Cambium Networks™

USER GUIDE

PTP 700 Series
System Release 700-02-70

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 Use 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 700 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:	https://support.cambiumnetworks.com
Main website:	http://www.cambiumnetworks.com
Sales enquiries:	solutions@cambiumnetworks.com
Support enquiries:	https://support.cambiumnetworks.com
RMA enquiries	https://support.cambiumnetworks.com
Telephone number list:	http://www.cambiumnetworks.com/contact-us/
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 us feedback at https://support.cambiumnetworks.com

Important regulatory information

Complying with rules for the country of operation

The PTP 700 product operates in frequency bands between 4.4 GHz and 5.8 GHz. These bands are made available for licensed or unlicensed operation according to the individual rules and regulations in force in each country.

Ensure that the equipment is operated in accordance with applicable regulations.

Obtain the necessary licenses or permits before using the equipment in licensed bands.

Some regional variants of PTP 700 are locked to a single country of operation. For the remaining regional variants, use the Cambium Networks Support Centre to obtain a country-specific license key for the country of operation. Country-specific license keys are automatically populated with the list of regulatory bands allowed in that country.

In some regulatory bands, PTP 700 may be allowed as a secondary user of the band, where operation is subject to the condition that the product does not cause interference to primary users of the band. In this case, take care to avoid causing interference to primary users.

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 700 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 700. If this is not done, installers and users may be liable to civil and criminal penalties.

Contact Cambium Customer Support if more guidance is required.

Application firmware

Download the latest PTP 700 Series firmware and install it in the Outdoor Units (ODUs) before deploying the PTP 700 equipment. Instructions for installing firmware are provided in Upgrading software image on page 7-75.

External antennas

When using an external connectorized antenna (as compared to the integrated antenna in the Conectorized+Integrated platform variant), 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 ranges 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 700 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 700 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.

Attention 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.

Precautionary statements

The following describes how precautionary statements are used in this document.

Warning

Precautionary statements with the Warning tag 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.

Attention

Precautionary statements with the Attention tag precede instructions that 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. An attention statement has the following format:

Attention Attention text and consequence for not following the instructions.

Note

Precautionary statements with the Note tag incidate the possibility of an undesirable situation or provide additional information to help the reader understand a topic or concept. A note has the following format:

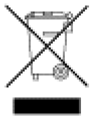
Note Note text.

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/weee-compliance

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 products in the PTP 700 series. 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 700 Series on page 1-2 introduces the key features, typical uses, product variants and components of the PTP 700 series.
- Wireless operation on page 1-7 describes how the PTP 700 wireless link is operated, including modulation modes, power control and spectrum management.
- Ethernet bridging on page 1-36 describes how the PTP 700 controls Ethernet data, in both the customer data and system management networks.
- System management on page 1-48 introduces the PTP 700 management system, including the web interface, installation, configuration, security, alerts and upgrades.
- FIPS 140-2 mode on page 1-67 describes the (optional) FIPS 140-2 approved mode of operation.

Overview of the PTP 700 Series

This section introduces the key features, typical uses, product variants and components of the PTP 700 series.

Purpose

Cambium PTP 700 Series Bridge products are designed for Ethernet bridging over point-to-point (PTP) and high-capacity multipoint (HCMP) microwave links in licensed, unlicensed and lightly-licensed frequency bands between 4400 MHz and 5875 MHz. Users must ensure that the PTP 700 Series complies with local operating regulations.

The PTP 700 Series acts as a transparent bridge between two or more segments of the operator's network. In this sense, it can be treated as a virtual wired connection between two or more points. The PTP 700 Series forwards 802.3 Ethernet frames destined for the other part or parts 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 700 is a high-performance wireless bridge for Ethernet traffic with a maximum throughput of 450 Mbps. It can operate in line-of-sight (LOS), near-LOS and non-LOS propagation conditions. Its maximum LOS range is 250 km. The PTP 700 operates in licensed, unlicensed and lightly-licensed frequency bands between 4400 MHz and 5875 MHz. It has a very high spectral efficiency of 10 bps/Hz and supports a channel bandwidth of up to 45 MHz. The PTP 700 Connectorized ODU is designed for use with an external antenna. The PTP 700 Connectorized+Integrated ODU can be used with an external antenna or with an integrated 22 dBi flat plate antenna.

PTP 700 operates in two distinct wireless topologies: point-to-point (PTP) and high-capacity multipoint (HCMP). A PTP link consists of one outdoor unit (ODU) configured as a Master and one ODU configured as a Slave. An HCMP sector consists of one ODU configured as a Master and up to eight ODUs configured as Slaves.

The wireless link uses Time Division Duplex (TDD) to connect in both directons over a single RF channel and supports both symmetric and asymmetric TDD configurations.

The PTP 700 wireless link forwards Ethernet traffic between wired Ethernet interfaces as a transparent Layer 2 bridge. Each ODU supports up to three Gigabit Ethernet ports. Two ports support twisted pair Gigabit Ethernet. One of them can provide 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.

The PTP 700 Series 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 or remote management).

PTP 700 supports both synchronous Ethernet and operation as an IEEE 1588-2008 transparent clock.

Table 1 gives a summary of the main PTP 700 characteristics.

Table 1 Main characteristics of the PTP 700 Series

Characteristic	Value
Topology	PTP, HCMP
Wireless link condition	LOS, near LOS or non-LOS
Range	Up to 250 km (PTP topology), up to 100 km (HCMP topology)
Duplexing	TDD (symmetric and asymmetric)
Modulation	OFDM
Connectivity	Ethernet
Synchronous Ethernet	ITU-T G.8262/Y.1362 EEC-Option 1 and EEC-Option 2
Transparent clock	IEEE 1588-2008 compliant
Operating frequencies	4400 MHz to 5875 MHz
Channel bandwidth	5, 10, 15, 20, 30, 40 or 45 MHz
High spectral efficiency	Up to 10 bps/Hz
Aggregate data capacity	Up to 450 Mbps (45 MHz channel BW)
Management protocols	cnMaestro, HTTP, HTTPS, SNMP v1/2c, SNMP v3, syslog, SMTP, RADIUS
Security	AES, FIPS 140-2 Level 2
Color	White, Green, Desert Tan

Frequency bands

The PTP 700 ODU can be configured by the user to operate in the following bands:

- 4.7 GHz band: 4400 MHz to 5000 MHz
- 4.9 GHz band: 4940 MHz to 4990 MHz
- 5.1 GHz band: 5150 MHz to 5250 MHz
- 5.2 GHz band: 5250 MHz to 5350 MHz
- 5.4 GHz band: 5470 MHz to 5725 MHz
- 5.8 GHz band: 5725 MHz to 5875 MHz

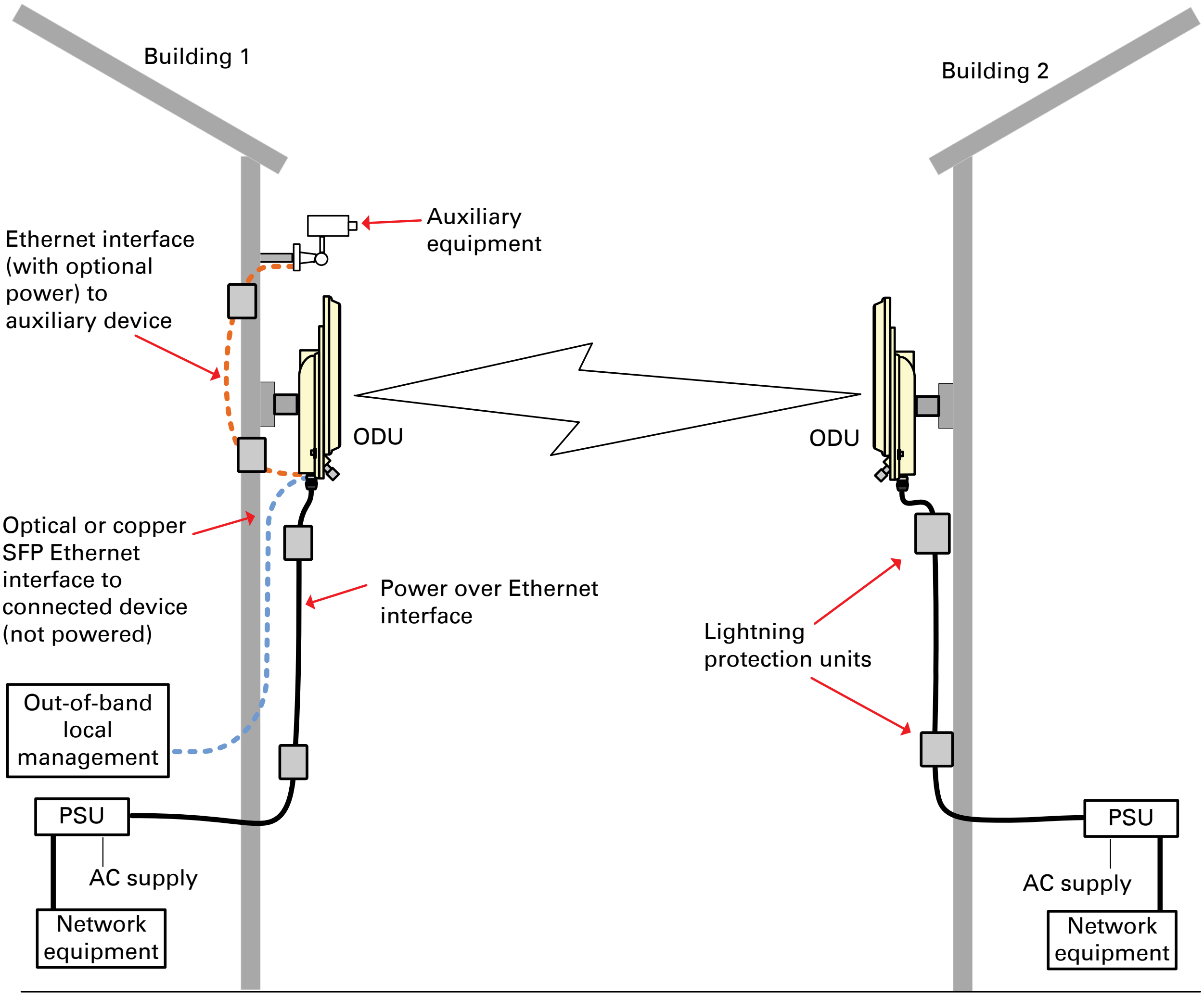
Note The supported frequency coverage may be restricted in some country licenses to comply with the applicable regulations.

Typical bridge deployment

The PTP 700 is an "all outdoor" solution consisting of a wireless bridge between two or more sites. Each site installation consists of a PTP 700 Connectorized outdoor unit (ODU) or a PTP 700 Connectorized+Integrated 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 customer data and/or network 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 700 typical bridge deployment



Hardware overview

The main hardware components of the PTP 700 are as follows:

- Outdoor unit (ODU): The ODU is a self-contained transceiver unit that houses both radio and networking electronics. The PTP 700 ODU is supplied in two configurations:
  - A PTP 700 Connectorized ODU intended to work with separately mounted external antennas.
  - A PTP 700 Connectorized+Integrated ODU intended to work with either separately mounted external antennas or with an integrated 22 dBi flat plate antenna.
- Power supply unit (PSU): PTP 700 provides two options for PSUs:
  - The AC+DC Power Injector 56V is required when powering a single PTP 700 ODU from a DC supply, when powering an auxiliary device, or when using PTP-SYNC.
  - The Cluster Management Module (CMM5) is a modular system consisting of power injectors, power supplies, a controller and a GPS receiver. Each Power and Sync Injector can power up to four ODUs. CMM5 also distributes a synchronization signal from a Universal GPS (UGPS) receiver to the ODUs.
- Antennas and antenna cabling: Connectorized ODUs require external antennas connected using RF cable.
- PTP SYNC unit (optional): The PTP SYNC unit can be used with the AC+DC Enhanced Power Injector 56V to provide TDD synchronization at a TDD Master ODU. PTP-SYNC must be used with the AC+DC Enhanced Power Injector 56V.
- GPS receivers: PTP 700 supports two different GPS receivers for network-wide TDD synchronization. The Trimble Acutime™GG GPS receiver is used with PTP-SYNC. The Universal GPS (UGPS) receiver is used with CMM5.
- 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.

Protected links

PTP 700 ODUs can be deployed as a high-availability Hot Standby PTP link for mission-critical applications. In a Hot Standby link, Primary and Secondary Master ODUs are collocated at one end of the link, and Primary and Secondary Slave ODUs are collocated at the other end of the link. The ODUs are connected to a standard Ethernet switch at each end of the link.

The Hot Standby link is resilient to failure of any single unit or interconnection, and resilient to some multiple failures.

The hardware components for a Hot Standby link are as follows:

- Four PTP 700 ODUs, Connectorized or Connectorized+Integrated
  - Two ODUs collocated at each end of the link
- Power Supply Units (PSUs):
  - Two AC+DC Power Injector 56V at each end of the link, or
  - One CMM5 with two unused ports at each end of the link
- Antennas and antenna cabling for individual antennas or shared antennas
- If AC+DC Power Injector 56V is used:
  - Two PTP SYNC units connected to ODUs at the Master end of the link
  - Two Trimble Acutime™GG GPS receivers connected to the PTP-SYNC units
- If CMM5 is used:
  - Universal GPS (UGPS) receiver connected to the CMM5 at the Master end of the link
- Ethernet cabling:
  - Copper Ethernet Cat5e connection from the ODUs (PSU port) to the PSUs
  - Copper Ethernet Cat5e connection (suitable for 1000BASE-T) as a Protection link between the Aux ports of collocated ODUs
- Lightning protection units (LPUs): LPUs installed in the PSU 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.

Wireless operation

This section describes how the PTP 700 wireless link is operated, including topology, modulation modes, power control and security.

Wireless topology

PTP 700 supports operation in two distinct topologies:

- Point to point (PTP)
- High-capacity multipoint (HCMP)

PTP topology

The PTP topology provides Ethernet bridging over a point-to-point wireless link consisting of one outdoor unit (ODU) configured as a TDD Master and one ODU configured as a TDD Slave.

The PTP topology supports the following features:

- Range: Up to 250 km
- Operating frequencies: 4400 MHz to 5875 MHz
- Channel bandwidth: 5 MHz, 10 MHz, 15 MHz, 20 MHz, 30 MHz, 40 MHz, 45 MHz
- TDD ratio: 1:5, 1:3, 1:2, 1:1, 2:1, 3:1, 5:1, adaptive
- Link optimization: IP or TDM
- TDD synchronization using PTP-SYNC
- Spectral efficiency: Up to 10 bps/Hz
- Aggregate data capacity: Up to 450 Mbps
- Dynamic Spectrum Optimization (DSO): Symmetric, Asymmetric
- Out-of-band management
- Synchronous Ethernet
- IEEE 1588 Transparent Clock
- Hot Standby link protection

HCMP topology

The optional HCMP topology provides Ethernet bridging over a star of individual point-to-point wireless links connecting one ODU configured as a TDD Master with up to eight ODUs configured as TDD Slaves. Each of the individual wireless links is connection-oriented and operates in a dedicated transmission burst in the TDD frame. The capacity of the sector is shared between the individual links, but apart from this each of the links has efficiency and performance similar to links provided in the PTP topology.

The Master ODU will normally be installed with a connectorized sector or omni-directional antenna. Slave ODUs will normally be installed with an integrated or connectorized directional antenna.

The Master ODU includes an Ethernet bridging function with address learning to forward Ethernet data traffic via a wireless link to the appropriate Slave, based on the destination address of the end-station reached through the Slave. Traffic with broadcast or unknown unicast destination address is duplicated in the Master and forwarded on each of the links separately.

The star of wireless links and the Ethernet bridging function in the Master together provide LAN-like connectivity between the wired ports at up to nine ODUs. Data traffic forwarded from a wired port on one Slave to a wired port on a different Slave is delivered via the Master ODU and thus consumes wireless capacity in two different time slots.

The HCMP topology supports the following features:

- Operating frequencies: 4400 MHz to 5875 MHz
- Channel bandwidth: 20 MHz or 40 MHz
- Range: Up to 100 km
- Number of Slaves: Up to eight
- Link symmetry: 4:1, 3:1, 2:1, 1:1, 1:2, 1:3, 1:4. Link symmetry at 20 MHz channel bandwidth depends on maximum range and the maximum number of Slaves
- Link optimization: IP
- TDD synchronization using PTP-SYNC
- Spectral efficiency: Up to 8.3 bps/Hz
- Aggregate data capacity: Up to 338 Mbit/s
- Dynamic Spectrum Optimization (DSO): Symmetric

Synchronous Ethernet and IEEE 1588 Transparent Clock are not supported for the HCMP topology in this release, but may be added in later releases.

Further reading

For information about…	Refer to…
Wireless encryption in HCMP topology	Wireless encryption on page 1-27
Capability upgrades for HCMP	Capability upgrades on page 1-63
Configuring encryption in HCMP	Wireless encryption on page 1-27
Configuring the Whitelist	Authorization Control page on page 6-60

Orthogonal Frequency Division Multiplexing (OFDM)

PTP 700 transmits using Orthogonal Frequency Division Multiplexing (OFDM) to encode data onto multiple RF carriers, with Low Density Parity Check (LDPC) for Forward Error Correction (FEC). The PTP 700 radio transmits on two orthogonal polarizations with polarization diversity (single payload, sometimes called MIMO-A) or polarization multiplexing (dual payload, sometimes called MIMO-B).

Time slots

PTP 700 transmit bursts always contain a multiple of 10 OFDM symbols. In most PTP and HCMP applications, the system selects the multiple of 10 symbols in a transmit burst automatically, based on configured attributes including Topology, Channel Bandwidth, Symmetry, Link Optimization, Link Range and (in the case where Link Optimization is set to Adaptive) traffic loading in each direction. In TDD Synchronized operation, the burst duration is again a multiple of 10 OFDM symbols but is selected directly with units of µs. The HCMP Expert mode offers a finer level of control over wireless operation in HCMP, and here burst duration is selected in terms of time slots.

A time slot is simply the time taken to transmit 10 OFDM symbols. The duration of a time slot varies inversely with Channel Bandwidth.

Link protection

This Hot Standby feature of PTP 700 provides a high-availability PTP link configuration for mission-critical applications.

The overall arrangement uses four ODUs, with Primary and Secondary Master ODUs collocated at one end of the link, and Primary and Secondary Slave ODUs collocated at the other end of the link.

The four ODUs are based on identical hardware and firmware, configured appropriately for four individual roles, as follows:

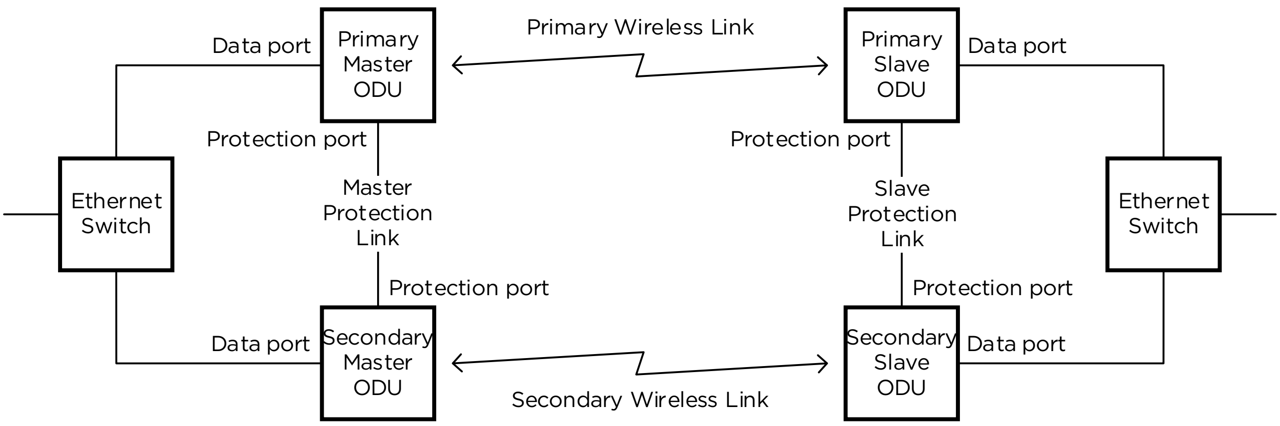
- Primary Master
- Primary Slave
- Secondary Master
- Secondary Slave

Use of Primary and Secondary wireless links

A Primary wireless link is established between the Primary ODUs, and a Secondary wireless link is established between the Secondary ODUs, as shown in Figure 2. The Primary and Secondary links have their TDD frames synchronized and interleaved to avoid mutual interference, and ideally share a single RF channel.

Primary and Secondary wireless links are established concurrently during normal operation. This is different from typical protection schemes for licensed microwave where only one link is established at any time. The protection scheme does not require (or allow) a Primary Master to establish a link with a Secondary Slave, or a Secondary Master to establish a link with a Primary Slave. This also is different from typical protection schemes.

Figure 2 Hot Standby Link



Protection state

Normally, one link (Primary or Secondary) in a Hot Standby arrangement is established and in the Active protection state, and the other link (Secondary or Primary respectively) is established and in the Standby protection state. A link in the Active state forwards traffic in the Data and Management services; a link in the Standby state blocks Data and Management services.

Any link with a fault is not available for service, and therefore necessarily in the Standby state. It follows that if both Primary and Secondary links have faults, both are in the Standby state.

A protection switch is the event where a link transitions from Active to Standby protection state, or from Standby to Active protection state. Protection switching is normally coordinated between Primary and Secondary links.

Channel bandwidth

The Hot Standby feature is available in the following bandwidths:

- 20 MHz
- 30 MHz
- 40 MHz
- 45 MHz

Burst duration

A Secondary link in Hot Standby scheme operates with the same bandwidth, same RF channel frequency, and same TDD frame duration as the associated Primary link. The Primary and Secondary links have synchronized TDD frames.

The transmit (or receive) burst duration of a link in the Standby state is always equivalent to a single time slot. The transmit (or receive) burst duration of an Active link is normally equivalent to several time slots. A transition between Active and Standby states therefore involves a modification of the transmit and receive burst duration.

Capacity

The capacity or spectral efficiency of the Active link is reduced compared with an equivalent unprotected link because the overall burst duration of the Hot Standby system is divided (unequally) between the Active and the Standby links, while only the Active link is used for customer data traffic. Longer burst durations increase the proportion of the burst that is used for customer traffic and thereby provide higher efficiency.

Time division duplexing in PTP wireless topology

TDD cycle

PTP 700 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 for a PTP link is illustrated in Figure 3. 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.

The frame duration must be long enough to allow the Master to receive the complete burst in 7 before starting to transmit in 8.

TDD frame parameters

The TDD burst duration varies depending on the following:

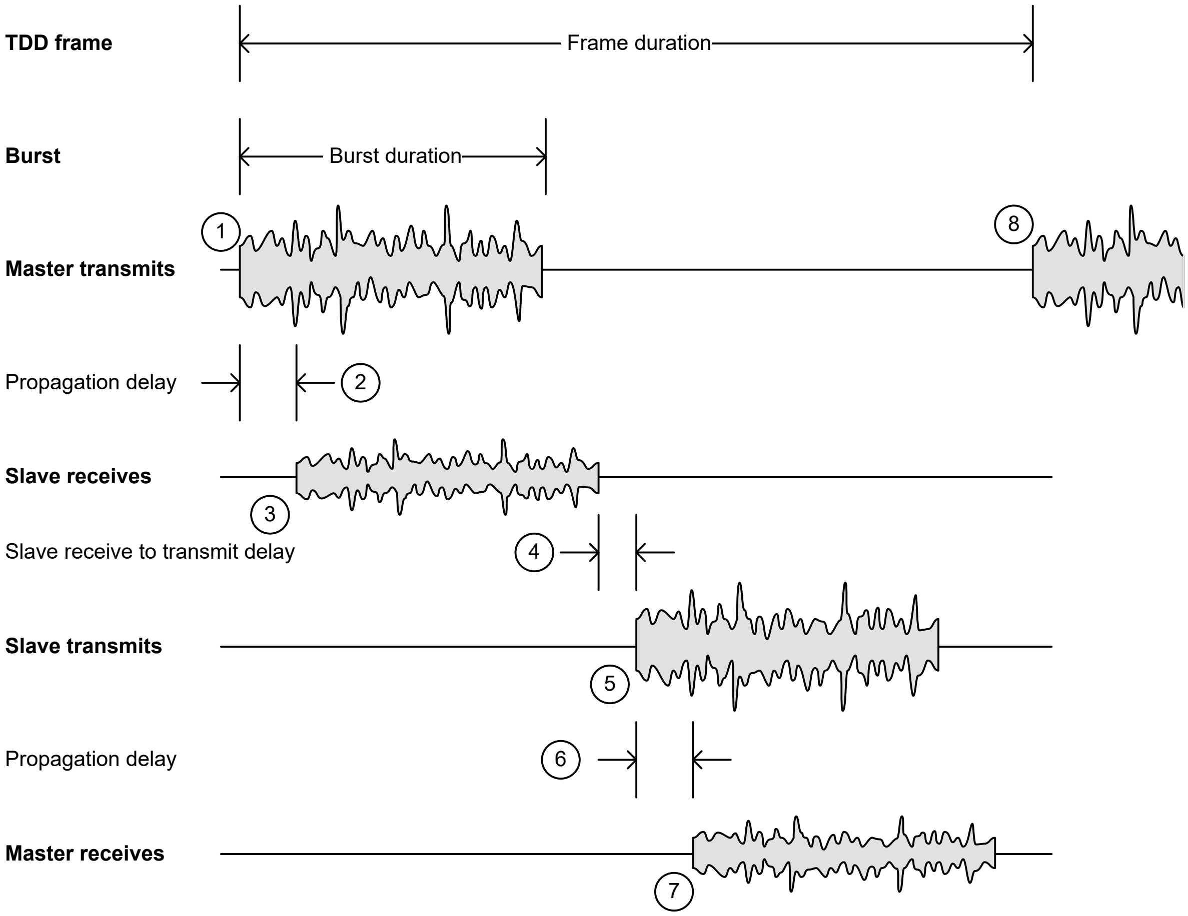
- Channel bandwidth
- Link range
- Link optimization mode
- Link symmetry
- Offered traffic loading.

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.

Figure 3 TDD cycle for PTP



Channel selection

The PTP 700 series links can transmit and receive 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, transmit and receive channels are always identical.

Time division duplexing in HCMP wireless topology

TDD cycle

The TDD cycle in HCMP operation is like the equivalent case for the PTP topology, except that the individual wireless links are accommodated in separate time slots within the TDD frame.

The TDD cycle for a simple HCMP sector with two Slave ODUs is illustrated in Figure 4. The steps in the cycle are as follows:

1 The TDD Master transmits a burst to the first TDD Slave.

2 A delay occurs as the Master-Slave burst propagates over the link.

3 The first Slave receives the burst from the Master.

4 The first Slave processes the Master-slave burst.

5 The first 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 first Slave.

8 The Master transmits a burst to the second TDD Slave. A similar set of steps leads to:

9 The Master receives the burst from the second Slave.

10 The Master transmits the next burst to the first Slave.

Sectors configured for more than two Slaves necessarily have extended frame duration to accommodate additional Master-Slave and Slave-Master transmissions.

TDD frame parameters

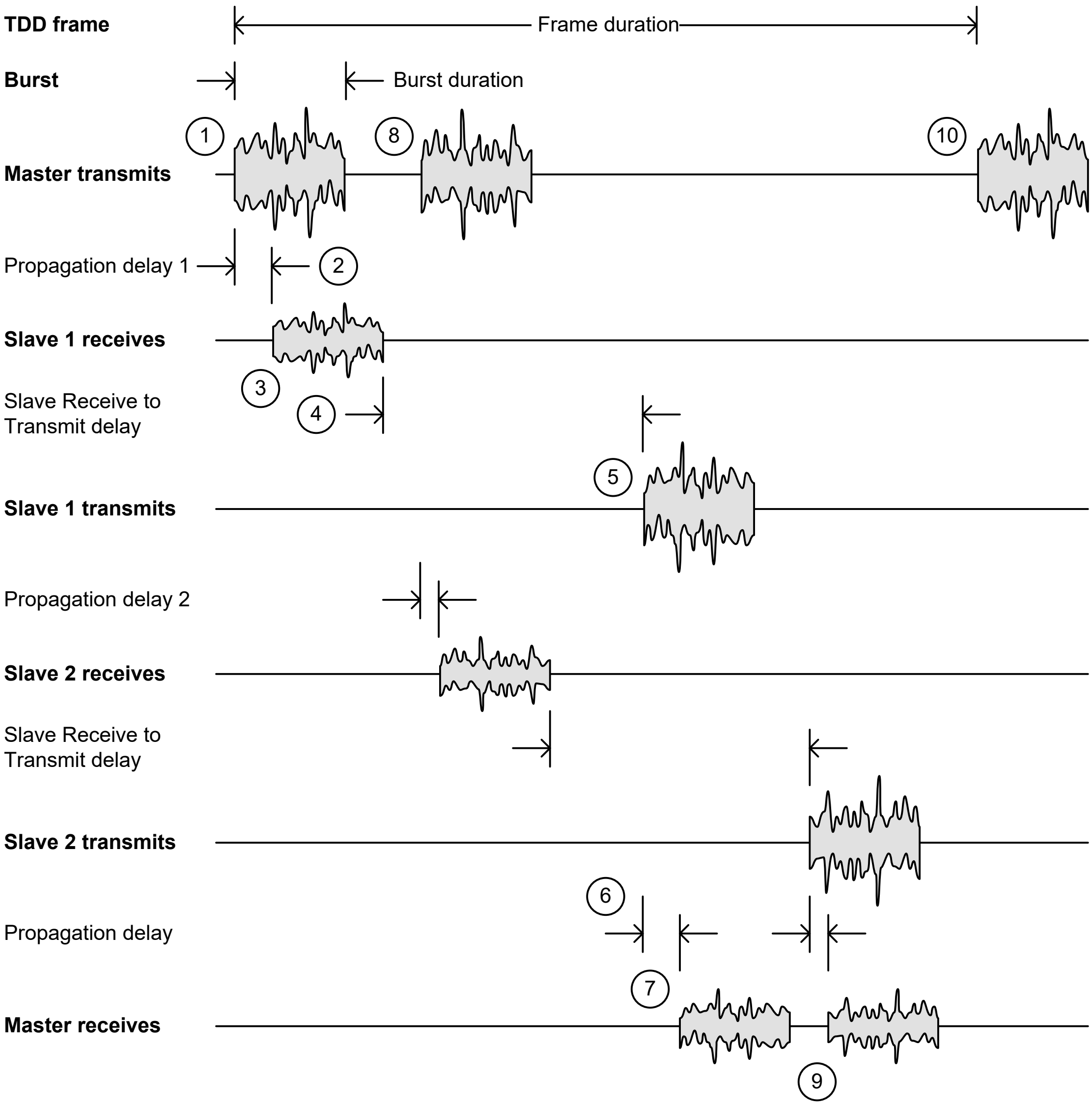
In the HCMP topology, the TDD burst duration is a multiple of the time slot duration.

The TDD frame duration varies depending on the following:

- Maximum number of Slaves
- Maximum link range
- Link symmetry

The propagation delay in Step 2 is necessarily equal to the propagation delay in Step 6, and is determined solely by the link range. The propagation delay for the second Slave will be different from the delay for the first Slave unless the two Slaves are at the same range.

Figure 4 TDD cycle for HCMP



Channel selection

In the HCMP topology, the ODUs in a sector all transmit and receive on a common channel.

Further reading

For information about...	Refer to...
TDD synchronization in PTP and HCMP networks	TDD synchronization on page 1-32

Link mode optimization

Link mode optimization allows the PTP 700 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 link optimization in the PTP topology

The IP link optimization mode provides the maximum possible link capacity. IP 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.

TDM link optimization in the PTP topology

The TDM link optimization mode provides the lowest possible latency. TDM 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 mode is an appropriate choice for delay intolerant data without reliable transmission (for example voice over IP data). TDM Traffic mode is selected automatically when TDM interfaces are enabled.

Link optimization in the HCMP topology

The HCMP topology supports only IP link optimization.

Further reading

For information about...	Refer to...
Effect of IP and TDM modes on link symmetry	Link symmetry on page 1-15
Effect of IP and TDM modes on link data throughput capacity	Calculating data rate capacity on page 3-26 Data throughput capacity tables on page 3-87
Effect of IP and TDM modes on system threshold, output power and link loss	System threshold, output power and link loss on page 3-64
How to configure link mode optimization	Wireless Configuration page on page 6-24
Link mode optimization alarms	Alarms on page 7-18

Link symmetry

PTP topology

The PTP 700 series provides eight configuration options for apportioning the available capacity between the two link directions.

- **Symmetric –** The Master and Slave have equal capacity. The PTP 700 series achieves this by allocating an equal Burst Duration for the Master and the Slave.
- **5:1 –** The capacity in the direction Master to Slave is five times that of the direction Slave to Master. The PTP 700 series achieves this by setting the Burst Duration of the Master to five times that of the Slave
- **3:1 –** The capacity in the direction Master to Slave is three times that of the direction Slave to Master. The PTP 700 series achieves this by setting the Burst Duration of the Master to three times that of the Slave.
- **2:1 –** The capacity in the direction Master to Slave is twice that of the direction Slave to Master. The PTP 700 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 700 series achieves this by setting the Burst Duration of the Slave to twice that of the Master.
- **1:3 –** The capacity in the direction Slave to Master is three times that of the direction Master to Slave. The PTP 700 series achieves this by setting the Burst Duration of the Slave to three times that of the Master.
- **1:5 –** The capacity in the direction Slave to Master is five times that of the direction Master to Slave. The PTP 700 series achieves this by setting the Burst Duration of the Slave to five times that of the Master.
- **Adaptive –** This is only available on the Full license. 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 700 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 700 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.

Note The 5:1, 3:1, 2:1, 1:2, 1:3 and 1:5 modes are not available when TDD synchronization is enabled.

Note Adaptive mode is not available in the following configurations:

- When link mode optimization is set to TDM Traffic (see Link mode optimization on page 1-14).
- When TDD synchronization is enabled.
- In regions where radar avoidance is operational (see Radar avoidance on page 1-25).
- When the ODU is not on a Full license.

HCMP topology with Standard TDD Frame Configuration

The PTP 700 series provides seven configuration options for apportioning the available capacity between the two link directions.

- **4:1 –** The capacity in the downlink (Master to Slave) direction is four times that of the uplink (Slave to Master) direction.
- **3:1 –** The capacity in the downlink direction is three times that of the uplink direction.
- **2:1 –** The capacity in the downlink direction is twice the uplink direction.
- **1:1 –** Uplink and downlink capacity is equal.
- **1:2 –** The capacity in the uplink direction is twice the downlink direction.
- **1:3 –** The capacity in the uplink direction is three times that of the downlink direction.
- **1:4 –** The capacity in the uplink direction is four times that of the downlink direction.

The asymmetric options are available independent of TDD Synchronization.

The available Link Symmetry options in HCMP topology depend on Channel Bandwidth, Maximum Link Range and the number of Slaves, as shown in Table 2.

Table 2 Link symmetry options in HCMP

Channel Bandwidth	Number of slaves	Maximum Link Range	Supported link symmetry options
20 MHz	Two, three, four	5.0 km to 100.0 km	4:1, 3:1, 2:1, 1:1, 1:2, 1:3, 1:4
	Five	5.0 km to 100.0 km	3:1, 2:1, 1:1, 1:2, 1:3
	Six	5.0 km to 100.0 km	2:1, 1:1, 1:2
	Seven	5.0 km to 57.0 km	2:1, 1:2
		5.0 km to 100.0 km	1:1
	Eight	5.0 km to 100.0 km	1:1
40 MHz	Two to eight	5.0 km to 100.0 km	4:1, 3:1, 2:1, 1:1, 1:2, 1:3, 1:4

HCMP topology with Expert TDD Frame Configuration

The Expert option for TDD Frame Configuration Mode offers a flexible approach to configuring link symmetry in HCMP sectors, allowing individual links to be provided with additional time slots in the uplink or downlink as required to meet differing traffic loads. This is useful where HCMP Slaves are deployed to serve different organizational functions.

In the Expert mode, the HCMP Master is configured for:

- TDD Frame Configuration Mode = Expert
- Channel Bandwidth
- HCMP Maximum Link Range
- Maximum Number of Slaves
- Total Downlink Time Slots
- Total Uplink Time Slots

The Master configuration determines the overall TDD frame structure for the HCMP sector.

The HCMP Slaves are all configured to match the HCMP Master, and individually configured with:

- Downlink Slots Request
- Uplink Slots Request
- Downlink Slots Limit
- Uplink Slots Limit

The HCMP Master allows a Slave to connect if it can provide at least the requested uplink and downlink time slots. If some capacity is available, but it is insufficient to meet the request then the Master rejects the connection attempt.

Table 3 shows the maximum number of time slots in the TDD frame as a function of Channel Bandwidth and Maximum Link Range.

Table 3 Maximum number of time slots in HCMP Expert mode

Channel Bandwidth	Maximum Link Range	Maximum total number of time slots
20 MHz	5.0 km to 57.0 km	21
	57.1 km to 100.0 km	20
40 MHz	5.0 km to 11.9 km	44
	12.0 km to 59.7 km	43
	59.8 km to 100.0 km	42

The minimum uplink or downlink request for one HCMP Slave is 1 time slot.

The maximum uplink or downlink request for one HCMP Slave is 15 time slots.

Note The Expert mode allows a population of Slaves to be created where the sum of all uplink or downlink requests exceeds the total time slots available at the Master. The system does not apply a check for this condition when Slaves are configured. If the time slots requested exceeds the total time slots, some Slaves will be unable to connect.

If it is important for all Slaves to be able to connect at the same time, take care not to over-subscribe the total number of time slots.

Further reading

For information about…	Refer to…
Link symmetry in synchronized PTP networks	TDD synchronization on page 1-32
Effect of link symmetry on link data throughput capacity	Calculating data rate capacity on page 3-26 Data throughput capacity tables on page 3-87
How to configure link symmetry	Wireless Configuration page on page 6-24

Dynamic time slot allocation in HCMP

Standard TDD Frame Configuration

In the Standard TDD Frame Configuration mode, the TDD frame is constructed with the number of time slots needed to support the maximum number of slaves at the configured asymmetry. For example, four Slaves and 3:1 asymmetry requires a total of 16 time slots.

If the number of Slaves connected at some time is less than the configured maximum, the surplus time slots will be temporarily assigned to the connected slaves. The temporarily assigned time slots may be reassigned in the future if a new Slave connects. It follows from this that the capacity of an HCMP link may be greater than the planned value.

The allocation of surplus time slots is on a round robin basis, aiming to provide even distribution of the surplus resources.

Note Dynamic time slot allocation is reassessed when HCMP Slaves connect or disconnect. Resources are not assigned based on traffic load or the volume of queued traffic.

Expert TDD Frame Configuration

In the Expert TDD Frame Configuration mode, the TDD frame is constructed with a configured number of uplink and downlink time slots. Time slots are assigned to Slaves when a link is established, based on the Requested Uplink Timeslots and Requested Downlink Timeslots attributes configured for the Slave.

If the sum of the requested time slots at some time is less than the total time slots available at the Master, the surplus time slots will be temporarily assigned to the connected slaves. The temporarily assigned time slots may be reassigned in the future if a new Slave connects.

The allocation of surplus time slots is on a round robin basis, aiming to provide even distribution of the surplus time slots, measured as a multiple of the requested time slots.

The allocation of surplus time slots is subject to a limit set by the Uplink Timeslot Limit and Downlink Timeslot Limit attributes.

Note Dynamic time slot allocation is reassessed when HCMP Slaves connect or disconnect. Resources are not assigned based on traffic load or the volume of queued traffic.

Note If there is no advantage in providing additional capacity to a particular Slave (for example because the link carries constant rate traffic) set the Timeslots Limit equal to the Requested Timeslots. This ensures that surplus resources are assigned to other links where there may be some benefit.

OFDM and channel bandwidth

The PTP 700 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.

In the PTP wireless topology, the channel bandwidth of the OFDM signal is configurable to one of the following values: 5, 10, 15, 20, 30, 40 and 45 MHz. Higher bandwidths provide greater link capacity at the expense of using more bandwidth. 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.

In the HCMP wireless topology, the channel bandwidth of the OFDM signal is 20 MHz or 40 MHz.

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

Further reading

For information about...	Refer to...
Channel bandwidths per frequency band	General wireless specifications on page 3-21
How to plan for channel bandwidth	Channel bandwidth on page 3-23
Effect of channel bandwidth on link data throughput capacity	Calculating data rate capacity on page 3-26 Data throughput capacity tables on page 3-87
How to configure channel bandwidth	Wireless Configuration page on page 6-24
How to monitor channel bandwidth	Spectrum Management on page 7-26

Adaptive modulation

The PTP 700 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 700 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 700 to operate in challenging non-line of sight radio channels.

Note 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.

Further reading

For information about...	Refer to...
Lowest data modulation mode	Lowest Data Modulation Mode on page 1-39

For information about...	Refer to...
Planning for adaptive modulation	Adaptive modulation on page 3-26
Effect of modulation mode on link data throughput capacity	Calculating data rate capacity on page 3-26 Data throughput capacity tables on page 3-87
Effect of modulation mode on system threshold, output power and link loss	System threshold, output power and link loss on page 3-64
How to configure modulation modes	Interface Configuration page on page 6-16 Wireless Configuration page on page 6-24 System Configuration page on page 6-42
Modulation mode when the ODU is armed	Checking that the units are armed on page 6-119
How to view the transmit and receive modulation modes	System Status page on page 7-3 Wireless Port Counters (PTP topology) on page 7-55

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 700 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 700 will adapt between two modes of operation:

- **Dual Payload**: When the radio channel conditions allow, the PTP 700 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 700.
- **Single Payload**: As the radio channel becomes more challenging, the PTP 700 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 700 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 1-20.

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.

Further reading

For information about...	Refer to...
How to configure dual or single payload	Wireless Configuration page on page 6-24
Single and dual payload modulation modes	System threshold, output power and link loss on page 3-64

Spectrum management

The spectrum management feature of the PTP 700 Series monitors the wireless spectrum and provides a real-time spectrum analyzer display to indicate the levels of interference in the available channels. This interference analysis supports a manual or automatic selection of the best operating channel.

Spectrum management measurements

The PTP 700 Series performs two signal measurements per TDD cycle. This measurement represents the mean received signal power during a 40 µs measurement period.

The Spectrum Management algorithm makes measurements using a round-robin channel selection process to collect an equal amount of measurements from each channel. The 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 Expert and Spectrum Management pages always shows a statistical summary of all channel measurement. The mean and percentile values displayed for each channel are calculated over a 20-minute statistics window period. All channel decisions are made using the values computed over the statistics window period.

Further reading

For information about...	Refer to...
How to perform spectrum management	Spectrum Management on page 7-26

RF channel selection

The PTP 700 Series supports two methods for Spectrum Management Control:

- Fixed frequency
- Dynamic Spectrum Optimization (DSO)

Master and Slave ODUs in a PTP link, or in an HCMP sector must be configured with the same setting for Spectrum Management Control.

Fixed frequency

Transmit and receive frequencies can be fixed in a PTP 700 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.

Dynamic spectrum optimization

Dynamic Spectrum Optimization (DSO) is an interference mitigation technique where the operating channel is selected based on background spectrum measurements at each of the ODUs. This is a dynamic process allowing the PTP 700 to move to a channel with a minimum level of co-channel and adjacent channel interference.

PTP topology

Two modes of DSO operation are available:

- Symmetric: the two link directions use the same frequency, determined by the Master ODU based on worst-case measurements at Master and Slave ODUs.
- Asymmetric: the frequency of operation is determined independently for each direction.

The Asymmetric mode is not permitted in radar regions.

Note Dynamic Spectrum Optimization is not supported in a PTP Hot Standby link.

HCMP topology

In the HCMP topology, only the Symmetric mode of DSO is supported. The Master ODU selects the optimum channel considering co-channel and adjacent channel interference measured in the uplink direction, together with co-channel and adjacent channel interference measured in the downlink direction and reported by each of the Slave ODUs.

Further reading

For information about...	Refer to...
Using DSO in PTP and HCMP networks	Using Dynamic Spectrum Optimization on page 1-31
Planning to use DSO	Frequency selection on page 3-23

For information about...	Refer to...
How to configure DSO	Wireless Configuration page on page 6-24
Asymmetric DSO in non-radar regions	Spectrum Management Settings on page 7-34

Slave scan in HCMP

A Slave ODU operating in the HCMP topology with Spectrum Management Control set to Fixed Frequency (meaning that DSO is disabled) provides three different approaches for determining the operating channel. These options are selected using the Slave Scan attribute:

- **Disabled:** The Slave must be configured with the same Fixed Frequency channels as the associated Master ODU. The channel is selected by management action.
- **Auto Single:** The Slave scans the selected Regulatory Band, connecting to the first suitable HCMP Master that it detects. This avoids the need to know the operating channel in advance and minimises the scan time.
- **Auto Optimum:** The Slave scans the whole of the selected Regulatory Band, connecting to the first suitable HCMP Master that it detects. This is a more reliable approach in a network where several HCMP Masters serve the same area. All Master and Slave ODUs must be configured with the same Group ID.

Note To use automatic Slave Scan in an HCMP sector, configure the HCMP Master with the same (fixed) Transmit and Receive frequencies.

Barring channels at the Slave ODU

An HCMP Slave ODU using Slave Scan provides an option to administratively bar RF channels using the Spectrum Expert page in the web-based interface. Barred channels are not scanned for Slave Scan.

If the channels used by the available Master ODUs are known, the remaining (unused) channels can be barred so that the Slave Scan considers only a small subset of channels. This approach reduces the scan time and allows Slaves to connect with less delay.

Force scan

Use the Force Scan button in the Spectrum Expert page to restart a new scan at the lowest channel. This may be useful if some aspect of the physical installation (for example antenna alignment) has been changed while the scan is in progress.

Auto optimum slave scan

The Auto Single behavior is appropriate and useful in a planned network, where the assignment of Slave ODUs to Master ODUs is unique and determined in advance.

However, other deployment models are possible, resulting in a network with a selection of Master ODUs on different RF channels but configured with the same Group ID. This situation typically occurs in the case in HCMP networks in tactical or rapidly-developing scenarios. If multiple Master ODUs are configured with the same Group ID, the first-come-first-served behavior of the standard Auto Single Scan technique can result in the Slave ignoring correctly-configured alternative Master ODUs that would have offered stronger RF signal level and/or greater unused capacity.

This problem is addressed by the Auto Optimum Slave Scan feature, allowing a Slave to survey the whole of the selected Regulatory Band, and to then select a Master based on received signal level and free capacity.

Auto Optimum Slave Scan necessarily involves an increase in scan time because the Slave cannot attempt to establish a link until the scan is complete.

Auto optimum selection method

An HCMP Slave ODU using Auto Optimum Slave Scan scans until it completes a complete scan having detected one or more correctly-configured Master ODUs. It then constructs a scan list of Masters with spare capacity, excluding from the list any Master ODU providing received signal level significantly below the level from the strongest Master. The remaining Masters in the scan list are then ranked according to spare capacity, from highest to lowest.

The threshold for excluding Masters with low receive signal level is set by the Master Receive Power Threshold attribute. If the threshold is set to a low value (say 6 dB) the selection method is predominantly based on signal strength. If the threshold is set to a high value (say 30 dB) the selection method is predominantly based on spare capacity.

In Standard TDD Frame Configuration, any Master with remaining capacity necessarily has capacity to connect at least one more Slave.

In Expert TDD Frame Configuration, the Slave additionally excludes from the scan list any Master that does not have spare capacity equal to or greater than the configured Uplink and Downlink Slots Request.

Note An HCMP Slave will not detect a Master ODU that has no remaining capacity.

Establishing a link

An HCMP Slave ODU using Auto Optimum Slave Scan attempts to connect to the highest ranked Master ODU in the scan list and, if this fails, tries the remaining Master ODUs in order until the list is exhausted. If none of the listed Master ODUs forms a link, the Slave ODU repeats the scan of the Regulatory Band.

Radar avoidance

In regions where protection of radars is part of the local regulations, the PTP 700 must detect interference from radar-like systems and avoid co-channel operation with these systems.

To meet this requirement, the PTP 700 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. Fixed frequency allocation is not recommended in radar avoidance regions, as any radar detection would cause a system outage of at least 30 minutes.

Note PTP 700 does not support Radar Avoidance in the HCMP topology.

Note Dynamic Spectrum Optimization is not supported in a Hot Standby link.

Further reading

For information about...	Refer to...
Radar avoidance in the country of operation	License keys and regulatory bands on page 1-30
Planning for mandatory radar detection	Frequency selection on page 3-23
Radar avoidance when aligning antennas	ODU installation tones on page 6-122
Effect of radar detection on spectrum management	Spectrum Expert page in radar avoidance mode on page 7-39

Access method

PTP topology

PTP 700 provides protection against accidentally establishing a PTP link to the wrong remote unit using a choice of three different access methods:

- **Link Access**: The MAC address of the remote unit must match the configured Target MAC Addess.
- **Link Name Access**: The Link Name of the remote unit must match the configured Link Name.
- **Group Access**: The Group ID of the remote unit must match the configured Group ID.

HCMP topology

In the HCMP wireless topology, PTP 700 always uses the Group Access method. The Master and Slave ODUs must all share the same Group ID.

Note The configured Access Method provides effective protection against an accidental attempt to form a link with the wrong remote unit. Use wireless encryption to protect against a malicious attempt to connect an unauthorized ODU to the wireless network.

Further reading

For information about...	Refer to...
Wireless encryption	Wireless encryption on page 1-27
Configuring Access Method	Wireless Configuration page on page 6-24
Configuring Target MAC Address	Wireless Configuration page on page 6-24
Authorization Control page	Authorization Control page on page 6-60

Wireless encryption

The PTP 700 supports optional encryption for data transmitted over the wireless link using a choice of three different encryption algorithms:

- TLS RSA: The ODUs exchange RSA certificates to authorize the remote unit and agree a randomly-generated master secret. The TLS RSA option supports unencrypted operation of the wireless link, or encryption with 128-bit or 256-bit AES.
- TLS PSK 128-bit: Both ends of the link are configured with the same 128-bit pre-shared key as a master secret. The wireless link is encrypted using 128-bit AES.
- TLS PSK 256-bit: Both ends of the link are configured with the same 256-bit pre-shared key as a master secret. The wireless link is encrypted using 256-bit AES.

The Advanced Encryption Standard (AES) is a symmetric encryption algorithm approved by U.S. Government organizations (and others) to protect sensitive information. The AES implementation in PTP 700 is approved to FIPS 197.

The use of AES encryption in PTP 700 is controlled by the AES license and enabled through the purchase of a capability upgrade.

Note Encryption Algorithm cannot be configured as TLS RSA when Access Method is Link Name Access. In this case, only the TLS PSK algorithms are supported.

TLS RSA

Wireless encryption TLS RSA can be used with the following Access Methods:

- Link Access
- Group Access

Access Method is automatically configured to Group Access in the HCMP topology.

Authentication using TLS RSA

TLS RSA uses the bidirectional exchange and verification of RSA device certificates to determine the authentic identity of both ODUs. The ODU will not form a wireless link if the encryption algorithm is TLS RSA and the certificate of the remote unit cannot be verified.

PTP 700 can be configured to use factory-installed device certificates, or user-supplied device certificates. Both ends of the link must use the same certificate type.

User-supplied device certificates must be RSA certificates with key size of 2048 bits and SHA-256, where the subject of the certificate is the MAC address of the ODU. For user-supplied certificates, each ODU must be additionally configured with a self-signed Root CA certificate that validates the device certificate of the remote ODU.

The private key for User-supplied device certificates is zeroized along with the other Critical Security Parameters (CSPs). Factory-installed certificates are in permanent memory and are never zeroized.

Authorization using TLS RSA with Link Access

When PTP 700 is configured for Wireless encryption of TLS RSA and Access Method of Link Access, the ODU will not connect unless the authenticated MAC address of the remote ODU is equal to the configured Target MAC Address attribute. The Target MAC Address authorizes the remote ODU.

Authorization using TLS RSA with Group Access

When PTP 700 is configured for Wireless encryption of TLS RSA and Access Method of Group Access, two options are available for authorizing the remote ODU. With the Whitelist option, the ODU will connect only if the authenticated MAC address of the remote unit has previously been added to a list of authorized ODUs. With the Blacklist option, the ODU will always connect unless the authenticated MAC address has previousy been added to a list of unauthorized ODUs. The Whitelist and Blacklist cannot be used at the same time. The selection of Whitelist and Blacklist is independent of the selection of Factory or User-provided certificates.

The default Blacklist/Factory combination offers limited benefits in a deployed network, since it is impossible to add all PTP 700 ODUs with Factory certificates to the Blacklist. However, this combination does provide a relatively simple way to build a network with the minimum of configuration, in applications where security is not an immediate priority, for example when evaluating wireless performance.

The Blacklist/User combination is attractive where links are to be established on an ad hoc basis, as units pre-configured with the user-supplied certificate form a closed group that is authomatically trusted, whilst only compromised units from the closed group need be added to the Blacklist.

Note Authentication is the process of verifying the identity of the remote unit that is attempting to form a connection. Authorization is the check that takes place to confirm that a unit with the authenticated identity is permitted to connect. For example, a genuine unit that is not under the control of the operator might be authenticated, but not authorized.

Negotiation of TLS RSA key size

In TLS RSA operation, the ODUs encrypt wireless traffic using the largest mutually supported key size provided in the respective AES licenses. For example, if the Master has the 256-bit AES license and the Slave has the 128-bit AES license, then the link may be encrypted using a key size of 128 bits.

PTP 700 also allows a TLS Minimum Security Level to be configured; this is the smallest key size that will be allowed in a link between Master and Slave. For example, if the Master has TLS Minimum Security Level of 128-bit AES and the Slave has no AES license then the link cannot be established.

In a network where all links must be encrypted, set TLS Minimum Security Level to TLS RSA 128-bit or TLS RSA 256-bit to prevent inadvertent connection of unencrypted links.

Further reading

For information about...	Refer to...
Description of Access Method	Access method on page 1-26
Authentication of the remote ODU	Wireless encryption on page 1-27
Licensing AES encryption	AES license on page 1-60 Capability upgrades on page 1-63
How to generate AES license keys	Generating license keys on page 6-2
How to configure AES encryption	System Configuration page on page 6-42
Configuring the Whitelist of approved ODUs for an HCMP sector.	Authorization Control page on page 6-60

TLS PSK 128-bit and TLS PSK 256-bit

Wireless Encryption TLS PSK can be used with the following Access Methods:

- Link Access
- Link Name Access
- Group Access

Access Method is automatically configured to Group Access in the HCMP topology.

Authentication and authorization in TLS PSK 128-bit or TLS PSK 256-bit occur as a single step, based on the secret pre-shared key. Bothe ends of the link must be configured for the same key size. Each unit will connect only to a remote unit that shares the same secret.

Further reading

For information about...	Refer to...
Description of Access Method	Access method on page 1-26
Authentication of the remote ODU	Wireless encryption on page 1-27
Licensing AES encryption	AES license on page 1-60 Capability upgrades on page 1-63
How to generate AES license keys	Generating license keys on page 6-2
How to configure AES encryption	System Configuration page on page 6-42

Over the air rekeying

PTP 700 provides an option for automatically refreshing the AES session keys after a configured interval. Over the air rekeying canbe used with TLS RSA or TLS PSK encryption algorithms. This capability is controlled by the Over the Air Rekey license.

Further reading

For information about...	Refer to...
General description of TLS-RSA	TLS RSA on page 1-28.
General description of TLS-PSK	TLS PSK 128-bit and TLS PSK 256-bit on page 1-29
Upgrading for Over the Air Rekey	Capability upgrades on page 1-63
Configuring Rekey Interval	System Configuration page on page 6-42

License keys and regulatory bands

The PTP 700 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 700 provides a choice between the available bands. In each regulatory band, PTP 700 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
- HCMP and/or PTP topology

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.

ODU kits (see Table 6, Table 9) provide an option to order CE-marked ODUs. CE marking indicates that the upgraded ODU complies with all applicable EU regulations including EMC, safety, hazardous materials, and wireless. CE-marked ODUs can only be used with country-specific License Keys for countries that are EU members, EEA members, or Turkey. These licenses necessarily restrict the maximum power that can be transmitted in 5 GHz bands to comply with EU regulations. Operation in 4 GHz bands is not regulated by the EU and is unchanged from the Global variant.

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

Further reading

For information about...	Refer to...
Planning PTP 700 links to conform to the regulatory band restrictions	Radio spectrum planning on page 3-21
Radio regulations in the country of operation	Compliance with radio regulations on page 4-23
How to generate a license key for the country of operation	Generating license keys on page 6-2
How to configure the regulatory band	Wireless Configuration page on page 6-24
How to view the regulatory band	System Status page on page 7-3
Regulatory band alarms	Alarms on page 7-18

Designing PTP networks

Using Dynamic Spectrum Optimization

The Dynamic Spectrum Optimization (DSO) feature allows a PTP 700 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

Synchronized networks

TDD synchronization can be used to relax constraints on the frequency planning of PTP networks. Synchronization has the following benefits:

- Allows tighter frequency re-use, and thus wider channel bandwidth.
- Allows more convenient collocation of units on a single mast.
- Allows use of smaller or lower performance antennas.
- Reduces inference, resulting in use of more efficient modulation modes.

In a correctly designed synchronised network, all links are configured with the same TDD frame duration, and the TDD frame contains guard periods longer than the propagation delay between the most distant interfering units.

Each synchronized unit is assigned to one of two phases. A master ODU can be assigned to either phase. A slave ODU must be assigned to a different phase from the associated master ODU. The phase is set by suitable configuration of TDD Frame Offset.

TDD synchronization eliminates RF interference between units in the same phase. This means that frequency planning in a synchronized network is concerned only with interference between units in different phases. Frequency planning is still necessary, but the number of potential interference paths to be considered is halved. Frequency planning in a synchronized TDD network has approximately the same level of complexity as frequency planning in a Frequency Division Duplex (FDD) network.

Further reading

For information about...	Refer to...
How to plan networks	Chapter 3: System planning, or contact your Cambium distributor or re-seller.

TDD synchronization

PTP 700 supports three hardware options for TDD Synchronization:

- **PTP-SYNC**: One PTP-SYNC unit is connected in line in the drop cable between the AC+DC Power Injector 56V and each Master ODU, close to the AC+DC Power Injector 56V. The PTP SYNC hardware option can synchronize an isolated or standalone cluster of PTP-SYNC units without a GPS receiver. An optional GPS receiver can be added to provide network-wide synchronization.
- **CMM5**: One CMM5 Power and Sync Injector provides power and optional synchronization for up to four ODUs. The Universal GPS (UGPS) receiver is always needed in synchronized networks, and network-wide synchronization is always provided when CMM5 is used for TDD synchronization.

- **Direct connection between two ODUs**: Two PTP 700 Master ODUs may be synchronized in a standalone configuration using a direct cable connection between wired Ethernet ports. There is no option in this case to synchronize with a GPS receiver, and so no possibility of network-wide synchronization. This option may be useful in an isolated 2+0 link, or at the centre point of a relay of two links using the same mast. For this option, the PSU could be the AC Power Injector 56V, the AC+DC Enhanced Power Injector 56V, or the CMM5.

PTP-SYNC

Up to ten PTP-SYNCs can be connected in a chain to share the timing signal from one timing reference.

PTP-SYNC provides two deployment options:

- An isolated or standalone cluster of PTP-SYNC units, without an external timing reference. In this case, one ODU acts as a reference for other collocated units. The associated ODUs may be synchronized with each other, but will not be synchronized with Master ODUs at other sites.
- One PTP-SYNC unit, or a cluster of several PTP-SYNC units, connected to an external timing reference, which is typically a GPS receiver. In this case, all of the associated ODUs may be synchronized with a network-wide reference, and thereby synchronized with other Master ODUs in the network. The timing reference can be from any timing system that provides a 1 Hz signal, accurately synchronized in frequency and phase with a network-wide master timing reference. GPS timing receivers are a very practical way of obtaining a suitable reference. The PTP-SYNC is compatible with the Trimble Acutime™ GG and Trimble Acutime™ Gold GPS receivers.

Attention The PTP-SYNC is compatible only with the AC+DC Power Injector 56V.

The AC Power Injector 56V and CMM5 will not work with a PTP-SYNC, and it is likely that a fuse will be blown in the PTP-SYNC if this is attempted.

PTP-SYNC is not compatible with standards-based power-over-Ethernet (PoE).

Cluster Management Module (CMM5)

The CMM5 Power and Sync Injector distributes a one pulse-per-second (1PPS) signal from the associated Universal PGS (UGPS) receiver to each of the connected ODUs. The Injector supports up to four ODUs. The synchronization signal can be daisy-chained between multiple CMM5 Power and Sync Injector units for installations with more than four collocated ODUs.

Direct connection between two ODUs

The Direct Connection option consists of one ODU configured as a free-running synchronization source, with a 1PPS output on its Aux port, and one ODU configured to receive the 1PPS signal at its Main PSU port or Aux port. The two ODUs must be interconnected using standard outdoor Cat5e cable that is gel-filled and shielded with copper-plated steel.

Configuring the TDD frame

In synchronized operation, frame duration and burst duration must be configured directly in the web-based management interface. Frame duration must be identical across all links in a synchronized network.

The PTP LINKPlanner provides a capability for computing suitable frame parameters in a synchronized network. Please refer to the *LINKPlanner User Guide* for guidance on configuring TDD synchronization.

Link symmetry is always 1:1 in synchronized PTP networks.

In the HCMP topology, frame duration is determined automatically as a function of the maximum number of Slaves and the maximum link range.

Link capacity in synchronized networks

The TDD frame duration is extended in synchronized networks to allow for the propagation delay of the longest link in the network and to incorporate additional guard periods. These guard periods protect against delayed interference from distant units in the same network.

The longer frame duration results in slightly lower link capacity than for an equivalent non-synchronized link with the same channel bandwidth and modulation mode. However, TDD synchronization also reduces interference, and this may allow operation in higher modulation modes. The benefit of operating in a higher modulation mode normally outweighs the penalty of the slightly longer TDD frame.

Links in Hot Standby

PTP links configured for Hot Standby can use extended TDD frame durations, identical to the frame durations used in HCMP topology. The longer frame duration ensures that the capacity sacrificed by operating a link in the Standby state is minimised, and the capacity of the associated Active state link is maximised.

End-to-end latency is increased when long frame durations are used.

Unprotected PTP links can be operated with the long frame durations, allowing constructions of synchronized links containing a mixture of protected and unprotected links. To use the extended frame duration, set the Long Frame Duration attribute to Enabled.

Further reading

For information about...	Refer to...
The PTP-SYNC unit	PTP-SYNC unit on page 2-32
Trimble GPS and UGPS receivers	GPS receivers on page 2-38
Typical deployment diagrams for GPS	GPS receiver interfaces on page 3-9
Choosing a site for the PTP-SYNC unit	PTP-SYNC location on page 3-15
Choosing a site for the GPS receiver	GPS receiver location on page 3-15
Use of LINKPlanner for TDD synchronization	LINKPlanner for synchronized networks on page 3-26
TDD synchronization methods that may be implemented using PTP-SYNC	Configuration options for TDD synchronization on page 3-33

For information about…	Refer to…
TDD frame duration in HCMP topology	Frame duration in HCMP topology with standard configuration on page 3-134 Frame duration in HCMP topology with expert configurationon on page 3-142
How to install a PTP-SYNC unit	Installing a PTP-SYNC unit on page 5-49
How to install an optional GPS receiver	Installing the Trimble Accutime GPS receiver on page 5-53
How to enable TDD synchronization	Wireless Configuration page on page 6-24
How to configure TDD synchronization	TDD Synchronization page (optional) on page 6-36
How to view TDD synchronization status	System Status page on page 7-3
TDD synchronization alarms	Alarms on page 7-18
How to test a PTP-SYNC installation when a fault is suspected	Testing PTP-SYNC on page 8-15

Ethernet bridging

This section describes how the PTP 700 ODU processes Ethernet data, and how Ethernet ports are allocated to the Data Service, Management Service and Local Management Service.

Ethernet ports

The PTP 700 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 56V or CMM5 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 kit.

Data and management services

The PTP 700 Series ODU supports three different types of virtual circuits providing data and management services.

- Data Service: This transparent service carries customer's data between Ethernet ports at the local ODU and Ethernet ports at an associated remote ODU.
- Management Service: This transparent service connects management systems at both ends of the link with the embedded management agents in the ODUs. The Management Service may be configured as:
    - In-Band Management
    - Out-of-Band Management
- Local Management Service: The Local Management service provides a connection to the embedded management agent, isolated from the customer data network. Management frames in the Local Management Service are not forwarded over the wireless link.

Further reading

For information about…	Refer to…
A more detailed description of the Data Service	Data Service on page 1-37
A more detailed description of the Out-of-Band Management Service	Out-of-Band Management Service on page 1-39
SFP optical or copper module kits	SFP module kits on page 2-29
The PSU, AUX and SFP ports of the ODU	ODU interfaces on page 2-10
Diagrams showing Ethernet connections	Typical deployment on page 3-2

For information about...	Refer to...
How to plan the use of Ethernet ports for customer and management traffic	Ethernet bridging on page 3-39
How to install the Ethernet interfaces to the ODU	Installing the copper Cat5e Ethernet interface on page 5-38 Installing an SFP Ethernet interface on page 5-49 Installing an Aux Ethernet interface on page 5-72
How to configure the ODU Ethernet ports	Interface Configuration page on page 6-16 LAN Configuration page on page 6-46
Ethernet port status attributes	Ethernet / Internet on page 7-7
Ethernet port alarms	Alarms on page 7-18

Ethernet switching

The ODU provides conventional Ethernet bridging between wired Ethernet ports configured for the same service, using an embedded Ethernet switch. The wired Ethernet ports may be configured as follows:

- One to three Ethernet ports may be allocated to the Data Service. If In Band Management is configured, management access shares the same set of ports.
- If Out of Band Management is configured, up to two ports may be allocated to the Management service. These ports are not used by the Data Service.
- Up to two ports can be allocated to the Local Management Service.

Data Service

Transparent Ethernet service

The PTP 700 Series provides an Ethernet service between Ethernet ports at a local ODU and 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.

There is no requirement for the customer data network to be connected to the same Ethernet ports 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 SFP and Aux ports to the customer data network at the other end of the link.

Layer two control protocols

The Data Service in the PTP 700 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 700 Series does not generate or respond to any L2CP traffic.

Quality of service for bridged Ethernet traffic

In the PTP wireless topology, the PTP 700 supports eight traffic queues in the Data Service for Ethernet frames waiting for transmission over the wireless link. In the HCMP wireless topology, the PTP 700 supports four queues for each 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 including DSCP in an IPv4 or IPv6 datagrams encapsulated in PPP and PPPoE headers, or the Traffic Class in an MPLS header.

PTP 700 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 700 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.

Data port wireless link down alert

The PTP 700 Series provides an optional indication of failure of the wireless link by means of a brief disconnection of the copper or 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.

Note PTP 700 does not support Data port wireless link down alert in the HCMP topology.

Lowest Data Modulation Mode

The PTP 700 ODU can be configured to discard Ethernet frames in the Data Service when the modulation mode is lower than the configured Lowest Data 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 Data 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 Data 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.

Further reading

For information about...	Refer to...
Factors to be considered when planning PTP 700 customer data networks	Data network planning on page 3-39
How to configure the Ethernet service	LAN Configuration page on page 6-46
How to configure Ethernet quality of service	QoS Configuration page on page 6-55
How to monitor Ethernet performance	System statistics on page 7-52

Out-of-Band Management Service

Transparent Ethernet service

The PTP 700 Series provides an optional Ethernet service for out-of-band network management between Ethernet ports at a local ODU and Ethernet ports at an associated remote ODU. The Ethernet service is based on conventional layer two transparent bridging. The PTP 700 maintains complete separation between Ethernet traffic in the customer Data Service and the Management Service.

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 management network is 2000 bytes.

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

Layer two control protocols

The Management Service in the PTP 700 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 management service in the PTP 700 Series does not generate or respond to any L2CP traffic.

Quality of service for bridged Ethernet traffic

The PTP 700 Series supports a single traffic queue in the Management Service for Ethernet frames waiting for transmission over the wireless link. The priority of the queue can be varied with respect to the eight queues used for the Data Service.

Fragmentation

Ethernet frames in the PTP 700 Series management service are always fragmented for transmission over the wireless link, even when the single queue for the management service has higher priority than all of the customer data queues.

Management port wireless Down Alert

The PTP 700 Series provides an optional indication of failure of the wireless link by means of a brief disconnection of the copper or optical data port allocated to the management 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 Data Modulation Mode

The Lowest Data Modulation Mode attribute does not prevent bridging in the management service. See Lowest Data Modulation Mode on page 1-39.

Further reading

For information about...	Refer to...
Factors to be considered when planning PTP 700 management data networks	Data network planning on page 3-39
How to configure the Ethernet service	LAN Configuration page on page 6-46
How to configure Ethernet quality of service	QoS Configuration page on page 6-55
How to monitor Ethernet performance	System statistics on page 7-52

Link protection

Ethernet switches

Hot Standby Link Protection depends on external Ethernet switches to forward Ethernet frames to the link in the Active protection state. The protection switch event in Hot Standby requires only standard Ethernet switch functions, but it does require the switch to flush entries from its Filter Database (FDB) when the ODU disconnects the Ethernet connection briefly. The FDB flush action is commonly supported by managed Ethernet switches, but is sometimes missing from basic desktop switches.

Note Ensure that external Ethernet switches used as part of a PTP Hot Standby link can be configured to flush corresponding entries in the Filter Database on disconnection of an Ethernet port.

Data bridging in the PTP link

Data bridging is disabled at the ODU wireless interface in a PTP link in the Standby protection state. This blocks end-to-end forwarding of traffic in the Data and Management services. The Management Agent in the ODU remains accessible via suitably configured wired Ethernet ports, but is not accessible via the wireless link.

Normally, the Management Agent at a remove ODU in the Standby protection state can be reached via the Active wireless link and the Ethernet switch at the remote site.

Mapping of Data and Management services

In standard non-protected operation, the embedded Ethernet switch offers relatively flexible configuration options, including the possibility of between one and three ports mapped to the Data service. When configured for Hot Standby, this flexibility is constrained as follows:

- Exactly one port must be mapped to the Data service
- Either the Aux port or SFP port must be configured as a Protection port.
- A Protection port cannot be mapped to the Data or Management services.

A consequence of this is that no more than one port can be mapped to the Management service.

Ethernet loopback mode

Note PTP 700 does not support the Ethernet loopback mode in the HCMP topology.

PTP 700 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 700 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 700 ODU. The Management Service and Local Management Service are disconnected from a port configured for loopback. 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.

Further reading

For information about…	Refer to…
How to configure Ethernet loopback	LAN Configuration page on page 6-46

Protocol model

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

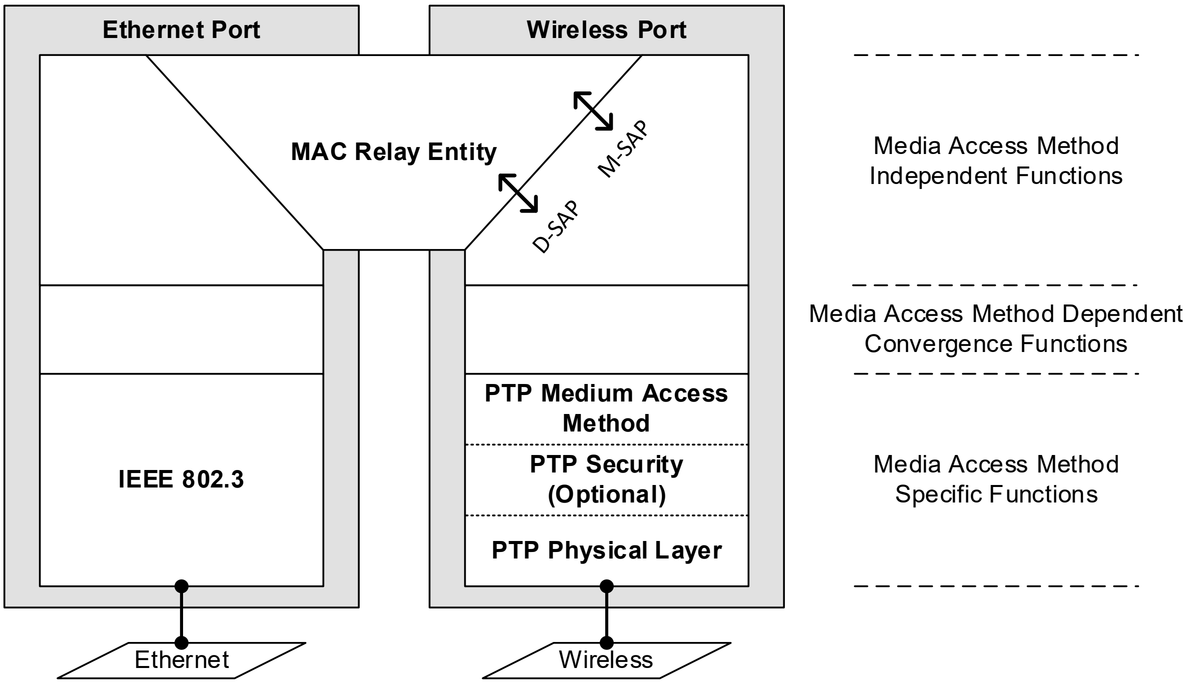
The wired ports may be allocated to the Data Service, Out-of-Band Management Service or Local Management Service. Ethernet frames are bridged between wired ports allocated to the same service. Frames are not bridged between different services.

Frames are transmitted at the Wireless port over a proprietary point-to-point circuit-mode link layer between ends of the PTP 700 link. The Wireless Port provides two distinct service access ports (SAPs) where the first is always used for the Data Service, while the second is used by the Out-of-Band Management Service.

Ethernet frames received at the Ethernet ports, or generated internally within the management agent, are encapsulated within a lightweight MAC layer for transmission over the wireless link.

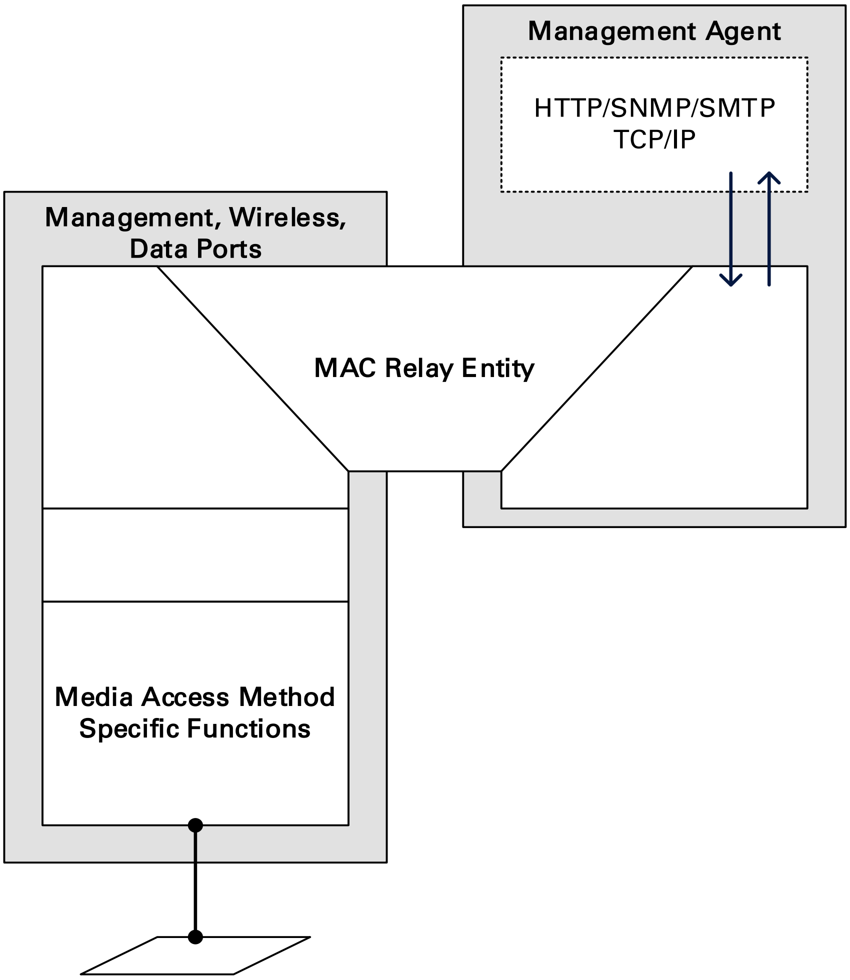
Protocol layers involved in bridging between Ethernet and wireless interfaces are shown in Figure 5. Protocol layers involved in bridging between external interfaces and the management agent are shown in Figure 6. In these figures, the layers have the meanings defined in IEEE 802.1Q-2005.

Figure 5 Protocol layers between Ethernet and wireless interfaces



D-SAP = Data Service Access Point
M-SAP = Management Service Access Point

Figure 6 Protocol layers between external interfaces and the management agent



Further reading

For information about...	Refer to...
Layer two control protocols (L2CPs) identified by PTP 700	Layer two control protocols on page 3-39

Synchronous Ethernet

Note PTP 700 does not support Synchronous Ethernet in the HCMP topology.

PTP 700 can be configured to relay a Synchronous Ethernet frequency reference across the wireless link, supporting operation as part of an ITU-T G.781 Synchronous Digital Hierarchy. A single PTP 700 link has at least two, and up to six, active Ethernet ports. When the link is synchronised to an external frequency reference, one of these active ports receives the reference (acting a Sync E slave port) and the remaining active ports transmit the frequency reference (acting as Sync E master ports).

At each end of the link, either the Main PSU port or the Fiber SFP port can be nominated as a candidate Sync E Slave Port.

In an established link, if the ODU detects a valid reference at the nominated port at the local end, or at the nominated port at the remote end, it relays the reference received at this port to all of the remaining Ethernet ports. If the ODU detects a valid reference at both ends of the link, it selects the best reference. If the ODU does not detect any valid reference at either end of the link, it operates in a free-running or holdover mode.

The nominated Sync E Slave Port can be set to Main PSU Port at one end of the link and to SFP Port at the other end of the link, forwarding the reference between two different media.

If the wireless link is down, the ODU configured as the TDD Master can relay the reference received at the nominated Sync E Slave Port to the remaining ports. The ODU configured as the TDD Slave does not forward the reference frequency until the link is established.

PTP 700 makes the selection of the best incoming reference based on the Quality Level (QL) in Synchronization Status Messages (SSMs) received at the nominated ports. SSMs are processed and transmitted as specified by ITU-T G.8264 and in Section 5 of G.781.

Note PTP 700 does not support Synchronous Ethernet on a copper SFP module.

Further reading

For information about...	Refer to...
Availability of synchronous Ethernet	Capability upgrades on page 1-63
Relationship between synchronous Ethernet and Ethernet port allocation	Additional port allocation rules on page 3-44
How to configure synchronous Ethernet	LAN Configuration page on page 6-46
Upgrading to synchronous Ethernet	Generating license keys on page 6-2
Synchronous Ethernet status indicators	Synchronous Ethernet on page 7-12
Synchronous Ethernet alarms	Alarms on page 7-18
Synchronous Ethernet status	SyncE Status page on page 7-67

IEEE 1588-2008 Transparent Clock

Note PTP 700 does not support IEEE 1588-2008 Transparent Clock in the HCMP topology.

PTP 700 is capable of operating as an IEEE 1588-2008 Transparent Clock. When operational, IEEE 1588-2008 event frames (Sync, Delay_Req, Pdelay_Req, Pdelay_Resp) have their “Correction Field” adjusted to reflect the residence time of the frame in the system. This results in greatly improved performance of downstream 1588-2008 slave clocks. The Transparent Clock feature is available at the Main PSU Port, Aux Port and at the SFP Port when a fiber SFP module is installed.

Unicast and multicast addressing models are supported, along with UDP over IPv4 or IPv6, and Ethernet communication services. The IEEE 1588 messages can be encapsulated in Untagged, C-tagged, S-tagged, S-C-tagged and C-C-tagged Ethernet frames.

Note For the most accurate residence time corrections, use Synchronous Ethernet in conjunction with the Transparent Clock feature. In this configuration, PTP 700 uses the Synchronous Ethernet clock to increase the accuracy of 1588 residence time measurements.

Note PTP 700 does not support IEEE 1588 Transparent Clock on a copper SFP module.

Further reading

For information about...	Refer to...
Availability of IEEE 1588-2008 Transparent Clock	Capability upgrades on page 1-63
Relationship between IEEE 1588-2008 Transparent Clock and Ethernet port allocation	Additional port allocation rules on page 3-44
Relationship between IEEE 1588-2008 Transparent Clock and VLAN membership	VLAN membership on page 3-47
Upgrading to IEEE 1588-2008	Generating license keys on page 6-2
How to configure IEEE 1588-2008 Transparent Clock	LAN Configuration page on page 6-46
IEEE 1588-2008 Transparent Clock status indicators	Synchronous Ethernet on page 7-12
IEEE 1588-2008 Transparent Clock alarms	Alarms on page 7-18

TDM bridging

This release of PTP 700 does not support the TDM bridging feature. TDM traffic (E1 or T1) may be carried over PTP 700 links using the Network Indoor Unit (NIDU) using System Release PTP 700-02-50.

System management

This section introduces the PTP 700 management system, including the web interface, installation, configuration, alerts and upgrades.

Management agent

PTP 700 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 network management modes. These modes are described in detail in Network management on page 1-49.

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)
- Domain Name Service (DNS)

Note PTP 700 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.

Network management

IPv4 and IPv6 interfaces

The PTP 700 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 700 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 frames of one of the following types: untagged, priority-tagged, C-tagged (IEEE 802.1Q) or S-tagged (IEEE 802.1ad). 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 DSCP priority

The management agent transmits IPv4 and IPv6 management packets with a configurable DSCP 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 DSCP 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 the Management Service or the Local Management Service.

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 the Management Service.

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 are filtered, that is, not forwarded in the customer data network or the management network.

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 the Management Service or Local Management Service. 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 700 learns the location of end stations from the source addresses in received management frames. The management agent filters transmitted management frames to ensure that each frame is transmitted at the appropriate Ethernet port, or over the wireless link as required to 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.

Further reading

For information about...	Refer to...
Planning the IP interface	IP interface on page 3-47
How to configure the IP interface	Interface Configuration page on page 6-16
How to configure the target MAC address	Wireless Configuration page on page 6-24
Planning VLAN membership	VLAN membership on page 3-47
How to configure VLAN for the management interface	Interface Configuration page on page 6-16 LAN Configuration page on page 6-46
Planning the Ethernet and IP (DSCP) priority	Priority for management traffic on page 3-47
Planning the use of Ethernet ports for customer and management traffic	Additional port allocation rules on page 3-44

IPv6

The PTP 700 management agent supports the following IPv6 features:

Neighbor discovery

PTP 700 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 700 sends router solicitations, but does not process router advertisements.

Path MTU discovery and packet size

PTP 700 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 700 supports ICMPv6 as specified in RFC 4443. PTP 700 does not support RFC 4884 (multi-part messages).

Addressing

The PTP 700 management agent is compatible with the IPv6 addressing architecture specified in RFC 4291. PTP 700 allows static configuration of the following:

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

PTP 700 additionally assigns an automatically configured Link Local address using stateless address auto-configuration (SLAAC) as specified in RFC 4862. PTP 700 does not assign a global unicast IP address using SLAAC.

PTP 700 responds on the standard management agent interfaces (HTTP, HTTPS, syslog, Telnet, SNMP, SMTP, SNTP) using the global unicast address.

Privacy extensions

PTP 700 does not support the privacy extensions specified in RFC 4941.

DHCPv6

PTP 700 does not support address assignment using DHCPv6. The address of the management agent must be configured statically.

Multicast listener discovery for IPv6

The PTP 700 management agent supports Multicast Listener Discovery version 1 (MLDv1) as specified in RFC 2710.

PTP 700 does not support Multicast Listener Discovery version 2 (MLDv2).

Textual representation of IPv6 addresses

PTP 700 allows users to input text-based IP addresses in any valid format defined in RFC 5952. IPv6 addresses are automatically converted by PTP 700 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 700 does not support IP security (IPsec).

Further reading

For information about...	Refer to...
Planning the IPv6 interface	IP interface on page 3-47
How to enable IPv6 capability	Software License Key page on page 6-13
How to configure IPv6	Interface Configuration page on page 6-16 LAN Configuration page on page 6-46

Web server

The PTP 700 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 700 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 700.

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 700.
- **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 700 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 700 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 700 unit. PTP 700 supports certificates with 2048-bit key size.

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

Note The PTP 700 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 700 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 700 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 700 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 700 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 700 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 is automatically and permanently disabled in the FIPS 140-2 mode.

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.

Further reading

For information about...	Refer to...
How to log in and use the menu	Using the web interface on page 6-6
Planning the security material needed for HTTPS/TLS.	Security planning on page 3-53

For information about...	Refer to...
How to configure user accounts	Local User Accounts page on page 6-70

cnMaestro device agent

The cnMaestro Wireless Network Management System is a cloud-based or on-premises software platform for secure, end-to-end network control. cnMaestro wireless network manager simplifies device management by offering full network visibility and zero touch provisioning.

The PTP 700 management agent includes the device agent function for cnMaestro. The device agent implementation in PTP 700 provides Fault Management and Performance Management. Support for additional functional areas may be introduced in later releases.

The device agent shares a common IP interface with the remaining management protocols (HTTP, HTTPS, SNMP, SMTP, syslog, RADIUS).

PTP 700 makes an outgoing connection to the cnMaestro server using the WebSocket Secure protocol. The connection between the PTP 700 and the cnMaestro server is encrypted using AES.

The cnMaestro server address is configured in the PTP 700 as follows:

- Cloud cnMaestro Server: Pre-configured Fully Qualified Domain Name (FQDN)
- On-Premises cnMaestro Server: Static IPv4 address or FQDN

PTP 700 supports the following Onboarding Methods:

- Cloud cnMaestro Server: Serial Number, Cambium ID
- On-Premises cnMaestro Server: MAC Address, Cambium ID, Auto

The device identity is authenticated to the server as follows:

- Serial number: Random characters embedded in the serial number
- MAC address: MAC address pre-configured in the cnMaestro server
- Cambium ID: Onboarding key.

The cnMaestro device agent operates in ODUs configured as PTP Master, PTP Slave, HCMP Master and HCMP Slave. Master devices do not act as proxy agents for the associated Slave devices. All ODUs must be configured for connection to the cnMaestro server.

RADIUS authentication

PTP 700 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 700 supports connections to primary and secondary RADIUS servers. The RADIUS interface is configured through the RADIUS Authentication page of the web-based interfaces.

PTP 700 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 700 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 700 is configured for Identity-based User Accounts.

Note The RADIUS feature is disabled in FIPS 140-2 approved mode.

