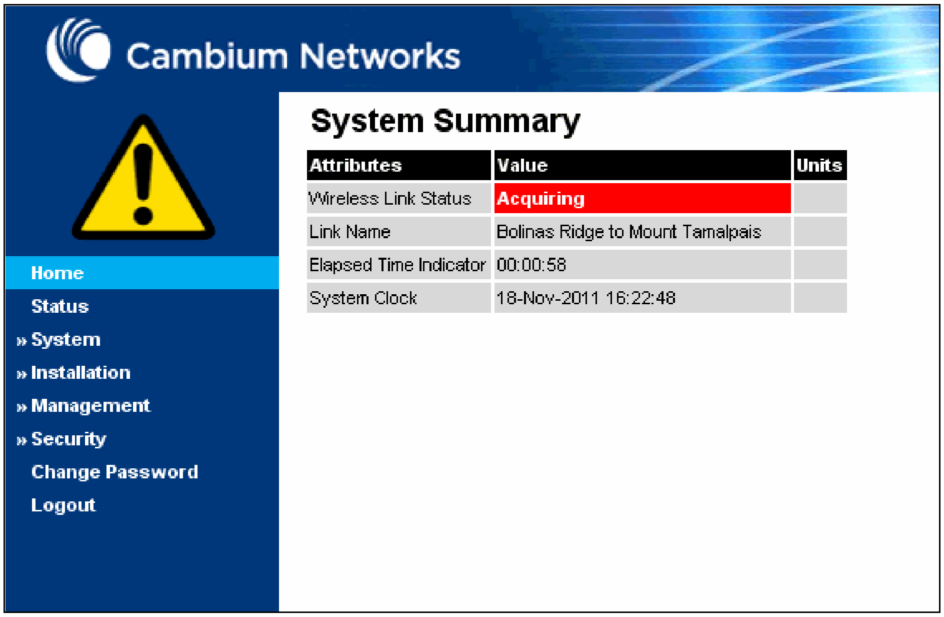
Procedure:

- Click the warning triangle (or menu option **Home**) to return to the System Summary page and view the alarms. If the warning triangle disappears when it is clicked, it indicates that the outstanding alarms have been cleared.

The example in Figure 113 shows the warning triangle in the navigation bar and an alarm displayed in the System Summary page. The alarms are defined in Table 101.

A change of state in most alarms generates an SNMP trap or an SMTP email alert.

Figure 113 Alarm warning triangle



System Summary

Attributes	Value	Units
Wireless Link Status	Acquiring	
Link Name	Bolinas Ridge to Mount Tamalpais	
Elapsed Time Indicator	00:00:58	
System Clock	18-Nov-2011 16:22:48	

Table 101 System alarms

Alarm	Meaning
Regulatory Band	The installed license key contains an invalid Regulatory Band. The wireless unit is prohibited from operating outside the regulated limits.
Install Status	Signaling was received with the wrong MAC address. It is very unusual to detect this, because units with wrongly configured Target MAC Address will normally fail to establish a wireless link. However, rare circumstances may establish a partial wireless link and detect this situation.
Install Arm State	A wireless unit is in installation mode. After installation, the wireless unit should be disarmed. This will increase the data-carrying capacity and stop the installation tone generator. The wireless link is disarmed from the “Installation” process, see Disarming the units on page 6-93.
Unit Out Of Calibration	The unit is out of calibration and must be returned to the factory using the RMA process for re-calibration.
Incompatible Regulatory Bands	The two linked units have different Regulatory Bands. To clear this alarm, obtain and install license keys for the correct country and select the same Regulatory Band at each end of the link.
Incompatible Master and Slave	The master and slave ends of the wireless link are different hardware products, or have different software versions. It is very unusual to detect this because incompatible units will normally fail to establish a wireless link. However, some combinations may establish a partial wireless link and detect this situation.
Main PSU Port Configuration Mismatch	Ethernet fragments (runt packets) have been detected when the PSU port is in full duplex. This indicates an auto-negotiation or forced configuration mismatch.
No Wireless Channel Available	Spectrum Management was unable to locate a suitable wireless channel to operate on.
SNTP Synchronization failed	SNTP has been enabled but the unit is unable to synchronize with the specified SNTP server.

Alarm	Meaning
Wireless Link Disabled Warning	The wireless link has been administratively disabled via the SNMP Interface. The wireless interface MIB-II ifAdminStatus attribute has been set to **DOWN**. To enable the Ethernet interface, set the ifAdminStatus attribute to **UP**.
Main PSU Port Disabled Warning	The PSU port link has been administratively disabled via the SNMP Interface.
Main PSU Port Status	The PSU port link is down. The most likely cause is that the unit has no Ethernet cable plugged into its Aux port.
SFP Error	A non-OK value indicates that the SFP link is down. There are two possible causes: • Either: the fiber link has been installed but disabled (because the license key does not include SFP support), • Or: the SFP link could not be established even though an SFP carrier was detected (due perhaps to a cabling fault or the link is disabled at the link partner).
SFP Port Configuration Mismatch	Ethernet fragments (runt packets) have been detected when the SFP port is in full duplex. This indicates an auto-negotiation or forced configuration mismatch.
SFP Port Disabled Warning	The SFP port link has been administratively disabled via the SNMP Interface.
SFP Port Status	The SFP port link is down. The most likely cause is that the unit has no Ethernet cable plugged into its SFP port.
Aux Port PoE Output Status	The Aux port link is down. The most likely cause is that the unit has no Ethernet cable plugged into its Aux port.
Aux Port Disabled Warning	The Aux port link has been administratively disabled via the SNMP Interface.
Aux Port Status	The Aux port link is down. The most likely cause is that the unit has no Ethernet cable plugged into its Aux port.
Link Mode Optimization Mismatch	The Master and Slave ODUs are configured to use different link mode optimization methods (one is set to IP and the other TDM).
Syslog Enabled/ Disabled Warning	The local log of event messages has been enabled or disabled.
Syslog Local Nearly Full	The local log of event messages is nearly full.

Alarm	Meaning
Syslog Local Wrapped	The local log of event messages is full and is now being overwritten by new messages.
Aux Port Configuration Mismatch	Ethernet fragments (runt packets) have been detected when the Aux port is in full duplex. This indicates an auto-negotiation or forced configuration mismatch.
Syslog Client Enabled/Disabled Warning	The local syslog client has been enabled or disabled.
Ethernet Bridging Status	"`Disabled`" means that the link has stopped bridging Ethernet frames because the Lowest Ethernet Modulation Mode is not being achieved or because the wireless link is down.
Remaining Full Capacity Time Trial	Time remaining on the full capability trial period. Activated when seven days or less of the trial period remain.
Capacity Variant Mismatch	The link ends are different capability variants, for example, one is Full and the other is Med.

Email alerts

The management agent can be configured to generate alerts by electronic mail when certain events occur. The alerts are defined in Table 102.

Table 102 Email alerts

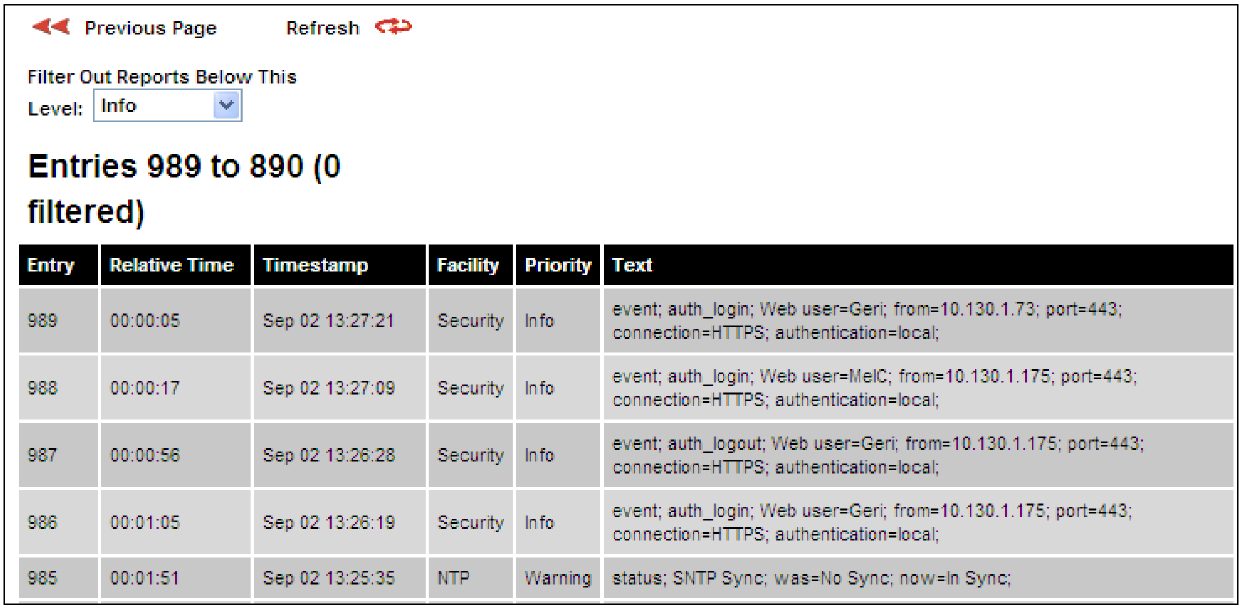
Alert	Meaning
Wireless Link Up Down	There has been a change in the status of the wireless link.
Channel Change	DFS has forced a change of channel.
DFS Impulse Interference	DFS has detected impulse interference.
Enabled Diagnostic Alarms	Diagnostic alarms have been enabled.
Main PSU Port Up Down	There has been a change in the status of the PSU data port.
Aux Port Up Down	There has been a change in the status of the Aux port.
SFP Port Up Down	There has been a change in the status of the SFP port.

Syslog page

Menu option: **Management > Syslog** (Figure 114).

Use this page to view the local log of event messages.

Figure 114 Syslog local log



Filter Out Reports Below This Level: Info

Entries 989 to 890 (0 filtered)

Entry	Relative Time	Timestamp	Facility	Priority	Text
989	00:00:05	Sep 02 13:27:21	Security	Info	event; auth_login; Web user=Geri; from=10.130.1.73; port=443; connection=HTTPS; authentication=local;
988	00:00:17	Sep 02 13:27:09	Security	Info	event; auth_login; Web user=MelC; from=10.130.1.175; port=443; connection=HTTPS; authentication=local;
987	00:00:56	Sep 02 13:26:28	Security	Info	event; auth_logout; Web user=Geri; from=10.130.1.175; port=443; connection=HTTPS; authentication=local;
986	00:01:05	Sep 02 13:26:19	Security	Info	event; auth_login; Web user=Geri; from=10.130.1.175; port=443; connection=HTTPS; authentication=local;
985	00:01:51	Sep 02 13:25:35	NTP	Warning	status; SNTP Sync; was=No Sync; now=In Sync;

Note

For more information about system logging, refer to:

- System logging (syslog) on page 1-32 describes the system logging feature.
- Syslog Configuration page on page 6-59 describes how to enable system logging.

Format of syslog server messages

PTP 650 generates syslog messages in this format:

```
SP = “ ” = %x20

CO = “:” = %x3A

SC = “;” = %x3B

LT = “<” = %x3C

GT = “>” = %x3E

syslog = pri header SP message

pri = LT “1”-“182” GT

header = timestamp SP hostname

timestamp = month SP days SP hours “:” minutes “:” seconds

month = “Jan”|“Feb”|“Mar”|“Apr”|“May”|“Jun”|
“Jul”|“Aug”|“Sep”|“Oct”|“Nov”|“Dec”

days = “ 1”-“31”

hours = “00”-“23”

minutes = seconds = “00”-“59”

hostname = “0.0.0.0”-“255.255.255.255”

message = “PTP650” CO SP (configuration | status | event)

configuration = “configuration” SC SP attribute-name SC SP (“Web
user”|“SNMP user”|“SNTP”) SC SP “was=” previous-value SC SP “now=”
new-value SC

status = “status” SC SP attribute-name SC SP “was=” previous-value SC
SP “now=” new-value SC

event = “event” SC SP identifier SC SP event-message-content SC
```

Configuration and status messages

Configuration and status messages contain all of the relevant attributes.

This is an example of a configuration message:

```
PTP650: configuration; IP Address; Web user; was=10.10.10.10;
now=169.254.1.1;
```

This is an example of a status message:

```
PTP650: status; Data Port Status; was=Down; now=Up;
```

Event messages

Event messages are listed in Table 103. Definition of abbreviations:

SC = ";"

SP = " "

This is an example of an event message:

```
PTP650: event; auth_login; web user=MarkT; from=169.254.1.1; port=80;
connection=HTTP; authentication=local;
```

Table 103 Event messages

Facility	Severity	Identifier	Message content
security(4)	warning(4)	auth_idle	"Web user=" user-name SC SP "from=" IP-address SC SP "port=" port-number SC SP "connection=" ("HTTP" | "HTTPS") SC SP "authentication=" ("local" | "RADIUS") SC
security(4)	info(6)	auth_login	
security(4)	warning(4)	auth_login_failed	
security(4)	warning(4)	auth_login_locked	
security(4)	info(6)	auth_logout	
kernel(0)	warning(4)	cold_start	"PTP wireless bridge has reinitialized, reason=" reset-reason SC
security(4)	warning(4)	License_update	"License Key updated" SC
syslog(5)	warning(4)	log_full	"Syslog local flash log is 90% full" SC
syslog(5)	warning(4)	log_wrap	"Syslog local flash log has wrapped" SC
security(4)	info(6)	radius_auth	"RADIUS user=" user-name SC SP "server " ("1" | "2") " at " IP-address SP "succeeded" SC
security(4)	warning(4)	radius_auth_fail	"RADIUS user=" user-name SC SP "server " ("1" | "2") " at " IP-address SP ("failed" | "succeeded" | "failed (no response)") SC
security(4)	alert(1)	resource_low	"Potential DoS attack on packet ingress " ("warning" | "cleared") SC
security(4)	warning(4)	sec_zeroize	"Critical Security Parameters (CSPs) zeroized" SC
local6(22)	warning(4)	snmpv3_asn1	"ASN.1 parse error" SC

Facility	Severity	Identifier	Message content
security(4)	warning(4)	snmpv3_auth	"Authentication failure" SC
local6(22)	warning(4)	snmpv3_decryption	"Decryption failure" SC
local6(22)	warning(4)	snmpv3_engine_id	"Unknown engine ID" SC
local6(22)	warning(4)	snmpv3_sec_level	"Unknown security level" SC
kernel(0)	warning(4)	sys_reboot	"System Reboot, reason=" reset-reason SC
security(4)	warning(4)	sys_software_upgrade	"Software upgraded from " software-version " to " software-version SC
local6(22)	warning(4)	telnet_idle	"Telnet user=" user-name SC SP "from=" IP-address SC SP "port=" port-number SC
local6(22)	info(6)	telnet_login	
local6(22)	warning(4)	telnet_login_failed	
local6(22)	info(6)	telnet_logout	
local6(22)	info(6)	tftp_complete	"TFTP software upgrade finished" SC
local6(22)	info(6)	tftp_failure	"TFTP software upgrade failed, reason=" reason SC
local6(22)	info(6)	tftp_start	"TFTP software upgrade started" SC
NTP(12)	info(6)	time_auth	"SNTP authentication succeeded at IP-address=" IP-address SC SP "port-number=" port SC
NTP(12)	warning(4)	time_auth_failed	"SNTP authentication failed at IP-address=" IP-address SC SP "port-number=" port SC
NTP(12)	warning(4)	time_conn_failed	"SNTP connection failed at IP-address=" IP-address SC SP "port-number=" port SC SP "reason=" reason SC

Spectrum management

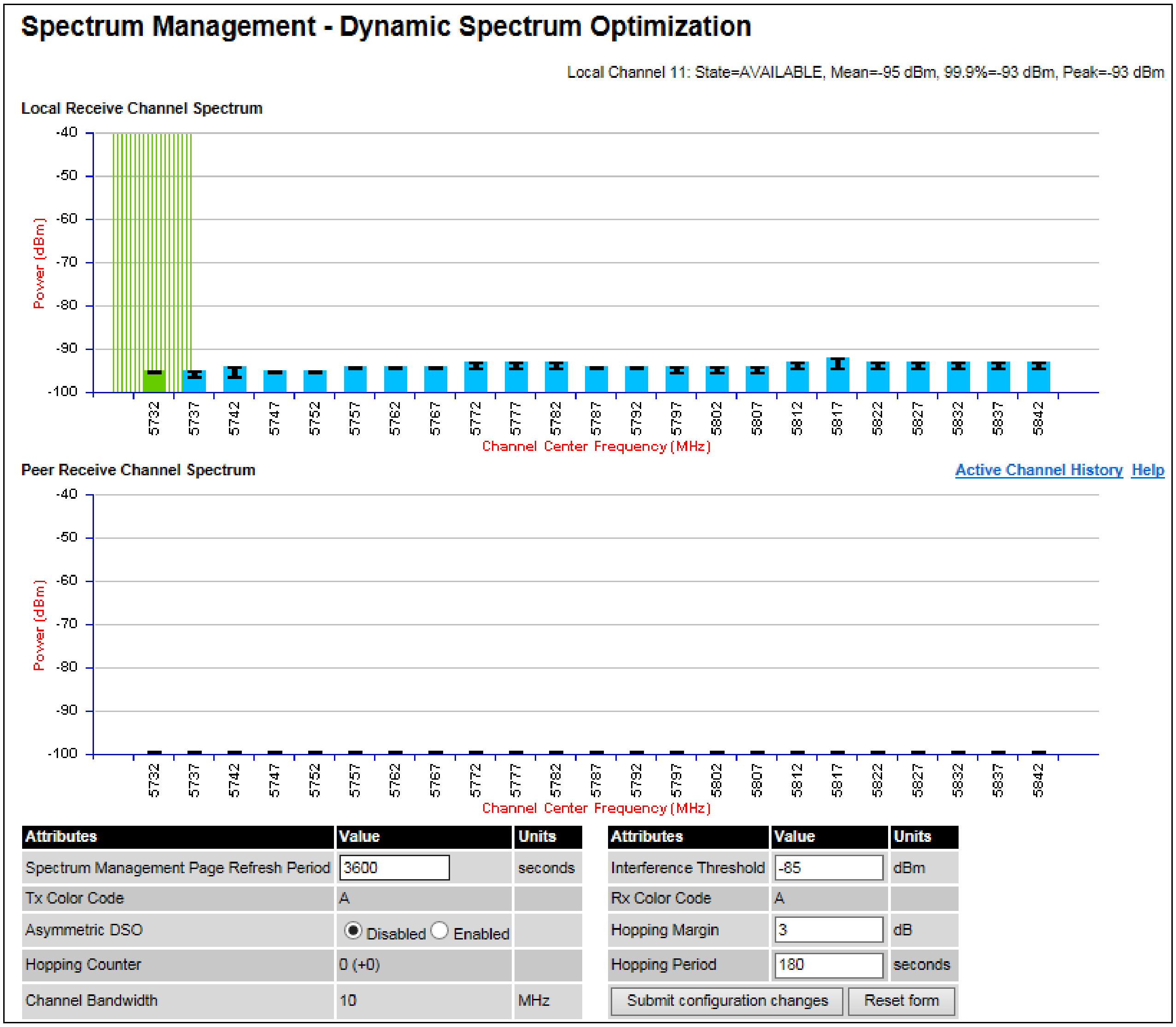
This section describes how to use the spectrum management pages to monitor the radio spectrum usage of the PTP 650 link.

Spectrum Management page

Menu option: **System > Spectrum Management** (Figure 115 and Figure 116).

Use this page to view and configure spectrum usage. The width of the vertical green bar represents the channel width (10 MHz illustrated).

Figure 115 Spectrum Management page (master unit)

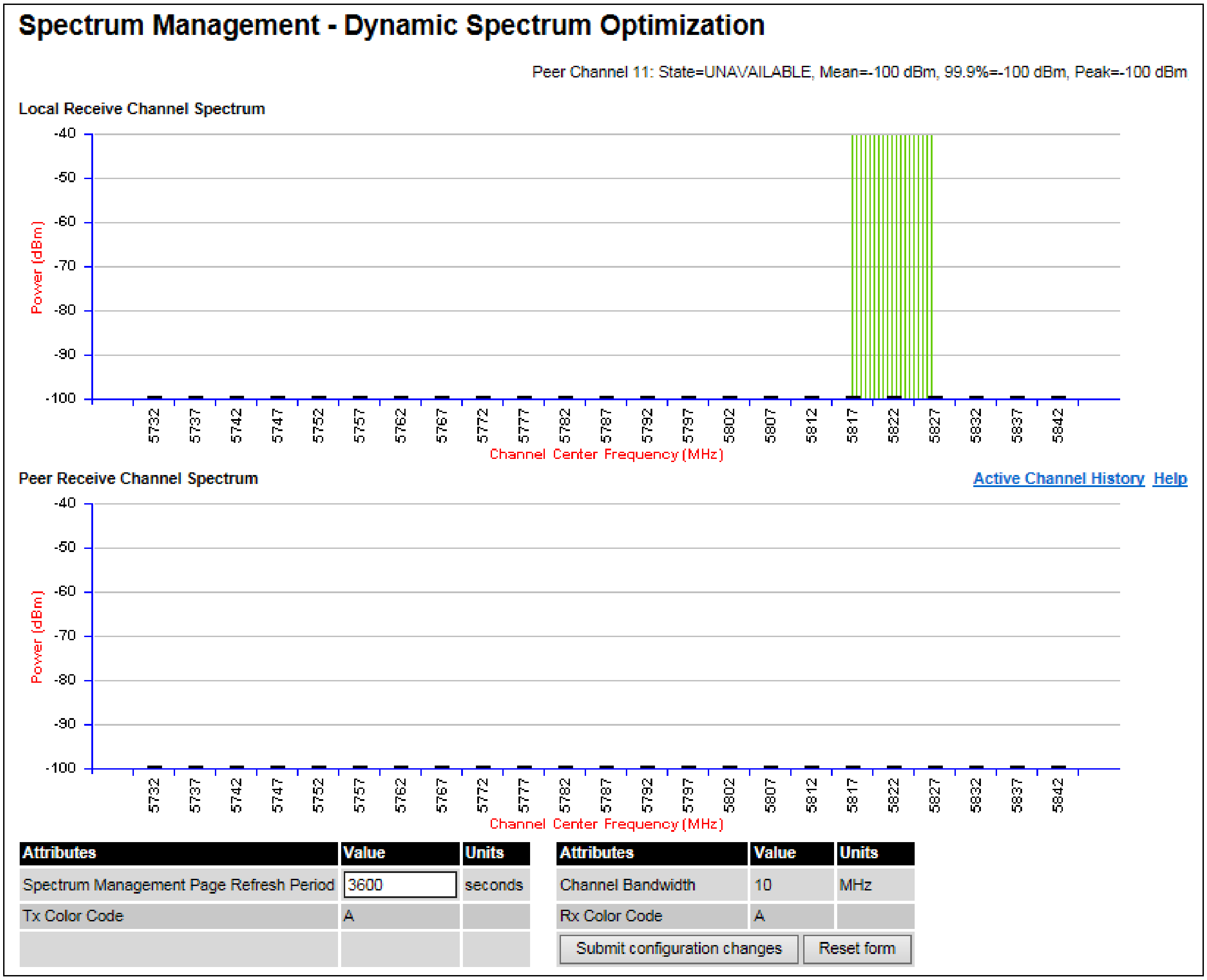


Spectrum Management - Dynamic Spectrum Optimization

Local Channel 11: State=AVAILABLE, Mean=-95 dBm, 99.9%=-93 dBm, Peak=-93 dBm

Attributes	Value	Units	Attributes	Value	Units
Spectrum Management Page Refresh Period	3600	seconds	Interference Threshold	-85	dBm
Tx Color Code	A		Rx Color Code	A	
Asymmetric DSO	● Disabled ○ Enabled		Hopping Margin	3	dB
Hopping Counter	0 (+0)		Hopping Period	180	seconds
Channel Bandwidth	10	MHz			

Figure 116 Spectrum Management page (slave unit)



Spectrum Management - Dynamic Spectrum Optimization

Peer Channel 11: State=UNAVAILABLE, Mean=-100 dBm, 99.9%=-100 dBm, Peak=-100 dBm

Local Receive Channel Spectrum

Peer Receive Channel Spectrum

Attributes	Value	Units
Spectrum Management Page Refresh Period	3600	seconds
Tx Color Code	A	

Attributes	Value	Units
Channel Bandwidth	10	MHz
Rx Color Code	A	

All spectrum management configuration changes are applied at the master ODU only. These changes are then sent from the master to the slave, so that both master and slave keep identical copies of spectrum management configuration. It is therefore possible to swap master and slave roles on an active PTP 650 link without modifying Spectrum Management configuration.

The default channelization can be modified by varying the lower center frequency attribute in the installation wizard, as described in Wireless Configuration page on page 6-15.

Note

Before attempting to improve the performance of the spectrum management algorithm by changing the default configuration, consult the Cambium Point-to-Point distributor or one of the system field support engineers.

Procedure:

- Review the configuration attributes (Table 104)
- Update the attributes as required. At the slave unit, only Page Refresh Period can be updated.
- To save changes, click Submit configuration changes.

Table 104 Spectrum Management attributes

Attribute	Meaning
Page Refresh Period	The page refreshes automatically according to the setting entered here (in seconds).
Hopping Margin	Spectrum Management uses this margin when making a channel hop decision. If the interference level of the target channel is lower than that of the active channel by at least the Hopping Margin, the link will hop to the target channel. The default setting is 3 dB in non-radar regions, or 10 dB in radar regions.
Asymmetric DSO	Only displayed in non-radar regions when DSO is enabled. The default configuration of symmetric operation constrains the link to operate symmetrically, using the same transmit and receive channels. When in symmetric mode the slave unit will always follow the master. If the master moves to a new channel the slave will hop to the same channel. When the Point-to-Point link is configured as an asymmetric link both the master and slave are free to select the best channel from their own set of local interference metrics.
Spectrum Management Control	Only displayed in radar regions. The options are **DFS** and **DFS with DSO**.
Hopping Period (not configurable)	The Spectrum Management algorithm evaluates the metrics every "Hopping Period" seconds (180 seconds by default) looking for a channel with lower levels of interference. If a better channel is located, Spectrum Management performs an automated channel hop. If SNMP or SMTP alerts are enabled an SNMP TRAP or an email alert is sent warning the system administrator of the channel change.
Hopping Counter	This is used to record the number of channel hops. The number in the (+) brackets indicates the number of channel changes since the last screen refresh.

Attribute	Meaning
Interference Threshold	Spectrum Management uses the interference threshold to perform instantaneous channel hops. If the measured interference on a channel exceeds the specified threshold, then DSO will instruct the wireless to immediately move to a better channel. If a better channel cannot be found the PTP 650 Series will continue to use the current active channel. (Default –85 dBm).
Channel Bandwidth (not configurable)	This shows the value of the variable channel bandwidth selected.

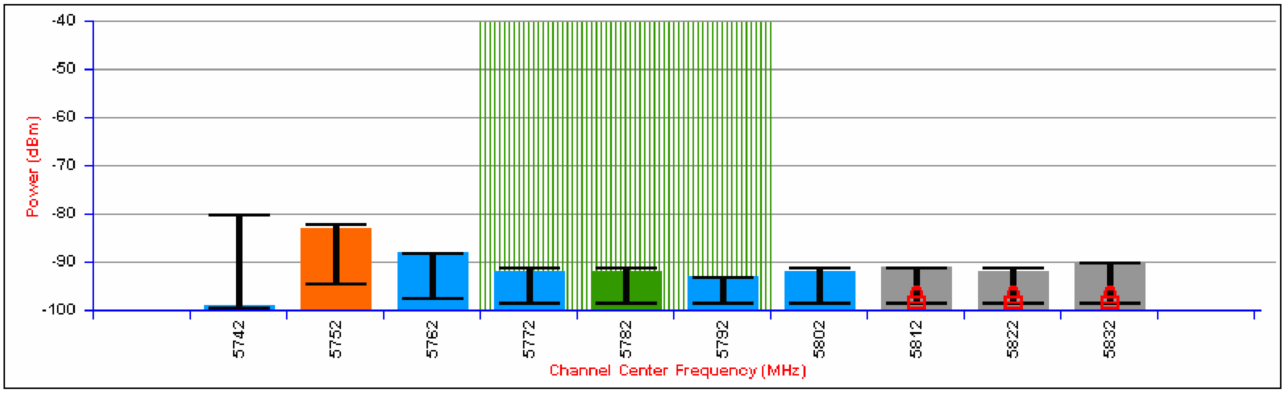
Interpreting the spectrum management plots

The Spectrum Management pages at the master and slave (Figure 115 and Figure 116) display two graphical plots:

- Local Receive Channel Spectrum
- Peer Receive Channel Spectrum

A more detailed example of one of these plots is shown in Figure 117.

Figure 117 Example spectrum management plot



Note

For more information, select the **Help** hyperlink from the Spectrum Management page.

X axis and Y axis

The X-axis shows a stylized view of the selectable wireless channels. Adjacent channels on the display have a 10 MHz overlap. Channels are displayed separately for clarity. The axis is labeled using the channel center frequencies in MHz.

The Y-axis shows the interference power levels from –100 to –40 dBm.

Channel states

The active channel (channel 5 in Figure 117) is always marked using hatched green and white lines. The width of the hatching is directly proportional the channel bandwidth spectral occupancy of the channel.

The individual channel metrics are displayed using a colored bar and an "I" bar. The colored bar represents the channel state (Table 105).

Table 105 Channel states represented in the spectrum management plot

Color	State	Meaning
Green	Active	The channel is currently in use, hosting the Point-to-Point wireless link.
Orange	Interference	The channel has interference above the interference threshold.
Blue	Available	The channel has an interference level below the interference threshold and is considered by the Spectrum Management algorithm suitable for hosting the Point-to-Point link.
Grey	Barred	The system administrator has barred this channel from use. For improved visibility, an additional red "lock" symbol is used to indicate that a channel is barred.

Key metrics

The "I" bar and top of the colored bar represent three key metrics (Table 106). The vertical part of the "I" bar represents the statistical spread between the peak and the mean of the statistical distribution.

Table 106 Key metrics represented in the spectrum management plot

Metric	Description	How represented
Peak of Means	The largest mean interference measurement encountered during the quantization period. The peak of means is useful for detecting slightly longer duration spikes in the interference environment.	Upper horizontal bar.
Mean of Means	The arithmetic mean of the measured means during a quantization period. The mean of means is a coarse measure of signal interference and gives an indication of the average interference level measured during the quantization period. The metric is not very good at predicting intermittent interference and is included to show the spread between the Mean of Means, the 99.9% Percentile and the Peak of Means.	Lower horizontal bar.
99.9% Percentile of the Means	The value of mean interference measurement which 99.9% of all mean measurements fall below, during the quantization period. The 99.9% percentile metric is useful for detecting short duration repetitive interference that by its very nature has a minimal effect of the mean of means.	Top of the colored bar.