Further reading

For information about...	Refer to...
How to plan the use of RADIUS	Planning for RADIUS operation on page 3-61
How to configure RADIUS.	RADIUS Configuration page on page 6-75

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 700 Series proprietary MIB.

Further reading

For information about...	Refer to...
How to plan for SNMPv1/2c	Planning for SNMP operation on page 3-50

For information about…	Refer to…
How to enable SNMP control of HTTP, Telnet and passwords	Web-Based Management page on page 6-68 HTTP and Telnet options on page 6-111.
How to configure SNMPv1 or SNMPv2c	SNMP pages (for SNMPv1/2c) on page 6-97
How to upgrade software remotely using Trivial FTP (TFTP) triggered by SNMP	Upgrading software using TFTP on page 6-128

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 700 can be configured to authenticate received NTP messages using an MD5 or SHA-1 signature.

Further reading

For information about…	Refer to…
How to plan for SNTP operation	Planning for SNTP operation on page 3-53
How to configure SNTP	Time Configuration page on page 6-82

SNMPv3 security

SNMP Engine ID

PTP 700 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 700 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 700 AES upgrade described in AES license on page 1-60.

View-based access control model

PTP 700 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 700 except for the security configuration of SNMPv3 itself. 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.

MIB-based management of SNMPv3 security

PTP 700 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 700 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 3-59.

PTP 700 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 1-57. 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 700 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 700 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 reset all configuration and entering new configuration.

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

Further reading

For information about...	Refer to...
How to plan for SNMPv3 operation	Planning for SNMPv3 operation on page 3-57
How to configure SNMPv3	SNMP pages (for SNMPv3) on page 6-88

System logging (syslog)

PTP 700 supports the standard syslog protocol to log important configuration changes, status changes and events. The protocol complies with RFC 3164.

PTP 700 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 700 additionally creates syslog messages for changes in any status variable displayed in the web-based interface.

PTP 700 creates syslog messages on a number of events (for example successful and unsuccessful attempts to log in to the web-based interface).

PTP 700 can be configured to send syslog messages to one or two standard syslog servers.

Additionally, PTP 700 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.

Further reading

For information about...	Refer to...
Configuring system logging	Syslog Configuration page on page 6-86
Syslog alarms	Alarms on page 7-18
How to view the local log of event messages	Syslog page on page 7-22
How to interpret syslog messages	Format of syslog server messages on page 7-23

Domain Name Service (DNS)

The PTP 700 Management Agent supports use of an external DNS server to resolve the Domain Name configured for network management servers to IPv4 or IPv6 addresses. PTP 700 allows the configuration of a primary DNS server and optionally a second DNS server.

When DNS is enabled and configured, the following server addresses can be configured as a Fully Qualified Domain Name (FQDN):

- cnMaestro Server
- RADIUS Server
- SMTP Server
- SNMP Trap
- SNTP Server
- Syslog Server
- TFTP Server

The FQDN must comply with the following:

- Not longer than 63 characters
- Must contain some structure (at least one “.”)
- Must consist of only the characters “0”..”9”, “a”..”z”, “A”..”Z”, "$", hyphen, underscore, dot/stop, plus, exclamation, star, single quote, left parenthesis, right parenthesis

Instant messaging

PTP 700 provides a simple text-based messaging service between the ODUs in a link. The Instant Messaging interface can be used to send messages to a technician or operator at the remote end of the link. The messaging service does not depend on external servers and can be used as soon as basic connectivity is achieved.

The maximum message size is 180 characters.

Unread messages are indicated by an alert in the Status Bar of the web-based interface.

AES license

PTP 700 provides optional encryption using the Advanced Encryption Standard (AES). Encryption is not available in the standard PTP 700 system.

AES upgrades are purchased from your Cambium Point-to-Point distributor or solutions provider. The upgrade authorizes AES operation for one ODU. Two upgrades are needed to operate AES on a link.

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.

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.

Wireless encryption can be configured for TLS RSA, TLS PSK 128-bit, or TLS PSK 256-bit algorithms. TLS RSA uses factory installed or user-supplied RSA device certificates to authorize remote units and agree a randomly-generated master secret. TLS RSA automatically uses the largest key size mutually supported by licensing at the two ends of the link. TLS PSK algorithms using a 128-bit or 256-bit pre-shared key are available only if the associated key size is supported by licensing at both ends of the link.

AES encryption for SNMPv3 or TLS is always based on a 128-bit key, regardless of level enabled in the PTP 700 license key.

Note that the connection between the PTP 700 and the cnMaestro server is always encrypted using AES. The optional AES license is not required for secure operation with cnMaestro.

Further reading

For information about...	Refer to...
General description of wireless encryption in PTP 700	Wireless encryption on page 1-27
Capability upgrades for AES	Capability upgrades on page 1-63
AES and HTTPS/TLS operation	Planning for HTTPS/TLS operation on page 3-57
AES and SNMPv3 operation	Planning for SNMPv3 operation on page 3-57
How to generate an AES license key	Generating license keys on page 6-2
How to enable AES capability	Software License Key page on page 6-13
How to configure AES encryption	System Configuration page on page 6-42
How to configure security with AES	Security menu on page 6-101

Critical security parameters

The critical security parameters (CSPs) are as follows:

- Key of keys.
- Entropy seed.
- AES encryption keys for the wireless interface.
- Private key for the HTTPS/TLS interface.
- User account passwords for the web-based interface.
- Private key for user-supplied device certificates.

- SNTP server keys for SHA1
- SNMPv3 USM authentication keys
- SNMPv3 USM privacy keys

CSPs can be reset (zeroized) along with other security-related attributes using the web-based interface.

Further reading

For information about...	Refer to...
How to zeroize CSPs	Zeroize CSPs page on page 6-115
How to zeroize CSPs (recovery mode)	Zeroize Critical Security Parameters on page 7-79

Software upgrade

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

PTP 700 software images are digitally signed, and the ODU will accept only images that contain a valid Cambium Networks 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.

Attention 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.

Attention Take care when upgrading ODU software using the wireless link to a remote ODU. Upgrade the remote unit first, reboot the remote ODU, and then upgrade the local unit to the same software version.

Further reading

For information about...	Refer to...
How to upgrade the software using the web interface	Software Upgrade page on page 6-64
How to upgrade software remotely using Trivial FTP (TFTP) triggered by SNMP	Upgrading software using TFTP on page 6-128

Capability upgrades

ODUs are shipped with a default License Key factory-installed. The default license key enables a limited set of capabilities which depend upon the ODU variant.

Capability upgrades are purchased from Cambium and supplied as an Entitlement Certificate, delivered by email. One Entitlement Certificate can deliver multiple upgrades. Follow the instructions in the certificate to redeem the purchased upgrade products at the Cambium Support Center.

Individual upgrades can then be activated by specifying the MAC address of a PTP 700 ODU. For each upgrade activated, the Support Center creates a new license key and delivers it by email. Install the license key using the ODU web interface to enable the purchased capability in the ODU.

Note License keys are bound to a single ODU and are not transferrable.

Further reading

For information about…	Refer to…
Capabilities of the PTP 700 Connectorized ODU	PTP 700 Connectorized ODU on page 2-5
Capabilities of the PTP 700 Connectorized+Integrated ODU	PTP 700 Connectorized+Integrated ODU on page 2-3
Ordering capability upgrades	ODU capability upgrades on page 2-7
How to obtain License Keys	Generating license keys on page 6-2
How to install capability upgrades	Software License Key page on page 6-13

Full capability trial period

A full capability trial period is available for PTP 700 units that are licensed for “Lite” (up to 225 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 capability afterwards. The trial period can be started, paused and resumed from the web interface.

Note PTP 700 does not support HCMP topology in units with the Lite capability, and the trial period is therefore not applicable to HCMP operation.

Further reading

For information about...	Refer to...
How to control the trial period	Software License Key page on page 6-13

Recovery mode

The PTP 700 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, and with default link settings. 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, Ethernet and security configuration
- Reset IP and Ethernet configuration.
- Reset (zeroize) critical security parameters.
- Reboot with existing software and configuration.

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.

Further reading

For information about...	Refer to...
How to recover from configuration errors or software image corruption	Recovery mode on page 7-73

Upgrade from earlier releases

PTP topology

To upgrade a PTP link to 700-02-67, upload the new firmware to the ODUs at the two ends of the link, program the firmware image into non-volatile memory in the two ODUs, and then reboot both ODUs together.

HCMP topology

To upgrade an HCMP sector from 700-02-65 to 700-02-67 use the following process:

- Upload firmware from 700-02-67 into the Master ODU, program the firmware image into non-volatile memory, and then reboot the Master ODU. At this stage, the Master ODU will be using 700-02-67 and the Slave ODUs will be using 700-02-65.
- Upload firmware from 700-02-67 into one of the Slave ODUs, program the firmware image into non-volatile memory, and then reboot this ODU. At this stage, the Slave ODUs will be a mixed population with 700-02-65 and 700-02-67.
- Repeat the previous step for the remaining Slave ODUs. At this stage all the (Master and Slave) ODUs in the sector will be operating with 700-02-67.

Note Do not install new Slave ODUs, or make further configuration changes, until all the Slave ODUs have been upgraded.

Note Upgrade new Slave ODUs with earlier firmware to 700-02-67 before installing on the upgraded Master ODU.

FIPS 140-2 mode

This section describes the (optional) FIPS 140-2 cryptographic mode of operation.

PTP 700 provides an optional secure cryptographic mode of operation that complies with the requirements for Level 2 of Federal Information Processing Standards (FIPS) Publication 140-2.

FIPS 140-2 approved mode

PTP 700 operates in the FIPS 140-2 approved mode whenever the special FIPS software is installed in the PTP 700 ODU.

Attention Use the following NIST web site to confirm that the FIPS software has been validated:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

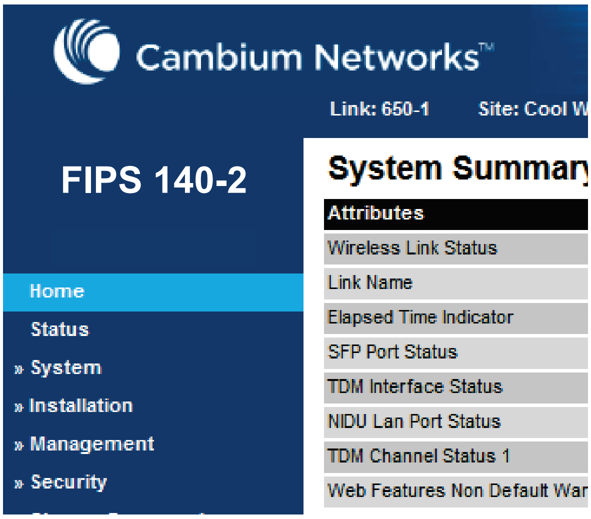
The special FIPS software image can be identified by a `FIPS-` prefix to the filename, for example: `FIPS-PTP700-01-00.DLD2`.

Note PTP 700 will not upload the FIPS software unless the unit is licensed for 128-bit or 256-bit AES encryption and for FIPS operation.

Indication of FIPS 140-2 approved mode

The FIPS 140-2 approved mode is indicated by the "FIPS 140-2" text displayed at the top of the navigation bar in the web-based interface, as shown in Figure 7.

Figure 7 Indication of FIPS 140-2 capability



Enforced configuration in FIPS approved mode

When the PTP 700 ODU operates in the FIPS approved mode, the following configuration settings are automatically enforced:

- Identity-based user accounts is Enabled.
- Telnet management interface is Disabled.
- SNMP control of HTTP and Telnet is Disabled.
- SNMP control of passwords is Disabled.
- TFTP client is Disabled.
- RADIUS client is Disabled.
- Minimum Password Length ≥ 8.
- Device Certificate is User.

In addition, the License Key must have a valid 2048-bit DSA signature.

Secure mode alarm

The Secure mode alarm indicates that the unit is operating in the FIPS approved mode, but that it has not been configured correctly for FIPS 140-2 operation. The secure mode alarm appears in the System Summary page as shown in Figure 8.

Figure 8 Secure mode alarm in the System Summary page

System Summary

Attributes	Value	Units
Wireless Link Status	Searching	
Link Name	Pikes Peak to Cripple Creek	
Elapsed Time Indicator	00:01:01	
Secure Mode Alarm	Secure Mode Is Not Configured	

The Secure mode alarm is also displayed in the first page of the Security Wizard as shown in Figure 9.

Figure 9 Secure mode alarm in the Security Wizard

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
Secure Mode Alarm	Secure Mode Is Not Configured	
Key of Keys	Not configured	
Private Key	Not configured	
Public Certificate	Not configured	

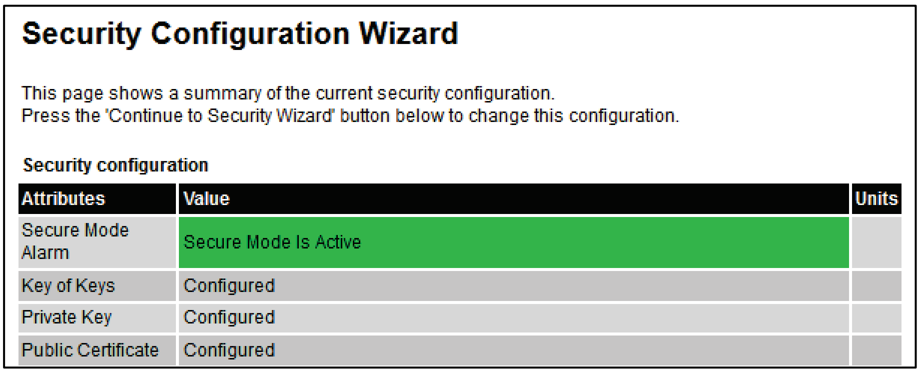
Security configuration for FIPS approved mode

The security configuration for the FIPS approved mode consists of the following:

- Key of keys (128-bit or 256-bit to match the AES license)
- Entropy (512-bit)
- The HTTPS/TLS management interface must be correctly configured, including:
    - Private key (2048-bit RSA key size)
    - Public key certificate (2048-bit RSA key size, signed using SHA-256 Secure Hash Algorithm)
- The HTTP management interface must be Disabled
- AES encryption must be configured and enabled at the wireless interface.
- Passwords must be configured (with minimum length eight characters) for enabled accounts in the web-based interface.

When the security configuration is completed correctly, the Secure mode alarm is cleared from the System Summary page and the Security Wizard displays the Active state as shown in Figure 10.

Figure 10 Secure mode active



Further reading

For information about...	Refer to...
Cryptographic material needed for FIPS operation	Planning for FIPS 140-2 operation on page 3-62
Installing license keys	Software License Key page on page 6-13
Loading software images	Software Upgrade page on page 6-65
Configuring the ODU for FIPS operation	Configuring security for FIPS 140-2 applications on page 6-116

Exiting from the FIPS operational state

A PTP 700 ODU in the FIPS operation state can be prepared to accept new security configuration by zeroizing critical security parameters (CSPs). The unit remains in the FIPS approved mode.

Further reading

For information about...	Refer to...
Zeroizing the CSPs	Zeroize CSPs page on page 6-115

Reverting to the standard (non-FIPS) mode

A FIPS 140-2 capable ODU can be used in standard (non-FIPS) mode by loading a standard (non-FIPS) software image and rebooting.

The critical security parameters (CSPs) are zeroized when the unit is no longer FIPS 140-2 capable.

Further reading

For information about...	Refer to...
Exiting the FIPS approved mode	Managing security on page 7-51

Chapter 2: System hardware

This chapter describes the hardware components of a PTP 700 link.

The following topics are described in this chapter:

Outdoor unit (ODU)

ODU description

The ODU is a self-contained transceiver unit that houses both radio and networking electronics.

Two ODUs are required for a PTP link.

One ODU is required as a Master in an HCMP sector, with up to eight ODUs configured as Slaves.

Hardware platform variants

PTP 700 ODUs are available in two different hardware platform variants:

- PTP 700 Connectorized+Integrated ODU
- PTP 700 Connectorized ODU

The Connectorized and Connectorized+Integrated ODUs are available in three color schemes:

- White
- Green
- Desert Tan

Regional variants

PTP 700 ODUs are available as a Global variant. The default License Key for country "Other" supports the following regulatory bands:

- 8 "5.4 GHz unrestricted"
- 35 "5.8 GHz unrestricted"
- 61 "4.9 GHz unrestricted"
- 62 "5.2 GHz unrestricted"
- 81 "4.7 GHz NATO Band IV"

ODUs may be configured for individual country licenses. Refer to Generating license keys on page 6-2 and Software License Key page on page 6-13. The list of available regulatory bands depends on the country.

ODU kits (see Table 6, Table 9) provide an option to order CE-marked ODUs. CE marking indicates that the upgraded ODU complies with all applicable EU regulations including EMC, safety, hazardous materials, and wireless. CE-marked ODUs can only be used with country-specific License Keys for countries that are EU members, EEA members, or Turkey. These licenses necessarily restrict the maximum power that can be transmitted in 5 GHz bands to comply with EU regulations. Operation in 4 GHz bands is not regulated by the EU and is unchanged from the Global variant.

Capacity variants

Some of the PTP 700 ODU variants were previously available with a Lite capacity license. The Lite capacity variant is no longer available from Cambium Networks. Existing ODUs licensed for Lite capacity can be operated at the reduced capacity, or can be licensed for the Full capacity by purchase of an upgrade (see ODU capability upgrades on page 2-7).

PTP 700 Connectorized+Integrated ODU

The PTP 700 Connectorized+Integrated ODU provides a choice between using external antennas, similar to the Connectorized ODU, or a 22 dBi integrated antenna (Figure 11 and Figure 12). The integrated antenna offers a convenient and easily-deployed solution where the additional gain of external antennas is not needed.

Figure 11 PTP 700 Connectorized+Integrated ODU – White (front and rear views)

Figure 12 PTP 700 Connectorized+Integrated ODU –Desert Tan (front and rear views)

Capacity and capability licensing

PTP 700 ODUs are available with “Lite” data throughput capability (up to 225 Mbps) or “Full” data throughput capability (up to 450 Mbps). ODUs additionally support the following capability upgrades (see ODU capability upgrades on page 2-7):

- Data throughput above 225 Mbps
- SFP port operation

- AES encryption
- Synchronous Ethernet and 1588 Transparent Clock
- Group access
- High-Capacity Multipoint (HCMP)
- Over-the air rekeying

Note The HCMP upgrade can only be applied to ODUs that already have the Full capacity license.

Full capability trial period

A full capability trial period is available for PTP 700 ODUs that are licensed for “Lite” (up to 225 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 Lite capability afterwards. The trial period can be started, paused and resumed from the web interface (Software License Key page on page 6-13).

Note The HCMP upgrade can only be applied to ODUs that already have the Full capacity license, and so the Full capability trial does not apply to ODUs operating in the HCMP topology.

Individual ODU part numbers

Order PTP 700 Connectorized+Integrated ODUs from Cambium Networks (Table 4). ODUs are supplied without mounting brackets.

Table 4 PTP 700 Connectorized+Integrated individual ODU part numbers

Cambium description	Cambium part number
PTP 700 Connectorized+Integrated ODU (Global) – White	C045070B004A
PTP 700 Connectorized+Integrated ODU (Global) – Green	C045070B038A
PTP 700 Connectorized+Integrated ODU (Global) – Desert Tan	C045070B040A

The Lite capacity ODU (Table 5) is no longer available from Cambium Networks. Existing Lite capacity ODUs are supported in the PTP 700 firmware and can be upgraded to the Full capacity license (see ODU capability upgrades on page 2-7).

Table 5 PTP 700 Lite Connectorized+Integrated individual ODU part numbers

Cambium description	Cambium part number
PTP 700 Lite Connectorized+Integrated ODU (Global) – White	C045070B010A

ODU kit part numbers

Order PTP 700 Connectorized+Integrated ODU kits from Cambium Networks (Table 6).

Each of the parts listed in Table 6 includes the following items:

- One Connectorized+Integrated ODU (Global).
- Upgrade to apply CE marking to the ODU.

Table 6 ODU kit part numbers for Connectorized+Integrated ODUs

Cambium description	Cambium part number
PTP 700 Connectorized+Integrated ODU with CE mark – White	C045070H032A
PTP 700 Connectorized+Integrated ODU with CE mark – Green	C045070H034A
PTP 700 Connectorized+Integrated ODU with CE mark – Desert Tan	C045070H036A

PTP 700 Connectorized ODU

The PTP 700 Connectorized ODU is intended to work with separately mounted external antennas (Figure 13). External antennas generally have higher gains than the integrated antennas, allowing the PTP 700 to cope with more difficult radio conditions.

Figure 13 PTP 700 Connectorized ODU – White (front and rear views)

Figure 14 PTP 700 Connectorized ODU – Green (front and rear views)

Note To determine when to install external antennas and to calculate their impact on link performance and regulatory limits, see Planning for connectorized units on page 3-31.

To select antennas, RF cables and connectors for connectorized units, see Antennas and antenna cabling on page 2-21.

Capacity and capability licensing

PTP 700 ODUs are available with “Lite” data throughput capability (up to 225 Mbps) or “Full” data throughput capability (up to 450 Mbps). ODUs additionally support the following capability upgrades (see ODU capability upgrades on page 2-7):

- Data throughput above 225 Mbps
- SFP port operation
- AES encryption
- Synchronous Ethernet and 1588 Transparent Clock
- Group access
- High-Capacity Multipoint (HCMP)
- Over-the air rekeying

Full capability trial period

A full capability trial period is available for PTP 700 ODUs that are licensed for “Lite” (up to 225 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 Lite capability afterwards. The trial period can be started, paused and resumed from the web interface (Software License Key page on page 6-13).

Individual ODU part numbers

Order PTP 700 Connectorized ODUs from Cambium Networks (Table 7). ODUs are supplied without mounting brackets.

Table 7 PTP 700 Connectorized individual ODU part numbers

Cambium description	Cambium part number
PTP 700 Connectorized ODU (Global) – White	C045070B003B
PTP 700 Connectorized ODU (Global) – Green	C045070B034A
PTP 700 Connectorized ODU (Global) – Desert Tan	C045070B039A

The Lite capacity ODU (Table 8) is no longer available from Cambium Networks. Existing Lite capacity ODUs are supported in the PTP 700 firmware and can be upgraded to the Full capacity license (see ODU capability upgrades on page 2-7).

Table 8 PTP 700 Lite Connectorized+Integrated individual ODU part numbers

Cambium description	Cambium part number
PTP 700 Lite Connectorized ODU (Global) – White	C045070B009B

ODU kit part numbers

Order PTP 700 Connectorized ODU kits from Cambium Networks (Table 9).

The part listed in Table 9 includes the following items:

- One Connectorized ODU (Global).
- Upgrade to apply CE marking to the ODU.

Table 9 ODU kit part numbers for Connectorized ODUs

Cambium description	Cambium part number
PTP 700 Connectorized ODU with CE mark – White	C045070H031A
PTP 700 Connectorized ODU with CE mark – Green	C045070H033A
PTP 700 Connectorized ODU with CE mark – Desert Tan	C045070H035A

ODU capability upgrades

To upgrade a PTP 700 ODU to one or more new capabilities, order the necessary upgrades from Cambium Networks (Table 10). For details of how to install the capability upgrades, refer to Generating license keys on page 6-2 and Software License Key page on page 6-13.

Table 10 Capability upgrades available for PTP 700 Series ODUs

Cambium description	Part number
PTP 700 128-bit AES Encryption – per END (*1)	C000070K001A
PTP 700 256-bit AES Encryption – per END (*1)	C000070K002A
PTP 700 Precise Network Timing Software License – per END	C000070K003A

Cambium description	Part number
PTP 700 Group Access Software License – per END	C000070K004A
PTP 700 FIPS 140-2 Upgrade including 128-bit AES – per END	C000070K005A
PTP 700 FIPS 140-2 Upgrade including 256-bit AES – per END	C000070K006A
PTP 700 Lite to Full Upgrade – per END	C000070K008A
PTP 700 High Capacity Multipoint Upgrade – per END (*2)	C000070K009A
PTP 700 Over-the-Air Rekey License (*3)	C000070K013A
Global to CE Conversion Kit (*4)	C045070K001A

(*1) Cambium Networks will supply AES upgrades only if there is official permission to export AES encryption to the country of operation.

(*2) Order one upgrade for every ODU that will be used as a TDD Master or TDD Slave in an HCMP sector. The HCMP upgrade can only be applied to ODUs that already have the Full capacity license.

(*3) Order one upgrade for every ODU that will be used as a TDD Master in an HCMP sector or PTP link.

(*4) The upgrade to apply CE marking is applied in the Distribution Centre when the ODU is ordered as part of an ODU Kit (C045070H031A, C045070H032A, C045070H033A, C045070H034A, C045070H035A, C045070H036A). The conversion kit (C045070K001A) cannot be ordered separately.

ODU accessories

Spare ODU port blanking plugs are available from Cambium Networks (Table 11).

Table 11 ODU accessory part numbers

Cambium description	Cambium part number
Blanking Plug Pack (Qty 10)	N000065L036A

ODU mounting brackets

The Tilt Bracket Assembly (Figure 15) and Mounting Bracket (Integrated) bracket (Figure 16) are used to mount a PTP 700 ODU on a pole with diameter in the range 40 mm to 80 mm (1.6 inches to 3.1 inches). The Tilt Bracket Assembly may be used with third-party band clamps to mount an ODU on pole with diameter in the range 90 mm to 230 mm (3.6 inches to 9.0 inches).

Order ODU mounting brackets from Cambium Networks (Table 12).

Figure 15 ODU Tilt Bracket Assembly

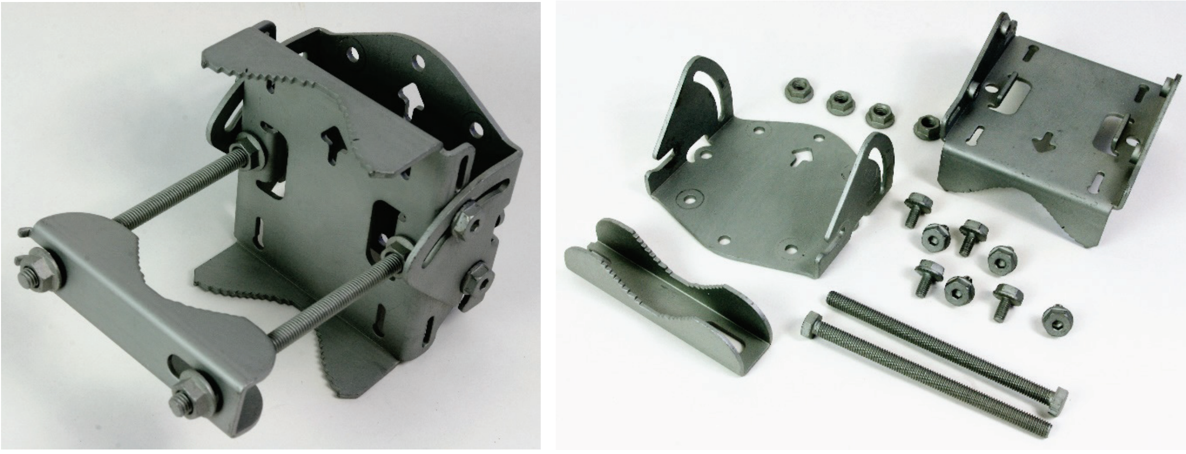


Figure 16 ODU Mounting Bracket (Integrated)

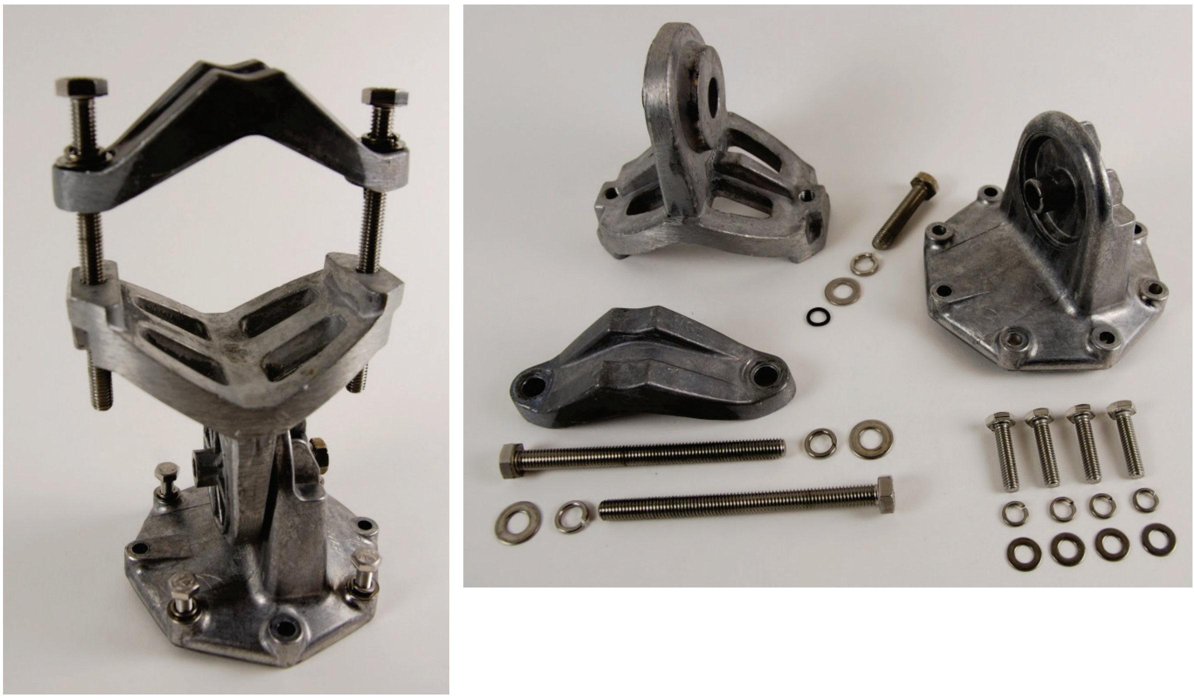


Table 12 ODU mounting bracket part numbers

Bracket	ODU variants	Bracket part number
Tilt Bracket Assembly	PTP 700 Connectorized+Integrated PTP 700 Connectorized	N000045L002A
Mounting Bracket (Integrated)	PTP 700 Connectorized+Integrated	N000065L031A

ODU interfaces

The PSU, AUX and SFP ports are on the rear of the ODUs (Figure 17). These interfaces are described in Table 13. Each of the PSU, AUX and SFP ports can be configured to disable Ethernet traffic, connected in a local loop-back between any two ports, or selected to the following services:

- Data Service
- Management Service
- Local Management Service

Figure 17 ODU rear interfaces

Table 13 ODU rear interfaces

Port name	Connector	Interface	Description
Main 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. Data and Management Services.
SFP	SFP	Optical or Copper Gigabit Ethernet	Data and Management Services. Plug-in SFP module must be purchased separately.

The front of the connectorized ODU (Figure 18) provides N type female connectors for RF cable interfaces to antennas with horizontal (H) and vertical (V) polarization.

Figure 18 Connectorized ODU antenna interfaces

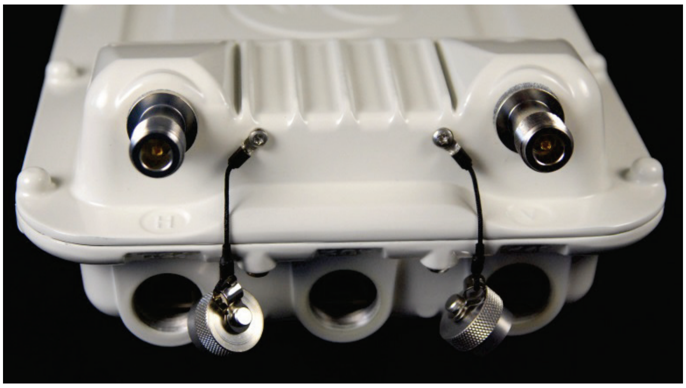


Figure 19 Connectorized+Integrated ODU antenna interfaces

ODU specifications

The PTP 700 ODU conforms to the specifications listed in Table 14.

Table 14 ODU specifications

Category	Specification
Dimensions	Connectorized+Integrated: 371 mm (14.6 in) x 430 mm (16.9 in) x 98 mm (3.9 in) Connectorized: 204 mm (8.0 in) x 318 mm (12.5 in) x 98 mm (3.9 in)
Weight	Connectorized+Integrated: 4.1 kg (9.0 lbs) excluding bracket Connectorized: 3.1 Kg (6.8 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 3-14.
Humidity	100% condensing
Liquid and particle ingress	IP66, IP67
UV exposure	10 year operational life (UL746C test evidence)
Static discharge	See Electromagnetic compatibility (EMC) compliance on page 4-20

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:

- The AC+DC Enhanced Power Injector 56V (Figure 20) supplies a single ODU, accepts both AC and DC input, 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. The AC+DC Power Injector 56V is approved for use with the 4.8 GHz to 5.9 GHz, and 4.9 GHz to 6.05 GHz frequency variants of the ODU.
- The Cluster Management Module (CMM5) (Figure 21, Figure 22 and Figure 23) is a modular system that powers ODUs and distributes a synchronization signal to TDD Master ODUs. CMM5 consists of the following components:
    - CMM5 Power and Sync Injector 56 Volts: Each Injector supplies power to up to four PTP 700 ODUs and operates from a 48 V DC input.
    - Optional 240 W Power Supply: An AC/DC converter with 48 V DC output. The 240 W variant supplies power for up to four PTP 700 ODUs. Use one Power Supply for each Power and Sync Injector.
    - Optional CMM5 Controller Module: The Controller Module is used to monitor and configure a CMM5 system consisting of one or more Power and Sync Injectors, associated Power Supplies and a UGPS receiver.
    - Optional Universal GPS (UGPS): An outdoor GPS receiver optimized for synchronization. One UGPS can synchronize several Power and Sync Injectors.

Note The CMM5 Power and Sync Injector is also available with a 29 V output. This variant is not suitable for use with PTP 700.

Figure 20 AC+DC Enhanced Power Injector 56V

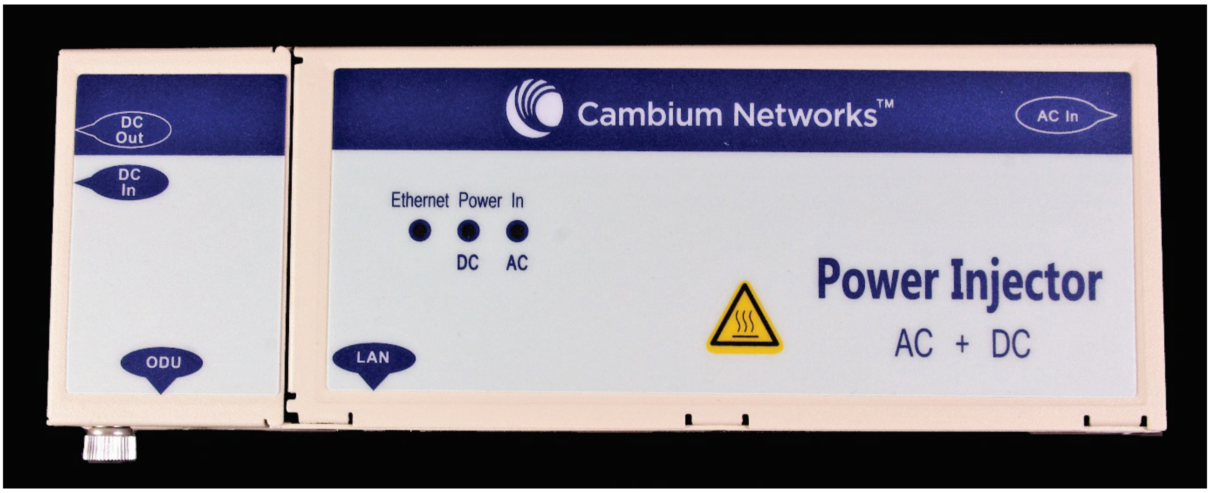
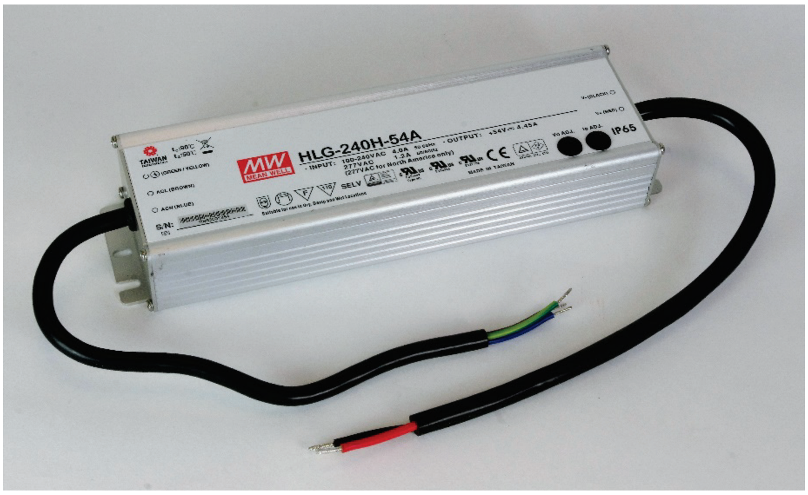


Figure 21 CMM5 Power and Sync Injector

Figure 22 CMM5 Controller

Figure 23 CMM5 240 watt AC/DC Power Supply



Warning Always use an appropriately rated and approved AC supply cord-set in accordance with the regulations of the country of use.

Attention The PSU ODU ports are designed to connect only to PTP 700 ODUs, PTP-SYNC units, 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 700 ODU or LPU.

Note Each of the ODU kits listed in Table 6 includes one PSU and one US or EU line cord as stated in the Cambium description.

Further reading

For information about…	Refer to…
General description of TDD Synchronization	TDD synchronization on page 1-32

For information about…	Refer to…
Further details of the CMM5	*PMP Syncronization Solutions User Guide*
Further details of the UGPS	*PMP Syncronization Solutions User Guide*

PSU part numbers

Order PSUs and (for AC power) line cords from Cambium Networks (Table 15).

Table 15 Power supply component part numbers

Cambium description	Cambium part number
AC+DC Enhanced Power Injector 56V	C000065L002C
US Line Cord Fig 8	N000065L003A
UK Line Cord Fig 8	N000065L004A
EU Line Cord Fig 8	N000065L005A
Australia Line Cord Fig 8	N000065L006A
CMM5 Power and Sync Injector 56 Volts	C000000L556A
CMM5 240 watt AC/DC Power Supply	N000000L054B
CMM5 Controller	C000000L500A
Universal GPS	1096H

AC+DC Enhanced Power Injector 56V interfaces

The AC+DC Enhanced Power Injector 56V interfaces are shown in Figure 24 and described in Table 16.

Figure 24 AC+DC Enhanced Power Injector 56V interfaces

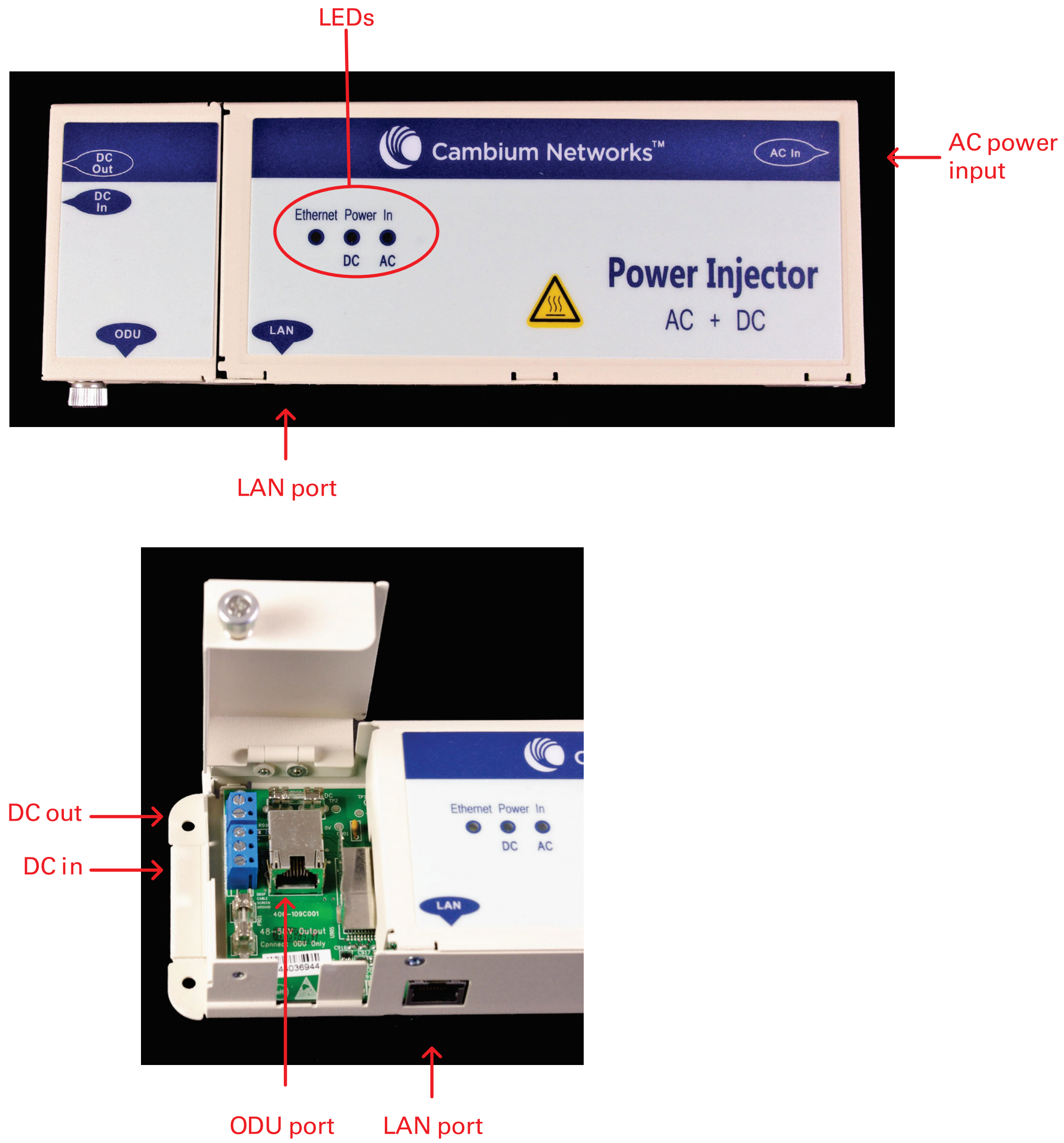


Table 16 AC+DC Enhanced Power Injector 56V interface functions

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

Interface	Function
Ethernet (yellow) LED	Ethernet traffic detection

CMM5 Power and Sync Injector interfaces

The CMM5 Power and Sync Injector interfaces are shown in Figure 25 and described in Table 17.

Figure 25 CMM5 Power and Sync Injector interfaces

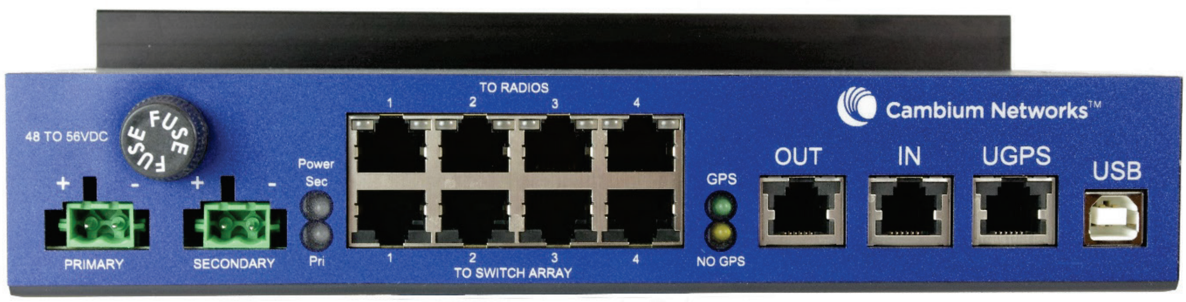


Table 17 CMM5 Power and Sync Injector interface functions

Interface	Function
Primary	Primary 48 V DC power connector
Secondary	Optional secondary 48 V DC power connector
To Radios 1, 2, 3, 4	To ODUs, RJ-45 connector
To Switch Array 1, 2, 3, 4	To network, RJ-45 connector
Out	Sync signal output, RJ-12 connector
In	Sync signal input, RJ-12 connector
UGPS	Universal GPS, RJ-12 connector
USB	Connection to Controller or PC, USB Type-B Receptacle

PSU specifications

The AC+DC Enhanced Power Injector 56V conforms to the specifications listed in Table 18.

The CMM5 Power and Sync Injector 56 V conforms to the specifications listed in Table 19.

Table 18 AC+DC Enhanced Power Injector 56V 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

Table 19 CMM5 Power and Sync Injector 56 Volts specifications

Category	Specification
Dimensions	225mm (8.85 in) × 400mm (15.75 in) × 42mm (1.65 in)
Weight	3 kg (6.6 lbs)
Temperature	-40°C (-40°F) to +55°C (131°F)
Humidity	0 to 90% non-condensing
Waterproofing	Not waterproof
Input Voltage	± 48 V DC
Input Power	400 W maximum
Output Voltage	± 55 V DC
Output Current	0–1.8 A per channel

Category	Specification
Output Power	0–90 W per channel
Power Interface Terminals	Two power input ports for 48 V DC Power
Data Interfaces	Four RJ45 Gigabit Powered output ports “To Radios” Four RJ45 Gigabit Data input ports “To Switch Array” One GPS timing port (RJ-12) One CMM5 USB Serial port for local administration One RJ12 Daisy Chain port “IN” One RJ12 Daisy Chain port “OUT”
Surge Suppresion	Lightning Suppression for each “To Radios” RJ45 Port
Max cable length from managed radios	100 m (328 ft)
Max cable length to GPS Antenna	30.5 m (100 ft)

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.

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 3-31.

RF cable and connectors

RF cable of generic type LMR-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 CNT-400 RF cable and N type male connectors from Cambium Networks (Table 20).

Table 20 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 Lightning protection unit (LPU) and grounding kit on page 2-26 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 700 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).

Hot Standby

For the highest availability, connect neighboring ODUs in a Hot Standby link to independent antennas. If this is not possible, consider connecting the two ODUs to a shared dual-polarized antenna through two suitable outdoor-rated RF combiners.

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

Table 22 specifies, for Aux and copper SFP interfaces, the Ethernet standards supported and the maximum permitted drop cable lengths.

Note For optical SFP interfaces, refer to SFP module kits on page 2-29 for details of the Ethernet standards supported and maximum permitted cable lengths.

Table 21 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+DC Enhanced Power Injector 56V	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)
CMM5 Power and Sync Injector	48 V dc	100BASE-TX 1000BASE-T	Yes	100 m (330 ft)

(*1) 10BASE-T is not supported by PTP 700.

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

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

Table 22 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 700.

(*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 26).

Attention 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 for the PTP 700..

Order Superior Essex type BBDGe cable from Cambium Networks (Table 23). Other lengths of this cable are available from Superior Essex.

Figure 26 Outdoor drop cable

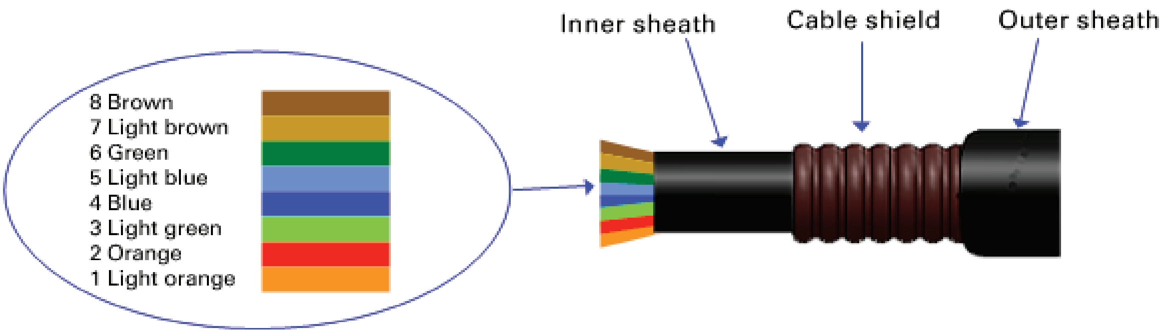


Table 23 Drop cable part numbers

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 27) is required for each grounding point on the PSU, Aux and copper SFP drop cables. Order cable grounding kits from Cambium Networks (Figure 35).

Attention 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 27 Cable grounding kit

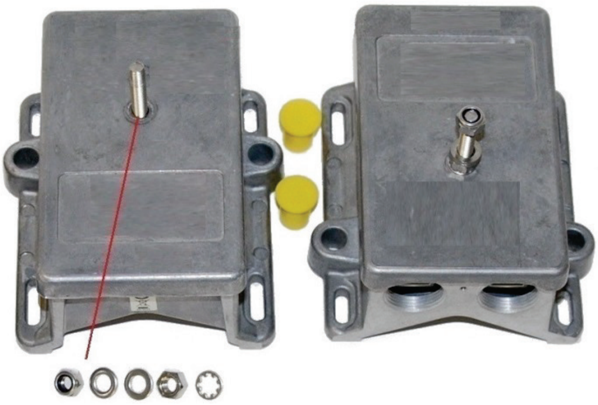
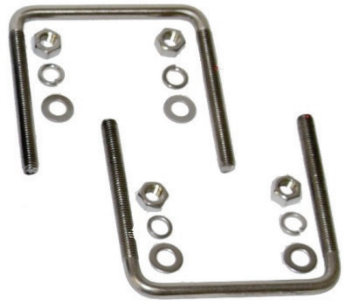
Table 24 Cable grounding kit part numbers

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

Lightning protection unit (LPU) and grounding kit

PTP 700 LPUs provide transient voltage surge suppression for PTP 700 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 25).

Table 25 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 25) 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 26).

Table 26 LPU and grounding kit part number

Cambium description	Cambium part number
LPU and Grounding Kit (One Kit Per End)	C000065L007

Note PTP 700 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.

LPU for GPS drop cables

When a GPS receiver is the timing reference source for PTP-SYNC (optional), an LPU must be installed near the point at which the GPS drop cable enters the building. A single LPU from the LPU and Grounding Kit (C000065L007) (Table 25) is suitable. Alternatively, the single LPU kit for PTP 250/300/500 (Figure 28) could be used.

Figure 28 LPU kit used for GPS receiver drop cables

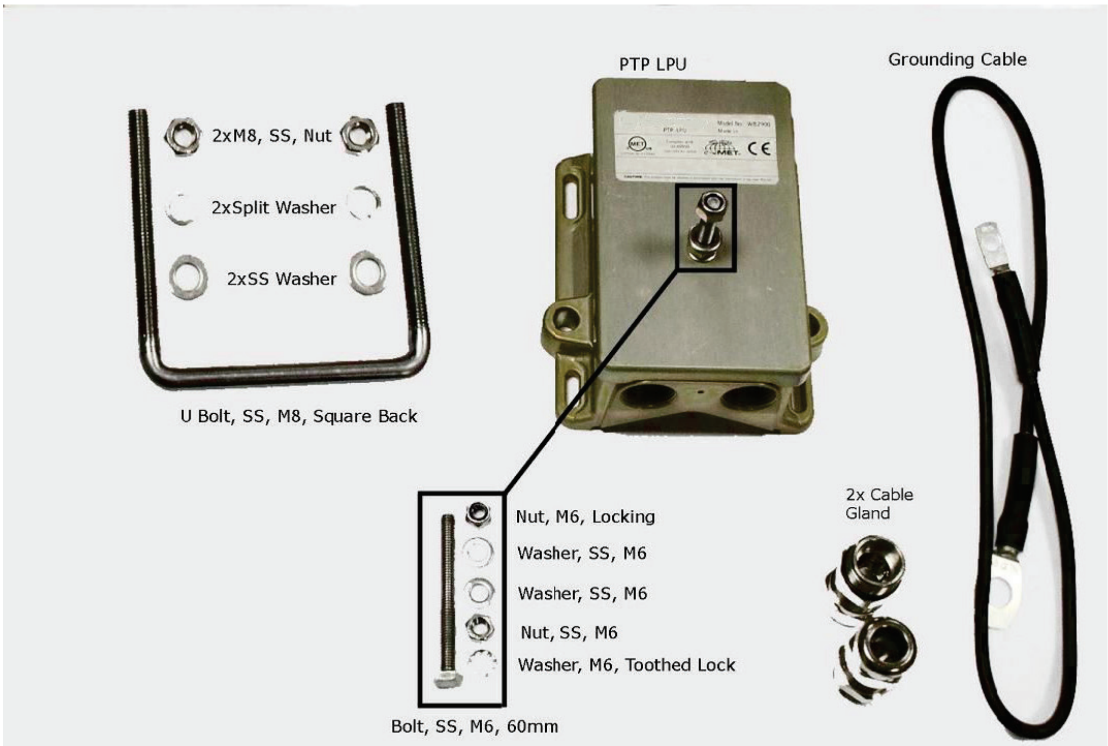


Table 27 LPU and grounding kit part number – Use with GPS receiver drop cable only

Cambium description	Cambium part number
LPU End Kit PTP 250/300/500	WB2978

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 28).

Note The RJ45 connectors and crimp tool listed in Table 28 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 29). These are identified with a black sealing nut. If extra glands are required, order them from Cambium Networks (in packs of 10) (Table 28).

One long EMC strain relief gland (Figure 32) 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 29 Cable gland

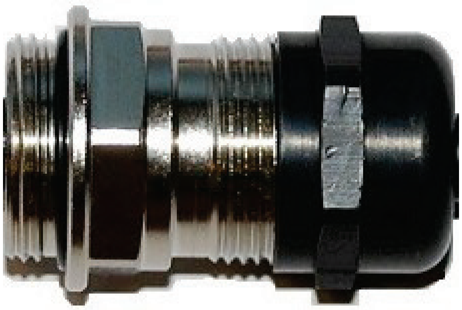


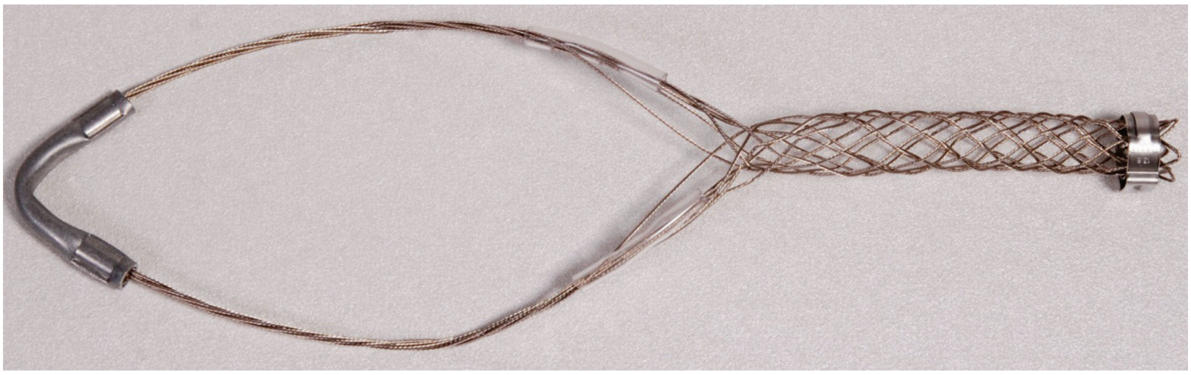
Table 28 RJ45 connector and spare gland part numbers

Cambium description	Cambium part number
Tyco/AMP, Mod Plug RJ45 Unscreened, 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 30). They are not supplied by Cambium Networks.

Figure 30 Cable hoisting grip



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 700 Series ODU to a network over a Gigabit Ethernet interface in one of the following full-duplex modes:

- Optical Gigabit Ethernet: 1000BASE-LX or 1000BASE-SX
- Copper Gigabit Ethernet: 100BASE-TX or 1000BASE-T

Order SFP module kits from Cambium Networks (Table 29).

Table 29 SFP module kit part numbers

Cambium description	Cambium part number
Single Mode Optical SFP Interface per ODU	C000065L008A
Multi-mode Optical SFP Interface per ODU	C000065L009A
Gig-Ethernet SFP Interface per ODU	C000065L010A

To compare the capabilities of the two optical SFP modules, refer to Table 30 and Table 31.

Table 30 Single Mode Optical SFP Interface (part number C000065L008A)

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)	2.35
50/125	Multi	400	550 m (1800 ft)	2.35
50/125	Multi	500	550 m (1800 ft)	2.35
10/125	Single	N/A	5000 m (16400 ft)	4.57

Table 31 Multi-mode Optical SFP Interface (part number C000065L009A)

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 31)
- Long EMC strain relief cable gland (Figure 32)
- The *Ethernet SFP Module Installation Guide*
- License key instructions and unique Access Key

Figure 31 Optical or copper SFP transceiver module

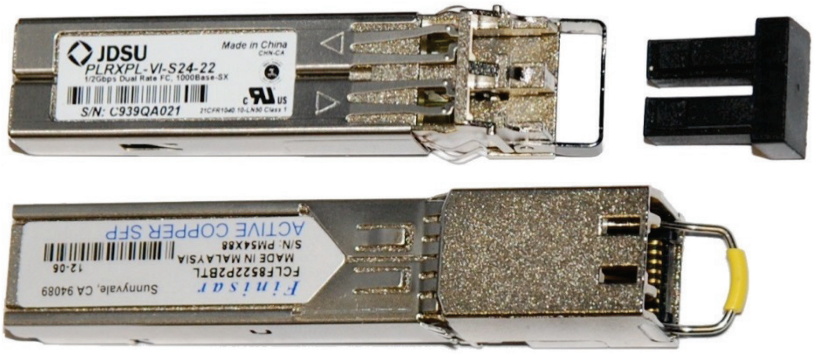
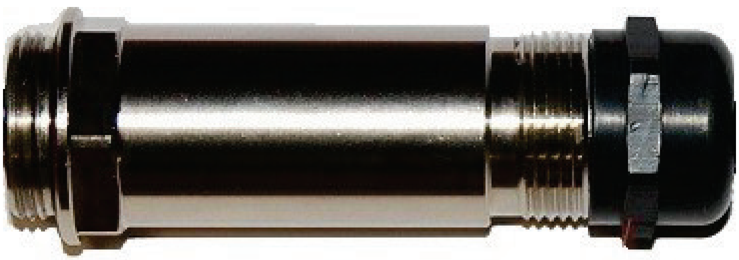


Figure 32 Long cable gland

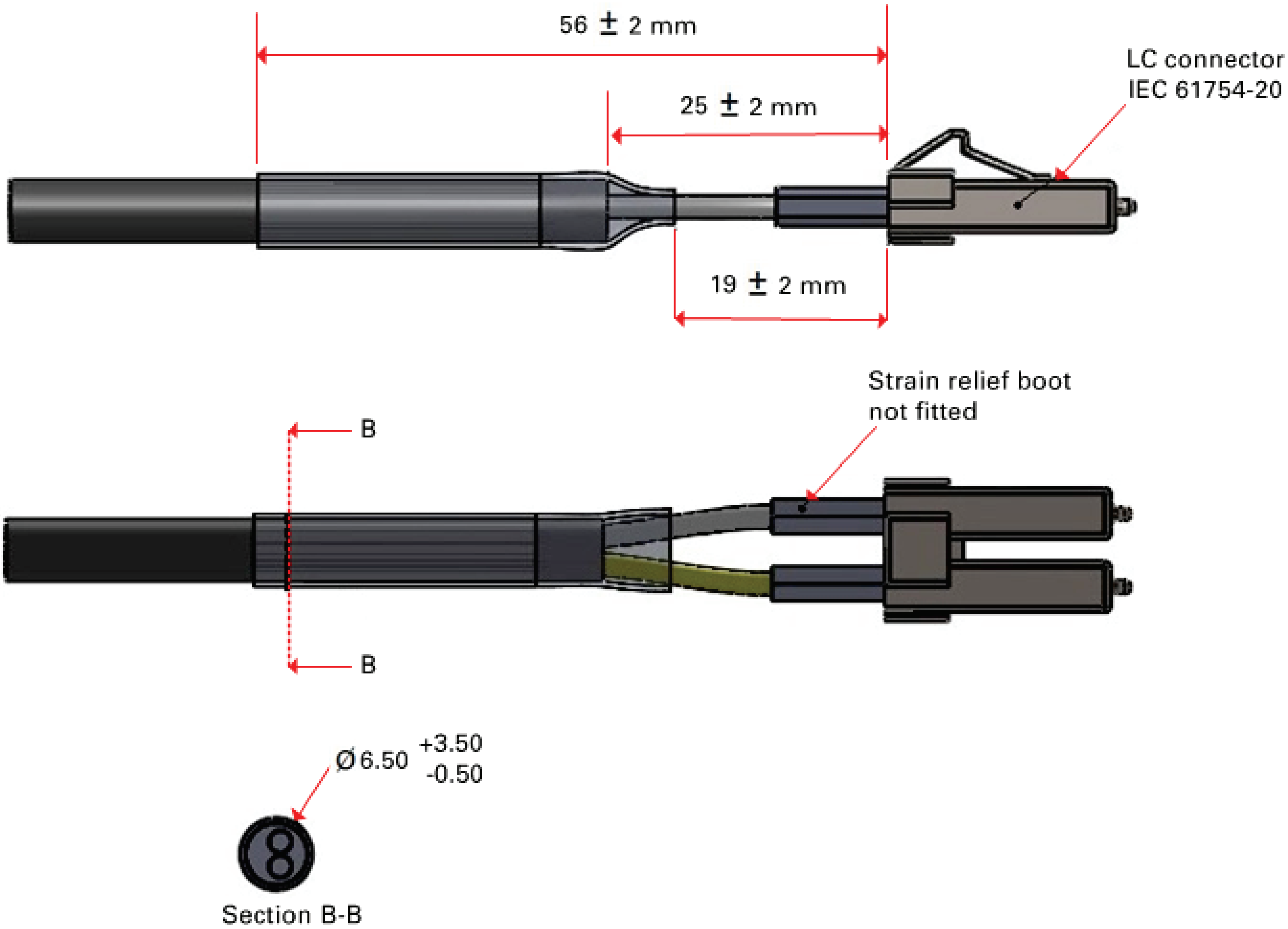


Note PTP 700 does not support the Synchronous Ethernet or 1588 Transparent Clock features using copper SFP transceivers.

Optical cable and connectors

Order an optical cable with LC connectors from a specialist fabricator, quoting the specification shown in Figure 33. 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 33 Optical optic cable and connector specification



PTP-SYNC unit

PTP-SYNC unit description

The PTP-SYNC unit is an optional component, used to synchronize the ODU TDD frame with a network-wide reference. It measures the difference between the TDD frame timing and a 1 Hz timing reference, and signals this time difference to the ODU. For more information on this feature, refer to TDD synchronization on page 1-32.

The PTP-SYNC unit is a compact indoor unit mounted on a wall, shelf or (using an optional rack mounting adaptor) in a standard 19 inch rack (Figure 35).

The PTP-SYNC unit is connected in line in the drop cable between the AC+DC Power Injector 56V and the ODU, and is collocated with the AC+DC Power Injector 56V. The PTP-SYNC draws power from the drop cable, and does not require a separate power supply.

PTP 700 supports an alternative approach to TDD synchronization using the CMM5 Power and Sync Injector. For further details, refer to TDD synchronization on page 1-32.

Attention The PTP-SYNC is compatible only with the AC+DC Power Injector 56V.

The AC Power Injector 56V and CMM5 will not work with a PTP-SYNC, and it is likely that a fuse will be blown in the PTP-SYNC if this is attempted.

PTP-SYNC is not compatible with standards-based power-over-Ethernet (PoE).

Figure 34 PTP-SYNC kit

Figure 35 PTP-SYNC rack mounting adapter

PTP-SYNC part numbers

Order PTP-SYNC kits and associated components from Cambium Networks (Table 32).

Table 32 PTP-SYNC component part numbers

Cambium description	Cambium part number
PTP-SYNC kit	WB3665
CMU/PTP-SYNC/NIDU 19inch Rack Mount Installation Kit	WB3486

The PTP-SYNC kit contains:

- 1 x PTP-SYNC unit
- 1 x M4 pan screw
- 2 x M4 washers
- 2 x M3 (6mm) torx drive screws
- 1 x lug for unit ground (cable not supplied)
- 1 x Cat5e cable (length 1 meter)
- Installation guide

If the 1 meter Cat5e cable supplied with the PTP-SYNC kit is not long enough, order a longer length of Cat5e cable, up to 2 meters long.

The PTP-SYNC rack mount kit contains:

- 1 x rack bracket
- 8 x M3 washers
- 8 x M3 screws
- 1 x rack mount blank plate
- 8 x M5 nuts
- 8 x M5 washers
- 2 x rack handles

PTP-SYNC unit interfaces

The PTP-SYNC front panel is illustrated in Figure 36. The annotated interfaces are described in Table 33 and Table 34.

Figure 36 PTP-SYNC front panel

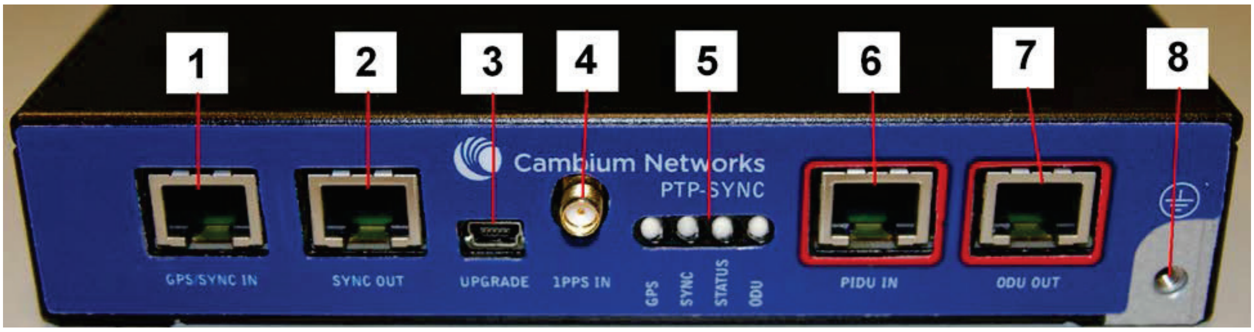


Table 33 PTP-SYNC interface functions

#	Description	Function
1	GPS/SYNC IN	Input from GPS receiver or from the daisy-chained SYNC OUT signal of another PTP-SYNC.
2	SYNC OUT	Output to daisy-chained PTP-SYNC units.
3	USB	Input for software upgrades. Contact Cambium for instructions.
4	1PPS IN	Coaxial alternative to GPS/SYNC IN. Peak input voltage must not exceed 5 V.
5	LED bank	LEDs and their functions are described in Table 34.
6	PIDU IN	Input from PSU.
7	ODU OUT	Output to ODU.
8	Ground stud	For connecting to a ground point.

Table 34 PTP-SYNC LED functions

LED	Function
GPS	GPS satellite data detection.
SYNC	SYNC OUT port data detection.
STATUS	Power and satellite lock detection.
ODU	ODU signal detection.

For a full list of LED states and fault-finding actions, refer to Testing PTP-SYNC on page 8-15.

PTP-SYNC specifications

The PTP-SYNC unit conforms to the specifications listed in Table 35, Table 36 and Table 37.

Table 35 PTP-SYNC unit physical specifications

Category	Specification
Dimensions	Width excluding ears 174 mm (6.69 in) Width including ears 196 mm (7.54 in) Height 31.5 mm (1.21 in) Depth 79 mm (3.04 in)
Weight	0.485 Kg (1.1 lbs)

Table 36 PTP-SYNC unit environmental specifications

Category	Specification
Temperature	-40°C (-40°F) to +60°C (140°F) Suitable for use indoors, or outdoors within a weatherproofed cabinet.
Humidity	0 to 95% non-condensing
Waterproofing	Not waterproof

Table 37 PTP-SYNC unit electrical specifications

Category	Specification
Power supply	Integrated with PSU
Power consumption	1.5 W max (extra power is required to supply a GPS receiver)

There are two timing inputs to the PTP-SYNC unit: GPS/SYNC IN (RJ-45) (Table 38) and 1PPS IN (SMA) (Table 39).

Table 38 PTP-SYNC unit timing specifications - GPS/SYNC IN (RJ-45)

Category	Specification
Signal type	Differential 1 Hz signal
Common mode range	–7 V to +7 V, relative to GPS/SYNC IN pin 2 (ground)
Maximum differential voltage	±5 V
Threshold	±0.4 V
Impedance	90 ohms to 110 ohms
Pulse width	1 µs to 500 ms
Polarity	Reference edge is when pin 3 (PPSA) is positive with respect to pin 6 (PPSB)

Table 39 PTP-SYNC unit timing specifications - 1PPS IN (SMA)

Category	Specification
Signal type	1 Hz signal
Pulse	Positive pulse, reference edge is rising edge
Maximum voltage	5 V
Threshold	0.4 V to 0.6 V
Input impedance	45 ohms to 55 ohms
Pulse width	1µs to 500ms

The pinouts of the PTP-SYNC unit GPS/SYNC IN port are specified in Table 40.

Table 40 GPS/SYNC IN port pinouts

Pin no.	Connector pinout signal name	Signal description
Pin 1	12VGPS	12 V output to GPS receiver module, 250 mA max
Pin 2	GND	Ground
Pin 3	GPS_1PPSA	1 Hz pulse input
Pin 4	GPS_RXDA	GPS receive data
Pin 5	GPS_RXDB	GPS receive data
Pin 6	GPS_1PPSB	1 Hz pulse input
Pin 7	GPS_TXDA	GPS transmit data
Pin 8	GPS_TXDB	GPS transmit data

Note The GPS_1PPS, GPS_RXD and GPS_TXD signals conform to International Telecommunication Union (ITU) recommendation V.11 (RS422)

Signal polarities

A 1 PPS timing datum is detected when GPS_1PPSA goes positive relative to GPS_1PPSB. A serial data start bit is detected when GPS_RXDA (or GPS_TXDA) goes positive relative to GPS_RXDB (or GPS_TXDB).

GPS receivers

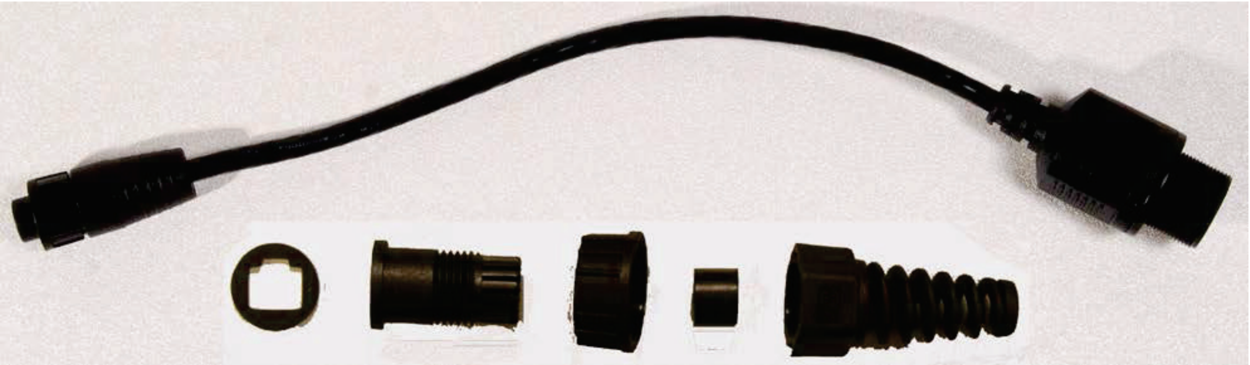
Trimble Acutime™ GG GPS receiver for PTP-SYNC

The GPS receiver (Figure 37) is an optional timing reference source for PTP-SYNC. It provides a 1 Hz signal, accurately synchronized in frequency and phase across the network.

Figure 37 GPS receiver

The GPS receiver is supplier with a GPS adapter cable kit (Figure 38). This avoids the need to fit a 12 way circular connector to the GPS drop cable. The kit contains one adapter cable (GPS receiver circular connector to RJ45 socket) and one RJ45 plug housing.

Figure 38 GPS adapter cable kit



GPS receiver part numbers

Order GPS receivers and associated components from Cambium Networks (Table 41).

Table 41 GPS receiver component part numbers

Cambium description	Cambium part number
Trimble Acutime™GG GPS receiver	WB4141
PTP-SYNC <-> Trimble Adapter Cable (*1)	WB3961
1000 ft Reel Outdoor Copper Clad CAT5E (*2)	WB3175
328 ft (100 m) Reel Outdoor Copper Clad CAT5E (*2)	WB3176
Tyco/AMP, Mod Plug RJ45 Unscreened, 100 pack (*3)	WB3177
Tyco/AMP Crimp Tool (*3)	WB3211
Cable Grounding Kits For 1/4" And 3/8" Cable (*4)	01010419001
LPU End Kit PTP 250/300/500 (*5)	WB2978D

(*1) This adapter cable is included with the GPS receiver (part number WB4141).

(*2) Other lengths of this BBDGe drop cable are available from Superior Essex.

(*3) The RJ45 connectors and crimp tool only work with Superior Essex type BBDGe cable.

(*4) One grounding kit is required per drop cable grounding point.

(*5) One LPU kit is required per GPS receiver.

Twelve way circular connector

As an alternative to the GPS adapter cable, the drop cable can be connected directly to the GPS unit via a 12 way circular connector, using the components and tools listed in Table 42.

Table 42 Recommended outdoor connectors for Trimble GPS receiver

Item	Manufacturer	Part number
12 way circular connector	Deutsch	IMC26-2212X
Size 22 crimp socket	Deutsch	6862-201-22278
Crimp tool	Daniels Manufacturing Corp	MH860
Positioner	Daniels Manufacturing Corp	86-5
Insertion / extraction tool	Deutsch	6757-201-2201
Adaptor	Deutsch	IMC2AD
Self amalgamating tape		

Universal GPS

For details of the Universal GPS (UGPS) receiver, see *PMP Synchronization Solutions User Guide* available from the Cambium Networks web site.

Chapter 3: System planning

This chapter provides information to help the user to plan a PTP 700 link.

The following topics are described in this chapter:

- Typical deployment on page 3-2 contains diagrams illustrating typical PTP 700 site deployments.
- Site planning on page 3-11 describes factors to be considered when planning the proposed link end sites, including grounding, lightning protection and equipment location.
- Radio spectrum planning on page 3-21 describes how to plan PTP 700 links to conform to the regulatory restrictions that apply in the country of operation.
- Link planning on page 3-25 describes factors to be taken into account when planning links, such as range, path loss and throughput.
- Planning for connectorized units on page 3-31 describes factors to be taken into account when planning to use connectorized ODUs with external antennas in PTP 700 links.
- Configuration options for TDD synchronization on page 3-33 describes the different configuration options that may be used for implementing TDD synchronization in the PTP 700 Series.
- Data network planning on page 3-39 describes factors to be considered when planning PTP 700 data networks.
- Network management planning on page 3-50 describes how to plan for PTP 700 links to be managed remotely using SNMP.
- Security planning on page 3-53 describes how to plan for PTP 700 links to operate in secure mode.
- System threshold, output power and link loss on page 3-64 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 3-87 contains tables and graphs to support calculation of the data rate capacity that can be provided by PTP 700 configurations.

Typical deployment

This section contains diagrams illustrating typical PTP 700 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 39), wall installation (Figure 40) and roof installation (Figure 41).

Figure 39 Mast or tower installation

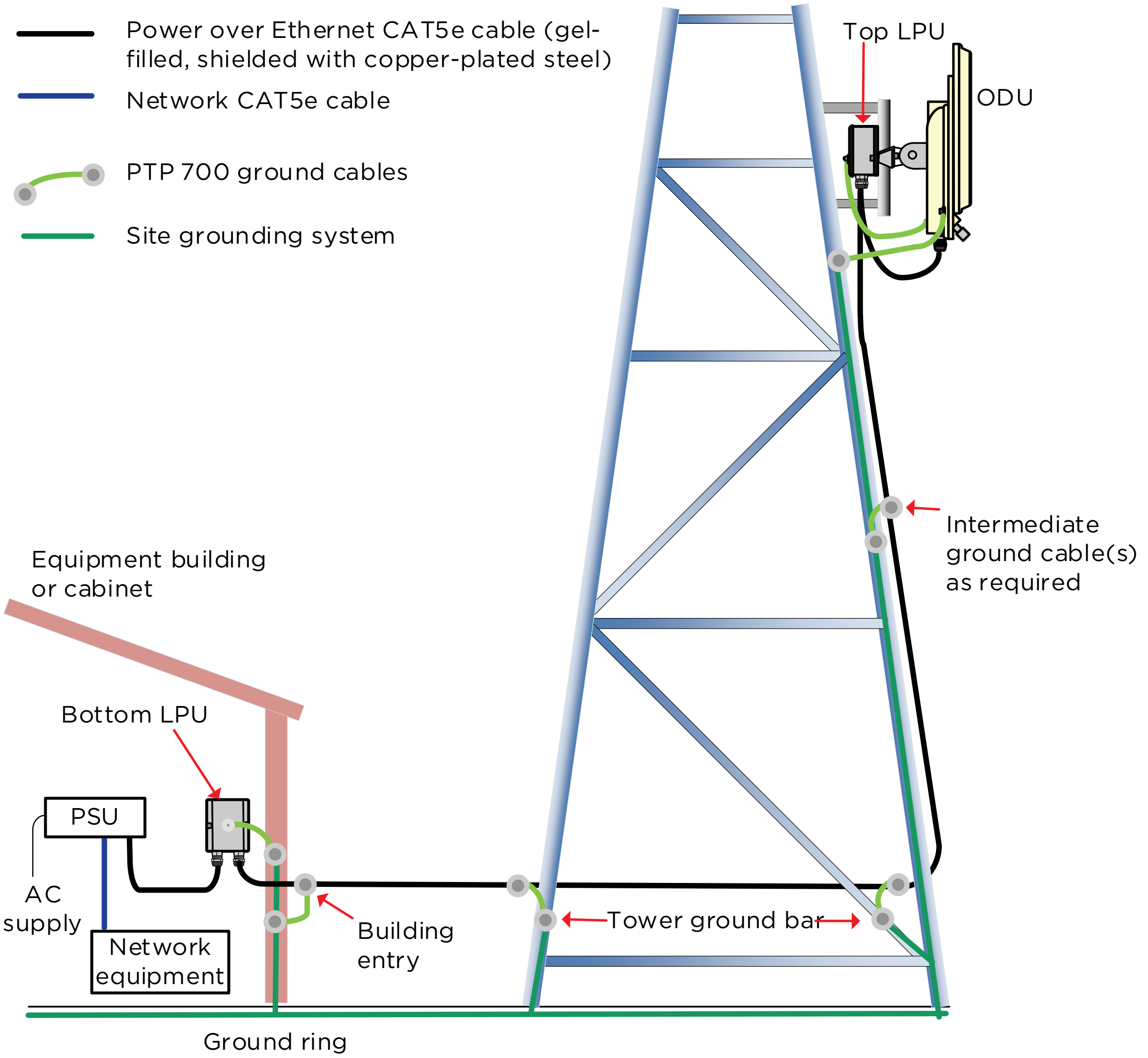


Figure 40 Wall installation

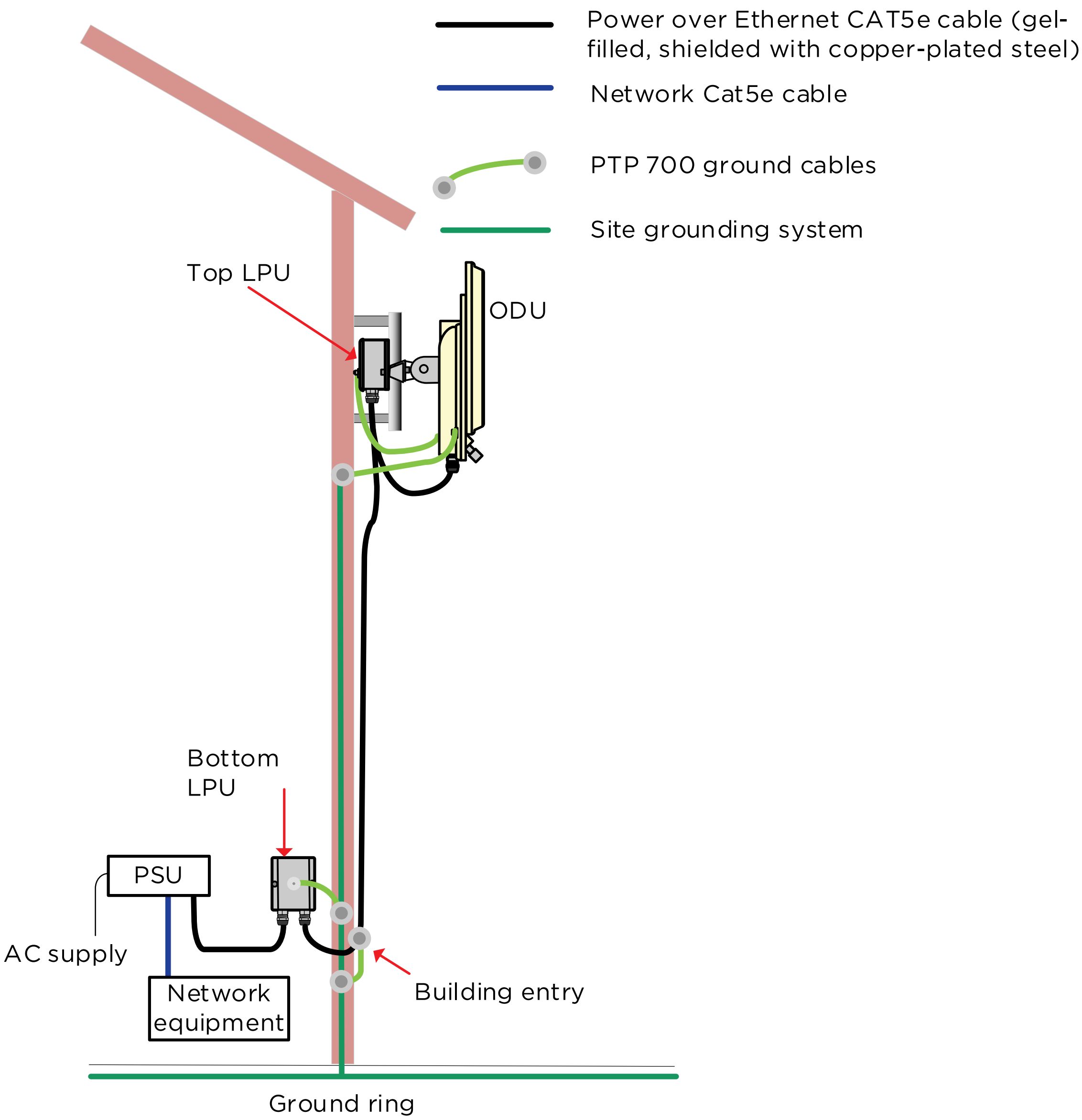
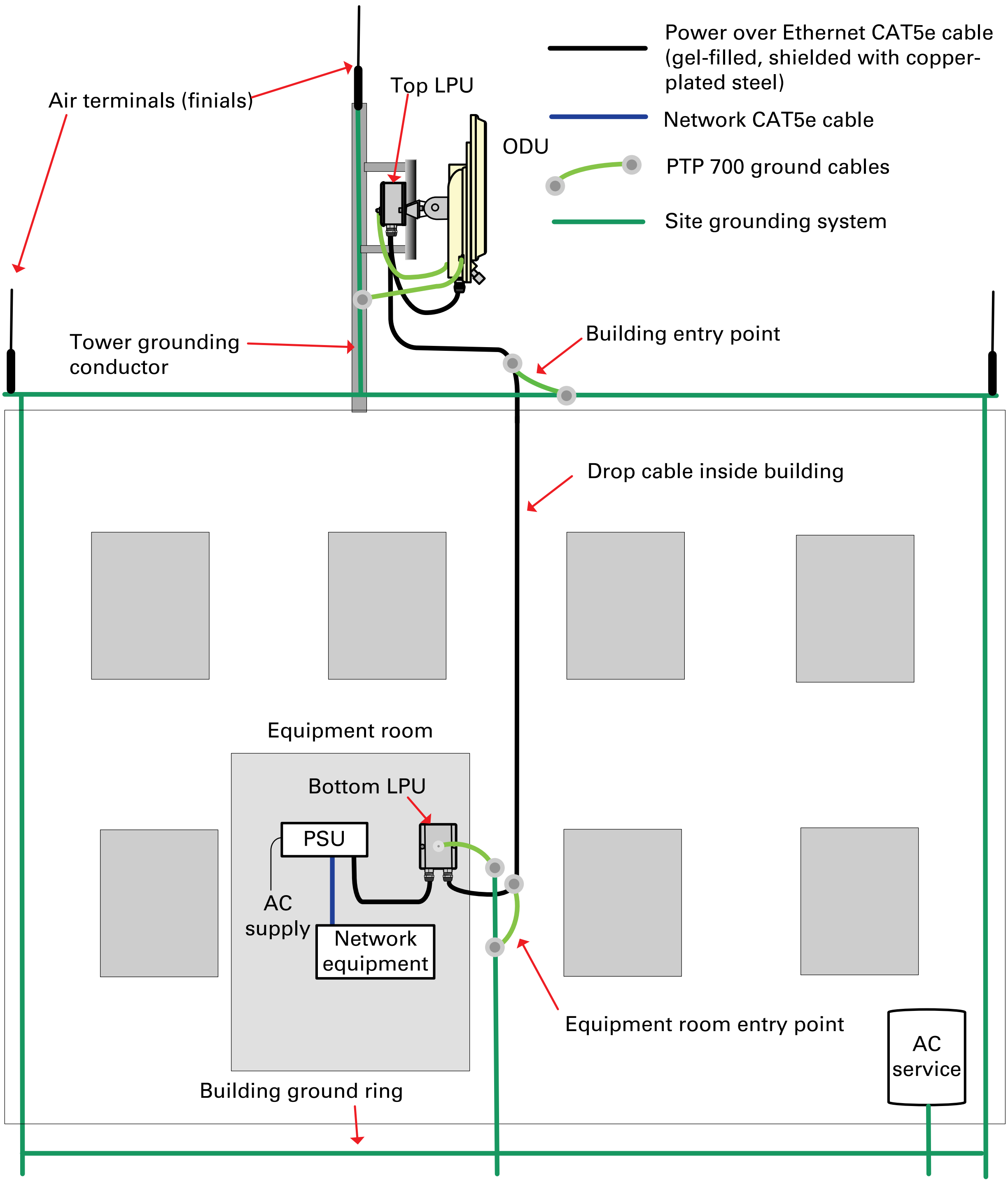


Figure 41 Roof installation



SFP and Aux Ethernet interfaces

Note PTP 700 does not support the Aux Ethernet interface at a Master ODU in the HCMP topology.

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 42
- ODU with optical SFP and PSU interfaces – Figure 43
- ODU with Aux and PSU interfaces – Figure 44

Figure 42 ODU with copper SFP and PSU interfaces

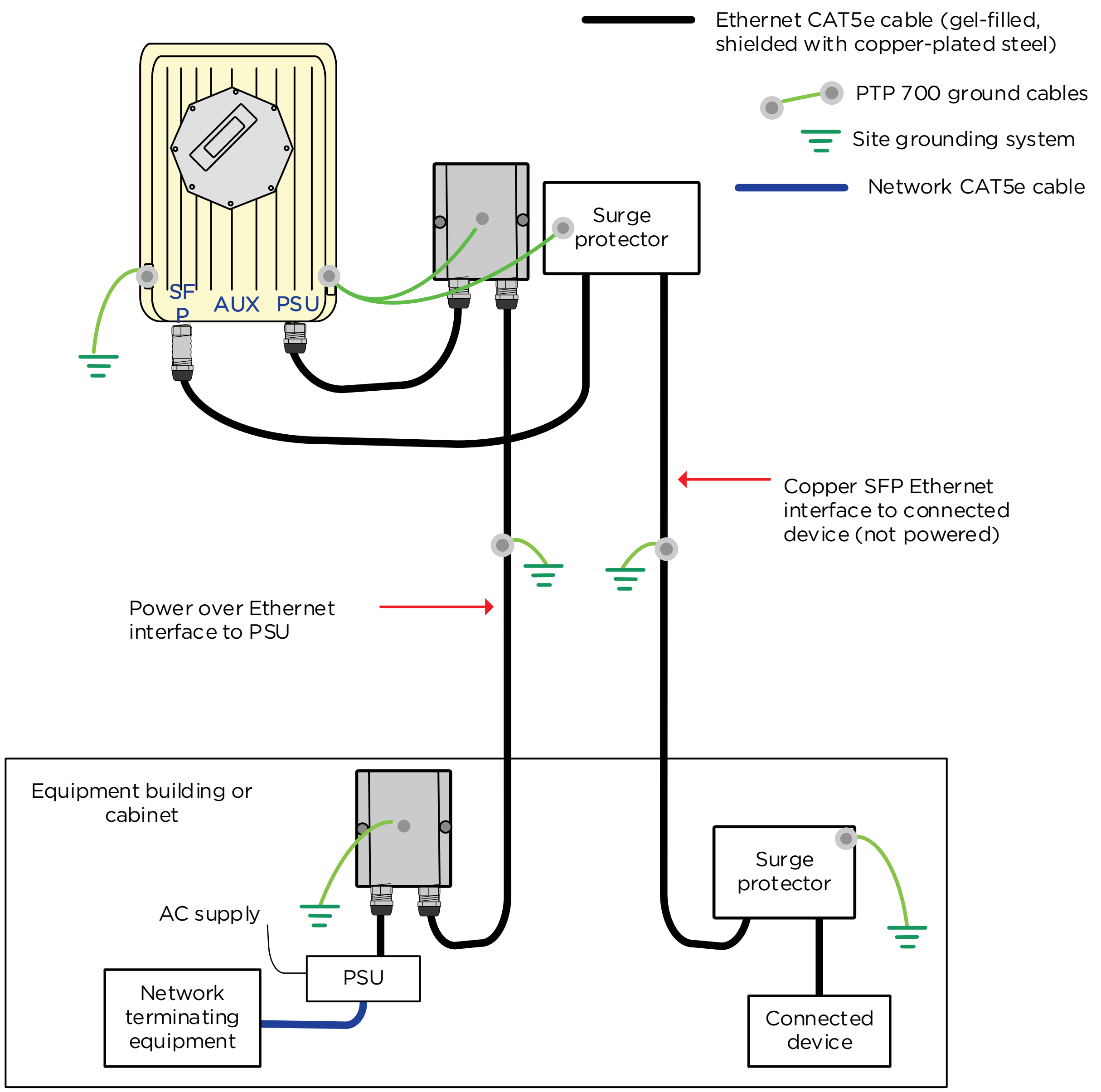


Figure 43 ODU with optical SFP and PSU interfaces

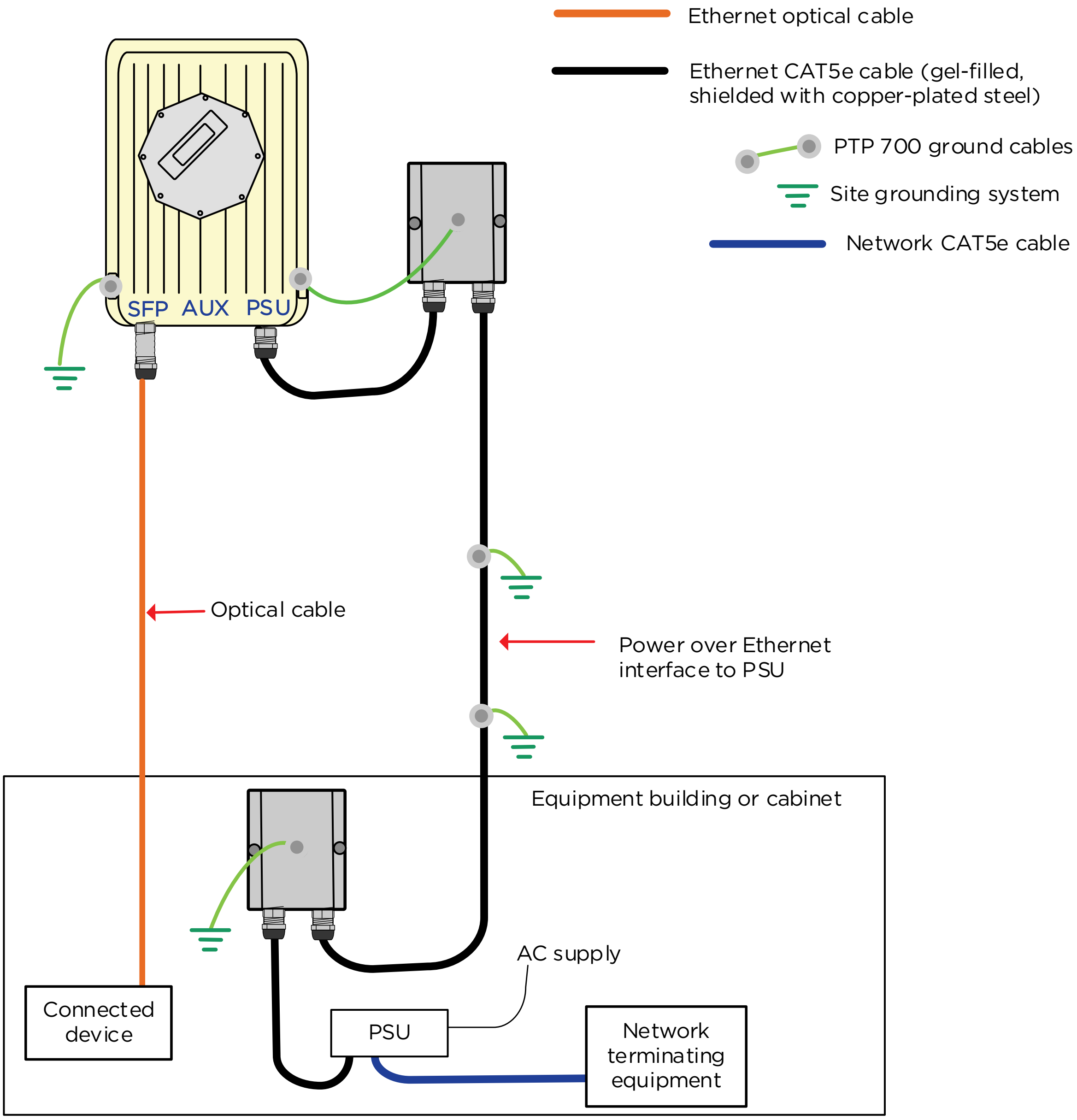
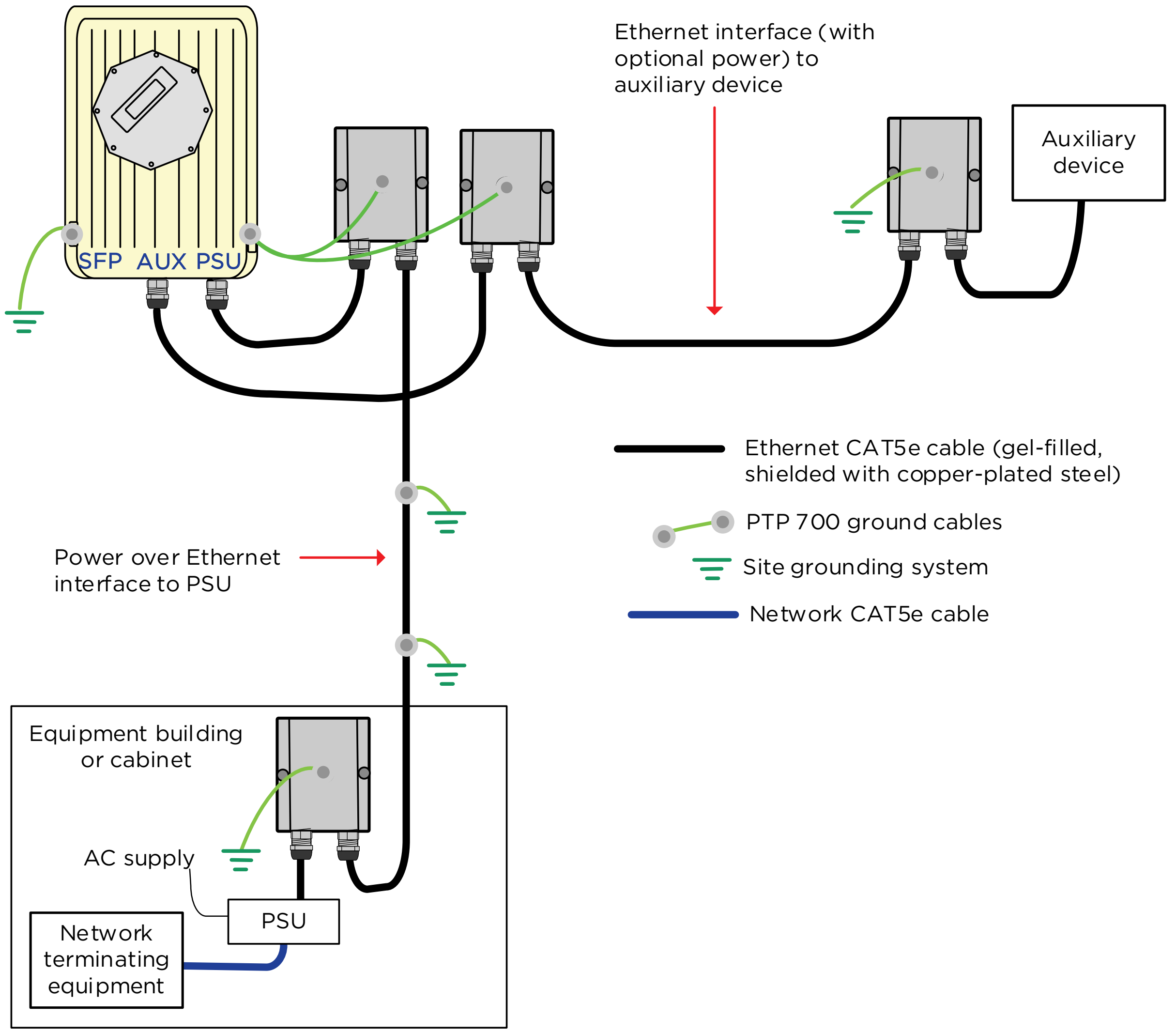


Figure 44 ODU with Aux and PSU interfaces



GPS receiver interfaces

If a GPS receiver is deployed for PTP-SYNC, it may be mounted on the wall of the equipment building (Figure 45) (preferred option), or on a metal tower or mast (Figure 46).

Figure 45 GPS receiver wall installation

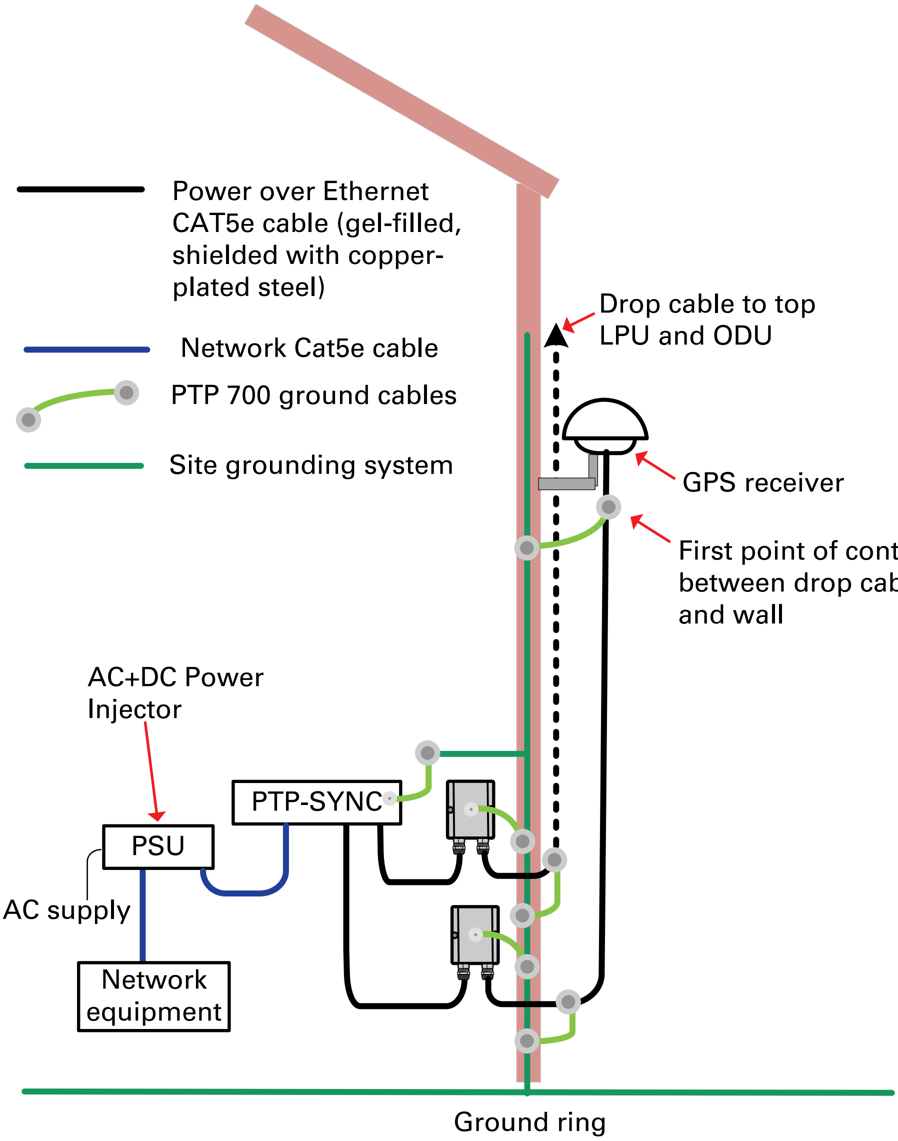
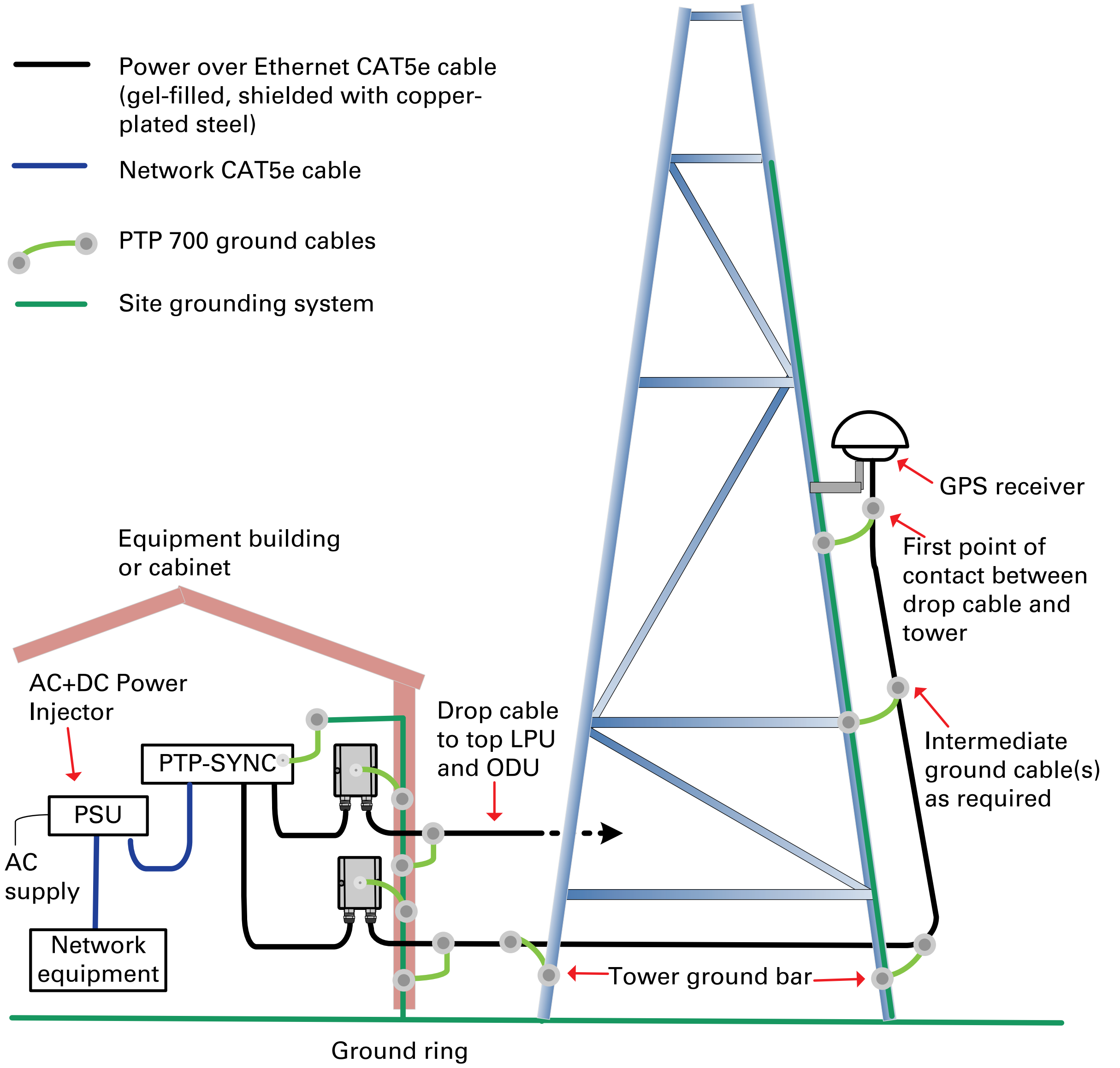


Figure 46 GPS receiver tower or mast installation



Site planning

This section describes factors to be considered when planning the proposed link end sites, including grounding, lightning protection and equipment location for the ODU, PSU, PTP-SYNC unit (if installed) and GPS receivers (if installed).

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 700 installation, both ground bonding and transient voltage surge suppression are required.

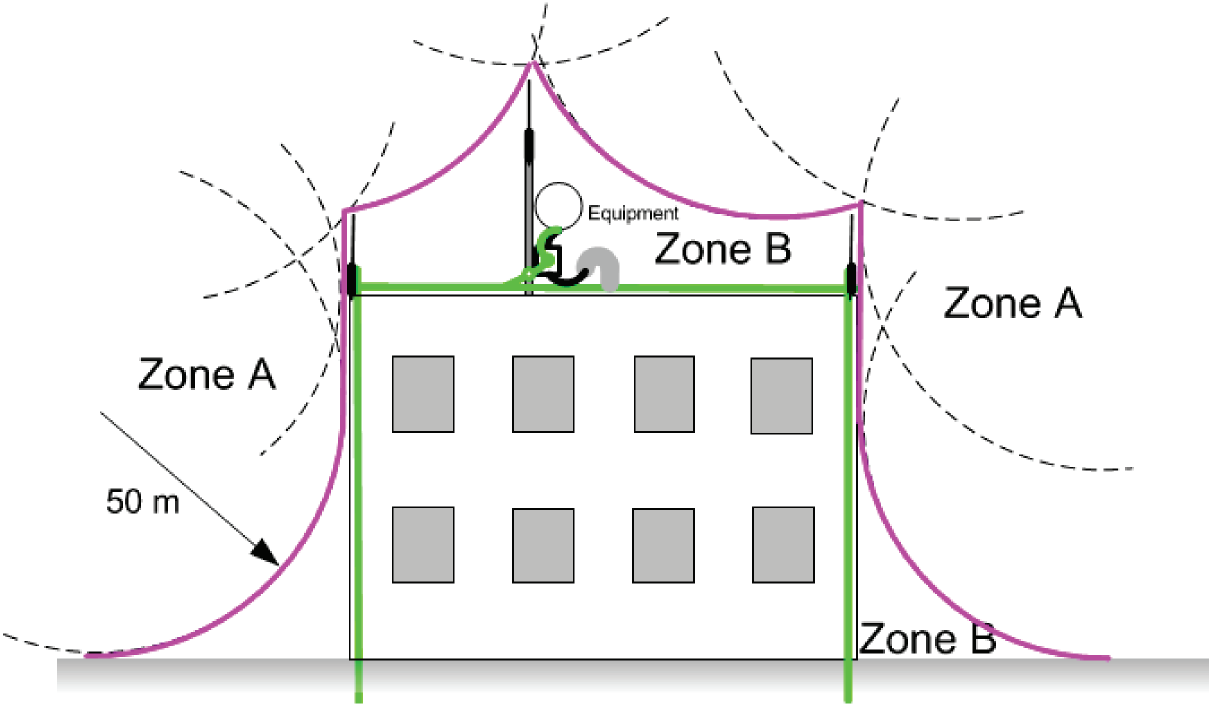
Full details of lightning protection methods and requirements can be found in the international standards IEC 61024-1 and IEC 61312-1, the U.S. National Electric Code ANSI/NFPA No. 70-1984 or section 54 of the Canadian Electric Code.

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

Lightning protection zones

Use the rolling sphere method (Figure 47) 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 47 Rolling sphere method to determine the lightning protection zones



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 700 equipment.

If the outdoor equipment is to be installed on the roof of a high building (Figure 41), 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 on page 4-22.
- 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 ambient temperature limits

Select a location where the ODU can operate within safe ambient temperature limits.

The ODU must be mounted in a Restricted Access Location (as defined in EN 60950-1) if the operating ambient temperature may exceed 40°C, including solar radiation.

If the ambient temperature never exceeds 40°C, the temperature of the external metal case parts of the ODU will not exceed the touch temperature limit of 70°C.

If the ambient temperature never exceeds 60°C, the temperature of the external metal case parts of the ODU will not exceed the touch temperature limit of 90°C.

Note A restricted access location is defined (in EN 60950-1) as one where access may only be gained by use of a tool or lock and key, or other means of security, and access is controlled by the authority responsible for the location. Access must only be gained by persons who have been instructed about the reasons for the restrictions applied to the location and about any precautions that must be taken. Examples of permissible restricted access locations are a lockable equipment room or a lockable cabinet.

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 700 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 325 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 the variant of the ODU. Wind loading is estimated using the following formulae:

- Force (in newtons) = $0.5 \times \rho \times V^2 \times A \times C_d$
  - "ρ" is the density of air = 1.225 kg/m^3,
  - "V" is the wind speed in meters per second,
  - "A" is the projected surface area of the ODU in square meters, and
  - "C_d" is the drag coefficient = 1.385.

The drag coefficient has been measured when the cover plate or antenna is perpendicular to the air flow.

Applying this formula to the PTP 700 ODUs at different wind speeds, the resulting wind loadings are shown in Table 43

Table 43 ODU wind loading (newtons)

Type of ODU	Max surface area (square meters)	Wind speed (kilometers per hour)				
		225	250	275	300	325
Connectorized+Integrated	0.160	530 N	655 N	792 N	943 N	1106 N
Connectorized	0.062	205 N	254 N	307 N	365 N	429 N

Equivalent results in US customary units are shown in Table 44.

Table 44 ODU wind loading (pounds force)

Type of ODU	Max surface area (square feet)	Wind speed (miles per hour)				
		140	155	170	185	200
Connectorized+Integrated	1.72	120 lb	147 lb	176 lb	209 lb	244 lb
Connectorized	0.67	46 lb	57 lb	68 lb	81 lb	95 lb

If an external antenna is installed, add the wind loading of the antenna to that of the ODU. The antenna manufacturer should be able to quote wind loading.

Hazardous locations

Check that the ODUs will not be exposed to hazardous gases, as defined by HAZLOC (USA) and ATEX (Europe) regulations.

PSU DC power supply

If using the DC input on the AC+DC Power Injector 56V, 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 AC power supply

Always use an appropriately rated and approved AC supply cord-set in accordance with the regulations of the country of use.

PSU location

Find a location for the PSU (AC+DC Enhanced Power Injector 56V or CMM5) that meets the following requirements:

- The AC+DC Enhanced Power Injector 56V can be mounted on a wall or other flat surface.
- The CMM5 Power and Sync Injector can be installed in a standard 19-inch rack.
- 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.
- The PSU can be connected to a compatible power supply. AC+DC Enhanced Power Injector 56V: the use of DC supplies of less than 55V will reduce the usable distance between the PSU and ODU.

PTP-SYNC location

If PTP-SYNC is to be installed, consider the following factors when selecting a site:

- Indoor location with no possibility of condensation.
- Accessibility for viewing status indicators.
- The maximum cable length between the PSU and the PTP-SYNC is 2 m (6 ft).

GPS receiver location

Mount the GPS receiver for PTP-SYNC at a location that meets the following requirements:

- It must be possible to protect the installation as described in Grounding and lightning protection on page 3-11.
- It must have an un-interrupted view of at least half of the sky. For a receiver mounted on a wall there must be no other significant obstructions in the view of the sky.

- It must be mounted at least 1 m (3 ft), preferably 2 m (6 ft), away from other GPS receiving equipment.
- It must not be sited in the field of radiation of co-located radio communications equipment and should be positioned at a distance of at least 3 m (10 ft) away.

Mount the GPS receiver on the wall of the equipment building, if there is a suitable location on the wall that can meet these requirements. Failing that, mount it on a metal tower or mast.

Attention The GPS receiver is not approved for operation in locations where gas hazards exist, as defined by HAZLOC (USA) and ATEX (Europe).

Mounting the GPS receiver module on the equipment building

If mounting the GPS receiver for PTP-SYNC on the equipment building (Figure 45), select a position on the wall that meets the following requirements:

- It must be below the roof height of the equipment building or below the height of any roof-mounted equipment (such as air conditioning plant).
- It must be below the lightning air terminals.
- It must not project more than 600mm (24 inches) from the wall of the building.

If these requirements cannot all be met, then the module must be mounted on a metal tower or mast.

Mounting the GPS receiver module on a metal tower or mast

If mounting the GPS receiver module on a metal tower or mast (Figure 46), select a position that meets the following requirements:

- It must not be mounted any higher than is necessary to receive an adequate signal from four GPS satellites.
- It must be protected by a nearby lightning air terminal that projects farther out from the tower than the GPS receiver module.

Drop cable grounding points

To estimate how many grounding kits are required for each drop cable, refer to the site installation diagrams (Figure 39 , Figure 40 and Figure 41) 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 39), 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 41), 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 700 LPU (Figure 48). Optical cables do not require LPUs or ground cables (Figure 49).

The copper SFP drop cable requires a bottom surge protector, not a PTP 700 LPU (Figure 50).

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

Figure 48 ODU with PSU, Aux and copper SFP interfaces

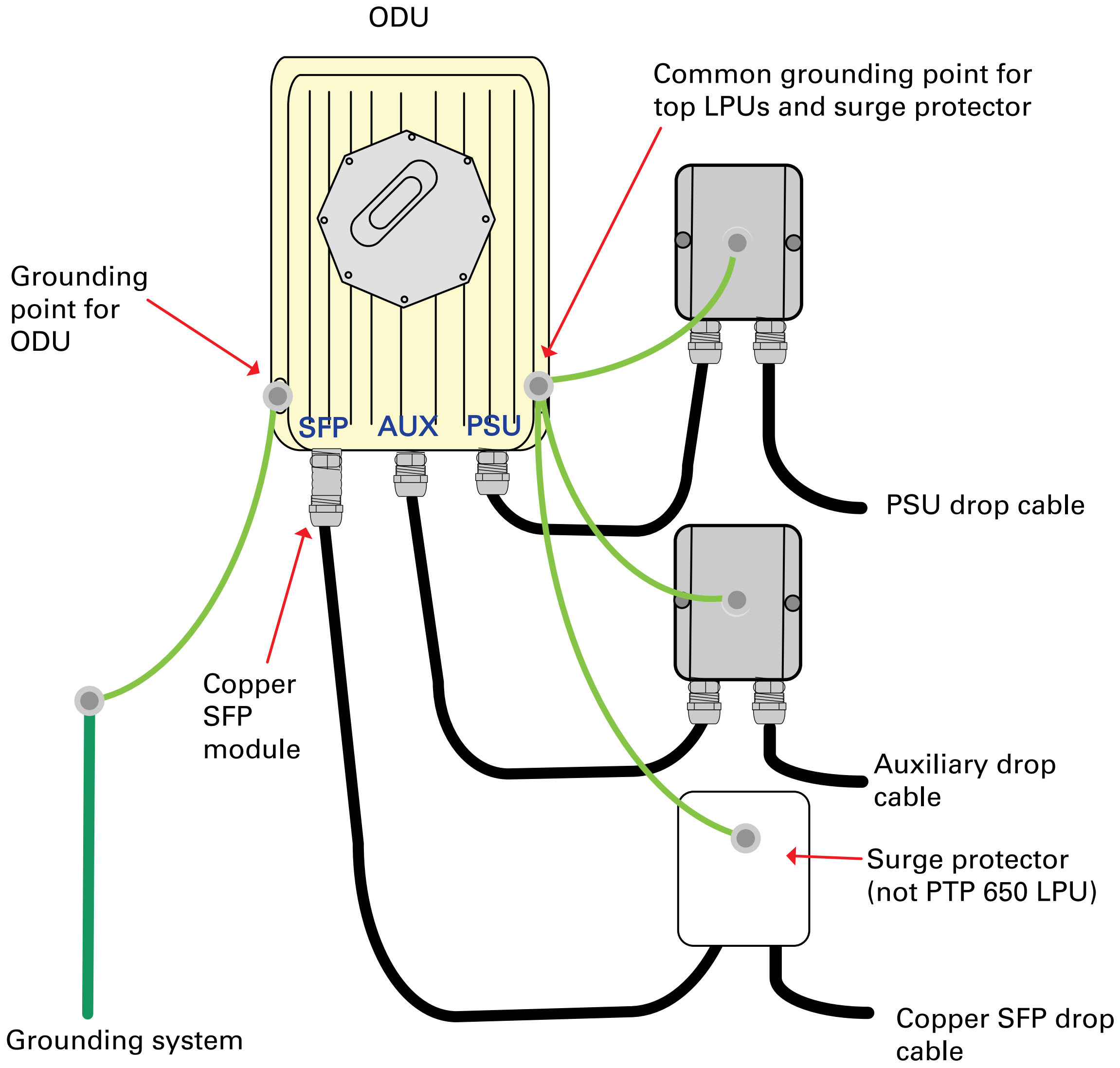


Figure 49 ODU with PSU, Aux and optical SFP interfaces

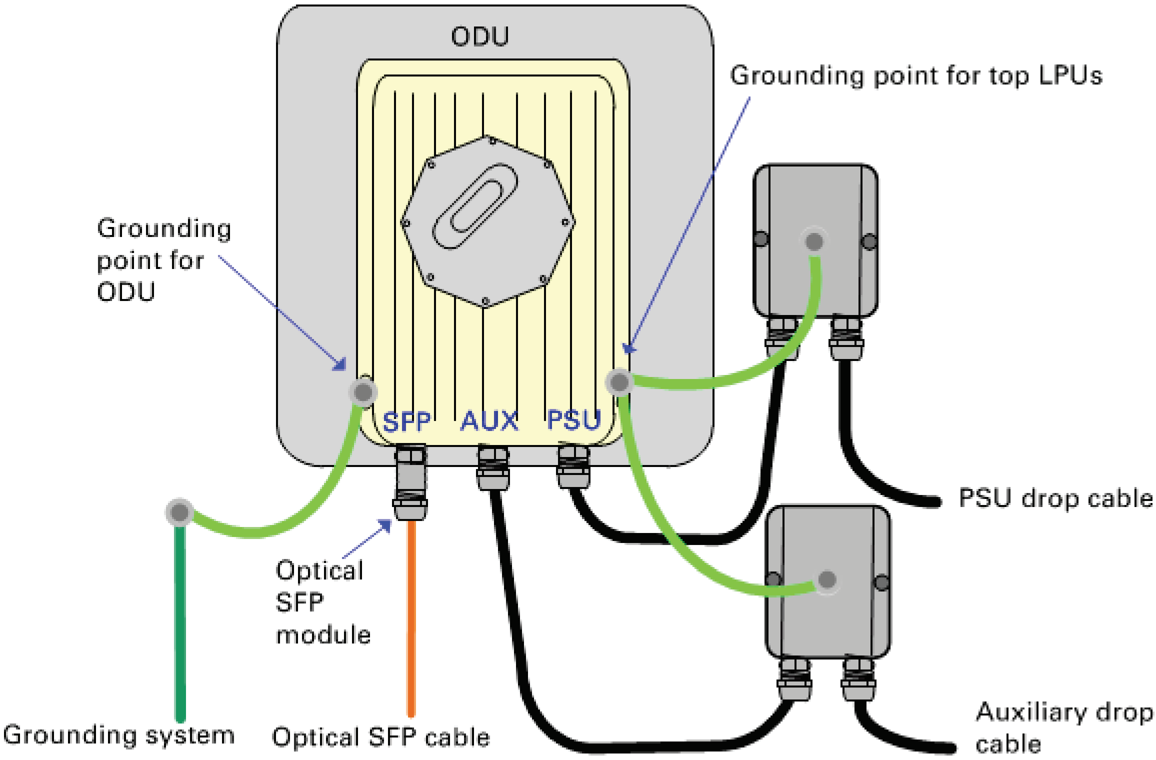
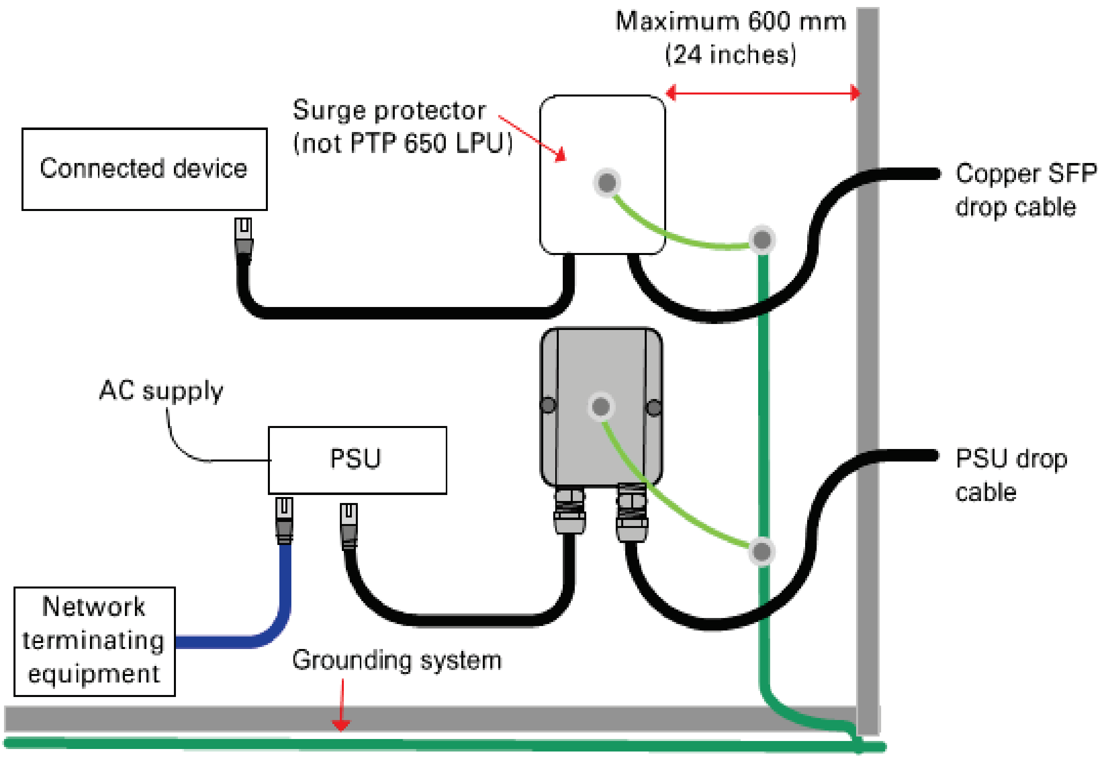


Figure 50 Bottom LPU and surge protector



Hot Standby

ODUs used in a Hot Standby link are installed in pairs. Neighbouring ODUs should normally be located close together and installed on the same grounded metal structure. In this case, the Protection Link can be made using suitable outdoor Ethernet cable of the same type as the drop cable, and LPUs are not needed.

If it is not possible to locate neighboring ODUs close together on the same structure, use only fiber interconnections with the optical SFP interface for the Protection Link.

Radio spectrum planning

This section describes how to plan PTP 700 links to conform to the regulatory restrictions that apply in the country of operation.

Attention 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 700 link is required.

General wireless specifications

Table 45 lists the wireless specifications that apply to all PTP 700 frequency bands. Table 46 lists the wireless specifications that are specific to a single frequency band.

Table 45 PTP 700 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	22 dBi Flat plate antenna (PTP 700 Connectorized+Integrated)
Duplex schemes	Symmetric fixed, asymmetric fixed and, for the Full license only, adaptive TDD.
Range	Line-of-Sight: 250 km (156 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 46 PTP 700 wireless specifications (per frequency band)

Item	4.7 GHz	4.9 GHz	5.1 GHz	5.2 GHz	5.4 GHz	5.8 GHz
RF band (MHz)	4400–5000	4900–4990	5150–5250	5250–5350	5470–5725	5725–5875
Channel bandwidth (MHz)	5, 10, 15, 20, 30, 40, 45	5, 10, 15, 20	5, 10, 15, 20, 30, 40, 45	5, 10, 15, 20, 30, 40, 45	5, 10, 15, 20, 30, 40, 45	5, 10, 15, 20, 30, 40, 45
Typical receiver noise	7.5 dB	7.5 dB	7.5 dB	7.8 dB	7.8 dB	8.1 dB
Typical antenna gain (integrated)	22.0 dBi	22.0 dBi	22.0 dBi	22.0 dBi	22.0 dBi	22.0 dBi
Antenna beamwidth (integrated)	8°	8°	8°	8°	8°	8°

Regulatory limits

Many countries impose EIRP limits (Allowed EIRP) on products operating in the bands used by the PTP 700 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. When using connectorized ODUs with external antennas, ensure that the antenna gain and feeder loss is configured correctly in the ODU.

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.

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 Expert and Spectrum Management web pages (Spectrum Expert page in radar avoidance mode on page 7-39).

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.

Note PTP 700 supports only the 20 and 40 MHz channel bandwidth in the HCMP topology.

Frequency selection

PTP topology in 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.

PTP topology in 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.

Frequency selection for HCMP topology

In the HCMP topology, the Master supports:

- Fixed Frequency

The HCMP Slave supports:

- Fixed Frequency
- Dynamic Spectrum Optimization (DSO): This allows the Slave to scan the frequency band to find the associated Master ODU.

HCMP topology cannot be used at present in Regulatory Bands that require DFS (radar detection).

Link planning

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

LINKPlanner

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

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. Use the installation report to compare predicted and actual link performance.

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 700 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 700 Series will operate at ranges from 100 m (330 ft) to 250 km (156 miles), within four ranging modes: 0-40 km (0-25 miles), 0-100 km (0-62 miles), 0-200 km (0-125 miles), and 0-250 km (0-156 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.

Note The maximum range for the HCMP topology is 100 km, limited by the round-trip time allowed in the TDD frame. The maximum range achieved for a link in the HCMP topology tends to be lower than in the PTP topology because the Master ODU is normally installed with a sector or omni-directional antenna.

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 700 to detect radar signals:

- With integrated antennas, the recommended minimum LoS operating range is 110 meters (360 ft) for 5.2 GHz or 5.4 GHz, and 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 5.2 GHz or 5.4 GHz) or below -58 dBm (for 5.8 GHz).

LINKPlanner for synchronized networks

TDD synchronization should be planned using LINKPlanner. This will provide the necessary TDD frame parameter values which are required to complete a synchronized installation. Please refer to the *LINKPlanner User Guide*.

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 3-64.

Calculating data rate capacity

The data capacity of a PTP or HCMP link is defined as the maximum end-to-end Ethernet throughput (including Ethernet headers) that it can support, assumed Ethernet frames of 1518 octets.

Data capacity is determined by the following factors:

- Wireless topology (PTP or HCMP)
- TDD Synchronization
- Licensed data throughput capability (ODU license: Full or Lite)
- Link Symmetry
- Link Mode Optimization (IP or TDM)
- Modulation Mode
- Channel Bandwidth
- Link Range
- TDD Frame Configuration Mode (Standard or Expert)
- Expert Mode configuration for HCMP

Calculation procedure for PTP topology without TDD synchronization

To calculate the data rate capacity of an unsyncronized PTP 700 link, proceed as follows:

1. Use the tables in Data capacity in PTP topology on page 3-87 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
   - Capacity License (Full or Lite)
2. The tables contain data rates for links of zero range. Use the range adjustment graphs 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 for PTP topology without TDD synchronization

Suppose that the link characteristics are:

- PTP 700 variant = Lite
- 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 109 to look up the data throughput capacity rates:

   Tx = 21 Mbits/s

   Rx = 21 Mbits/s

   Aggregated = 42 Mbits/s

2. Use Figure 79 to look up the Throughput Factor for 1:1, TDM, 10 MHz, Lite 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 = 18.1 Mbits/s

   Rx = 18.1 Mbits/s

   Aggregated = 36.1 Mbits/s

Calculation procedure for PTP topology with TDD synchronization

The capacity of a PTP link with TDD synchronization can be determined from the following attributes:

- Channel Bandwidth
- Burst Duration
- TDD Frame Duration
- Modulation Mode

Proceed as follows:

1. Use Table 114 to look up the number of time slots per TDD frame for the required combination of:
   - Channel Bandwidth
   - Burst Duration
2. Use Table 120 to look up the one-way data capacity per time slot for the required combination of:
   - TDD Frame Duration
   - Modulation Mode
3. The one-way link capacity is the capacity per time slot from Step 2 multiplied by the number of time slots per frame from Step 1. The aggregate (two-way) capacity is the sum of two one-way capacities.

Calculation procedure for PTP topology with long frame duration

The capacity of a synchronized PTP link with Long Frame Duration enabled can be determined from the following attributes:

- Channel Bandwidth
- Burst Duration

- TDD Frame Duration
- Modulation Mode

Proceed as follows:

1. Use Table 115 to look up the number of time slots per TDD frame for the required combination of:
   - Channel Bandwidth
   - Burst Duration

   The number of time slots in a Hot Standby link is exactly one less than the equivalent unprotected link.
2. Use Table 120 to look up the one-way data capacity per time slot for the required combination of:
   - TDD Frame Duration
   - Modulation Mode
3. The one-way link capacity is the capacity per time slot from Step 2 multiplied by the number of time slots from Step 1. The aggregate (two-way) capacity is the sum of two one-way capacities.

Calculation procedure for HCMP topology with standard TDD frame

To calculate the data rate capacity of a PTP 700 link with Standard TDD Frame Configuration Mode, with or without TDD synchronization, proceed as follows:

1. Use Table 117, Table 118 or Table 119 to look up the TDD frame duration for the required combination of:
   - Channel bandwidth
   - Maximum link range
   - Maximum number of Slaves
2. Use Table 120 to look up the one-way data capacity per time slot for the required combination of:
   - TDD frame duration
   - Modulation mode
3. The one-way capacity for a single Slave is the capacity per time slot multiplied by the number of time slots. The aggregate (two-way) capacity for one Slave is the sum of two one-way capacities. The aggregate capacity for the Master is the capacity for one Slave multiplied by the number of Slaves.

Note The capacity of a link in the HCMP topology depends on the maximum link range configured in the ODU but does not depend on the range of the individual link. The number of Slaves is the maximum number that can be supported by the Master, and not the number presently connected.

Calculation example for HCMP topology with standard TDD frame

Suppose that:

- Channel Bandwidth = 40 MHz
- TDD synchronization = Disabled
- Link Symmetry = 2:1 Symmetry
- Maximum number of Slaves = 3
- Maximum Range = 15 km
- Modulation mode = 256QAM 0.81 dual.

The calculation procedure for this example is as follows:

1. Look up the TDD Frame Duration in Table 118

   Frame Duration = 3145 µs

2. Look up the time slot capacity in Table 120

   Time slot capacity = 35.32 Mbit/s

3. Calculate the capacity of the link

   The capacity for the link is 70.64 Mbit/s from Master to Slave, and 35.32 Mbit/s from Slave to Master.

   The aggregate capacity for one link is 70.64 Mbit/s + 35.32 Mbit/s = 105.96 Mbit/s.

   The aggregate capacity of the HCMP sector with three links is 3 × 105.96 Mbit/s, or 317.88 Mbit/s.

Calculation procedure for HCMP topology with expert mode TDD frame

To calculate the data rate capacity of a PTP 700 link with Standard TDD Frame Configuration Mode, with or without TDD synchronization, proceed as follows:

1. Find the number of time slots and TDD frame duration from the ODU configuration.
2. Use Table 120 to look up the one-way data capacity per time slot for the required combination of:
   - TDD frame duration
   - Modulation Mode
3. The one-way capacity for a single Slave is the capacity per time slot multiplied by the number of time slots used by that Slave. The aggregate (two-way) capacity for one Slave is the sum of two one-way capacities. The aggregate capacity for the Master is the capacity for all of the available time slots.

Planning for connectorized units

This section describes factors to be considered when planning to use connectorized ODUs with external antennas in PTP 700 links.

When to install connectorized units

PTP topology

Most radio links can be successfully deployed with the integrated antenna in the Connectorized+Integrated ODU. However, the integrated antenna may not have sufficient antenna gain 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.

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

In these areas, use the Connectorized ODU or the Connectorized+Integrated ODU with external antennas.

HCMP topology

The Master ODU in an HCMP sector will normally be installed with a connectorized antenna with sector or omni-directional coverage.

Slave ODUs in an HCMP sector will normally be installed using the integrated antenna in the Connectorized+Integrated ODU, but might be installed using a connectorized antenna, for example:

- Where the path is heavily obscured by dense woodland on an NLOS link.
- Where there are known to be high levels of interference.

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.

Configuration options for TDD synchronization

This section describes the different configuration options that may be used for implementing TDD synchronization in the PTP 700 Series. Schematic diagrams are included.

Using PTP-SYNC

The PTP 700 supports the following TDD synchronization configurations:

- Single PTP link or HCMP sector configuration with PTP-SYNC on page 3-34.
- Cluster with PTP-SYNC and GPS receiver on page 3-35.
- Cluster with PTP-SYNC and no GPS receiver on page 3-35.

Attention The PTP-SYNC is compatible only with the AC+DC Power Injector 56V.

The AC Power Injector 56V and CMM5 will not work with a PTP-SYNC, and it is likely that a fuse will be blown in the PTP-SYNC if this is attempted.

PTP-SYNC is not compatible with standards-based power-over-Ethernet (PoE).

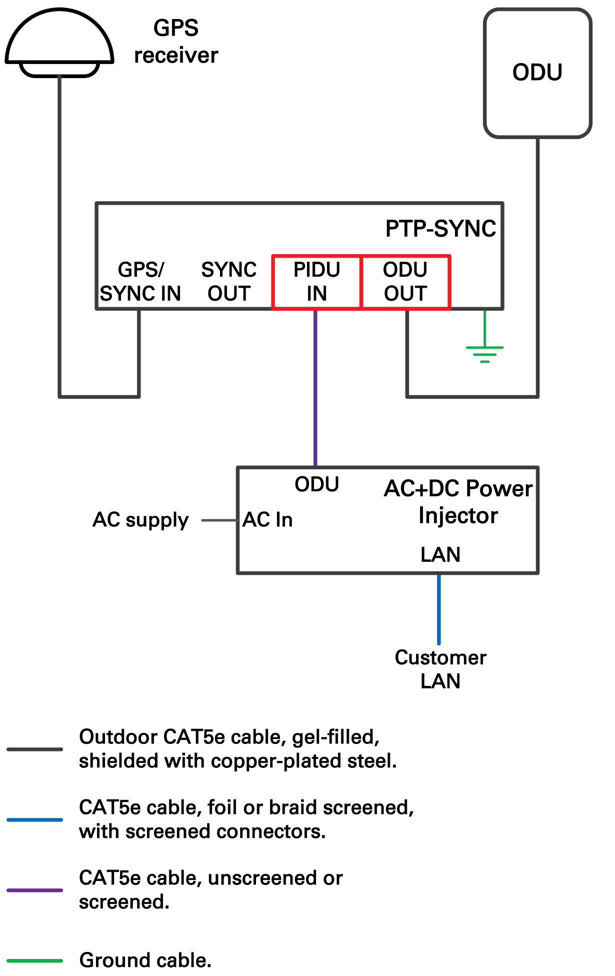
Single PTP link or HCMP sector configuration with PTP-SYNC

Each PTP link or HCMP sector requires one PTP-SYNC unit connected to the Master ODU and one compatible GPS receiver. Use this configuration where a site contains only one TDD master ODU. The GPS receiver and LPU can be replaced by an alternative compatible 1 Hz timing reference (Figure 51).

The wireless configuration settings are:

- Master Slave Mode = **Master**.
- TDD Synchronization Mode = **Enabled**.
- TDD Sync Device = **PTPSYNC**.
- Cluster Master Slave = **Cluster Master**.
- PTP Sync Site Reference = **GPS/1PPS External**.

Figure 51 TDD synchronization configuration – single link or sector with PTP-SYNC



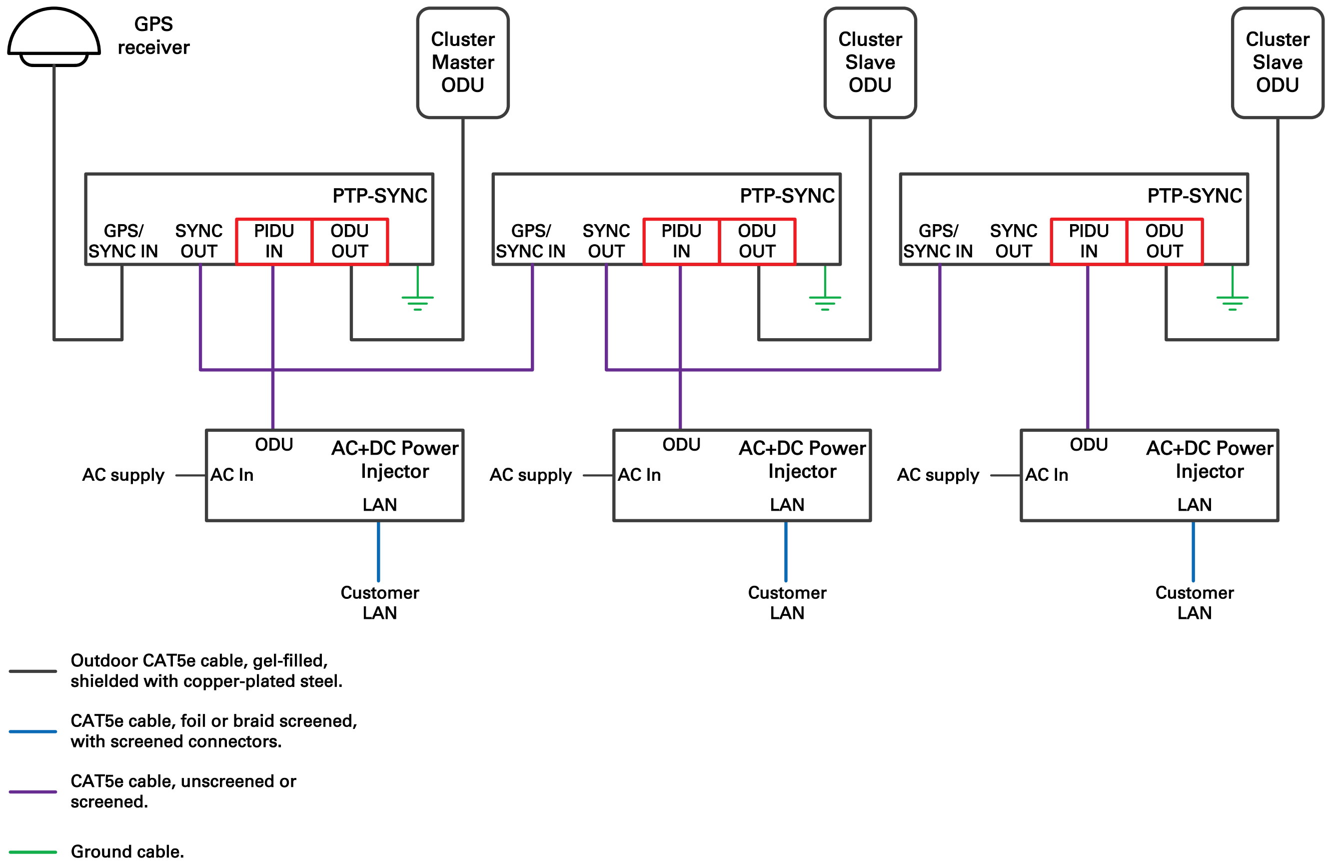
Cluster with PTP-SYNC and GPS receiver

Each PTP link or HCMP sector requires one PTP-SYNC unit. Each site requires one compatible GPS receiver. Collocated PTP-SYNC units are connected together in a daisy-chain. Between two and ten PTP-SYNCs may be chained in this way. Use this configuration where a site contains collocated TDD Master ODUs in an extended network and where multiple sites have TDD master ODUs (Figure 52).

The wireless configuration settings are:

- Master Slave Mode = **Master** (all ODUs in cluster).
- TDD Synchronization Mode = **Enabled**.
- TDD Sync Device = **PTPSYNC** (all ODUs in cluster).
- Cluster Master Slave = **Cluster Master** (first ODU) and **Cluster Slave** (others).
- PTP Sync Site Reference = **GPS/1PPS External** (all ODUs in cluster).

Figure 52 TDD synchronization configuration – cluster with PTP-SYNC and GPS



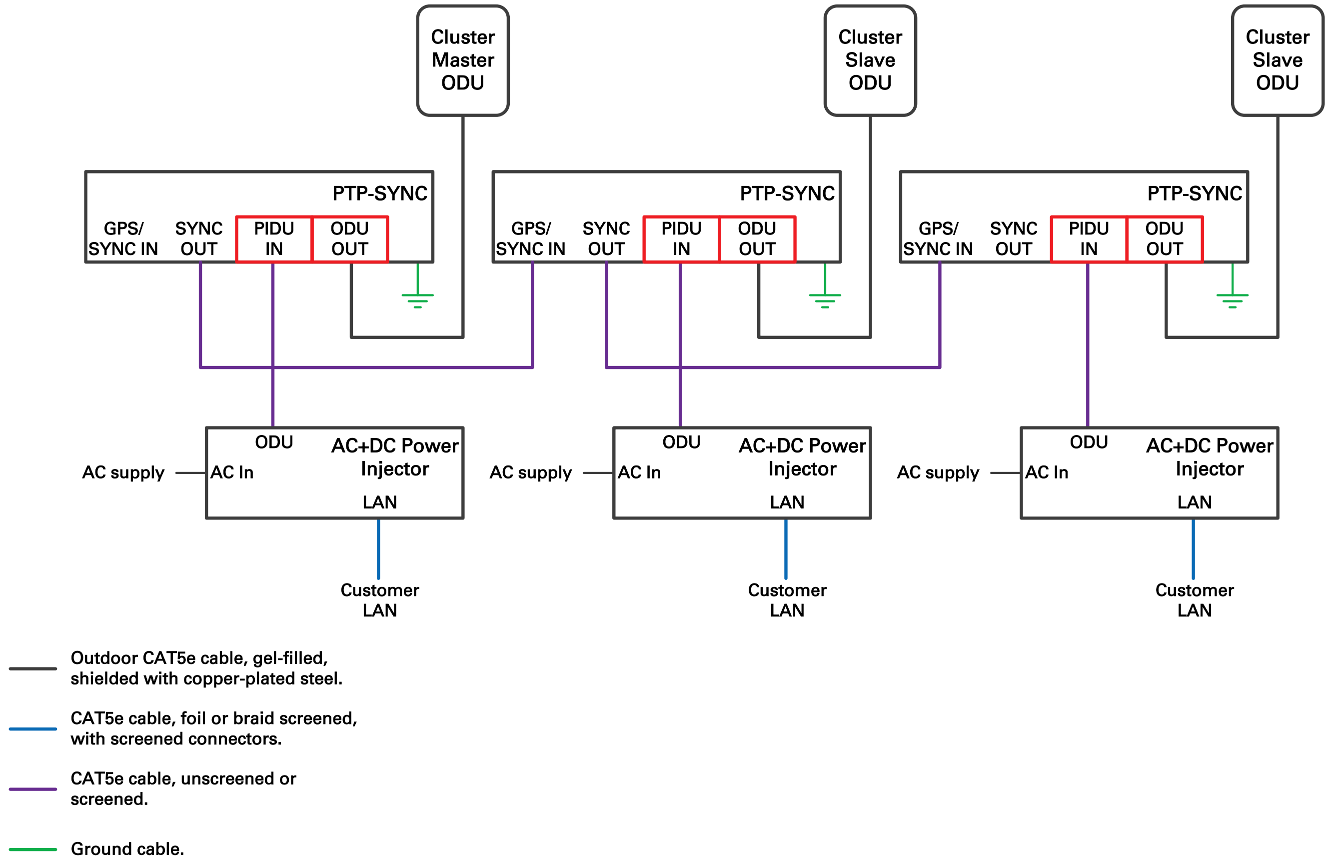
Cluster with PTP-SYNC and no GPS receiver

Each PTP link or HCMP sector requires one PTP-SYNC unit. PTP-SYNC units are connected together in a daisy-chain. Between two and ten PTP-SYNCs may be chained in this way. One ODU is designated as a cluster master. Use this configuration where all Master ODUs are colocated at a single site. As this configuration does not require a GPS receiver, it provides additional flexibility, particularly in applications requiring rapid deployment (Figure 53).

The wireless configuration settings are:

- Master Slave Mode = **Master** (all ODUs in cluster).
- TDD Synchronization Mode = **Enabled**.
- TDD Sync Device = **PTPSYNC** (all ODUs in cluster).
- Cluster Master Slave = **Cluster Master** (first ODU) and **Cluster Slave** (others).
- PTP Sync Site Reference = **Internal** (all ODUs in cluster).

Figure 53 TDD synchronization configuration – cluster with PTP-SYNC and no GPS



Using CMM5

Each ODU must be connected to the CMM5 Power and Sync Injector. The CMM5 Power and Sync Injector must be connected directly or indirectly to a UGPS receiver.

The wireless configuration settings are:

- Master Slave Mode = **Master** (all ODUs in cluster).
- TDD Synchronization Mode = **Enabled**.
- TDD Sync Device = **Cambium Sync Injector**.
- Cambium Sync Input Port = **Main PSU**.
- Cambium Sync Output Port = **None**.

Using a direct connection between ODUs

Aux Port to Aux Port

Configure one ODU to provide a free-running reference with the following settings:

- Master Slave Mode = **Master** (all ODUs in cluster).
- TDD Synchronization Mode = **Enabled**.
- TDD Sync Device = **Cambium Sync Injector**.
- Cambium Sync Input Port = **Internal**.
- Cambium Sync Output Port = **Aux**.

Configure a second ODU to synchronize with the first ODU with the following settings:

- Master Slave Mode = **Master** (all ODUs in cluster).
- TDD Synchronization Mode = **Enabled**.
- TDD Sync Device = **Cambium Sync Injector**.
- Cambium Sync Input Port = **Aux**.
- Cambium Sync Output Port = **None**.

Aux Port to Main PSU Port

Configure one ODU to provide a free-running reference and auxiliary power to a second ODU with the following settings:

- Master Slave Mode = **Master** (all ODUs in cluster).
- TDD Synchronization Mode = **Enabled**.
- TDD Sync Device = **Cambium Sync Injector**.
- Cambium Sync Input Port = **Internal**.
- Cambium Sync Output Port = **Aux**.
- Aux Port Power Over Ethernet Output = **Enabled**.

Configure a second ODU to synchronize with the first ODU with the following settings:

- Master Slave Mode = **Master** (all ODUs in cluster).
- TDD Synchronization Mode = **Enabled**.

- TDD Sync Device = Cambium Sync Injector.
- Cambium Sync Input Port = Main PSU.
- Cambium Sync Output Port = None.

Data network planning

This section describes factors to be considered when planning PTP 700 data networks.

Ethernet bridging

Table 47 summarizes Ethernet bridging specifications for PTP 700.

Table 47 PTP 700 Ethernet bridging specifications

Ethernet Bridging	Specification
Protocol	IEEE802.1; IEEE802.1p; IEEE802.3 compatible
QoS	PTP topology: 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, DSCP in PPP Session Stage HCMP topology: Four 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, DSCP in PPP Session Stage
Interfaces	100BASE-TX, 1000BASE-T, 1000BASE-SX, 1000BASE-LX MDI/MDIX auto crossover supported
Max Ethernet frame size	9600 bytes
Service classes for traffic	PTP topology: Eight classes HCMP topology: Four 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 two control protocols

PTP 700 identifies layer two control protocols (L2CPs) from the Ethernet destination address of bridged frames. The QoS classification can be separately configured for these protocols.

Table 48 Destination address in layer two 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)

Destination address	Protocol
00-e0-2b-00-00-04	Ethernet Automatic Protection Switching (EAPS)

Ethernet port allocation

Note Port allocation options are restricted (and thereby simplified) when Hot Standby link protection is used. See Ethernet port allocation in Hot Standby protection on page 3-44 for further details.

Port allocation rules

Decide how the three ODU Ethernet ports will be allocated to the Data Service, Management Service and Local Management Service based on the following rules:

- Map the **Data Service** to at least one of the available wired Ethernet ports.
- Map the **Management Service** to **In-Band**, or to any combination of the remaining unused Ethernet ports. If the Management Service is mapped to **In-Band**, it shares all of the ports selected for the Data Service. The Management Service can be disabled by mapping to **None**.
- Map the **Local Management Service** to any combination of the remaining unused Ethernet ports. The Local Management Service can be disabled by mapping to **None**.

The LAN Configuration page ensures that the Management Agent can always be reached using either the **Management Service** or the **Local Management Service**.

Mapping of ports and services

The rules described above allow for the following thirteen distinct combinations of services:

Table 49 Combinations of services for one ODU

Service combination			Figure
Port #1	**Port #2**	**Port #3**	
Data	Local Management		
Data	Local Management	Local Management	Figure 54
Data	Out-of-Band Management		
Data	Out-of-Band Management	Out-of-Band Management	Figure 55
Data	Out-of-Band Management	Local Management	Figure 56
Data	Data	Out-of-Band Management	Figure 57
Data	Data	Local Management	Figure 58
Data with In-Band			
Data with In-Band	Local Management		

Data with In-Band	Local Management	Local Management	Figure 59
Data with In-Band	Data with In-Band		
Data with In-Band	Data with In-Band	Local Management	Figure 60
Data with In-Band	Data with In-Band	Data with In-Band	Figure 61

Figure 54 to Figure 61 illustrate the internal routing of Ethernet traffic in eight three-port combinations of the services listed in Table 49.

Figure 54 Ports and Services: Data + Local + Local

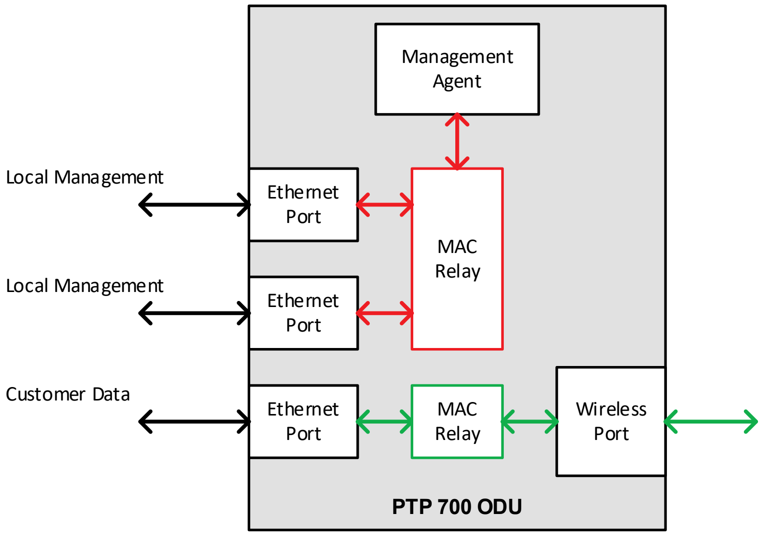


Figure 55 Ports and Services: Data + Out-of-Band + Out-of-Band

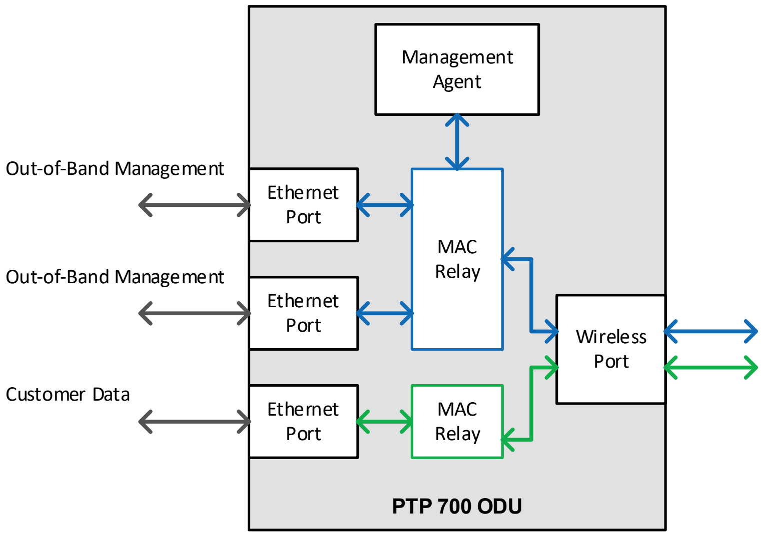


Figure 56 Ports and Services: Data + Out-of-Band + Local

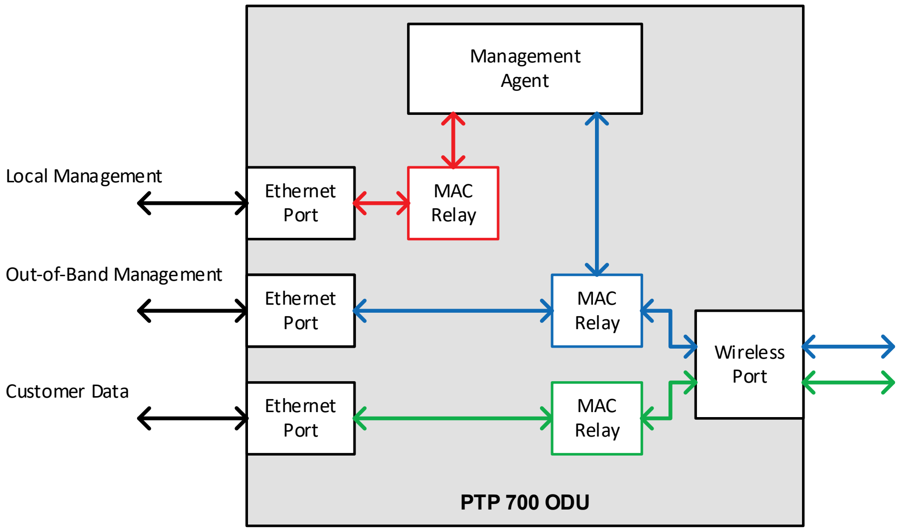


Figure 57 Ports and Services: Data + Data + Out-of-Band

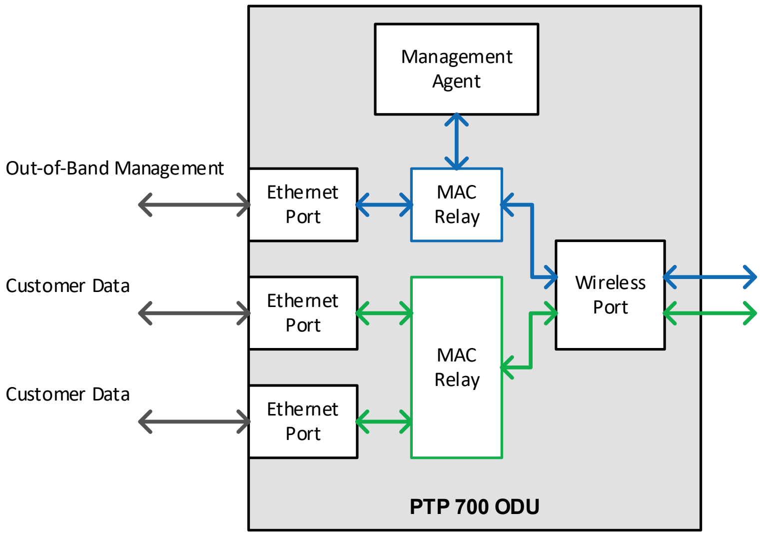


Figure 58 Ports and Services: Data + Data + Local

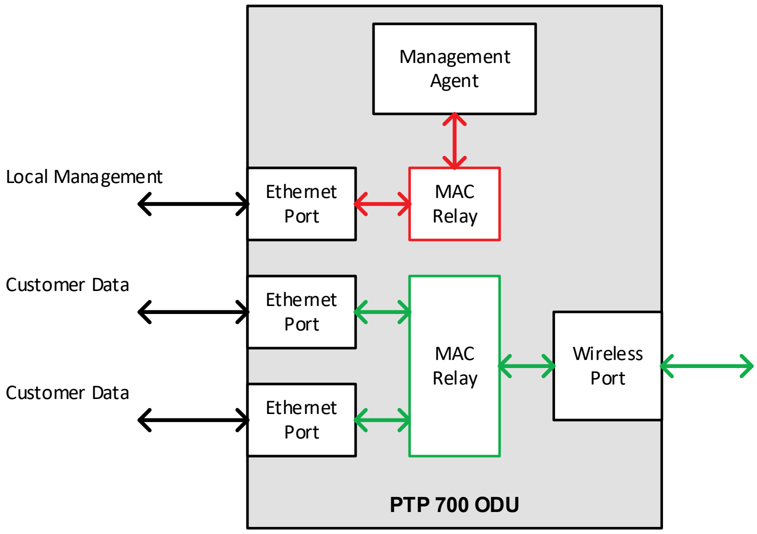


Figure 59 Ports and Services: Data/In-Band + Local + Local

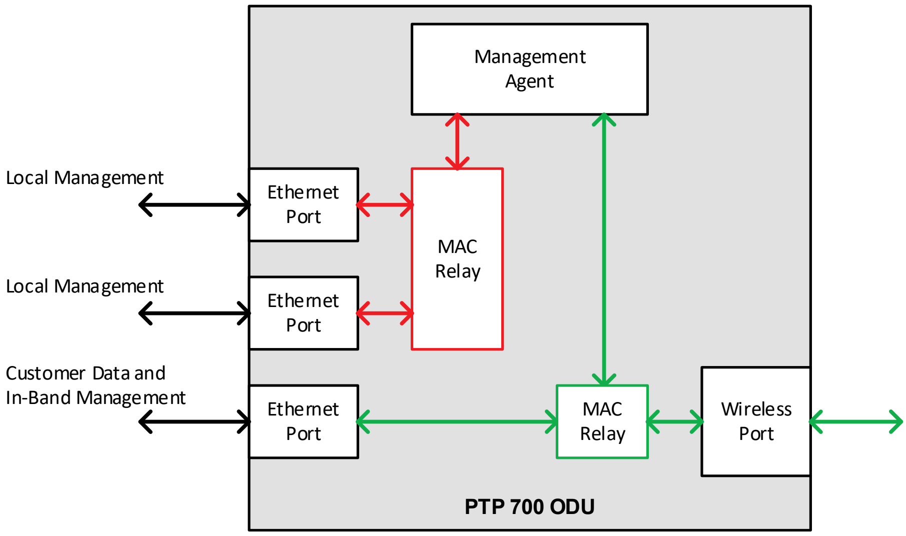


Figure 60 Ports and Services: Data/In-Band + Data/In-Band + Local

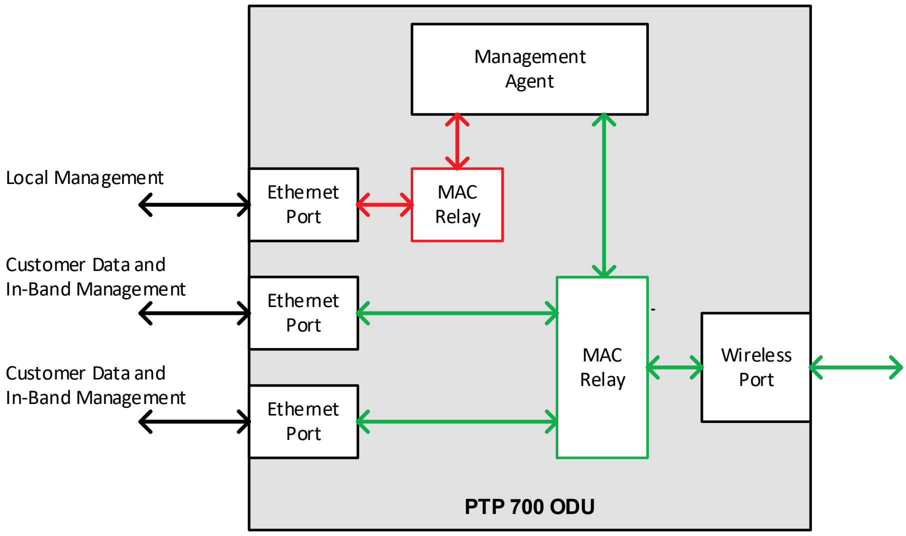
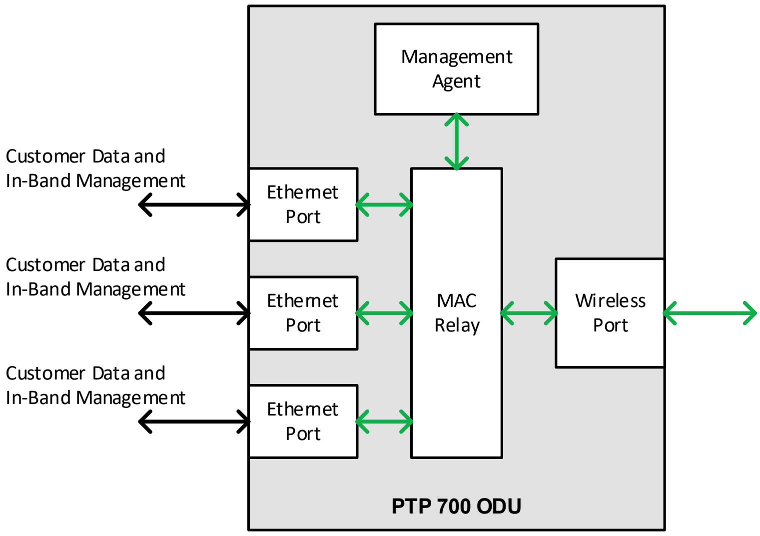


Figure 61 Ports and Services: Data/In-Band + Data/In-Band + Data/In-Band



Use a compatible combination of services at both ends of the link

PTP 700 supports flexible allocation of ports to services, and this allocation may be different at the two ends of the link. However, the management service configuration must be compatible between the two ends of the link. Ensure that both ends of the link are configured for In-Band management, or both ends are configured for Out-of-Band Management, or the management services is disabled at both ends.

Warning Do not mix In-band and Out-of-Band management in the same link.

Additional port allocation rules

The three Ethernet ports are generally interchangeable, except for some specific additional rules listed below:

- If the system is to be used in a Synchronous Ethernet hierarchy, ensure that the upstream timing source is connected to the Main PSU or Fiber SFP ports (downstream devices can be connected to any port)
- If the system is operating as an IEEE 1588-2008 Transparent Clock, ensure the data path does not traverse the Copper SFP port.

Note The Main PSU port is always used to supply power to the ODU, even when it is not allocated to a data or management service.

Note The procedure for configuring these ports at the web interface is described in LAN Configuration page on page 6-46.

Note Transparent Clock is not supported over the SFP port with Copper connectivity.

Ethernet port allocation in Hot Standby protection

Decide how the three ODU Ethernet ports will be allocated to the Data Service, Management Service, Local Management Service or Protection service based on the following rules:

- Map the **Data Service** to exactly one of the available wired Ethernet ports. This will normally be the Main PSU port but need not be so.
- Map the **Protection Service** to either the Aux port or the SFP port.
- Map the **Management Service** to **In-Band**, or to the remaining wired Ethernet Port. The Management Service can be disabled by mapping to **None**.

- If the **Management Service** is mapped to **None**, map the **Local Management Service** to the remaining unused Ethernet port. Otherwise, all three ports are already in use, and the **Local Management Service** must be disabled by mapping to **None**.

The LAN Configuration page ensures that the Management Agent can always be reached using either the **Management Service** or the **Local Management Service**.

The rules described above allow for the following four distinct combinations of services:

Table 50 Combinations of services for one Hot Standby ODU

Service combination			Figure
Port #1	**Port #2**	**Port #3**	
Protection	Data	Local Management	Figure 62
Protection	Data	Out-of-Band Management	Figure 63
Protection	Data with In-Band		Figure 64
Protection	Data with In-Band	Local Management	Figure 65

Figure 62 Ports and Services: Protection + Local + Data

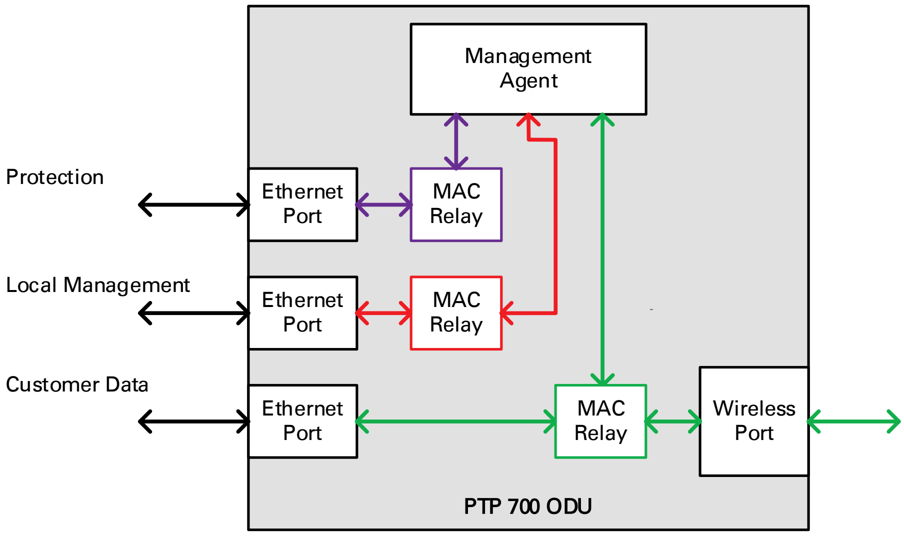


Figure 63 Ports and Services: Protection + Out-of-Band + Data

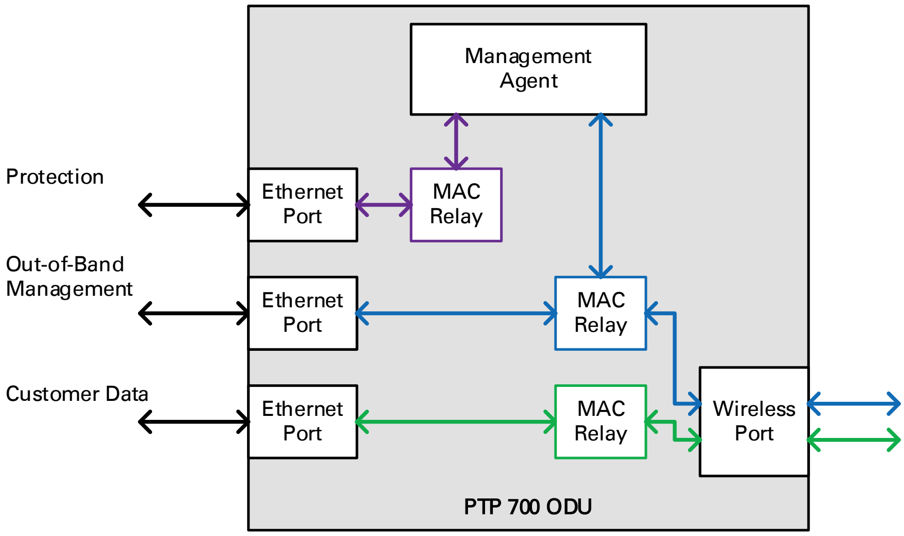


Figure 64 Ports and Services: Protection + Data/In-Band

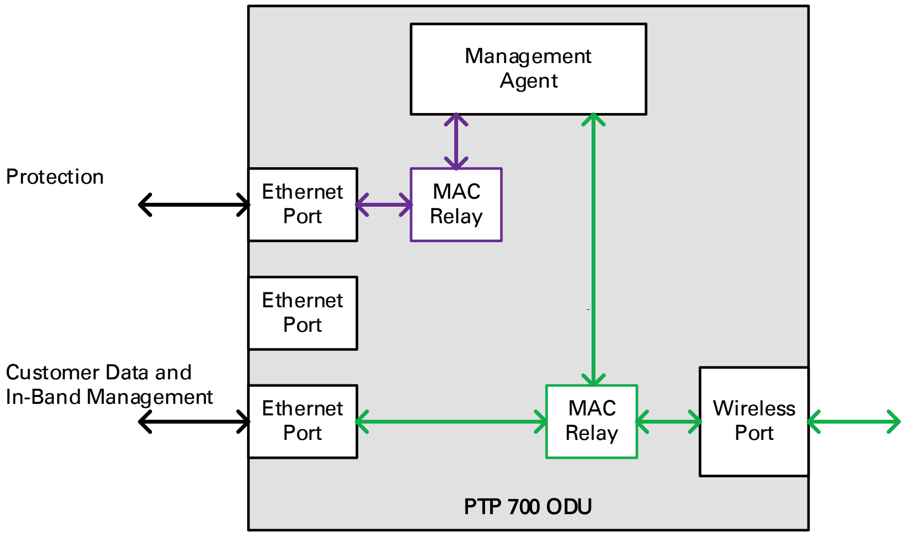
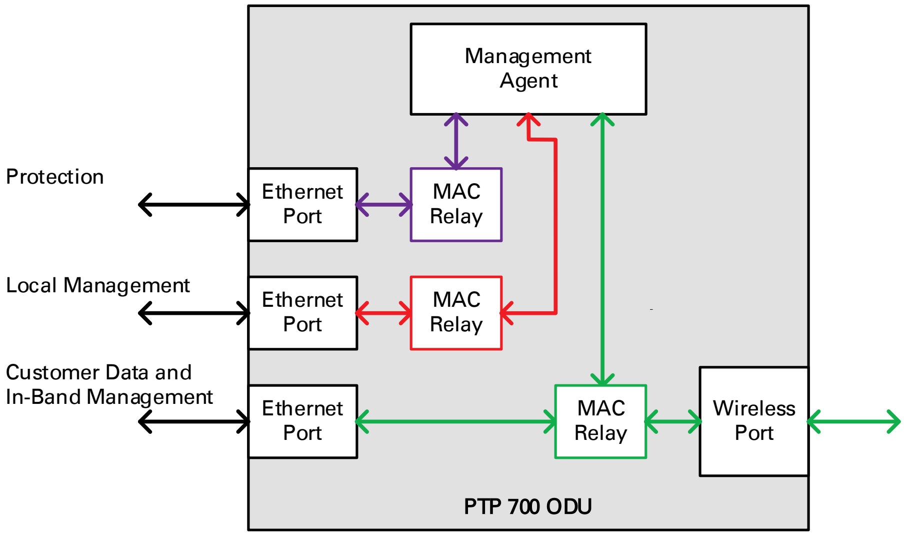


Figure 65 Ports and Services: Protection + Local + Data/In-Band



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.

If the system is to operate as an IEEE 1588-2008 Transparent Clock, decide if residence time corrections should be made to:

- All 1588 event frames, regardless of VLAN membership, or
- Only 1588 event frames in a specific customer bridged VLAN, or
- Only 1588 event frames in a specific provider bridged VLAN

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 700 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 700 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.

In the PTP topology, PTP 700 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.

In the HCMP topology the general arrangement is similar but the ODU provides four queues for traffic awaiting transmission in each of the wireless links.

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 700 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 determined by the DSCP value encoded in the ToS field in IPv4 and Traffic Class in IPv6. PTP 700 can locate the DSCP value in IP headers encapsulated within VLAN tags and/or PPP and PPPoE headers. The DSCP field provides 64 levels of priority. PTP 700 selects a suitable mapping from these DSCP values to the eight (PTP) or four (HCMP) PTP 700 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) or four (HCMP) PTP 700 queues.

“Daisy-chaining” PTP 700 links

When connecting two or more PTP 700 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 700 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 2-23.

- 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 2-23.
- 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 2-29.

Green Ethernet switches

Do not connect PTP 700 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 700 PSU.

Network management planning

Planning for cnMaestro

When configured for management using cnMaestro, the PTP 700 ODU creates an outgoing HTTPS connection to the server from the IP interface of the management agent. To use the cnMaestro Cloud server, ensure that the management network allows outgoing connections to the public Internet. This normally involves the use of a security firewall to protect the management network from incoming connections. To use the On-Premises server, ensure that the server is reachable from the PTP 700 management network.

PTP 700 ODUs are authenticated to the cnMaestro server as part of the Onboarding process to prevent them from being claimed by other operators. To use the ODU's MAC Addresses for device authentication, ensure that the device is included in the list of PTP 700 device addresses on the server. To use Cambium ID for device authentication, ensure that the Cambium ID is known for the network, and ensure that a suitable Onboarding Key is configured on the server and issued to the installer.

To use a Fully Qualified Domain Name (FQDN) for the server address, ensure that the DNS feature is enabled and configured in the PTP 700. The FQDN (and thus DNS) is always used for the cnMaestro Cloud server.

Planning for SNMP operation

This section describes how to plan for PTP 700 links to be managed remotely using SNMP.

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 700 Series proprietary MIB

Note The proprietary MIBs are provided in the PTP 700 Series software download files in the support website (see Contacting Cambium Networks on page 1).

Supported diagnostic alarms

PTP 700 supports the diagnostic alarms listed in Table 179.

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)

Planning for Domain Name Service (DNS)

The PTP 700 Management Agent supports use of an external DNS server to resolve the Domain Name configured for network management servers to IPv4 or IPv6 addresses. PTP 700 allows one or two DNS servers to be configured.