Note

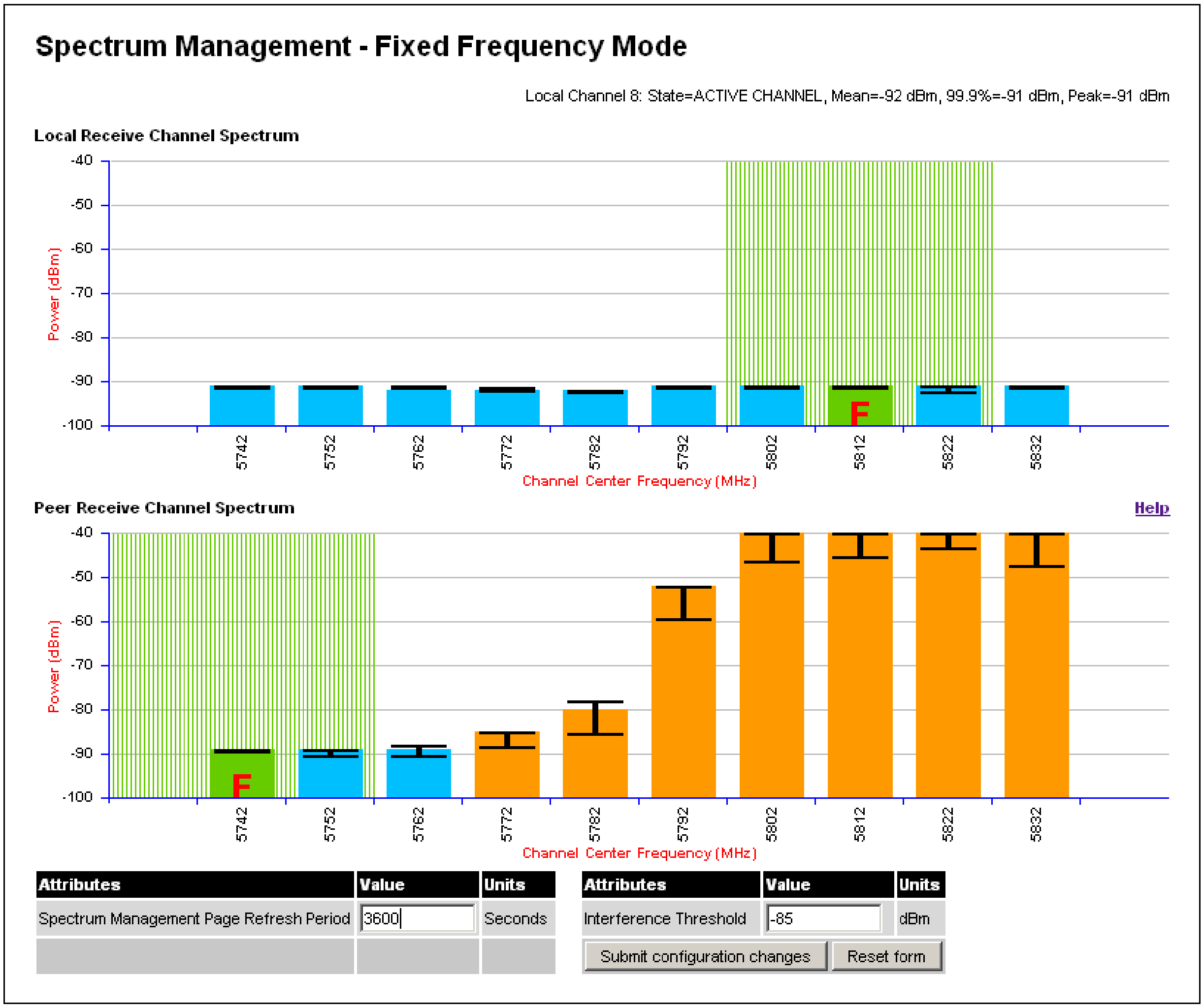
The arithmetic mean is the true power mean and not the mean of the values expressed in dBm.

Spectrum Management uses the 99.9% Percentile as the prime interference measurement. All subsequent references to interference level refer to this percentile measurement.

Spectrum management in fixed frequency mode

When the link is operating in fixed frequency mode, the Spectrum Management page uses two visual cues (Figure 118). The main page title has the "`Fixed Frequency Mode`" suffix and the selected channels are identified by a red capital "F".

Figure 118 Spectrum Management Fixed Frequency Mode page



Spectrum Management - Fixed Frequency Mode

Local Channel 8: State=ACTIVE CHANNEL, Mean=-92 dBm, 99.9%=-91 dBm, Peak=-91 dBm

Attributes	Value	Units
Spectrum Management Page Refresh Period	3600	Seconds

Attributes	Value	Units
Interference Threshold	-85	dBm

Channel barring is disabled in fixed frequency mode; it is not required as dynamic channel hopping is prohibited in this mode.

The only controls available to the master are the Page Refresh Period and Interference Threshold attributes. They will have no effect on the operation of the wireless link and will only effect the generation of the channel spectrum graphics.

The active channel history menu is removed in this mode of operation, as channel hopping is prohibited.

Spectrum management in radar avoidance mode

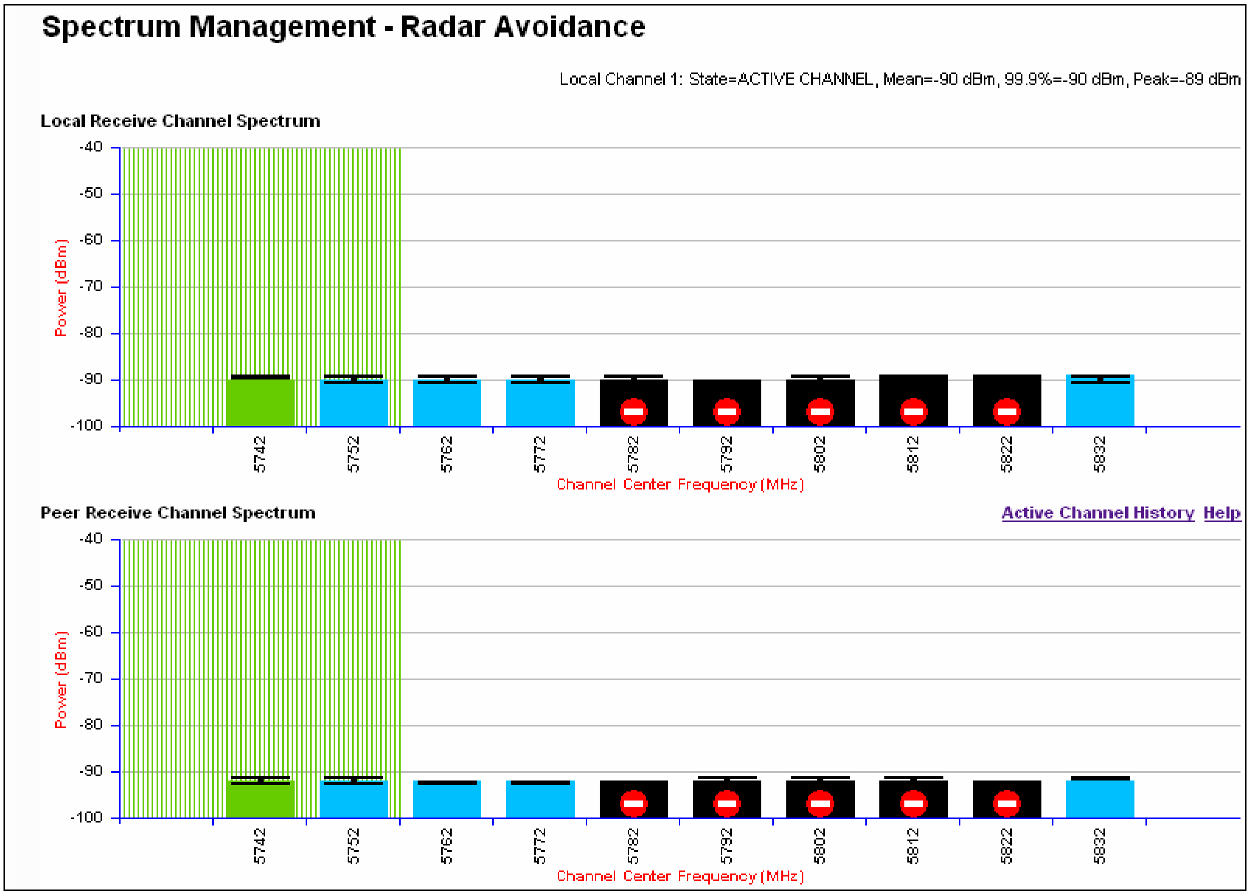
When the link is operating in radar avoidance mode, the Spectrum Management page (Figure 119 and Figure 120) contains the following additional information:

- The main page title has the "`Radar Avoidance`" suffix.
- The only controls available to the master are the Interference Threshold attribute. This has no effect on the operation of the wireless link and will only affect the generation of the channel spectrum graphics.
- Extra color coding of the interference histogram is provided (Table 107).

When operating with RTTT (Road transport and Traffic Telematics) Avoidance enabled or other regulatory restrictions on channel usage, the page contains the following additional information:

- All channels marked with a "no entry" symbol with their associated statistics colored black are the prohibited channels. These channels are never used to host the wireless link, but CAC measurements are still taken so that adjacent channel biases can be calculated correctly and so the user can see if other equipment is in use.

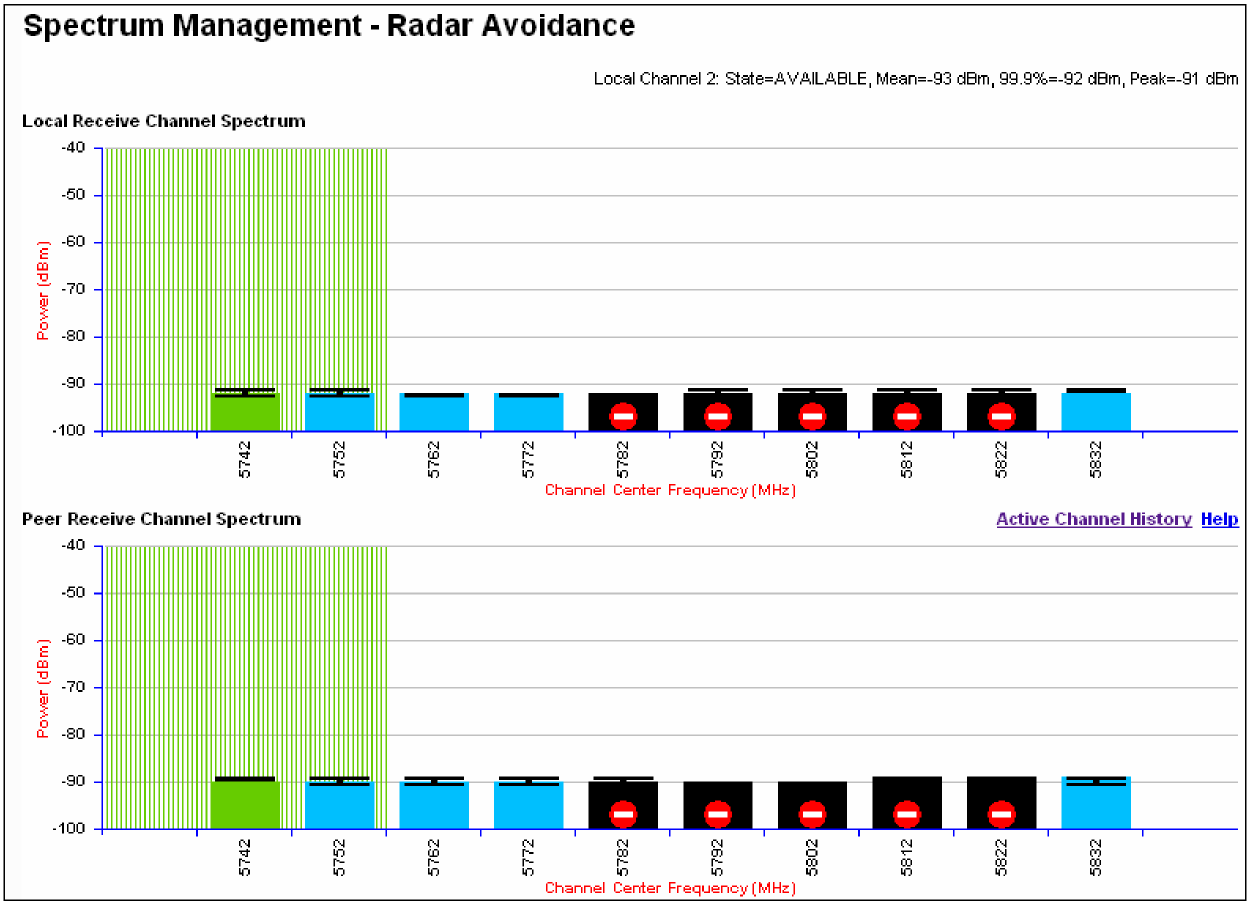
Figure 119 Spectrum Management page with radar avoidance - master



Spectrum Management - Radar Avoidance

Local Channel 1: State=ACTIVE CHANNEL, Mean=-90 dBm, 99.9%=-90 dBm, Peak=-89 dBm

Figure 120 Spectrum Management page with radar avoidance - slave



Spectrum Management - Radar Avoidance

Local Channel 2: State=AVAILABLE, Mean=-93 dBm, 99.9%=-92 dBm, Peak=-91 dBm

Table 107 Channel states in the spectrum management plot (radar avoidance)

Color	State and color	Meaning
Green	Active	This channel is currently in use hosting the Point-to-Point wireless link.
Orange	Interference	This channel has interference above the interference threshold
Blue	Available	This channel has an interference level below the interference threshold and is considered by the Spectrum Management algorithm suitable for hosting the Point-to-Point link
Dark grey	Barred	The system administrator has barred this channel from use. Because the low signal levels encountered when a unit is powered up in a laboratory environment prior to installation (which makes the grey of the channel bar difficult to see). An additional red "lock" symbol is used to indicate that a channel is barred.

Color	State and color	Meaning
Light grey	Unavailable	This channel needs to be monitored for one minute and found free of radar signal before it can be used for transmitting.
Red	Radar Detected	Impulsive Radar Interference has been detected on this channel and the channel is unavailable for 30 minutes. At the end of the 30 minute period a Channel Availability Check is required to demonstrate no radar signals remain on this channel before it can be used for the radio link.
Black	Region Bar	This channel has been barred from use by the local region regulator

Viewing the active channel history

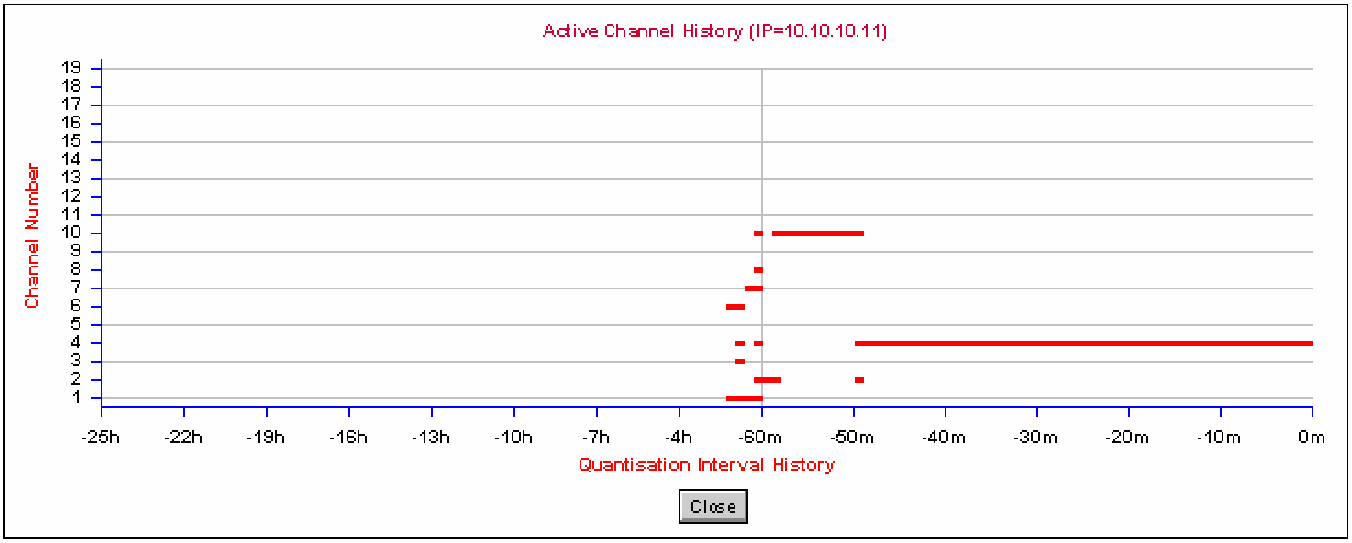
Use this procedure to view the active channel history. This is a time series display of the channels used by the PTP 650 Series over the last 25 hours.

Procedure:

- Select the **Active Channel History** hyperlink from the Spectrum Management page.

An example of the active channel history display is shown in Figure 121. Where there are parallel entries on the display this signifies that the wireless link occupied this channel during the measurement period. The measurement periods are one minute (from zero to sixty minutes) and twenty minutes from (60 minutes to twenty five hours).

Figure 121 Active channel history screen



Viewing historic spectrum management metrics

Use this procedure to view the results of previous measurement quantization periods from both the master and slave Spectrum Management pages.

Procedure:

- Hold down the shift key and click the appropriate channel on the Local Receive Channel Separation plot. The time series plot is displayed (Figure 122). This plot displays the results of all previous measurement quantization periods, up to a maximum of 132 periods. The colored lines represent interference measurements (Table 108).

Figure 122 Spectrum management time series plot

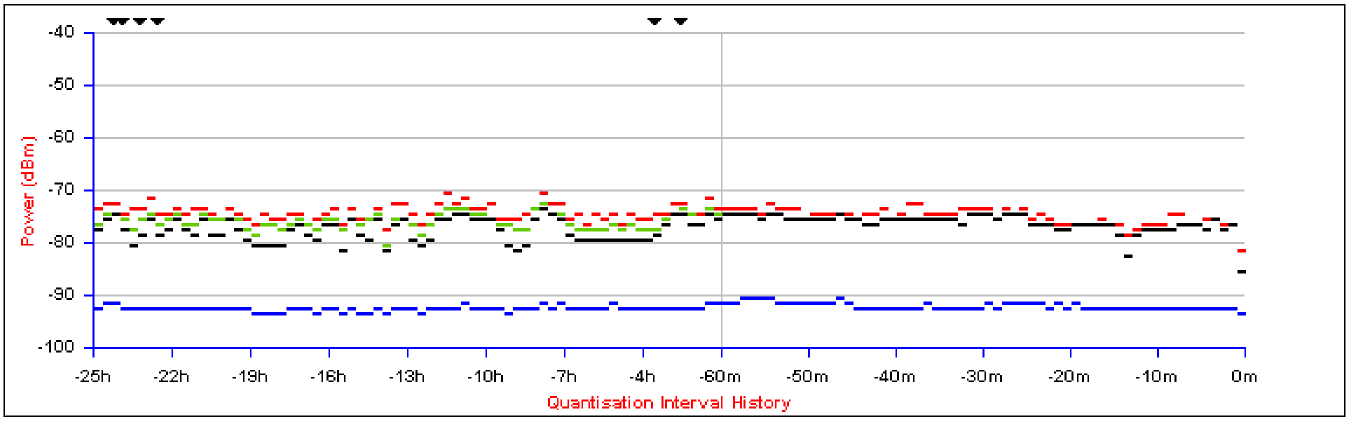


Table 108 Interference represented in the time series plot

Color	Meaning
GREEN	Peak of Means interference measurement
BLACK	99.9% percentile of means interference measurement
BLUE	Mean of Means interference measurement

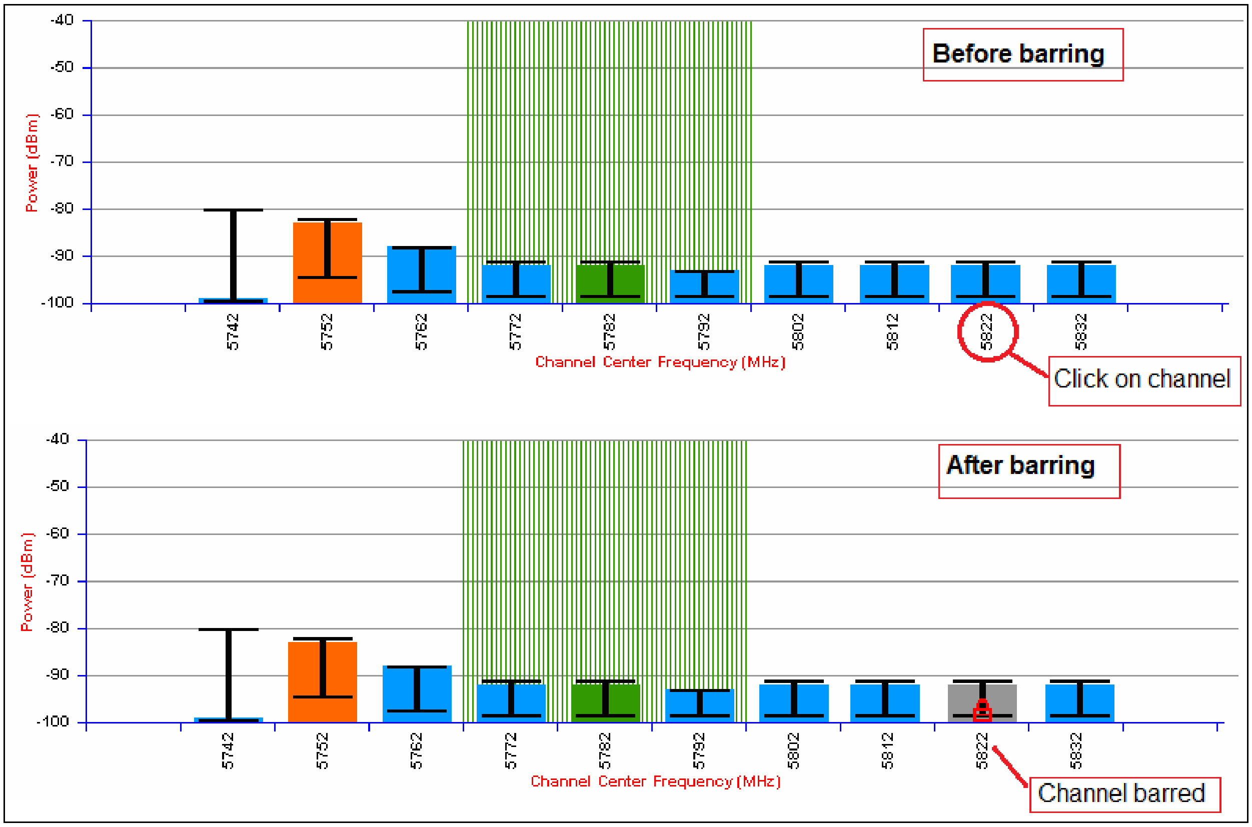
Barring channels

To comply with FCC rules, bar any channels that may interfere with TDWR radars. This must be done before the units are allowed to radiate on site. The system designer will have provided a list of any affected channels, based on the instructions in Avoidance of weather radars (USA only) on page 3-20.

Procedure:

- Log into the master unit.
- Select menu option **System > Spectrum Management**. The Spectrum Management page is displayed.
- Click on the appropriate channel center frequencies on the Local or Peer channel spectrum plots. The example in Figure 123 shows how to bar one channel (5822 MHz).
- When the confirmation dialog is displayed, click **OK**.

Figure 123 Barring a channel



System statistics

This section describes how to use the system statistics pages to manage the performance of the PTP 650 link, use the following web pages:

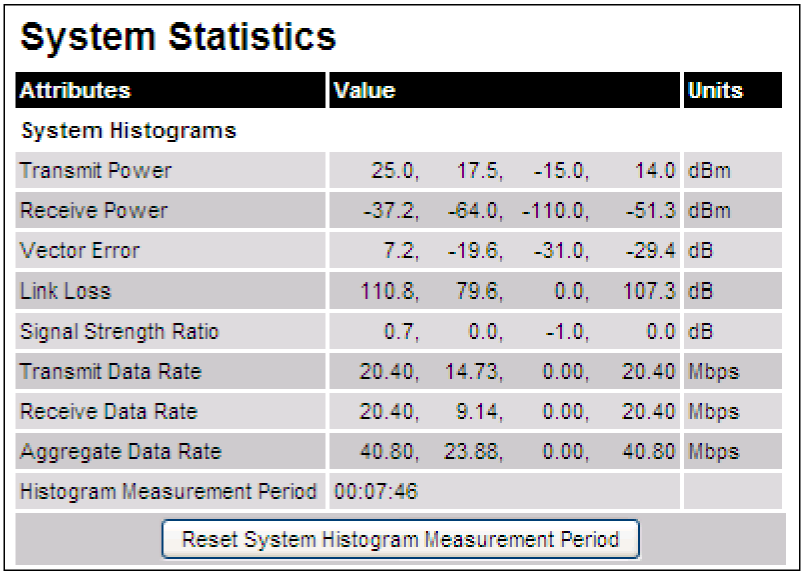
System Statistics page

Menu option: **System > Statistics**. Use this page to check system statistics.

System histograms

The System Histograms section of the System Statistics page (Figure 124) contains eight diagnostic attributes that are presented as arrays of four elements (Table 109).

Figure 124 System Histograms section of the System Statistics page



System Statistics

Attributes	Value	Units
System Histograms		
Transmit Power	25.0, 17.5, -15.0, 14.0	dBm
Receive Power	-37.2, -64.0, -110.0, -51.3	dBm
Vector Error	7.2, -19.6, -31.0, -29.4	dB
Link Loss	110.8, 79.6, 0.0, 107.3	dB
Signal Strength Ratio	0.7, 0.0, -1.0, 0.0	dB
Transmit Data Rate	20.40, 14.73, 0.00, 20.40	Mbps
Receive Data Rate	20.40, 9.14, 0.00, 20.40	Mbps
Aggregate Data Rate	40.80, 23.88, 0.00, 40.80	Mbps
Histogram Measurement Period	00:07:46	

The element arrays represent the following:

- Max: The maximum value measured over the last hour.
- Mean: The mean of a set of values recorded at one second intervals over the last hour.
- Min: The minimum value measured over the last hour.
- Latest: The latest value measured.

The values are calculated over the time that has elapsed since the link was established or since the measurement period was reset.

Note

Use the Diagnostics Plotter page on page 7-42 to plot these attributes against time. Use the Generate Downloadable Diagnostics page on page 7-43 to extract historical data for these attributes to a CSV file.

Procedure:

- To reset and restart measurement, click **Reset System Histograms and Measurement Period**.

Table 109 System Histogram attributes in the System Statistics page

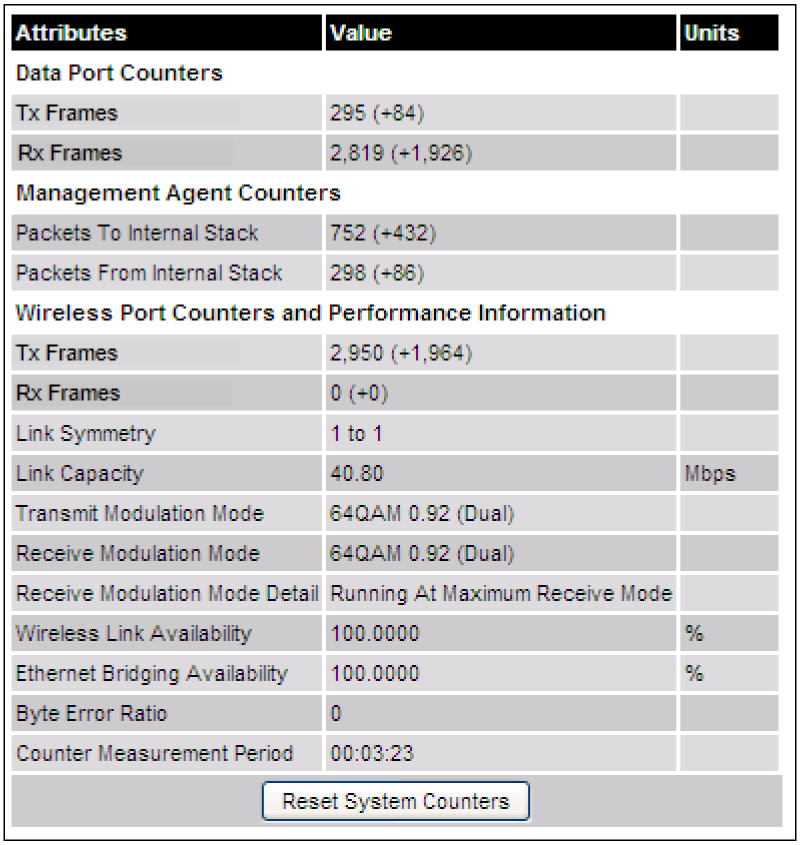
Attribute	Meaning
Transmit Power	The transmit power histogram, calculated over a one hour period.
Receive Power	The receive power histogram, calculated over a one hour period.
Vector Error	The vector error measurement compares (over a one hour period) the received signal IQ modulation characteristics to an ideal signal to determine the composite vector error magnitude.
Link Loss	Link loss calculated (over a one hour period) as follows: Peer_Tx_Power (dBm) – Local_Rx_Power (dBm) + 2 x Antenna_Pattern (dBi)
Signal Strength Ratio	The Signal Strength Ratio (calculated over a one hour period) is: Power received by the vertical antenna input (dB) ÷ Power received by the horizontal antenna input (dB) This ratio is presented as: max, mean, min, and latest. The max, min and latest are true instantaneous measurements; the mean is the mean of a set of one second means. Signal Strength Ratio is an aid to debugging a link. If it has a large positive or negative value then investigate the following potential problems: • An antenna coaxial lead may be disconnected. • When spatial diversity is employed, the antenna with the lower value may be pointing in the wrong direction. • When a dual polar antenna is deployed, the antenna may be directed using a side lobe rather than the main lobe. When there is a reflection from water on the link and spatial diversity is employed, then one expects large, slow swings in Signal Strength Ratio . This indicates the antenna system is doing exactly as intended.

Attribute	Meaning
Transmit, Receive and Aggregate Data Rates	The data rates in the transmit direction, the receive direction and in both directions, expressed in Mbps (max, mean, min, and latest). The max, min and latest are true instantaneous measurements. The mean is the mean of a set of one second means.
Histogram Measurement Period	The time over which the system histograms were collected.

System counters

The System Counters section of the System Statistics page (Figure 125) contains Data Port Counters (Table 110), Management Agent Counters (Table 111) and Wireless Port Counters and Performance Information (Table 112).

Figure 125 System Counters section of the System Statistics page



Attributes	Value	Units
Data Port Counters		
Tx Frames	295 (+84)	
Rx Frames	2,819 (+1,926)	
Management Agent Counters		
Packets To Internal Stack	752 (+432)	
Packets From Internal Stack	298 (+86)	
Wireless Port Counters and Performance Information		
Tx Frames	2,950 (+1,964)	
Rx Frames	0 (+0)	
Link Symmetry	1 to 1	
Link Capacity	40.80	Mbps
Transmit Modulation Mode	64QAM 0.92 (Dual)	
Receive Modulation Mode	64QAM 0.92 (Dual)	
Receive Modulation Mode Detail	Running At Maximum Receive Mode	
Wireless Link Availability	100.0000	%
Ethernet Bridging Availability	100.0000	%
Byte Error Ratio	0	
Counter Measurement Period	00:03:23	

Procedure:

- To reset all system counters to zero, click **Reset System Counters**.

The packet counter attributes each contain a number in parentheses; this shows the number of packets received since the last page refresh.

Table 110 Data Port Counters

Attribute	Meaning
Tx Frames	The total number of good frames the bridge has sent for transmission by the local Ethernet interface.
Rx Frames	The total number of good frames the bridge has received from transmission by the remote Ethernet interface.

Table 111 Management Agent Counters

Attribute	Meaning
Packets To Internal Stack	The total number of good packets the bridge has transmitted to the internal stack (for example, ARP, PING and HTTP requests).
Packets From Internal Stack	The total number of good packets the bridge has received from the internal stack (ARP responses, PING replies, HTTP responses).

Table 112 Wireless Port Counters and Performance Information

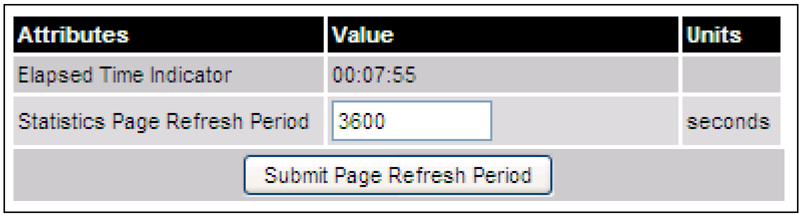
Attribute	Meaning
Tx Frames	Total number of good frames the bridge has sent for transmission by the wireless interface.
Rx Frames	Total number of good frames the bridge has received from the wireless interface.
Link Symmetry	Ratio between transmit and receive time in the TDD frame. The first number is the time allowed for the transmit direction and the second number is the time allowed for the receive direction.
Link Capacity	The maximum aggregate data capacity available for user traffic under the current radio link conditions, assuming the units have been connected using Gigabit Ethernet. The sum of the displayed Transmit and Receive data rates may be lower than this figure if the link is not fully loaded by the current traffic profile.
Transmit Modulation Mode	The modulation mode currently being used on the transmit channel. The number in brackets after the modulation mode and coding rate string is the effective data rate available to all MAC layer protocols.

Attribute	Meaning
Receive Modulation Mode	The modulation mode currently being used on the receive channel. The number in brackets after the modulation mode and coding rate string is the effective data rate available to all MAC layer protocols.
Receive Modulation Mode Detail	The receive modulation mode in use. For a list of values and their meanings, see Table 100.
Wireless Link Availability	Wireless link availability calculated since the last system counters reset.
Ethernet Bridging Availability	Link availability for bridging Ethernet traffic calculated since the last reset of the system counters. This is the percentage of time in which the Ethernet Bridging Status attribute has been set to "`Enabled`".
Byte Error Ratio	The ratio of detected Byte errors to the total number of bytes since the last system reboot. This measurement is made continually using null frames when there is no user data to transport.
Counter Measurement Period	The time over which the system counters were collected.

Other attributes

The bottom section of the System Statistics page (Figure 126) contains two attributes (Table 113).

Figure 126 Other attributes section of the System Statistics page



Attributes	Value	Units
Elapsed Time Indicator	00:07:55	
Statistics Page Refresh Period	3600	seconds

Procedure:

- After updating the Statistics Page Refresh Period field, click **Submit Page Refresh Period**.