To use DNS, establish the network address of the DNS server or servers as follows:

- DNS Server 1 IPv4 or IPv6 address
- DNS Server 1 Port Number (default 53)
- DNS Server 2 IPv4 or IPv6 address
- DNS Server 2 Port Number (default 53)

Select DNS Server 1 or DNS Server 2 as the Primary Server.

Establish some or all of the following server addresses as Fully Qualified Domain Names (FQDN):

- cnMaestro Server
- RADIUS Server
- SMTP Server
- SNMP Trap
- SNTP Server
- Syslog Server

- TFTP Server

The FQDN must comply with the following:

- Not longer than 63 characters
- Must contain some structure (at least one “.”)
- Must consist of only the characters “0”..”9”, “a”..”z”, “A”..”Z”, "$", hyphen, underscore, dot/stop, plus, exclamation, star, single quote, left parenthesis, right parenthesis

Hot Standby links

The four ODUs in a Hot Standby link are managed separately, through four unique IP addresses. The Primary ODU is not a proxy for managing the corresponding Secondary ODU.

Security planning

This section describes how to plan for PTP 700 links to operate in secure mode.

License key DSA signature

The License Key used to enable individually-licensed ODU capabilities is signed with a DSA signature based on a 1024-bit key pair and, optionally, with a DSA signature based on a 2048-bit key pair.

For the highest levels of security, ensure that License Keys have the 2048-bit DSA signature. If necessary, re-generate the License Key using the Cambium Networks support web site to obtain a key with the larger signature size.

The 2048-bit DSA signature is encoded in the License Key using the “/Q” field. The 1024-bit DSA signature is encoded using the “/K” field. See Figure 66 for an example of a License Key with 1024-bit and 2048-bit DSA signatures.

Figure 66 Example License Key with 2048-bit DSA signature

```
/A 5800B8
/C Other
/I 1
/P 1
/R 8 /R 35 /R 61 /R 62 /R 81
/H M2XF5UCQSLWOCQ63ALLV2CHSTM======
/Q DT2E33OFPJ4MLUII5YXWXH3QFANHXVCVSHGEN2ZNS6BNLY255OJEWEZDIATQNR4WEL
NPMROSTFNSNKD7NLUQCZEM3CGBPJDR5RV4O5A=
/K K5JKJMLIYEUJ2SISRCQSLL4X3IJL7O5XVOXYQ5LZ2CCX5MWU53UH7FTTBEJZJ5WT/
```

Planning for SNTP operation

Note PTP 700 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: FQDN or IP address, port number and server key.
- Establish if the NTP server is configured for authenticated operation. If NTP is authenticated, determine if authentication is based on MD5 or SHA-1, and identify the associated server keys.

Using the Security Wizard

Basic wireless encryption can be configured without using the Security Wizard, by using only the System Configuration page and optionally the Authorization Control page. For other security features, use the Security Wizard.

Plan to use the Security Wizard for the following:

- To configure the Key of Keys. The Key of Keys is used to encrypt non-volatile Critical Security Parameters for storage in the ODU. The Key of Keys is erased by the Zeroize CSPs action, meaning that stored CSPs cannot later be accessed, even by an attacker with internal access to the ODU memory.
- To configure Entropy. Entropy is an externally-generated random number used as a seed in many of the cryptographic methods implemented within the ODU. Generate Entropy in an approved random number generator and install in the ODU to enhance security in wireless encryption and HTTPS/TLS.
- To install user-supplied certificates and configure HTTPS/TLS for the web-based management interface.
- To install optional user-supplied device certificates for TLS-RSA. User-supplied device certificates provide enhanced security for TLS-RSA.
- To configure an optional banner providing warnings and notices to be read by the user before logging in to the ODU.

Note The Key of Keys attribute must be configured using the Security Wizard. It cannot be updated after the Security Wizard is submitted, except by first zeroizing CSPs.

Table 51 Security Wizard attributes

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.
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.
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.

Planning for wireless encryption

AES license

Ensure that both ODUs have an AES license that allows the required key size for wireless encryption. The 128-bit AES license allows 128-bit encryption. The 256-bit AES license allows 128-bit and 256-bit encryption.

TLS-RSA can be used without an AES license, but this option supports only authentication and authorization, but not encryption.

Encryption algorithms

Select one of the three supported Encryption Algorithms:

- TLS-RSA
- TLS-PSK 128-bit
- TLS-PSK 256-bit

Configure the same algorithm at both ends of the link.

TLS-RSA provides authentication and authorization in any ODU. This option additionally provides encryption if both ODUs have an AES license.

TLS-PSK 128-bit provides authentication, authorization and encryption using a 128-bit pre-shared key. TLS-PSK 128-bit requires the 128-bit or 256-bit AES license.

TLS-PSK 256-bit provides authentication, authorization and encryption using a 256-bit pre-shared key. TLS-PSK 256-bit requires the 256-bit AES license.

TLS-RSA

Determine TLS Minimum Security Level. This is the smallest key size that will be allowed in a link between Master and Slave. For example, if the Master has TLS Minimum Security Level of 128-bit AES and the Slave has no AES license then the link cannot be established.

In a network where all links must be encrypted, set TLS Minimum Security Level to TLS RSA 128-bit or TLS RSA 256-bit to prevent inadvertent connection of unencrypted links.

Select Factory-installed or User-supplied device certificates. Factory-installed certificates are convenient because they can be used without needing to generate any additional cryptographic material. Generate and install User-supplied certificates where the additional security of 2048-bit key size is required, or where there is an operational requirement to be able to zeroize the private key in the event that the ODU may be compromised.

For Group Access, select Whitelist or Blacklist operation. The selection of Whitelist and Blacklist is independent of the selection of Factory or User-provided certificates.

> **Note** The default combination of Blacklist and Factory certificates offers limited benefits in a deployed network, because the system will authorize any genuine PTP 700 ODU. Use the Whitelist and/or User-supplied certificates to ensure that access is allowed only for trusted ODUs.

A disadvantage of TLS-RSA is that the Whitelist must be updated if new hardware is introduced to the network. This may require access to both ends of the link. Consider using TLS-PSK if it is important to replace hardware without needing access to both ends of the link.

TLS-RSA is not available if Access Method is configured for Link Name Access.

Install User-supplied device certificates using the Security Wizard.

Table 52 User-supplied device certificates for wireless encryption

Item	Description	Quntity required
Device Private Key and Public Certificates	An RSA private key of size 2048 bits, generated in either PKCS#1 or PKCS#5 format, unencrypted, and encoded in the ASN.1 DER format. An X.509 certificate containing a 2048-bit RSA public key, signed using SHA-256, 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 MAC address of the ODU as a string of 12 hexadecimal characters without punctuation. The public key certificate must form a valid pair with the private key.	Two pairs per link. These items are unique to the MAC address.
Root CA Public Certificate	The self-signed public key certificate for the Root CA that signed the Device Certificate in the remote ODU. The Root CA must form a certificate chain with the Device Certificate without intermediate certificates.	Normally one per network.

TLS-PSK

Select the key size for the pre-shared key. This must be supported by AES licenses at each end of the link.

TLS-PSK can be used with Access Method of Link Access, Link Name Access and Group Access.

Ensure that the following cryptographic material is available.

Table 53 Pre-shared Key for wireless encryption

Item	Description	Quntity required
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.

Hot Standby

In a PTP link with Hot Standby, the Primary Master ODU does not connect to the Secondary Slave ODU (or the Secondary Master with the Primary Slave) and so encryption in the Primary and Secondary links can and should be configured independently.

When TLS-PSK is used, configure a PSK for the Primary link and a different PSK for the Secondary link.

Planning for HTTPS/TLS operation

Before starting to configure HTTPS/TLS operation, ensure that the cryptographic material listed in Table 54 is available.

Table 54 HTTPS/TLS security material

Item	Description	Quantity required
TLS Private Key and Public Certificates	An RSA private key of size 2048 bits, generated in either PKCS#1 or PKCS#5 format, unencrypted, and encoded in the ASN.1 DER format. An X.509 certificate containing a 2048-bit RSA public key, signed using SHA-256, 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.

Planning for protocols and ports

Detemine the protocols that will be enabled at the Management Agent, and the port numbers to be used.

Table 55 Protocol and port settings

Item	Description	Quantity required
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 700 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 700 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 56.

Table 56 Permitted character set for SNMPv3 passphrases

Character	Code	Character	Code
<space>	32	;	59
!	33	<	60
“	34	=	61
#	35	>	62

Character	Code	Character	Code
$	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 57.

Table 57 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 700 creates default view trees and access as shown in Table 58 and Table 59.

Table 58 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 59 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 700. 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 700 provides a choice of the following authentication methods:

- CHAP
- MS-CHAPv2

Ensure that the authentication method selected in PTP 700 is supported by the RADIUS server.

Note The RADIUS feature is disabled in FIPS 140-2 approved mode.

RADIUS attributes

If the standard RADIUS attribute session-timeout (Type 27) is present in a RADIUS response, PTP 700 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 700 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 700 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 700 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 700 selects the Read Only role.

The auth-role vendor-specific attribute is defined in Table 60.

Table 60 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).

Internally-generated random keys

In networks that carry sensitive data, generate random security keys in an approved external system. This is the only approach that guarantees the highest level of entropy. Random keys are required for the following security parameters:

- Key of keys
- Entropy
- TLS-PSK in the Security Wizard
- TLS-PSK in the Configuration page

PTP 700 provides an alternative option to generate random keys within the ODU. This method cannot match the entropy of the best external random number generators, but nevertheless offers a useful option where ultimate security is not needed.

Planning for FIPS 140-2 operation

If the link is to operate in FIPS 140-2 secure mode, ensure that the following cryptographic material is generated using a FIPS-approved cryptographic generator:

- Key of Keys
- Entropy Input

- TLS Private Key and Public Certificates, RSA 2048-bit key size, signed using the SHA-256 Secure Hash Algorithm.
- For TLS-RSA:
  - Device Private Key and Public Certificates RSA 2048-bit key size, signed using the SHA-256 Secure Hash Algorithm.
  - Root CA Certificate for Device Certificates.
- For TLS-PSK:
  - Wireless Link Pre-shared Key for AES

Internal generation of random numbers is not available in the FIPS-approved mode.

Ensure that the web browsers used are enabled for HTTPS/TLS operation using FIPS-approved cipher specifications.

Ensure that following attributes of user accounts for the web-based management interface have been configured to match the operator's network security policy:

- Auto Logout Period.
- Maximum Number of Login Attempts.
- Login Attempt Lockout.
- Minimum Password Change Period.
- Password Expiry Period.
- Webpage Session Control

Ensure that the following are configured:

- User account passwords compliant with the network security policy.

Ensure that the License Key has the larger DSA signature based on the 2048-bit key pair.

Attention Configure all the above correctly to ensure that PTP 700 is operating in compliance with the FIPS 140-2 validation.

Further reading

For information about...	Refer to...
Generating security material for the HTTPS/TLS interface	Planning for HTTPS/TLS operation on page 3-57

System threshold, output power and link loss

Use the following tables to look up the system threshold (dBm), output power (dBm) and maximum link loss (dB) per channel bandwidth and modulation mode:

Platform variant	Band	Mode	System threshold and output power (dBm)	Maximum link loss (dB)
Connectorized+ Integrated	4.7 GHz	IP	Table 61	Table 62
		TDM	Table 63	Table 64
	4.9 GHz	IP	Table 65	Table 66
		TDM	Table 67	Table 68
	5.1 GHz and 5.2 GHz	IP	Table 69	Table 70
		TDM	Table 71	Table 72
	5.4 GHz	IP	Table 73	Table 74
		TDM	Table 75	Table 76
	5.8 GHz	IP	Table 77	Table 78
		TDM	Table 79	Table 80
Connectorized	4.7 GHz	IP	Table 81	Table 82
		TDM	Table 83	Table 84
	4.9 GHz	IP	Table 85	Table 86
		TDM	Table 87	Table 88
	5.1 GHz and 5.2 GHz	IP	Table 89	Table 90
		TDM	Table 91	Table 92
	5.4 GHz	IP	Table 93	Table 94
		TDM	Table 95	Table 96
	5.8 GHz	IP	Table 97	Table 98
		TDM	Table 99	Table 100

Note Maximum link loss has been calculated assuming use of the integrated antenna in PTP 700 Connectorized+Integrated ODUs.

Note For the discontinued Connectorized ODUs Cambium part number C045070B003A and C045070B009A use the tables for Connectorized+Integrated ODUs.

Connectorized+Integrated ODUs

Table 61 4.7 GHz IP mode: system threshold per channel bandwidth and output power (P) (dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-93.5	-92.0	-90.2	-89.0	-87.2	-86.0	-85.5	28
QPSK 0.63 single	-90.0	-88.5	-86.7	-85.5	-83.7	-82.5	-82.0	27
QPSK 0.87 single	-86.0	-84.5	-82.7	-81.5	-79.7	-78.5	-77.9	26
16QAM 0.63 single	-84.1	-82.6	-80.8	-79.5	-77.8	-76.5	-76.0	25
16QAM 0.63 dual	-81.0	-79.5	-77.8	-76.5	-74.8	-73.5	-73.0	25
16QAM 0.87 single	-79.4	-77.9	-76.1	-74.8	-73.1	-71.8	-71.3	24
16QAM 0.87 dual	-76.3	-74.8	-73.0	-71.8	-70.0	-68.8	-68.3	24
64QAM 0.75 single	-76.4	-74.9	-73.1	-71.9	-70.1	-68.9	-68.4	23
64QAM 0.75 dual	-73.3	-71.8	-70.0	-68.8	-67.0	-65.8	-65.3	23
64QAM 0.92 single	-72.6	-71.1	-69.4	-68.1	-66.3	-65.1	-64.6	23
64 QAM 0.92 dual	-69.4	-67.9	-66.1	-64.8	-63.1	-61.8	-61.3	23
256QAM 0.81 single	-69.4	-67.9	-66.1	-64.8	-63.1	-61.8	-61.3	23
256QAM 0.81 dual	-65.8	-64.3	-62.5	-61.3	-59.5	-58.3	-57.8	23

Table 62 4.7 GHz IP mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	166.7	165.2	163.4	162.2	160.4	159.2	158.7
QPSK 0.63 single	162.2	160.7	158.9	157.7	155.9	154.7	154.2
QPSK 0.87 single	157.2	155.7	153.9	152.7	150.9	149.7	149.1
16QAM 0.63 single	154.3	152.8	151.0	149.7	148.0	146.7	146.2
16QAM 0.63 dual	149.8	148.2	146.5	145.2	143.5	142.2	141.7
16QAM 0.87 single	148.6	147.1	145.3	144.0	142.3	141.0	140.5
16QAM 0.87 dual	145.5	144.0	142.2	141.0	139.2	138.0	137.5
64QAM 0.75 single	144.6	143.1	141.3	140.1	138.3	137.1	136.6
64QAM 0.75 dual	141.5	140.0	138.2	137.0	135.2	134.0	133.5
64QAM 0.92 single	140.8	139.3	137.6	136.3	134.5	133.3	132.8
64 QAM 0.92 dual	137.6	136.1	134.3	133.0	131.3	130.0	129.5
256QAM 0.81 single	137.6	136.1	134.3	133.0	131.3	130.0	129.5
256QAM 0.81 dual	134.0	132.5	130.7	129.5	127.7	126.5	126.0

Table 63 4.7 GHz TDM mode: System threshold per channel bandwidth and output power (P) (dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-93.5	-92.0	-90.2	-89.0	-87.2	-86.0	-85.5	26
QPSK 0.63 single	-87.0	-85.5	-83.7	-82.5	-80.7	-79.5	-79.0	25
QPSK 0.87 single	-83.0	-81.4	-79.7	-78.4	-76.7	-75.4	-74.9	24
16QAM 0.63 single	-81.0	-79.5	-77.7	-76.5	-74.7	-73.5	-73.0	23
16QAM 0.63 dual	-78.0	-76.5	-74.7	-73.4	-71.7	-70.4	-69.9	23
16QAM 0.87 single	-76.2	-74.7	-72.9	-71.7	-69.9	-68.7	-68.2	23
16QAM 0.87 dual	-73.1	-71.6	-69.8	-68.6	-66.8	-65.6	-65.0	23
64QAM 0.75 single	-73.1	-71.6	-69.8	-68.6	-66.8	-65.6	-65.1	23
64QAM 0.75 dual	-69.9	-68.4	-66.6	-65.3	-63.6	-62.3	-61.8	23
64QAM 0.92 single	-70.8	-69.3	-67.5	-66.3	-64.5	-63.3	-62.8	23
64 QAM 0.92 dual	-67.4	-65.9	-64.1	-62.9	-61.1	-59.9	-59.4	23
256QAM 0.81 single	-69.4	-67.9	-66.1	-64.8	-63.1	-61.8	-61.3	23
256QAM 0.81 dual	-65.8	-64.3	-62.5	-61.3	-59.5	-58.3	-57.8	23

Table 64 4.7 GHz TDM mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	164.7	163.2	161.4	160.2	158.4	157.2	156.7
QPSK 0.63 single	157.2	155.7	153.9	152.7	150.9	149.7	149.2
QPSK 0.87 single	152.2	150.6	148.9	147.6	145.9	144.6	144.1
16QAM 0.63 single	149.2	147.7	145.9	144.7	142.9	141.7	141.2
16QAM 0.63 dual	144.7	143.2	141.4	140.2	138.4	137.1	136.6
16QAM 0.87 single	144.4	142.9	141.1	139.9	138.1	136.9	136.4
16QAM 0.87 dual	141.3	139.8	138.0	136.8	135.0	133.8	133.2
64QAM 0.75 single	141.3	139.8	138.0	136.8	135.0	133.8	133.3
64QAM 0.75 dual	138.1	136.6	134.8	133.5	131.8	130.5	130.0
64QAM 0.92 single	139.0	137.5	135.7	134.5	132.7	131.5	131.0
64 QAM 0.92 dual	135.6	134.1	132.3	131.1	129.3	128.1	127.6
256QAM 0.81 single	137.6	136.1	134.3	133.0	131.3	130.0	129.5
256QAM 0.81 dual	134.0	132.5	130.7	129.5	127.7	126.5	126.0

Table 65 4.9 GHz IP mode: system threshold per channel bandwidth and output power (P) (dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-93.6	-92.1	-90.3	-89.1	-87.3	-86.1	-85.6	28
QPSK 0.63 single	-90.1	-88.6	-86.8	-85.6	-83.8	-82.6	-82.1	27
QPSK 0.87 single	-86.1	-84.6	-82.8	-81.6	-79.8	-78.6	-78.0	26
16QAM 0.63 single	-84.2	-82.7	-80.9	-79.6	-77.9	-76.6	-76.1	25
16QAM 0.63 dual	-81.1	-79.6	-77.9	-76.6	-74.9	-73.6	-73.1	25
16QAM 0.87 single	-79.5	-78.0	-76.2	-74.9	-73.2	-71.9	-71.4	24
16QAM 0.87 dual	-76.4	-74.9	-73.1	-71.9	-70.1	-68.9	-68.4	24
64QAM 0.75 single	-76.5	-75.0	-73.2	-72.0	-70.2	-69.0	-68.5	23
64QAM 0.75 dual	-73.4	-71.9	-70.1	-68.9	-67.1	-65.9	-65.4	23
64QAM 0.92 single	-72.7	-71.2	-69.5	-68.2	-66.4	-65.2	-64.7	23
64 QAM 0.92 dual	-69.5	-68.0	-66.2	-64.9	-63.2	-61.9	-61.4	23
256QAM 0.81 single	-69.5	-68.0	-66.2	-64.9	-63.2	-61.9	-61.4	23
256QAM 0.81 dual	-65.9	-64.4	-62.6	-61.4	-59.6	-58.4	-57.9	23

Table 66 4.9 GHz IP mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	167.0	165.5	163.7	162.5	160.7	159.5	159.0
QPSK 0.63 single	162.5	161.0	159.2	158.0	156.2	155.0	154.5
QPSK 0.87 single	157.5	156.0	154.2	153.0	151.2	150.0	149.4
16QAM 0.63 single	154.6	153.1	151.3	150.0	148.3	147.0	146.5
16QAM 0.63 dual	150.1	148.5	146.8	145.5	143.8	142.5	142.0
16QAM 0.87 single	148.9	147.4	145.6	144.3	142.6	141.3	140.8
16QAM 0.87 dual	145.8	144.3	142.5	141.3	139.5	138.3	137.8
64QAM 0.75 single	144.9	143.4	141.6	140.4	138.6	137.4	136.9
64QAM 0.75 dual	141.8	140.3	138.5	137.3	135.5	134.3	133.8
64QAM 0.92 single	141.1	139.6	137.9	136.6	134.8	133.6	133.1
64 QAM 0.92 dual	137.9	136.4	134.6	133.3	131.6	130.3	129.8
256QAM 0.81 single	137.9	136.4	134.6	133.3	131.6	130.3	129.8
256QAM 0.81 dual	134.3	132.8	131.0	129.8	128.0	126.8	126.3

Table 67 4.9 GHz TDM mode:system threshold per channel bandwidth and output power (P) (dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-93.6	-92.1	-90.3	-89.1	-87.3	-86.1	-85.6	26
QPSK 0.63 single	-87.1	-85.6	-83.8	-82.6	-80.8	-79.6	-79.1	25
QPSK 0.87 single	-83.1	-81.5	-79.8	-78.5	-76.8	-75.5	-75.0	24
16QAM 0.63 single	-81.1	-79.6	-77.8	-76.6	-74.8	-73.6	-73.1	23
16QAM 0.63 dual	-78.1	-76.6	-74.8	-73.5	-71.8	-70.5	-70.0	23
16QAM 0.87 single	-76.3	-74.8	-73.0	-71.8	-70.0	-68.8	-68.3	23
16QAM 0.87 dual	-73.2	-71.7	-69.9	-68.7	-66.9	-65.7	-65.1	23
64QAM 0.75 single	-73.2	-71.7	-69.9	-68.7	-66.9	-65.7	-65.2	23
64QAM 0.75 dual	-70.0	-68.5	-66.7	-65.4	-63.7	-62.4	-61.9	23
64QAM 0.92 single	-70.9	-69.4	-67.6	-66.4	-64.6	-63.4	-62.9	23
64 QAM 0.92 dual	-67.5	-66.0	-64.2	-63.0	-61.2	-60.0	-59.5	23
256QAM 0.81 single	-69.5	-68.0	-66.2	-64.9	-63.2	-61.9	-61.4	23
256QAM 0.81 dual	-65.9	-64.4	-62.6	-61.4	-59.6	-58.4	-57.9	23

Table 68 4.9 GHz TDM mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	165.0	163.5	161.7	160.5	158.7	157.5	157.0
QPSK 0.63 single	157.5	156.0	154.2	153.0	151.2	150.0	149.5
QPSK 0.87 single	152.5	150.9	149.2	147.9	146.2	144.9	144.4
16QAM 0.63 single	149.5	148.0	146.2	145.0	143.2	142.0	141.5
16QAM 0.63 dual	145.0	143.5	141.7	140.5	138.7	137.4	136.9
16QAM 0.87 single	144.7	143.2	141.4	140.2	138.4	137.2	136.7
16QAM 0.87 dual	141.6	140.1	138.3	137.1	135.3	134.1	133.5
64QAM 0.75 single	141.6	140.1	138.3	137.1	135.3	134.1	133.6
64QAM 0.75 dual	138.4	136.9	135.1	133.8	132.1	130.8	130.3
64QAM 0.92 single	139.3	137.8	136.0	134.8	133.0	131.8	131.3
64 QAM 0.92 dual	135.9	134.4	132.6	131.4	129.6	128.4	127.9
256QAM 0.81 single	137.9	136.4	134.6	133.3	131.6	130.3	129.8
256QAM 0.81 dual	134.3	132.8	131.0	129.8	128.0	126.8	126.3

Table 69 5.1/5.2 GHz IP mode: system threshold per channel bandwidth and o/p power (P) (dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-93.6	-92.1	-90.3	-89.1	-87.3	-86.1	-85.6	28
QPSK 0.63 single	-90.1	-88.6	-86.8	-85.6	-83.8	-82.6	-82.1	27
QPSK 0.87 single	-86.1	-84.6	-82.8	-81.6	-79.8	-78.6	-78.0	26
16QAM 0.63 single	-84.2	-82.7	-80.9	-79.7	-77.9	-76.6	-76.1	25
16QAM 0.63 dual	-81.1	-79.6	-77.9	-76.6	-74.9	-73.6	-73.1	25
16QAM 0.87 single	-79.5	-78.0	-76.2	-75.0	-73.2	-72.0	-71.4	24
16QAM 0.87 dual	-76.4	-74.9	-73.2	-71.9	-70.1	-68.9	-68.4	24
64QAM 0.75 single	-76.6	-75.0	-73.3	-72.0	-70.3	-69.0	-68.5	23
64QAM 0.75 dual	-73.5	-71.9	-70.2	-68.9	-67.2	-65.9	-65.4	23
64QAM 0.92 single	-72.8	-71.3	-69.5	-68.3	-66.5	-65.3	-64.8	23
64 QAM 0.92 dual	-69.6	-68.1	-66.3	-65.1	-63.3	-62.1	-61.5	23
256QAM 0.81 single	-69.6	-68.1	-66.4	-65.1	-63.3	-62.1	-61.6	23
256QAM 0.81 dual	-66.2	-64.7	-62.9	-61.6	-59.9	-58.6	-58.1	23

Table 70 5.1/5.2 GHz IP mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	168.2	166.7	164.9	163.7	161.9	160.7	160.2
QPSK 0.63 single	163.7	162.2	160.4	159.2	157.4	156.2	155.7
QPSK 0.87 single	158.7	157.2	155.4	154.2	152.4	151.2	150.6
16QAM 0.63 single	155.8	154.3	152.5	151.3	149.5	148.2	147.7
16QAM 0.63 dual	151.3	149.7	148.0	146.7	145.0	143.7	143.2
16QAM 0.87 single	150.1	148.6	146.8	145.6	143.8	142.6	142.0
16QAM 0.87 dual	147.0	145.5	143.8	142.5	140.7	139.5	139.0
64QAM 0.75 single	146.2	144.6	142.9	141.6	139.9	138.6	138.1
64QAM 0.75 dual	143.1	141.5	139.8	138.5	136.8	135.5	135.0
64QAM 0.92 single	142.4	140.9	139.1	137.9	136.1	134.9	134.4
64 QAM 0.92 dual	139.2	137.7	135.9	134.7	132.9	131.7	131.1
256QAM 0.81 single	139.2	137.7	136.0	134.7	132.9	131.7	131.2
256QAM 0.81 dual	135.8	134.3	132.5	131.2	129.5	128.2	127.7

Table 71 5.1/5.2 GHz TDM mode: system threshold per channel bandwidth and o/p pwr (P) (dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-93.6	-92.1	-90.3	-89.1	-87.3	-86.1	-85.6	26
QPSK 0.63 single	-87.1	-85.6	-83.8	-82.6	-80.8	-79.6	-79.1	25
QPSK 0.87 single	-83.1	-81.6	-79.8	-78.5	-76.8	-75.5	-75.0	24
16QAM 0.63 single	-81.1	-79.6	-77.9	-76.6	-74.8	-73.6	-73.1	23
16QAM 0.63 dual	-78.1	-76.6	-74.8	-73.6	-71.8	-70.6	-70.0	23
16QAM 0.87 single	-76.3	-74.8	-73.1	-71.8	-70.1	-68.8	-68.3	23
16QAM 0.87 dual	-73.2	-71.7	-70.0	-68.7	-67.0	-65.7	-65.2	23
64QAM 0.75 single	-73.3	-71.8	-70.0	-68.7	-67.0	-65.7	-65.2	23
64QAM 0.75 dual	-70.1	-68.6	-66.8	-65.5	-63.8	-62.5	-62.0	23
64QAM 0.92 single	-71.0	-69.5	-67.8	-66.5	-64.7	-63.5	-63.0	23
64 QAM 0.92 dual	-67.7	-66.2	-64.4	-63.2	-61.4	-60.2	-59.6	23
256QAM 0.81 single	-69.6	-68.1	-66.4	-65.1	-63.3	-62.1	-61.6	23
256QAM 0.81 dual	-66.2	-64.7	-62.9	-61.6	-59.9	-58.6	-58.1	23

Table 72 5.1/5.2 GHz TDM mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	166.2	164.7	162.9	161.7	159.9	158.7	158.2
QPSK 0.63 single	158.7	157.2	155.4	154.2	152.4	151.2	150.7
QPSK 0.87 single	153.7	152.2	150.4	149.1	147.4	146.1	145.6
16QAM 0.63 single	150.7	149.2	147.5	146.2	144.4	143.2	142.7
16QAM 0.63 dual	146.2	144.7	142.9	141.7	139.9	138.7	138.2
16QAM 0.87 single	145.9	144.4	142.7	141.4	139.7	138.4	137.9
16QAM 0.87 dual	142.8	141.3	139.6	138.3	136.6	135.3	134.8
64QAM 0.75 single	142.9	141.4	139.6	138.3	136.6	135.3	134.8
64QAM 0.75 dual	139.7	138.2	136.4	135.1	133.4	132.1	131.6
64QAM 0.92 single	140.6	139.1	137.4	136.1	134.3	133.1	132.6
64 QAM 0.92 dual	137.3	135.8	134.0	132.8	131.0	129.8	129.2
256QAM 0.81 single	139.2	137.7	136.0	134.7	132.9	131.7	131.2
256QAM 0.81 dual	135.8	134.3	132.5	131.2	129.5	128.2	127.7

Table 73 5.4 GHz IP mode: system threshold per channel bandwidth and output power (P) (dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-93.6	-91.6	-89.8	-88.6	-86.8	-85.6	-85.1	28
QPSK 0.63 single	-90.1	-88.1	-86.3	-85.1	-83.3	-82.1	-81.6	27
QPSK 0.87 single	-86.1	-84.1	-82.3	-81.1	-79.3	-78.1	-77.5	26
16QAM 0.63 single	-84.2	-82.2	-80.4	-79.2	-77.4	-76.1	-75.6	25
16QAM 0.63 dual	-81.1	-79.1	-77.4	-76.1	-74.4	-73.1	-72.6	25
16QAM 0.87 single	-79.5	-77.5	-75.7	-74.5	-72.7	-71.5	-70.9	24
16QAM 0.87 dual	-76.4	-74.4	-72.7	-71.4	-69.6	-68.4	-67.9	24
64QAM 0.75 single	-76.6	-74.5	-72.8	-71.5	-69.8	-68.5	-68.0	23
64QAM 0.75 dual	-73.5	-71.4	-69.7	-68.4	-66.7	-65.4	-64.9	23
64QAM 0.92 single	-72.8	-70.8	-69.0	-67.8	-66.0	-64.8	-64.3	23
64 QAM 0.92 dual	-69.6	-67.6	-65.8	-64.6	-62.8	-61.6	-61.0	23
256QAM 0.81 single	-69.6	-67.6	-65.9	-64.6	-62.8	-61.6	-61.1	23
256QAM 0.81 dual	-66.2	-64.2	-62.4	-61.1	-59.4	-58.1	-57.6	23

Table 74 5.4 GHz IP mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	169.0	167.0	165.2	164.0	162.2	161.0	160.5
QPSK 0.63 single	164.5	162.5	160.7	159.5	157.7	156.5	156.0
QPSK 0.87 single	159.5	157.5	155.7	154.5	152.7	151.5	150.9
16QAM 0.63 single	156.6	154.6	152.8	151.6	149.8	148.5	148.0
16QAM 0.63 dual	152.1	150.0	148.3	147.0	145.3	144.0	143.5
16QAM 0.87 single	150.9	148.9	147.1	145.9	144.1	142.9	142.3
16QAM 0.87 dual	147.8	145.8	144.1	142.8	141.0	139.8	139.3
64QAM 0.75 single	147.0	144.9	143.2	141.9	140.2	138.9	138.4
64QAM 0.75 dual	143.9	141.8	140.1	138.8	137.1	135.8	135.3
64QAM 0.92 single	143.2	141.2	139.4	138.2	136.4	135.2	134.7
64 QAM 0.92 dual	140.0	138.0	136.2	135.0	133.2	132.0	131.4
256QAM 0.81 single	140.0	138.0	136.3	135.0	133.2	132.0	131.5
256QAM 0.81 dual	136.6	134.6	132.8	131.5	129.8	128.5	128.0

Table 75 5.4 GHz TDM mode: system threshold per channel bandwidth and output power (P)(dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-93.6	-91.6	-89.8	-88.6	-86.8	-85.6	-85.1	26
QPSK 0.63 single	-87.1	-85.1	-83.3	-82.1	-80.3	-79.1	-78.6	25
QPSK 0.87 single	-83.1	-81.1	-79.3	-78.0	-76.3	-75.0	-74.5	24
16QAM 0.63 single	-81.1	-79.1	-77.4	-76.1	-74.3	-73.1	-72.6	23
16QAM 0.63 dual	-78.1	-76.1	-74.3	-73.1	-71.3	-70.1	-69.5	23
16QAM 0.87 single	-76.3	-74.3	-72.6	-71.3	-69.6	-68.3	-67.8	23
16QAM 0.87 dual	-73.2	-71.2	-69.5	-68.2	-66.5	-65.2	-64.7	23
64QAM 0.75 single	-73.3	-71.3	-69.5	-68.2	-66.5	-65.2	-64.7	23
64QAM 0.75 dual	-70.1	-68.1	-66.3	-65.0	-63.3	-62.0	-61.5	23
64QAM 0.92 single	-71.0	-69.0	-67.3	-66.0	-64.2	-63.0	-62.5	23
64 QAM 0.92 dual	-67.7	-65.7	-63.9	-62.7	-60.9	-59.7	-59.1	23
256QAM 0.81 single	-69.6	-67.6	-65.9	-64.6	-62.8	-61.6	-61.1	23
256QAM 0.81 dual	-66.2	-64.2	-62.4	-61.1	-59.4	-58.1	-57.6	23

Table 76 5.4 GHz TDM mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	167.0	165.0	163.2	162.0	160.2	159.0	158.5
QPSK 0.63 single	159.5	157.5	155.7	154.5	152.7	151.5	151.0
QPSK 0.87 single	154.5	152.5	150.7	149.4	147.7	146.4	145.9
16QAM 0.63 single	151.5	149.5	147.8	146.5	144.7	143.5	143.0
16QAM 0.63 dual	147.0	145.0	143.2	142.0	140.2	139.0	138.5
16QAM 0.87 single	146.7	144.7	143.0	141.7	140.0	138.7	138.2
16QAM 0.87 dual	143.6	141.6	139.9	138.6	136.9	135.6	135.1
64QAM 0.75 single	143.7	141.7	139.9	138.6	136.9	135.6	135.1
64QAM 0.75 dual	140.5	138.5	136.7	135.4	133.7	132.4	131.9
64QAM 0.92 single	141.4	139.4	137.7	136.4	134.6	133.4	132.9
64 QAM 0.92 dual	138.1	136.1	134.3	133.1	131.3	130.1	129.5
256QAM 0.81 single	140.0	138.0	136.3	135.0	133.2	132.0	131.5
256QAM 0.81 dual	136.6	134.6	132.8	131.5	129.8	128.5	128.0

Table 77 5.8 GHz IP mode: system threshold per channel bandwidth and output power (P) (dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-93.1	-91.1	-89.3	-88.1	-86.3	-85.1	-84.6	28
QPSK 0.63 single	-89.6	-87.6	-85.8	-84.6	-82.8	-81.6	-81.1	27
QPSK 0.87 single	-85.6	-83.6	-81.8	-80.6	-78.8	-77.6	-77.0	26
16QAM 0.63 single	-83.7	-81.7	-79.9	-78.6	-76.9	-75.6	-75.1	25
16QAM 0.63 dual	-80.6	-78.6	-76.9	-75.6	-73.9	-72.6	-72.1	25
16QAM 0.87 single	-78.9	-76.9	-75.2	-73.9	-72.2	-70.9	-70.4	24
16QAM 0.87 dual	-75.9	-73.9	-72.1	-70.9	-69.1	-67.8	-67.3	24
64QAM 0.75 single	-76.0	-74.0	-72.2	-71.0	-69.2	-67.9	-67.4	23
64QAM 0.75 dual	-72.9	-70.8	-69.1	-67.8	-66.1	-64.8	-64.3	23
64QAM 0.92 single	-72.1	-70.1	-68.4	-67.1	-65.4	-64.1	-63.6	23
64 QAM 0.92 dual	-68.8	-66.8	-65.1	-63.8	-62.1	-60.8	-60.3	23
256QAM 0.81 single	-68.8	-66.8	-65.0	-63.7	-62.0	-60.7	-60.2	23
256QAM 0.81 dual	-65.1	-63.1	-61.3	-60.1	-58.3	-57.1	-56.6	23

Table 78 5.8 GHz IP mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	168.7	166.7	164.9	163.7	161.9	160.7	160.2
QPSK 0.63 single	164.2	162.2	160.4	159.2	157.4	156.2	155.7
QPSK 0.87 single	159.2	157.2	155.4	154.2	152.4	151.2	150.6
16QAM 0.63 single	156.3	154.3	152.5	151.2	149.5	148.2	147.7
16QAM 0.63 dual	151.7	149.7	148.0	146.7	145.0	143.7	143.2
16QAM 0.87 single	150.5	148.5	146.8	145.5	143.8	142.5	142.0
16QAM 0.87 dual	147.5	145.5	143.7	142.5	140.7	139.4	138.9
64QAM 0.75 single	146.6	144.6	142.8	141.6	139.8	138.5	138.0
64QAM 0.75 dual	143.5	141.4	139.7	138.4	136.7	135.4	134.9
64QAM 0.92 single	142.7	140.7	139.0	137.7	136.0	134.7	134.2
64 QAM 0.92 dual	139.4	137.4	135.7	134.4	132.7	131.4	130.9
256QAM 0.81 single	139.4	137.4	135.6	134.3	132.6	131.3	130.8
256QAM 0.81 dual	135.7	133.7	131.9	130.7	128.9	127.7	127.2

Table 79 5.8 GHz TDM mode: system threshold per channel bandwidth and output power (P)(dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-93.1	-91.1	-89.3	-88.1	-86.3	-85.1	-84.6	26
QPSK 0.63 single	-86.6	-84.6	-82.8	-81.6	-79.8	-78.6	-78.0	25
QPSK 0.87 single	-82.5	-80.5	-78.8	-77.5	-75.8	-74.5	-74.0	24
16QAM 0.63 single	-80.6	-78.6	-76.8	-75.6	-73.8	-72.6	-72.1	23
16QAM 0.63 dual	-77.6	-75.5	-73.8	-72.5	-70.8	-69.5	-69.0	23
16QAM 0.87 single	-75.8	-73.8	-72.0	-70.7	-69.0	-67.7	-67.2	23
16QAM 0.87 dual	-72.6	-70.6	-68.9	-67.6	-65.9	-64.6	-64.1	23
64QAM 0.75 single	-72.6	-70.6	-68.8	-67.6	-65.8	-64.6	-64.1	23
64QAM 0.75 dual	-69.3	-67.3	-65.6	-64.3	-62.6	-61.3	-60.8	23
64QAM 0.92 single	-70.3	-68.3	-66.5	-65.2	-63.5	-62.2	-61.7	23
64 QAM 0.92 dual	-66.8	-64.8	-63.0	-61.8	-60.0	-58.8	-58.3	23
256QAM 0.81 single	-68.8	-66.8	-65.0	-63.7	-62.0	-60.7	-60.2	23
256QAM 0.81 dual	-65.1	-63.1	-61.3	-60.1	-58.3	-57.1	-56.6	23

Table 80 5.8 GHz TDM mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	166.7	164.7	162.9	161.7	159.9	158.7	158.2
QPSK 0.63 single	159.2	157.2	155.4	154.2	152.4	151.2	150.6
QPSK 0.87 single	154.1	152.1	150.4	149.1	147.4	146.1	145.6
16QAM 0.63 single	151.2	149.2	147.4	146.2	144.4	143.2	142.7
16QAM 0.63 dual	146.7	144.7	142.9	141.6	139.9	138.6	138.1
16QAM 0.87 single	146.4	144.4	142.6	141.3	139.6	138.3	137.8
16QAM 0.87 dual	143.2	141.2	139.5	138.2	136.5	135.2	134.7
64QAM 0.75 single	143.2	141.2	139.4	138.2	136.4	135.2	134.7
64QAM 0.75 dual	139.9	137.9	136.2	134.9	133.2	131.9	131.4
64QAM 0.92 single	140.9	138.9	137.1	135.8	134.1	132.8	132.3
64 QAM 0.92 dual	137.4	135.4	133.6	132.4	130.6	129.4	128.9
256QAM 0.81 single	139.4	137.4	135.6	134.3	132.6	131.3	130.8
256QAM 0.81 dual	135.7	133.7	131.9	130.7	128.9	127.7	127.2

Connectorized ODUs

Table 81 4.7 GHz IP mode: system threshold per channel bandwidth and output power (P) (dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-95.0	-93.5	-91.7	-90.5	-88.7	-87.5	-87.0	29
QPSK 0.63 single	-91.5	-90.0	-88.2	-87.0	-85.2	-84.0	-83.5	28
QPSK 0.87 single	-87.5	-86.0	-84.2	-83.0	-81.2	-80.0	-79.4	27
16QAM 0.63 single	-85.6	-84.1	-82.3	-81.0	-79.3	-78.0	-77.5	26
16QAM 0.63 dual	-81.1	-79.5	-77.8	-76.5	-74.8	-73.5	-73.0	26
16QAM 0.87 single	-80.9	-79.4	-77.6	-76.3	-74.6	-73.3	-72.8	25
16QAM 0.87 dual	-77.8	-76.3	-74.5	-73.3	-71.5	-70.3	-69.8	25
64QAM 0.75 single	-77.9	-76.4	-74.6	-73.4	-71.6	-70.4	-69.9	24
64QAM 0.75 dual	-74.8	-73.3	-71.5	-70.3	-68.5	-67.3	-66.8	24
64QAM 0.92 single	-74.1	-72.6	-70.9	-69.6	-67.8	-66.6	-66.1	24
64 QAM 0.92 dual	-70.9	-69.4	-67.6	-66.3	-64.6	-63.3	-62.8	24
256QAM 0.81 single	-70.9	-69.4	-67.6	-66.3	-64.6	-63.3	-62.8	24
256QAM 0.81 dual	-67.3	-65.8	-64.0	-62.8	-61.0	-59.8	-59.3	24

Table 82 4.7 GHz IP mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	169.2	167.7	165.9	164.7	162.9	161.7	161.2
QPSK 0.63 single	164.7	163.2	161.4	160.2	158.4	157.2	156.7
QPSK 0.87 single	159.7	158.2	156.4	155.2	153.4	152.2	151.6
16QAM 0.63 single	156.8	155.3	153.5	152.2	150.5	149.2	148.7
16QAM 0.63 dual	152.3	150.7	149.0	147.7	146.0	144.7	144.2
16QAM 0.87 single	151.1	149.6	147.8	146.5	144.8	143.5	143.0
16QAM 0.87 dual	148.0	146.5	144.7	143.5	141.7	140.5	140.0
64QAM 0.75 single	147.1	145.6	143.8	142.6	140.8	139.6	139.1
64QAM 0.75 dual	144.0	142.5	140.7	139.5	137.7	136.5	136.0
64QAM 0.92 single	143.3	141.8	140.1	138.8	137.0	135.8	135.3
64 QAM 0.92 dual	140.1	138.6	136.8	135.5	133.8	132.5	132.0
256QAM 0.81 single	140.1	138.6	136.8	135.5	133.8	132.5	132.0
256QAM 0.81 dual	136.5	135.0	133.2	132.0	130.2	129.0	128.5

Table 83 4.7 GHz TDM mode:system threshold per channel bandwidth and output power (P) (dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-95.0	-93.5	-91.7	-90.5	-88.7	-87.5	-87.0	27
QPSK 0.63 single	-88.5	-87.0	-85.2	-84.0	-82.2	-81.0	-80.5	26
QPSK 0.87 single	-84.5	-82.9	-81.2	-79.9	-78.2	-76.9	-76.4	25
16QAM 0.63 single	-82.5	-81.0	-79.2	-78.0	-76.2	-75.0	-74.5	24
16QAM 0.63 dual	-78.0	-76.5	-74.7	-73.5	-71.7	-70.4	-69.9	24
16QAM 0.87 single	-77.7	-76.2	-74.4	-73.2	-71.4	-70.2	-69.7	24
16QAM 0.87 dual	-74.6	-73.1	-71.3	-70.1	-68.3	-67.1	-66.5	24
64QAM 0.75 single	-74.6	-73.1	-71.3	-70.1	-68.3	-67.1	-66.6	24
64QAM 0.75 dual	-71.4	-69.9	-68.1	-66.8	-65.1	-63.8	-63.3	24
64QAM 0.92 single	-72.3	-70.8	-69.0	-67.8	-66.0	-64.8	-64.3	24
64 QAM 0.92 dual	-68.9	-67.4	-65.6	-64.4	-62.6	-61.4	-60.9	24
256QAM 0.81 single	-70.9	-69.4	-67.6	-66.3	-64.6	-63.3	-62.8	24
256QAM 0.81 dual	-67.3	-65.8	-64.0	-62.8	-61.0	-59.8	-59.3	24

Table 84 4.7 GHz TDM mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	167.2	165.7	163.9	162.7	160.9	159.7	159.2
QPSK 0.63 single	159.7	158.2	156.4	155.2	153.4	152.2	151.7
QPSK 0.87 single	154.7	153.1	151.4	150.1	148.4	147.1	146.6
16QAM 0.63 single	151.7	150.2	148.4	147.2	145.4	144.2	143.7
16QAM 0.63 dual	147.2	145.7	143.9	142.7	140.9	139.6	139.1
16QAM 0.87 single	146.9	145.4	143.6	142.4	140.6	139.4	138.9
16QAM 0.87 dual	143.8	142.3	140.5	139.3	137.5	136.3	135.7
64QAM 0.75 single	143.8	142.3	140.5	139.3	137.5	136.3	135.8
64QAM 0.75 dual	140.6	139.1	137.3	136.0	134.3	133.0	132.5
64QAM 0.92 single	141.5	140.0	138.2	137.0	135.2	134.0	133.5
64 QAM 0.92 dual	138.1	136.6	134.8	133.6	131.8	130.6	130.1
256QAM 0.81 single	140.1	138.6	136.8	135.5	133.8	132.5	132.0
256QAM 0.81 dual	136.5	135.0	133.2	132.0	130.2	129.0	128.5

Table 85 4.9 GHz IP mode: system threshold per channel bandwidth and output power (P) (dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-95.1	-93.6	-91.8	-90.6	-88.8	-87.6	-87.1	29
QPSK 0.63 single	-91.6	-90.1	-88.3	-87.1	-85.3	-84.1	-83.6	28
QPSK 0.87 single	-87.6	-86.1	-84.3	-83.1	-81.3	-80.1	-79.5	27
16QAM 0.63 single	-85.7	-84.2	-82.4	-81.1	-79.4	-78.1	-77.6	26
16QAM 0.63 dual	-81.2	-79.6	-77.9	-76.6	-74.9	-73.6	-73.1	26
16QAM 0.87 single	-81.0	-79.5	-77.7	-76.4	-74.7	-73.4	-72.9	25
16QAM 0.87 dual	-77.9	-76.4	-74.6	-73.4	-71.6	-70.4	-69.9	25
64QAM 0.75 single	-78.0	-76.5	-74.7	-73.5	-71.7	-70.5	-70.0	24
64QAM 0.75 dual	-74.9	-73.4	-71.6	-70.4	-68.6	-67.4	-66.9	24
64QAM 0.92 single	-74.2	-72.7	-71.0	-69.7	-67.9	-66.7	-66.2	24
64 QAM 0.92 dual	-71.0	-69.5	-67.7	-66.4	-64.7	-63.4	-62.9	24
256QAM 0.81 single	-71.0	-69.5	-67.7	-66.4	-64.7	-63.4	-62.9	24
256QAM 0.81 dual	-67.4	-65.9	-64.1	-62.9	-61.1	-59.9	-59.4	24

Table 86 4.9 GHz IP mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	169.5	168.0	166.2	165.0	163.2	162.0	161.5
QPSK 0.63 single	165.0	163.5	161.7	160.5	158.7	157.5	157.0
QPSK 0.87 single	160.0	158.5	156.7	155.5	153.7	152.5	151.9
16QAM 0.63 single	157.1	155.6	153.8	152.5	150.8	149.5	149.0
16QAM 0.63 dual	152.6	151.0	149.3	148.0	146.3	145.0	144.5
16QAM 0.87 single	151.4	149.9	148.1	146.8	145.1	143.8	143.3
16QAM 0.87 dual	148.3	146.8	145.0	143.8	142.0	140.8	140.3
64QAM 0.75 single	147.4	145.9	144.1	142.9	141.1	139.9	139.4
64QAM 0.75 dual	144.3	142.8	141.0	139.8	138.0	136.8	136.3
64QAM 0.92 single	143.6	142.1	140.4	139.1	137.3	136.1	135.6
64 QAM 0.92 dual	140.4	138.9	137.1	135.8	134.1	132.8	132.3
256QAM 0.81 single	140.4	138.9	137.1	135.8	134.1	132.8	132.3
256QAM 0.81 dual	136.8	135.3	133.5	132.3	130.5	129.3	128.8

Table 87 4.9 GHz TDM mode:system threshold per channel bandwidth and output power (P) (dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-95.1	-93.6	-91.8	-90.6	-88.8	-87.6	-87.1	27
QPSK 0.63 single	-88.6	-87.1	-85.3	-84.1	-82.3	-81.1	-80.6	26
QPSK 0.87 single	-84.6	-83.0	-81.3	-80.0	-78.3	-77.0	-76.5	25
16QAM 0.63 single	-82.6	-81.1	-79.3	-78.1	-76.3	-75.1	-74.6	24
16QAM 0.63 dual	-78.1	-76.6	-74.8	-73.6	-71.8	-70.5	-70.0	24
16QAM 0.87 single	-77.8	-76.3	-74.5	-73.3	-71.5	-70.3	-69.8	24
16QAM 0.87 dual	-74.7	-73.2	-71.4	-70.2	-68.4	-67.2	-66.6	24
64QAM 0.75 single	-74.7	-73.2	-71.4	-70.2	-68.4	-67.2	-66.7	24
64QAM 0.75 dual	-71.5	-70.0	-68.2	-66.9	-65.2	-63.9	-63.4	24
64QAM 0.92 single	-72.4	-70.9	-69.1	-67.9	-66.1	-64.9	-64.4	24
64 QAM 0.92 dual	-69.0	-67.5	-65.7	-64.5	-62.7	-61.5	-61.0	24
256QAM 0.81 single	-71.0	-69.5	-67.7	-66.4	-64.7	-63.4	-62.9	24
256QAM 0.81 dual	-67.4	-65.9	-64.1	-62.9	-61.1	-59.9	-59.4	24

Table 88 4.9 GHz TDM mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	167.5	166.0	164.2	163.0	161.2	160.0	159.5
QPSK 0.63 single	160.0	158.5	156.7	155.5	153.7	152.5	152.0
QPSK 0.87 single	155.0	153.4	151.7	150.4	148.7	147.4	146.9
16QAM 0.63 single	152.0	150.5	148.7	147.5	145.7	144.5	144.0
16QAM 0.63 dual	147.5	146.0	144.2	143.0	141.2	139.9	139.4
16QAM 0.87 single	147.2	145.7	143.9	142.7	140.9	139.7	139.2
16QAM 0.87 dual	144.1	142.6	140.8	139.6	137.8	136.6	136.0
64QAM 0.75 single	144.1	142.6	140.8	139.6	137.8	136.6	136.1
64QAM 0.75 dual	140.9	139.4	137.6	136.3	134.6	133.3	132.8
64QAM 0.92 single	141.8	140.3	138.5	137.3	135.5	134.3	133.8
64 QAM 0.92 dual	138.4	136.9	135.1	133.9	132.1	130.9	130.4
256QAM 0.81 single	140.4	138.9	137.1	135.8	134.1	132.8	132.3
256QAM 0.81 dual	136.8	135.3	133.5	132.3	130.5	129.3	128.8

Table 89 5.1/5.2 GHz IP mode: system threshold per channel bandwidth and o/p power (P) (dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-95.1	-93.6	-91.8	-90.6	-88.8	-87.6	-87.1	29
QPSK 0.63 single	-91.6	-90.1	-88.3	-87.1	-85.3	-84.1	-83.6	28
QPSK 0.87 single	-87.6	-86.1	-84.3	-83.1	-81.3	-80.1	-79.5	27
16QAM 0.63 single	-85.7	-84.2	-82.4	-81.2	-79.4	-78.1	-77.6	26
16QAM 0.63 dual	-81.2	-79.6	-77.9	-76.6	-74.9	-73.6	-73.1	26
16QAM 0.87 single	-81.0	-79.5	-77.7	-76.5	-74.7	-73.5	-72.9	25
16QAM 0.87 dual	-77.9	-76.4	-74.7	-73.4	-71.6	-70.4	-69.9	25
64QAM 0.75 single	-78.1	-76.5	-74.8	-73.5	-71.8	-70.5	-70.0	24
64QAM 0.75 dual	-75.0	-73.4	-71.7	-70.4	-68.7	-67.4	-66.9	24
64QAM 0.92 single	-74.3	-72.8	-71.0	-69.8	-68.0	-66.8	-66.3	24
64 QAM 0.92 dual	-71.1	-69.6	-67.8	-66.6	-64.8	-63.6	-63.0	24
256QAM 0.81 single	-71.1	-69.6	-67.9	-66.6	-64.8	-63.6	-63.1	24
256QAM 0.81 dual	-67.7	-66.2	-64.4	-63.1	-61.4	-60.1	-59.6	24

Table 90 5.1/5.2 GHz IP mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	170.7	169.2	167.4	166.2	164.4	163.2	162.7
QPSK 0.63 single	166.2	164.7	162.9	161.7	159.9	158.7	158.2
QPSK 0.87 single	161.2	159.7	157.9	156.7	154.9	153.7	153.1
16QAM 0.63 single	158.3	156.8	155.0	153.8	152.0	150.7	150.2
16QAM 0.63 dual	153.8	152.2	150.5	149.2	147.5	146.2	145.7
16QAM 0.87 single	152.6	151.1	149.3	148.1	146.3	145.1	144.5
16QAM 0.87 dual	149.5	148.0	146.3	145.0	143.2	142.0	141.5
64QAM 0.75 single	148.7	147.1	145.4	144.1	142.4	141.1	140.6
64QAM 0.75 dual	145.6	144.0	142.3	141.0	139.3	138.0	137.5
64QAM 0.92 single	144.9	143.4	141.6	140.4	138.6	137.4	136.9
64 QAM 0.92 dual	141.7	140.2	138.4	137.2	135.4	134.2	133.6
256QAM 0.81 single	141.7	140.2	138.5	137.2	135.4	134.2	133.7
256QAM 0.81 dual	138.3	136.8	135.0	133.7	132.0	130.7	130.2

Table 91 5.1/5.2 GHz TDM mode: system threshold per channel bandwidth and o/p pwr (P) (dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-95.1	-93.6	-91.8	-90.6	-88.8	-87.6	-87.1	27
QPSK 0.63 single	-88.6	-87.1	-85.3	-84.1	-82.3	-81.1	-80.6	26
QPSK 0.87 single	-84.6	-83.1	-81.3	-80.0	-78.3	-77.0	-76.5	25
16QAM 0.63 single	-82.6	-81.1	-79.4	-78.1	-76.3	-75.1	-74.6	24
16QAM 0.63 dual	-78.1	-76.6	-74.8	-73.6	-71.8	-70.6	-70.1	24
16QAM 0.87 single	-77.8	-76.3	-74.6	-73.3	-71.6	-70.3	-69.8	24
16QAM 0.87 dual	-74.7	-73.2	-71.5	-70.2	-68.5	-67.2	-66.7	24
64QAM 0.75 single	-74.8	-73.3	-71.5	-70.2	-68.5	-67.2	-66.7	24
64QAM 0.75 dual	-71.6	-70.1	-68.3	-67.0	-65.3	-64.0	-63.5	24
64QAM 0.92 single	-72.5	-71.0	-69.3	-68.0	-66.2	-65.0	-64.5	24
64 QAM 0.92 dual	-69.2	-67.7	-65.9	-64.7	-62.9	-61.7	-61.1	24
256QAM 0.81 single	-71.1	-69.6	-67.9	-66.6	-64.8	-63.6	-63.1	24
256QAM 0.81 dual	-67.7	-66.2	-64.4	-63.1	-61.4	-60.1	-59.6	24

Table 92 5.1/5.2 GHz TDM mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	168.7	167.2	165.4	164.2	162.4	161.2	160.7
QPSK 0.63 single	161.2	159.7	157.9	156.7	154.9	153.7	153.2
QPSK 0.87 single	156.2	154.7	152.9	151.6	149.9	148.6	148.1
16QAM 0.63 single	153.2	151.7	150.0	148.7	146.9	145.7	145.2
16QAM 0.63 dual	148.7	147.2	145.4	144.2	142.4	141.2	140.7
16QAM 0.87 single	148.4	146.9	145.2	143.9	142.2	140.9	140.4
16QAM 0.87 dual	145.3	143.8	142.1	140.8	139.1	137.8	137.3
64QAM 0.75 single	145.4	143.9	142.1	140.8	139.1	137.8	137.3
64QAM 0.75 dual	142.2	140.7	138.9	137.6	135.9	134.6	134.1
64QAM 0.92 single	143.1	141.6	139.9	138.6	136.8	135.6	135.1
64 QAM 0.92 dual	139.8	138.3	136.5	135.3	133.5	132.3	131.7
256QAM 0.81 single	141.7	140.2	138.5	137.2	135.4	134.2	133.7
256QAM 0.81 dual	138.3	136.8	135.0	133.7	132.0	130.7	130.2

Table 93 5.4 GHz IP mode: system threshold per channel bandwidth and output power (P) (dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-95.1	-93.1	-91.3	-90.1	-88.3	-87.1	-86.6	29
QPSK 0.63 single	-91.6	-89.6	-87.8	-86.6	-84.8	-83.6	-83.1	28
QPSK 0.87 single	-87.6	-85.6	-83.8	-82.6	-80.8	-79.6	-79.0	27
16QAM 0.63 single	-85.7	-83.7	-81.9	-80.7	-78.9	-77.6	-77.1	26
16QAM 0.63 dual	-81.2	-79.1	-77.4	-76.1	-74.4	-73.1	-72.6	26
16QAM 0.87 single	-81.0	-79.0	-77.2	-76.0	-74.2	-73.0	-72.4	25
16QAM 0.87 dual	-77.9	-75.9	-74.2	-72.9	-71.1	-69.9	-69.4	25
64QAM 0.75 single	-78.1	-76.0	-74.3	-73.0	-71.3	-70.0	-69.5	24
64QAM 0.75 dual	-75.0	-72.9	-71.2	-69.9	-68.2	-66.9	-66.4	24
64QAM 0.92 single	-74.3	-72.3	-70.5	-69.3	-67.5	-66.3	-65.8	24
64 QAM 0.92 dual	-71.1	-69.1	-67.3	-66.1	-64.3	-63.1	-62.5	24
256QAM 0.81 single	-71.1	-69.1	-67.4	-66.1	-64.3	-63.1	-62.6	24
256QAM 0.81 dual	-67.7	-65.7	-63.9	-62.6	-60.9	-59.6	-59.1	24

Table 94 5.4 GHz IP mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	171.5	169.5	167.7	166.5	164.7	163.5	163.0
QPSK 0.63 single	167.0	165.0	163.2	162.0	160.2	159.0	158.5
QPSK 0.87 single	162.0	160.0	158.2	157.0	155.2	154.0	153.4
16QAM 0.63 single	159.1	157.1	155.3	154.1	152.3	151.0	150.5
16QAM 0.63 dual	154.6	152.5	150.8	149.5	147.8	146.5	146.0
16QAM 0.87 single	153.4	151.4	149.6	148.4	146.6	145.4	144.8
16QAM 0.87 dual	150.3	148.3	146.6	145.3	143.5	142.3	141.8
64QAM 0.75 single	149.5	147.4	145.7	144.4	142.7	141.4	140.9
64QAM 0.75 dual	146.4	144.3	142.6	141.3	139.6	138.3	137.8
64QAM 0.92 single	145.7	143.7	141.9	140.7	138.9	137.7	137.2
64 QAM 0.92 dual	142.5	140.5	138.7	137.5	135.7	134.5	133.9
256QAM 0.81 single	142.5	140.5	138.8	137.5	135.7	134.5	134.0
256QAM 0.81 dual	139.1	137.1	135.3	134.0	132.3	131.0	130.5

Table 95 5.4 GHz TDM mode: system threshold per channel bandwidth and output power (P)(dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-95.1	-93.1	-91.3	-90.1	-88.3	-87.1	-86.6	27
QPSK 0.63 single	-88.6	-86.6	-84.8	-83.6	-81.8	-80.6	-80.1	26
QPSK 0.87 single	-84.6	-82.6	-80.8	-79.5	-77.8	-76.5	-76.0	25
16QAM 0.63 single	-82.6	-80.6	-78.9	-77.6	-75.8	-74.6	-74.1	24
16QAM 0.63 dual	-78.1	-76.1	-74.3	-73.1	-71.3	-70.1	-69.6	24
16QAM 0.87 single	-77.8	-75.8	-74.1	-72.8	-71.1	-69.8	-69.3	24
16QAM 0.87 dual	-74.7	-72.7	-71.0	-69.7	-68.0	-66.7	-66.2	24
64QAM 0.75 single	-74.8	-72.8	-71.0	-69.7	-68.0	-66.7	-66.2	24
64QAM 0.75 dual	-71.6	-69.6	-67.8	-66.5	-64.8	-63.5	-63.0	24
64QAM 0.92 single	-72.5	-70.5	-68.8	-67.5	-65.7	-64.5	-64.0	24
64 QAM 0.92 dual	-69.2	-67.2	-65.4	-64.2	-62.4	-61.2	-60.6	24
256QAM 0.81 single	-71.1	-69.1	-67.4	-66.1	-64.3	-63.1	-62.6	24
256QAM 0.81 dual	-67.7	-65.7	-63.9	-62.6	-60.9	-59.6	-59.1	24

Table 96 5.4 GHz TDM mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	169.5	167.5	165.7	164.5	162.7	161.5	161.0
QPSK 0.63 single	162.0	160.0	158.2	157.0	155.2	154.0	153.5
QPSK 0.87 single	157.0	155.0	153.2	151.9	150.2	148.9	148.4
16QAM 0.63 single	154.0	152.0	150.3	149.0	147.2	146.0	145.5
16QAM 0.63 dual	149.5	147.5	145.7	144.5	142.7	141.5	141.0
16QAM 0.87 single	149.2	147.2	145.5	144.2	142.5	141.2	140.7
16QAM 0.87 dual	146.1	144.1	142.4	141.1	139.4	138.1	137.6
64QAM 0.75 single	146.2	144.2	142.4	141.1	139.4	138.1	137.6
64QAM 0.75 dual	143.0	141.0	139.2	137.9	136.2	134.9	134.4
64QAM 0.92 single	143.9	141.9	140.2	138.9	137.1	135.9	135.4
64 QAM 0.92 dual	140.6	138.6	136.8	135.6	133.8	132.6	132.0
256QAM 0.81 single	142.5	140.5	138.8	137.5	135.7	134.5	134.0
256QAM 0.81 dual	139.1	137.1	135.3	134.0	132.3	131.0	130.5

Table 97 5.8 GHz IP mode: system threshold per channel bandwidth and output power (P) (dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-94.6	-92.6	-90.8	-89.6	-87.8	-86.6	-86.1	29
QPSK 0.63 single	-91.1	-89.1	-87.3	-86.1	-84.3	-83.1	-82.6	28
QPSK 0.87 single	-87.1	-85.1	-83.3	-82.1	-80.3	-79.1	-78.5	27
16QAM 0.63 single	-85.2	-83.2	-81.4	-80.1	-78.4	-77.1	-76.6	26
16QAM 0.63 dual	-80.6	-78.6	-76.9	-75.6	-73.9	-72.6	-72.1	26
16QAM 0.87 single	-80.4	-78.4	-76.7	-75.4	-73.7	-72.4	-71.9	25
16QAM 0.87 dual	-77.4	-75.4	-73.6	-72.4	-70.6	-69.3	-68.8	25
64QAM 0.75 single	-77.5	-75.5	-73.7	-72.5	-70.7	-69.4	-68.9	24
64QAM 0.75 dual	-74.4	-72.3	-70.6	-69.3	-67.6	-66.3	-65.8	24
64QAM 0.92 single	-73.6	-71.6	-69.9	-68.6	-66.9	-65.6	-65.1	24
64 QAM 0.92 dual	-70.3	-68.3	-66.6	-65.3	-63.6	-62.3	-61.8	24
256QAM 0.81 single	-70.3	-68.3	-66.5	-65.2	-63.5	-62.2	-61.7	24
256QAM 0.81 dual	-66.6	-64.6	-62.8	-61.6	-59.8	-58.6	-58.1	24

Table 98 5.8 GHz IP mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	171.2	169.2	167.4	166.2	164.4	163.2	162.7
QPSK 0.63 single	166.7	164.7	162.9	161.7	159.9	158.7	158.2
QPSK 0.87 single	161.7	159.7	157.9	156.7	154.9	153.7	153.1
16QAM 0.63 single	158.8	156.8	155.0	153.7	152.0	150.7	150.2
16QAM 0.63 dual	154.2	152.2	150.5	149.2	147.5	146.2	145.7
16QAM 0.87 single	153.0	151.0	149.3	148.0	146.3	145.0	144.5
16QAM 0.87 dual	150.0	148.0	146.2	145.0	143.2	141.9	141.4
64QAM 0.75 single	149.1	147.1	145.3	144.1	142.3	141.0	140.5
64QAM 0.75 dual	146.0	143.9	142.2	140.9	139.2	137.9	137.4
64QAM 0.92 single	145.2	143.2	141.5	140.2	138.5	137.2	136.7
64 QAM 0.92 dual	141.9	139.9	138.2	136.9	135.2	133.9	133.4
256QAM 0.81 single	141.9	139.9	138.1	136.8	135.1	133.8	133.3
256QAM 0.81 dual	138.2	136.2	134.4	133.2	131.4	130.2	129.7

Table 99 5.8 GHz TDM mode: system threshold per channel bandwidth and output power (P)(dBm)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz	P (all bands)
BPSK 0.63 single	-94.6	-92.6	-90.8	-89.6	-87.8	-86.6	-86.1	27
QPSK 0.63 single	-88.1	-86.1	-84.3	-83.1	-81.3	-80.1	-79.5	26
QPSK 0.87 single	-84.0	-82.0	-80.3	-79.0	-77.3	-76.0	-75.5	25
16QAM 0.63 single	-82.1	-80.1	-78.3	-77.1	-75.3	-74.1	-73.6	24
16QAM 0.63 dual	-77.6	-75.6	-73.8	-72.5	-70.8	-69.5	-69.0	24
16QAM 0.87 single	-77.3	-75.3	-73.5	-72.2	-70.5	-69.2	-68.7	24
16QAM 0.87 dual	-74.1	-72.1	-70.4	-69.1	-67.4	-66.1	-65.6	24
64QAM 0.75 single	-74.1	-72.1	-70.3	-69.1	-67.3	-66.1	-65.6	24
64QAM 0.75 dual	-70.8	-68.8	-67.1	-65.8	-64.1	-62.8	-62.3	24
64QAM 0.92 single	-71.8	-69.8	-68.0	-66.7	-65.0	-63.7	-63.2	24
64 QAM 0.92 dual	-68.3	-66.3	-64.5	-63.3	-61.5	-60.3	-59.8	24
256QAM 0.81 single	-70.3	-68.3	-66.5	-65.2	-63.5	-62.2	-61.7	24
256QAM 0.81 dual	-66.6	-64.6	-62.8	-61.6	-59.8	-58.6	-58.1	24

Table 100 5.8 GHz TDM mode: maximum link loss per channel bandwidth (dB)

Modulation mode	5 MHz	10 MHz	15 MHz	20 MHz	30 MHz	40 MHz	45 MHz
BPSK 0.63 single	169.2	167.2	165.4	164.2	162.4	161.2	160.7
QPSK 0.63 single	161.7	159.7	157.9	156.7	154.9	153.7	153.1
QPSK 0.87 single	156.6	154.6	152.9	151.6	149.9	148.6	148.1
16QAM 0.63 single	153.7	151.7	149.9	148.7	146.9	145.7	145.2
16QAM 0.63 dual	149.2	147.2	145.4	144.1	142.4	141.1	140.6
16QAM 0.87 single	148.9	146.9	145.1	143.8	142.1	140.8	140.3
16QAM 0.87 dual	145.7	143.7	142.0	140.7	139.0	137.7	137.2
64QAM 0.75 single	145.7	143.7	141.9	140.7	138.9	137.7	137.2
64QAM 0.75 dual	142.4	140.4	138.7	137.4	135.7	134.4	133.9
64QAM 0.92 single	143.4	141.4	139.6	138.3	136.6	135.3	134.8
64 QAM 0.92 dual	139.9	137.9	136.1	134.9	133.1	131.9	131.4
256QAM 0.81 single	141.9	139.9	138.1	136.8	135.1	133.8	133.3
256QAM 0.81 dual	138.2	136.2	134.4	133.2	131.4	130.2	129.7

Data throughput capacity tables

Data capacity in PTP topology

Use the following tables to look up the data throughput rates (Mbit/s) that are achieved when two PTP 700 ODUs are linked and the link distance (range) is 0 km:

PTP 700 variant	Link symmetry	Link optimization	Table
Full	1:1	IP	Table 101
		TDM	Table 102
	2:1	IP	Table 103
		TDM	Table 104
	3:1	IP	Table 105
	5:1	IP	Table 106
	Adaptive	IP	Table 107
Lite	1:1	IP	Table 108
		TDM	Table 109
	2:1	IP	Table 110
		TDM	Table 111
	3:1	IP	Table 112
	5:1	IP	Table 113

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**	**30 MHz**	**20 MHz**
1:1	IP	Figure 67	Figure 68	Figure 69	Figure 70
	TDM	Figure 74	Figure 75	Figure 76	Figure 77
2:1	IP	Figure 81	Figure 82	Figure 83	Figure 84
	TDM	Figure 87	Figure 88	Figure 89	Figure 90
3:1	IP	Figure 93	Figure 94	Figure 95	Figure 96
5:1	IP	Figure 99	Figure 100	Figure 101	-
Adaptive	IP	Figure 102	Figure 103	Figure 104	Figure 105

Link symmetry	Link optimization	Bandwidth		
		15 MHz	**10 MHz**	**5 MHz**
1:1	IP	Figure 71	Figure 72	Figure 73
	TDM	Figure 78	Figure 79	Figure 80
2:1	IP	Figure 85	Figure 86	-
	TDM	Figure 91	Figure 92	-
3:1	IP	Figure 97	Figure 98	-
5:1	IP	-	-	-
Adaptive	IP	Figure 106	Figure 107	-

Note Throughput for link symmetry 5:1, 3:1 and 2:1 are the same as 1:5, 1:3, and 1:2; but the Tx and Rx data rates are interchanged.

Table 101 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	225.56	225.56	451.11	205.84	205.84	411.68
64QAM 0.92 dual	190.04	190.04	380.07	173.42	173.42	346.85
64QAM 0.75 dual	155.29	155.29	310.59	141.72	141.72	283.44
16QAM 0.87 dual	120.81	120.81	241.63	110.25	110.25	220.51
16QAM 0.63 dual	86.85	86.85	173.70	79.26	79.26	158.52
256QAM 0.81 single	112.78	112.78	225.55	102.92	102.92	205.83
64QAM 0.92 single	95.02	95.02	190.03	86.71	86.71	173.42
64QAM 0.75 single	77.65	77.65	155.29	70.86	70.86	141.72
16QAM 0.87 single	60.40	60.40	120.81	55.12	55.12	110.25
16QAM 0.63 single	43.42	43.42	86.85	39.63	39.63	79.25
QPSK 0.87 single	30.20	30.20	60.40	27.56	27.56	55.12
QPSK 0.63 single	21.71	21.71	43.42	19.81	19.81	39.62
BPSK 0.63 single	10.85	10.85	21.71	9.90	9.90	19.81

Modulation mode	30 MHz (Tx/Rx/Aggregate)			20 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	150.76	150.76	301.53	99.80	99.80	199.59
64QAM 0.92 dual	127.02	127.02	254.04	84.08	84.08	168.16
64QAM 0.75 dual	103.80	103.80	207.60	68.71	68.71	137.42
16QAM 0.87 dual	80.75	80.75	161.51	53.45	53.45	106.91
16QAM 0.63 dual	58.05	58.05	116.10	38.43	38.43	76.85
256QAM 0.81 single	75.38	75.38	150.76	49.90	49.90	99.79
64QAM 0.92 single	63.51	63.51	127.02	42.04	42.04	84.08
64QAM 0.75 single	51.90	51.90	103.80	34.35	34.35	68.71
16QAM 0.87 single	40.37	40.37	80.75	26.73	26.73	53.45
16QAM 0.63 single	29.02	29.02	58.05	19.21	19.21	38.42
QPSK 0.87 single	20.19	20.19	40.37	13.36	13.36	26.72
QPSK 0.63 single	14.51	14.51	29.02	9.60	9.60	19.21
BPSK 0.63 single	7.25	7.25	14.51	4.80	4.80	9.60

Modulation mode	15 MHz (Tx/Rx/Aggregate)			10 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	75.19	75.19	150.38	49.98	49.98	99.96
64QAM 0.92 dual	63.35	63.35	126.70	42.11	42.11	84.22
64QAM 0.75 dual	51.77	51.77	103.54	34.41	34.41	68.82
16QAM 0.87 dual	40.27	40.27	80.55	26.77	26.77	53.54
16QAM 0.63 dual	28.95	28.95	57.90	19.24	19.24	38.49
256QAM 0.81 single	37.59	37.59	75.19	24.99	24.99	49.98
64QAM 0.92 single	31.67	31.67	63.35	21.05	21.05	42.11
64QAM 0.75 single	25.88	25.88	51.77	17.20	17.20	34.41
16QAM 0.87 single	20.14	20.14	40.27	13.38	13.38	26.77
16QAM 0.63 single	14.47	14.47	28.95	9.62	9.62	19.24
QPSK 0.87 single	10.07	10.07	20.13	6.69	6.69	13.38
QPSK 0.63 single	7.24	7.24	14.47	4.81	4.81	9.62
BPSK 0.63 single	3.62	3.62	7.23	2.40	2.40	4.81

Modulation mode	5 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	24.14	24.14	48.28
64QAM 0.92 dual	20.34	20.34	40.68
64QAM 0.75 dual	16.62	16.62	33.24
16QAM 0.87 dual	12.93	12.93	25.86
16QAM 0.63 dual	9.29	9.29	18.59
256QAM 0.81 single	12.07	12.07	24.14
64QAM 0.92 single	10.17	10.17	20.34
64QAM 0.75 single	8.31	8.31	16.62
16QAM 0.87 single	6.46	6.46	12.93
16QAM 0.63 single	4.65	4.65	9.29
QPSK 0.87 single	3.23	3.23	6.46
QPSK 0.63 single	2.32	2.32	4.64
BPSK 0.63 single	1.16	1.16	2.32

Table 102 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	198.33	198.33	396.66	184.65	184.65	369.29
64QAM 0.92 dual	167.10	167.10	334.20	155.57	155.57	311.14
64QAM 0.75 dual	136.55	136.55	273.10	127.13	127.13	254.26
16QAM 0.87 dual	106.23	106.23	212.46	98.90	98.90	197.80
16QAM 0.63 dual	76.37	76.37	152.73	71.10	71.10	142.20
256QAM 0.81 single	99.16	99.16	198.33	92.32	92.32	184.64
64QAM 0.92 single	83.55	83.55	167.09	77.78	77.78	155.57
64QAM 0.75 single	68.27	68.27	136.55	63.56	63.56	127.13
16QAM 0.87 single	53.11	53.11	106.23	49.45	49.45	98.90
16QAM 0.63 single	38.18	38.18	76.36	35.55	35.55	71.09
QPSK 0.87 single	26.55	26.55	53.11	24.72	24.72	49.45
QPSK 0.63 single	19.09	19.09	38.18	17.77	17.77	35.54
BPSK 0.63 single	9.54	9.54	19.09	8.88	8.88	17.77

Modulation mode	30 MHz (Tx/Rx/Aggregate)			20 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	139.97	139.97	279.95	95.52	95.52	191.04
64QAM 0.92 dual	117.93	117.93	235.86	80.48	80.48	160.96
64QAM 0.75 dual	96.37	96.37	192.74	65.77	65.77	131.53
16QAM 0.87 dual	74.97	74.97	149.95	51.16	51.16	102.33
16QAM 0.63 dual	53.90	53.90	107.79	36.78	36.78	73.56
256QAM 0.81 single	69.99	69.99	139.97	47.76	47.76	95.52
64QAM 0.92 single	58.96	58.96	117.93	40.24	40.24	80.48
64QAM 0.75 single	48.19	48.19	96.37	32.88	32.88	65.76
16QAM 0.87 single	37.49	37.49	74.97	25.58	25.58	51.16
16QAM 0.63 single	26.95	26.95	53.89	18.39	18.39	36.78
QPSK 0.87 single	18.74	18.74	37.48	12.79	12.79	25.58
QPSK 0.63 single	13.47	13.47	26.94	9.19	9.19	18.39
BPSK 0.63 single	6.73	6.73	13.47	4.59	4.59	9.19

Modulation mode	15 MHz (Tx/Rx/Aggregate)			10 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	72.60	72.60	145.19	48.96	48.96	97.92
64QAM 0.92 dual	61.16	61.16	122.33	41.25	41.25	82.50
64QAM 0.75 dual	49.98	49.98	99.96	33.71	33.71	67.42
16QAM 0.87 dual	38.88	38.88	77.77	26.22	26.22	52.45
16QAM 0.63 dual	27.95	27.95	55.90	18.85	18.85	37.70
256QAM 0.81 single	36.30	36.30	72.59	24.48	24.48	48.96
64QAM 0.92 single	30.58	30.58	61.16	20.62	20.62	41.25
64QAM 0.75 single	24.99	24.99	49.98	16.85	16.85	33.71
16QAM 0.87 single	19.44	19.44	38.88	13.11	13.11	26.22
16QAM 0.63 single	13.97	13.97	27.95	9.42	9.42	18.85
QPSK 0.87 single	9.72	9.72	19.44	6.55	6.55	13.11
QPSK 0.63 single	6.99	6.99	13.97	4.71	4.71	9.42
BPSK 0.63 single	3.49	3.49	6.98	2.35	2.35	4.71

Modulation mode	5 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	24.14	24.14	48.28
64QAM 0.92 dual	20.34	20.34	40.68
64QAM 0.75 dual	16.62	16.62	33.24
16QAM 0.87 dual	12.93	12.93	25.86
16QAM 0.63 dual	9.29	9.29	18.59
256QAM 0.81 single	12.07	12.07	24.14
64QAM 0.92 single	10.17	10.17	20.34
64QAM 0.75 single	8.31	8.31	16.62
16QAM 0.87 single	6.46	6.46	12.93
16QAM 0.63 single	4.65	4.65	9.29
QPSK 0.87 single	3.23	3.23	6.46
QPSK 0.63 single	2.32	2.32	4.64
BPSK 0.63 single	1.16	1.16	2.32

Table 103 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	298.95	149.47	448.42	272.96	136.48	409.44
64QAM 0.92 dual	251.87	125.94	377.81	229.98	114.99	344.96
64QAM 0.75 dual	205.83	102.91	308.74	187.93	93.97	281.90
16QAM 0.87 dual	160.13	80.06	240.19	146.21	73.10	219.31
16QAM 0.63 dual	115.11	57.55	172.67	105.10	52.55	157.65
256QAM 0.81 single	149.47	74.73	224.21	136.48	68.24	204.72
64QAM 0.92 single	125.93	62.97	188.90	114.99	57.49	172.48
64QAM 0.75 single	102.91	51.46	154.37	93.97	46.98	140.95
16QAM 0.87 single	80.06	40.03	120.09	73.10	36.55	109.65
16QAM 0.63 single	57.55	28.78	86.33	52.55	26.27	78.82
QPSK 0.87 single	40.03	20.01	60.04	36.55	18.27	54.82
QPSK 0.63 single	28.77	14.39	43.16	26.27	13.14	39.41
BPSK 0.63 single	14.38	7.19	21.58	13.13	6.57	19.70

Modulation mode	30 MHz (Tx/Rx/Aggregate)			20 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	199.99	99.99	299.98	133.06	66.53	199.59
64QAM 0.92 dual	168.50	84.25	252.74	112.11	56.05	168.16
64QAM 0.75 dual	137.69	68.85	206.54	91.61	45.81	137.42
16QAM 0.87 dual	107.12	53.56	160.68	71.27	35.63	106.91
16QAM 0.63 dual	77.01	38.50	115.51	51.24	25.62	76.85
256QAM 0.81 single	99.99	50.00	149.99	66.53	33.26	99.79
64QAM 0.92 single	84.25	42.12	126.37	56.05	28.03	84.08
64QAM 0.75 single	68.85	34.42	103.27	45.81	22.90	68.71
16QAM 0.87 single	53.56	26.78	80.34	35.63	17.82	53.45
16QAM 0.63 single	38.50	19.25	57.75	25.62	12.81	38.42
QPSK 0.87 single	26.78	13.39	40.16	17.82	8.91	26.72
QPSK 0.63 single	19.25	9.62	28.87	12.81	6.40	19.21
BPSK 0.63 single	9.62	4.81	14.43	6.40	3.20	9.60

Modulation mode	15 MHz (Tx/Rx/Aggregate)			10 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	100.26	50.13	150.38	66.18	33.09	99.27
64QAM 0.92 dual	84.47	42.23	126.70	55.76	27.88	83.64
64QAM 0.75 dual	69.03	34.51	103.54	45.56	22.78	68.35
16QAM 0.87 dual	53.70	26.85	80.55	35.45	17.72	53.17
16QAM 0.63 dual	38.60	19.30	57.90	25.48	12.74	38.22
256QAM 0.81 single	50.13	25.06	75.19	33.09	16.54	49.63
64QAM 0.92 single	42.23	21.12	63.35	27.88	13.94	41.82
64QAM 0.75 single	34.51	17.26	51.77	22.78	11.39	34.17
16QAM 0.87 single	26.85	13.42	40.27	17.72	8.86	26.58
16QAM 0.63 single	19.30	9.65	28.95	12.74	6.37	19.11
QPSK 0.87 single	13.42	6.71	20.13	8.86	4.43	13.29
QPSK 0.63 single	9.65	4.82	14.47	6.37	3.18	9.55
BPSK 0.63 single	4.82	2.41	7.23	3.18	1.59	4.77

Table 104 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	277.05	138.52	415.57	256.25	128.12	384.37
64QAM 0.92 dual	233.42	116.71	350.13	215.89	107.95	323.84
64QAM 0.75 dual	190.75	95.37	286.12	176.43	88.21	264.64
16QAM 0.87 dual	148.39	74.20	222.59	137.25	68.63	205.88
16QAM 0.63 dual	106.68	53.34	160.02	98.67	49.33	148.00
256QAM 0.81 single	138.52	69.26	207.78	128.12	64.06	192.18
64QAM 0.92 single	116.71	58.35	175.06	107.94	53.97	161.92
64QAM 0.75 single	95.37	47.69	143.06	88.21	44.10	132.32
16QAM 0.87 single	74.20	37.10	111.29	68.62	34.31	102.94
16QAM 0.63 single	53.34	26.67	80.00	49.33	24.66	74.00
QPSK 0.87 single	37.10	18.55	55.64	34.31	17.15	51.46
QPSK 0.63 single	26.67	13.33	40.00	24.66	12.33	36.99
BPSK 0.63 single	13.33	6.66	20.00	12.33	6.16	18.49

Modulation mode	30 MHz (Tx/Rx/Aggregate)			20 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	192.13	96.07	288.20	130.15	65.07	195.22
64QAM 0.92 dual	161.88	80.94	242.81	109.65	54.83	164.48
64QAM 0.75 dual	132.28	66.14	198.42	89.61	44.80	134.41
16QAM 0.87 dual	102.91	51.45	154.37	69.71	34.85	104.57
16QAM 0.63 dual	73.98	36.99	110.97	50.11	25.06	75.17
256QAM 0.81 single	96.06	48.03	144.10	65.07	32.54	97.61
64QAM 0.92 single	80.94	40.47	121.40	54.83	27.41	82.24
64QAM 0.75 single	66.14	33.07	99.21	44.80	22.40	67.20
16QAM 0.87 single	51.45	25.73	77.18	34.85	17.43	52.28
16QAM 0.63 single	36.99	18.49	55.48	25.06	12.53	37.58
QPSK 0.87 single	25.73	12.86	38.59	17.43	8.71	26.14
QPSK 0.63 single	18.49	9.25	27.74	12.53	6.26	18.79
BPSK 0.63 single	9.24	4.62	13.87	6.26	3.13	9.39

Modulation mode	15 MHz (Tx/Rx/Aggregate)			10 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	98.49	49.25	147.74	66.18	33.09	99.27
64QAM 0.92 dual	82.98	41.49	124.48	55.76	27.88	83.64
64QAM 0.75 dual	67.81	33.91	101.72	45.56	22.78	68.35
16QAM 0.87 dual	52.76	26.38	79.13	35.45	17.72	53.17
16QAM 0.63 dual	37.92	18.96	56.89	25.48	12.74	38.22
256QAM 0.81 single	49.25	24.62	73.87	33.09	16.54	49.63
64QAM 0.92 single	41.49	20.74	62.24	27.88	13.94	41.82
64QAM 0.75 single	33.91	16.95	50.86	22.78	11.39	34.17
16QAM 0.87 single	26.38	13.19	39.56	17.72	8.86	26.58
16QAM 0.63 single	18.96	9.48	28.44	12.74	6.37	19.11
QPSK 0.87 single	13.19	6.59	19.78	8.86	4.43	13.29
QPSK 0.63 single	9.48	4.74	14.22	6.37	3.18	9.55
BPSK 0.63 single	4.74	2.37	7.11	3.18	1.59	4.77

Table 105 Throughput at zero link range (Mbit/s), Full, symmetry 3:1, optimization IP

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	336.32	112.10	448.42	307.08	102.36	409.44
64QAM 0.92 dual	283.36	94.45	377.81	258.72	86.24	344.96
64QAM 0.75 dual	231.56	77.18	308.74	211.43	70.47	281.90
16QAM 0.87 dual	180.14	60.05	240.19	164.48	54.83	219.31
16QAM 0.63 dual	129.50	43.17	172.67	118.24	39.41	157.65
256QAM 0.81 single	168.16	56.05	224.21	153.54	51.18	204.72
64QAM 0.92 single	141.68	47.22	188.90	129.36	43.12	172.48
64QAM 0.75 single	115.78	38.59	154.37	105.71	35.24	140.95
16QAM 0.87 single	90.07	30.02	120.09	82.24	27.41	109.65
16QAM 0.63 single	64.75	21.58	86.33	59.12	19.70	78.82
QPSK 0.87 single	45.03	15.01	60.04	41.12	13.70	54.82
QPSK 0.63 single	32.37	10.79	43.16	29.56	9.85	39.41
BPSK 0.63 single	16.18	5.39	21.58	14.78	4.92	19.70