Table 113 Other attributes in the System Statistics page

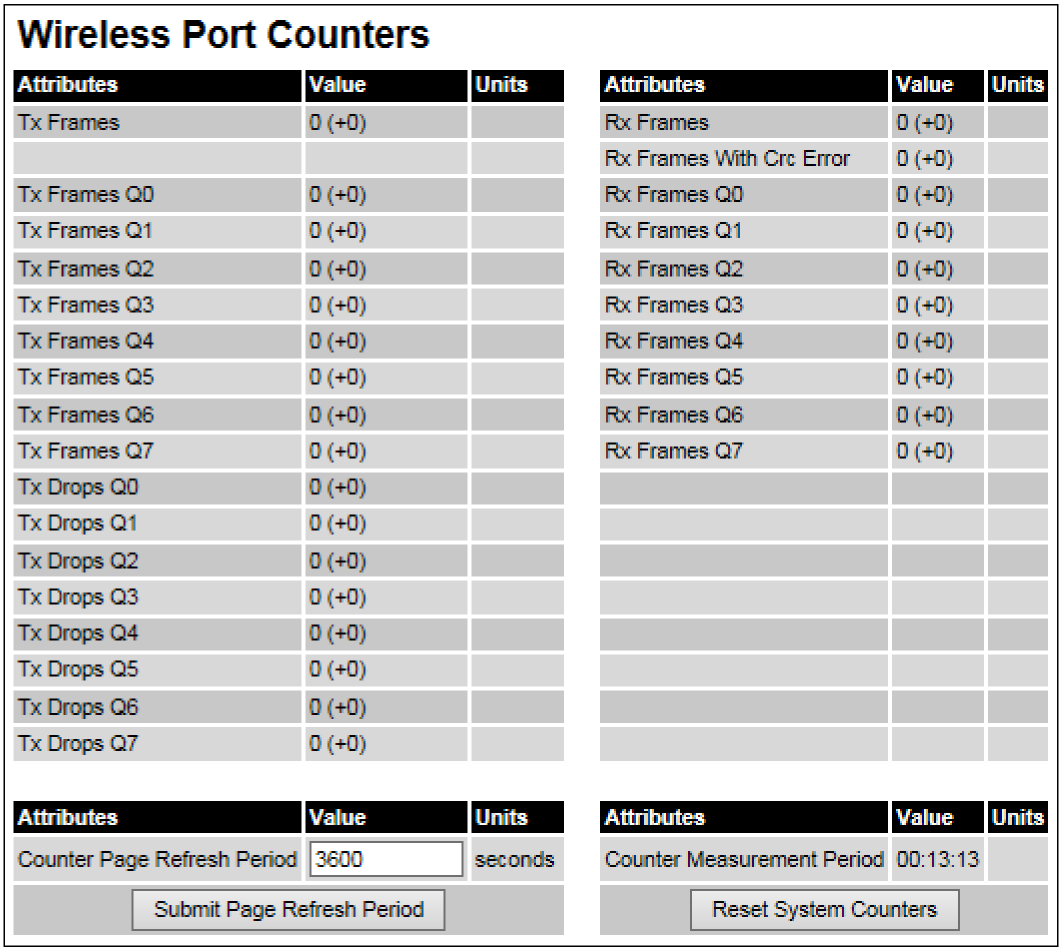
Attribute	Meaning
Elapsed Time Indicator	Elapsed time since the last system reboot.
Statistics Page Refresh Period	The statistics page refreshes automatically according to the setting entered here (in seconds).

Wireless Port Counters page

Menu option: **System > Statistics > Wireless Port Counters** (Figure 127).

Use this page to check the Ethernet performance of the wireless bridge.

Figure 127 Wireless Port Counters page



Wireless Port Counters

Attributes	Value	Units	Attributes	Value	Units
Tx Frames	0 (+0)		Rx Frames	0 (+0)	
			Rx Frames With Crc Error	0 (+0)	
Tx Frames Q0	0 (+0)		Rx Frames Q0	0 (+0)	
Tx Frames Q1	0 (+0)		Rx Frames Q1	0 (+0)	
Tx Frames Q2	0 (+0)		Rx Frames Q2	0 (+0)	
Tx Frames Q3	0 (+0)		Rx Frames Q3	0 (+0)	
Tx Frames Q4	0 (+0)		Rx Frames Q4	0 (+0)	
Tx Frames Q5	0 (+0)		Rx Frames Q5	0 (+0)	
Tx Frames Q6	0 (+0)		Rx Frames Q6	0 (+0)	
Tx Frames Q7	0 (+0)		Rx Frames Q7	0 (+0)	
Tx Drops Q0	0 (+0)				
Tx Drops Q1	0 (+0)				
Tx Drops Q2	0 (+0)				
Tx Drops Q3	0 (+0)				
Tx Drops Q4	0 (+0)				
Tx Drops Q5	0 (+0)				
Tx Drops Q6	0 (+0)				
Tx Drops Q7	0 (+0)				

Attributes	Value	Units	Attributes	Value	Units
Counter Page Refresh Period	3600	seconds	Counter Measurement Period	00:13:13	

Procedure:

- Review the attributes (Table 114).
- To change the refresh period, update the Counter Page Refresh Period attribute and click **Submit Page Refresh Period**.
- To reset all counters to zero, click **Reset System Counters**.

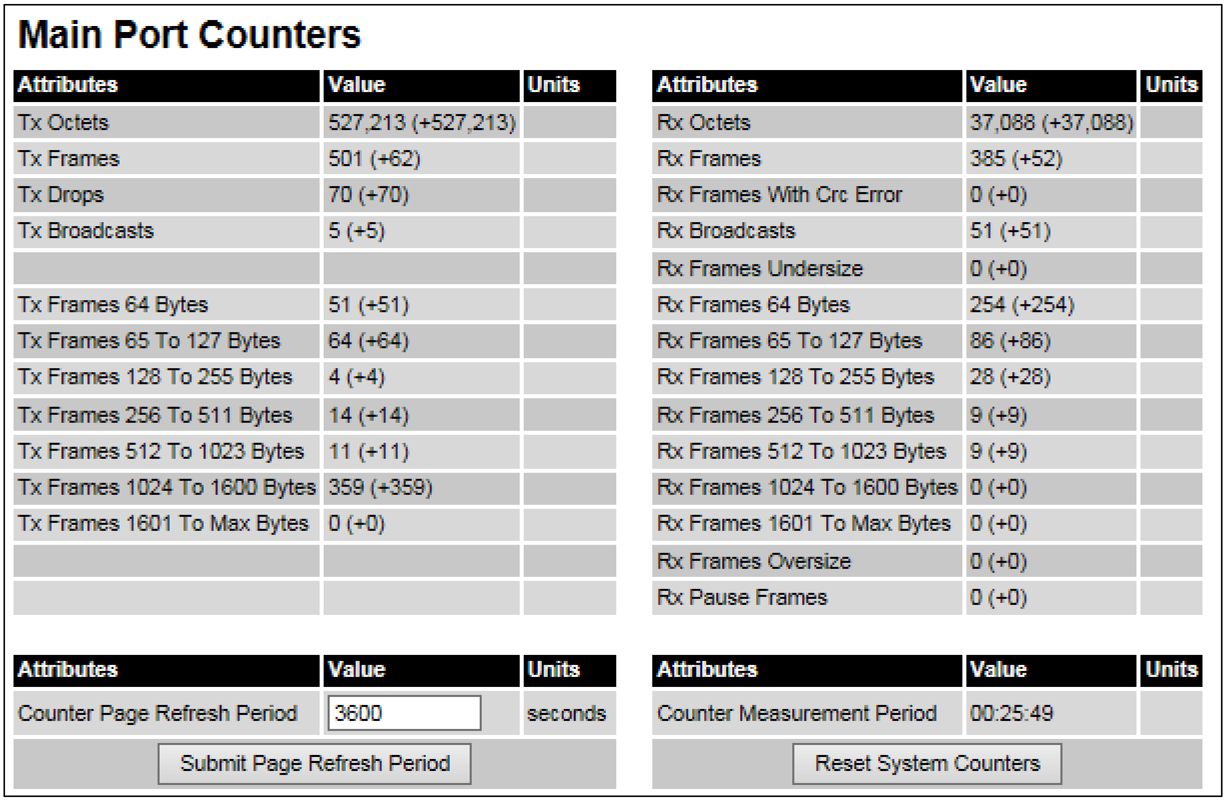
Table 114 Wireless Port Counters attributes

Attribute	Meaning
Tx/Rx Frames	Number of frames transmitted and received over the wireless bridge.
Rx Frames With Crc Error	Number of received frames with CRC errors.
Tx/Rx Frames Q0…Q7	Number of transmitted and received frames for each Traffic Class.
Tx Drops Q0…Q7	Number of transmitted frames dropped for each Traffic Class.
Rx Drops Q0…Q7	Total number of frames dropped due to the lack of sufficient capacity in the receive buffer, for each Traffic Class.

Main Port Counters page

Menu option: **System > Statistics > Main Port Counters** (Figure 128). Use this page to check the Ethernet performance of the PSU port. The displayed counters vary depending on which port is being used to bridge the traffic.

Figure 128 Main Port Counters page (when main port is bridging traffic)



Main Port Counters

Attributes	Value	Units
Tx Octets	527,213 (+527,213)	
Tx Frames	501 (+62)	
Tx Drops	70 (+70)	
Tx Broadcasts	5 (+5)	
Tx Frames 64 Bytes	51 (+51)	
Tx Frames 65 To 127 Bytes	64 (+64)	
Tx Frames 128 To 255 Bytes	4 (+4)	
Tx Frames 256 To 511 Bytes	14 (+14)	
Tx Frames 512 To 1023 Bytes	11 (+11)	
Tx Frames 1024 To 1600 Bytes	359 (+359)	
Tx Frames 1601 To Max Bytes	0 (+0)	

Attributes	Value	Units
Rx Octets	37,088 (+37,088)	
Rx Frames	385 (+52)	
Rx Frames With Crc Error	0 (+0)	
Rx Broadcasts	51 (+51)	
Rx Frames Undersize	0 (+0)	
Rx Frames 64 Bytes	254 (+254)	
Rx Frames 65 To 127 Bytes	86 (+86)	
Rx Frames 128 To 255 Bytes	28 (+28)	
Rx Frames 256 To 511 Bytes	9 (+9)	
Rx Frames 512 To 1023 Bytes	9 (+9)	
Rx Frames 1024 To 1600 Bytes	0 (+0)	
Rx Frames 1601 To Max Bytes	0 (+0)	
Rx Frames Oversize	0 (+0)	
Rx Pause Frames	0 (+0)	

Attributes	Value	Units
Counter Page Refresh Period	3600	seconds

Attributes	Value	Units
Counter Measurement Period	00:25:49	

Procedure:

- Review the attributes (Table 115).
- To change the refresh period, update the Counter Page Refresh Period attribute and click **Submit Page Refresh Period**.
- To reset all counters to zero, click **Reset System Counters**.

Table 115 Main Port Counters attributes

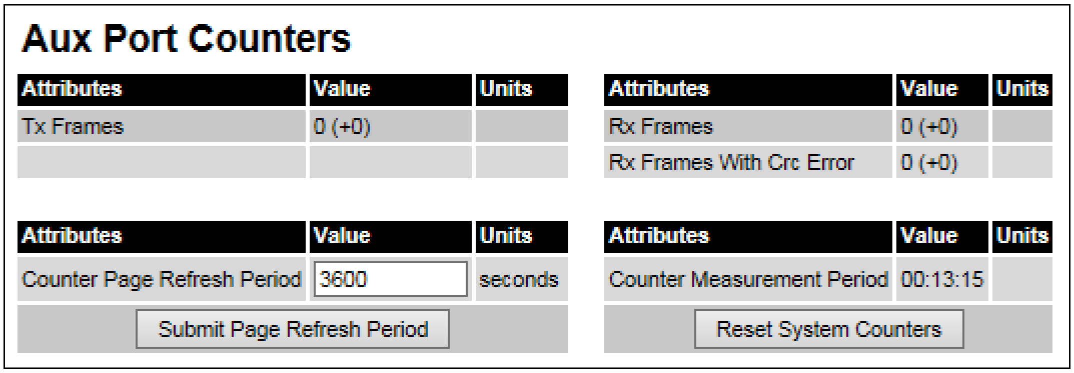
Attribute	Meaning
Tx/Rx Octets	Total number of octets (bytes) transmitted and received over the interface.
Tx/Rx Frames	Total number of frames transmitted and received over the interface. This includes both good and bad frames.
Tx Drops	Total number of transmit frames dropped.
Rx Frames With Crc Error	Total number of received frames with CRC errors.
Tx/Rx Broadcasts	Total number of good transmitted and received broadcast packets.
Rx Frames Undersize	Total number of frames received that are less than 64 bytes.
Tx/Rx Frames 64 Bytes	Total number 64 byte frames transmitted and received.
Tx/Rx Frames xxxx to yyyy Bytes	Total number of frames transmitted and received in the size range xxxx to yyyy bytes.
Tx/Rx Frames 1601 to Max bytes	Total number of frames transmitted and received in the size range 1601 to maximum bytes.
Rx Frames Oversize	Total number of frames received that are greater than the maximum number of bytes.
Rx Pause Frames	Total number of received pause frames.

Aux Port Counters page

Menu option: System > Statistics > **Aux Port Counters** (Figure 129).

Use this page to check the Ethernet performance of the Aux port.

Figure 129 Aux Port Counters page (when Aux port is out-of-band local)



Aux Port Counters

Attributes	Value	Units
Tx Frames	0 (+0)	

Attributes	Value	Units
Rx Frames	0 (+0)	
Rx Frames With Crc Error	0 (+0)	

Attributes	Value	Units
Counter Page Refresh Period	3600	seconds

Attributes	Value	Units
Counter Measurement Period	00:13:15	

Procedure:

- Review the attributes (Table 116).
- To change the refresh period, update the Counter Page Refresh Period attribute and click **Submit Page Refresh Period.**
- To reset all counters to zero, click **Reset System Counters**.

Table 116 Aux Port Counters attributes

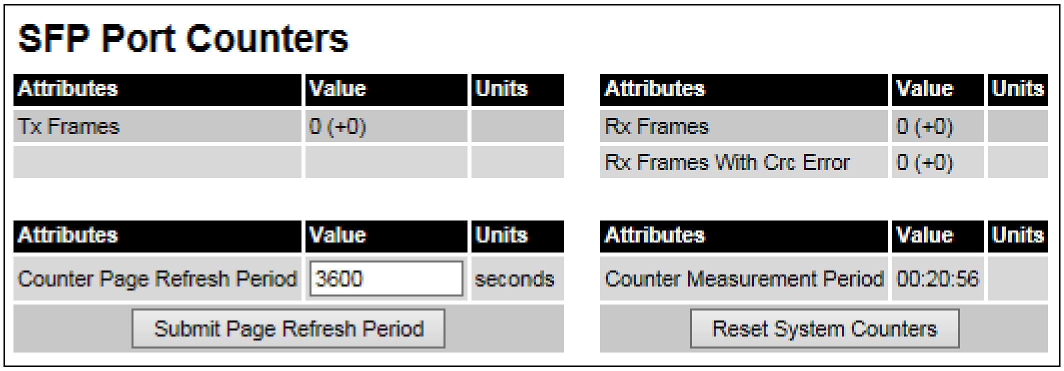
Attribute	Meaning
Tx/Rx Frames	Total number of frames transmitted and received over the interface. This includes both good and bad frames.
Rx Frames With Crc Error	Total number of received frames with CRC errors.

SFP Port Counters page

Menu option: System > Statistics > **SFP Port Counters** (Figure 130).

Use this page to check the Ethernet performance of the SFP port.

Figure 130 SFP Port Counters page (when SFP port is out-of-band local)



SFP Port Counters

Attributes	Value	Units
Tx Frames	0 (+0)	

Attributes	Value	Units
Rx Frames	0 (+0)	
Rx Frames With Crc Error	0 (+0)	

Attributes	Value	Units
Counter Page Refresh Period	3600	seconds

Attributes	Value	Units
Counter Measurement Period	00:20:56	

Procedure:

- Update the attributes (Table 117).
- To change the refresh period, update the Counter Page Refresh Period attribute and click **Submit Page Refresh Period**.
- To reset all counters to zero, click **Reset System Counters**.

Table 117 SFP Port Counters attributes

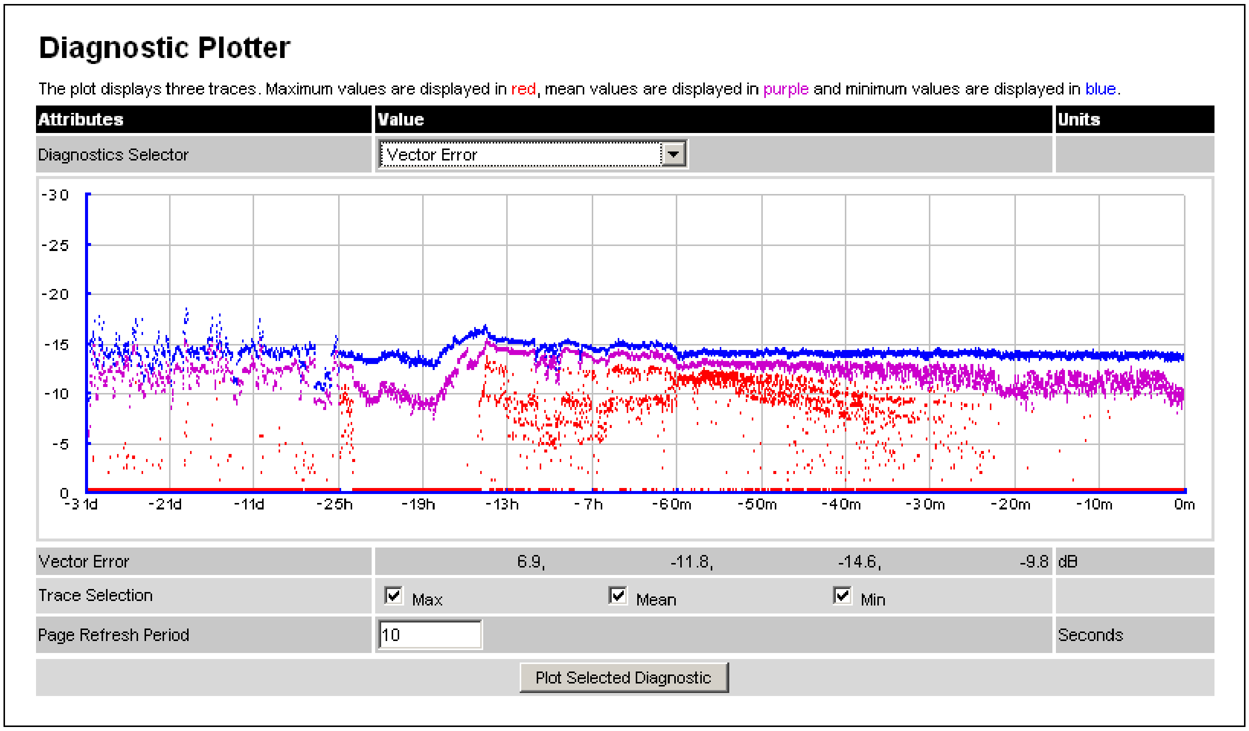
Attribute	Meaning
Tx/Rx Frames	Total number of frames transmitted and received over the interface. This includes both good and bad frames.
Rx Frames With Crc Error	Total number of received frames with CRC errors.

Diagnostics Plotter page

Menu option: **System** > **Diagnostics Plotter** (Figure 131).

Use this page to monitor the performance of an operational PTP 650 link over time.

Figure 131 Diagnostic Plotter page



Diagnostic Plotter

The plot displays three traces. Maximum values are displayed in red, mean values are displayed in purple and minimum values are displayed in blue.

Attributes	Value				Units
Diagnostics Selector	Vector Error ▾				
Vector Error	6.9,	-11.8,	-14.6,	-9.8	dB
Trace Selection	☑ Max	☑ Mean	☑ Min		
Page Refresh Period	10				Seconds

Procedure:

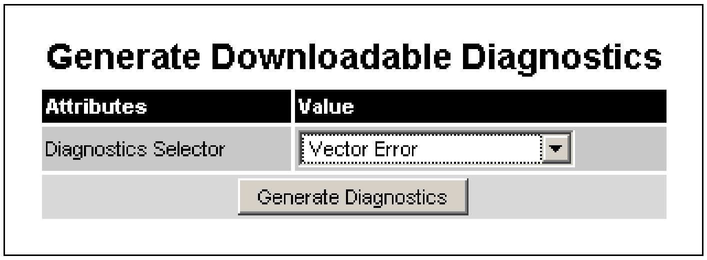
- Select a diagnostic from the Diagnostics Selector drop-down list. These are the same as the System Histogram attributes in the System Statistics page (Table 109).
- Tick the required Trace Selection boxes: Max, Mean and Min.
- Update the Page Refresh Period as required. The default period is 3600 seconds (1 hour). To monitor the performance of a link in real time, select a much shorter period, for example 60 seconds.
- Click **Plot Selected Diagnostic**. The selected diagnostic trace is displayed in the graph. Maximum values are displayed in red, mean values are displayed in purple and minimum values are displayed in blue.

Generate Downloadable Diagnostics page

Menu option: **System > Diagnostics Plotter > CSV Download** (Figure 132).

Use this page to download diagnostics data to a CSV file.

Figure 132 Generate Downloadable Diagnostics page



Generate Downloadable Diagnostics

Attributes	Value
Diagnostics Selector	Vector Error

Procedure:

- Select a diagnostic from the Diagnostics Selector drop-down list.
- Click **Generate Diagnostics**. The Generate Downloadable Diagnostics page is redisplayed with the name of the generated CSV file.
- Click on the CSV file name and save the CSV file to the hard drive of the local computer.
- Open the CSV file in MS Excel and use it to generate reports and diagrams. The CSV file contains at most 5784 entries, recorded over a 32 day period:
  - 3600 entries recorded in the last hour.
  - 1440 entries recorded in the previous 24 hours.
  - 744 entries recorded in the previous 31 days.

Recovery mode

This section describes how to recover a PTP 650 unit from configuration errors or software image corruption.

Entering recovery mode

Use this procedure to enter recovery mode manually.

Note

The unit may enter recovery mode automatically, in response to some failures.

Note

Once the unit has entered recovery, it will switch back to normal operation if no access has been made to the recovery web page within 30 seconds.

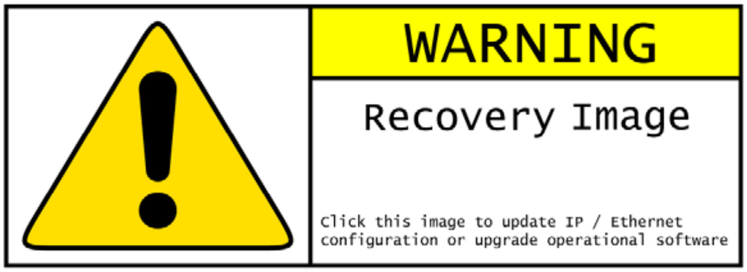
Procedure:

1 Apply power to PSU for at least 10 seconds.

2 Remove power for 5 seconds.

3 Re-apply power to the PSU.

4 When the unit is in recovery mode, access the web interface by entering the default IP address **169.254.1.1**. The Recovery Image Warning page is displayed:



WARNING

Recovery Image

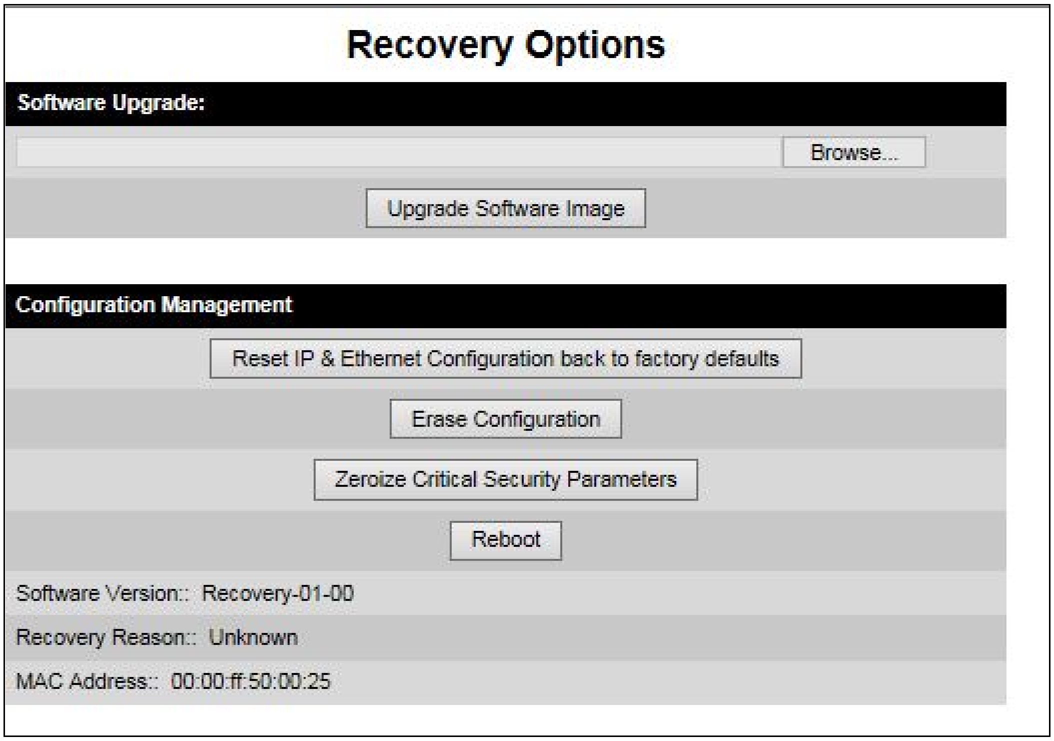
Click this image to update IP / Ethernet configuration or upgrade operational software

5 Click on the warning page image. The Recovery Option Page is displayed (Figure 133).`

6 Review the Software Version and Recovery Reason (Table 118).

7 Select a recovery option (Table 119).

Figure 133 Recovery Options page



Recovery Options

Software Upgrade:

Browse...
Upgrade Software Image

Configuration Management

Reset IP & Ethernet Configuration back to factory defaults
Erase Configuration
Zeroize Critical Security Parameters
Reboot

Software Version:: Recovery-01-00

Recovery Reason:: Unknown

MAC Address:: 00:00:ff:50:00:25

Table 118 Recovery Options attributes

Attribute	Meaning
Software Version	The software version of the recovery operating system permanently installed during manufacture.
Recovery Reason	The reason the unit is operating in Recovery mode, for example "Invalid or corrupt image". "Unknown" usually means there has been a power outage.
MAC Address	The MAC address of the unit programmed during manufacture.

Table 119 Recovery Options buttons

Button	Purpose
Upgrade Software Image	Use this option to restore a working software version when software corruption is suspected, or when an incorrect software image has been loaded. Refer to Upgrading software image on page 7-46.
Reset IP & Ethernet Configuration back to factory defaults	Use this option to restore the IP and Ethernet attributes to their defaults. Refer to Resetting IP & Ethernet configuration on page 7-47.
Erase Configuration	Use this option to erase the entire configuration of the unit. Refer to Erasing configuration on page 7-48.
Zeroize Critical Security Parameters	Use this option to reset encryption keys and the system administrator password. Refer to Zeroize Critical Security Parameters page on page 7-50.
Reboot	Use this option to reboot the unit. Refer to Rebooting the unit on page 7-51.

Upgrading software image

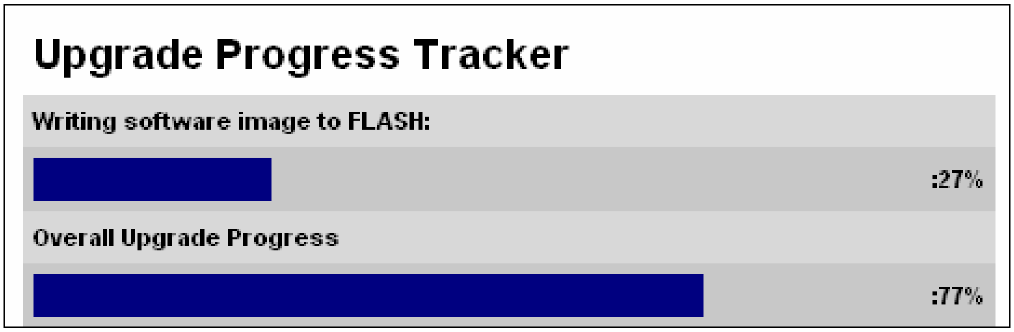
Use this option to restore a working software image from the Recovery Options page (Figure 133).

Procedure:

1 Click **Browse**.

2 Navigate to the required software image. This may be the most recent image if software corruption is suspected, or an older image if an incorrect image has just been loaded. Click on the image and click **Open**.

3 Click **Upgrade Software Image**. The Confirmation page is displayed. Click **Program Software Image into Non-Volatile Memory**. The Upgrade Progress Tracker page is displayed:



Upgrade Progress Tracker

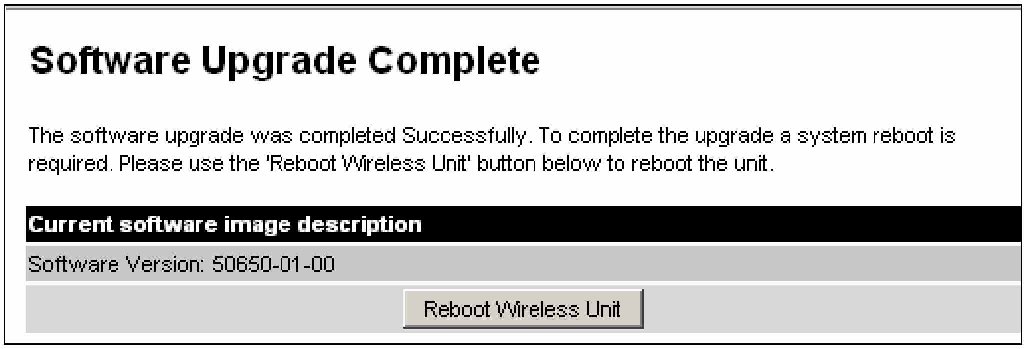
Writing software image to FLASH:

:27%

Overall Upgrade Progress

:77%

4 When the Software Upgrade Complete page is displayed, check that the correct image has been downloaded:



Software Upgrade Complete

The software upgrade was completed Successfully. To complete the upgrade a system reboot is required. Please use the 'Reboot Wireless Unit' button below to reboot the unit.

Current software image description

Software Version: 50650-01-00

5 Click **Reboot Wireless Unit**. When the "`Are you sure?`" message is displayed, click **OK**.

6 The unit will now reboot and restart in normal operational mode, and the link should recover. If the unit or link fails to recover, refer to Testing link end hardware on page 8-2.

Resetting IP & Ethernet configuration

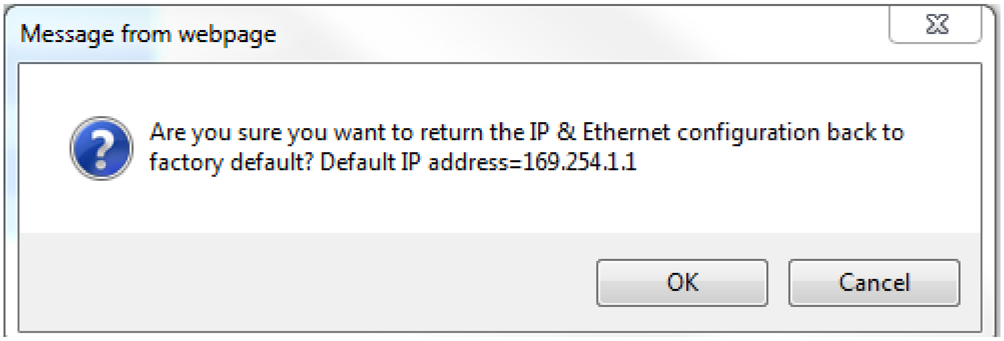
Use this option to reset IPv4, IPv6 and Ethernet configuration back to defaults from the Recovery Options page (Figure 133).

Note

This procedure resets the IP Version attribute to **IPv4**. It also resets the IPv6 configuration.