Modulation mode	30 MHz (Tx/Rx/Aggregate)			20 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	224.42	74.80	299.22	148.04	49.34	197.38
64QAM 0.92 dual	189.08	63.02	252.10	124.73	41.57	166.30
64QAM 0.75 dual	154.51	51.50	206.01	101.92	33.97	135.90
16QAM 0.87 dual	120.20	40.07	160.27	79.29	26.43	105.72
16QAM 0.63 dual	86.41	28.80	115.21	57.00	19.00	76.00
256QAM 0.81 single	112.21	37.40	149.61	74.02	24.67	98.69
64QAM 0.92 single	94.54	31.51	126.05	62.36	20.79	83.15
64QAM 0.75 single	77.25	25.75	103.00	50.96	16.99	67.95
16QAM 0.87 single	60.10	20.03	80.13	39.65	13.21	52.86
16QAM 0.63 single	43.20	14.40	57.60	28.50	9.50	38.00
QPSK 0.87 single	30.05	10.01	40.06	19.82	6.61	26.43
QPSK 0.63 single	21.60	7.20	28.80	14.25	4.75	19.00
BPSK 0.63 single	10.80	3.60	14.40	7.12	2.37	9.50

Modulation mode	15 MHz (Tx/Rx/Aggregate)			10 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	111.79	37.26	149.05	74.97	24.99	99.96
64QAM 0.92 dual	94.19	31.39	125.58	63.16	21.05	84.22
64QAM 0.75 dual	76.97	25.65	102.62	51.62	17.20	68.82
16QAM 0.87 dual	59.88	19.96	79.83	40.15	13.38	53.54
16QAM 0.63 dual	43.04	14.35	57.39	28.87	9.62	38.49
256QAM 0.81 single	55.89	18.63	74.52	37.48	12.49	49.98
64QAM 0.92 single	47.09	15.70	62.79	31.58	10.53	42.11
64QAM 0.75 single	38.48	12.83	51.31	25.81	8.60	34.41
16QAM 0.87 single	29.94	9.98	39.91	20.08	6.69	26.77
16QAM 0.63 single	21.52	7.17	28.69	14.43	4.81	19.24
QPSK 0.87 single	14.97	4.99	19.95	10.04	3.34	13.38
QPSK 0.63 single	10.76	3.58	14.34	7.21	2.40	9.62
BPSK 0.63 single	5.38	1.79	7.17	3.61	1.20	4.81

Table 106 Throughput at zero link range (Mbit/s), Full, symmetry 5:1, optimization IP

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	373.69	74.74	448.42	333.94	66.79	400.73
64QAM 0.92 dual	314.84	62.97	377.81	281.35	56.27	337.62
64QAM 0.75 dual	257.28	51.46	308.74	229.92	45.98	275.90
16QAM 0.87 dual	200.16	40.03	240.19	178.87	35.77	214.64
16QAM 0.63 dual	143.89	28.78	172.67	128.58	25.72	154.30
256QAM 0.81 single	186.84	37.37	224.21	166.97	33.39	200.36
64QAM 0.92 single	157.42	31.48	188.90	140.67	28.13	168.81
64QAM 0.75 single	128.64	25.73	154.37	114.96	22.99	137.95
16QAM 0.87 single	100.08	20.01	120.09	89.43	17.88	107.32
16QAM 0.63 single	71.94	14.39	86.33	64.29	12.86	77.15
QPSK 0.87 single	50.04	10.01	60.04	44.71	8.94	53.65
QPSK 0.63 single	35.97	7.19	43.16	32.14	6.43	38.57
BPSK 0.63 single	17.98	3.59	21.58	16.07	3.21	19.28

Modulation mode	30 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	247.46	49.49	296.95
64QAM 0.92 dual	208.49	41.70	250.19
64QAM 0.75 dual	170.38	34.07	204.45
16QAM 0.87 dual	132.55	26.51	159.05
16QAM 0.63 dual	95.28	19.06	114.34
256QAM 0.81 single	123.73	24.74	148.47
64QAM 0.92 single	104.24	20.85	125.09
64QAM 0.75 single	85.19	17.04	102.22
16QAM 0.87 single	66.27	13.25	79.52
16QAM 0.63 single	47.64	9.53	57.17
QPSK 0.87 single	33.13	6.63	39.76
QPSK 0.63 single	23.82	4.76	28.58
BPSK 0.63 single	11.91	2.38	14.29

Table 107 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	405.94	40.59	446.54	366.90	40.77	407.67
64QAM 0.92 dual	342.02	34.20	376.22	309.12	34.35	343.47
64QAM 0.75 dual	279.49	27.95	307.44	252.61	28.07	280.68
16QAM 0.87 dual	217.44	21.74	239.18	196.52	21.83	218.36
16QAM 0.63 dual	156.31	15.63	171.94	141.28	15.70	156.97
256QAM 0.81 single	202.97	20.30	223.26	183.45	20.38	203.83
64QAM 0.92 single	171.01	17.10	188.11	154.56	17.17	171.73
64QAM 0.75 single	139.75	13.97	153.72	126.30	14.03	140.34
16QAM 0.87 single	108.71	10.87	119.58	98.26	10.92	109.17
16QAM 0.63 single	78.15	7.81	85.97	70.64	7.85	78.48
QPSK 0.87 single	54.35	5.43	59.79	49.13	5.46	54.58
QPSK 0.63 single	39.07	3.91	42.98	35.32	3.92	39.24
BPSK 0.63 single	19.53	1.95	21.49	17.65	1.96	19.61

Modulation mode	30 MHz (Tx/Rx/Aggregate)			20 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	261.82	37.40	299.22	158.96	39.74	198.70
64QAM 0.92 dual	220.59	31.51	252.10	133.93	33.48	167.41
64QAM 0.75 dual	180.26	25.75	206.01	109.45	27.36	136.81
16QAM 0.87 dual	140.24	20.03	160.27	85.15	21.28	106.43
16QAM 0.63 dual	100.81	14.40	115.21	61.21	15.30	76.51
256QAM 0.81 single	130.91	18.70	149.61	79.48	19.87	99.35
64QAM 0.92 single	110.29	15.75	126.05	66.96	16.74	83.70
64QAM 0.75 single	90.13	12.87	103.00	54.72	13.68	68.40
16QAM 0.87 single	70.12	10.01	80.13	42.57	10.64	53.21
16QAM 0.63 single	50.40	7.20	57.60	30.60	7.65	38.25
QPSK 0.87 single	35.06	5.01	40.06	21.28	5.32	26.60
QPSK 0.63 single	25.20	3.60	28.80	15.30	3.82	19.12
BPSK 0.63 single	12.60	1.80	14.40	7.65	1.91	9.56

Modulation mode	15 MHz (Tx/Rx/Aggregate)			10 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	119.88	29.97	149.85	66.18	33.09	99.27
64QAM 0.92 dual	101.00	25.25	126.25	55.76	27.88	83.64
64QAM 0.75 dual	82.54	20.63	103.17	45.56	22.78	68.35
16QAM 0.87 dual	64.21	16.05	80.26	35.45	17.72	53.17
16QAM 0.63 dual	46.16	11.54	57.70	25.48	12.74	38.22
256QAM 0.81 single	59.94	14.98	74.92	33.09	16.54	49.63
64QAM 0.92 single	50.50	12.62	63.12	27.88	13.94	41.82
64QAM 0.75 single	41.27	10.32	51.58	22.78	11.39	34.17
16QAM 0.87 single	32.10	8.02	40.13	17.72	8.86	26.58
16QAM 0.63 single	23.08	5.77	28.85	12.74	6.37	19.11
QPSK 0.87 single	16.05	4.01	20.06	8.86	4.43	13.29
QPSK 0.63 single	11.54	2.88	14.42	6.37	3.18	9.55
BPSK 0.63 single	5.77	1.44	7.21	3.18	1.59	4.77

Table 108 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	113.00	113.00	226.00	103.00	103.00	206.00
64QAM 0.92 dual	95.00	95.00	190.00	87.00	87.00	174.00
64QAM 0.75 dual	78.00	78.00	156.00	71.00	71.00	142.00
16QAM 0.87 dual	60.00	60.00	120.00	55.00	55.00	110.00
16QAM 0.63 dual	43.00	43.00	86.00	40.00	40.00	80.00
256QAM 0.81 single	56.00	56.00	112.00	52.00	52.00	104.00
64QAM 0.92 single	48.00	48.00	96.00	43.00	43.00	86.00
64QAM 0.75 single	39.00	39.00	78.00	35.00	35.00	70.00
16QAM 0.87 single	30.00	30.00	60.00	28.00	28.00	56.00
16QAM 0.63 single	22.00	22.00	44.00	20.00	20.00	40.00
QPSK 0.87 single	15.00	15.00	30.00	14.00	14.00	28.00
QPSK 0.63 single	11.00	11.00	22.00	10.00	10.00	20.00
BPSK 0.63 single	5.00	5.00	10.00	5.00	5.00	10.00

Modulation mode	30 MHz (Tx/Rx/Aggregate)			20 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	75.00	75.00	150.00	50.00	50.00	100.00
64QAM 0.92 dual	64.00	64.00	128.00	42.00	42.00	84.00
64QAM 0.75 dual	52.00	52.00	104.00	34.00	34.00	68.00
16QAM 0.87 dual	40.00	40.00	80.00	27.00	27.00	54.00
16QAM 0.63 dual	29.00	29.00	58.00	19.00	19.00	38.00
256QAM 0.81 single	38.00	38.00	76.00	25.00	25.00	50.00
64QAM 0.92 single	32.00	32.00	64.00	21.00	21.00	42.00
64QAM 0.75 single	26.00	26.00	52.00	17.00	17.00	34.00
16QAM 0.87 single	20.00	20.00	40.00	13.00	13.00	26.00
16QAM 0.63 single	15.00	15.00	30.00	10.00	10.00	20.00
QPSK 0.87 single	10.00	10.00	20.00	7.00	7.00	14.00
QPSK 0.63 single	7.00	7.00	14.00	5.00	5.00	10.00
BPSK 0.63 single	5.00	5.00	10.00	4.80	4.80	9.60

Modulation mode	15 MHz (Tx/Rx/Aggregate)			10 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	38.00	38.00	76.00	25.00	25.00	50.00
64QAM 0.92 dual	32.00	32.00	64.00	21.00	21.00	42.00
64QAM 0.75 dual	26.00	26.00	52.00	17.00	17.00	34.00
16QAM 0.87 dual	20.00	20.00	40.00	13.00	13.00	26.00
16QAM 0.63 dual	14.00	14.00	28.00	10.00	10.00	20.00
256QAM 0.81 single	19.00	19.00	38.00	12.00	12.00	24.00
64QAM 0.92 single	16.00	16.00	32.00	11.00	11.00	22.00
64QAM 0.75 single	13.00	13.00	26.00	9.00	9.00	18.00
16QAM 0.87 single	10.00	10.00	20.00	7.00	7.00	14.00
16QAM 0.63 single	7.00	7.00	14.00	5.00	5.00	10.00
QPSK 0.87 single	5.00	5.00	10.00	5.00	5.00	10.00
QPSK 0.63 single	5.00	5.00	10.00	4.81	4.81	9.62
BPSK 0.63 single	3.62	3.62	7.23	2.40	2.40	4.81

Modulation mode	5 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	12.00	12.00	24.00
64QAM 0.92 dual	10.00	10.00	20.00
64QAM 0.75 dual	8.00	8.00	16.00
16QAM 0.87 dual	6.00	6.00	12.00
16QAM 0.63 dual	5.00	5.00	10.00
256QAM 0.81 single	6.00	6.00	12.00
64QAM 0.92 single	5.00	5.00	10.00
64QAM 0.75 single	5.00	5.00	10.00
16QAM 0.87 single	5.00	5.00	10.00
16QAM 0.63 single	4.65	4.65	9.30
QPSK 0.87 single	3.24	3.24	6.47
QPSK 0.63 single	2.33	2.33	4.65
BPSK 0.63 single	1.16	1.16	2.32

Table 109 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	99.00	99.00	198.00	92.00	92.00	184.00
64QAM 0.92 dual	84.00	84.00	168.00	78.00	78.00	156.00
64QAM 0.75 dual	68.00	68.00	136.00	64.00	64.00	128.00
16QAM 0.87 dual	53.00	53.00	106.00	50.00	50.00	100.00
16QAM 0.63 dual	38.00	38.00	76.00	36.00	36.00	72.00
256QAM 0.81 single	50.00	50.00	100.00	46.00	46.00	92.00
64QAM 0.92 single	42.00	42.00	84.00	39.00	39.00	78.00
64QAM 0.75 single	34.00	34.00	68.00	32.00	32.00	64.00
16QAM 0.87 single	27.00	27.00	54.00	25.00	25.00	50.00
16QAM 0.63 single	19.00	19.00	38.00	18.00	18.00	36.00
QPSK 0.87 single	13.00	13.00	26.00	12.00	12.00	24.00
QPSK 0.63 single	10.00	10.00	20.00	9.00	9.00	18.00
BPSK 0.63 single	5.00	5.00	10.00	5.00	5.00	10.00

Modulation mode	30 MHz (Tx/Rx/Aggregate)			20 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	70.00	70.00	140.00	48.00	48.00	96.00
64QAM 0.92 dual	59.00	59.00	118.00	40.00	40.00	80.00
64QAM 0.75 dual	48.00	48.00	96.00	33.00	33.00	66.00
16QAM 0.87 dual	37.00	37.00	74.00	26.00	26.00	52.00
16QAM 0.63 dual	27.00	27.00	54.00	18.00	18.00	36.00
256QAM 0.81 single	35.00	35.00	70.00	24.00	24.00	48.00
64QAM 0.92 single	29.00	29.00	58.00	20.00	20.00	40.00
64QAM 0.75 single	24.00	24.00	48.00	16.00	16.00	32.00
16QAM 0.87 single	19.00	19.00	38.00	13.00	13.00	26.00
16QAM 0.63 single	13.00	13.00	26.00	9.00	9.00	18.00
QPSK 0.87 single	9.00	9.00	18.00	6.00	6.00	12.00
QPSK 0.63 single	7.00	7.00	14.00	5.00	5.00	10.00
BPSK 0.63 single	5.00	5.00	10.00	4.59	4.59	9.19

Modulation mode	15 MHz (Tx/Rx/Aggregate)			10 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	36.00	36.00	72.00	24.00	24.00	48.00
64QAM 0.92 dual	31.00	31.00	62.00	21.00	21.00	42.00
64QAM 0.75 dual	25.00	25.00	50.00	17.00	17.00	34.00
16QAM 0.87 dual	19.00	19.00	38.00	13.00	13.00	26.00
16QAM 0.63 dual	14.00	14.00	28.00	9.00	9.00	18.00
256QAM 0.81 single	18.00	18.00	36.00	12.00	12.00	24.00
64QAM 0.92 single	15.00	15.00	30.00	10.00	10.00	20.00
64QAM 0.75 single	12.00	12.00	24.00	8.00	8.00	16.00
16QAM 0.87 single	10.00	10.00	20.00	7.00	7.00	14.00
16QAM 0.63 single	7.00	7.00	14.00	5.00	5.00	10.00
QPSK 0.87 single	5.00	5.00	10.00	5.00	5.00	10.00
QPSK 0.63 single	5.00	5.00	10.00	4.71	4.71	9.42
BPSK 0.63 single	3.49	3.49	6.98	2.35	2.35	4.71

Modulation mode	5 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	12.00	12.00	24.00
64QAM 0.92 dual	10.00	10.00	20.00
64QAM 0.75 dual	8.00	8.00	16.00
16QAM 0.87 dual	6.00	6.00	12.00
16QAM 0.63 dual	5.00	5.00	10.00
256QAM 0.81 single	6.00	6.00	12.00
64QAM 0.92 single	5.00	5.00	10.00
64QAM 0.75 single	5.00	5.00	10.00
16QAM 0.87 single	5.00	5.00	10.00
16QAM 0.63 single	4.65	4.65	9.29
QPSK 0.87 single	3.23	3.23	6.46
QPSK 0.63 single	2.32	2.32	4.64
BPSK 0.63 single	1.16	1.16	2.32

Table 110 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	149.00	75.00	224.00	136.00	68.00	204.00
64QAM 0.92 dual	126.00	63.00	189.00	115.00	57.00	172.00
64QAM 0.75 dual	103.00	51.00	154.00	94.00	47.00	141.00
16QAM 0.87 dual	80.00	40.00	120.00	73.00	37.00	110.00
16QAM 0.63 dual	58.00	29.00	87.00	53.00	26.00	79.00
256QAM 0.81 single	75.00	37.00	112.00	68.00	34.00	102.00
64QAM 0.92 single	63.00	31.00	94.00	57.00	29.00	86.00
64QAM 0.75 single	51.00	26.00	77.00	47.00	23.00	70.00
16QAM 0.87 single	40.00	20.00	60.00	37.00	18.00	55.00
16QAM 0.63 single	29.00	14.00	43.00	26.00	13.00	39.00
QPSK 0.87 single	20.00	10.00	30.00	18.00	9.00	27.00
QPSK 0.63 single	14.00	7.00	21.00	13.00	7.00	20.00
BPSK 0.63 single	7.00	5.00	12.00	7.00	5.00	12.00

Modulation mode	30 MHz (Tx/Rx/Aggregate)			20 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	100.00	50.00	150.00	67.00	33.00	100.00
64QAM 0.92 dual	84.00	42.00	126.00	56.00	28.00	84.00
64QAM 0.75 dual	69.00	34.00	103.00	46.00	23.00	69.00
16QAM 0.87 dual	54.00	27.00	81.00	36.00	18.00	54.00
16QAM 0.63 dual	39.00	19.00	58.00	26.00	13.00	39.00
256QAM 0.81 single	50.00	25.00	75.00	33.00	17.00	50.00
64QAM 0.92 single	42.00	21.00	63.00	28.00	14.00	42.00
64QAM 0.75 single	34.00	17.00	51.00	23.00	11.00	34.00
16QAM 0.87 single	27.00	13.00	40.00	18.00	9.00	27.00
16QAM 0.63 single	19.00	10.00	29.00	13.00	6.00	19.00
QPSK 0.87 single	13.00	7.00	20.00	9.00	5.00	14.00
QPSK 0.63 single	10.00	5.00	15.00	6.00	5.00	11.00
BPSK 0.63 single	5.00	4.81	9.81	5.00	3.20	8.20

Modulation mode	15 MHz (Tx/Rx/Aggregate)			10 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	50.00	25.00	75.00	33.00	17.00	50.00
64QAM 0.92 dual	42.00	21.00	63.00	28.00	14.00	42.00
64QAM 0.75 dual	35.00	17.00	52.00	23.00	11.00	34.00
16QAM 0.87 dual	27.00	13.00	40.00	18.00	9.00	27.00
16QAM 0.63 dual	19.00	10.00	29.00	13.00	6.00	19.00
256QAM 0.81 single	25.00	13.00	38.00	17.00	8.00	25.00
64QAM 0.92 single	21.00	11.00	32.00	14.00	7.00	21.00
64QAM 0.75 single	17.00	9.00	26.00	11.00	6.00	17.00
16QAM 0.87 single	13.00	7.00	20.00	9.00	5.00	14.00
16QAM 0.63 single	10.00	5.00	15.00	6.00	5.00	11.00
QPSK 0.87 single	7.00	5.00	12.00	5.00	4.43	9.43
QPSK 0.63 single	5.00	4.82	9.82	5.00	3.18	8.18
BPSK 0.63 single	4.82	2.41	7.23	3.18	1.59	4.77

Table 111 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	139.00	69.00	208.00	128.00	64.00	192.00
64QAM 0.92 dual	117.00	58.00	175.00	108.00	54.00	162.00
64QAM 0.75 dual	95.00	48.00	143.00	88.00	44.00	132.00
16QAM 0.87 dual	74.00	37.00	111.00	69.00	34.00	103.00
16QAM 0.63 dual	53.00	27.00	80.00	49.00	25.00	74.00
256QAM 0.81 single	69.00	35.00	104.00	64.00	32.00	96.00
64QAM 0.92 single	58.00	29.00	87.00	54.00	27.00	81.00
64QAM 0.75 single	48.00	24.00	72.00	44.00	22.00	66.00
16QAM 0.87 single	37.00	19.00	56.00	34.00	17.00	51.00
16QAM 0.63 single	27.00	13.00	40.00	25.00	12.00	37.00
QPSK 0.87 single	19.00	9.00	28.00	17.00	9.00	26.00
QPSK 0.63 single	13.00	7.00	20.00	12.00	6.00	18.00
BPSK 0.63 single	7.00	5.00	12.00	6.00	5.00	11.00

Modulation mode	30 MHz (Tx/Rx/Aggregate)			20 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	96.00	48.00	144.00	65.00	33.00	98.00
64QAM 0.92 dual	81.00	40.00	121.00	55.00	27.00	82.00
64QAM 0.75 dual	66.00	33.00	99.00	45.00	22.00	67.00
16QAM 0.87 dual	51.00	26.00	77.00	35.00	17.00	52.00
16QAM 0.63 dual	37.00	18.00	55.00	25.00	13.00	38.00
256QAM 0.81 single	48.00	24.00	72.00	33.00	16.00	49.00
64QAM 0.92 single	40.00	20.00	60.00	27.00	14.00	41.00
64QAM 0.75 single	33.00	17.00	50.00	22.00	11.00	33.00
16QAM 0.87 single	26.00	13.00	39.00	17.00	9.00	26.00
16QAM 0.63 single	18.00	9.00	27.00	13.00	6.00	19.00
QPSK 0.87 single	13.00	6.00	19.00	9.00	5.00	14.00
QPSK 0.63 single	9.00	5.00	14.00	6.00	5.00	11.00
BPSK 0.63 single	5.00	4.62	9.62	5.00	3.13	8.13

Modulation mode	15 MHz (Tx/Rx/Aggregate)			10 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	49.00	25.00	74.00	33.00	17.00	50.00
64QAM 0.92 dual	41.00	21.00	62.00	28.00	14.00	42.00
64QAM 0.75 dual	34.00	17.00	51.00	23.00	11.00	34.00
16QAM 0.87 dual	26.00	13.00	39.00	18.00	9.00	27.00
16QAM 0.63 dual	19.00	9.00	28.00	13.00	6.00	19.00
256QAM 0.81 single	25.00	12.00	37.00	17.00	8.00	25.00
64QAM 0.92 single	21.00	10.00	31.00	14.00	7.00	21.00
64QAM 0.75 single	17.00	8.00	25.00	11.00	6.00	17.00
16QAM 0.87 single	13.00	7.00	20.00	9.00	5.00	14.00
16QAM 0.63 single	9.00	5.00	14.00	6.00	5.00	11.00
QPSK 0.87 single	7.00	5.00	12.00	5.00	4.43	9.43
QPSK 0.63 single	5.00	4.74	9.74	5.00	3.18	8.18
BPSK 0.63 single	4.74	2.37	7.11	3.18	1.59	4.77

Table 112 Throughput at zero link range (Mbit/s), Lite, symmetry 3:1, optimization IP

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	168.00	56.00	224.00	154.00	51.00	205.00
64QAM 0.92 dual	142.00	47.00	189.00	129.00	43.00	172.00
64QAM 0.75 dual	116.00	39.00	155.00	106.00	35.00	141.00
16QAM 0.87 dual	90.00	30.00	120.00	82.00	27.00	109.00
16QAM 0.63 dual	65.00	22.00	87.00	59.00	20.00	79.00
256QAM 0.81 single	84.00	28.00	112.00	77.00	26.00	103.00
64QAM 0.92 single	71.00	24.00	95.00	65.00	22.00	87.00
64QAM 0.75 single	58.00	19.00	77.00	53.00	18.00	71.00
16QAM 0.87 single	45.00	15.00	60.00	41.00	14.00	55.00
16QAM 0.63 single	32.00	11.00	43.00	30.00	10.00	40.00
QPSK 0.87 single	23.00	8.00	31.00	21.00	7.00	28.00
QPSK 0.63 single	16.00	5.00	21.00	15.00	5.00	20.00
BPSK 0.63 single	8.00	5.00	13.00	7.00	4.92	11.92

Modulation mode	30 MHz (Tx/Rx/Aggregate)			20 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	112.00	37.00	149.00	74.00	25.00	99.00
64QAM 0.92 dual	95.00	32.00	127.00	62.00	21.00	83.00
64QAM 0.75 dual	77.00	26.00	103.00	51.00	17.00	68.00
16QAM 0.87 dual	60.00	20.00	80.00	40.00	13.00	53.00
16QAM 0.63 dual	43.00	14.00	57.00	29.00	9.00	38.00
256QAM 0.81 single	56.00	19.00	75.00	37.00	12.00	49.00
64QAM 0.92 single	47.00	16.00	63.00	31.00	10.00	41.00
64QAM 0.75 single	39.00	13.00	52.00	25.00	8.00	33.00
16QAM 0.87 single	30.00	10.00	40.00	20.00	7.00	27.00
16QAM 0.63 single	22.00	7.00	29.00	14.00	5.00	19.00
QPSK 0.87 single	15.00	5.00	20.00	10.00	5.00	15.00
QPSK 0.63 single	11.00	5.00	16.00	7.00	4.75	11.75
BPSK 0.63 single	5.00	3.60	8.60	5.00	2.37	7.37

Modulation mode	15 MHz (Tx/Rx/Aggregate)			10 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	56.00	19.00	75.00	37.00	12.00	49.00
64QAM 0.92 dual	47.00	16.00	63.00	32.00	11.00	43.00
64QAM 0.75 dual	38.00	13.00	51.00	26.00	9.00	35.00
16QAM 0.87 dual	30.00	10.00	40.00	20.00	7.00	27.00
16QAM 0.63 dual	22.00	7.00	29.00	14.00	5.00	19.00
256QAM 0.81 single	28.00	9.00	37.00	19.00	6.00	25.00
64QAM 0.92 single	24.00	8.00	32.00	16.00	5.00	21.00
64QAM 0.75 single	19.00	6.00	25.00	13.00	5.00	18.00
16QAM 0.87 single	15.00	5.00	20.00	10.00	5.00	15.00
16QAM 0.63 single	11.00	5.00	16.00	7.00	4.81	11.81
QPSK 0.87 single	7.00	4.99	11.99	5.00	3.34	8.34
QPSK 0.63 single	5.00	3.58	8.58	5.00	2.40	7.40
BPSK 0.63 single	5.00	1.79	6.79	3.61	1.20	4.81

Table 113 Throughput at zero link range (Mbit/s), Lite, symmetry 5:1, optimization IP

Modulation mode	45 MHz (Tx/Rx/Aggregate)			40 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	187.00	37.00	224.00	167.00	33.00	200.00
64QAM 0.92 dual	157.00	31.00	188.00	141.00	28.00	169.00
64QAM 0.75 dual	129.00	26.00	155.00	115.00	23.00	138.00
16QAM 0.87 dual	100.00	20.00	120.00	89.00	18.00	107.00
16QAM 0.63 dual	72.00	14.00	86.00	64.00	13.00	77.00
256QAM 0.81 single	93.00	19.00	112.00	83.00	17.00	100.00
64QAM 0.92 single	79.00	16.00	95.00	70.00	14.00	84.00
64QAM 0.75 single	64.00	13.00	77.00	57.00	11.00	68.00
16QAM 0.87 single	50.00	10.00	60.00	45.00	9.00	54.00
16QAM 0.63 single	36.00	7.00	43.00	32.00	6.00	38.00
QPSK 0.87 single	25.00	5.00	30.00	22.00	5.00	27.00
QPSK 0.63 single	18.00	5.00	23.00	16.00	5.00	21.00
BPSK 0.63 single	9.00	3.59	12.59	8.00	3.21	11.21

Modulation mode	30 MHz (Tx/Rx/Aggregate)		
256QAM 0.81 dual	124.00	25.00	149.00
64QAM 0.92 dual	104.00	21.00	125.00
64QAM 0.75 dual	85.00	17.00	102.00
16QAM 0.87 dual	66.00	13.00	79.00
16QAM 0.63 dual	48.00	10.00	58.00
256QAM 0.81 single	62.00	12.00	74.00
64QAM 0.92 single	52.00	10.00	62.00
64QAM 0.75 single	43.00	9.00	52.00
16QAM 0.87 single	33.00	7.00	40.00
16QAM 0.63 single	24.00	5.00	29.00
QPSK 0.87 single	17.00	5.00	22.00
QPSK 0.63 single	12.00	4.76	16.76
BPSK 0.63 single	6.00	2.38	8.38

Figure 67 Range adjustment for PTP 700, symmetry 1:1, optimization IP, bandwidth 45 MHz

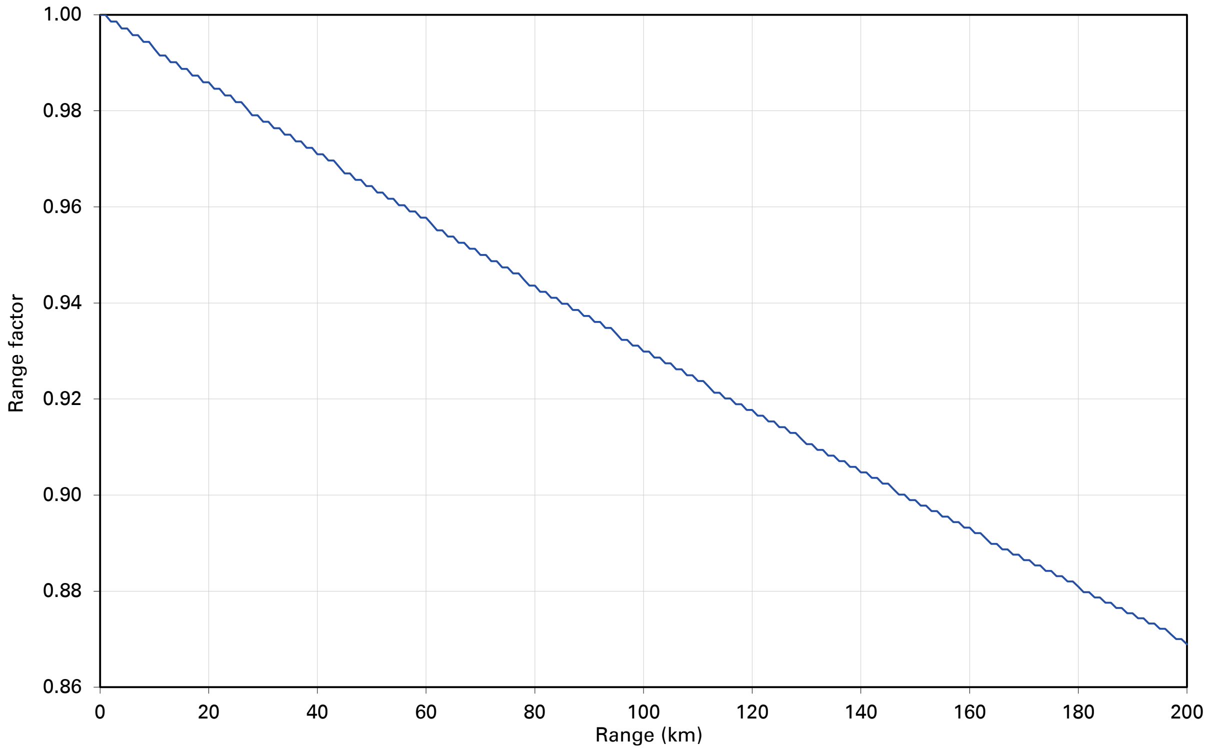


Figure 68 Range adjustment for PTP 700, symmetry 1:1, optimization IP, bandwidth 40 MHz

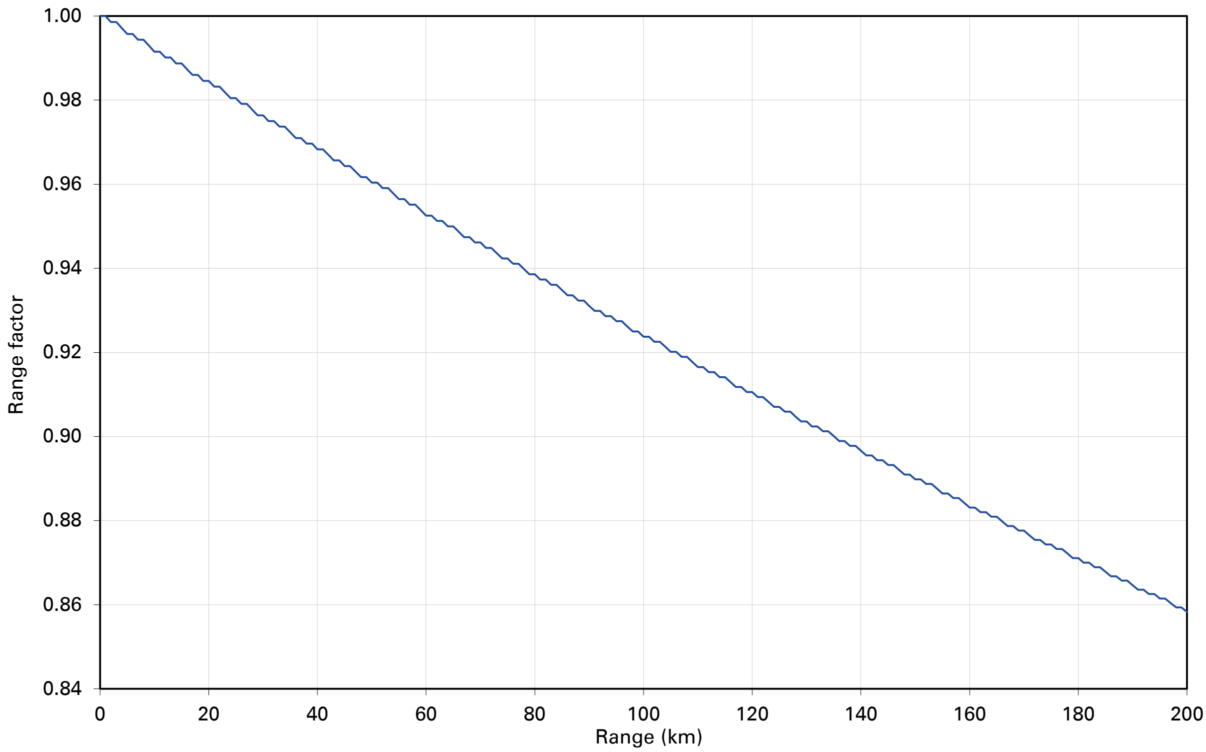


Figure 69 Range adjustment for PTP 700, symmetry 1:1, optimization IP, bandwidth 30 MHz

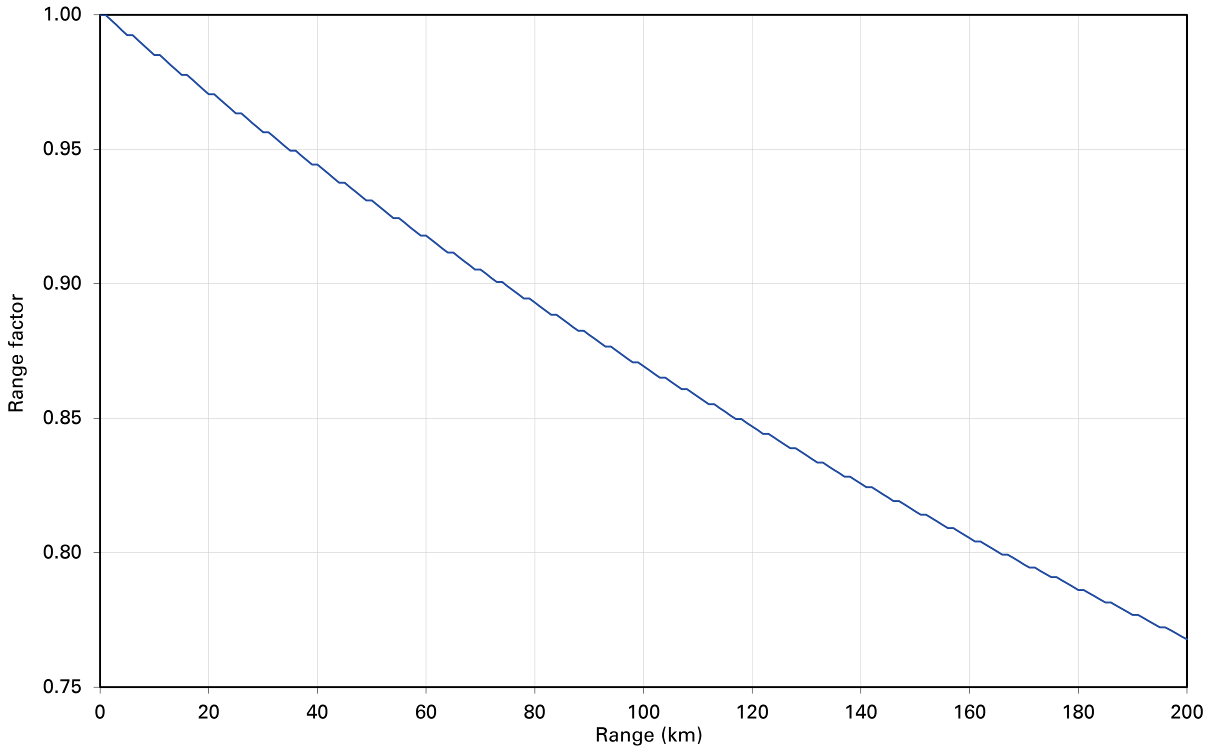


Figure 70 Range adjustment for PTP 700, symmetry 1:1, optimization IP, bandwidth 20 MHz

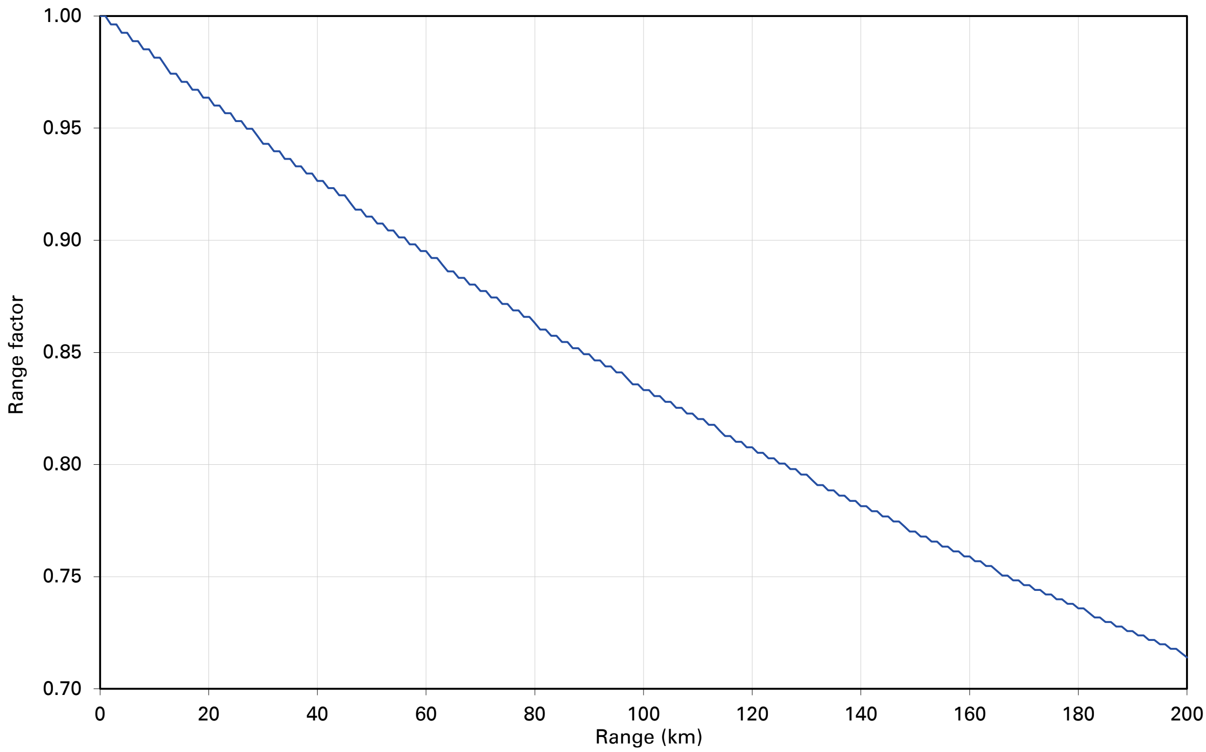


Figure 71 Range adjustment for PTP 700, symmetry 1:1, optimization IP, bandwidth 15 MHz

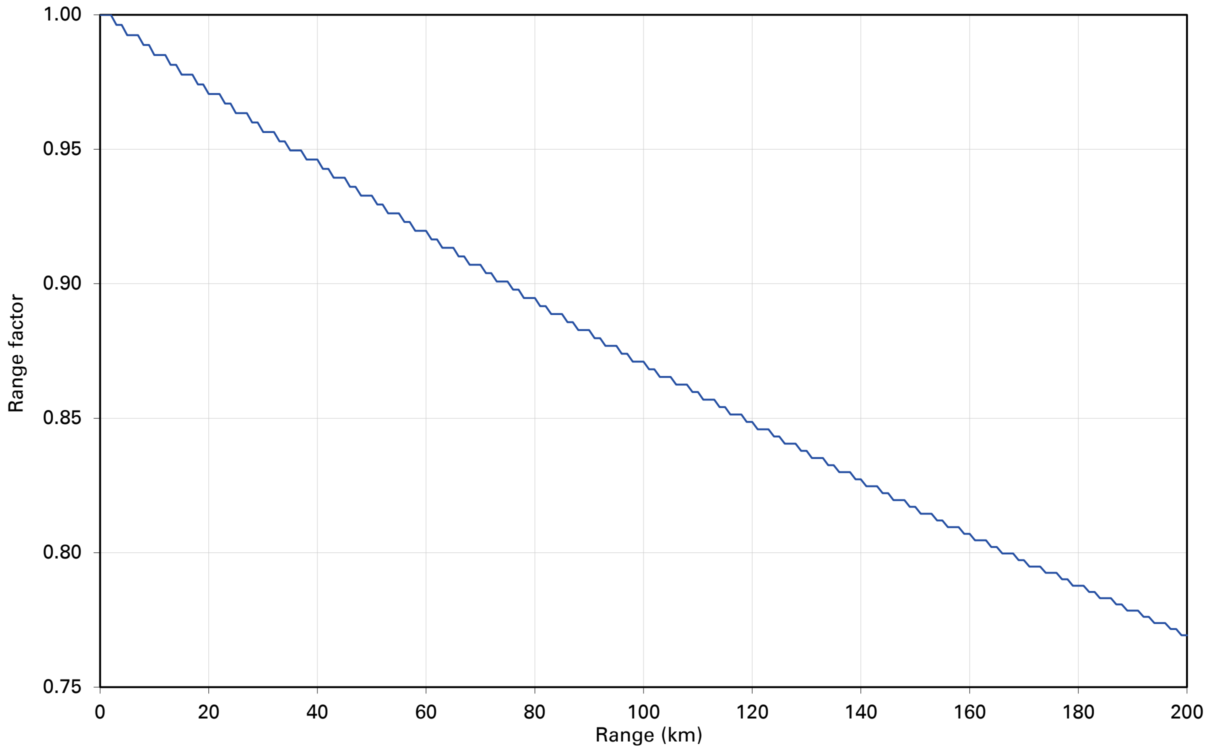


Figure 72 Range adjustment for PTP 700, symmetry 1:1, optimization IP, bandwidth 10 MHz

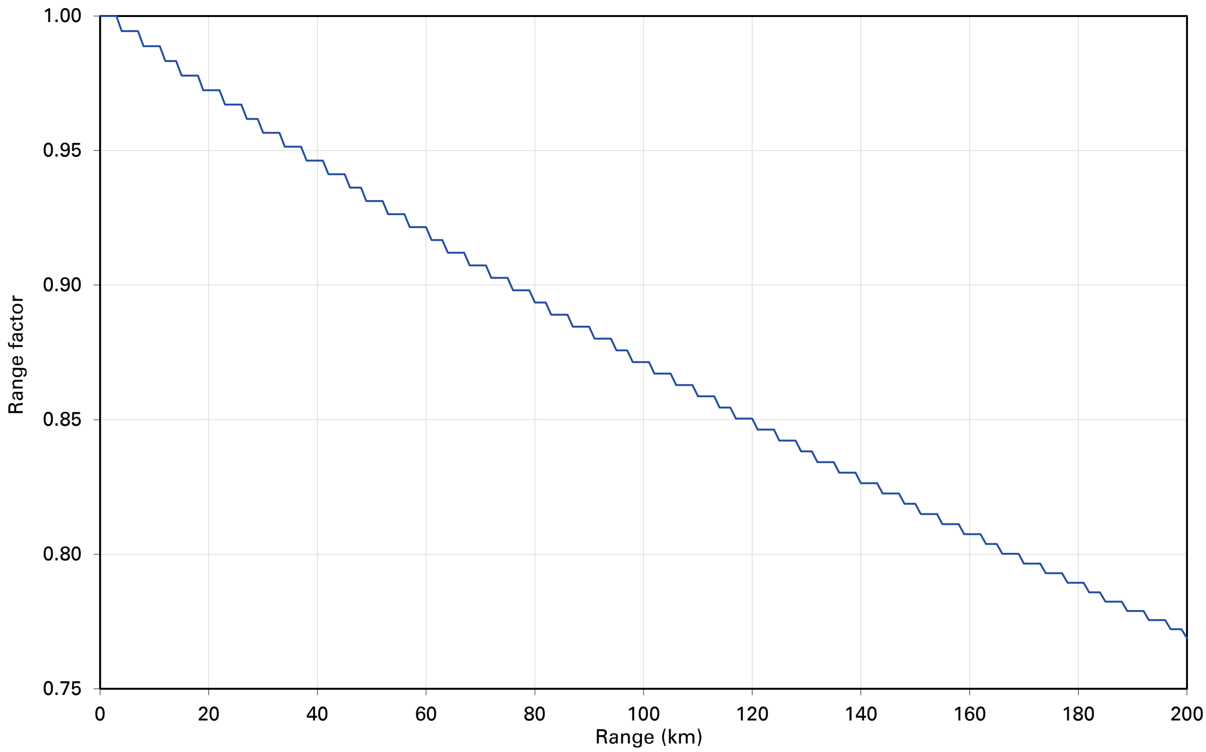


Figure 73 Range adjustment for PTP 700, symmetry 1:1, optimization IP, bandwidth 5 MHz

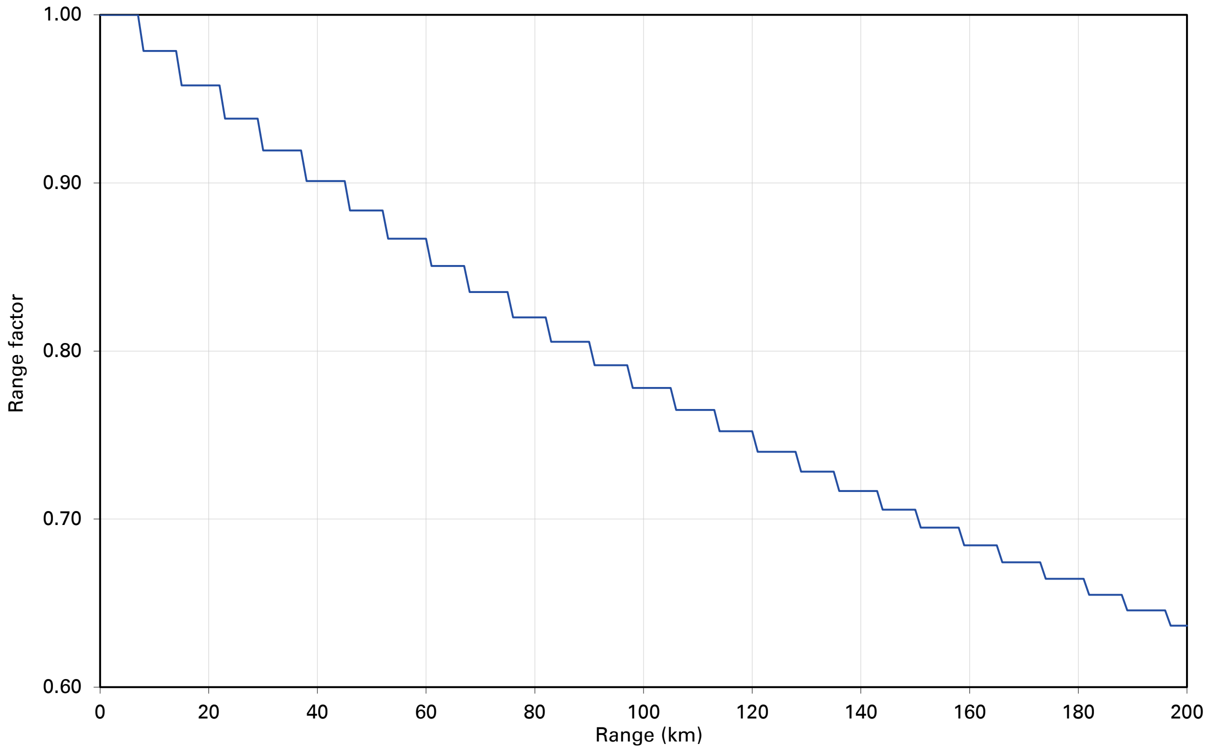


Figure 74 Range adjustment for PTP 700, symmetry 1:1, optimization TDM, bandwidth 45 MHz

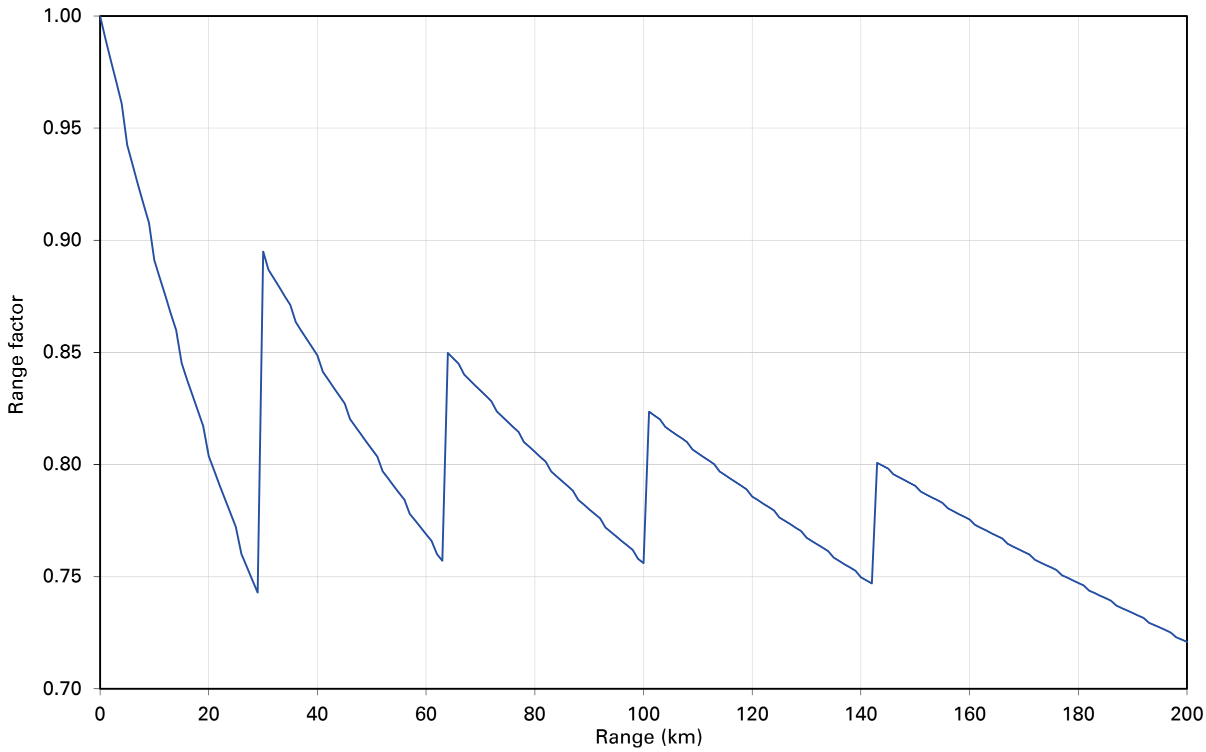


Figure 75 Range adjustment for PTP 700, symmetry 1:1, optimization TDM, bandwidth 40 MHz

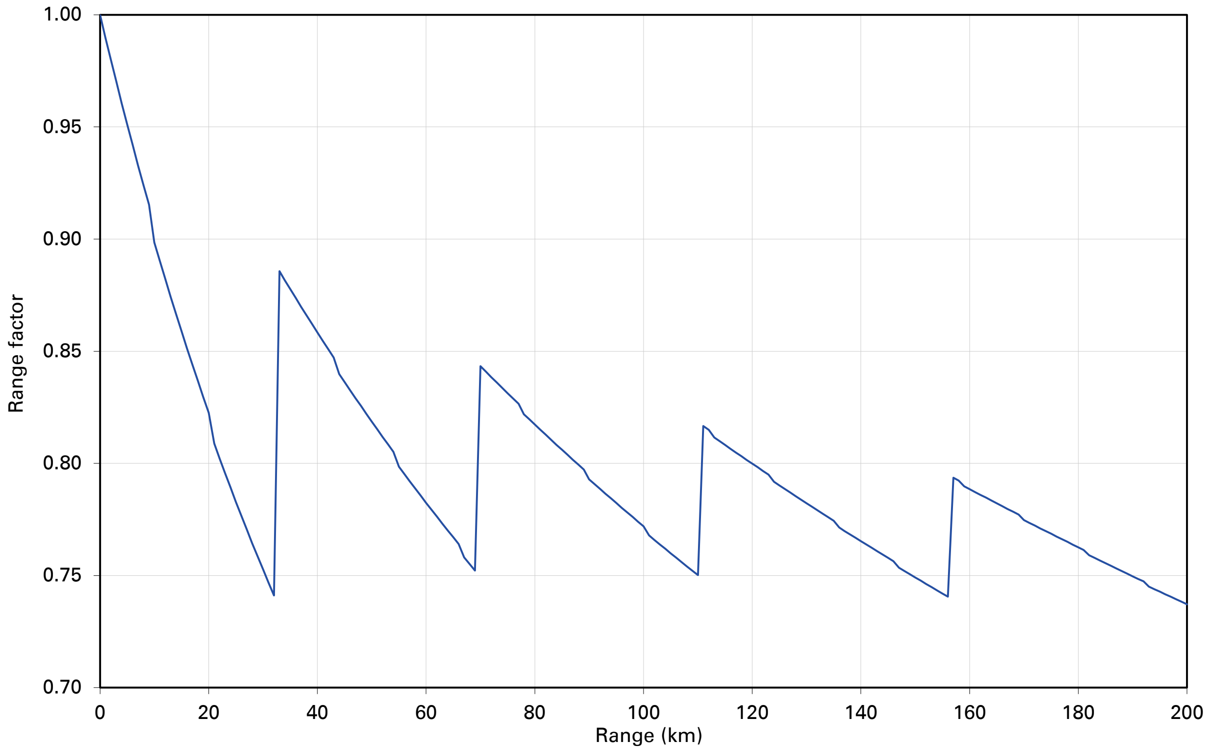


Figure 76 Range adjustment for PTP 700, symmetry 1:1, optimization TDM, bandwidth 30 MHz

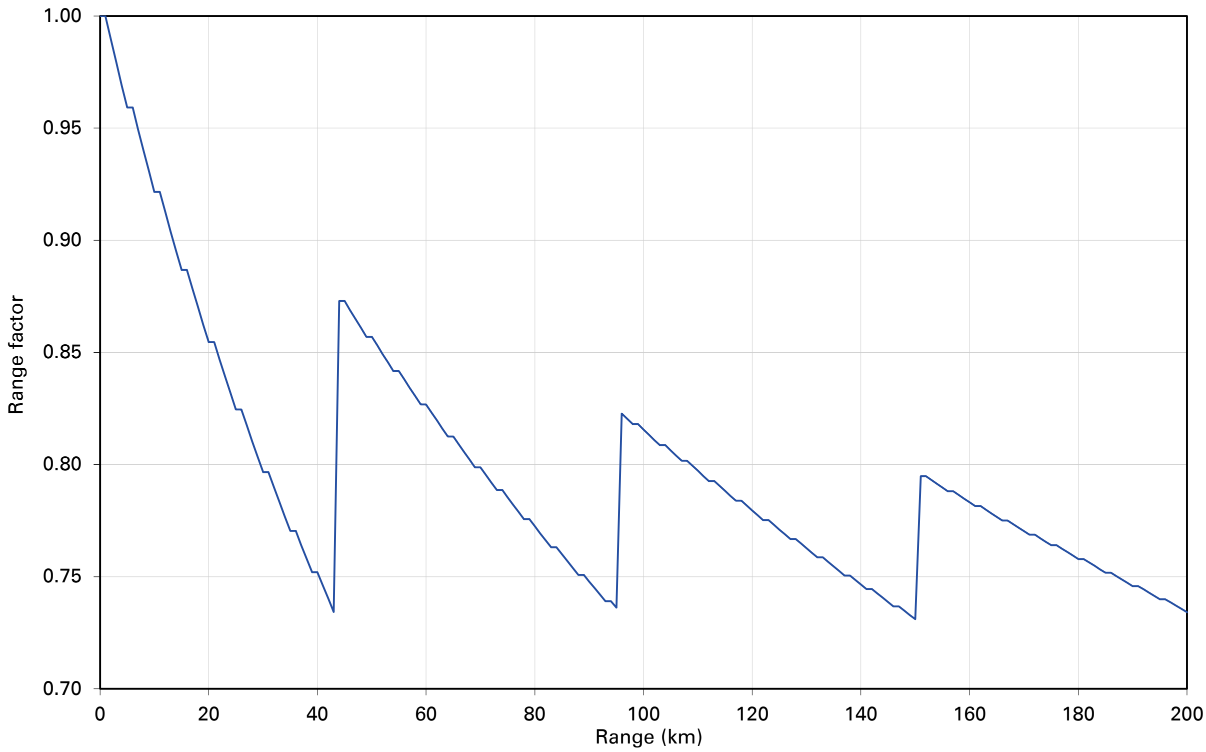


Figure 77 Range adjustment for PTP 700, symmetry 1:1, optimization TDM, bandwidth 20 MHz

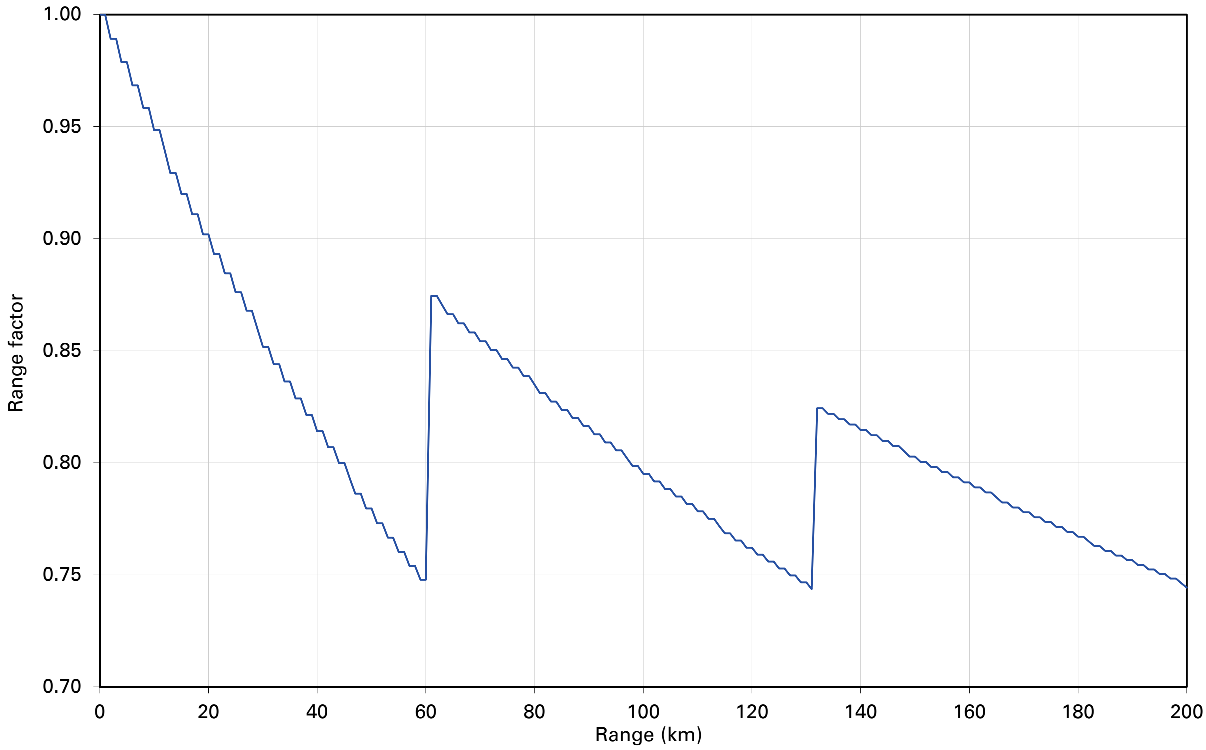


Figure 78 Range adjustment for PTP 700, symmetry 1:1, optimization TDM, bandwidth 15 MHz

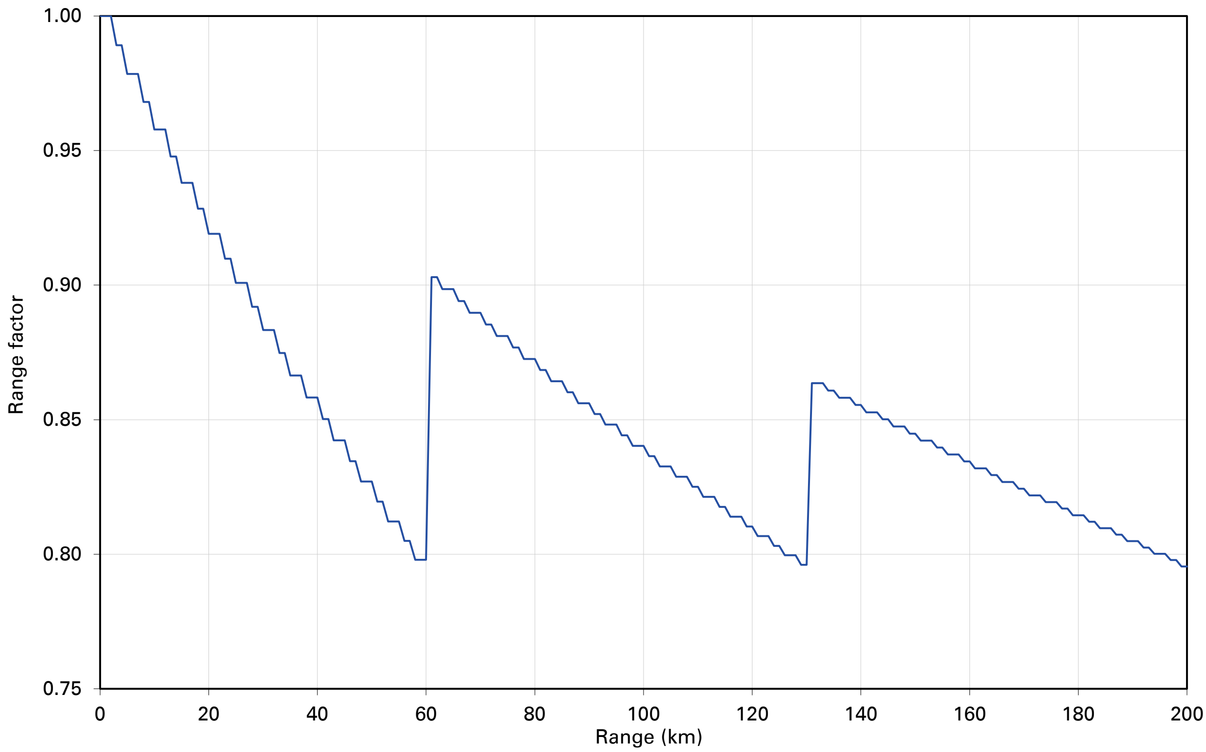


Figure 79 Range adjustment for PTP 700, symmetry 1:1, optimization TDM, bandwidth 10 MHz

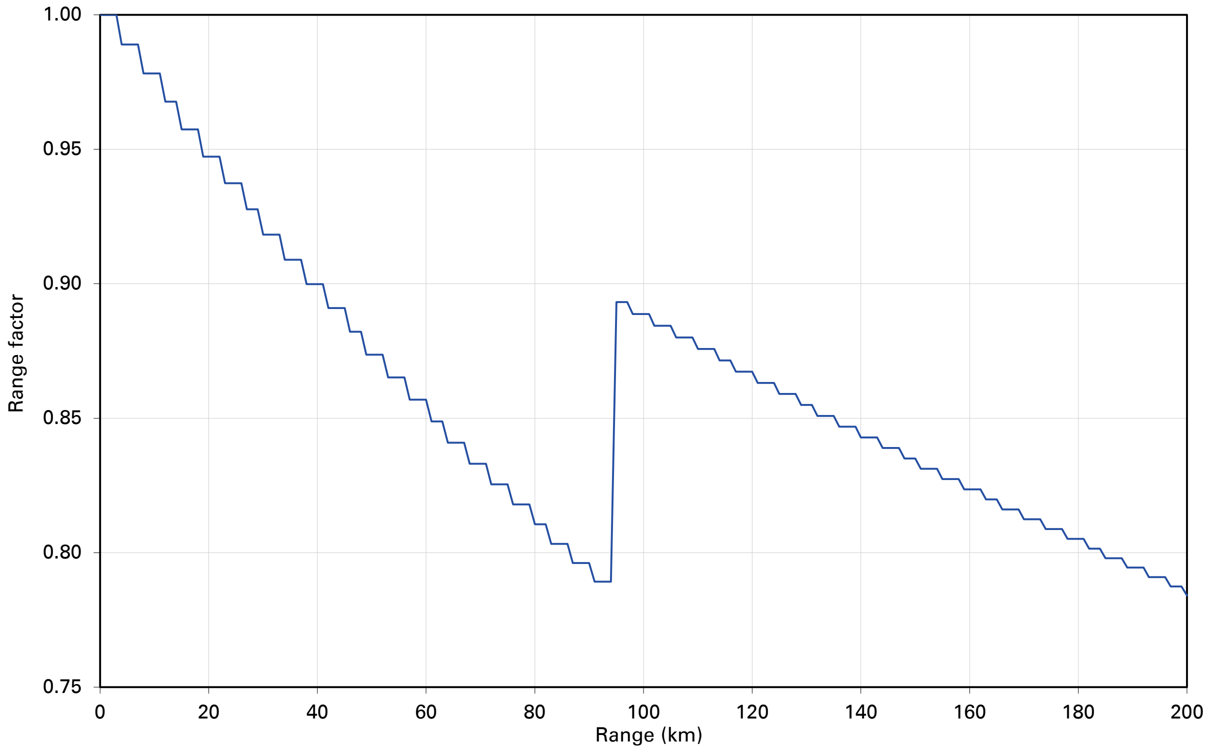


Figure 80 Range adjustment for PTP 700, symmetry 1:1, optimization TDM, bandwidth 5 MHz

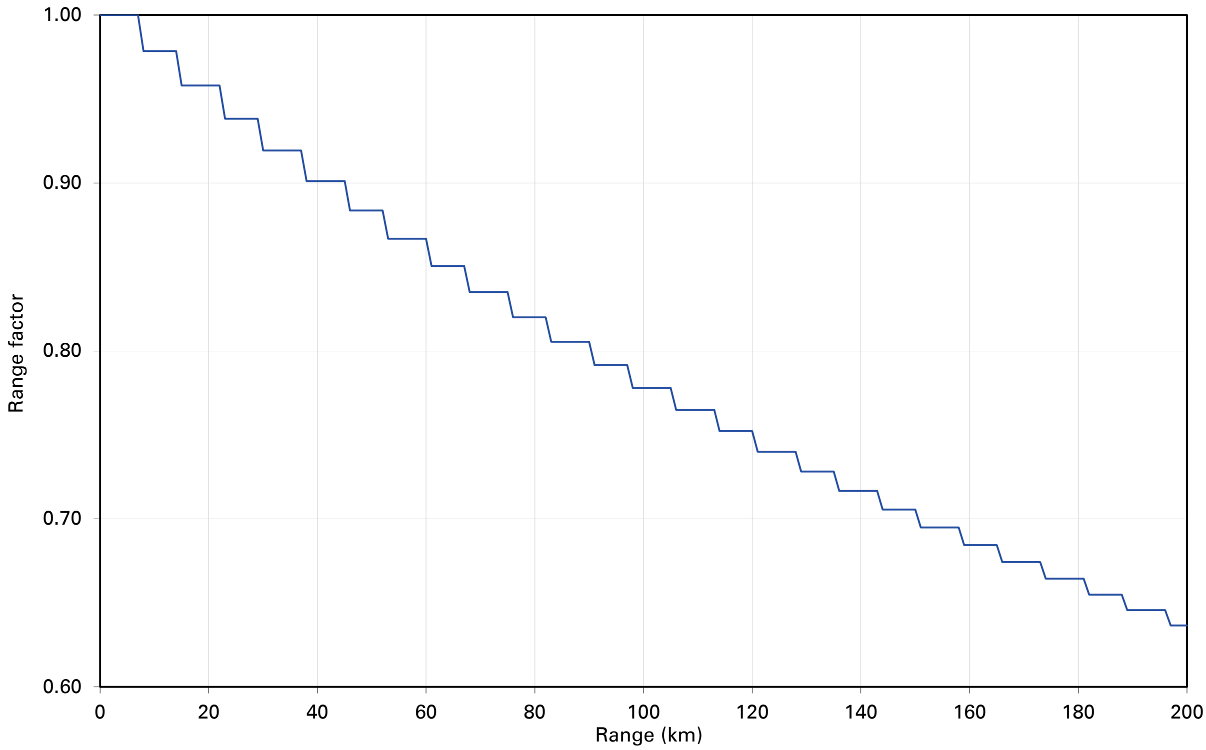


Figure 81 Range adjustment for PTP 700, symmetry 2:1, optimization IP, bandwidth 45 MHz

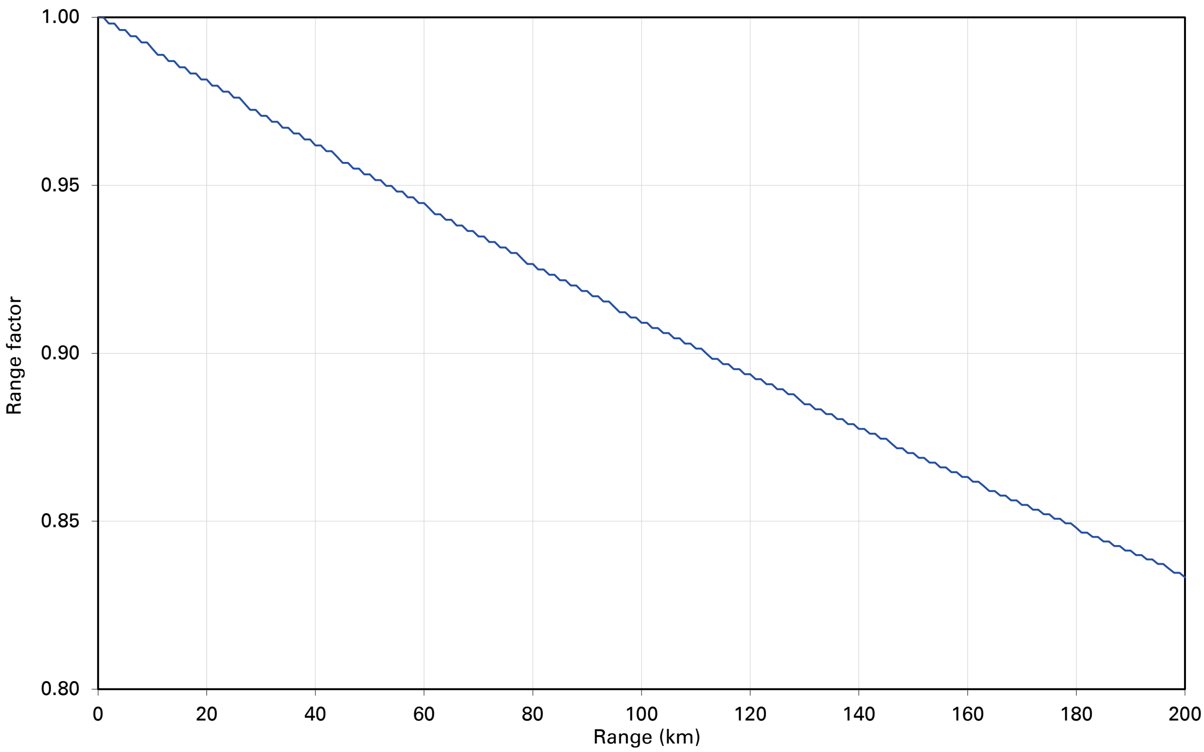


Figure 82 Range adjustment for PTP 700, symmetry 2:1, optimization IP, bandwidth 40 MHz

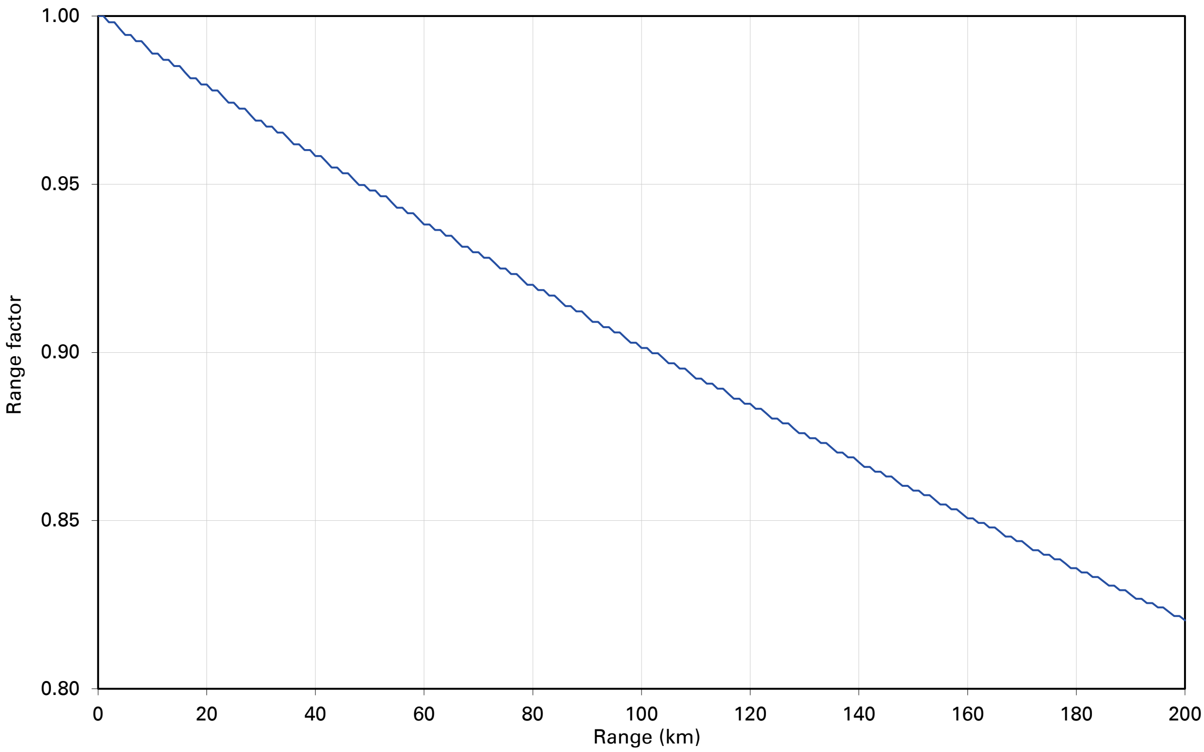


Figure 83 Range adjustment for PTP 700, symmetry 2:1, optimization IP, bandwidth 30 MHz

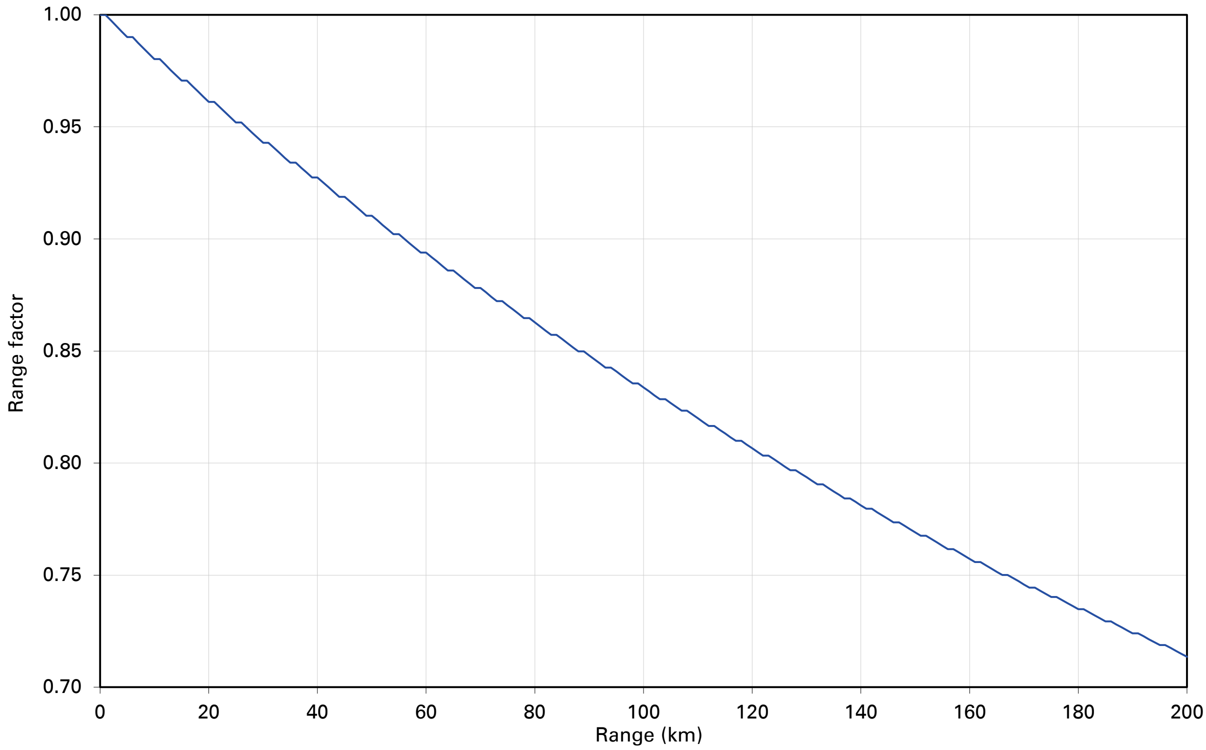


Figure 84 Range adjustment for PTP 700, symmetry 2:1, optimization IP, bandwidth 20 MHz

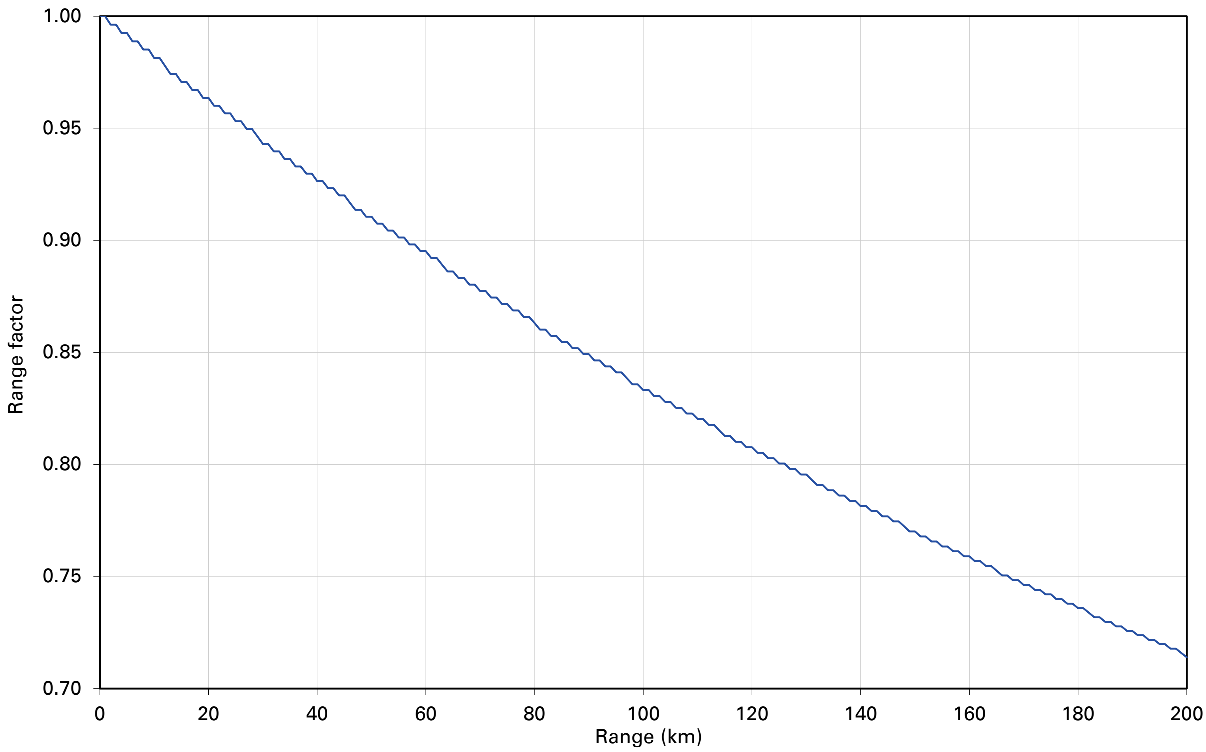


Figure 85 Range adjustment for PTP 700, symmetry 2:1, optimization IP, bandwidth 15 MHz

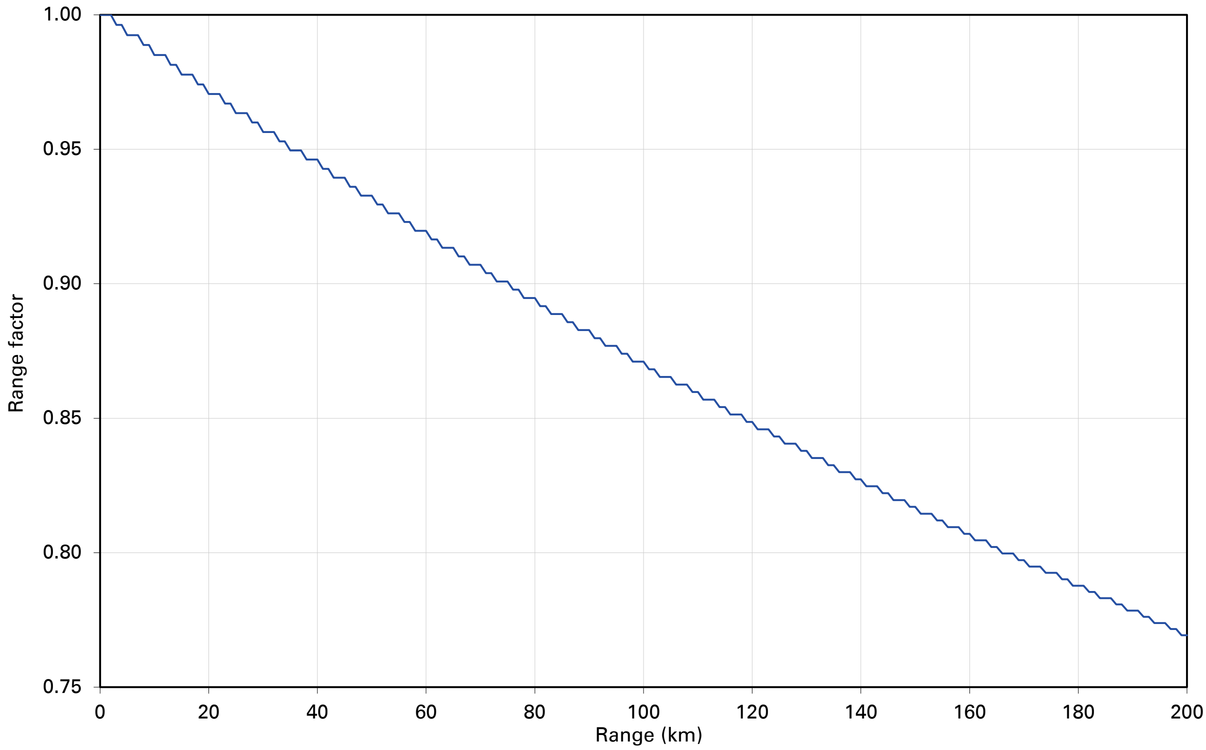


Figure 86 Range adjustment for PTP 700, symmetry 2:1, optimization IP, bandwidth 10 MHz

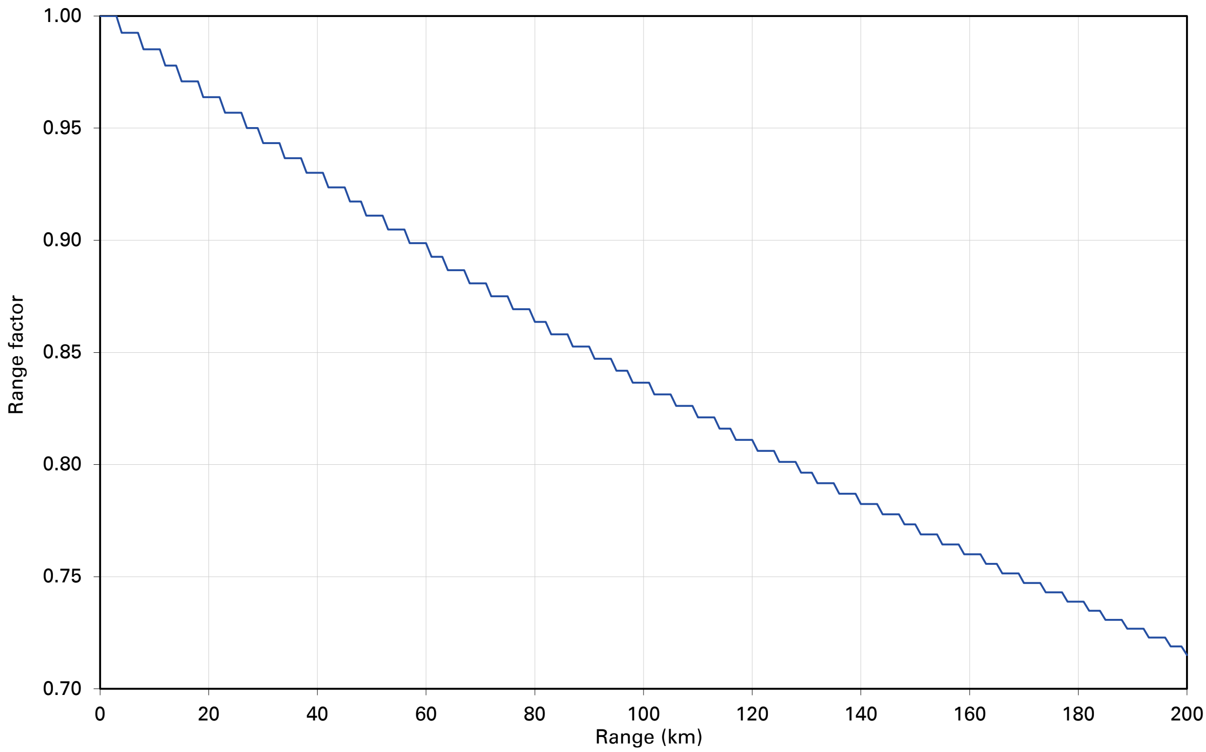


Figure 87 Range adjustment for PTP 700, symmetry 2:1, optimization TDM, bandwidth 45 MHz

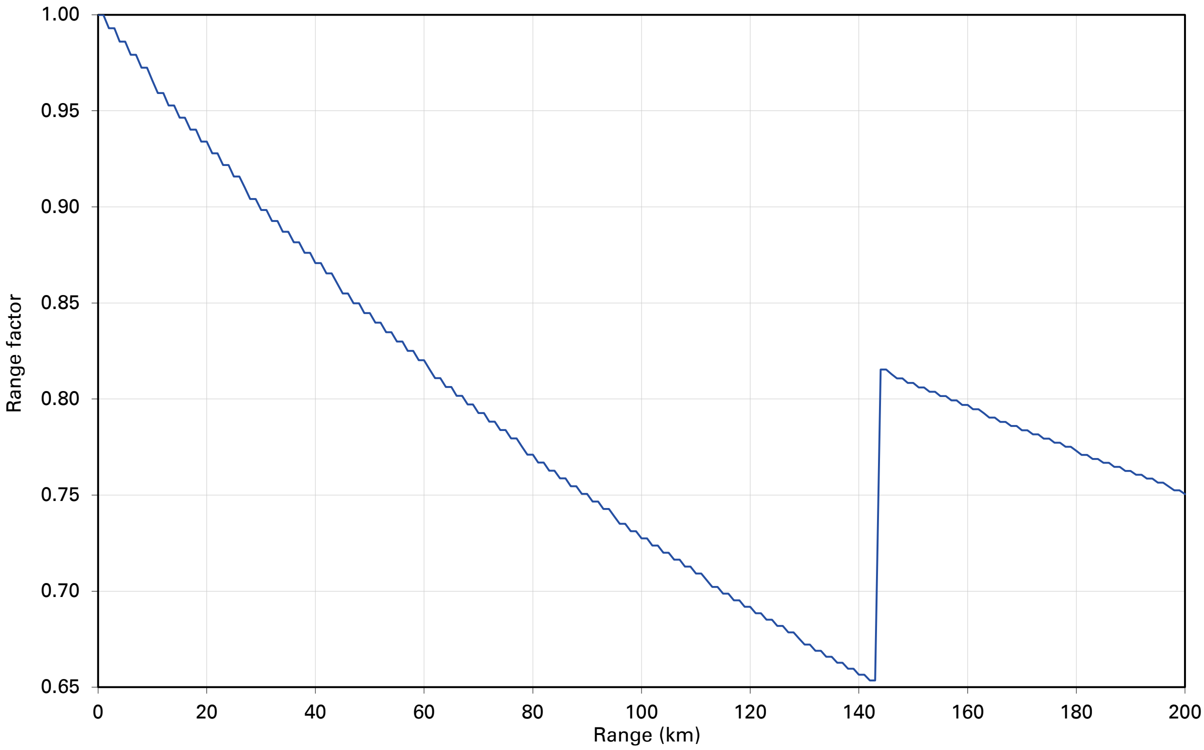


Figure 88 Range adjustment for PTP 700, symmetry 2:1, optimization TDM, bandwidth 40 MHz

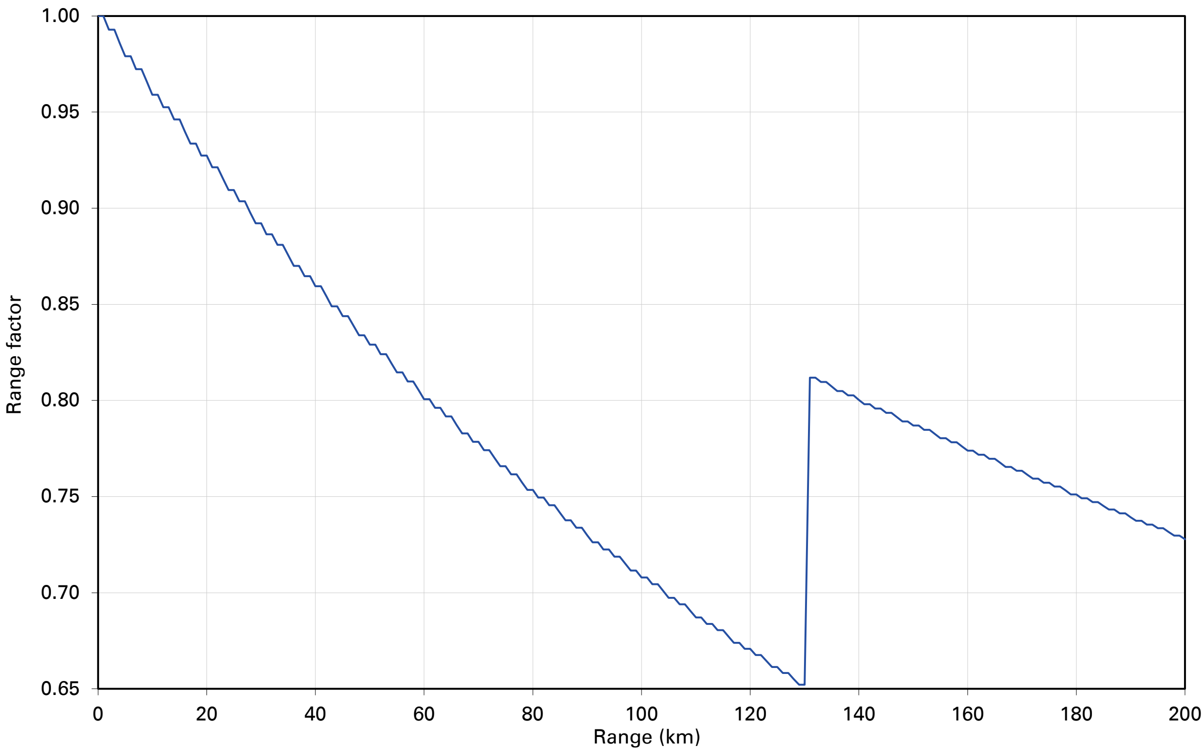


Figure 89 Range adjustment for PTP 700, symmetry 2:1, optimization TDM, bandwidth 30 MHz

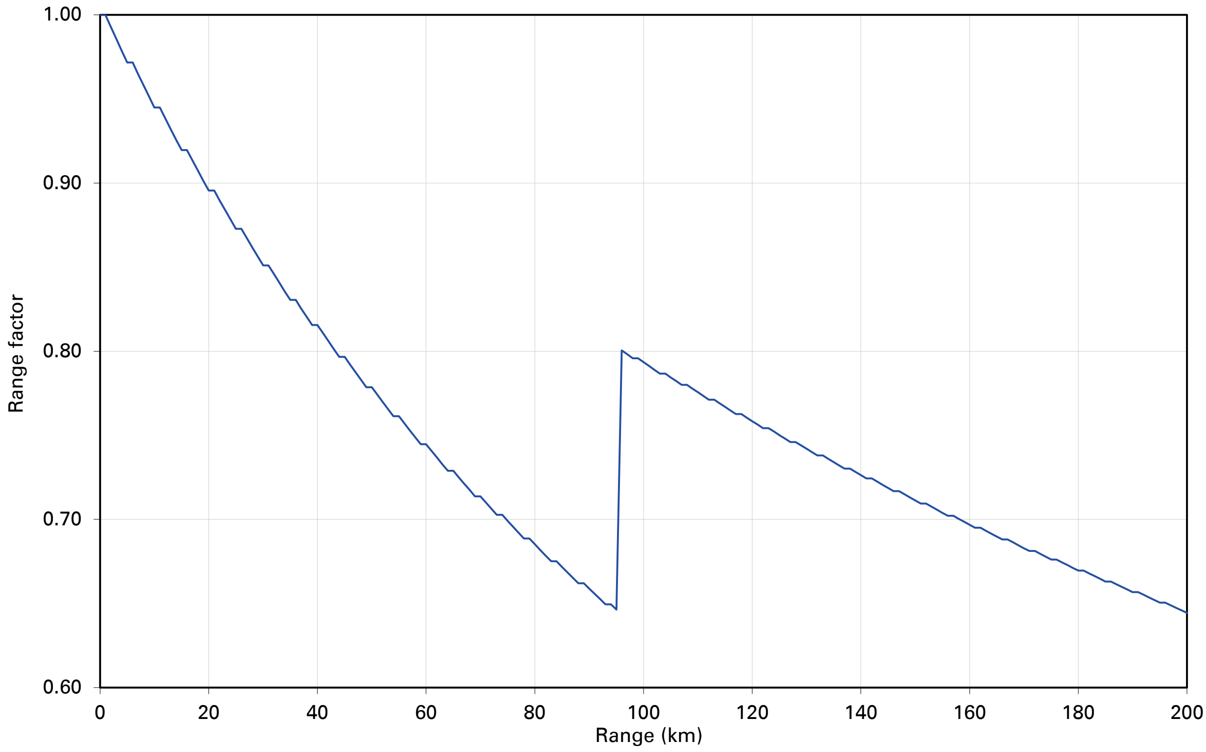


Figure 90 Range adjustment for PTP 700, symmetry 2:1, optimization TDM, bandwidth 20 MHz

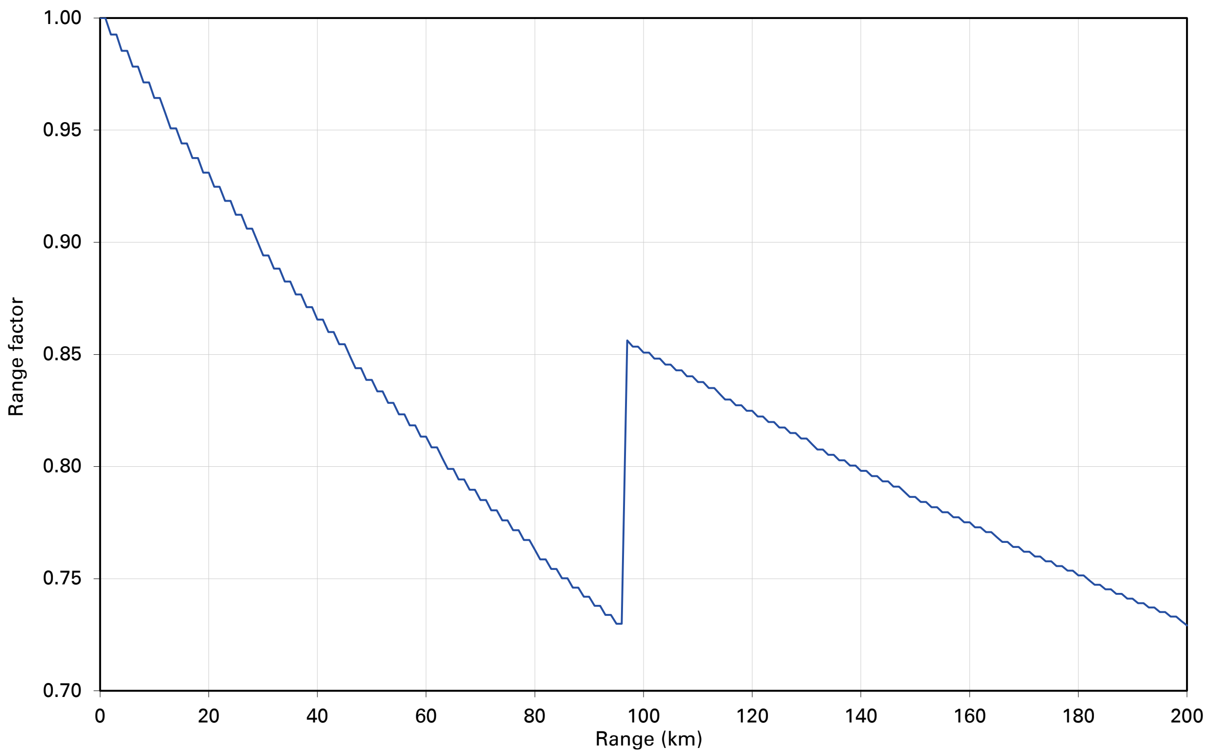


Figure 91 Range adjustment for PTP 700, symmetry 2:1, optimization TDM, bandwidth 15 MHz

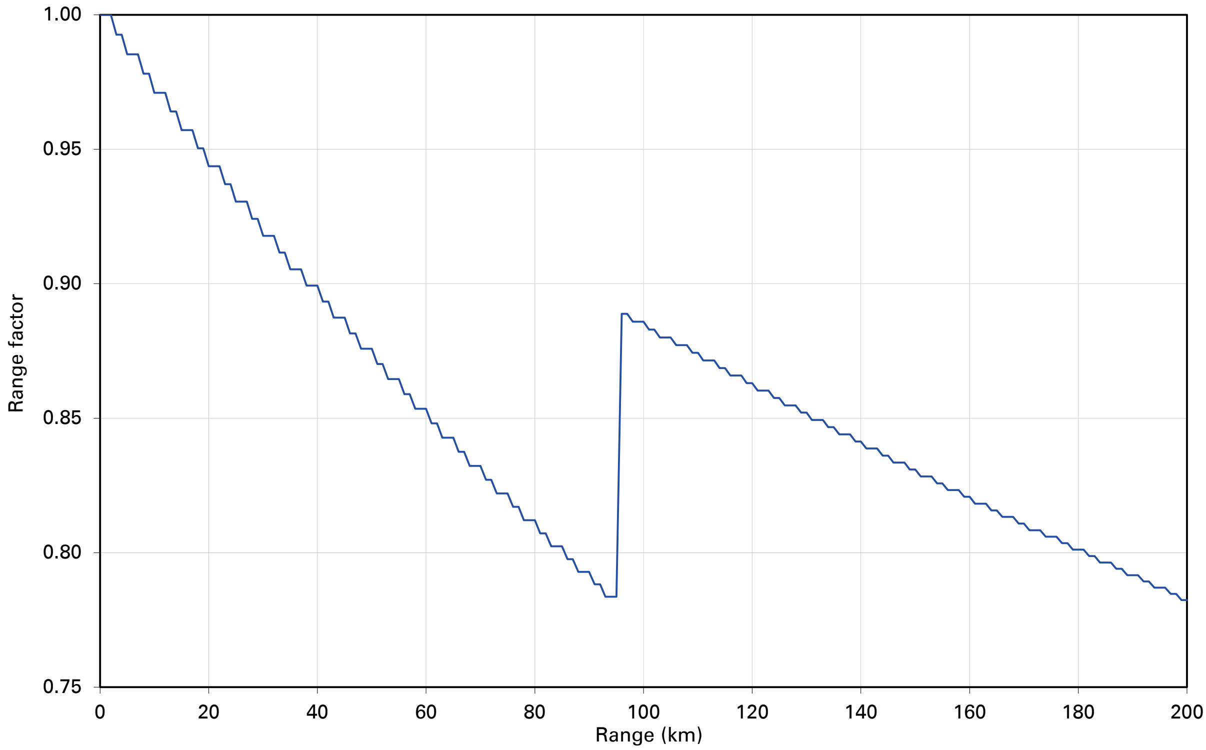


Figure 92 Range adjustment for PTP 700, symmetry 2:1, optimization TDM, bandwidth 10 MHz

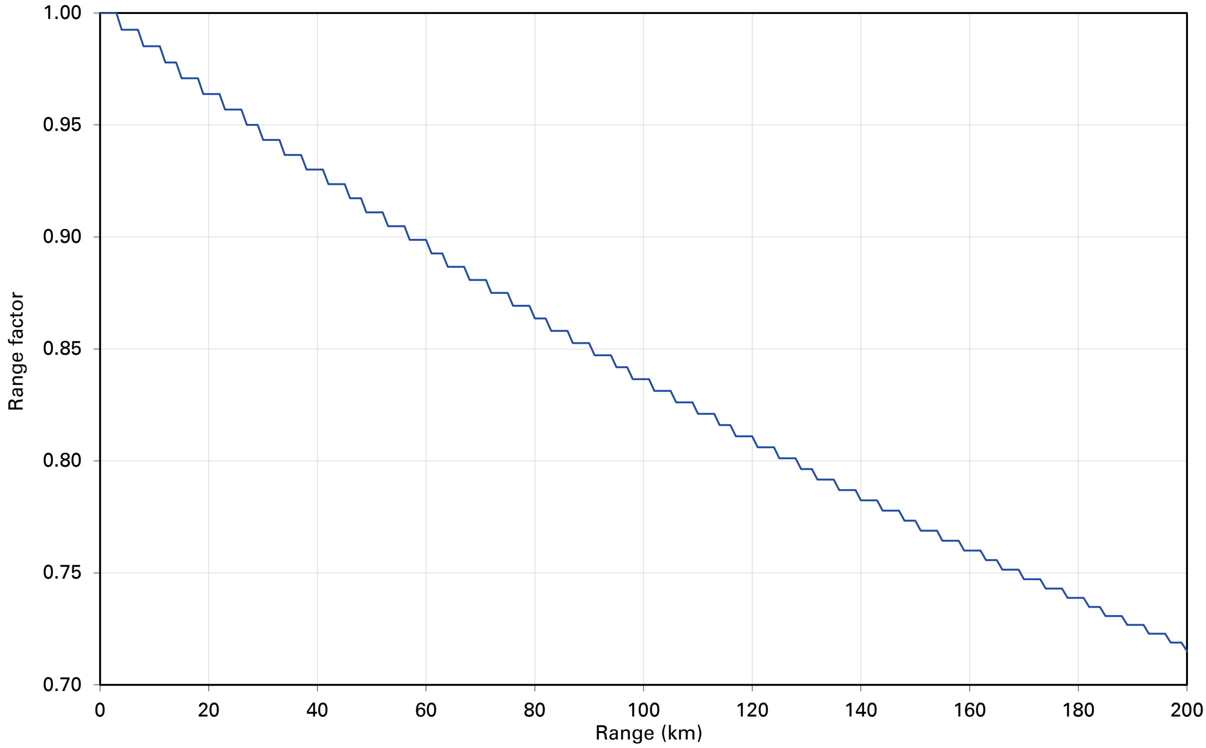


Figure 93 Range adjustment for PTP 700, symmetry 3:1, optimization IP, bandwidth 45 MHz

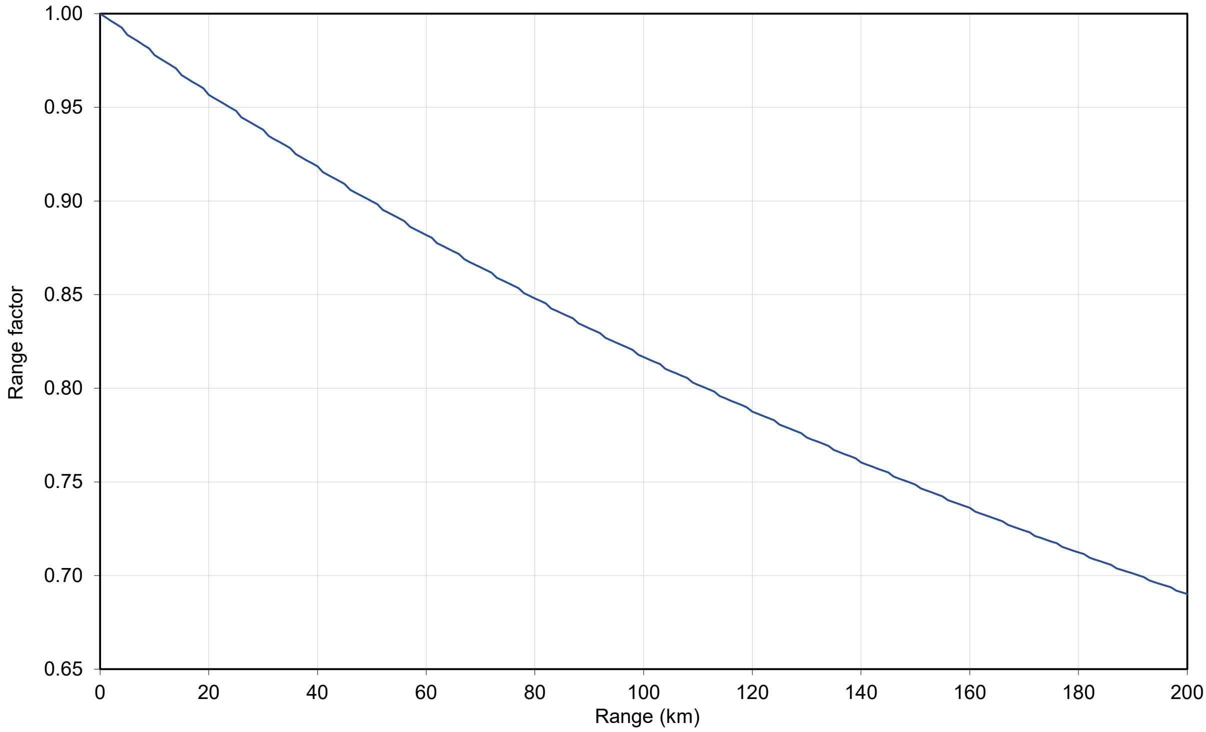


Figure 94 Range adjustment for PTP 700, symmetry 3:1, optimization IP, bandwidth 40 MHz

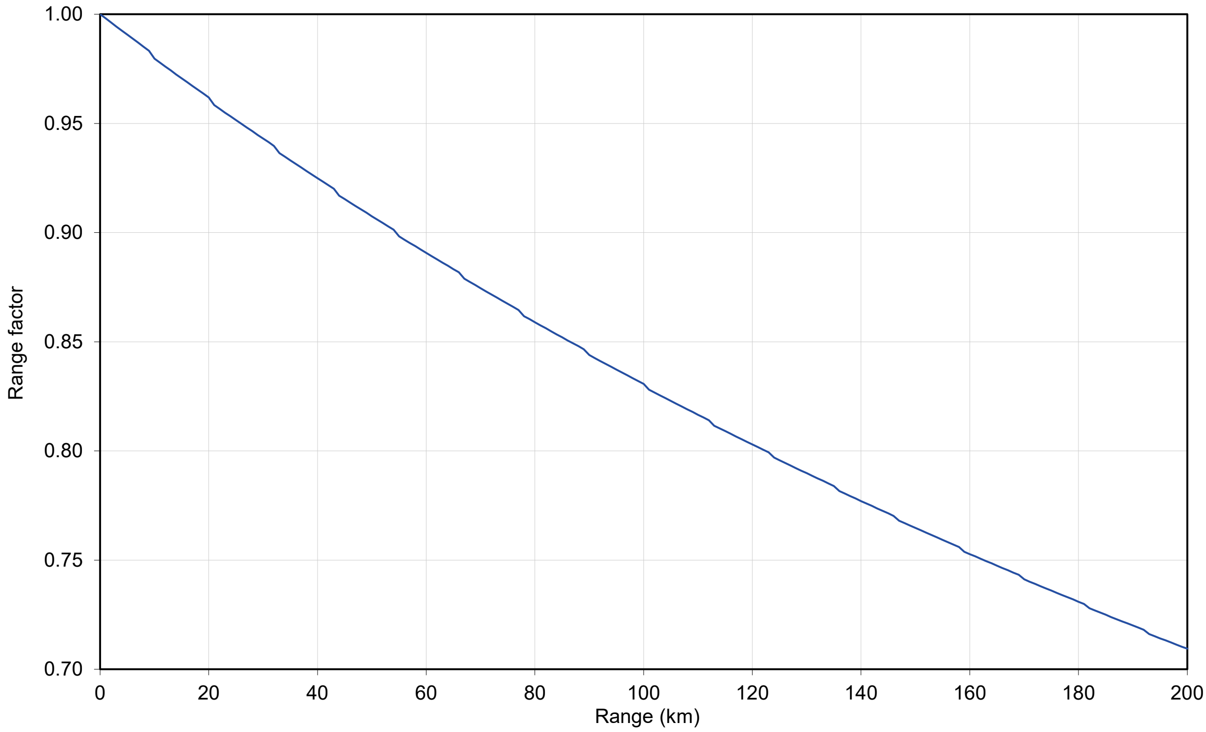


Figure 95 Range adjustment for PTP 700, symmetry 3:1, optimization IP, bandwidth 30 MHz

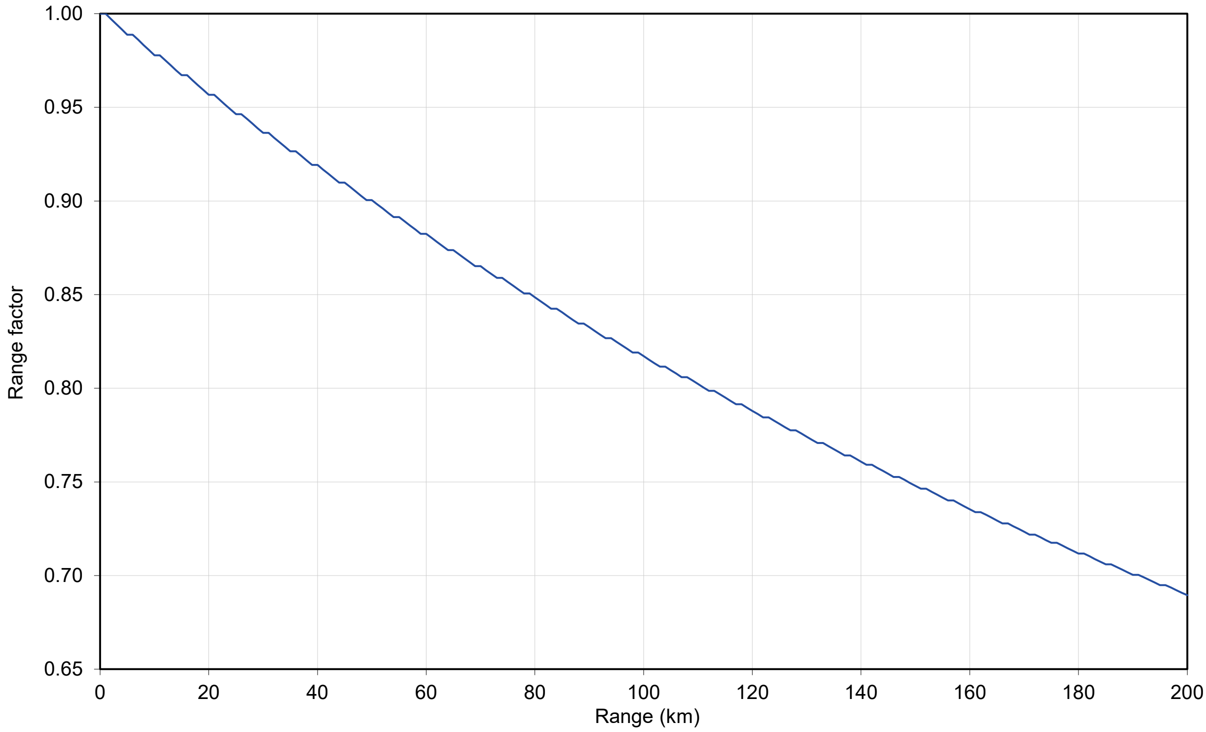


Figure 96 Range adjustment for PTP 700, symmetry 3:1, optimization IP, bandwidth 20 MHz

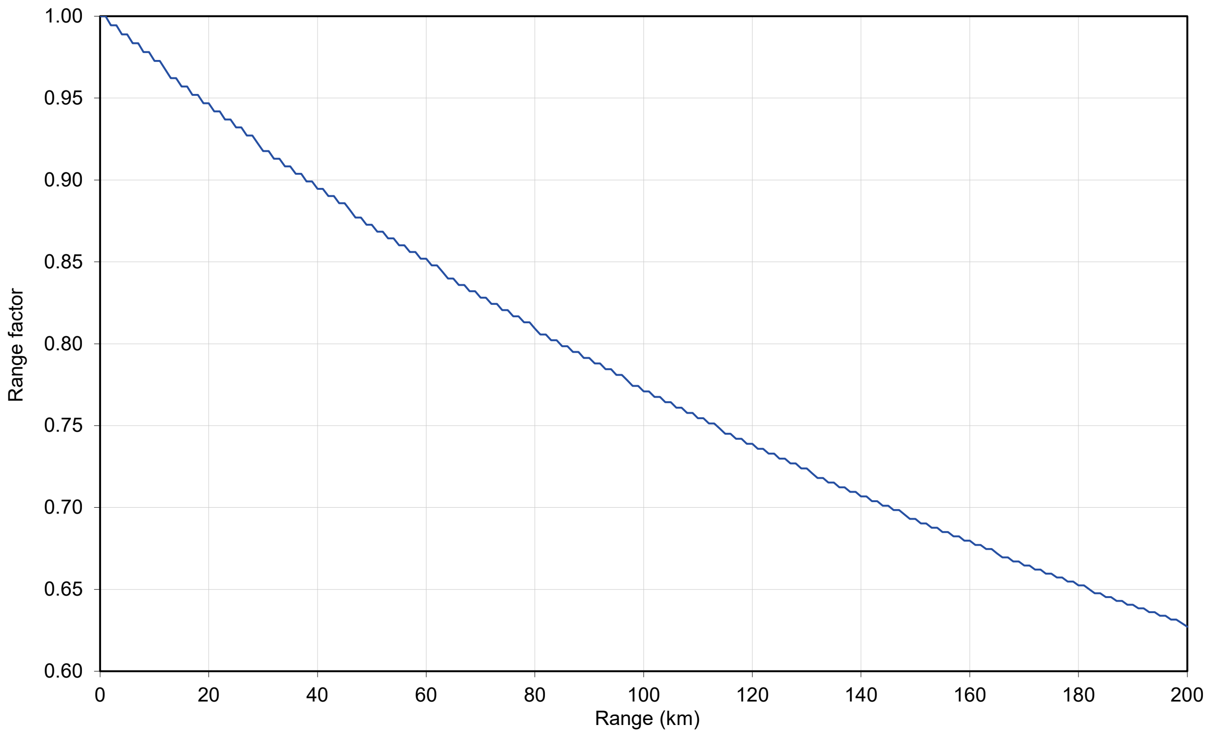


Figure 97 Range adjustment for PTP 700, symmetry 3:1, optimization IP, bandwidth 15 MHz

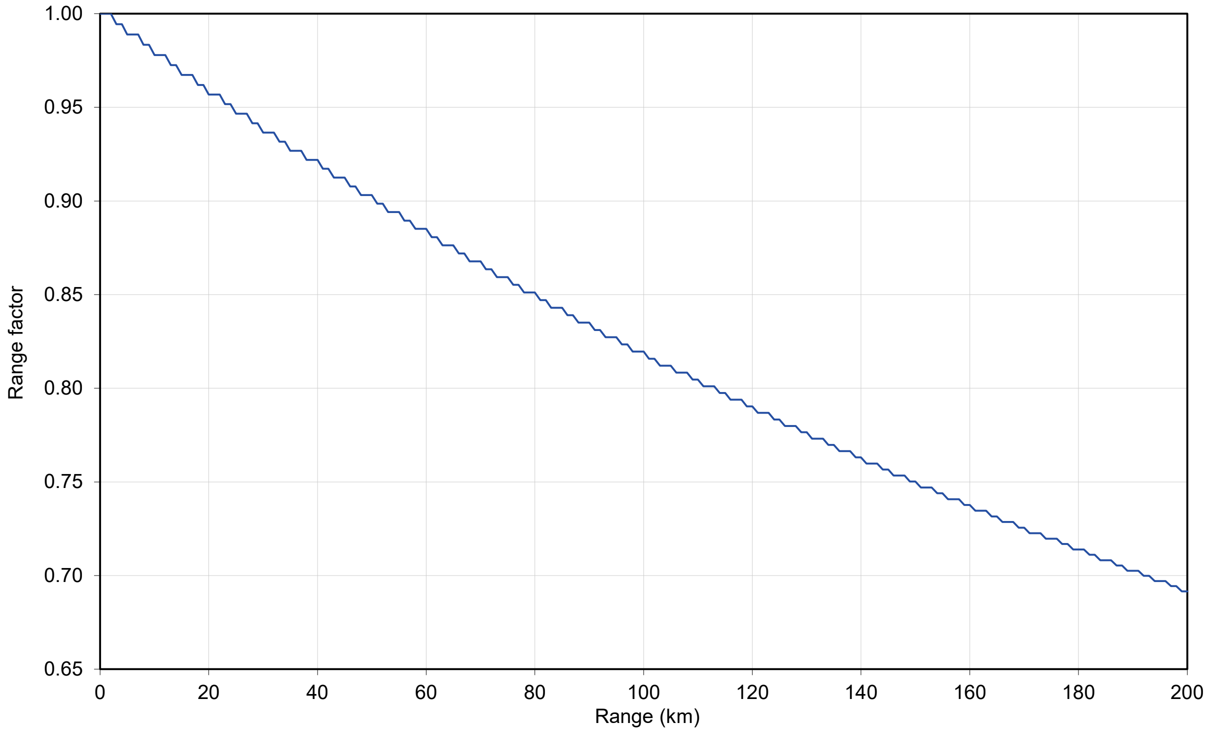


Figure 98 Range adjustment for PTP 700, symmetry 3:1, optimization IP, bandwidth 10 MHz

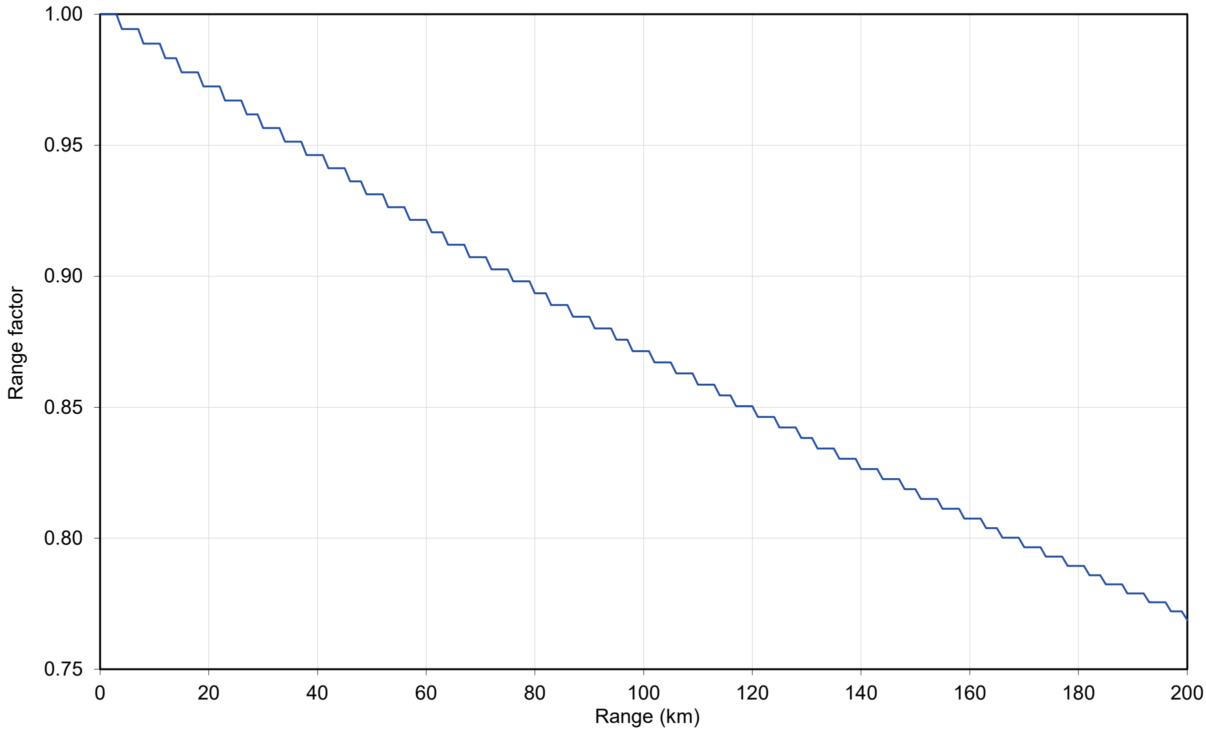


Figure 99 Range adjustment for PTP 700, symmetry 5:1, optimization IP, bandwidth 45 MHz

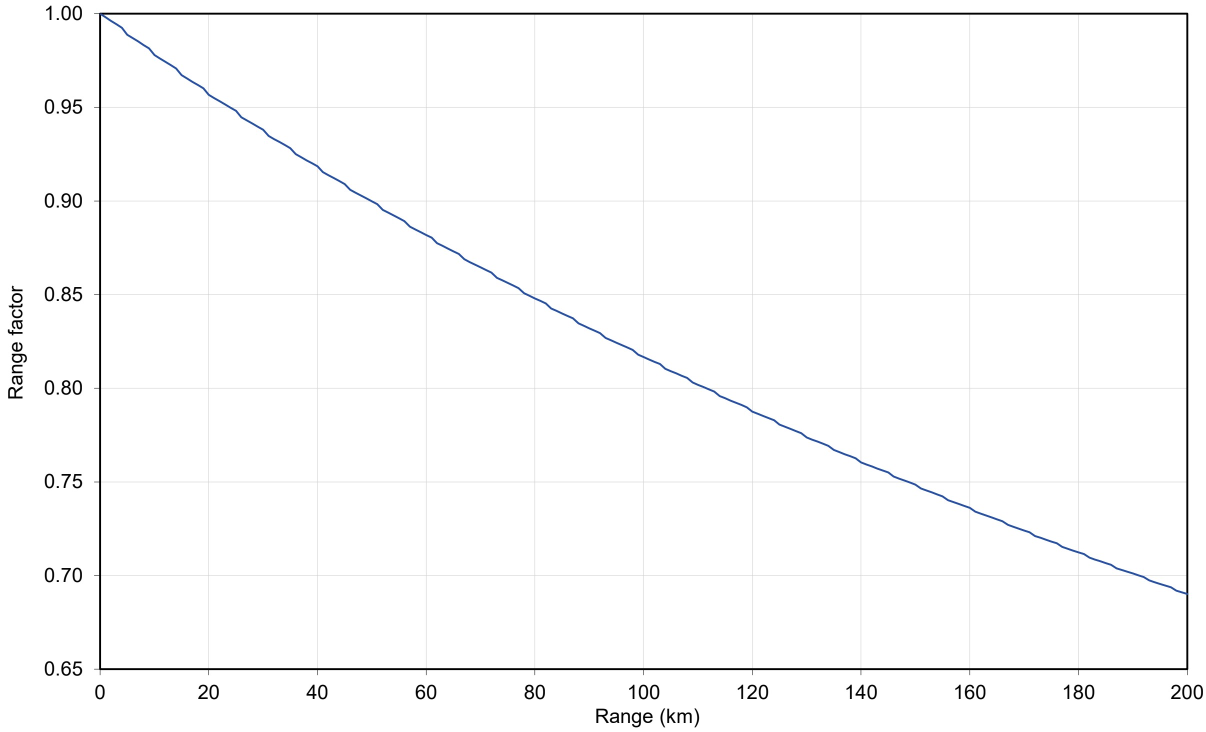


Figure 100 Range adjustment for PTP 700, symmetry 5:1, optimization IP, bandwidth 40 MHz

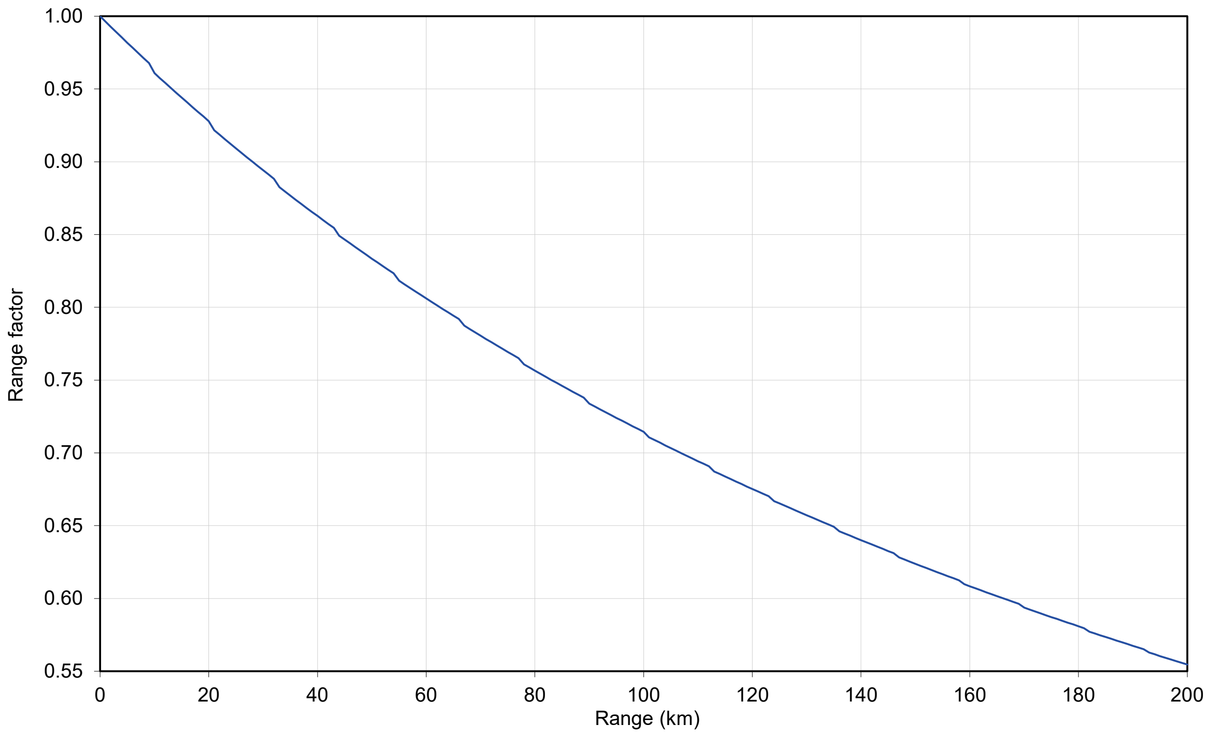


Figure 101 Range adjustment for PTP 700, symmetry 5:1, optimization IP, bandwidth 30 MHz

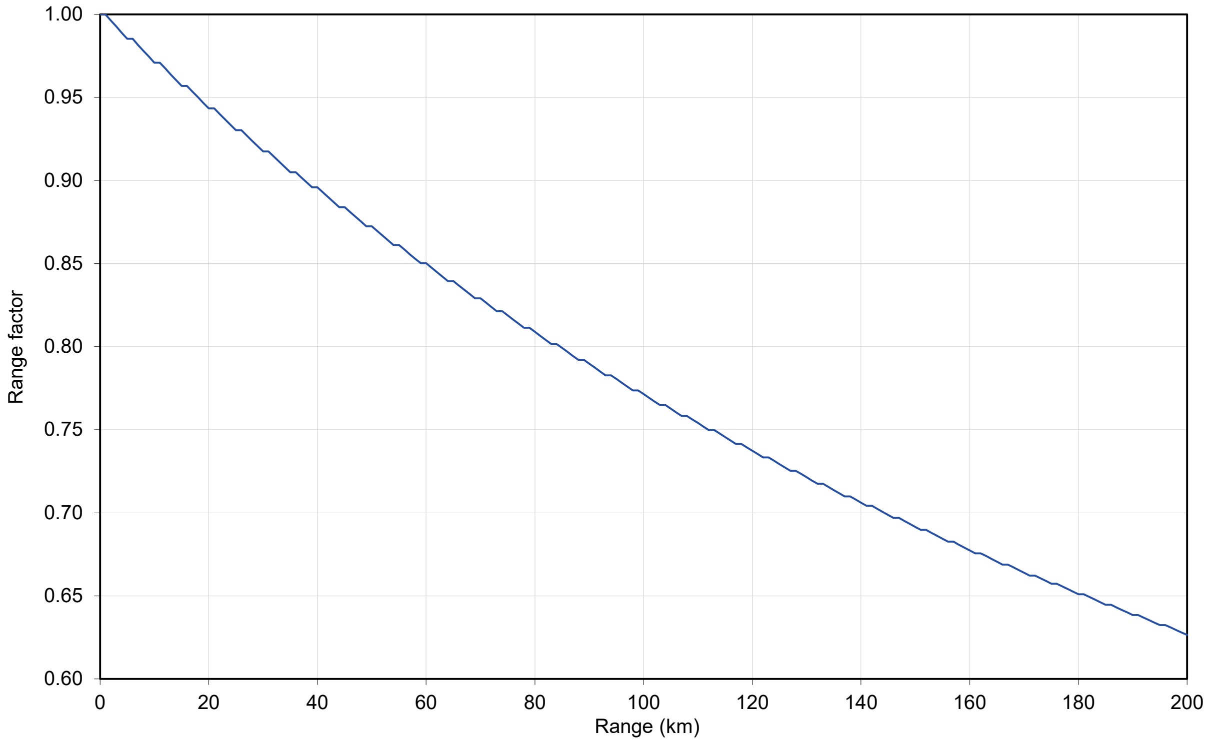


Figure 102 Range adjustment for PTP 700, adaptive, optimization IP, bandwidth 45 MHz

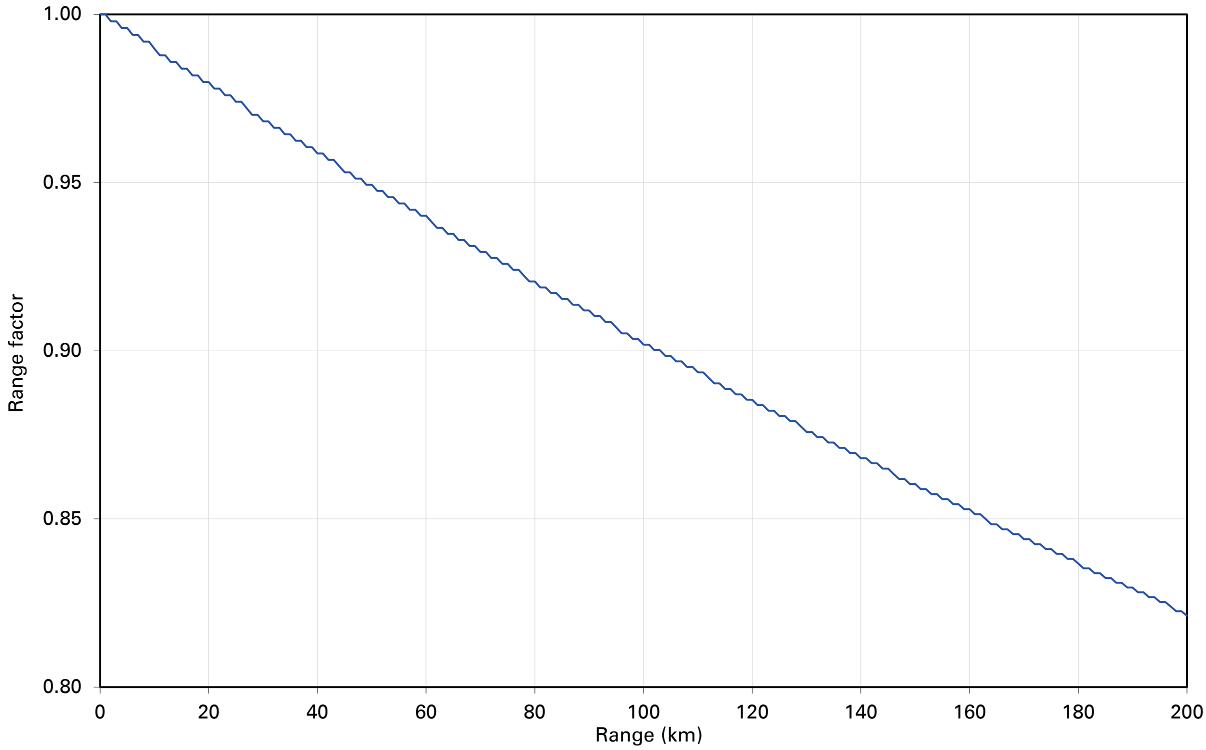


Figure 103 Range adjustment for PTP 700, adaptive, optimization IP, bandwidth 40 MHz

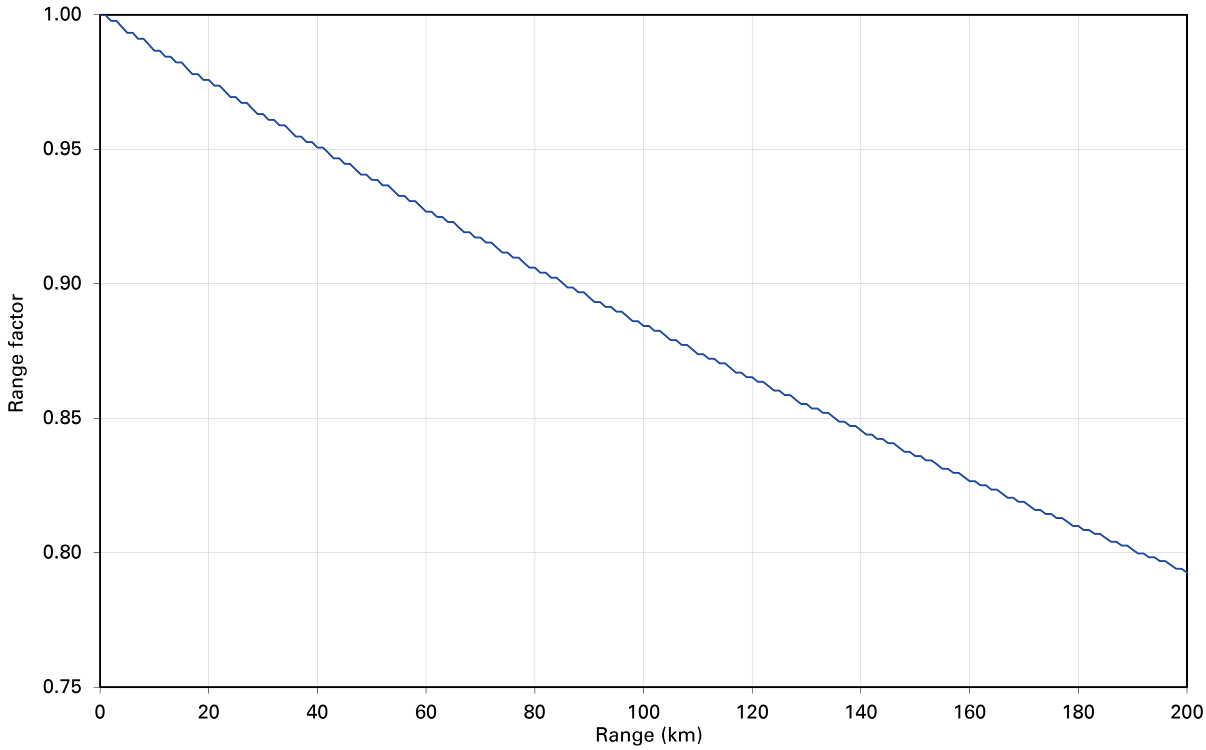


Figure 104 Range adjustment for PTP 700, adaptive, optimization IP, bandwidth 30 MHz

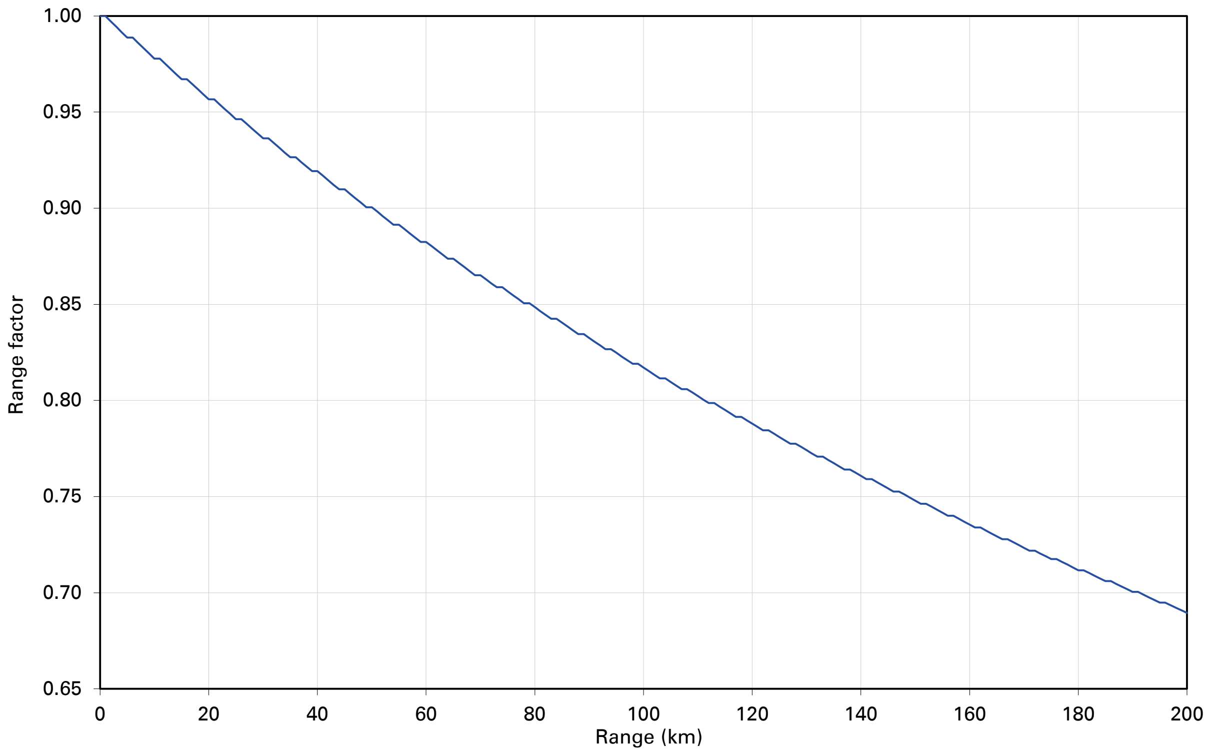


Figure 105 Range adjustment for PTP 700, adaptive, optimization IP, bandwidth 20 MHz

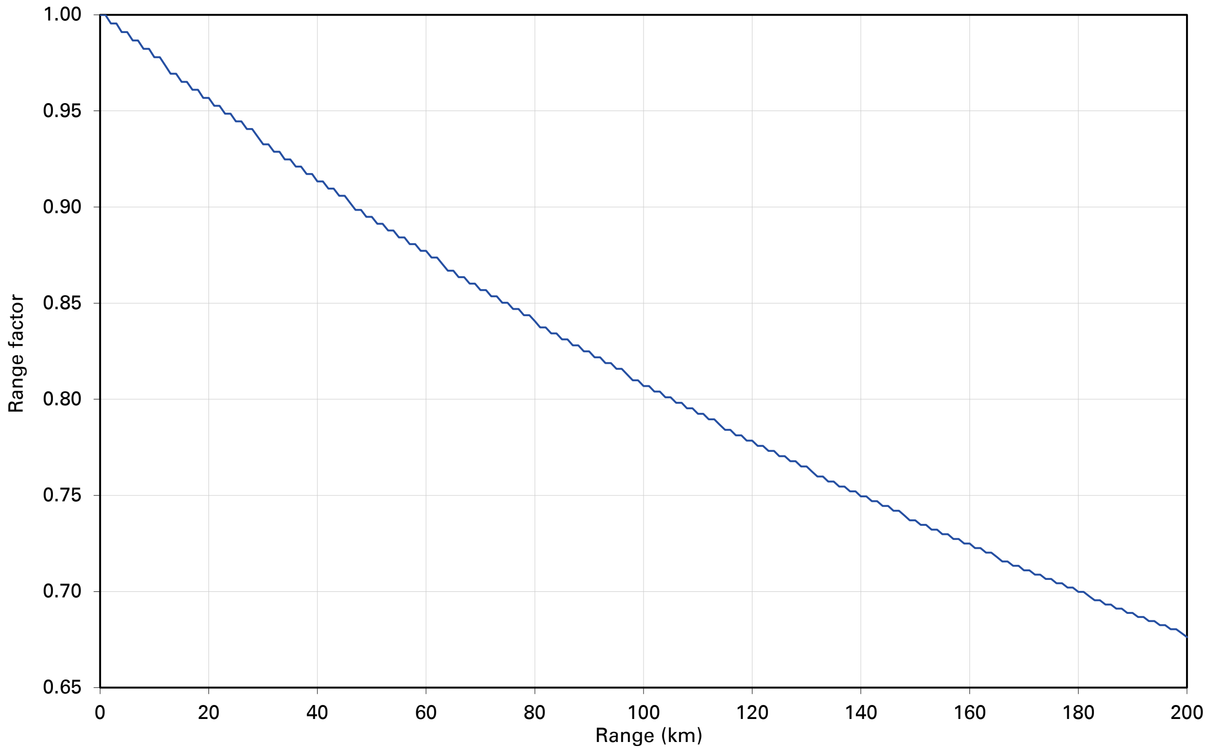


Figure 106 Range adjustment for PTP 700, adaptive, optimization IP, bandwidth 15 MHz

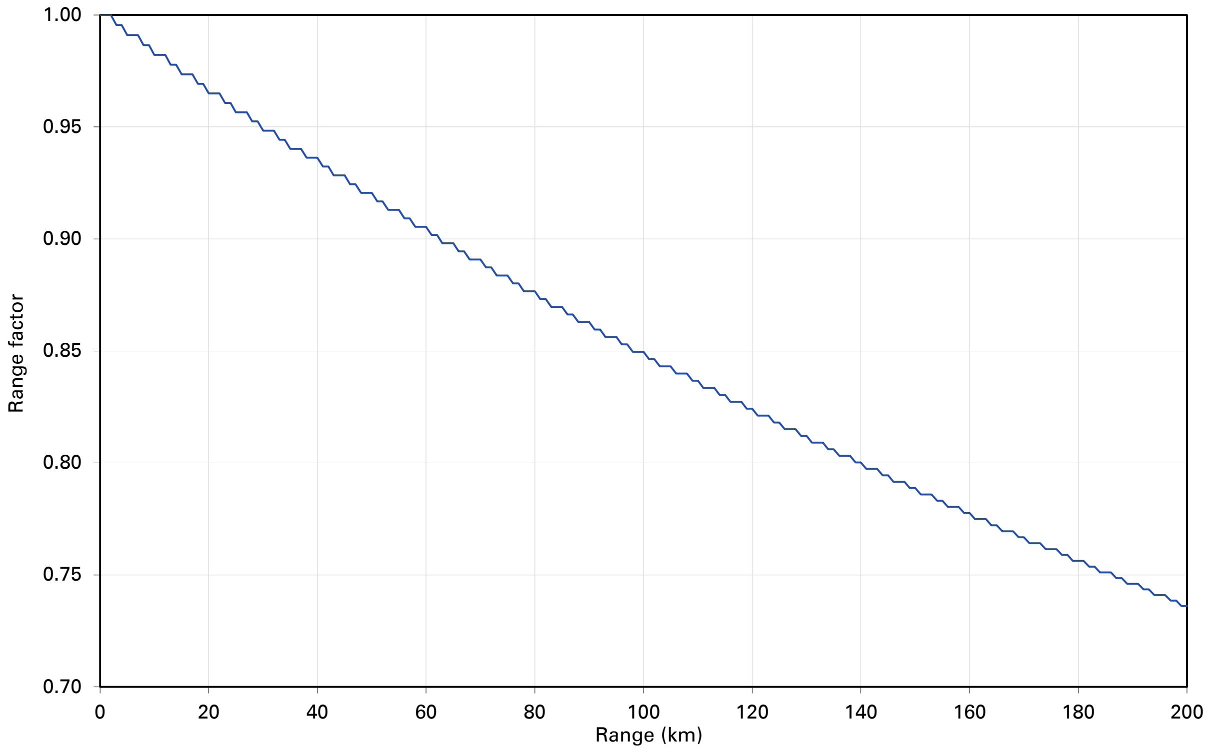
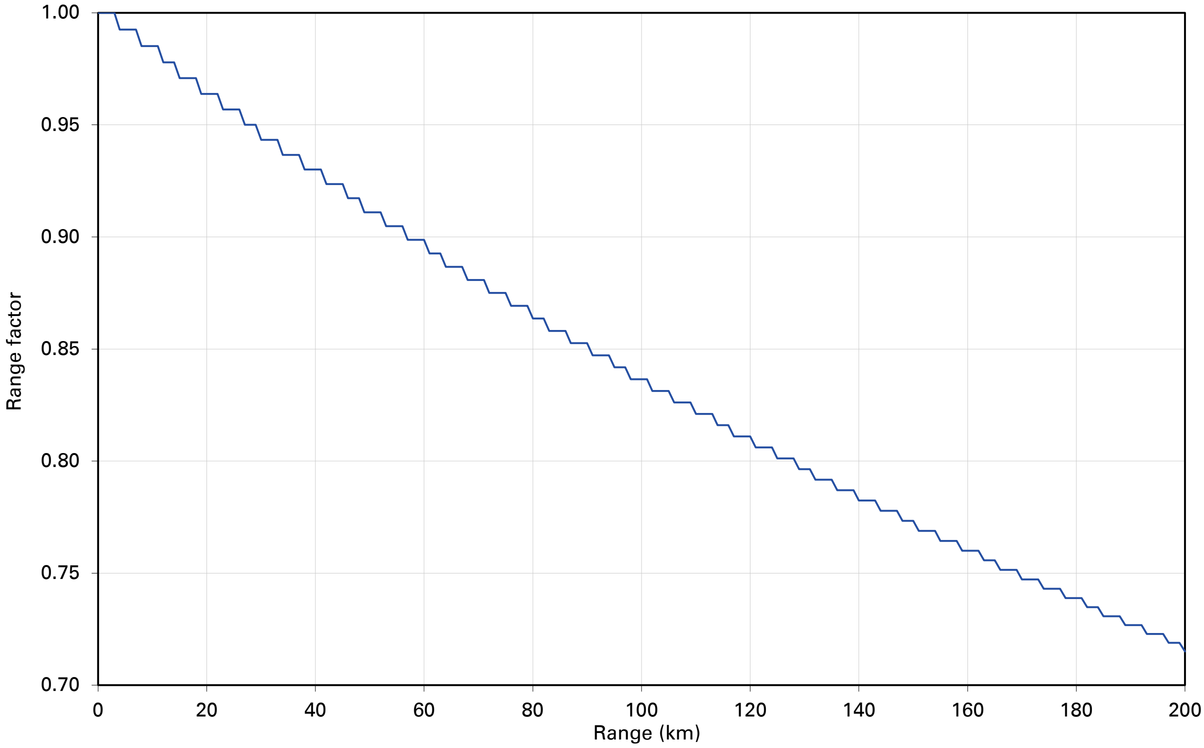


Figure 107 Range adjustment for PTP 700, adaptive, optimization IP, bandwidth 10 MHz



Time slots per frame in PTP topology with synchronization

Use the tables in this section to look up the number of time slots per TDD frame in PTP topology with TDD synchronization, including links with Hot Standby protection. Use this information with the capacity per time slot in Table 120 to calculate link capacity in each direction.

PTP topology with standard frame duration

Table 114 Number of time slots in synchronized PTP links

Channel Bandwidth	Burst Duration	Number of time slots
10 MHz	1088 µs	1
	2176 µs	2
15 MHz	726 µs	1
	1451 µs	2
	2176 µs	3
20 MHz	544 µs	1
	1088 µs	2
	1632 µs	3
	2176 µs	4
30 MHz	726 µs	2
	1088 µs	3
	1453 µs	4
	2176 µs	6
40 MHz	544 µs	2
	816 µs	3
	1088 µs	4
	1632 µs	6
	2176 µs	8
45 MHz	484 µs	2
	726 µs	3
	970 µs	4
	1453 µs	6
	1937 µs	8

PTP topology with long frame duration

Table 115 Number of time slots in synchronized PTP links with long frame duration

Channel Bandwidth	Burst Duration	Number of time slots	
		Unprotected	Hot Standby
20 MHz	1088 µs	2	1
	1632 µs	3	2
	2176 µs	4	3
	2720 µs	5	4
	3264 µs	6	5
	3808 µs	7	6
	4352 µs	8	7
	4896 µs	9	8
	5440 µs	10	9
	5984 µs	11	10
	6528 µs	12	11
30 MHz	726 µs	2	1
	1088 µs	3	2
	1451 µs	4	3
	1814 µs	5	4
	2176 µs	6	5
	2539 µs	7	6
	2902 µs	8	7
	3264 µs	9	8
	3627 µs	10	9
	3990 µs	11	10
	4352 µs	12	11
	4715 µs	13	12
	5078 µs	14	13
	5440 µs	15	14
40 MHz	532 µs	2	1
	798 µs	3	2

Channel Bandwidth	Burst Duration	Number of time slots	
		Unprotected	Hot Standby
	1064 µs	4	3
	1330 µs	5	4
	1596 µs	6	5
	1862 µs	7	6
	2128 µs	8	7
	2394 µs	9	8
	2660 µs	10	9
	2926 µs	11	10
	3192 µs	12	11
	3458 µs	13	12
	3724 µs	14	13
	3990 µs	15	14
45 MHz	486 µs	2	1
	728 µs	3	2
	971 µs	4	3
	1214 µs	5	4
	1456 µs	6	5
	1699 µs	7	6
	1942 µs	8	7
	2184 µs	9	8
	2427 µs	10	9
	2670 µs	11	10
	2912 µs	12	11
	3155 µs	13	12
	3398 µs	14	13
	3640 µs	15	14

Frame duration in HCMP topology with standard configuration

Use the tables in this section to look up the TDD frame duration as a function of bandwidth, number of Slaves and Link Symmetry. Then look up one-way capacity (Mbit/s) achieved in each time slot of an HCMP sector as a function of frame duration and modulation mode.

The one-way capacity for a single Slave is the capacity per time slot multiplied by the number of time slots. The aggregate (two-way) capacity for one Slave is the sum of two one-way capacities. The aggregate capacity for the Master is the capacity for one Slave multiplied by the number of Slaves.

Determine the frame duration from the following tables:

Table 116 HCMP frame duration table of tables

Channel Bandwidth	TDD Synchronization	Frame Duration Table	Capacity Table
20 MHz	Disabled	Table 117	Table 120
	Enabled		
40 MHz	Disabled	Table 118	
	Enabled	Table 119	

Table 117 HCMP frame duration, 20 MHz Channel Bandwidth

Number of Slaves	Link symmetry	Maximum range	Frame Duration
Two	1:1	5.0 km to 16.3 km	2882 µs
		16.4 km to 32.6 km	3012 µs
		32.7 km to 57.0 km	3145 µs
		57.1 km to 81.5 km	3311 µs
		81.6 km to 97.8 km	3460 µs
		97.9 km to 100.0 km	3610 µs
	1:2 and 2:1	5.0 km to 16.3 km	4184 µs
		16.4 km to 40.7 km	4367 µs
		40.8 km to 73.3 km	4566 µs
		73.4 km to 100.0 km	4785 µs
	1:3 and 3:1	5.0 km to 16.3 km	5495 µs
		16.4 km to 48.9 km	5714 µs
		49.0 km to 97.8 km	6024 µs
		97.9 km to 100.0 km	6410 µs

Number of Slaves	Link symmetry	Maximum range	Frame Duration
	1:4 and 4:1	5.0 km to 24.4 km	6849 µs
		24.5 km to 65.2 km	7143 µs
		65.3 km to 100.0 km	8065 µs
Three	1:1	5.0 km to 16.3 km	4184 µs
		16.4 km to 40.7 km	4367 µs
		40.8 km to 73.3 km	4566 µs
		73.4 km to 100.0 km	4785 µs
	1:2 and 2:1	5.0 km to 57.0 km	6410 µs
		57.1 km to 100.0 km	6849 µs
	1:3 and 3:1	5.0 km to 8.1 km	8065 µs
		8.2 km to 81.5 km	8547 µs
		81.6 km to 100.0 km	9259 µs
	1:4 and 4:1	5.0 km to 8.1 km	10000 µs
		8.2 km to 81.5 km	10526 µs
		81.6 km to 100.0 km	10989 µs
Four	1:1	5.0 km to 16.3 km	5495 µs
		16.4 km to 48.9 km	5714 µs
		49.0 km to 97.8 km	6024 µs
		97.9 km to 100.0 km	6410 µs
	1:2 and 2:1	5.0 km to 8.1 km	8065 µs
		8.2 km to 81.5 km	8547 µs
		81.6 km to 100.0 km	9259 µs
	1:3 and 3:1	5.0 km to 57.0 km	10989 µs
		57.1 km to 100.0 km	11628 µs
	1:4 and 4:1	5.0 km to 40.7 km	13514 µs
		40.8 km to 100.0 km	14286 µs
Five	1:1	5.0 km to 24.4 km	6849 µs
		24.5 km to 65.2 km	7143 µs
		65.3 km to 100.0 km	8065 µs

Number of Slaves	Link symmetry	Maximum range	Frame Duration
	1:2 and 2:1	5.0 km to 8.1 km	10000 µs
		8.2 km to 81.5 km	10526 µs
		81.6 km to 100.0 km	10989 µs
	1:3 and 3:1	5.0 km to 40.7 km	13514 µs
		40.8 km to 100.0 km	14286 µs
Six	1:1	5.0 km to 8.1 km	8065 µs
		8.2 km to 81.5 km	8547 µs
		81.6 km to 100.0 km	9259 µs
	1:2 and 2:1	5.0 km to 40.7 km	12195 µs
		40.8 km to 100.0 km	13514 µs
Seven	1:1	5.0 km to 32.6 km	9524 µs
		32.7 km to 100.0 km	10000 µs
	1:2 and 2:1	5.0 km to 57.0 km	14286 µs
Eight	1:1	5.0 km to 57.0 km	10989 µs
		57.1 km to 100.0 km	11628 µs

Table 118 HCMP frame duration, 40 MHz Channel Bandwidth, without TDD Sync

Number of Slaves	Link symmetry	Maximum range	Frame Duration
Two	1:1	5.0 km to 7.9 km	1439 µs
		8.0 km to 15.9 km	1504 µs
		16.0 km to 27.9 km	1575 µs
		28.0 km to 31.8 km	1623 µs
		31.9 km to 39.8 km	1650 µs
		39.9 km to 51.8 km	1730 µs
		51.9 km to 59.7 km	1805 µs
		59.8 km to 67.7 km	1859 µs
		67.8 km to 75.7 km	1908 µs
		75.8 km to 91.6 km	2000 µs
		91.7 km to 100.0 km	2079 µs

Number of Slaves	Link symmetry	Maximum range	Frame Duration
	2:1	5.0 km to 7.9 km	2079 µs
		8.0 km to 19.9 km	2179 µs
		20.0 km to 35.8 km	2283 µs
		35.9 km to 51.8 km	2392 µs
		51.9 km to 67.7 km	2500 µs
		67.8 km to 87.6 km	2618 µs
		87.7 km to 100.0 km	2747 µs
	3:1	5.0 km to 11.9 km	2747 µs
		12.0 km to 31.8 km	2882 µs
		31.9 km to 51.8 km	3012 µs
		51.9 km to 71.7 km	3145 µs
		71.8 km to 95.6 km	3311 µs
		95.7 km to 100.0 km	3460 µs
	4:1	5.0 km to 19.9 km	3460 µs
		20.0 km to 43.8 km	3610 µs
		43.9 km to 75.7 km	3817 µs
		75.8 km to 100.0 km	4000 µs
Three	1:1	5.0 km to 7.9 km	2079 µs
		8.0 km to 19.9 km	2179 µs
		20.0 km to 35.8 km	2283 µs
		35.9 km to 51.8 km	2392 µs
		51.9 km to 67.7 km	2500 µs
		67.8 km to 87.6 km	2618 µs
		87.7 km to 100.0 km	2747 µs
	2:1	5.0 km to 19.9 km	3145 µs
		20.0 km to 47.8 km	3311 µs
		47.9 km to 67.7 km	3460 µs
		67.8 km to 91.6 km	3610 µs
		91.7 km to 100.0 km	3817 µs

Number of Slaves	Link symmetry	Maximum range	Frame Duration
	3:1	5.0 km to 7.9 km	4000 µs
		8.0 km to 31.8 km	4184 µs
		31.9 km to 59.7 km	4367 µs
		59.8 km to 91.6 km	4566 µs
		91.7 km to 100.0 km	4785 µs
	4:1	5.0 km to 11.9 km	5000 µs
		12.0 km to 47.8 km	5236 µs
		47.9 km to 87.6 km	5495 µs
		87.7 km to 100.0 km	5714 µs
Four	1:1	5.0 km to 11.9 km	2747 µs
		12.0 km to 31.8 km	2882 µs
		31.9 km to 51.8 km	3012 µs
		51.9 km to 71.7 km	3145 µs
		71.8 km to 95.6 km	3311 µs
		95.7 km to 100.0 km	3460 µs
	2:1	5.0 km to 7.9 km	4000 µs
		8.0 km to 31.8 km	4184 µs
		31.9 km to 59.7 km	4367 µs
		59.8 km to 91.6 km	4566 µs
		91.7 km to 100.0 km	4785 µs
	3:1	5.0 km to 39.8 km	5495 µs
		39.9 km to 71.7 km	5714 µs
		71.8 km to 100.0 km	6024 µs
	4:1	5.0 km to 47.8 km	6849 µs
		47.9 km to 91.6 km	7143 µs
		91.7 km to 100.0 km	8065 µs
Five	1:1	5.0 km to 19.9 km	3460 µs
		20.0 km to 43.8 km	3610 µs
		43.9 km to 75.7 km	3817 µs

Number of Slaves	Link symmetry	Maximum range	Frame Duration
		75.8 km to 100.0 km	4000 µs
	2:1	5.0 km to 11.9 km	5000 µs
		12.0 km to 47.8 km	5236 µs
		47.9 km to 87.6 km	5495 µs
		87.7 km to 100.0 km	5714 µs
	3:1	5.0 km to 47.8 km	6849 µs
		47.9 km to 91.6 km	7143 µs
		91.7 km to 100.0 km	8065 µs
	4:1	5.0 km to 63.7 km	8547 µs
		63.8 km to 100.0 km	9259 µs
Six	1:1	5.0 km to 7.9 km	4000 µs
		8.0 km to 31.8 km	4184 µs
		31.9 km to 59.7 km	4367 µs
		59.8 km to 91.6 km	4566 µs
		91.7 km to 100.0 km	4785 µs
	2:1	5.0 km to 19.9 km	6024 µs
		20.0 km to 79.7 km	6410 µs
		79.8 km to 100.0 km	6849 µs
	3:1	5.0 km to 39.8 km	8065 µs
		39.9 km to 100.0 km	8547 µs
	4:1	5.0 km to 39.8 km	10000 µs
		39.9 km to 100.0 km	10526 µs
Seven	1:1	5.0 km to 27.9 km	4785 µs
		28.0 km to 59.7 km	5000 µs
		59.8 km to 95.6 km	5236 µs
		95.7 km to 100.0 km	5495 µs
	2:1	5.0 km to 43.8 km	7143 µs
		43.9 km to 100.0 km	8065 µs
	3:1	5.0 km to 27.9 km	9259 µs

Number of Slaves	Link symmetry	Maximum range	Frame Duration
		28.0 km to 63.7 km	9524 µs
		63.8 km to 100.0 km	10000 µs
	4:1	5.0 km to 43.8 km	11628 µs
		43.9 km to 100.0 km	12195 µs
Eight	1:1	5.0 km to 39.8 km	5495 µs
		39.9 km to 71.7 km	5714 µs
		71.8 km to 100.0 km	6024 µs
	2:1	5.0 km to 39.8 km	8065 µs
		39.9 km to 100.0 km	8547 µs
	3:1	5.0 km to 23.9 km	10526 µs
		24.0 km to 91.6 km	10989 µs
		91.7 km to 100.0 km	11628 µs
	4:1	5.0 km to 87.6 km	13514 µs
		87.7 km to 100.0 km	14286 µs

Table 119 HCMP frame duration, 40 MHz Channel Bandwidth, with TDD Sync

Number of Slaves	Link symmetry	Maximum range	Frame Duration
Two	1:1	5.0 km to 91.6 km	2000 µs
		91.7 km to 100.0 km	2283 µs
	2:1	5.0 km to 35.8 km	2283 µs
		35.9 km to 100.0 km	2747 µs
	3:1	5.0 km to 11.9 km	2747 µs
		12.0 km to 100.0 km	4000 µs
	4:1	5.0 km to 100.0 km	4000 µs
Three	1:1	5.0 km to 35.8 km	2283 µs
		35.9 km to 100.0 km	2747 µs
	2:1	5.0 km to 100.0 km	4000 µs
	3:1	5.0 km to 7.9 km	4000 µs
		8.0 km to 31.8 km	4184 µs

Number of Slaves	Link symmetry	Maximum range	Frame Duration
		31.9 km to 91.6 km	4566 µs
		91.7 km to 100.0 km	5495 µs
	4:1	5.0 km to 87.6 km	5495 µs
		87.7 km to 100.0 km	6024 µs
Four	1:1	5.0 km to 11.9 km	2747 µs
		12.0 km to 100.0 km	4000 µs
	2:1	5.0 km to 7.9 km	4000 µs
		8.0 km to 31.8 km	4184 µs
		31.9 km to 91.6 km	4566 µs
		91.7 km to 100.0 km	5495 µs
	3:1	5.0 km to 39.8 km	5495 µs
		39.9 km to 100.0 km	6024 µs
	4:1	5.0 km to 47.8 km	6849 µs
		47.9 km to 91.6 km	7143 µs
		91.7 km to 100.0 km	8065 µs
Five	1:1	5.0 km to 100.0 km	4000 µs
	2:1	5.0 km to 87.6 km	5495 µs
		87.7 km to 100.0 km	6024 µs
	3:1	5.0 km to 47.8 km	6849 µs
		47.9 km to 91.6 km	7143 µs
		91.7 km to 100.0 km	8065 µs
	4:1	5.0 km to 63.7 km	8547 µs
		63.8 km to 100.0 km	9259 µs
Six	1:1	5.0 km to 7.9 km	4000 µs
		8.0 km to 31.8 km	4184 µs
		31.9 km to 91.6 km	4566 µs
		91.7 km to 100.0 km	5495 µs
	2:1	5.0 km to 19.9 km	6024 µs
		20.0 km to 79.7 km	6410 µs

Number of Slaves	Link symmetry	Maximum range	Frame Duration
		79.8 km to 100.0 km	6849 µs
	3:1	5.0 km to 39.8 km	8065 µs
		39.9 km to 100.0 km	8547 µs
	4:1	5.0 km to 39.8 km	10000 µs
		39.9 km to 100.0 km	10526 µs
Seven	1:1	5.0 km to 100.0 km	5495 µs
	2:1	5.0 km to 43.8 km	7143 µs
		43.9 km to 100.0 km	8065 µs
	3:1	5.0 km to 27.9 km	9259 µs
		28.0 km to 63.7 km	9524 µs
		63.8 km to 100.0 km	10000 µs
	4:1	5.0 km to 43.8 km	11628 µs
		43.9 km to 100.0 km	12195 µs
Eight	1:1	5.0 km to 39.8 km	5495 µs
		39.9 km to 100.0 km	6024 µs
	2:1	5.0 km to 39.8 km	8065 µs
		39.9 km to 100.0 km	8547 µs
	3:1	5.0 km to 23.9 km	10526 µs
		24.0 km to 91.6 km	10989 µs
		91.7 km to 100.0 km	11628 µs
	4:1	5.0 km to 87.6 km	13514 µs
		87.7 km to 100.0 km	14286 µs

Frame duration in HCMP topology with expert configuration

When TDD Frame Configuration Mode is set to Expert Mode, the ODU is configured by setting the maximum link range in the Wireless Configuration page of the Installation Wizard and selecting the number of time slots reserved for uplink and downlink directions in the TDD Frame page. The ODU calculates the TDD Frame Duration and displays this in the TDD Synchronization page of the Installation Wizard. TDD Frame Duration depends on:

- Channel Bandwidth
- Maximum Range

- TDD Synchronization
- Number of Uplink Time Slots at the Master
- Number of Downlink Time Slots at the Master

Frame Duration in HCMP Frame Configuration Expert Mode can be determined using the ODU or the LINKPlanner.

Capacity per time slot

The following table shows the data capacity of a PTP 700 wireless link for one time slot at any Modulation Mode and any Frame Duration.

Table 120 Throughput (Mbit/s) per time slot

	Frame duration						
Modulation mode	**1439 µs**	**1504 µs**	**1575 µs**	**1623 µs**	**1650 µs**	**1730 µs**	**1805 µs**
256QAM 0.81 dual	77.19	73.86	70.53	68.42	67.31	64.20	61.53
64QAM 0.92 dual	65.04	62.23	59.42	57.64	56.71	54.09	51.84
64QAM 0.75 dual	53.15	50.85	48.56	47.11	46.34	44.20	42.36
16QAM 0.87 dual	41.35	39.56	37.78	36.65	36.05	34.39	32.96
16QAM 0.63 dual	29.72	28.44	27.16	26.34	25.92	24.72	23.69
256QAM 0.81 single	38.60	36.93	35.26	34.21	33.65	32.10	30.77
64QAM 0.92 single	32.52	31.11	29.71	28.82	28.35	27.04	25.92
64QAM 0.75 single	26.57	25.43	24.28	23.55	23.17	22.10	21.18
16QAM 0.87 single	20.67	19.78	18.89	18.32	18.03	17.19	16.48
16QAM 0.63 single	14.86	14.22	13.58	13.17	12.96	12.36	11.85
QPSK 0.87 single	10.34	9.89	9.44	9.16	9.01	8.60	8.24
QPSK 0.63 single	7.43	7.11	6.79	6.59	6.48	6.18	5.92
BPSK 0.63 single	3.72	3.56	3.39	3.29	3.24	3.09	2.96

	Frame duration						
Modulation mode	**1859 µs**	**1908 µs**	**2000 µs**	**2079 µs**	**2179 µs**	**2283 µs**	**2392 µs**
256QAM 0.81 dual	59.75	58.20	55.53	53.42	50.98	48.65	46.43
64QAM 0.92 dual	50.34	49.03	46.79	45.01	42.95	40.99	39.12
64QAM 0.75 dual	41.14	40.07	38.24	36.78	35.10	33.49	31.96
16QAM 0.87 dual	32.01	31.17	29.75	28.62	27.31	26.06	24.87
16QAM 0.63 dual	23.01	22.41	21.38	20.57	19.63	18.73	17.88

	Frame duration						
Modulation mode	1859 µs	1908 µs	2000 µs	2079 µs	2179 µs	2283 µs	2392 µs
256QAM 0.81 single	29.88	29.10	27.77	26.71	25.49	24.32	23.21
64QAM 0.92 single	25.17	24.52	23.39	22.51	21.48	20.49	19.56
64QAM 0.75 single	20.57	20.04	19.12	18.39	17.55	16.75	15.98
16QAM 0.87 single	16.00	15.59	14.87	14.31	13.65	13.03	12.43
16QAM 0.63 single	11.50	11.21	10.69	10.29	9.82	9.37	8.94
QPSK 0.87 single	8.00	7.79	7.44	7.15	6.83	6.51	6.22
QPSK 0.63 single	5.75	5.60	5.35	5.14	4.91	4.68	4.47
BPSK 0.63 single	2.88	2.80	2.67	2.57	2.45	2.34	2.23

	Frame duration						
Modulation mode	2500 µs	2618 µs	2747 µs	2882 µs	3012 µs	3145 µs	3311 µs
256QAM 0.81 dual	44.43	42.43	40.43	38.54	36.87	35.32	33.54
64QAM 0.92 dual	37.43	35.75	34.06	32.47	31.07	29.76	28.26
64QAM 0.75 dual	30.59	29.21	27.84	26.54	25.39	24.32	23.09
16QAM 0.87 dual	23.80	22.73	21.65	20.64	19.75	18.92	17.97
16QAM 0.63 dual	17.11	16.34	15.57	14.84	14.20	13.60	12.92
256QAM 0.81 single	22.21	21.21	20.21	19.27	18.44	17.66	16.77
64QAM 0.92 single	18.72	17.87	17.03	16.24	15.53	14.88	14.13
64QAM 0.75 single	15.29	14.61	13.92	13.27	12.69	12.16	11.55
16QAM 0.87 single	11.90	11.36	10.83	10.32	9.88	9.46	8.98
16QAM 0.63 single	8.55	8.17	7.78	7.42	7.10	6.80	6.46
QPSK 0.87 single	5.95	5.68	5.41	5.16	4.94	4.73	4.49
QPSK 0.63 single	4.28	4.08	3.89	3.71	3.55	3.40	3.23
BPSK 0.63 single	2.14	2.04	1.95	1.86	1.77	1.70	1.61

	Frame duration						
Modulation mode	3460 µs	3610 µs	3817 µs	4000 µs	4184 µs	4367 µs	4566 µs
256QAM 0.81 dual	32.10	30.77	29.10	27.77	26.55	25.43	24.32
64QAM 0.92 dual	27.04	25.92	24.52	23.39	22.37	21.43	20.49

	Frame duration						
Modulation mode	**3460 µs**	**3610 µs**	**3817 µs**	**4000 µs**	**4184 µs**	**4367 µs**	**4566 µs**
64QAM 0.75 dual	22.10	21.18	20.04	19.12	18.28	17.51	16.75
16QAM 0.87 dual	17.19	16.48	15.59	14.87	14.22	13.62	13.03
16QAM 0.63 dual	12.36	11.85	11.21	10.69	10.22	9.79	9.37
256QAM 0.81 single	16.05	15.38	14.55	13.88	13.27	12.72	12.16
64QAM 0.92 single	13.52	12.96	12.26	11.70	11.18	10.71	10.25
64QAM 0.75 single	11.05	10.59	10.02	9.56	9.14	8.76	8.37
16QAM 0.87 single	8.60	8.24	7.79	7.44	7.11	6.81	6.51
16QAM 0.63 single	6.18	5.92	5.60	5.35	5.11	4.90	4.68
QPSK 0.87 single	4.30	4.12	3.90	3.72	3.55	3.41	3.26
QPSK 0.63 single	3.09	2.96	2.80	2.67	2.56	2.45	2.34
BPSK 0.63 single	1.54	1.48	1.40	1.34	1.28	1.22	1.17

	Frame duration						
Modulation mode	**4785 µs**	**5000 µs**	**5236 µs**	**5495 µs**	**5714 µs**	**6024 µs**	**6410 µs**
256QAM 0.81 dual	23.21	22.21	21.21	20.21	19.44	18.44	17.33
64QAM 0.92 dual	19.56	18.72	17.87	17.03	16.38	15.53	14.60
64QAM 0.75 dual	15.98	15.29	14.61	13.92	13.38	12.69	11.93
16QAM 0.87 dual	12.43	11.90	11.36	10.83	10.41	9.88	9.28
16QAM 0.63 dual	8.94	8.55	8.17	7.78	7.48	7.10	6.67
256QAM 0.81 single	11.61	11.11	10.61	10.11	9.72	9.22	8.66
64QAM 0.92 single	9.78	9.36	8.94	8.52	8.19	7.77	7.30
64QAM 0.75 single	7.99	7.65	7.30	6.96	6.69	6.35	5.96
16QAM 0.87 single	6.22	5.95	5.68	5.41	5.21	4.94	4.64
16QAM 0.63 single	4.47	4.28	4.08	3.89	3.74	3.55	3.34
QPSK 0.87 single	3.11	2.97	2.84	2.71	2.60	2.47	2.32
QPSK 0.63 single	2.23	2.14	2.04	1.95	1.87	1.77	1.67
BPSK 0.63 single	1.12	1.07	1.02	0.97	0.94	0.89	0.83

	Frame duration						
Modulation mode	**6849 μs**	**7143 μs**	**8065 μs**	**8547 μs**	**9259 μs**	**9524 μs**	**10000 μs**
256QAM 0.81 dual	16.22	15.55	13.77	12.99	12.00	11.66	11.11
64QAM 0.92 dual	13.66	13.10	11.60	10.95	10.11	9.83	9.36
64QAM 0.75 dual	11.16	10.71	9.48	8.95	8.26	8.03	7.65
16QAM 0.87 dual	8.69	8.33	7.38	6.96	6.43	6.25	5.95
16QAM 0.63 dual	6.24	5.99	5.30	5.00	4.62	4.49	4.28
256QAM 0.81 single	8.11	7.77	6.89	6.50	6.00	5.83	5.55
64QAM 0.92 single	6.83	6.55	5.80	5.47	5.05	4.91	4.68
64QAM 0.75 single	5.58	5.35	4.74	4.47	4.13	4.01	3.82
16QAM 0.87 single	4.34	4.16	3.69	3.48	3.21	3.12	2.97
16QAM 0.63 single	3.12	2.99	2.65	2.50	2.31	2.25	2.14
QPSK 0.87 single	2.17	2.08	1.84	1.74	1.61	1.56	1.49
QPSK 0.63 single	1.56	1.50	1.33	1.25	1.15	1.12	1.07
BPSK 0.63 single	0.78	0.75	0.66	0.63	0.58	0.56	0.53

	Frame duration					
Modulation mode	**10526 μs**	**10989 μs**	**11628 μs**	**12195 μs**	**13514 μs**	**14286 μs**
256QAM 0.81 dual	10.55	10.11	9.55	9.11	8.22	7.77
64QAM 0.92 dual	8.89	8.52	8.05	7.67	6.92	6.55
64QAM 0.75 dual	7.26	6.96	6.58	6.27	5.66	5.35
16QAM 0.87 dual	5.65	5.41	5.12	4.88	4.40	4.16
16QAM 0.63 dual	4.06	3.89	3.68	3.51	3.16	2.99
256QAM 0.81 single	5.28	5.05	4.78	4.55	4.11	3.89
64QAM 0.92 single	4.44	4.26	4.02	3.84	3.46	3.28
64QAM 0.75 single	3.63	3.48	3.29	3.14	2.83	2.68
16QAM 0.87 single	2.83	2.71	2.56	2.44	2.20	2.08
16QAM 0.63 single	2.03	1.95	1.84	1.75	1.58	1.50
QPSK 0.87 single	1.41	1.35	1.28	1.22	1.10	1.04
QPSK 0.63 single	1.02	0.97	0.92	0.88	0.79	0.75
BPSK 0.63 single	0.51	0.49	0.46	0.44	0.40	0.37

Chapter 4: Legal and regulatory information

This chapter provides end user license agreements and regulatory notifications.