Procedure:

1 Click **Reset IP & Ethernet Configuration back to factory defaults.** The reset pop up box is displayed:

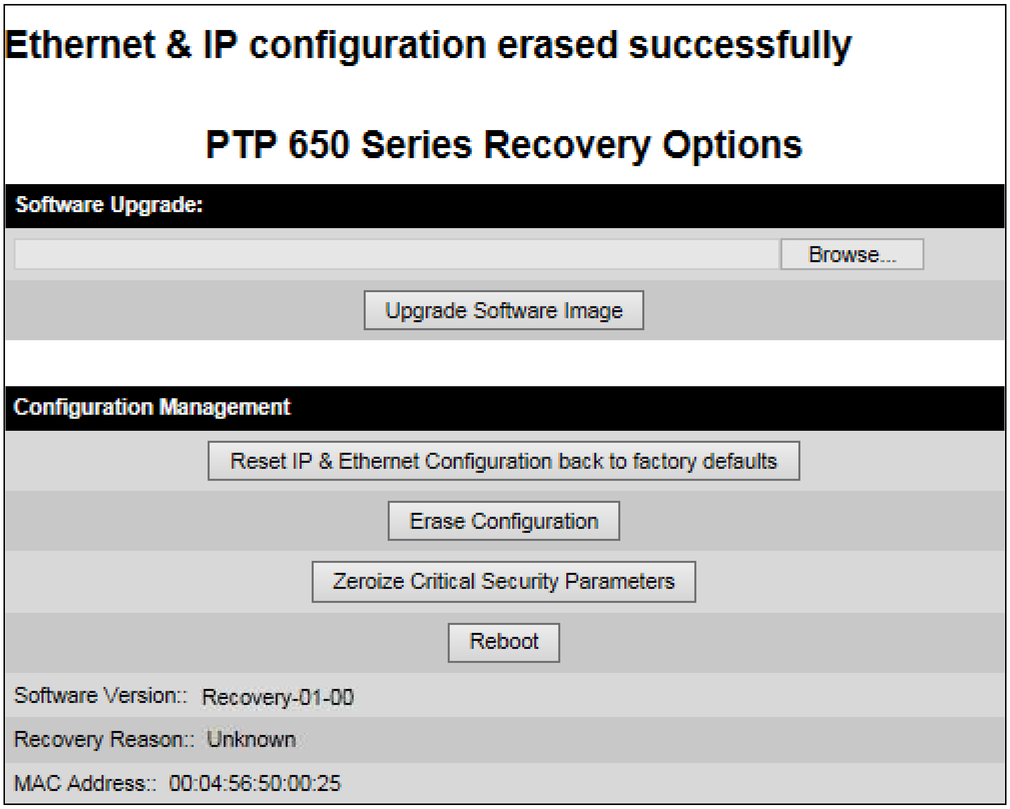


Message from webpage

Are you sure you want to return the IP & Ethernet configuration back to factory default? Default IP address=169.254.1.1

2 Record the IP address, as it will be needed to log into the unit after recovery.

3 Click **OK**. The reset confirmation page is displayed:



Ethernet & IP configuration erased successfully

PTP 650 Series Recovery Options

Software Upgrade:

Software Version:: Recovery-01-00

Recovery Reason:: Unknown

MAC Address:: 00:04:56:50:00:25

Browse...
Upgrade Software Image
Configuration Management
Reset IP & Ethernet Configuration back to factory defaults
Erase Configuration
Zeroize Critical Security Parameters
Reboot

4 Click **Reboot**. When the “`Are you sure you want to REBOOT this unit?`” message is displayed, click **OK**.

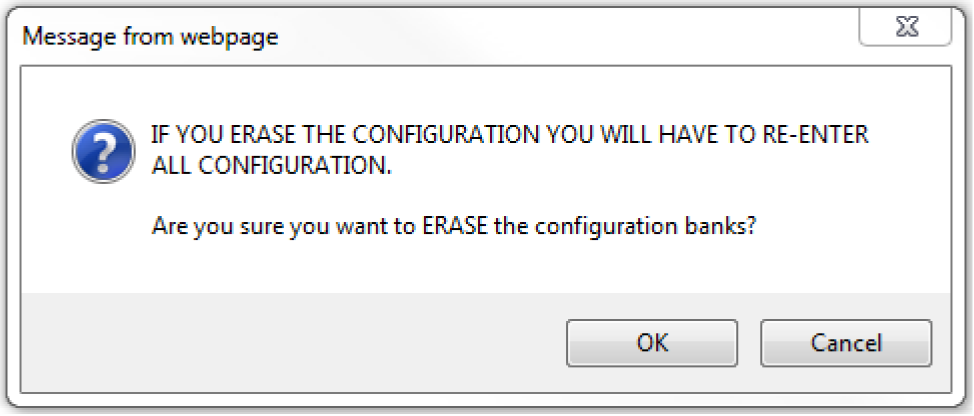
5 The unit will now reboot. The unit should now start up in normal mode but with the IP and Ethernet configuration reset to factory defaults. If the unit fails to recover, refer to Testing link end hardware on page 8-2.

Erasing configuration

Use this option to erase the entire configuration of the unit from the Recovery Options page (Figure 133).

Procedure:

1 Click **Erase Configuration**. The erase pop up box is displayed:

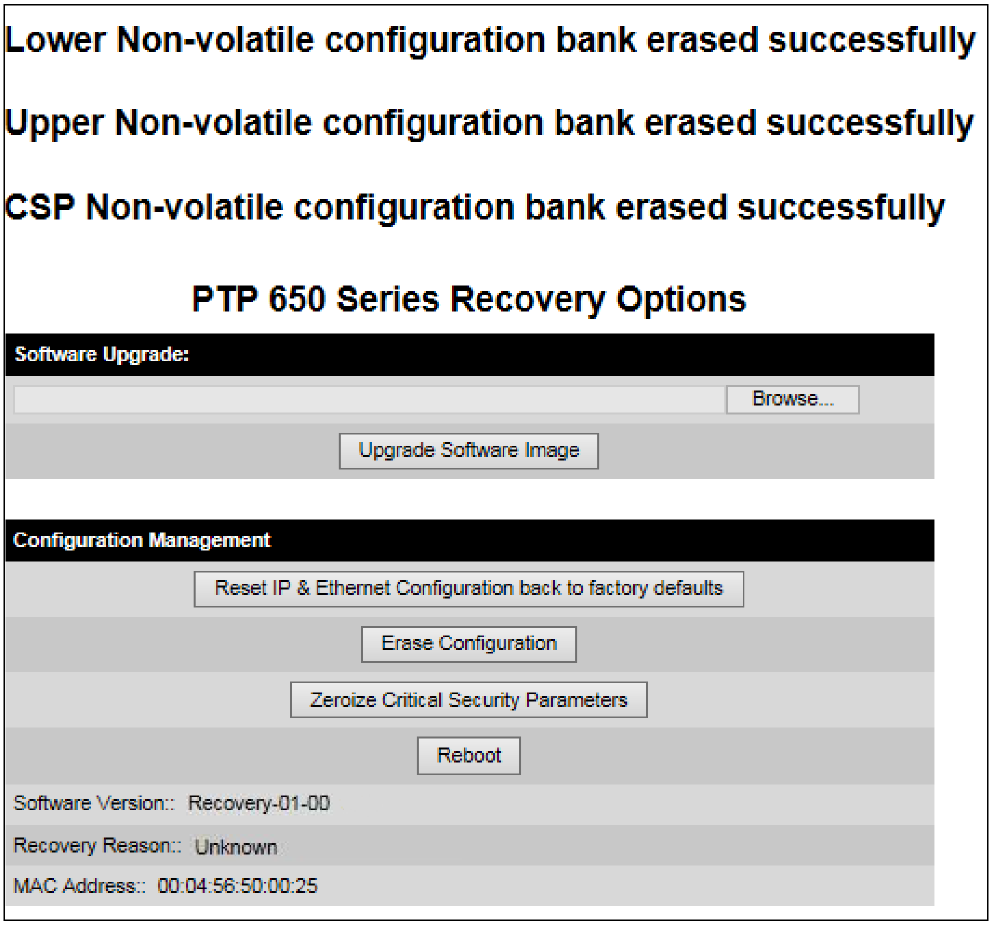


Message from webpage

IF YOU ERASE THE CONFIGURATION YOU WILL HAVE TO RE-ENTER ALL CONFIGURATION.

Are you sure you want to ERASE the configuration banks?

2 Click **OK**. The erase confirmation page is displayed:



Lower Non-volatile configuration bank erased successfully

Upper Non-volatile configuration bank erased successfully

CSP Non-volatile configuration bank erased successfully

PTP 650 Series Recovery Options

Software Upgrade:

Configuration Management

Software Version:: Recovery-01-00

Recovery Reason:: Unknown

MAC Address:: 00:04:56:50:00:25

Browse...
Upgrade Software Image
Reset IP & Ethernet Configuration back to factory defaults
Erase Configuration
Zeroize Critical Security Parameters
Reboot

3 Click **Reboot**. When the confirmation message is displayed, click **OK**.

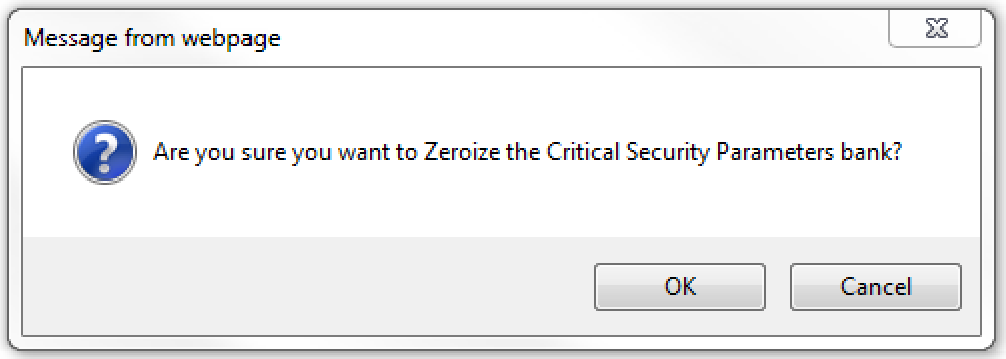
4 The unit reboots and starts up in normal mode but with all configuration erased. If the unit fails to start up, refer to Testing link end hardware on page 8-2.

Zeroize Critical Security Parameters page

Use this option to zeroize the critical security parameters (CSPs) of the unit from the Recovery Options page (Figure 133).

Procedure:

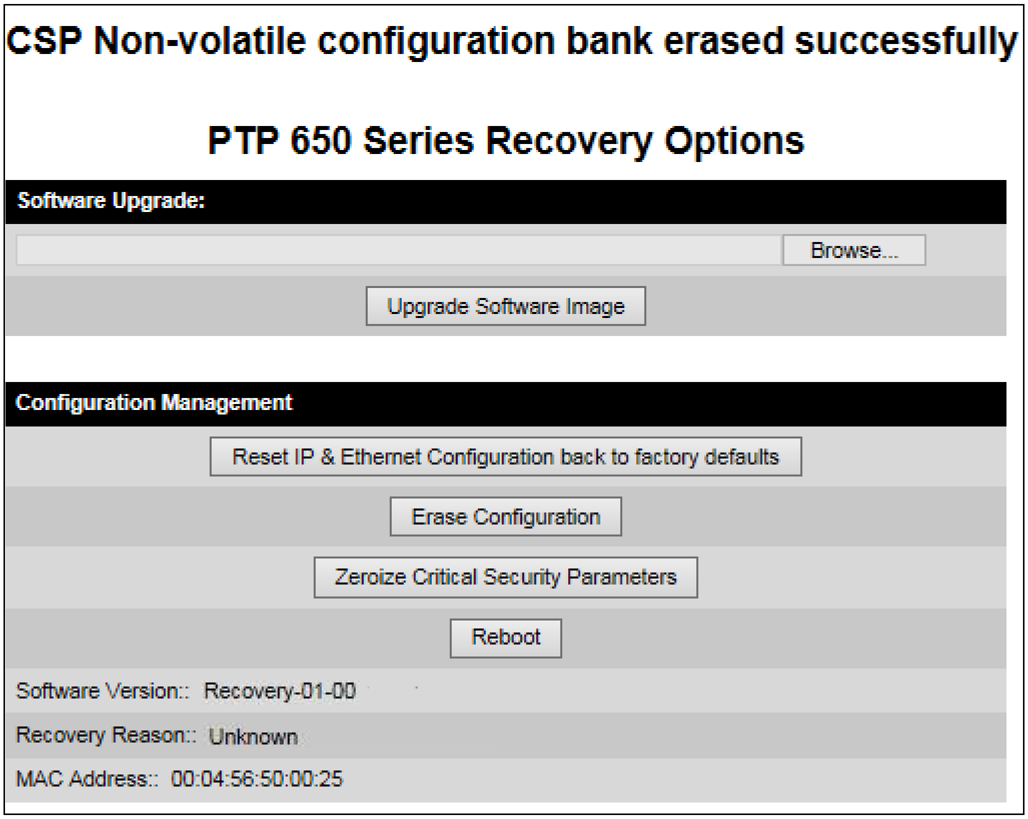
1 Click **Zeroize Critical Security Parameters.** The confirmation pop up box is displayed:



Message from webpage

Are you sure you want to Zeroize the Critical Security Parameters bank?

2 Click **OK.** The zeroize CSPs confirmation page is displayed:



CSP Non-volatile configuration bank erased successfully

PTP 650 Series Recovery Options

Software Upgrade:

Configuration Management

Software Version:: Recovery-01-00

Recovery Reason:: Unknown

MAC Address:: 00:04:56:50:00:25

Browse...
Upgrade Software Image
Reset IP & Ethernet Configuration back to factory defaults
Erase Configuration
Zeroize Critical Security Parameters
Reboot

3 Click **Reboot**. When the "`Are you sure you want to REBOOT this unit?`" message is displayed, click **OK**.

4 The unit will now reboot. The unit should now start up in normal mode but with the CSPs zeroized. If the unit fails to recover, refer to Testing link end hardware on page 8-2.

Rebooting the unit

Use this option to reboot the unit from the Recovery Options page (Figure 133).

Procedure:

- Click **Reboot**.
- When the "`Are you sure you want to REBOOT this unit?`" message is displayed, click **OK**. The unit will now reboot. The unit should now start up in normal operational mode. If the unit fails to start up, refer to Testing link end hardware on page 8-2.

Chapter 8: Troubleshooting

This chapter contains procedures for identifying and correcting faults in a PTP 650 link. These procedures can be performed either on a newly installed link, or on an operational link if communication is lost, or after a lightning strike.

The following topics are described in this chapter:

- Testing link end hardware on page 8-2 describes how to test the link end hardware, either when it fails on startup, or after a lightning strike.
- Testing the radio link on page 8-9 describes how to test the link when there is no radio communication, or when it is unreliable, or when the data throughput rate is too low.

Testing link end hardware

This section describes how to test the link end hardware when it fails on startup or during operation.

Before testing link end hardware, confirm that all outdoor drop cables, that is those that connect the ODU to equipment inside the building, are of the supported type, as defined in Outdoor copper Cat5e Ethernet cable on page 2-21.

AC Power Injector LED sequence

When the AC Power Injector is connected to the AC mains, the Power (green) LED should illuminate within 5 seconds of connection. If this does not happen, the AC injector is either not receiving power from the AC mains or there is a fault on the drop cable causing the power injector to sense an over current condition on the ODU output connector.

Action: Remove the ODU cable from the PSU and observe the effect on the power LED:

- If the power LED does not illuminate, confirm that the mains supply is working, for example check the plug and fuse (if fitted). If the power supply is working, report a suspected PSU fault to Cambium Networks.
- If the Power LED does illuminate, perform Test resistance in the drop cable on page 5-20.

AC+DC Enhanced power injector LED sequence

For the AC+DC Enhanced power injector, the expected power-up LED sequence is:

- The Power (green) LED illuminates steadily.
- After about 45 seconds, the Ethernet (yellow) LED blinks slowly 10 times.
- The Ethernet (yellow) LED illuminates steadily, then blinks randomly to show Ethernet activity.

If this sequence does not occur, take appropriate action depending on the LED states:

- Power LED is off on page 8-3
- Power LED is blinking on page 8-3
- Ethernet LED did not blink 10 times on page 8-3
- Ethernet LED blinks ten times then stays off on page 8-4
- Ethernet LED blinks irregularly on page 8-5 (for example a short blink followed by a long blink)
- Power LED is on, Ethernet LED blinks randomly on page 8-5

If a fault is suspected in the ODU-PSU drop cable, perform Test resistance in the drop cable on page 5-20.

Power LED is off

Meaning: Either the PSU is not receiving power from the AC/DC outlet, or there is a wiring fault in the ODU cable.

Action: Remove the ODU cable from the PSU and observe the effect on the Power LED:

- If the Power LED does not illuminate, confirm that the mains power supply is working, for example, check the plug and fuse (if fitted). If the power supply is working, report a suspected PSU fault to Cambium Networks.
- If the Power LED does illuminate, perform Test resistance in the drop cable on page 5-20.

Power LED is blinking

Meaning: The PSU is sensing there is an overload on the ODU port; this could be caused by a wiring error on the drop cable or a faulty ODU.

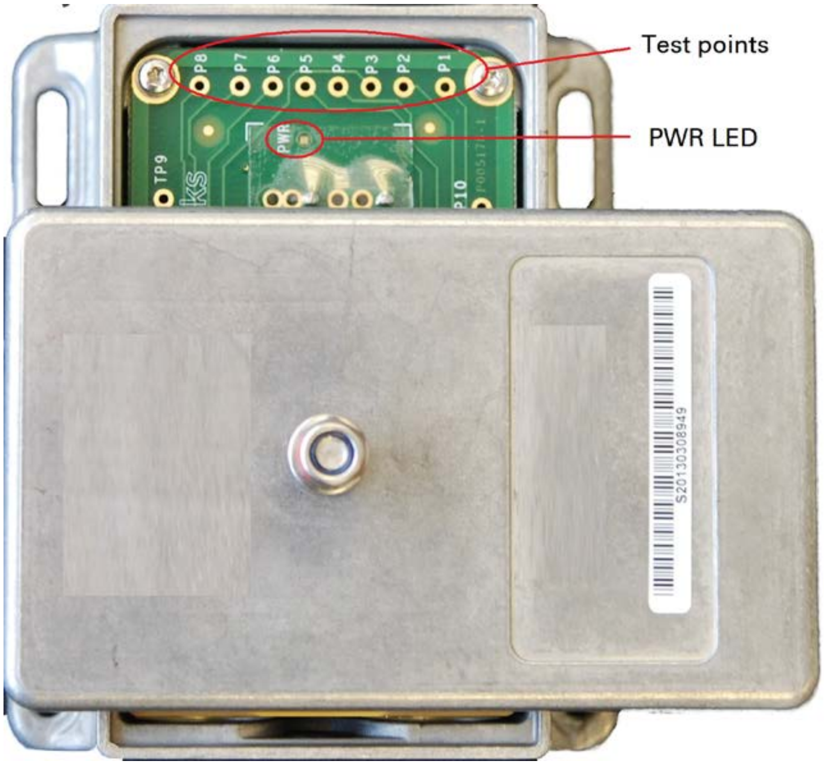
Action: Remove the ODU cable from the PSU. Check that pins 4&5 and 7&8 are not crossed with pins 1&2 and 3&6. Check that the resistance between pins 1&8 is greater than 100K ohms. If either check fails, replace or repair the ODU cable.

Ethernet LED did not blink 10 times

Meaning: The ODU flashes the LED on the AC+DC Enhanced Power Injector 10 times to show that the ODU is powered and booted correctly.

Action:

1. Remove the ODU cable from the PSU. Examine it for signs of damage. Check that the ODU cable resistances are correct, as specified in Test resistance in the drop cable on page 5-20. If the ODU cable is suspect, replace it.
2. Use the LPU (if installed) to check that power is available on the cable to the ODU. Access the connections by rotating the LPU lid as shown (slacken the lid nut but do not remove it):



4 Check that test point P1 on the LPU PCB corresponds to pin 1 on the RJ45. Repeat for points P2 to P8. This test is only valid if both the PSU and the ODU are disconnected.

5 Reconnect the ODU cable to the PSU.

6 Check that the PWR LED near the top right of the LPU PCB is illuminated to indicate power in the Ethernet cable.

7 If any test fails, replace or repair the cable that connects the PSU to the LPU or ODU.

Ethernet LED blinks ten times then stays off

Meaning: There is no Ethernet traffic between the PSU and ODU.

Action: The fault may be in the LAN or ODU cable:

- Confirm that Ethernet traffic is connected to the AC+DC injector LAN port, confirm the cable is not faulty, replace if necessary.
- If the LAN connection to the AC+DC power injector is working, check the drop cable is correctly wired using a suitable cable tester. Repeat the drop cable tests on page Test resistance in the drop cable on page 5-20.

Ethernet LED blinks irregularly

Meaning: If the Ethernet LED blinks irregularly, for example two rapid blinks followed by a longer gap, this indicates that the ODU has booted in recovery mode. The causes may be: installation wiring, or a corrupt ODU software load, or sufficient time has not been allowed between a repeat power up.

Action: Refer to Recovery mode on page 7-44.

Power LED is on, Ethernet LED blinks randomly

Meaning: Both LEDs are in their normal states, implying that the PSU is receiving power from the AC/DC outlet and there is normal Ethernet traffic between the PSU and ODU.

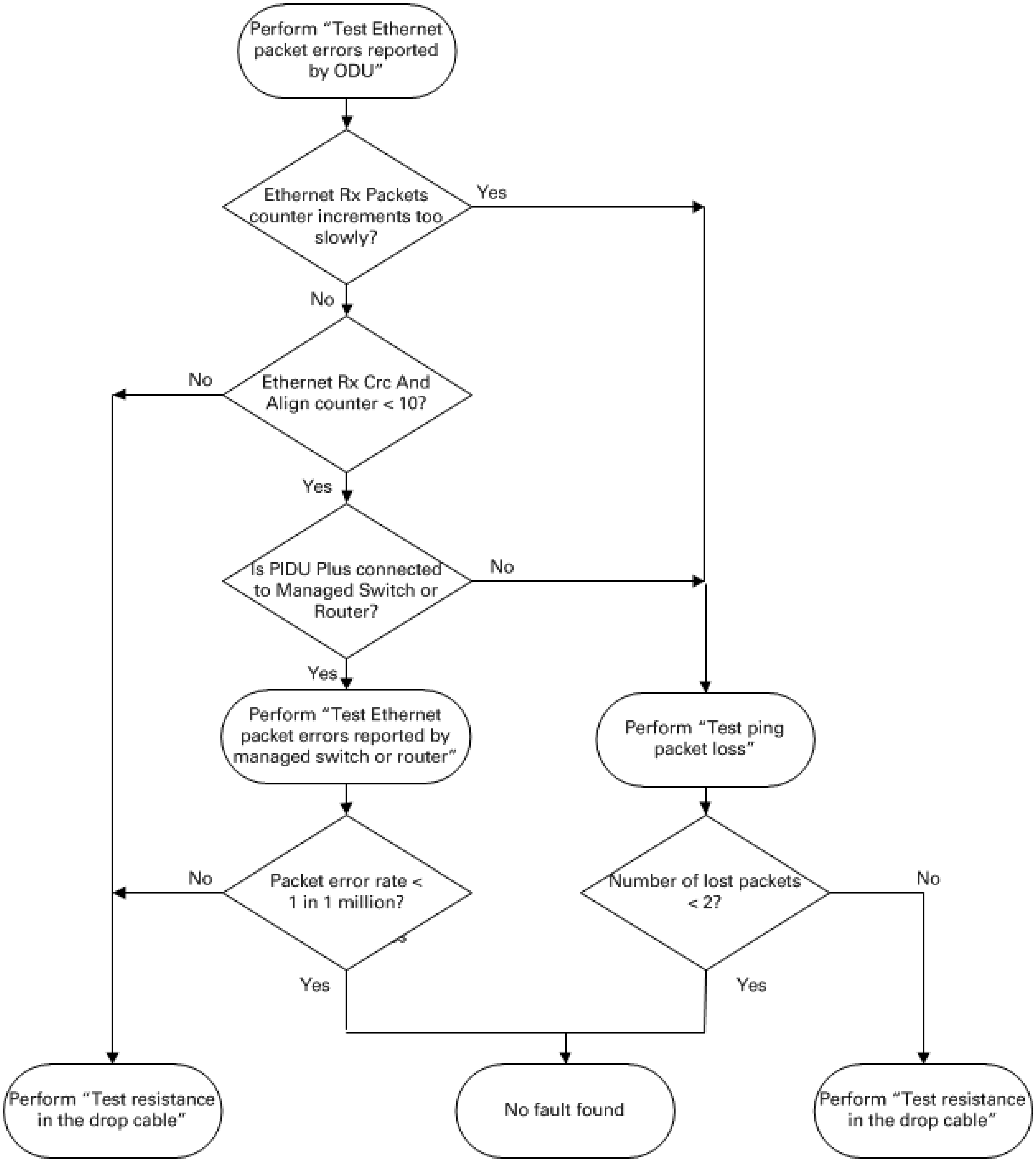
Action: If, in spite of this, a fault is suspected in the link end hardware:

- If the Ethernet connection to the network is only 100BASE-TX, when 1000BASE-T is expected: remove the ODU cable from the PSU, examine it, and check that the wiring to pins 4&5 and 7&8 is correct and not crossed.
- Perform Ethernet packet test on page 8-6.

Ethernet packet test

Follow the Ethernet packet test flowchart (Figure 134) and procedures below.

Figure 134 Ethernet packet test flowchart


Perform "Test Ethernet packet errors reported by ODU"
Ethernet Rx Packets counter increments too slowly?
Yes
No
Ethernet Rx Crc And Align counter < 10?
No
Yes
Is PIDU Plus connected to Managed Switch or Router?
No
Yes
Perform "Test Ethernet packet errors reported by managed switch or router"
Perform "Test ping packet loss"
Packet error rate < 1 in 1 million?
No
Yes
Number of lost packets < 2?
No
Yes
Perform "Test resistance in the drop cable"
No fault found
Perform "Test resistance in the drop cable"

Test Ethernet packet errors reported by ODU

Log into the unit and click **Administration**, **Statistics**, **Detailed Counters**. Click **Reset System Counters** at the bottom of the page and wait until the Ethernet Rx Packets counter has reached 1 million (the count will only update when the page is refreshed. If the counter does not increment or increments too slowly, because for example the PTP 650 is newly installed and there is no offered Ethernet traffic, then abandon this procedure and consider using the procedure Test ping packet loss on page 8-7.

Read the Ethernet Rx Crc And Align counter. The test has passed if this is less than 10.

Test Ethernet packet errors reported by managed switch or router

If the ODU is connected to a managed Ethernet switch or router, it may be possible to monitor the error rate of Ethernet packets. Please refer to the user guide of the managed network equipment. The test has passed if the rate of packet errors reported by the managed Ethernet switch or router is less than 10 in 1 million packets.

Test ping packet loss

Using a computer, it is possible to generate and monitor packets lost between the PSU and the ODU. This can be achieved by executing the Command Prompt application which is supplied as standard with Windows and MAC operating systems.

Caution

This procedure disrupt network traffic carried by the PTP 650 under test:

Procedure:

1. Ensure that the IP address of the computer is configured appropriately for connection to the PTP 650 under test, and does not clash with other devices connected to the network.
2. If the PSU is connected to an Ethernet switch or router then connect the computer to a spare port, if available.
3. If it is not possible to connect the computer to a spare port of an Ethernet switch or router, then the PSU will need to be disconnected from the network in order to execute this test:
   - Disconnect the PSU from the network.
   - Connect the computer directly to the LAN port of the PSU.
4. On the computer, open the Command Prompt application.

5 Send 1000 ping packets of length 1500 bytes. The process will take 1000 seconds, which is approximately 17 minutes.

If the computer is running a Windows operating system, this is achieved by typing (for an IPv6 address, use the **ping6** command):

```
ping –n 1000 –l 1500 <ipaddress>
```

where <ipaddress> is the IP address of the PTP 650 ODU under test.

If the computer is running a MAC operating system, this is achieved by typing:

```
ping –c 1000 –s 1492 <ipaddress>
```

where <ipaddress> is the IP address of the PTP 650 ODU under test.

6 Record how many Ping packets have been lost. This is reported by Command Prompt on completion of the test.

The test has passed if the number of lost packets is less than 2.

Testing the radio link

This section describes how to test the link when there is no radio communication, when it is unreliable, when the data throughput rate is too low, or when a unit is causing radio or TV interference. It may be necessary to test the units at both ends of the link.

No activity

If there is no wireless activity, proceed as follows:

1. Check for Alarm conditions on Home page.
2. Check that the software at each end of the link is the same version.
3. Check that the Target Mac address is correctly configured at each end of the link.
4. Check Range.
5. Check Tx Power.
6. Check License keys to ensure that both units are the same product variant.
7. Check Master/Slave status for each unit and ensure that one unit is Master and the other unit is slave.
8. Check that the link is not obstructed or the ODU misaligned.
9. Check the DFS page at each end of the link and establish that there is a quiet wireless channel to use.
10. If there are no faults found in the configuration and there is absolutely no wireless signal, retry the installation procedure.
11. If this does not work then report a suspected ODU fault to Cambium Networks.

Some activity

If there is some activity but the link is unreliable or does not achieve the data rates required, proceed as follows:

1. Check that the interference has not increased using the DSO measurements.
2. If a quieter channel is available check that it is not barred.
3. Check that the path loss is low enough for the communication rates required.
4. Check that the ODU has not become misaligned.

Radio and television interference

If a PTP 650 unit is interfering with radio or television reception (this can be determined by turning the equipment off and on), attempt the following corrective actions:

- Realign or relocate the antenna.
- Increase the separation between the affected equipment and antenna.
- Connect the ODU and PSU power supply into a power outlet on a circuit different from that to which the receiver is connected.
- Contact Cambium Point-to-Point for assistance.

Glossary

Term	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institution
ARP	Address Resolution Protocol
ATPC	Automatic Transmit Power Control
Aux	Auxiliary
BBDR	Broadband Disaster Relief
BPSK	Binary Phase Shift Keying
BW	Bandwidth
CFM	Connection Fault Management
CHAP	Challenge Handshake Authentication Protocol
CSP	Critical Security Parameter
DC	Direct Current
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Services Code Point
DSO	Dynamic Spectrum Optimization
EAPS	Ethernet Automatic Protection Switching
EIRP	Equivalent Isotropic Radiated Power
EMC	Electromagnetic Compatibility
EMD	Electro-Magnetic Discharge
EPL	Ethernet Private Line
ETSI	European Telecommunications Standards Institute
EU	European Union
FAQ	Frequently Asked Question

Term	Definition
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
GARP	Generic Attribute Registration Protocol
GE	Gigabit Ethernet
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IB	In-Band
IC	Industry Canada
ICMP	Internet Control Message Protocol
ICNIRP	International Commission on Non-Ionizing Radiation Protection
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
IPSec	Internet Protocol Security
ISM	Industrial Scientific and Medical
ITPE	Initial Transmit Power Estimate
KDB	Knowledge Database
L2CP	Layer Two Control Protocols
LACP	Link Aggregation Control Protocol
LLDP	Link Layer Discovery Protocol
LAN	Local Area Network
LOS	Line-of-Sight (clear line-of-sight, and Fresnel zone is clear)
LPU	Lightning Protection Unit
MAC	Medium Access Control Layer
MDI (-X)	Medium Dependent Interface (-Crossover)
MEF	Metro Ethernet Forum
MIB	Management Information Base
MIMO	Multiple-Input Multiple-Output
MLD	Multicast Listener Discovery
MPLS	Multiprotocol Label Switching
MRP	Multiple Registration Protocol

Term	Definition
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NA	Neighbor Advertisement
NLOS	Non-Line-of-Sight
NMEA	National Marine Electronics Association
NS	Neighbor Solicitation
NTP	Network Time Protocol
NUD	Neighbor Un-reachability Detection
ODU	Outdoor Unit
OFDM	Orthogonal Frequency Division Multiplex
OOB	Out-of-Band
PC	IBM Compatible Personal Computer
PEAP	Protected Extensible Authentication Protocol
PIDU	Powered Indoor Unit
POE	Power over Ethernet
PSU	Power Supply Unit
PTP	Point-to-Point
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
R-APS	Ring Automatic Protection Switching
RADIUS	Remote Authentication Dial-In Service
RAM	Random Access Memory
RF	Radio Frequency
RFC	Request for Comments
RoW	Rest of World
RMA	Return Material Authorization
RSSI	Received Signal Strength Indication
RSTP	Rapid Spanning Tree Protocol
SELV	Safety Extra Low Voltage

Term	Definition
SFP	Small Form-factor Pluggable
SLAAC	Stateless Address Auto-configuration
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
STP	Spanning Tree Protocol
Syslog	System Logging
TC	Traffic Class
TCP	Transmission Control Protocol
TDD	Time Division Duplexing
TDM	Time Division Multiplexing
TDWR	Terminal Doppler Weather Radar
TGB	Tower Ground Bus bar
TLS	Transport Layer Security
UNII	Unlicensed National Information Infrastructure
URL	Universal Resource Location
USM	User-based Security Model
UTC time	Coordinated Universal Time
UTP	Unshielded Twisted Pair
UV	Ultraviolet
VACM	View-based Access Control Model
VLAN	Virtual Local Area Network
WEEE	Waste Electrical and Electronic Equipment