Attention 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 700 Series products.
- Compliance with safety standards on page 4-20 lists the safety specifications against which the PTP 700 has been tested and certified. It also describes how to keep RF exposure within safe limits.
- Compliance with radio regulations on page 4-23 describes how the PTP 700 complies with the radio regulations that are in force in various countries, and contains notifications made to regulatory bodies for the PTP 700.

Cambium Networks end user license 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.

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.

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) -----

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) -----

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) -----

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

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

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

Copyright (c) 2013, Michael Bostock

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 Michael Bostock 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 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 MICHAEL BOSTOCK 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.

Compliance with safety standards

This section lists the safety specifications against which the PTP 700 has been tested and certified. It also describes how to keep RF exposure within safe limits.

Electrical safety compliance

The PTP 700 hardware has been tested for compliance to the electrical safety specifications listed in Table 121.

Table 121 PTP 700 safety compliance specifications

Region	Standard
USA	UL 60950-1, 2nd Edition; UL60950-22
Canada	CSA-C22.2 NO. 60950-1-07 (R2012) CSA-C22.2 NO. 60950-22-07 (R2012)
EU	EN 60950-1:2006 + Amendment 12:2011, EN 60950-22
	IEC 60950-1, IEC60950-22

Electromagnetic compatibility (EMC) compliance

The PTP 700 complies with European EMC Specification EN301 489-1 with testing carried out to the detailed requirements of EN301 489-17.

Note For EN 61000-4-2: 1995 to 2009 Electro Static Discharge (ESD), Class 2, 8 kV air, 4 kV contact discharge, the PTP 700 has been tested to ensure immunity to 15 kV air and 8 kV contact.

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 2013/35/EU of the European Parliament and of the Council of 26 June 2013* on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) (20th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC) and repealing Directive 2004/40/EC

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.

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 700 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 between 4400 MHz and 5875 MHz is 10 W/m^2.

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:

$$S = \frac{PG}{4\pi d^2}$$

Where:

- S is the power density in W/m^2
- P is the average transmit power capability of the radio in W, equal to the configured maximum transmitter power as a linear number, multiplied by 0.8 to account for the worst case transmit/receive ratio
- G is the effective antenna gain, including cable losses, expressed as a linear number (not in dBi)
- d is the distance from the antenna

Rearranging terms to solve for distance yields:

$$d = \sqrt{\frac{PG}{4\pi S}}$$

Calculated distances

Table 122 shows calculated minimum separation distances each frequency band and for the highest gain antenna of each type, assuming that the equipment is operating at the maximum transmit power for PTP 700. At these and greater separation distances, the power density from the RF field is below generally accepted limits for the general population.

Table 122 Minimum safe distances for PTP 700 at maximum transmitter power

Antenna	P (W) (*1)	G (*2)	S (W/m^2)	d (m) (*3)
Parabolic 6 ft (38.1 dBi)	0.635	5248.1	10	5.15
Parabolic 4 ft (35.3 dBi)	0.635	3388.4	10	3.73
Flat plate 2 ft (28.5 dBi)	0.635	575.4	10	1.71
Integrated (21.0 dBi)	0.635	125.9	10	0.80
Sectorized (17.0 dBi)	0.635	40.7	10	0.45
Omni (13.0 dBi)	0.635	16.2	10	0.29

(*1) P: maximum average transmit power capability of the radio (Watt)

(*2) G: total transmit gain as a factor, converted from dB, including 0.9 dB cable loss for connectorised antennas

(*3) d: minimum distance from the antenna (meters)

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.

Minimum separation distances for other transmitter powers and antenna gains

The minimum separation distances can be calculated for any transmit power or antenna gain using the formula provided in Calculation of power density on page 4-21.

In many deployments, the antenna gains will be lower than the maximum listed in Table 122 and the transmitter power will be reduced to comply with applicable regulations; in such cases, the minimum separation distances will be significantly reduced compared with the results in Table 122.

Compliance with radio regulations

This section describes how the PTP 700 complies with the radio regulations that are in force in various countries.

Attention 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.

Attention Changes or modifications not expressly approved by Cambium Networks could void the user's authority to operate the system.

Attention 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.

Chapter 5: Installation

This chapter describes how to install and test the hardware for a PTP 700 link. It contains the following topics:

- Safety on page 5-25 contains important safety guidelines that must be observed by personnel installing or operating PTP 700 equipment.
- ODU variants and mounting bracket options on page 5-28 provides details of six different bracket options, including the type of ODu and range of pole diameters supported by each option.
- Installing the ODU and top LPU on page 5-29 describes how to mount and ground a Connectorized+Integrated or Connectorized ODU, and how to mount and ground the top LPU.
- Install external antennas on page 5-36 describes how to mount and connect an external antenna for the Connectorized or Connectorized+Integrated ODU.
- Installing the copper Cat5e Ethernet interface on page 5-38 describes how to install the copper Cat5e power over Ethernet interface from the ODU (PSU port) to the PSU.
- Installing the PSU on page 5-46 describes how how to install a power supply unit for the PTP 700, either the AC+DC Enhanced Power Injector 56V or the CMM5.
- Installing a PTP-SYNC unit on page 5-49 describes how to install a PTP-SYNC unit for TDD synchronization.
- Installing the Trimble Accutime GPS receiver on page 5-53 describes how to install a GPS receiver as the timing reference source for PTP-SYNC or CMM5.
- Installing an SFP Ethernet interface on page 5-49 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 5-72 describes how to install a copper Cat5e Ethernet interface from the ODU (Aux port) to a connected device.
- Supplemental installation information on page 5-73 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 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 700 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 700. Ensure that only qualified personnel install a PTP 700 link.

Power lines

Exercise extreme care when working near power lines.

Working at heights

Exercise extreme care when working at heights.

PSU

Always use the AC+DC Enhanced Power Injector 56V or CMM5 to power the ODU. Failure to use these Cambium supplied PSUs 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.

AC supply

To power the ODU from an AC supply, use the AC+DC Enhanced Power Injector 56V (Cambium part number C000065L002C) or the CMM5

Always use an appropriately rated and approved AC supply cord-set in accordance with the regulations of the country of use.

DC supply

To power the ODU from a DC supply, use the AC+DC Enhanced Power Injector 56V (Cambium part number C000065L002C) or CMM5. Ensure that the DC power supply meets the requirements specified in PSU DC power supply on page 3-15.

Powering down before servicing

Before servicing PTP 700 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 56V 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 for the PTP 700..

Drop cable tester

The PSU output voltage may be hazardous in some conditions, for example in wet weather. Do NOT connect a drop cable tester to the PSU, either directly or via LPUs.

Grounding PTP-SYNC

In order to meet the safety requirements for deployment in Australia and New Zealand (AS/NZS 60950-1), the PTP-SYNC unit, if deployed, must be grounded to a Protective Ground in accordance with Local Electrical Regulations.

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 on page 4-22.

Grounding and lightning protection requirements

Ensure that the installation meets the requirements defined in Grounding and lightning protection on page 3-11.

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 200 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, external antennas and GPS receivers for PTP-SYNC 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 3-11. Mounting in Zone A may put equipment, structures and life at risk.

Thermal Safety

The ODU enclosure may be hot to the touch when in operation. The ODU must not be operated in ambient temperatures exceeding 40°C unless mounted in a Restricted Access Location. For more information, see ODU ambient temperature limits on page 3-13.

Warning Do not install the ODU in a location where the ambient temperature could exceed 40°C unless this is a Restricted Access Location as defined by EN 60950-1.

Alerte L’unité externe ne doit pas être installée dans un endroit où la température ambiante est supérieure à 40C à moins que l’accès soit limité au personnel autorisé.

ODU variants and mounting bracket options

Mounting bracket options

The PTP 700 series supports four mounting bracket options. Select the optimum mounting bracket arrangement based on the pole diameter and the ODU variant:

Table 123 ODU mounting bracket part numbers

Bracket	Pole diameter	ODU variants	Bracket part number
Mounting bracket (integrated)	40 mm to 82 mm (1.6 inches to 3.2 inches)	PTP 700 Connectorized+Integrated	N000065L031
Mounting bracket (connectorized)	40 mm to 82 mm (1.6 inches to 3.2 inches)	PTP 700 Connectorized	N000065L032
Extended integrated mounting bracket	89 mm *OR* 114 mm (3.5 inches *OR* 4.5 inches)	PTP 700 Connectorized PTP 700 Connectorized+Integrated	N000065L030
Mounting bracket (integrated) with large diameter extension kit	89 mm to 229 mm (3.5 inches to 9.0 inches)	PTP 700 Connectorized PTP 700 Connectorized+Integrated	N000065L031 with N000065L042

Note The connectorized mounting bracket is included with the PTP 700 Connectorized ODU. Order a bracket separately for PTP 700 Connectorized+Integrated ODUs.

Installing the ODU and top LPU

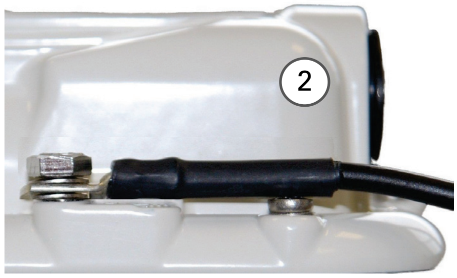
To install the ODU and top LPU, use the following procedures:

- Attach ground cables to the ODU on page 5-29
- Mount the ODU on the mast on page 5-29
- Mount the top LPU on page 5-34
- Interconnect and ground the ODU and top LPU on page 5-34

Attach ground cables to the ODU

1 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.

2 Tighten both ODU grounding bolts to a torque of 5 Nm (3.9 lb ft).



Mount the ODU on the mast

Select the most appropriate bracket mounting arrangement from the options listed in Mounting bracket options on page 5-28. Refer to individual procedures below for each of the options:

- Mounting bracket (integrated) on page 5-30
- Mounting bracket (connectorized) on page 5-31
- Extended integrated mounting bracket on page 5-32
- Mounting bracket (integrated) with large diameter extension kit on page 5-33

The procedure for the Mounting bracket (connectorized) can be readily adapted to attach the ODU to a horizontal pole of similar size.

The procedure for the Mounting bracket (integrated) and the Extended integrated mounting bracket can be adapted to attach the ODU to a suitable horizontal pole, but the adjustment of azimuth angle is necessarily limited compared with an installation on a vertical pole.

Mounting bracket (integrated)

Attention Do not reverse the bracket clamp, as this arrangement may lead to failure of the assembly. Do not over-tighten the bolts as this may lead to failure of the assembly.

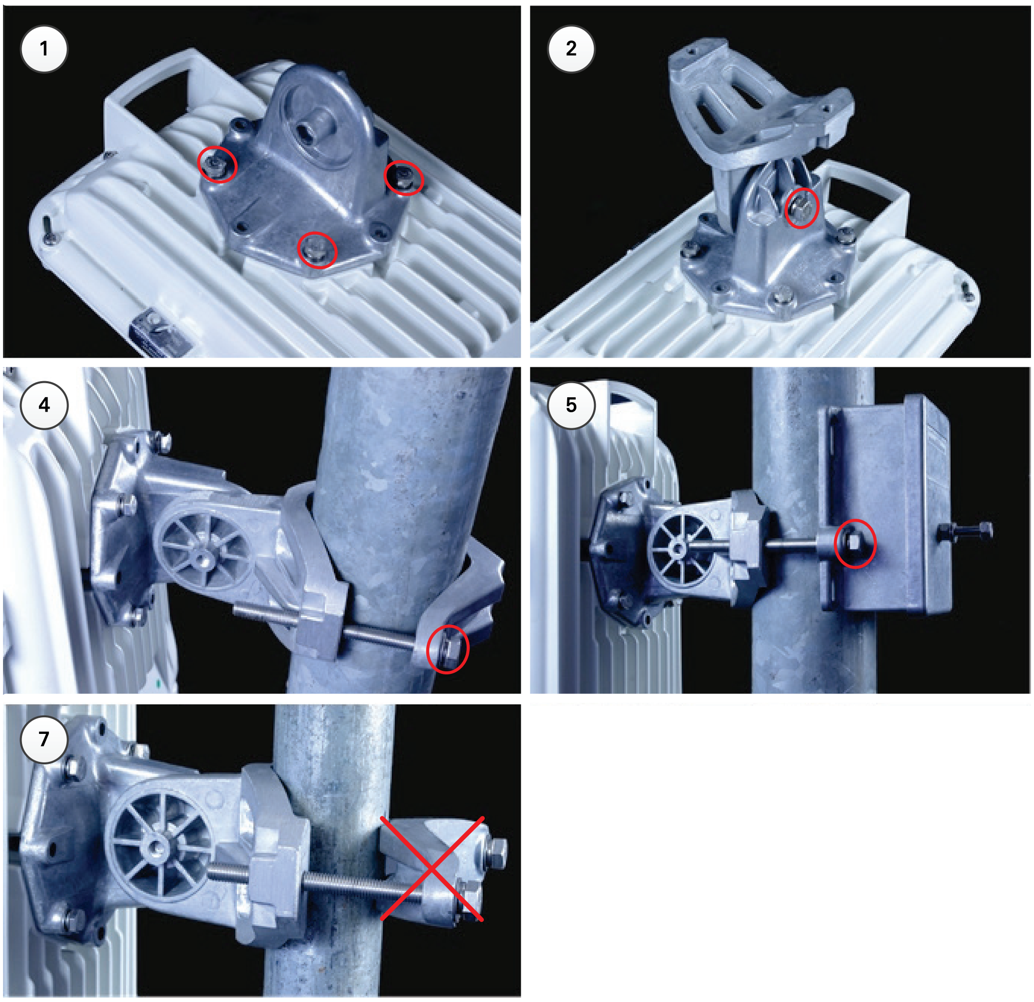
1 Fix the mounting plate to the back of the ODU using the four bolts, and spring and plain washers provided. Tighten the bolts to a torque setting of 5.0 Nm (3.7 lb ft).

2 Attach the bracket body to the mounting plate using the M8 bolt, spring and plain washers.

3 Hoist the ODU to the mounting position.

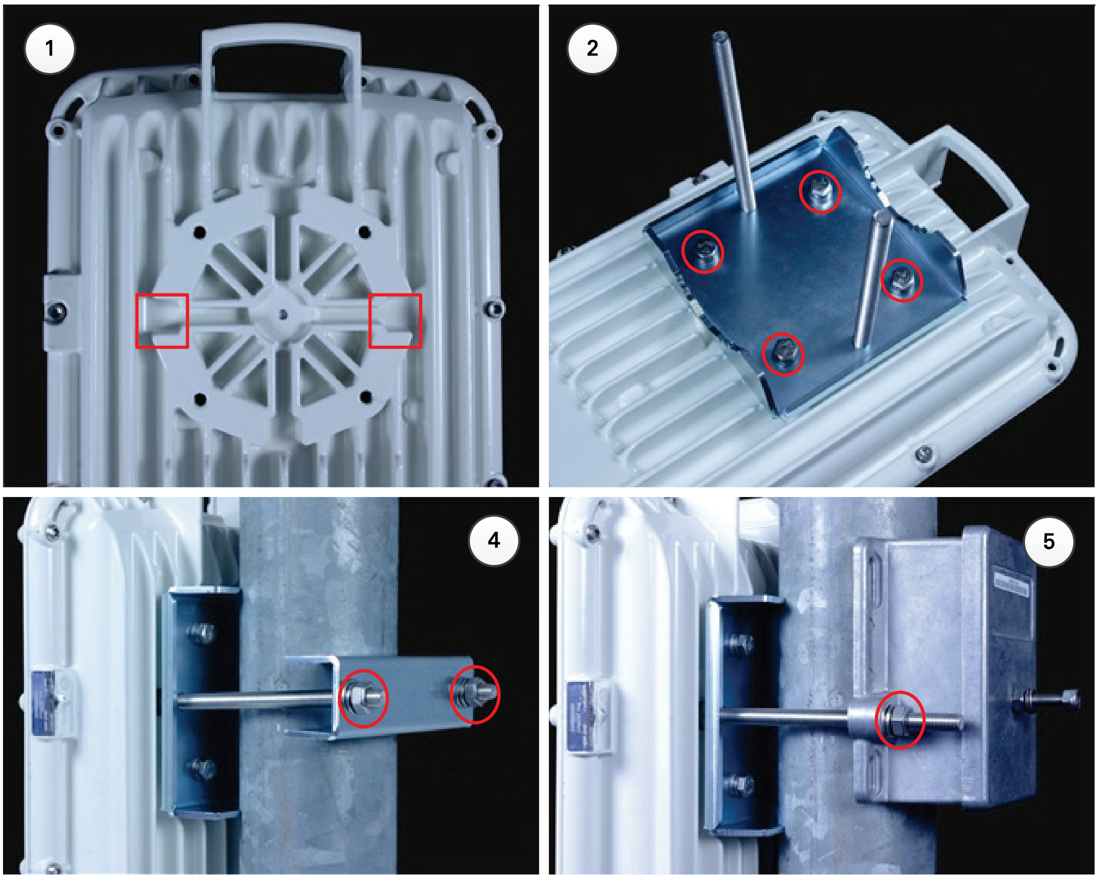
4 Attach the bracket body to the pole using the bracket clamp, M8 bolts, and spring and plain washers. For back-to-back mounting, use the LPU in place of the clamp.

5 Adjust the elevation and azimuth to achieve visual alignment. Tighten all three bracket bolts to a torque of 8.0 Nm (6.0 lb ft).



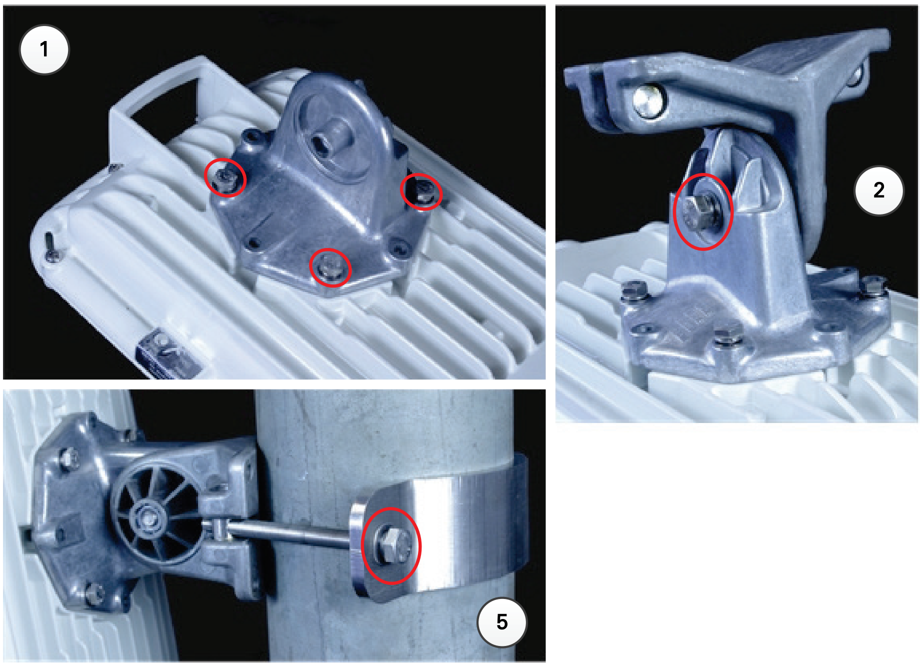
Mounting bracket (connectorized)

1. Identify the square cavities in the casting on the back of the ODU. These cavities will be used to accommodate the heads of two M8 bracket bolts.
2. Fix the mounting plate to the ODU using the four M6 bolts, and spring and plain washers provided. Ensure that the M8 bolts are correctly held between the mounting plate and the ODU. Tighten the M6 bolts to a torque setting of 5.0 Nm (3.7 lb ft).
3. Hoist the ODU to the mounting position.
4. Attach the bracket body to the pole using the bracket clamp, spring and plain washers, and M8 nuts.
5. Alternatively, use the LPU in place of the clamp to provide a back-to-back arrangement.
6. Tighten the two M8 bracket bolts to a torque setting of 8.0 Nm (6.0 lb ft). Do not over-tighten the bolts as this may lead to failure of the assembly.



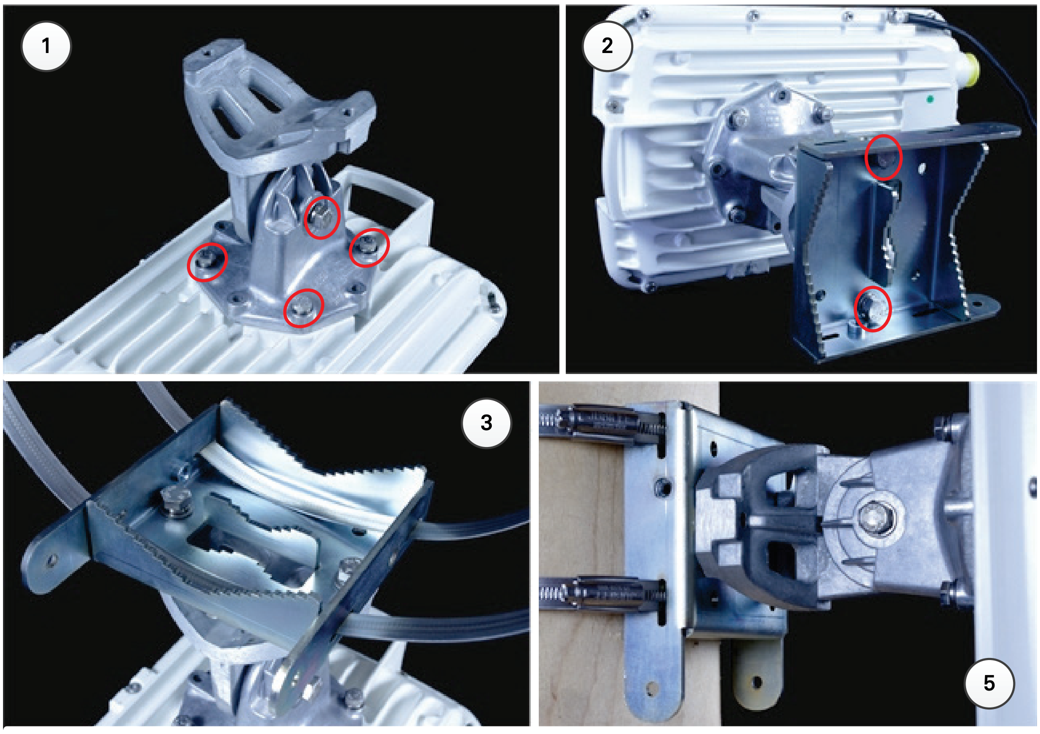
Extended integrated mounting bracket

1. Fix the mounting plate to the back of the ODU using the four M6 bolts, and spring and plain washers provided. Tighten the bolts to a torque setting of 5.0 Nm (3.7 lb ft). The step is common with the standard integrated bracket.
2. Attach the bracket body of the extended bracket on the mounting plate on the ODU to using the M8 bolt and spring and plain washer.
3. Hoist the ODU to the mounting position.
4. Select the correct clamp. The larger clamp is intended for poles of diameter 114 mm (4.5 inches). The smaller clamp is intended for poles of diameter 89 mm (3.5 inches).
5. Attach the bracket body to the pole using the selected bracket clamp, washers and M8 bolts.
6. Adjust the elevation and azimuth to achieve visual alignment. Tighten all three M8 bracket bolts to a torque setting of 8.0 Nm (6.0 lb ft). Do not over-tighten the bolts as this may lead to failure of the assembly.



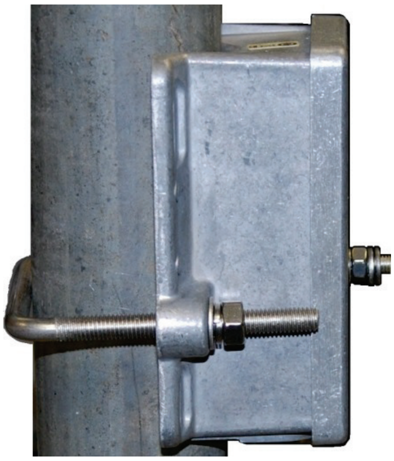
Mounting bracket (integrated) with large diameter extension kit

1. Fix the mounting plate to the back of the ODU using the bolts and washers provided. Tighten the four bolts to a torque setting of 5.0 Nm (3.7 lb ft). Attach the bracket body to the mounting plate using the M8 bolt and spring and plain washer. This is equivalent to the first two steps for the standard integrated bracket.
2. Attach the adaptor plate of the large diameter extension kit to the bracket body using the bolts and washers provided. Tighten the two bolts to a torque setting of 5.0 Nm (3.7 lb ft).
3. Feed the Jubilee straps through the slots in the adaptor plate.
4. Hoist the ODU to the mounting position.
5. Attach the adaptor plate to the pole using the Jubilee straps.
6. Adjust the azimuth to achieve visual alignment. Tighten the Jubilee straps to a torque setting of 6.0 Nm (4.5 lb ft).
7. Adjust the elevation to achieve visual alignment. Tighten M8 bracket bolt to a torque setting of 8.0 Nm (6.0 lb ft). Do not over-tighten this bolt as this may lead to failure of the assembly.

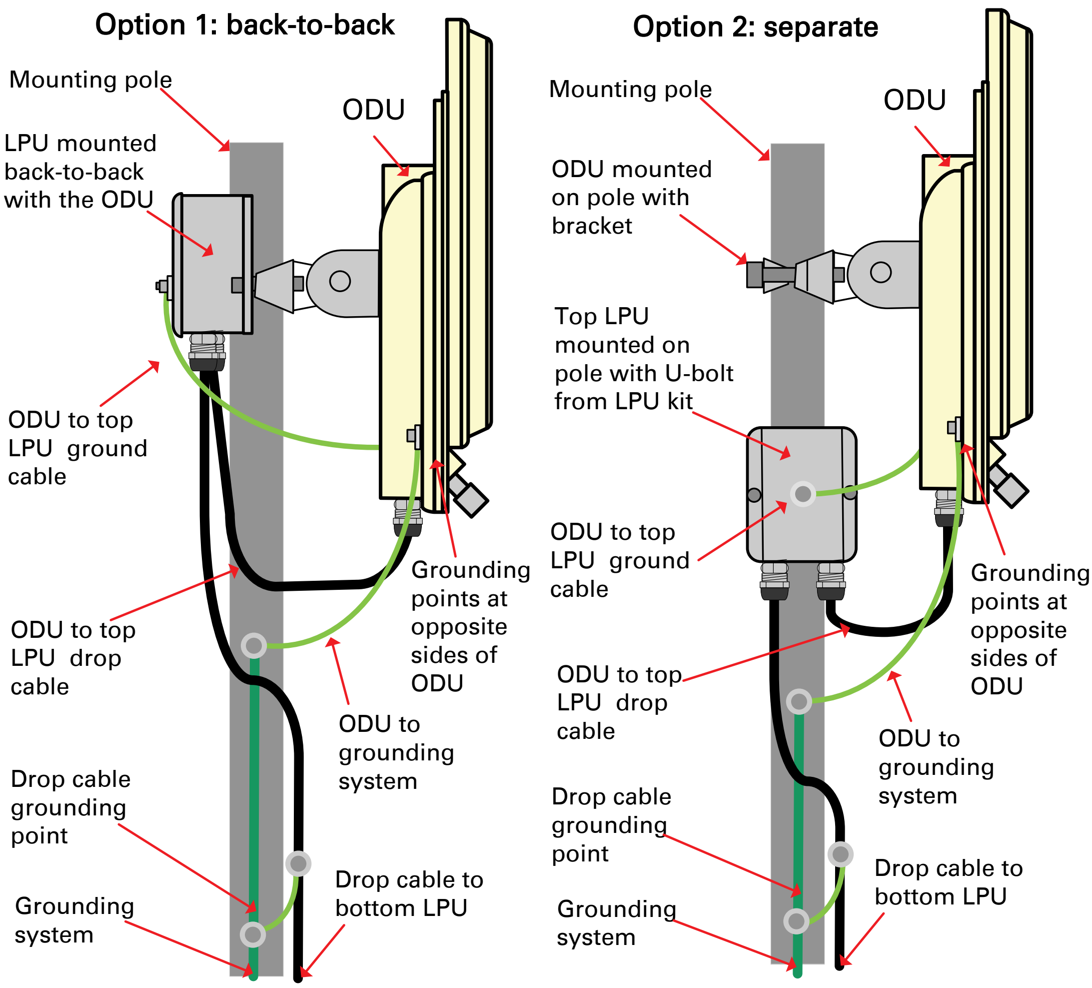


Mount the top LPU

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 7.0 Nm (5.2 lb ft):

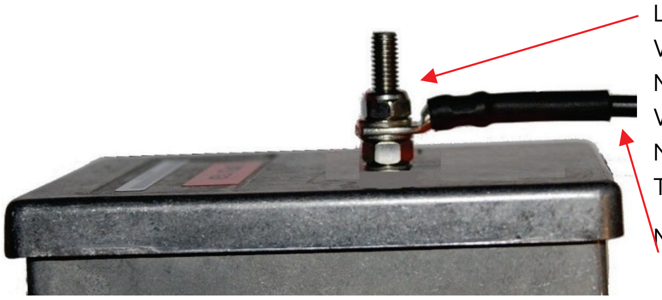


Interconnect and ground the ODU and top LPU



Attention Do not attach grounding cables to the ODU mounting bracket bolts, as this arrangement will not provide full protection.

1 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):



2 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.

3 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

To mount and connect an external antenna, proceed as follows:

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.

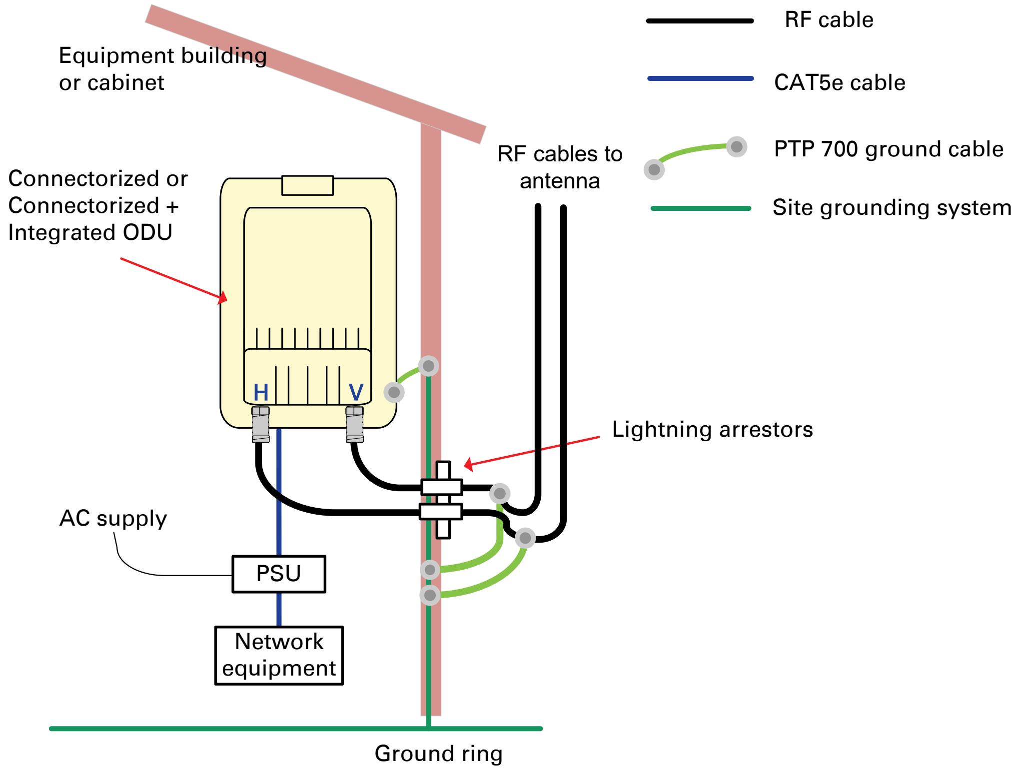
2 Connect the ODU V and H interfaces to the antenna(s) with RF cable of type LMR-400 (Cambium part numbers 30010194001 and 30010195001) and N type connectors (Cambium part number 09010091001). Tighten the N type connectors to a torque setting of 1.7 Nm (1.3 lb ft).

3 If the ODU is mounted indoors, install lightning arrestors at the building entry point:

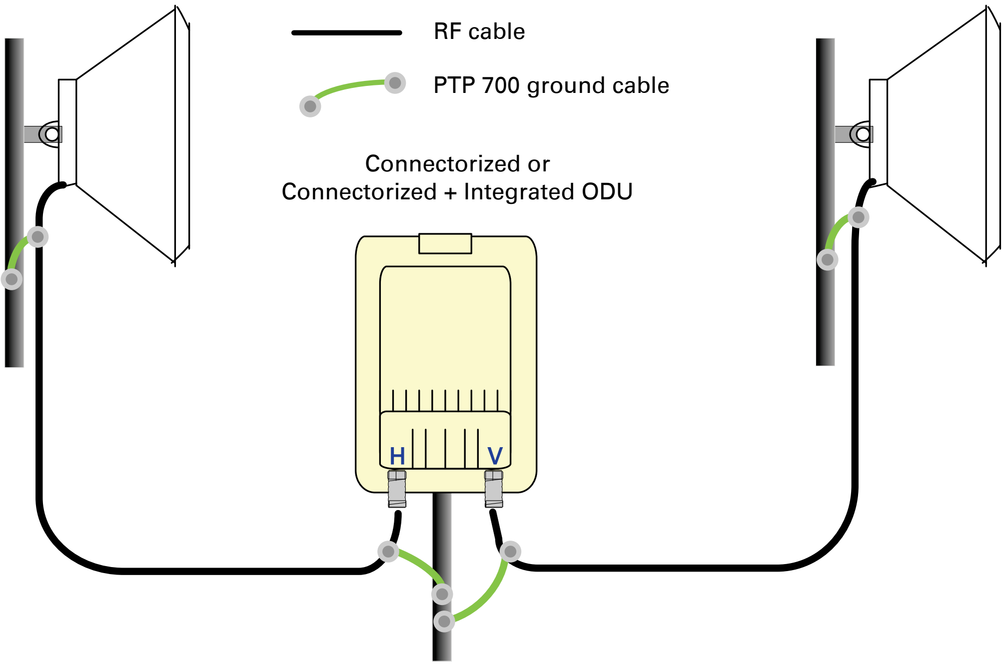
4 Form drip loops near the lower ends of the antenna cables. These ensure that water is not channeled towards the connectors.

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. 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

To install the copper Cat5e Ethernet interface, use the following procedures:

- Install the ODU to top LPU drop cable on page 5-38
- Install the main drop cable on page 5-40
- Install the bottom LPU to PSU drop cable on page 5-43
- Test resistance in the drop cable on page 5-45

Attention 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.

Attention Do not connect the SFP or Aux drop cables to the PSU, as this may damage equipment.

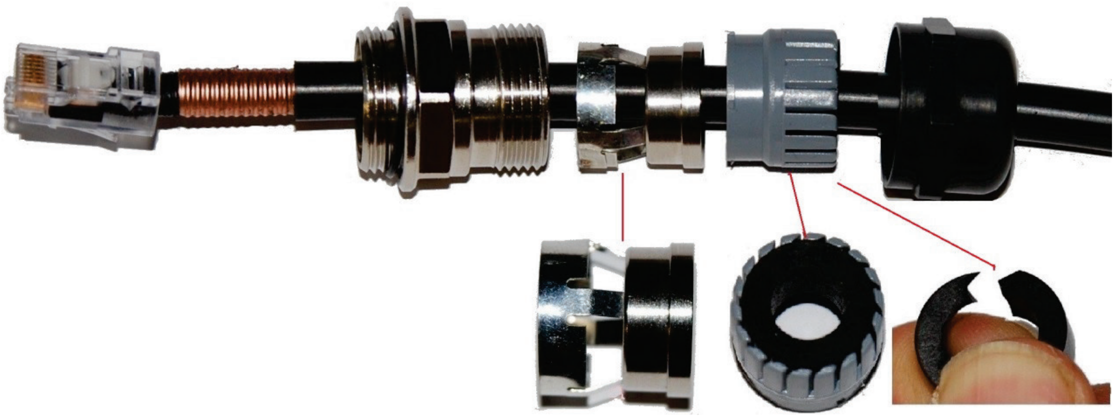
Attention Always use Cat5e cable that is gel-filled and shielded with copper-plated steel. Alternative types of Cat5e cable are not supported by Cambium Networks. Cambium Networks supply this cable (Cambium part numbers WB3175 and WB3176), RJ45 connectors (Cambium part number WB3177) and a crimp tool (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

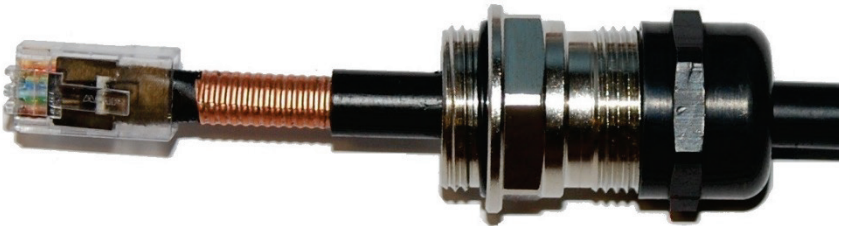
Fit glands to the ODU to top LPU drop cable

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.

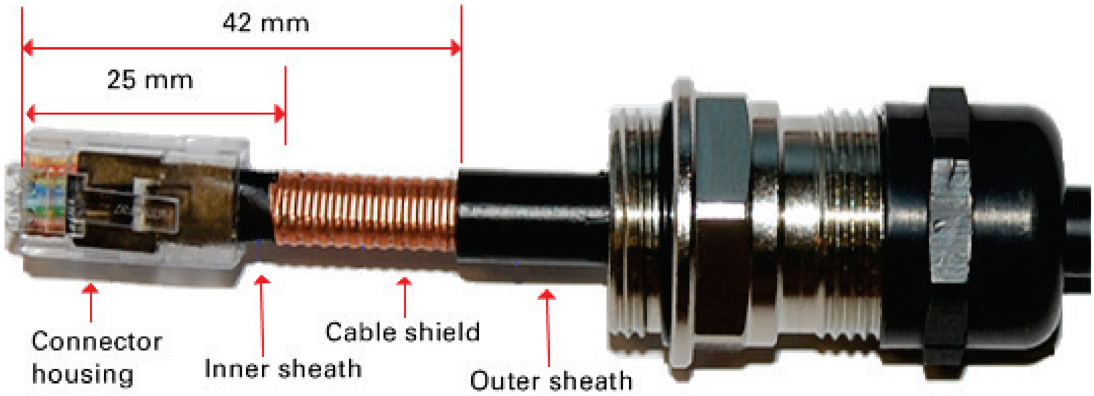
Terminate with RJ45 connectors and glands

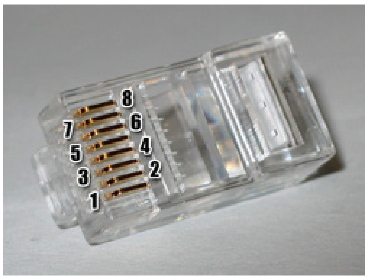
Attention Check that the crimp tool matches the RJ45 connector, otherwise the cable or connector may be damaged.

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:



Pin	Color (Supplied cable)	Color (Conventional)	Pins on plug face
1	Light Orange	White/Orange	
2	Orange	Orange	
3	Light Green	White/Green	
4	Blue	Blue	
5	Light Blue	White/Blue	
6	Green	Green	
7	Light Brown	White/Brown	
8	Brown	Brown	

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.

Attention 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 5-39.
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

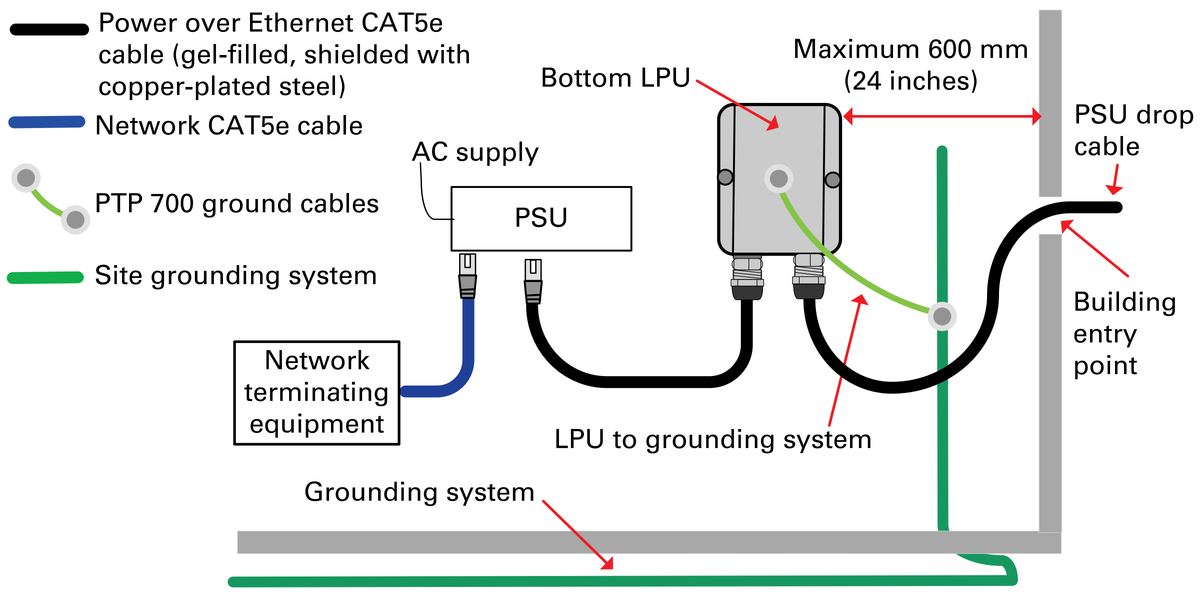
At all required grounding points, connect the screen of the main drop cable to the metal of the supporting structure using the cable grounding kit (Cambium part number 01010419001).

Install the bottom LPU to PSU drop cable

Install the bottom LPU

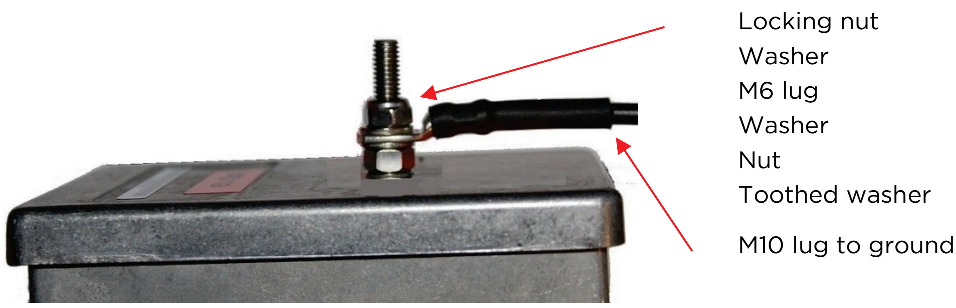
Install the bottom LPU, ground it, and connect it to the main drop cable.

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 5-39.

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.

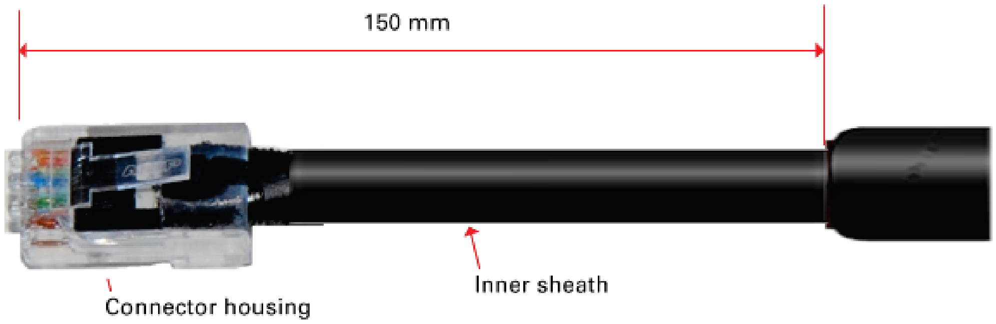
Attention Check that the crimp tool matches the RJ45 connector, otherwise the cable or connector may be damaged.

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 5-41.
- 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 5-39.

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 suitable 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.

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):

- AC+DC Enhanced Power Injector 56V (Cambium part number C000065L002C). Refer to Installing the AC+DC Enhanced Power Injector 56V on page 5-46.
- Cluster Management Module (CMM5). Refer to Installing the CMM5 on page 5-48.

Warning Always use an appropriately rated and approved AC supply cord-set in accordance with the regulations of the country of use.

Attention 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.

Attention Do not plug any device other than a PTP 700 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 700 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+DC Enhanced Power Injector 56V

Follow this procedure to install the AC+DC Enhanced Power Injector 56V (Cambium part number C000065L002C):

1 Mount the AC+DC Power Injector 56V by screwing it to a vertical or horizontal surface using the four screw holes (two 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 or the cable from the PTP-SYNC 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 the CMM5

Installation instructions for the CMM5 are provided in *PMP Synchronization Solutions User Guide* available from the Cambium web site.

Installing a PTP-SYNC unit

To install a PTP-SYNC unit (for TDD synchronization), use the following procedures:

- Mounting the PTP-SYNC unit on page 5-49
- Connecting up the PTP-SYNC unit on page 5-50
- Powering up the PTP-SYNC installation on page 5-52

Attention The PTP-SYNC unit must be installed indoors in a non-condensing environment, otherwise it will be prone to water damage.

Attention To protect the PTP-SYNC from damage, disconnect the power supply from the PSU before connecting up the PTP-SYNC.

Mounting the PTP-SYNC unit

Use this procedure to install the PTP-SYNC unit in the equipment building, either in a rack or on a wall.

- Racking mounting option: fix the PTP-SYNC to the rack mount using the M3 screws from the rack mount installation kit (Figure 108).
- Wall mounting option: mount the PTP-SYNC vertically with interfaces and cabling facing downwards (Figure 109).

Figure 108 PTP-SYNC mounted in a rack

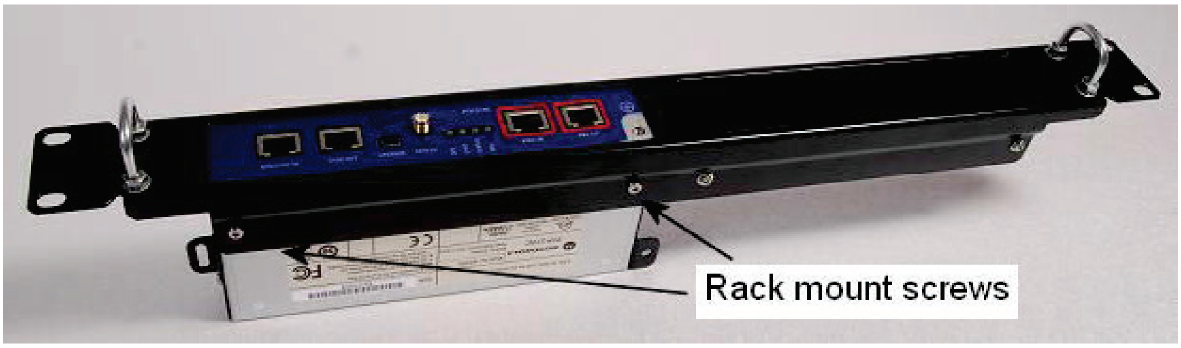
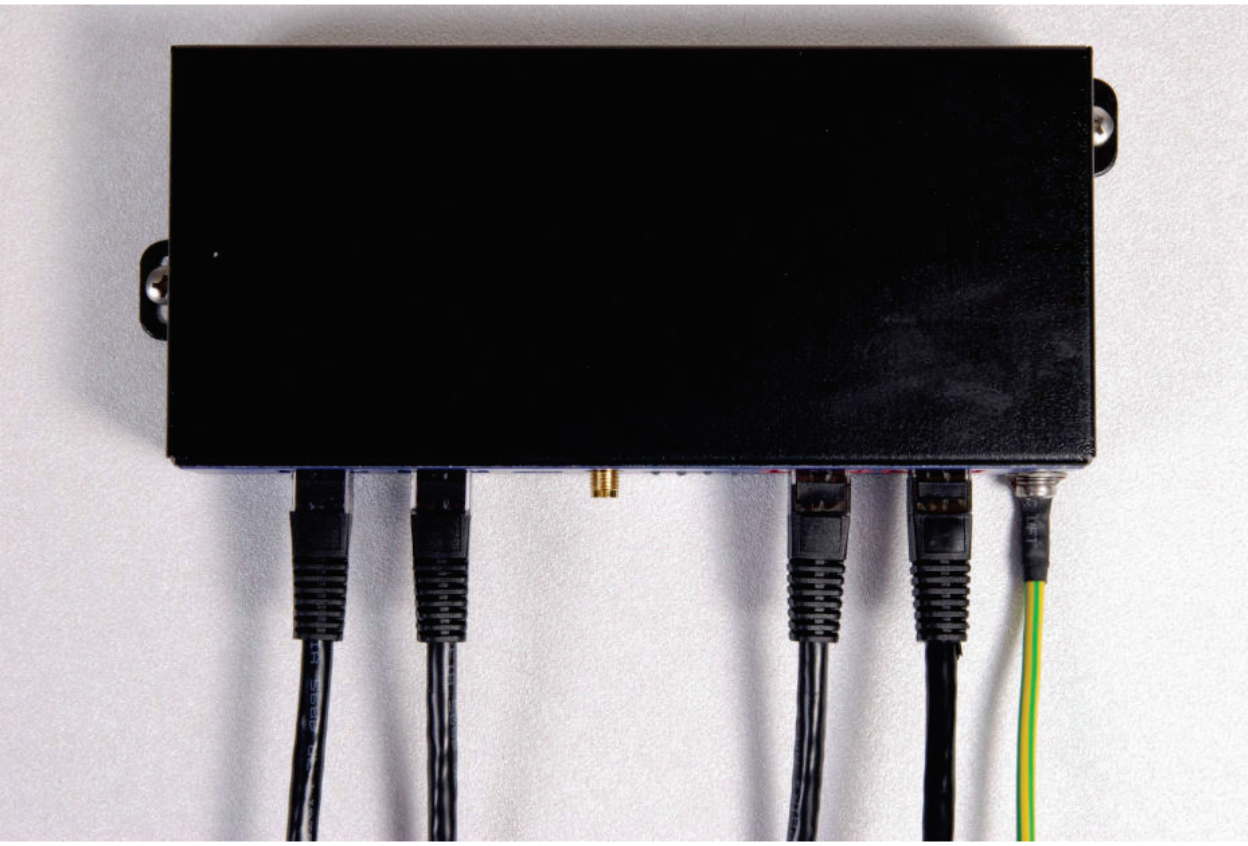


Figure 109 PTP-SYNC mounted on a wall

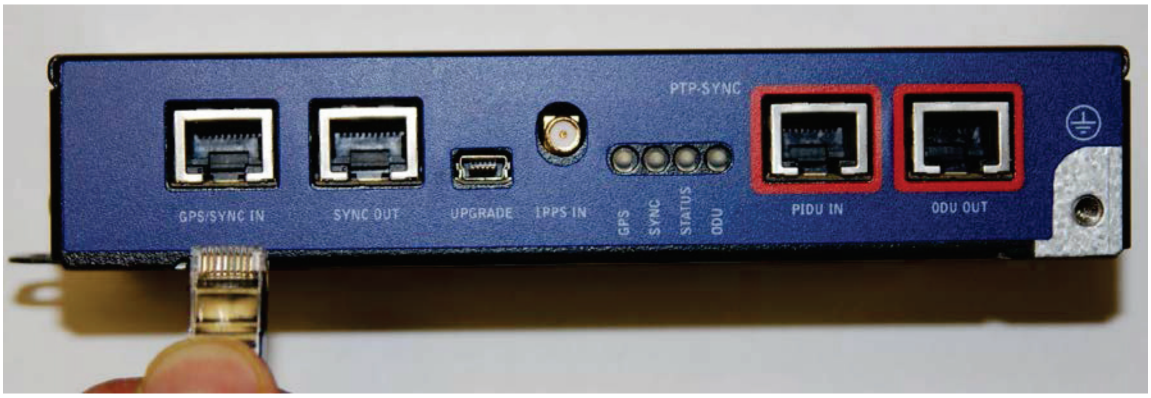


Connecting up the PTP-SYNC unit

Use this procedure to connect the PTP-SYNC to the AC+DC Power Injector 56V, ODU, GPS receiver (if fitted), and LPU (if fitted).

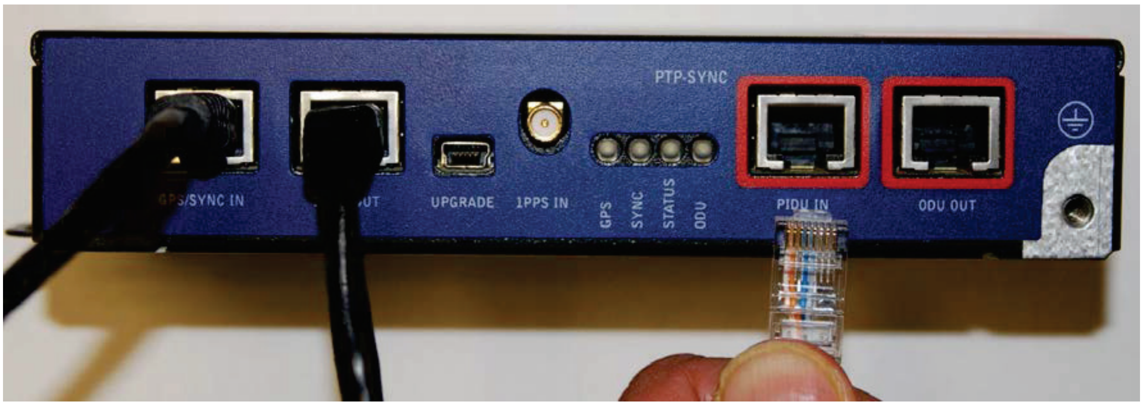
1 Disconnect the power supply from the AC+DC Power Injector 56V.

2 If using GPS, connect the cable from the GPS unit to the GPS/SYNC IN port.



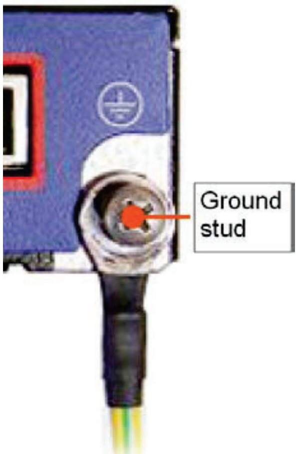
3 To link clustered PTP-SYNC units, connect the SYNC OUT port of the first PTP-SYNC to the GPS/SYNC IN port of the second PTP-SYNC in the chain. Repeat for subsequent PTP-SYNC units in the chain.

4 Connect the cable from the PSU to the PIDU IN port. A suitable 1 meter cable is included in the PTP-SYNC kit.



5 Connect the cable from the ODU to the ODU OUT port.

6 Use a grounding cable to connect the ground stud of the PTP-SYNC to the master ground bar of the building, or to the rack ground bar.



Powering up the PTP-SYNC installation

Use this procedure to power up the PTP-SYNC installation.

Attention Ensure that all cables are connected to the correct interfaces of the PTP SYNC unit and the GPS receiver (if used). Ensure that the installation is correctly grounded Failure to do so may result in damage to the equipment.

1 Connect the power supply to the PSU.

2 Within 90 seconds, the PTP-SYNC STATUS LED should blink once every second to show that satellite lock has been achieved.

3 If the system does not operate correctly, refer to Testing PTP-SYNC on page 8-15.

Installing the Trimble Accutime GPS receiver

To install a GPS receiver as the timing reference source for PTP-SYNC, use the following procedures:

- Mounting the GPS receiver on page 5-53
- Preparing the GPS drop cable on page 5-53
- Assembling an RJ45 plug and housing for GPS on page 5-54
- Assembling a 12 way circular connector on page 5-56
- Connecting the GPS drop cable on page 5-60
- Top grounding point for GPS adapter cable on page 5-60
- Installing and connecting the GPS LPU on page 5-62

Attention A Prior to power-up of equipment, ensure that all cables are connected to the correct interfaces of the PTP-SYNC unit and the GPS receiver module. Failure to do so may result in damage to the equipment.

Mounting the GPS receiver

Mount the GPS receiver (following manufacturer's instructions) upon either an external wall (Figure 45) or a metal tower or mast (Figure 46).

Preparing the GPS drop cable

Use this procedure to make the main drop cable that will connect the GPS receiver to its bottom LPU. GPS drop cables do not require top LPUs.

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

1. Measure the distance from the GPS receiver to the LPU site at building entry.
2. Cut the required length of drop cable.
3. Attach one or more hoisting grips to the top end of the cable, as described in Install the main drop cable on page 5-40.

4 Fit a suitable GPS connector to the top end of the drop cable:

- If a GPS adapter cable kit is available, attach the plug housing and an RJ45 plug to the top end of the main GPS drop cable, as described in Assembling an RJ45 plug and housing for GPS on page 5-54.
- If a GPS adapter cable kit is not available, fit a 12 way circular connector to the top end of the main drop cable as described in Assembling a 12 way circular connector on page 5-56.

5 Hoist the GPS drop cable safely up a tower or building, as described in Install the main drop cable. on page 5-40.

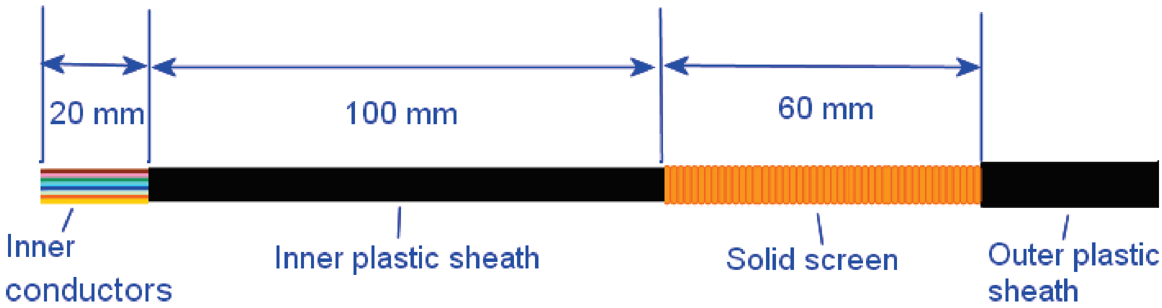
Assembling an RJ45 plug and housing for GPS

Use this procedure to assemble the plug housing over the end of the drop cable. This procedure is only performed when a GPS adapter cable kit is available. This kit is used to connect the Trimble Acutime™ GG GPS receiver or the Trimble Acutime™ Gold GPS receiver to the GPS drop cable.

The kit contains an adapter cable (GPS receiver circular connector to RJ45 socket) and an RJ45 plug housing. The plug housing should be assembled over the end of the drop cable to provide a sealed connection to the adapter cable.

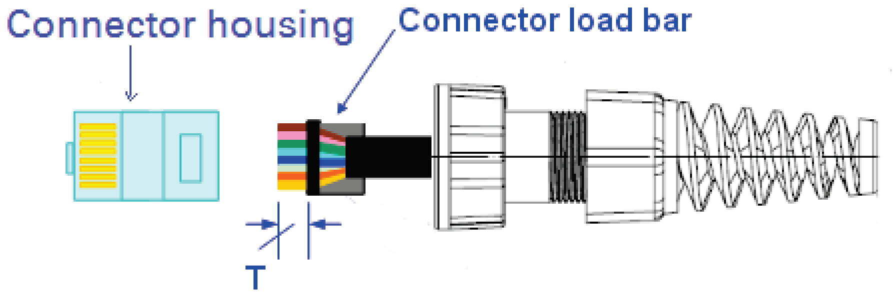
Note These instructions are for the preparation of the Cambium-supplied drop cable type (Superior Essex BBDGE). Other types of cable may need different preparation methods.

1 Prepare the top end of the GPS drop cable.



2 Install plug housing from the converter kit onto the prepared cable. Do not tighten the nuts at this stage.

3 Install the RJ45 crimp plug.



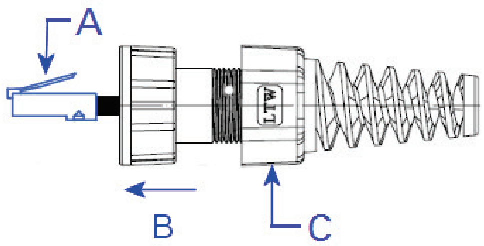
Start with tails over-length to assist insertion into load bar, then trim them to 5 mm (T). Connect the RJ45 pins to the following conductors (Superior Essex BBDGe colors):

4 Assemble plug housing:

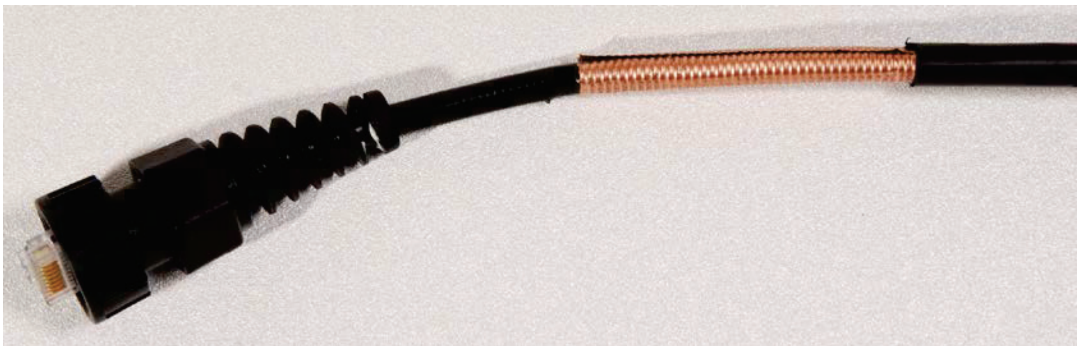
Depress the RJ45 locking tab (A).

Slide the plug housing assembly (B) over the RJ45 plug.

Tighten the sealing nut (C). This is easier to fully tighten when the plug housing is mated to the socket of the adapter cable.



5 Check the assembly. This is an exampled of an assembled plug housing on the end of a drop cable:



Assembling a 12 way circular connector

Use this procedure to connect the GPS drop cable to a 12 way circular connector. This procedure is only performed when a GPS adapter cable kit is NOT available.

Note This procedure requires a soldering iron and solder.

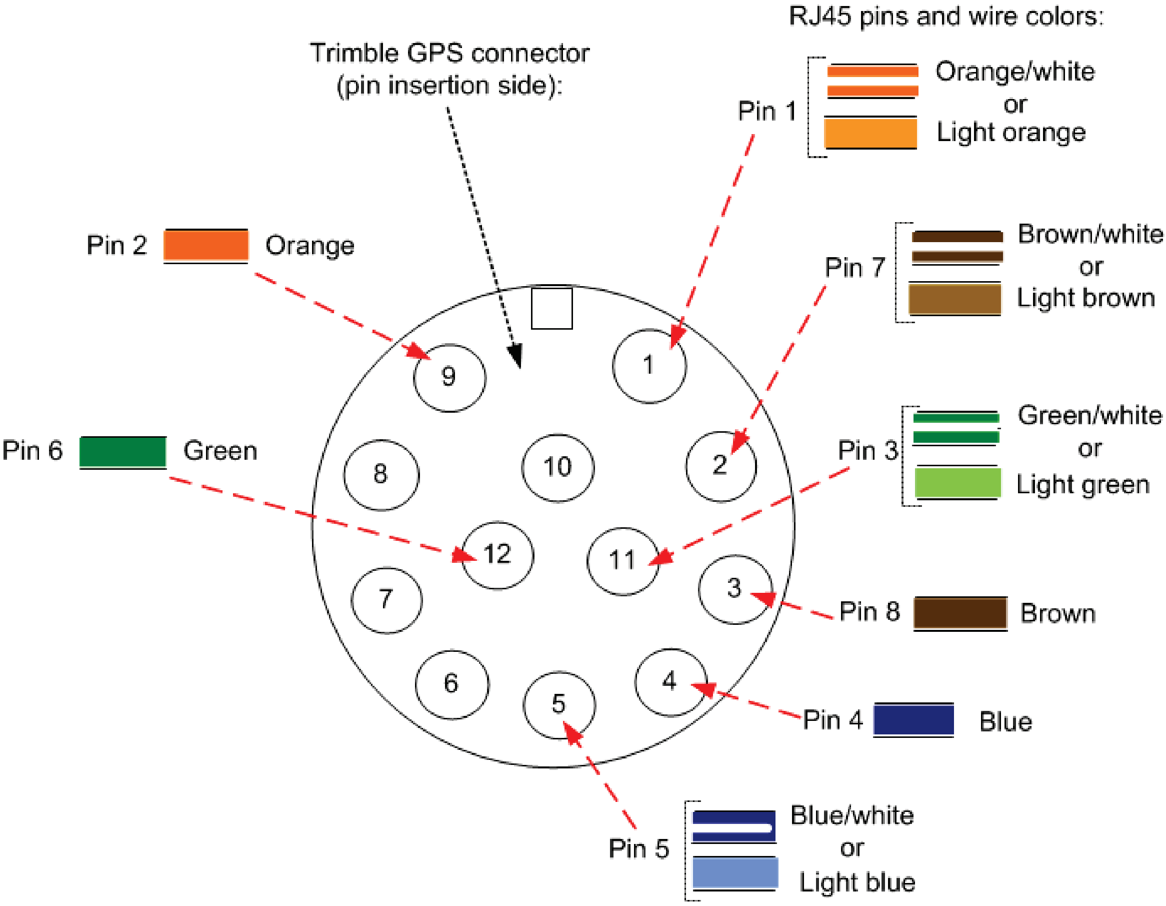
Attention The drop cable has solid copper conductors. There are a limited number of times each conductor can be bent before it fatigues and fails.

Table 124 shows how the 12 way circular connector locations map to the PTP-SYNC RJ45 pins. Figure 110 illustrates this mapping.

Table 124 GPS 12 way circular connector to RJ45 pin mappings

GPS connector location	Function	Cat5e wire color		PTP-SYNC (J10) RJ45 pin	PTP-SYNC signal name
		Conventional	Supported drop cable		
1	DC Pwr (12V)	Orange/White	Light Orange	1	12VGPS
2	RxB-	Brown/White	Light Brown	7	GPS_TXDA
3	RxB+	Brown	Brown	8	GPS_TXDB
4	TxB-	Blue	Blue	4	GPS_RXDA
5	TxB+	Blue/White	Light Blue	5	GPS_RXDB
6	RxA-	N.C	N.C	---	
7	RxA+	N.C	N.C	---	
8	TxA-	N.C	N.C	---	
9	DC Ground	Orange	Orange	2	GND
10	TxA+	N.C	N.C	---	
11	Tx1PPS+	Green/White	Light Green	3	GPS_1PPSA
12	Tx1PPS-	Green	Green	6	GPS_1PPSB

Figure 110 Inserting RJ45 pins into the 12 way circular connector



1 Prepare the drop cable end as follows:

- Bare back the cable outer and copper screen to 50mm.
- Bare back the cable inner to 17mm.
- Un-twist the cable pairs.
- Strip the individual conductors to 5mm.

2 Fit the plug outer, associated boot, and boot insert.

3 Connect the socket contacts using either of the following techniques:

- Crimp: Crimp the socket contacts onto each of the conductors using the correct crimp tool and positioner, setting the wire size selector to “3” for 24AWG wire.

- Solder: When soldering the socket contacts onto each of the conductors, ensure that there is no solder or flux residue on the outside of the contact. Care should also be taken that the individual conductor insulation does not peel back with the soldering heat, allowing possible shorts when assembled into the plug shell.

4 Fit four dummy contacts into the unused 12 way circular connector locations (6, 7, 8 and 10), to provide strength and sealing. Push the contacts in from the pin insertion side.

Pin insertion side:

Plug mating side:

5 Insert the eight RJ45 contact pins into the pin insertion side of the 12 way circular connector in accordance with Figure 110.

It is easiest to insert the pins from the center out, in descending order of Trimble location number, that is, 12, 11, 9, 5, 4, 3, 2, 1. Push the contacts in so that the shoulder on the contact fits into the hole in the plug shell. When all contacts have been fitted, push them in further to engage with the locking mechanism in the plug shell. This can be done by applying pressure to the contact with a small diameter stiff object, such as tweezers.

Note If a contact is pushed in to the point where the locking mechanism engages before all of the contacts have been inserted it will limit the amount of room availabl to fit the remaining contacts, requiring harder bends to be applied.

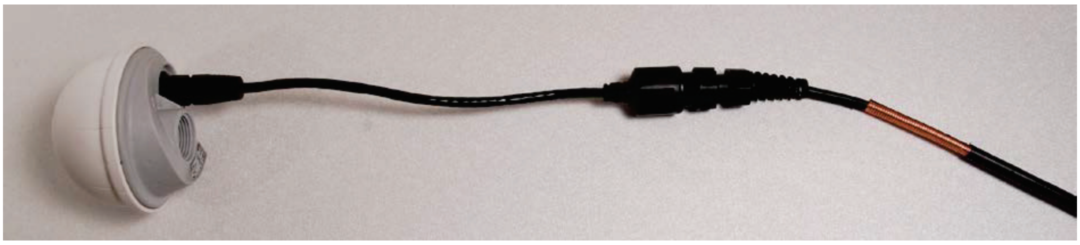
6 Fit the plug to its shell. The plastic ring fits inside the rubber boot and ensures a tight fit when the plug body is clipped onto the plug shell. Be aware that the plug body is a hard push fit onto the plug shell.

7 Fit the strain relief clip.

Connecting the GPS drop cable

Use this procedure to connect the GPS drop cable to the GPS unit and supporting structure.

1 If a GPS adapter cable is available, use it to connect the main GPS drop cable to the GPS unit:



2 If a GPS adapter cable is not available, connect the main GPS drop cable to the GPS unit via a 12 way circular connector. Weatherproof the connection as follows:

- Wrap a layer of self-amalgamating tape, starting 25mm below the bared back outer of the cable and finishing at the GPS housing.
- Wrap a layer of PVC tape, starting just below the start of the self-amalgamating tape and finishing at the GPS housing, overlapping at half width.
- Repeat with four more layers of PVC tape alternating the start and finish ends.

3 Lay the main drop cable as far as the building entry point, ensuring there is enough length to extend through the wall of the building to the LPU.

4 Attach the main GPS drop cable to the supporting structure using site approved methods.

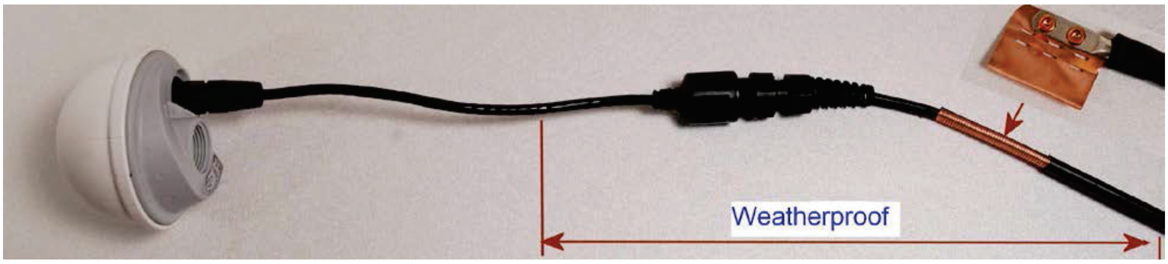
5 Ground the GPS drop cable to the supporting structure at the points shown in Figure 45 (wall installation) or Figure 46 (mast or tower installation):

- For standard grounding instructions, see Creating a drop cable grounding point on page 5-74.
- If a GPS adapter cable has been installed, see Top grounding point for GPS adapter cable on page 5-60.

Top grounding point for GPS adapter cable

If a GPS adapter cable has been installed (Figure 111), use this procedure to ground the drop cable at the point where the solid screen is already exposed, and weatherproof both the ground cable joint and the RJ45 connection.

Figure 111 Grounding and weatherproofing requirements for GPS adapter cable



Follow the procedure described in Creating a drop cable grounding point on page 5-74, but observe the following differences:

- There is no need to remove 60mm (2.5inches) of the drop cable outer sheath, as this has already been done.
- Wrap the top layer of self-amalgamating tape around the complete assembly (not just the ground cable joint), including the RJ45 connection with the GPS adapter cable (Figure 112).
- Wrap all five layers of PVC tape around the complete assembly (Figure 113). Wrap the layers in alternate directions: (1st) bottom to top; (2nd) top to bottom; (3rd) bottom to top; (4th) top to bottom; (5th) 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.
- Check that the joint between the GPS adapter cable, drop cable and ground cable is fully weatherproofed (Figure 114).

Figure 112 Wrapping self-amalgamating tape around the GPS adapter cable joint

Figure 113 Wrapping PVC tape around the GPS adapter cable joint

Figure 114 Grounding and weatherproofing example for GPS adapter cable

Installing and connecting the GPS LPU

Install and ground the GPS drop cable LPU at the building (or cabinet) entry point, and install the LPU-PTP-SYNC drop cable, as described in Install the bottom LPU on page 5-43.

Connect this cable to the PTP-SYNC unit as described in Connecting up the PTP-SYNC unit on page 5-50.

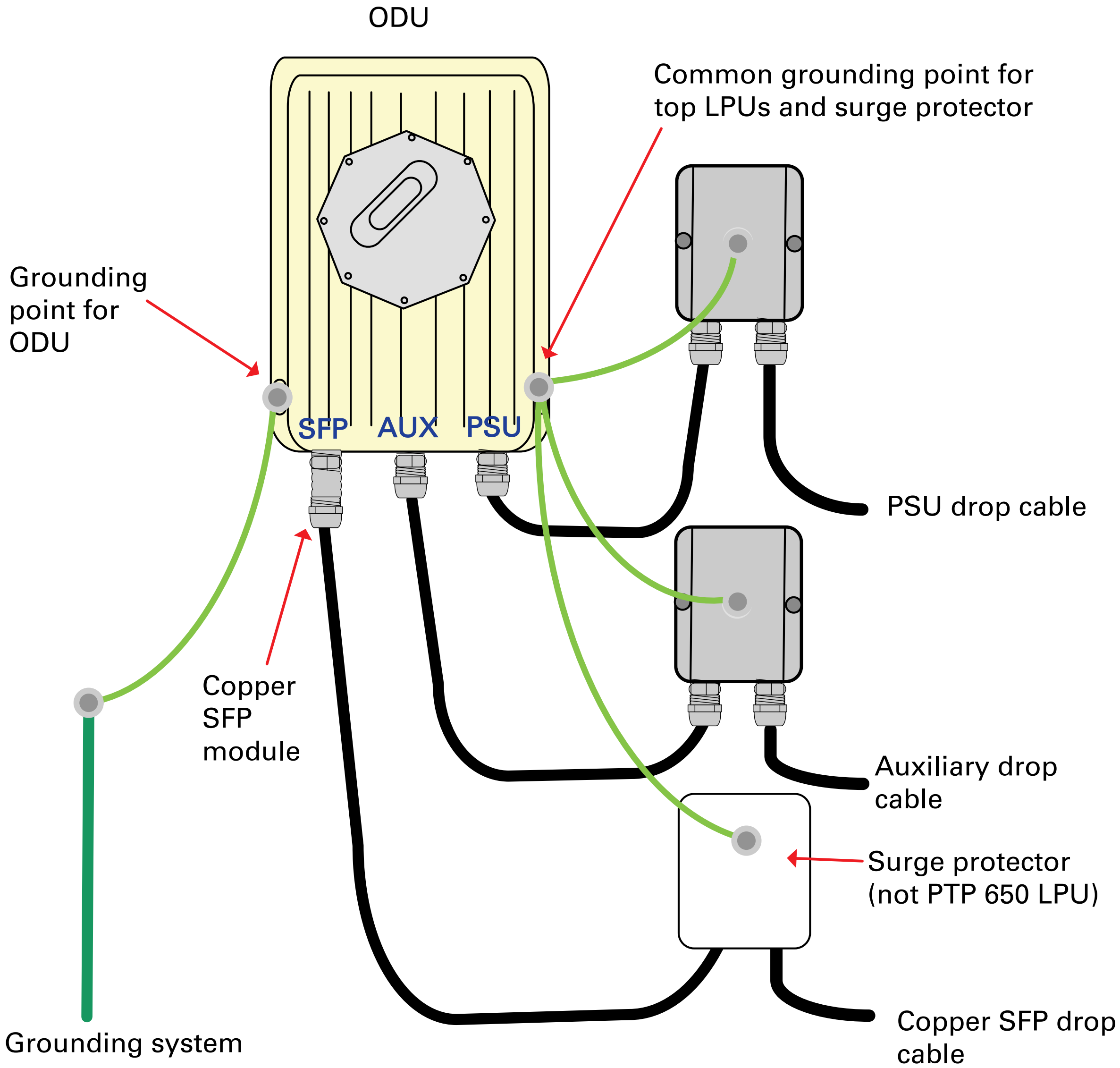
Installing an SFP Ethernet interface

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 5-65
  - Inserting the SFP module on page 5-66
  - Connecting the cable on page 5-68
  - Fitting the gland on page 5-69
  - Removing the cable and SFP module on page 5-71
- 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 700 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 115).

Figure 115 ODU with copper Cat5e connections to all three Ethernet ports



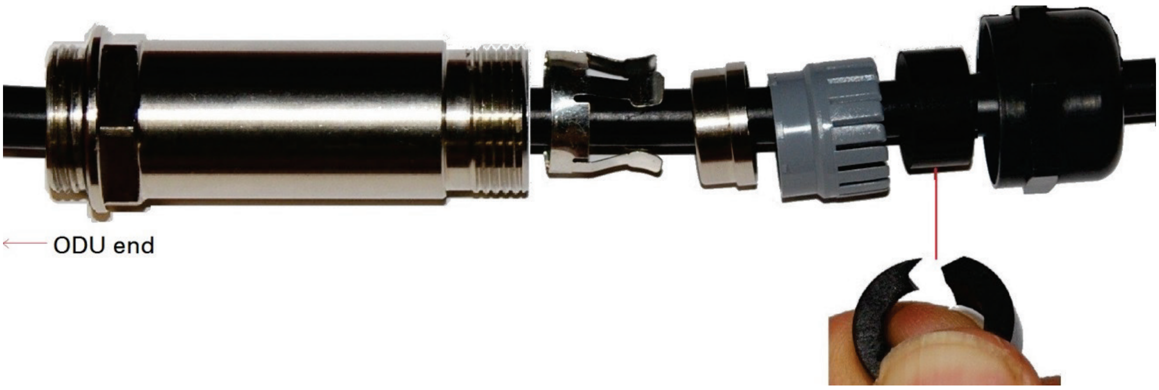
Fitting the long cable gland

Optical SFP interface: Disassemble the long cable gland and thread its components over the LC connector at the ODU end as shown below.

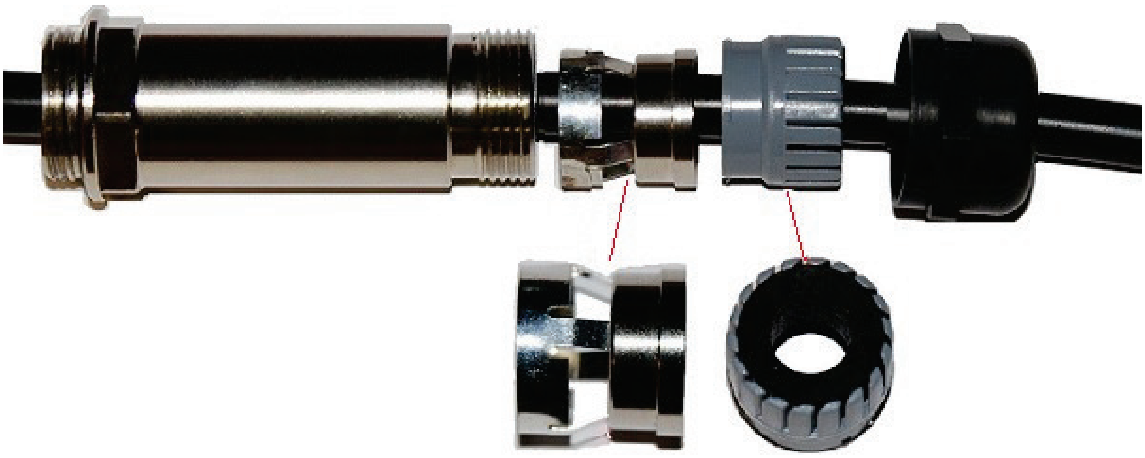
Copper Cat5e SFP interface: Disassemble the long cable gland and thread its components over the RJ45 connector at the ODU end as shown below.

1 Disassemble the gland:

2 Thread each part onto the cable (the rubber bung is split):

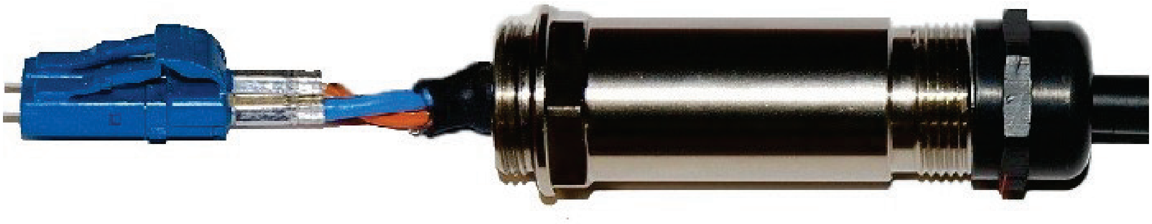


3 Assemble the spring clip and the rubber bung (the clips go inside the ring):



4 Fit the parts into the body and lightly screw on the gland nut (do not tighten it):

Optical

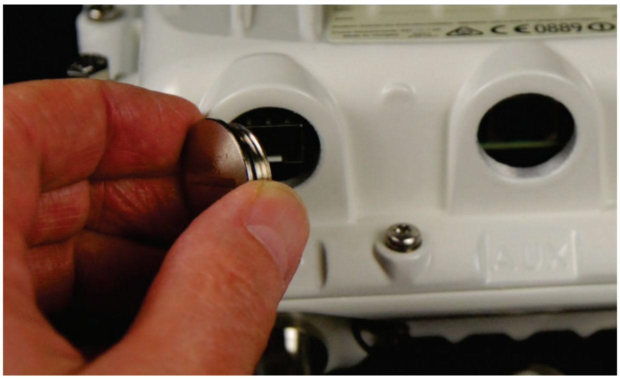


Copper

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

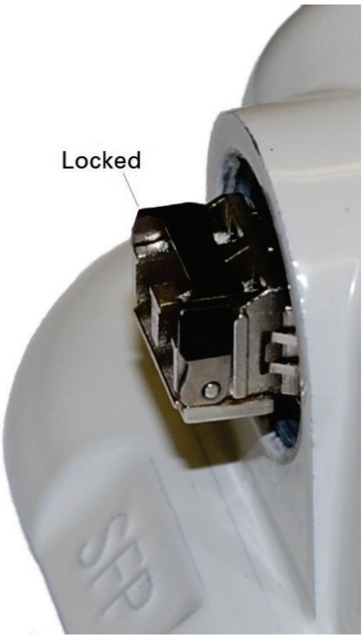
3 Push the module home until it clicks into place:

Optical

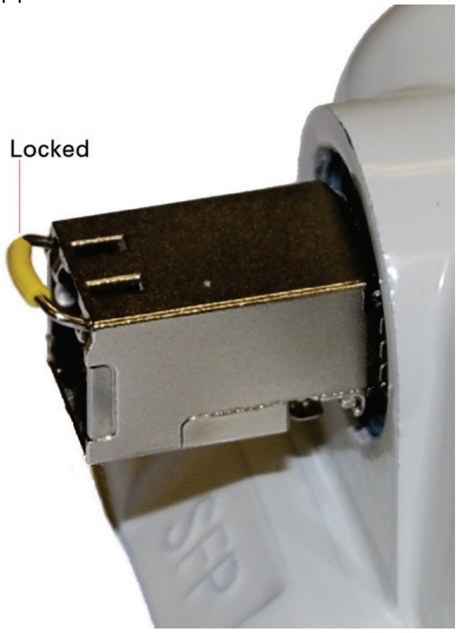
Copper

4 Rotate the latch to the locked position:

Optical



Copper

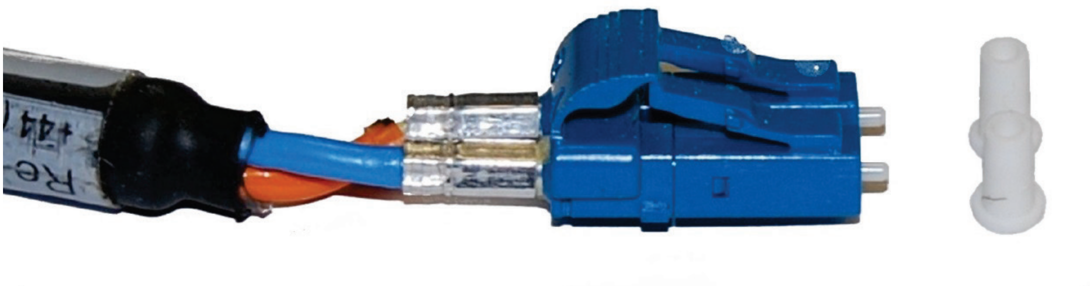


Connecting the cable

Attention 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:

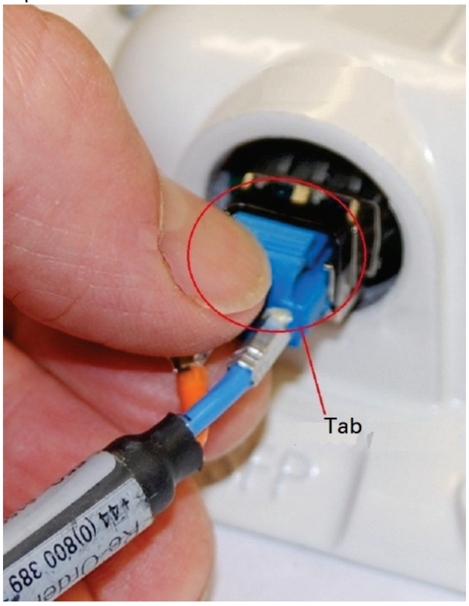

Correct
Incorrect

Removing the cable and SFP module

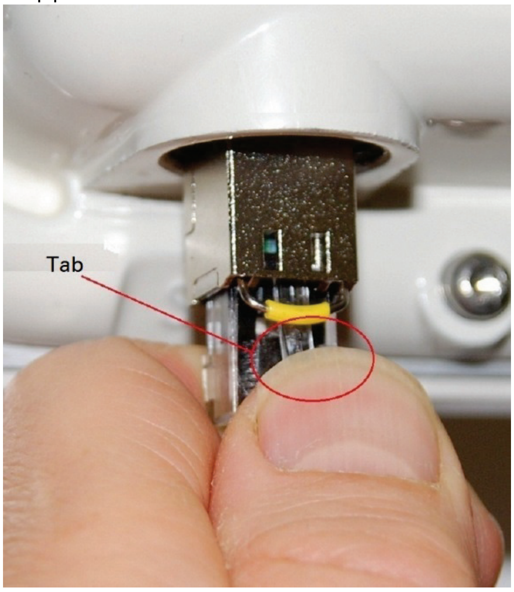
Do not attempt to remove the module without disconnecting the cable, otherwise the locking mechanism in the ODU will be damaged.

1 Remove the cable connector by pressing its release tab before pulling it out:

Optical

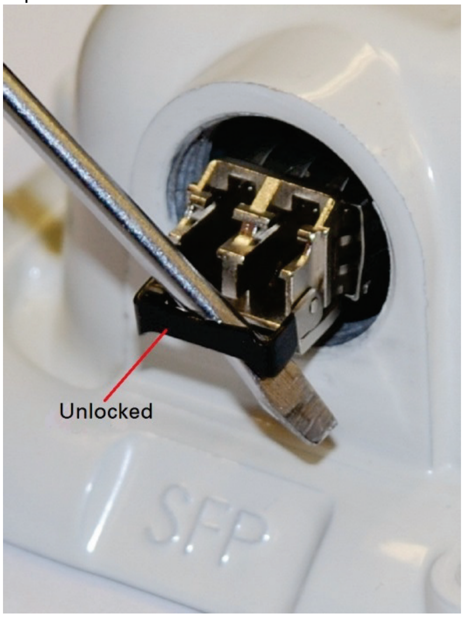


Copper

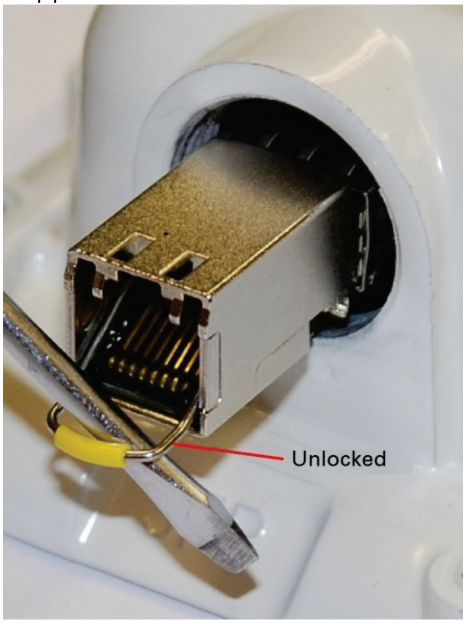


2 Rotate the latch to the unlocked position. Extract the module by using a screwdriver:

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:

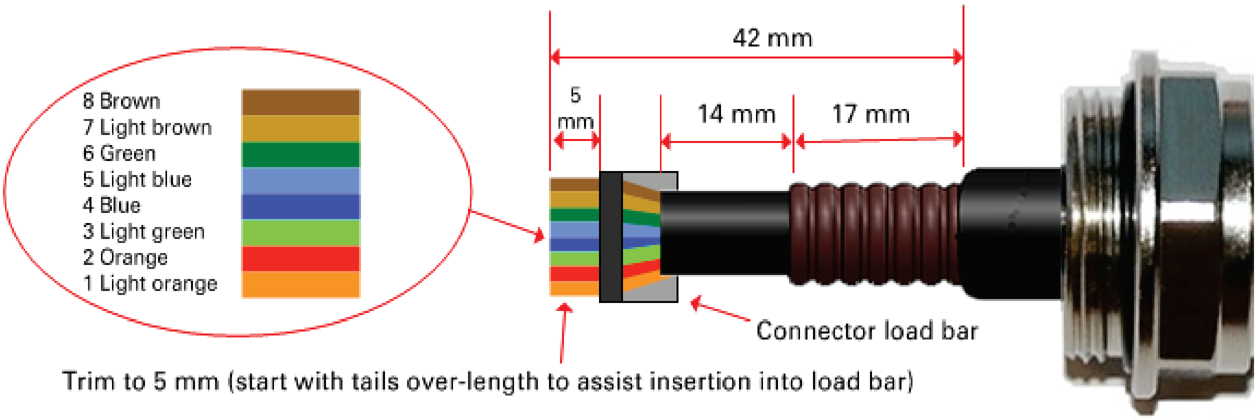
- At the remote end of the Aux drop cable, use an appropriate termination for the connected device (for example, a video camera or wireless access point).
- If the connected device is outdoors, not in the equipment building or cabinet, adapt the grounding instructions as appropriate.
- Ground the top LPUs and surge protector to the same point on the ODU (Figure 115).

Supplemental installation information

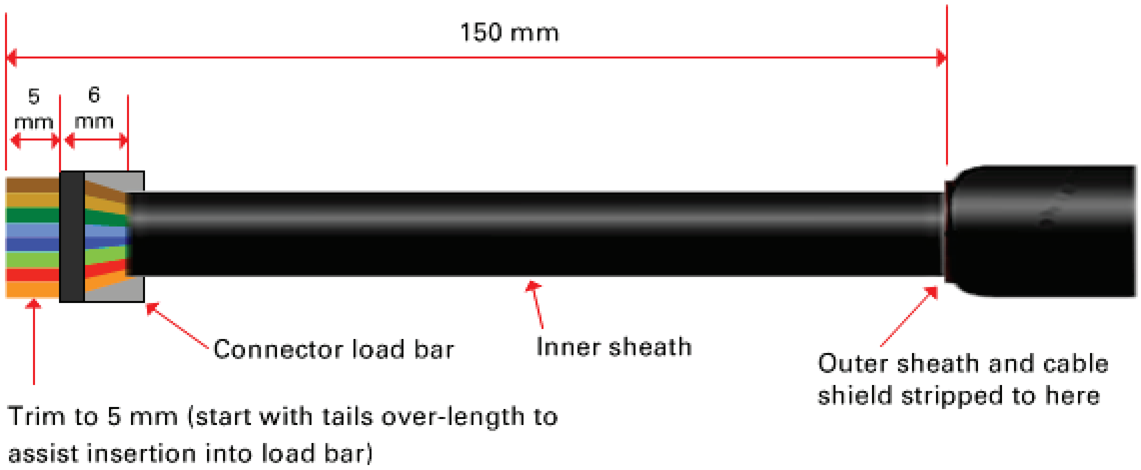
This section contains detailed installation procedures that are not included in the above topics, such as how to strip cables, create grounding points and weatherproof connectors.

Stripping drop cable

When preparing drop cable for connection to the PTP 700 ODU or LPU, use the following measurements:



When preparing drop cable for connection to the PTP 700 PSU (without a cable gland), use the following measurements:

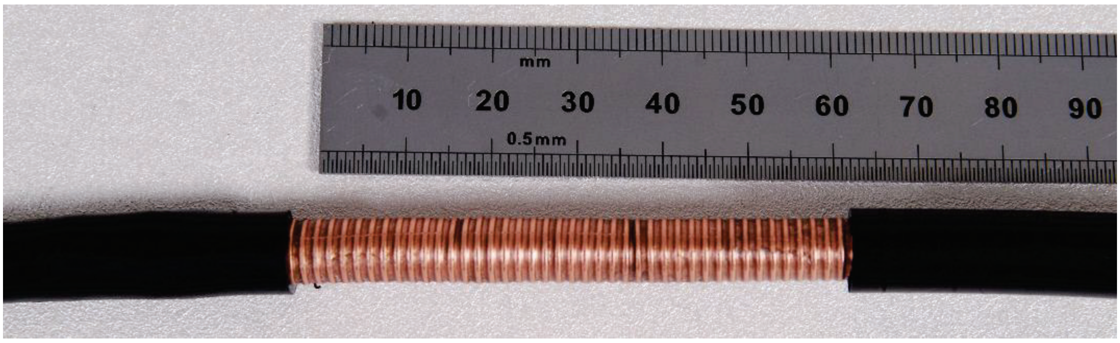


Creating a drop cable grounding point

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).

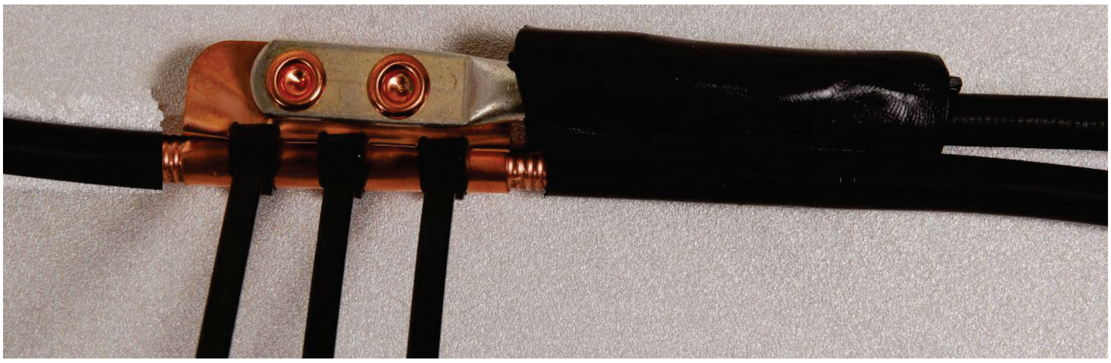
To identify suitable grounding points, refer to Drop cable grounding points on page 3-16.

1 Remove 60 mm (2.5 inches) of the drop cable outer sheath.

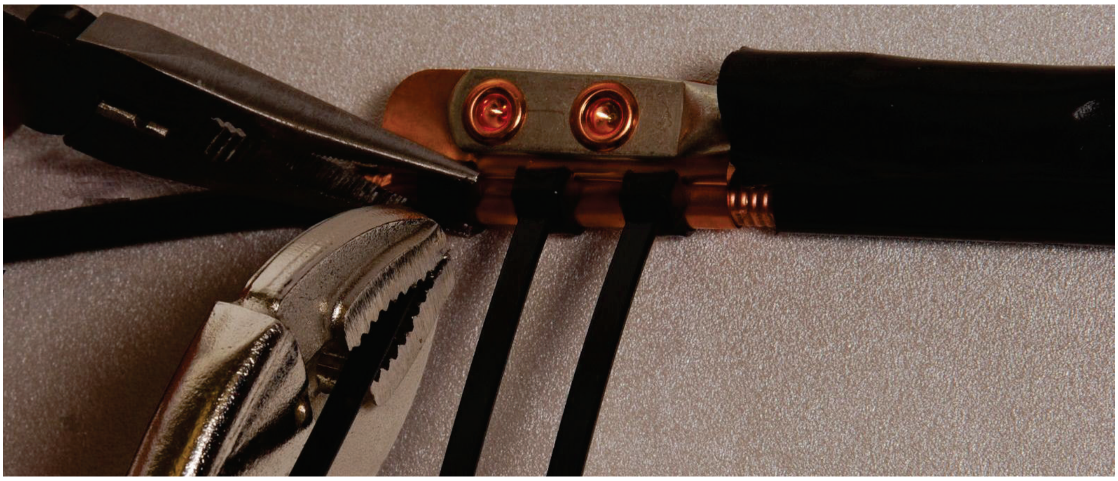


2 Cut 38mm (1.5 inches) of rubber tape (self-amalgamating) and fit to the ground cable lug. Wrap the tape completely around the lug and cable.

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.

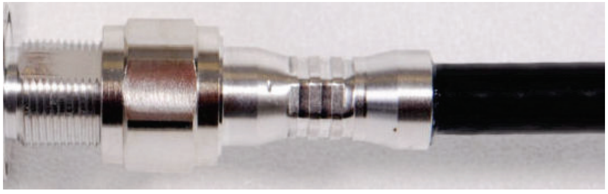
9 Prepare the metal grounding point of the supporting structure to provide a good electrical contact with the grounding cable clamp. Remove paint, grease or dirt, if present. Apply anti-oxidant compound liberally between the two metals.

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).

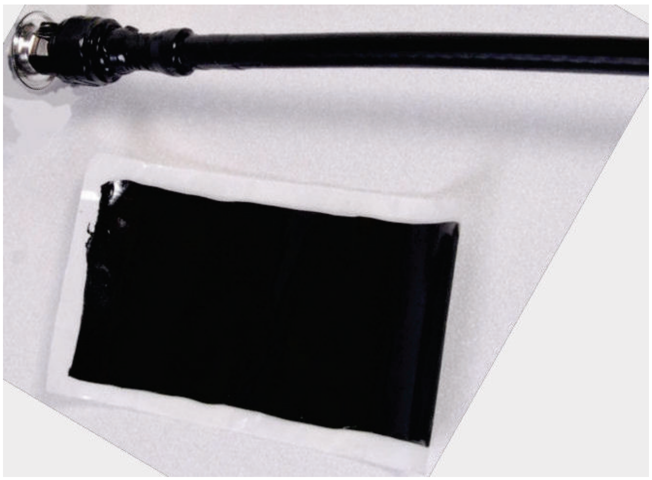
1 Ensure the connection is tight. A torque wrench should be used if available:



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:

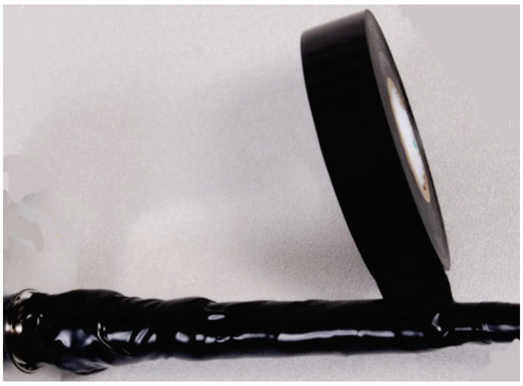
6 Press the tape edges together so that there are no gaps. The tape should extend 25 mm (1 inch) beyond the PVC tape:

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 56V 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 56V.

Chapter 6: Configuration and alignment

This chapter describes how to use the web interface to configure the PTP 700 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 4-20, 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 4-23.

Attention 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 7-41.

Selecting configuration options

Use the installation report to determine which configuration options are required. Refer to LINKPlanner on page 3-25.

Generating license keys

To obtain License Keys for capabilities that are not factory-installed, proceed as follows:

1. Identify and purchase the required entitlement for additional capabilities by referring to ODU capability upgrades on page 2-7.

2 Obtain the MAC Address of the ODU (it is on the System Status page).

3 Follow instructions, supplied in the email, to apply the entitlement to the ODU at the Cambium Networks support web site. Generated license keys are displayed in the License Keys page

Use the Software License Key page to configure the ODU with new license keys (Software License Key page on page 6-13).

Connecting to the unit

This section describes how to connect the unit to a management PC and power it up.

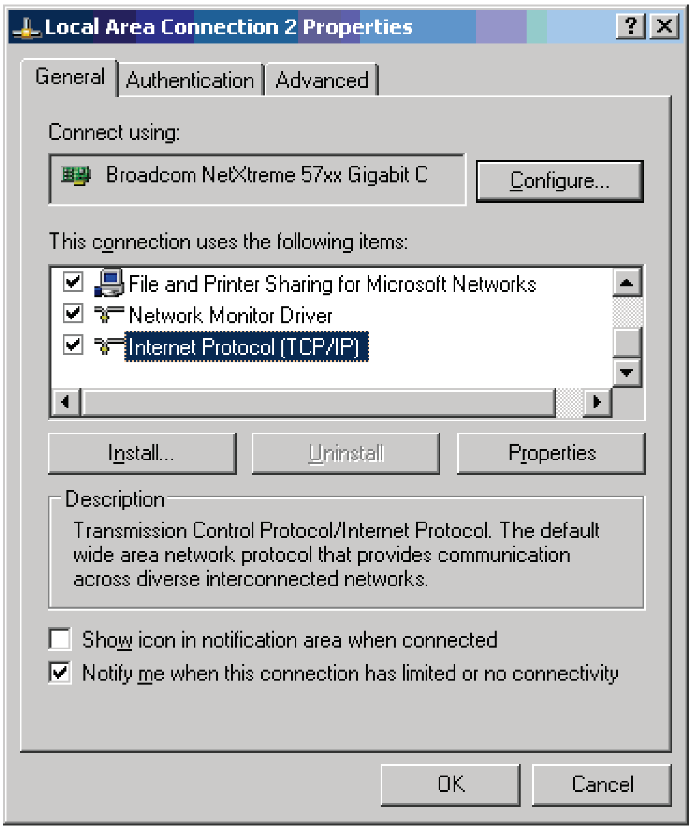
Configuring the management PC

Use this procedure to configure the local management PC to communicate with the PTP 700.

Procedure:

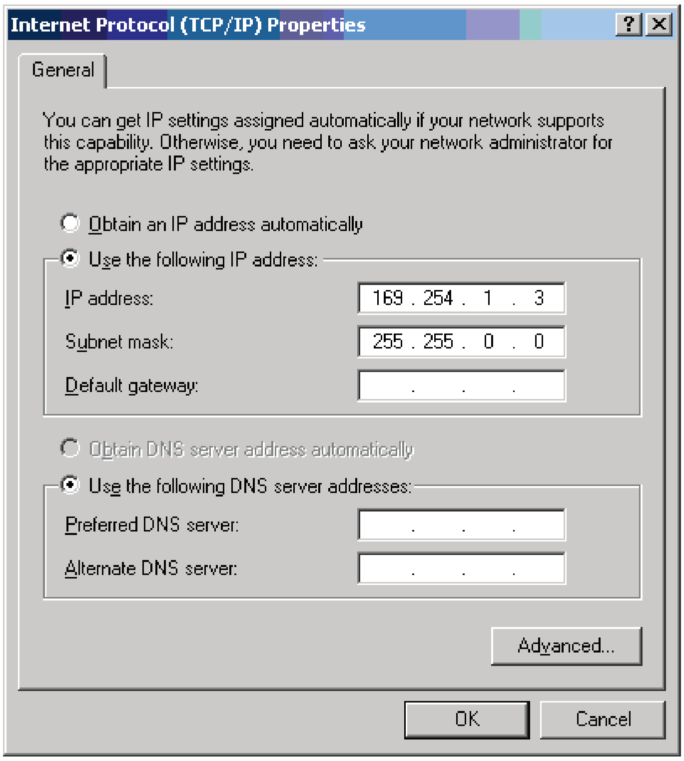
1 Select **Properties** for the Ethernet port. In Windows 7 this is found in **Control Panel > Network and Internet > Network Connections > Local Area Connection**.

2 Select **Internet Protocol (TCP/IP)**:



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:



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 700.

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 8-7.

Using the web interface

This section describes how to log into the PTP 700 web interface and use its menus.

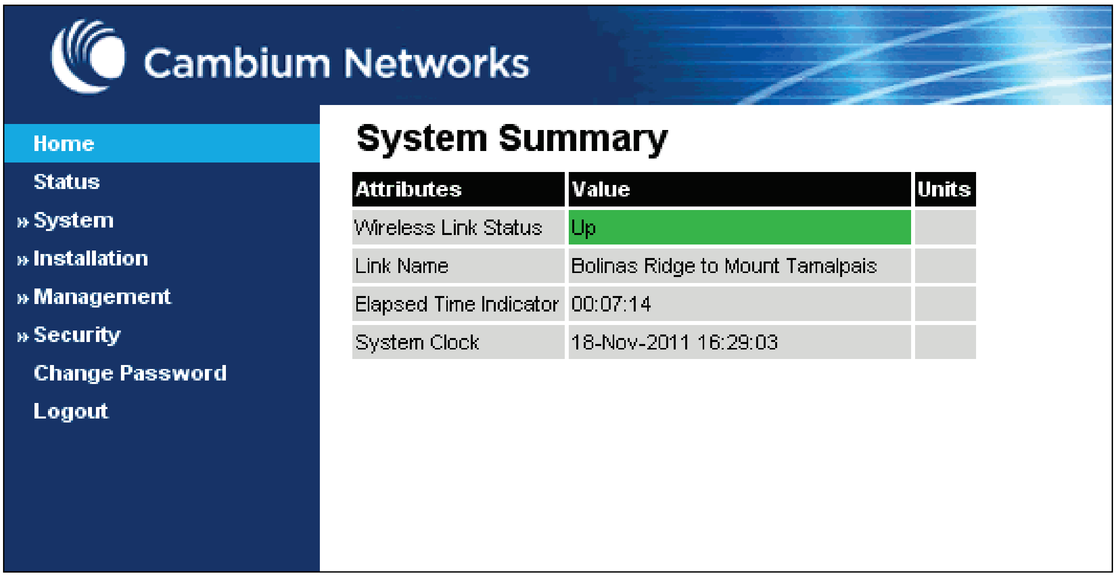
Logging into the web interface

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:



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):

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 125 to locate information about using each web page.

Table 125 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
Alarms		Alarms on page 7-18
System		
	Configuration	System Configuration page on page 6-42
	LAN Configuration	LAN Configuration page on page 6-46
	QoS Configuration	QoS Configuration page on page 6-55
	SFP Configuration	SFP Configuration page on page 6-58
	Whitelist Configuration	Authorization Control page on page 6-60
	Save and Restore	Save and Restore Configuration page on page 6-62
	Reset Configuration	Reset Configuration page on page 6-63
	Spectrum Expert or Spectrum Management	Spectrum Management on page 7-26
	Statistics	System Statistics page on page 7-52 Comparing actual to predicted performance on page 6-126
	Wireless Port Counters	Wireless Port Counters page on page 7-58 Test Ethernet packet errors reported by ODU on page 8-11
	Main Port Counters	Main Port Counters page on page 7-61
	Aux Port Counters	Aux Port Counters page on page 7-63
	SFP Port Counters	SFP Port Counters page on page 7-64
	SyncE Status	SyncE Status page on page 7-67
	Diagnostics Plotter	Diagnostics Plotter page on page 7-70
	CSV Download	Generate Downloadable Diagnostics page on page 7-71
	Cable Diagnostics	Cable Diagnostics on page 8-2

Main menu	Menu option	Web page information
	Software Upgrade	Software Upgrade page on page 6-64
	Reboot	Reboot Wireless Unit page on page 7-16
Installation		Installation menu on page 6-9
	Graphical Install	Graphical Install page on page 6-124
Management		
	Web	Web-Based Management page on page 6-68
	Local User Accounts	Local User Accounts page on page 6-70
	RADIUS Configuration	RADIUS Configuration page on page 6-75
	Login Information	Login Information page on page 7-16
	Web Properties	Webpage Properties page on page 6-76
	SNMP	SNMP pages (for SNMPv3) on page 6-88 SNMP pages (for SNMPv1/2c) on page 6-97
	Email	Email Configuration page on page 6-79
	Instant Messaging	Instant Messaging page on page 6-80
	Diagnostic Alarms	Diagnostic Alarms page on page 6-81
	Time	Time Configuration page on page 6-82
	Syslog	Syslog page on page 7-22
	Syslog Configuration	Syslog Configuration page on page 6-86
Security		Security menu on page 6-101
	Zeroize CSPs	Zeroize CSPs page on page 6-124
Change Password		Change Password page on page 7-17
Logout		Logging out on page 7-17

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.

Attention 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 7-41.

Starting the Installation Wizard

To start the Installation Wizard: on the menu, click **Installation**. The response depends upon the state of the unit:

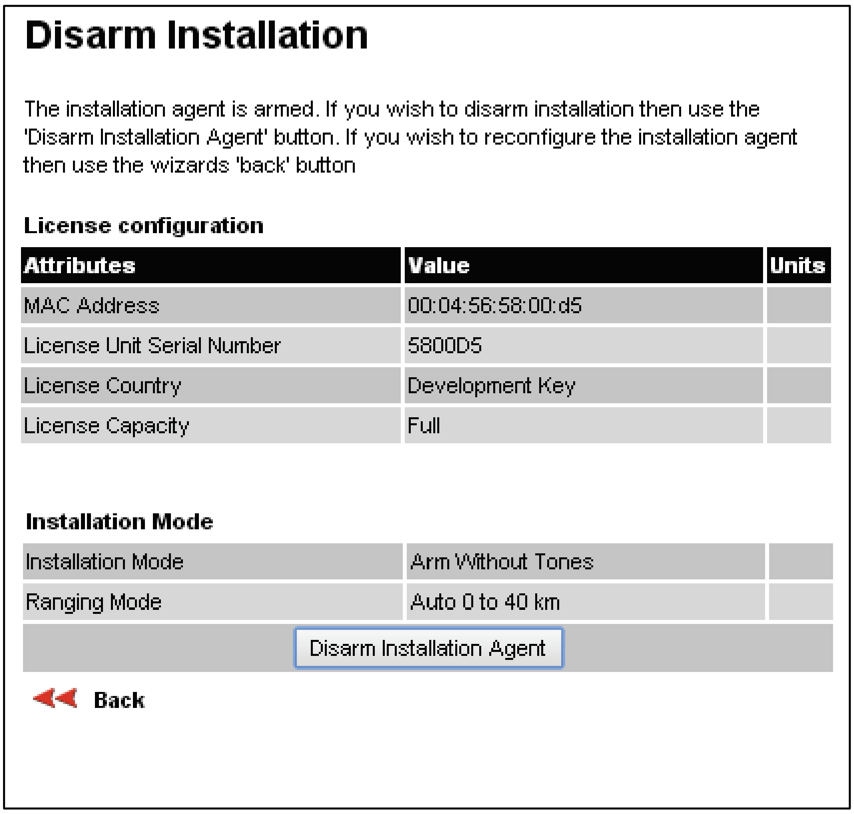
- If the unit is newly installed, the Software License Key page is displayed. Continue at Software License Key page on page 6-13.
- If the unit is armed for alignment, the Disarm Installation page is displayed. Continue at Disarm Installation page on page 6-10.
- If the unit is not armed, the Current Installation Summary page is displayed. Continue at Current Installation Summary page on page 6-10.

Disarm Installation page

Menu option: **Installation** (Figure 116). This page is displayed only when unit is armed.

> **Note** The Installation agent cannot be armed (or disarmed) when the ODU operates as a Master in the HCMP topology.

Figure 116 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	00:04:56:58:00:d5	
License Unit Serial Number	5800D5	
License Country	Development Key	
License Capacity	Full	

Installation Mode

Installation Mode	Arm Without Tones	
Ranging Mode	Auto 0 to 40 km	

Disarm Installation Agent

Back

To disarm the unit, click **Disarm Installation Agent**.

Current Installation Summary page

Menu option: **Installation** (Figure 117 and Figure 118). This page is displayed only when unit is not armed.

Figure 117 Current Installation Summary page (PTP topology)

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	00:04:56:58:00:d5	
License Unit Serial Number	5800D5	
License Country	Development Key	
License Capacity	Full	
Installation Configuration		
IP Version	IPv4	
IPv4 Address	169.254.1.11	
Subnet Mask	255.0.0.0	
Gateway IP Address	169.254.0.0	
Use VLAN For Management Interfaces	No VLAN Tagging	
DSCP Management Priority	00 - DF	
Data Service	Main PSU Port	
Second Data Service	None	
Management Service	Main PSU Port	
Local Management Service	✔ Out-of-Band Aux Port	
TDM Interface Control	None	
Wireless Configuration		
Master Slave Mode	Master	
Access Method	Link Name Access	
Link Name	Ashburton to Widecombe	
Dual Payload	Enabled	
Max Receive Modulation Mode	256QAM 0.81	
Lowest Data Modulation Mode	BPSK 0.63	
Link Mode Optimization	IP Traffic	
TDD Synchronization Mode	Disabled	
Regulatory Band	8 - 5.4 GHz Unrestricted EIRP	
Channel Bandwidth	15	MHz
Link Symmetry	1 to 1	
Spectrum Management Control	DSO	
Extended Spectrum Scanning	Disabled	
Channel Raster	5	MHz
Lower Center Frequency	5478	MHz
Tx Color Code	A	
Rx Color Code	A	
Antenna Gain	23.0	dBi
Cable Loss	0.0	dB
Maximum Transmit Power	23	dBm
EIRP	46.0	dBm
ATPC Peer Rx Max Power	-35	dBm
Installation Mode		
Installation Mode	Arm Without Tones	
Ranging Mode	Auto 0 to 40 km	

Continue to Installation Wizard

Click **Continue to Installation Wizard**.

Figure 118 Current Installation Summary page (HCMP topology)

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	00:04:56:58:00:58	
License Unit Serial Number	580058	
License Country	Development Key	
License Capacity	Full	
Installation Configuration		
IP Version	IPv4	
IPv4 Address	169.254.1.11	
Subnet Mask	255.255.0.0	
Gateway IP Address	169.254.0.0	
Use VLAN For Management Interfaces	No VLAN Tagging	
DSCP Management Priority	00 - DF	
Data Service	Main PSU Port + SFP Port	
Management Service	In-Band	
Local Management Service	None In-Band	
Wireless Configuration		
Wireless Topology	High Capacity Multi-Point	
Master Slave Mode	Master	
Access Method	Group Access	
Group ID	0	
Dual Payload	Enabled	
Max Receive Modulation Mode	256QAM 0.81	
Lowest Data Modulation Mode	BPSK 0.63	
Link Mode Optimization	IP Traffic	
HCMP Maximum Link Range	24.0	km
Maximum Number Of Slaves	4	
HCMP Link Symmetry	1 to 1	
Downlink Ratio	50.0	%
Maximum Downlink Capacity	80.42	Mbps
Maximum Uplink Capacity	80.42	Mbps
TDD Frame Duration	5495	μs
TDD Synchronization Mode	Disabled	
Antenna Selection	Connectorized	
Connectorized Antenna Type	Directional, Integrated flat plate	
Regulatory Band	81 - 4.7 GHz	
Channel Bandwidth	20	MHz
Spectrum Management Control	Fixed Frequency	
Extended Spectrum Scanning	Disabled	
Channel Raster	5	MHz
Fixed Transmit Frequency	4410	MHz
Tx Color Code	A	
Fixed Receive Frequency	4410	MHz
Rx Color Code	A	
Antenna Gain	23.0	dBi
Cable Loss	0.0	dB
Maximum Transmit Power	27	dBm
EIRP	50.0	dBm
Atpc Hcmp Master Target Rx Power	-56	dBm
Installation Mode		
Installation Mode	Arm Without Tones	
Ranging Mode	Auto 0 to 40 km	

Continue to Installation Wizard

Click **Continue to Installation Wizard**.

Software License Key page

Menu option: **Installation**. Use this page to configure the unit with a new License Key and to review the capabilities of an installed License Key. The appearance of this page varies depending upon which capabilities are enabled by the entered license key. For example, Figure 119 shows the licensed capabilities for a PTP 700 in the USA market with a Full Capability Trial License, whereas Figure 120 shows IPv6 and other capabilities. Use the Cambium Networks License Key Generator to generate new License Keys (Generating license keys on page 6-2).

Figure 119 Software License Key page (PTP 700 USA market)

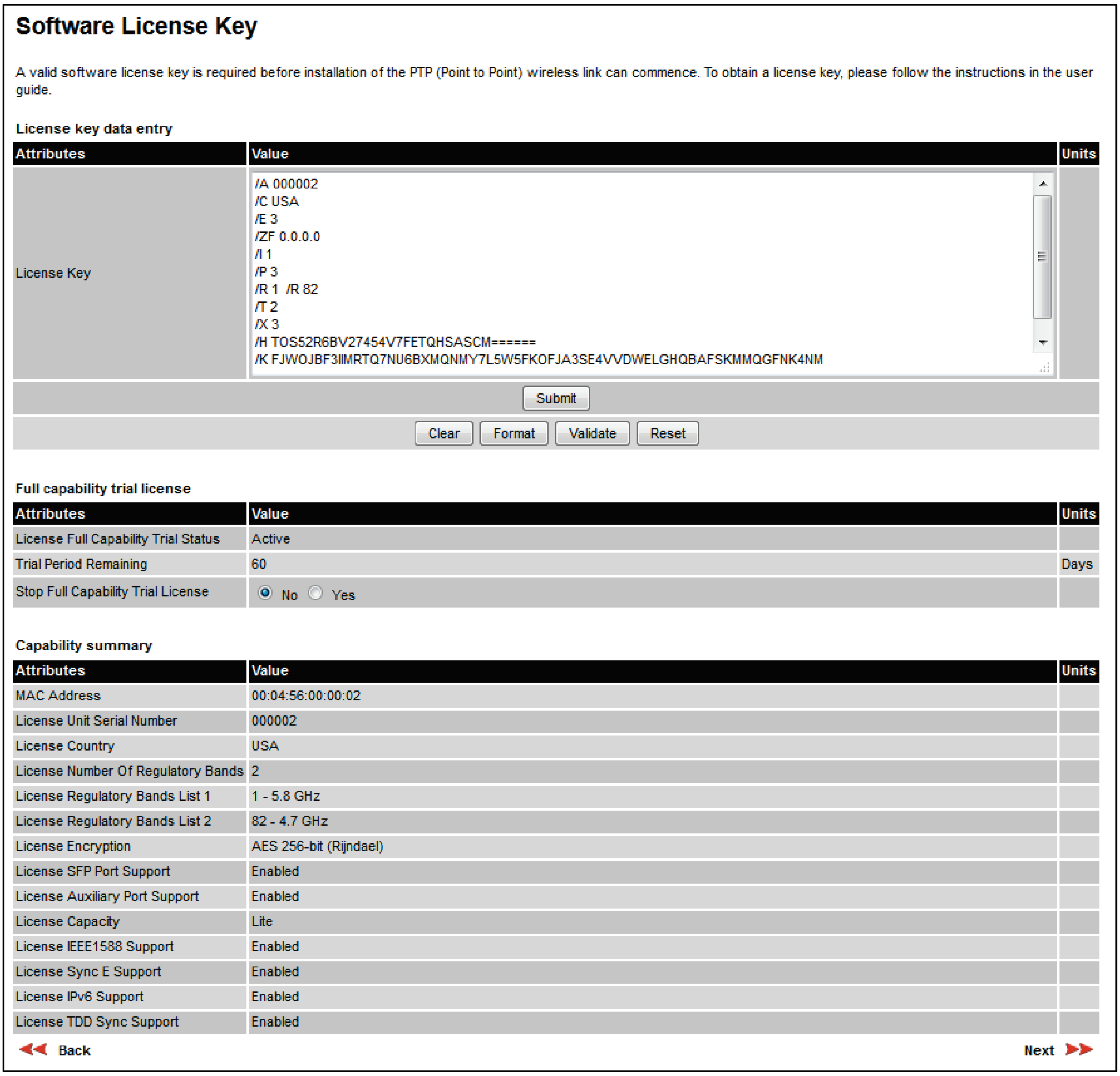


Figure 120 Software License Key page (IPv6 and other capabilities)

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 000002 /C Development_Key /G 1 /I 1 /M 1 /R 1 /R 13 /R 14 /R 25 /R 26 /R 255 /W 8 /X 3 /H XYQZJG4CDV	

Submit

Clear Format Validate Reset

Capability summary

Attributes	Value	Units
MAC Address	00:04:56:00:00:02	
License Unit Serial Number	000002	
License Country	Development Key	
License Number Of Regulatory Bands	6	
License Regulatory Bands List 1	1 - 5.8 GHz	
License Regulatory Bands List 2	13 - 5.4 GHz	
License Regulatory Bands List 3	14 - 4.9 GHz Public Safety	
License Regulatory Bands List 4	25 - 5.8 GHz ETSI	
License Regulatory Bands List 5	26 - 5.4 GHz ETSI	
License Regulatory Bands List 6	255	
License Group Access	Enabled	
License OOB Management Support	Enabled	
License Capacity	Full	
License Max Number Of TDM Channels	8	
License IEEE1588 Support	Enabled	
License Sync E Support	Enabled	
License IPv6 Support	Enabled	
License TDD Sync Support	Enabled	

Back Next

Procedures:

Note Full capability in PTP topology 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 122). This shows the number of days remaining before the full capability trial period expires.

To enter a new License Key, proceed as follows:

- 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.
- To enter the new License Key, click **Submit**. The page is redisplayed with the Capability Summary updated.

To control the full capability trial (Lite license only), proceed as follows:

- If License Full Capability Trial Status is **Available** (Figure 121), start the full capability trial period by setting Activate Full Capability Trial License to **Yes**.
- If License Full Capability Trial Status is **Active** (Figure 122), suspend the full capability trial period by setting Stop Full Capability Trial License to **Yes**.
- If License Full Capability Trial Status is **Inactive** (Figure 123), resume the full capability trial period by setting Start Full Capability Trial License to **Yes**.

To continue with the Installation Wizard, click **Next**.

Figure 121 Software License Key page (extract) with full capability trial available

Full capability trial license

Attributes	Value	Units
License Full Capability Trial Status	Available	
Activate Full Capability Trial License	(•) No ( ) Yes	

Figure 122 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 123 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	

Wireless Topology Configuration page

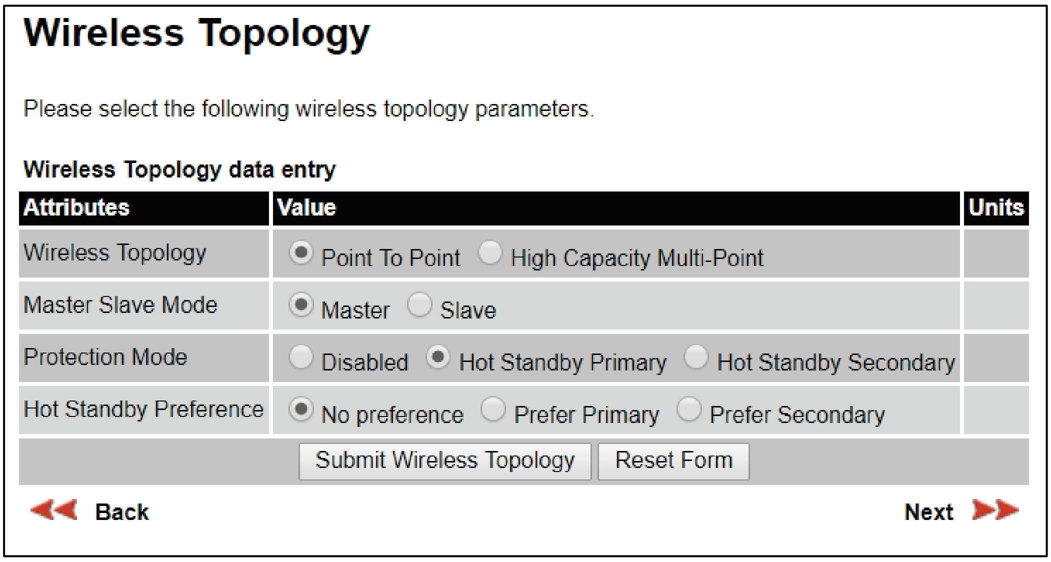
Menu option: **Wireless Topology**. Use this page to update Wireless Topology and Master Slave Mode.

The appearance of this page varies depending upon which capabilities have been enabled by license key. The HCMP option is only available if enabled in the license key.

Procedure:

- Review and update the Wireless Topology.
- Review and update the Master Slave Mode.
- If Wireless Topology = Point To Point, review and update Protection Mode.
- If Protection Mode = Hot Standby Primary, review and update Hot Standby Preference.

Figure 124 Wireless Topology page



Interface Configuration page

Menu option: **Installation**. Use this page to update the IP interface attributes.

The appearance of this page varies depending upon which capabilities have been enabled by license key. For example, Figure 125 shows the attributes that are displayed when IPv6, Aux Port, SFP Port and Out-of-Band Management support are enabled.

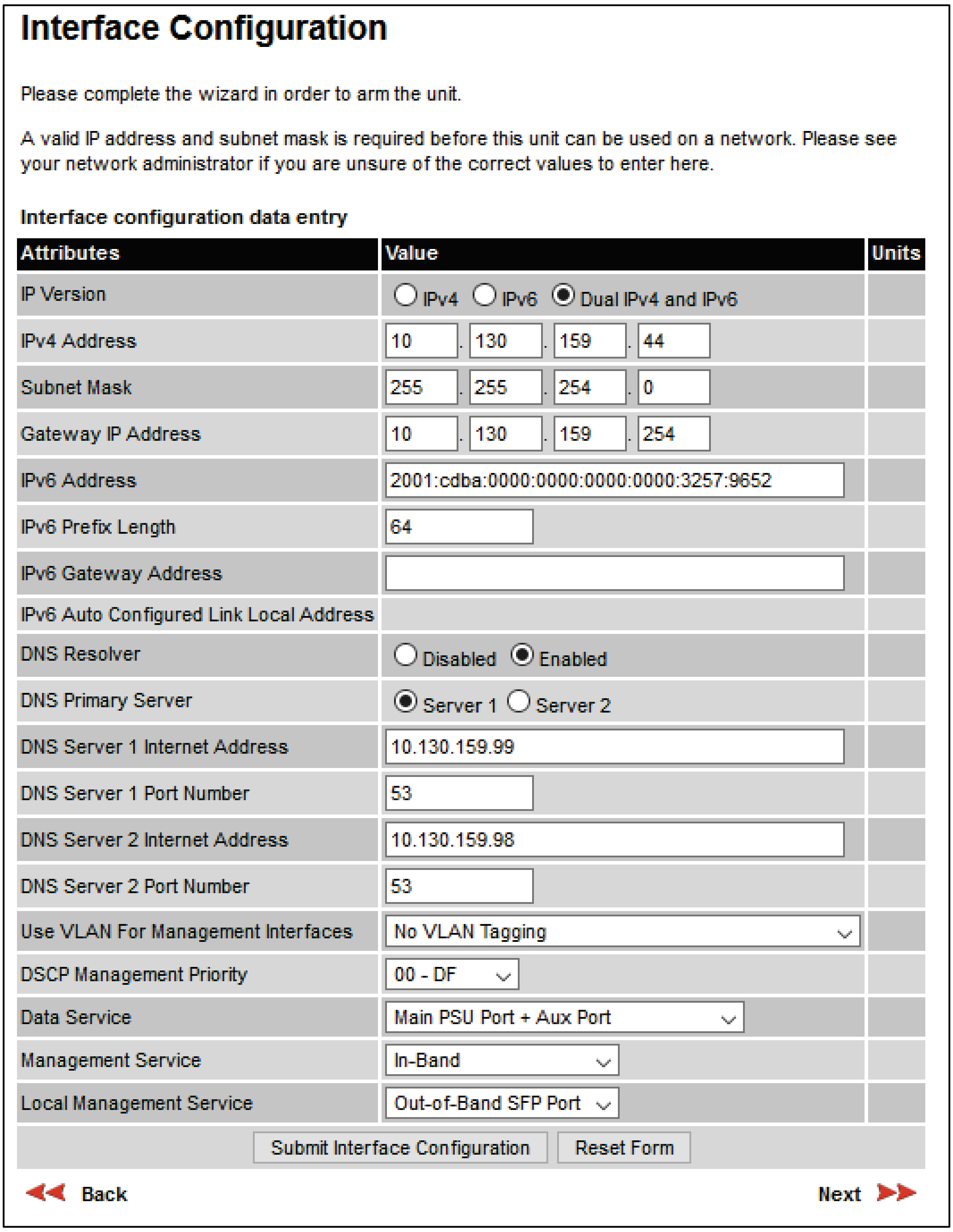
Attention Before configuring a VLAN for management interfaces, ensure that the VLAN is accessible, otherwise the unit will be inaccessible after the next reboot.

Note Synchronous Ethernet and IEEE 1588 Transparent Clock are disabled when TDM is enabled (LAN Configuration page on page 6-46).

Procedure:

- Review and update the IP and VLAN attributes (Table 126).
- To continue with the Installation Wizard, click **Next** or **Submit Interface Configuration**.

Figure 125 Interface Configuration page (IPv6, Aux, SFP, and OOB support)



Interface Configuration

Please complete the wizard in order to arm the unit.

A valid IP address and subnet mask is required before this 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	10 . 130 . 159 . 44	
Subnet Mask	255 . 255 . 254 . 0	
Gateway IP Address	10 . 130 . 159 . 254	
IPv6 Address	2001:cdba:0000:0000:0000:0000:3257:9652	
IPv6 Prefix Length	64	
IPv6 Gateway Address		
IPv6 Auto Configured Link Local Address		
DNS Resolver	Disabled Enabled	
DNS Primary Server	Server 1 Server 2	
DNS Server 1 Internet Address	10.130.159.99	
DNS Server 1 Port Number	53	
DNS Server 2 Internet Address	10.130.159.98	
DNS Server 2 Port Number	53	
Use VLAN For Management Interfaces	No VLAN Tagging	
DSCP Management Priority	00 - DF	
Data Service	Main PSU Port + Aux Port	
Management Service	In-Band	
Local Management Service	Out-of-Band SFP Port	

Submit Interface Configuration Reset Form

Back Next

Figure 126 Interface Configuration page (Hot Standby support)

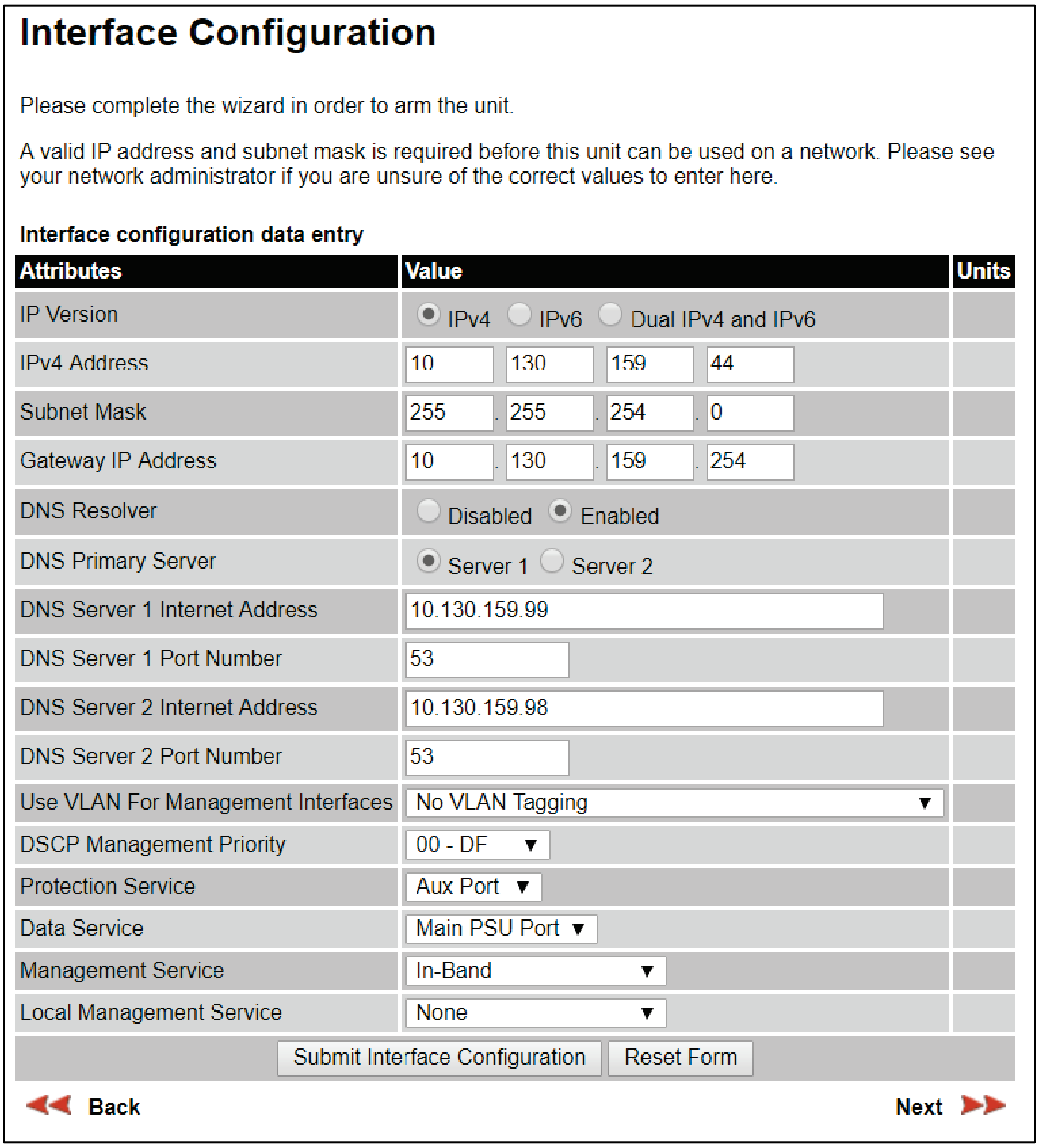


Table 126 Interface Configuration attributes

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.

Attribute	Meaning
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).
DNS Resolver	Options for using the internal DNS Resolver: **Disabled**: The DNS Resolver is not used. **Enabled**: The DNS Resolver is used.
DNS Primary Server	Select **Server 1** or **Server 2** as the Primary Server. The selected server will be used to resolve addresses configured as FQDNs to IPv4 or IPv6. The Secondary Server will be used if the Primary Server is not available.
DNS Server 1 Internet Address	The IPv4 or IPv6 address of DNS Server 1.
DNS Server 1 Port Number	The UDP Port Number used by DNS Server 1. The default is Port 53.
DNS Server 2 Internet Address	The IPv4 or IPv6 address of DNS Server 2.
DNS Server 2 Port Number	The UDP Port Number used by DNS Server 2. The default is Port 53.
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 700 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.
Protection Service	The port allocation for the Protection Service in Hot Standby links: **Aux Port**: The Protection Service uses the Aux Port **SFP Port**: The Protection Service uses the SFP Port
Data Service	The port allocation for the Data Service: **Main PSU Port**: The Data Service is connected to the Main PSU Port **Aux Port**: The Data Service is connected to the Aux Port **SFP Port**: The Data Service is connected to the SFP Port **Main PSU Port + Aux Port**: The Data Service is connected to the Main PSU Port and the Aux Port **Main PSU Port + SFP Port**: The Data Service is connected to the Main PSU Port and the SFP Port **Aux Port + SFP Port**: The Data Service is connected to the Aux Port and the SFP Port **Main PSU Port + Aux Port + SFP Port**: The Data Service is connected to the Main PSU, Aux Port and the SFP Port The Data Service must always be assigned to at least one of the wired ports. For more help, see Ethernet port allocation on page 3-40.

Attribute	Meaning
Management Service	The port allocation for the end-to-end Management Service: **None**: The Management Service is not used. **In-Band**: The Management Service is connected to the port or ports allocated to the Data Service. **Out-Of-Band Main PSU Port**: The Management Service is connected to the Main PSU Port **Out-Of-Band Aux Port**: The Management Service is connected to the Aux Port **Out-Of-Band SFP Port**: The Management Service is connected to the SFP Port **Out-Of-Band Main PSU Port + Aux Port**: The Management Service is connected to the Main PSU Port and the Aux Port **Out-Of-Band Main PSU Port + SFP Port**: The Management Service is connected to the Main PSU Port and the SFP Port **Out-Of-Band Aux Port + SFP Port**: The Management Service is connected to the Aux Port and the SFP Port For more help, see Ethernet port allocation on page 3-40.
Local Management Service	Any port not already selected to the Data or Management Service is available for connection as an out-of-band port for the Local Management Service. Ports already selected to the Data or Management services are not displayed as options. For more help, see Ethernet port allocation on page 3-40.

Configuring port allocations

The Interface Configuration page controls the allocation of the Main PSU Port, Aux Port and SFP Port to the Data Service, Management Service and Local Management Service.

PTP 700 supports exactly one instance of the Data Service, and this service is always mapped to one or more of the three wired ports. It is not possible to operate a link without any port selected to the Data Service.

PTP 700 supports zero or one instances of the optional Management Service. The Management Service can be used to access the management agent at the local unit. If the wireless link is established, the Management Service can also be used to access the management agent at the remote unit and other devices connected in the remote management network. The Management Service can be mapped to the set of ports that are already used for the Data Service to provide In-Band Management. Alternatively, the Management Service can be allocated to one or more dedicated ports to provide Out-of-Band Management.

PTP 700 also supports an optional Local Management Service, providing a connection from a wired port to the local management agent. Any port not already selected is available for selection to the Local Management Service. The Local Management Service does not connect across the wireless link.

The PTP 700 must always be manageable through one of three ports. Therefore, it is not possible to disable the Management Service unless at least one port is allocated to the Local Management Service.

For more details, see Ethernet port allocation on page 3-40.

Management Configuration page

Menu option: **Management Configuration**. Use this page to configure the cnMaestro device agent for connection to a cnMaestro server.

The appearance of the page depends on whether cnMaestro is configured, which type of server is selected, and which type of authentication is selected. See Figure 127 to Figure 129.

Figure 127 Management Configuration, cnMaestro disabled

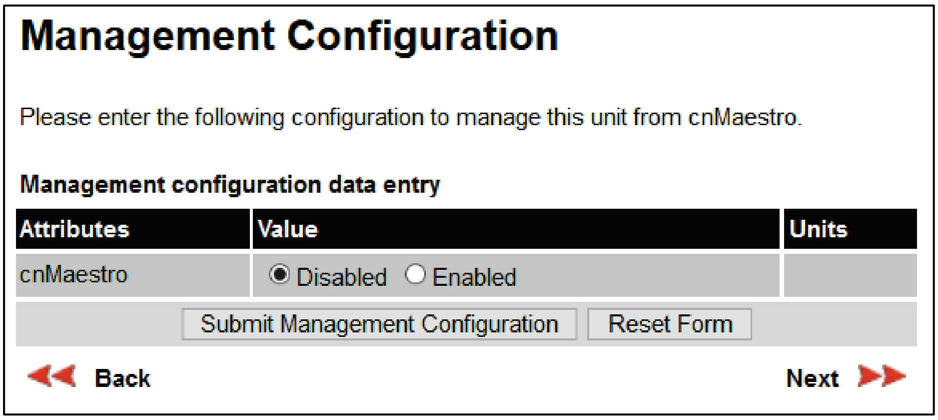


Figure 128 Management Configuration, cnMaestro Cloud

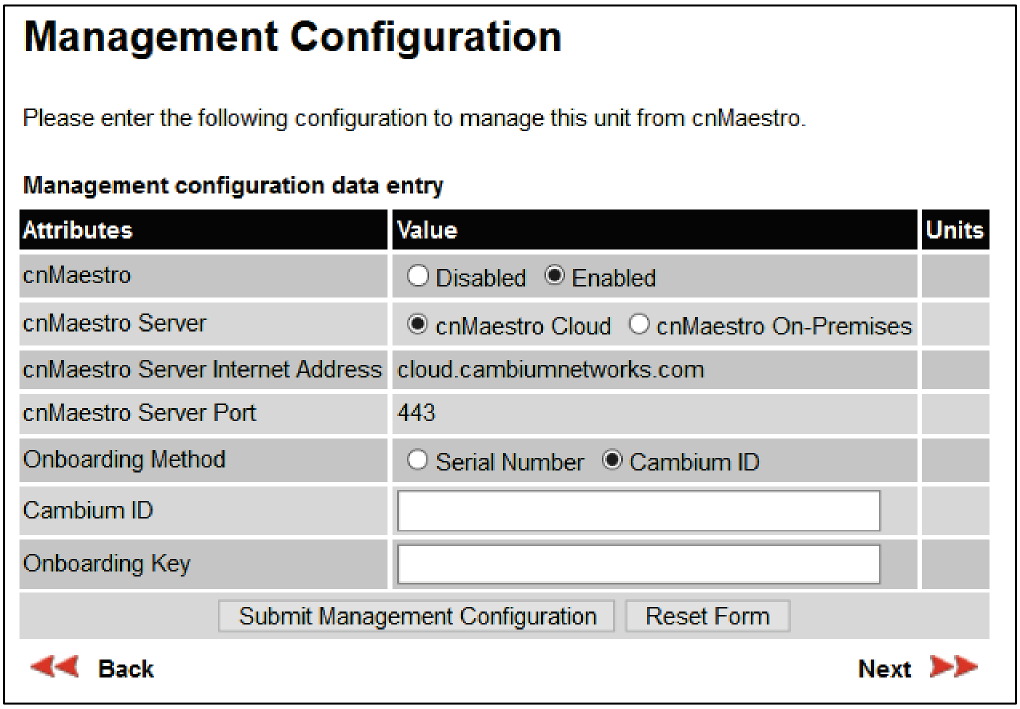


Figure 129 – Management Configuration, cnMaestro On-Premises

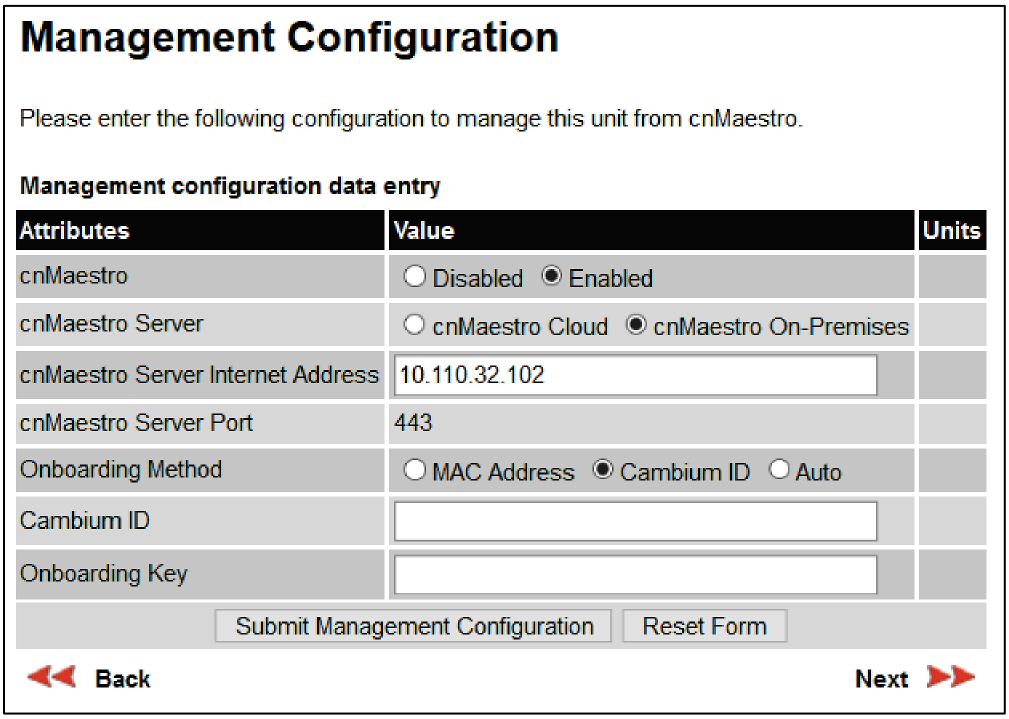


Table 127 Management Configuration attributes

Attribute	Meaning
cnMaestro	**Enabled**: The cnMaestro device agent is enabled. **Disabled**: The cnMaestro device agent is disabled.
cnMaestro Server	**cnMaestro Cloud**: The device agent will connect to the Cloud server. **cnMaestro On-Premises**: The device agent will connect to an On-Premises server.
cnMaestro Server Internet Address	The Internet Address of the cnMaestro server. For a Cloud server, the address is always "cloud.cambiumnetworks.com". For an On Premises server, configure the IPv4 address or FQDN of the server.
cnMaestro Server Port	The protocol port used by the HTTPS protocol. This is always 443.
Onboarding Method	**Serial Number**: The device agent will be authenticated for Onboarding using the ODU's MSN. This option is supported for the Cloud server only. The Serial Number option is hidden unless the ODU has a 12-character MSN. **Cambium ID**: The device agent will be authenticated for Onboarding using the operator's Cambium ID and secret Onboarding Key. This option is supported for Cloud and On Premises servers. **MAC Address**: The device agent will be authenticated for Onboarding using the ODU's MAC Address. This option is supported for the On Premises server only. **Auto**: This option is supported for the On Premises server only.

Attribute	Meaning
	Note: Cambium ID is not enabled by default in the cnMaestro On Premises server; to use this onboarding method, enable authentication using Cambium ID at the server before the ODU attempts to connect.
Cambium ID	The operator's Cambium ID entered as a text string of up to 60 characters. Cambium ID is erased automatically after successful onboarding.
Onboarding Key	The secret Onboarding Key associated with the Cambium ID entered as a text string of up to 32 characters. Onboarding Key is erased automatically after successful onboarding. If the ODU is subsequently removed from cnMaestro, the Onboarding Key must be entered again.

Wireless Configuration page

Menu option: **Installation** (Figure 130 and Figure 131).

This page is part of the Installation Wizard. Use it to update the wireless attributes.

Figure 130 Wireless Configuration page (PTP topology)

Wireless Configuration

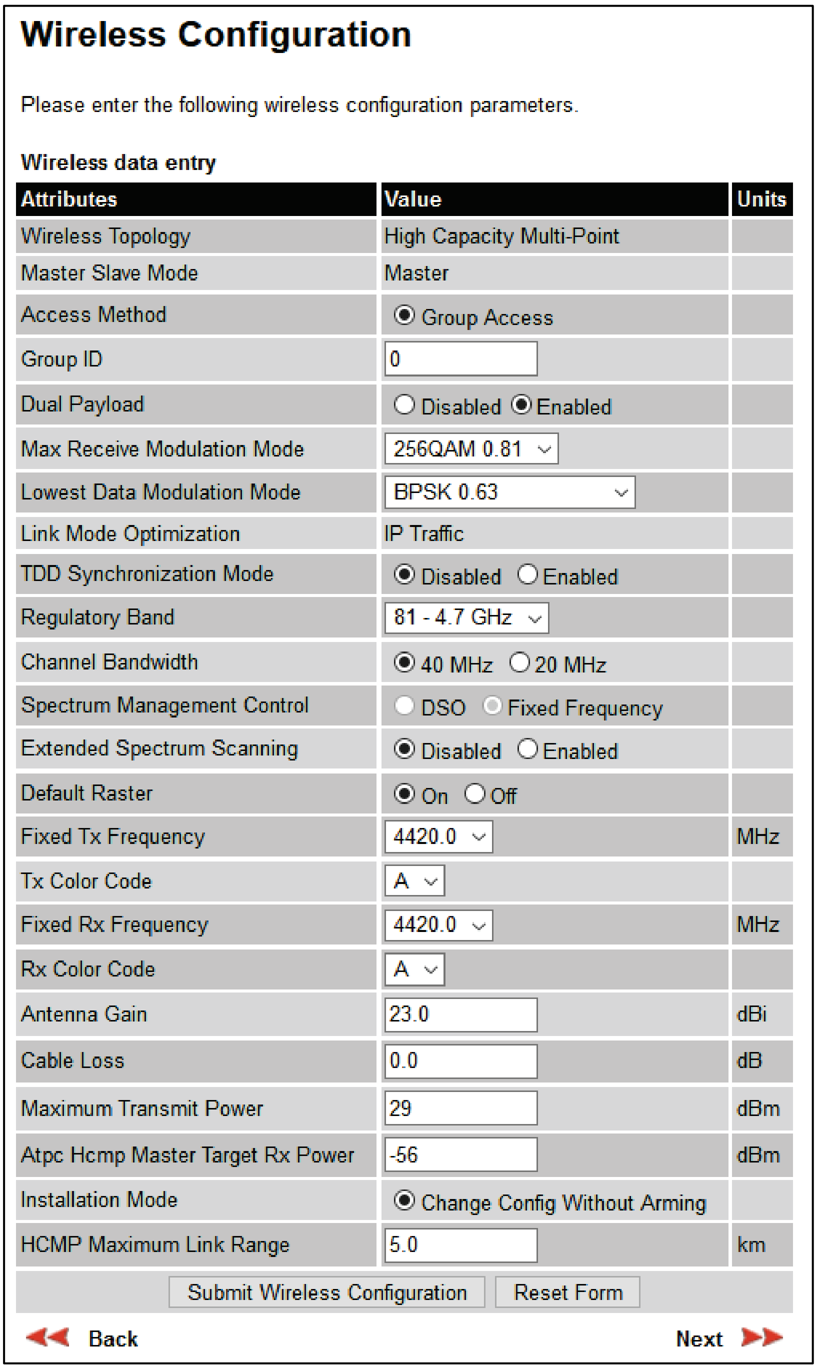
Please enter the following wireless configuration parameters.

Wireless data entry

Attributes	Value	Units
Wireless Topology	Point To Point	
Master Slave Mode	Master	
Protection Mode	Hot Standby Primary	
Access Method	Link Access, Link Name Access, Group Access	
Group ID	123	
Dual Payload	Disabled, Enabled	
Max Receive Modulation Mode	256QAM 0.81 ▼	
Link Mode Optimization	IP Traffic, TDM Traffic	
TDD Synchronization Mode	Disabled, Enabled	
Long Frame Duration	Enabled	
Regulatory Band	81 - 4.7 GHz ▼	
Channel Bandwidth	45 MHz, 40 MHz, 30 MHz, 20 MHz	
Spectrum Management Control	DSO, Fixed Frequency	
Extended Spectrum Scanning	Disabled, Enabled	
Default Raster	On, Off	
Fixed Tx Frequency	4423.0 ▼	MHz
Tx Color Code	A ▼	
Fixed Rx Frequency	4423.0 ▼	MHz
Rx Color Code	A ▼	
Antenna Gain	23.0	dBi
Cable Loss	0.0	dB
Transmitter Channels	H and V, H Only, V Only	
Maximum Transmit Power	29	dBm
ATPC Peer Rx Max Power	-35	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, Auto 0 to 250 km, Target Range	
	Submit Wireless Configuration, Reset Form	

Back Next

Figure 131 Wireless Configuration page (HCMP topology)



Wireless Configuration

Please enter the following wireless configuration parameters.

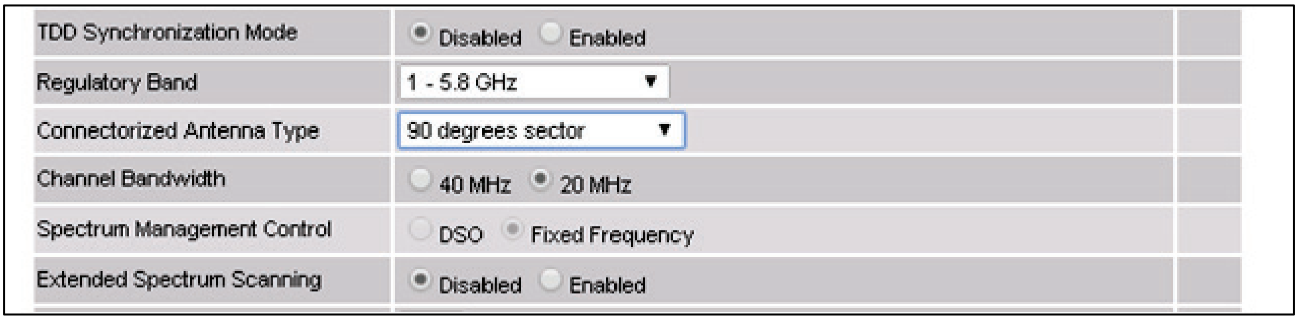
Wireless data entry

Attributes	Value	Units
Wireless Topology	High Capacity Multi-Point	
Master Slave Mode	Master	
Access Method	Group Access	
Group ID	0	
Dual Payload	Disabled Enabled	
Max Receive Modulation Mode	256QAM 0.81	
Lowest Data Modulation Mode	BPSK 0.63	
Link Mode Optimization	IP Traffic	
TDD Synchronization Mode	Disabled Enabled	
Regulatory Band	81 - 4.7 GHz	
Channel Bandwidth	40 MHz 20 MHz	
Spectrum Management Control	DSO Fixed Frequency	
Extended Spectrum Scanning	Disabled Enabled	
Default Raster	On Off	
Fixed Tx Frequency	4420.0	MHz
Tx Color Code	A	
Fixed Rx Frequency	4420.0	MHz
Rx Color Code	A	
Antenna Gain	23.0	dBi
Cable Loss	0.0	dB
Maximum Transmit Power	29	dBm
Atpc Hcmp Master Target Rx Power	-56	dBm
Installation Mode	Change Config Without Arming	
HCMP Maximum Link Range	5.0	km

Submit Wireless Configuration Reset Form

Back Next

Figure 132 Wireless Configuration page (Connectorized Antenna Type, HCMP topology)



TDD Synchronization Mode	Disabled Enabled	
Regulatory Band	1 - 5.8 GHz	
Connectorized Antenna Type	90 degrees sector	
Channel Bandwidth	40 MHz 20 MHz	
Spectrum Management Control	DSO Fixed Frequency	
Extended Spectrum Scanning	Disabled Enabled	

Procedure:

- Update the attributes (Table 128).
- To save any changes and continue with the Installation Wizard, click **Next** or click **Submit Wireless Configuration**.

Attention 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 128 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.
Protection Mode	**Disabled**: Hot Standby is disabled. **Hot Standby Primary**: The ODU is configured as the Primary ODU in a Hot Standby link. **Hot Standby Secondary**: The ODU is configured as the Secondary ODU in a Hot Standby link.
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. **Group Access:** Only displayed when a Group Access license key has been generated (Generating license keys on page 6-2) and submitted (Software License Key page on page 6-13). Both ODUs in a PTP link, and all ODUs in an HCMP sector, must be configured with the same Group ID attributes. Group Access is the only Access Method supported in the HCMP topology.

Attribute	Meaning
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.
Group ID	Only displayed when Access Method is set to **Group Access**. A link can only be established between units that have identical Group IDs.
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.
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 Data Modulation Mode	The lowest modulation mode that must be achieved before the link is allowed to bridge customer data Ethernet frames. This does not affect the bridging of management data: if out-of-band remote management is enabled, this will continue regardless of modulation mode.
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. This is the only available setting when TDM is enabled (Interface Configuration page on page 6-16).
TDD Synchronization Mode	**Enabled:** The ODU will synchronized the TDD frames at the wireless interface to an external or internal 1 Hz reference.
Long Frame Duration	Always enabled for a PTP link in Hot Standby. Can optionally be enabled for an unprotected PTP link to provide synchronization between protected and unprotected links.
Antenna Selection	**Integrated:** The unit uses the integrated antenna. The antenna connectors are disabled. **Connectorized:** The unit uses the antenna connectors. The integrated antenna is disabled. This attribute is only displayed in a Connectorized+Integrated unit.
Regulatory Band	The regulatory band selected from the list in the license key.

Attribute	Meaning
Connectorized Antenna Type	Only displayed in the HCMP topology, and only when the Regulatory Band applies different limits for PTP and PMP operation. Select one of the following for an HCMP Master: • 60 degrees sector • 90 degrees sector • 120 degrees sector • Omni-directional • Other
Channel Bandwidth	Bandwidth of the transmit and receive radio channels.
Link Symmetry	Only displayed when Wireless Topology is set to **Point To Point** and 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**. **“5 to 1”**, **“3 to 1**, **“2 to 1”**, “**1 to 1”**, “**1 to 2”**, **“1 to 3”** or **“1 to 5”**: 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. When TDM is enabled (Interface Configuration page on page 6-16), Link Symmetry is limited to “**1 to 1**”.
Spectrum Management Control	**PTP topology** 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
	HCMP topology The options are: **DSO** **Fixed Frequency**
Slave Scan	Only displayed at an HCMP Slave ODU. **Disabled:** The Slave will be configured with fixed frequencies. **Auto Single:** The Slave **Auto Optimum:** The Slave
Extended Spectrum Scanning	Enables scanning of the entire frequency spectrum supported by the device (4400 MHz to 5875 MHz). **Disabled:** The extended Spectrum Scanning is disabled. **Enabled:** The extended Spectrum Scanning is enabled. **Attention** Extended Spectrum Scanning decreases DSO performance. Do not leave Extended Spectrum Scanning enabled during normal operation.
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 700 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 for a Connectorized ODU, or a Connectorized+Integrated ODU where Anntena Selection is set to **Connectorized**. Gain of the remote antenna.

Attribute	Meaning
Cable Loss	Only displayed for a Connectorized ODU, or a Connectorized+Integrated ODU where Anntena Selection is set to **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.
Transmitter Channels	Only displayed when the Transmitter Channels Control attribute is enabled (see Webpage Properties page on page 6-76). **H and V:** The ODU transmits on Horizontal and Vertical polarisation **H Only:** The ODU transmits on Horizontal polarisation (or at the H output of a Connectorized unit) only. **V Only:** The ODU transmits on Vertical polarisation (or at the V output of a Connectorized unit) only. **Note** Operation using a single polarisation cannot provide polarisation diversity or polarisation multiplexing. This will reduce availability in non-line-of-sight paths and will reduce capacity in line-of-sight or near-line-of-sight paths.
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 combination of the selected Regulatory Band, Bandwidth and (for connectorized units) Antenna Gain and Cable Loss. Set this attribute to the value specified in the installation report (LINKPlanner). **Note** Maximum Transmit Power is the maximum combined power for the normal case where H and V channels operate together. When Transmitter Channels is set to H Only or V Only, the maximum transmitted power will be 3 dB lower than the configured Maximum Transmit Power.
ATPC Peer Rx Max Power	This attribute is only displayed if: • The unit is in PTP topology • The operating regulatory band does not require radar detection. Set this attribute to the maximum receive power the ATPC mechanism must try to achieve at the peer unit.
ATPC HCMP Master Transmit Power	This attribute is only visible if the unit is configured as an HCMP Slave. This attribute must be set to the same value as the Maximum Power Power on the HCMP Master.

Attribute	Meaning
	Note The wireless link may fail to establish if the value of this attribute is not set as recommended.
ATPC HCMP Master Target Receive Power	This attribute is only visible if Wireless Topology is set to HCMP. This determines the HCMP Master receive power the ATPC mechanism on the HCMP Slave must try to reach. **Note** Setting a high value may reduce sensitivity of the HCMP Master to low receive signal while setting it low value may prevent the HCMP Master to reach top rate mode. The default value of –56 dBm ensures that the top modulation mode can be reached whilst not degrading the performance at low receive signal level.
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. This is the only option supported for the Master ODU in HCMP topology.
Ranging Mode	This can only be modified if the unit is operating in the PTP topology, and 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 100 km** (0 to 62 miles). **Auto 0 to 200 km** (0 to 125 miles). **Auto 0 to 250 km** (0 to 156 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 6-76.
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.
HCMP Maximum Link Range	The maximum link range that will be supported for any link in an HCMP sector. Configure a value between 5.0 km and 100.0 km (3 miles to 62 miles).

TDD Frame page

The TDD Frame page (Figure 133) is displayed in the Installation Wizard page after the Wireless Configuration page when the ODU is operating in the HCMP topology.

Procedure:

- Update the attributes (Table 129).
- Click **Next**.

Figure 133 TDD Frame page (HCMP Master, Standard TDD Frame Configuration)

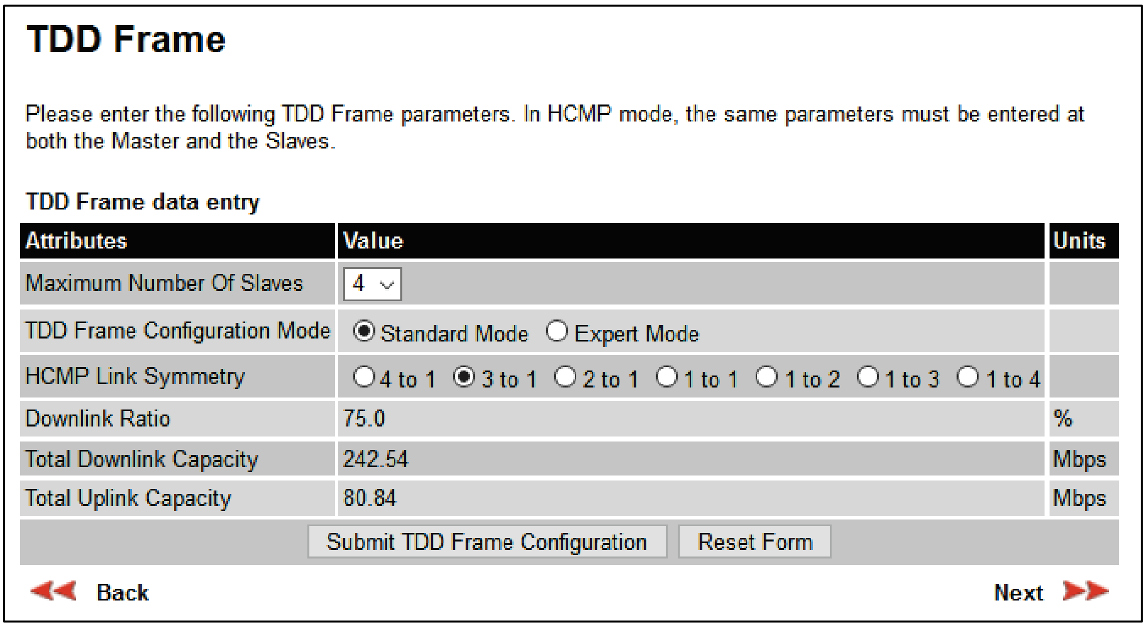


Figure 134 TDD Frame page (HCMP Master, Expert TDD Frame Configuration)

TDD Frame

Please enter the following TDD Frame parameters. In HCMP mode, the same parameters must be entered at both the Master and the Slaves.

TDD Frame data entry

Attributes	Value	Units
Maximum Number Of Slaves	4	
TDD Frame Configuration Mode	○ Standard Mode ◉ Expert Mode	
Downlink Timeslots in TDD period	10	
Uplink Timeslots in TDD period	6	
Downlink Ratio	62.5	%
Total Downlink Capacity	202.12	Mbps
Total Uplink Capacity	121.27	Mbps
Submit TDD Frame Configuration	Reset Form	

Back **Next**

Figure 135 TDD Frame page (HCMP Slave, Standard TDD Frame Configuration)

TDD Frame

Please enter the following TDD Frame parameters. In HCMP mode, the same parameters must be entered at both the Master and the Slaves.

TDD Frame data entry

Attributes	Value	Units
Maximum Number Of Slaves	4	
TDD Frame Configuration Mode	◉ Standard Mode ○ Expert Mode	
HCMP Link Symmetry	○ 4 to 1 ◉ 3 to 1 ○ 2 to 1 ○ 1 to 1 ○ 1 to 2 ○ 1 to 3 ○ 1 to 4	
Downlink Ratio	75.0	%
Total Downlink Capacity	242.54	Mbps
Total Uplink Capacity	80.84	Mbps
Slave Downlink Capacity	60.63	Mbps
Slave Uplink Capacity	20.21	Mbps
Submit TDD Frame Configuration	Reset Form	

Back **Next**

Figure 136 TDD Frame page (HCMP Slave, Expert TDD Frame Configuration)

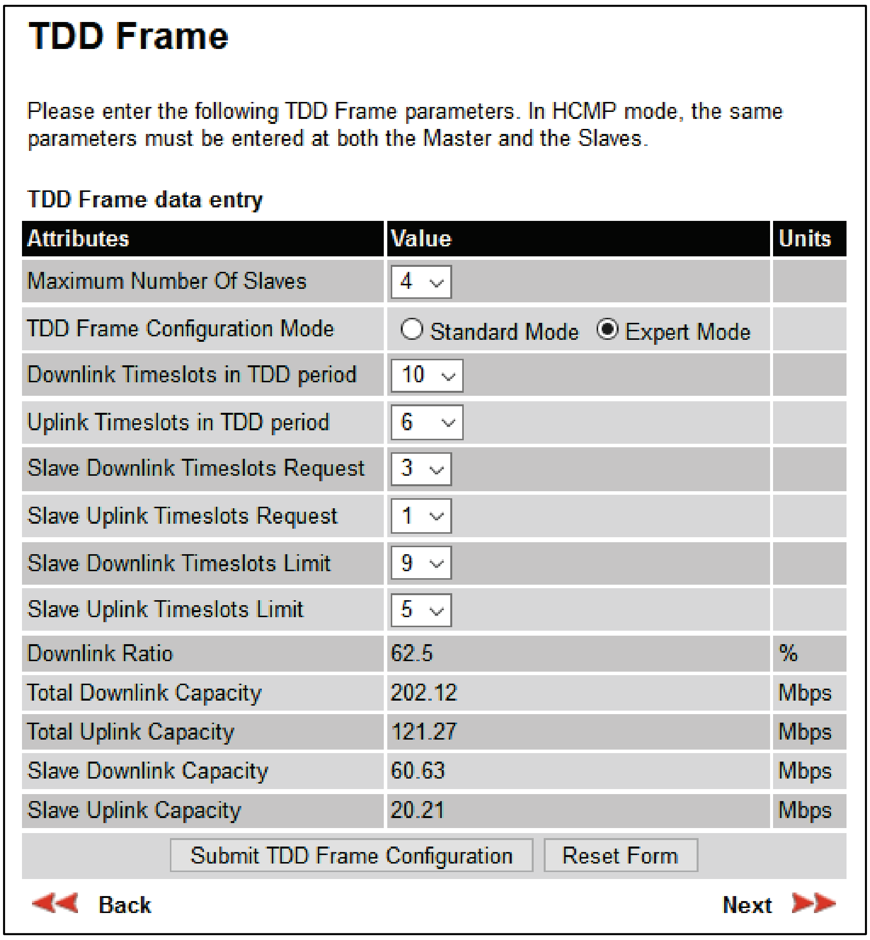


Table 129 TDD Frame attributes

Attribute	Meaning
Maximum Number Of Slaves	**2** to **8** The maximum number of HCMP Slaves that can simultaneously connect to the HCMP Master. The same value must be used on the HCMP Master and all the HCMP Slaves that connect to it.
TDD Frame Configuration Mode	**Standard**, **Expert** Select **Expert** to configure individual time slot allocations to each Slave ODU.
HCMP Link Symmetry	Standard TDD Frame Configuration Mode only. **“4 to 1”**, **“3 to 1**, **“2 to 1”**, **“1 to 1”**, **“1 to 2”**, **“1 to 3”** or **“1 to 4”**: The ratio of capacity between the downlink direction and the uplink direction.
Downlink Ratio	The proportion of total (uplink and downlink) time slots assigned to the downlink as a percentage.
Total Downlink Capacity	The combined capacity for all downlink time slots assuming the highest modulation mode

Attribute	Meaning
Total Uplink Capacity	The combined capacity for all uplink time slots assuming the highest modulation mode
Downlink Timeslots in TDD Period Uplink Timeslots in TDD Period	Expert TDD Frame Configuration Mode only. The number of downlink and uplink time slots configured in the TDD frame at the HCMP Master.
Slave Downlink Capacity	The capacity for downlink time slots assigned to the Slave ODU assuming the highest modulation mode
Slave Uplink Capacity	The capacity for uplink time slots assigned to the slave assuming the highest modulation mode
Slave Downlink Timeslots Request Slave Uplink Timeslots Request	Expert TDD Frame Configuration Mode only. The number of downlink and uplink time slots requested for the Slave ODU.
Slave Downlink Timeslots Limit Slave Uplink Timeslots Limit	Expert TDD Frame Configuration Mode only. The maximum number of downlink and uplink time slots that can be assigned by dynamic allocation to the Slave ODU. See Dynamic time slot allocation in HCMP on page 1-18

TDD Synchronization page (optional)

If TDD Synchronization Mode is set to **Enabled** in the Wireless Configuration page, the TDD Synchronization page (Figure 137, Figure 138, Figure 139, Figure 140, Figure 141) is the fourth Installation Wizard page.

For more information on the available options, refer to Configuration options for TDD synchronization on page 3-33.

Procedure:

- Update the attributes (Table 130 and Table 131)
- Click **Next**.

Figure 137 TDD Synchronization page, PTP-SYNC, PTP topology

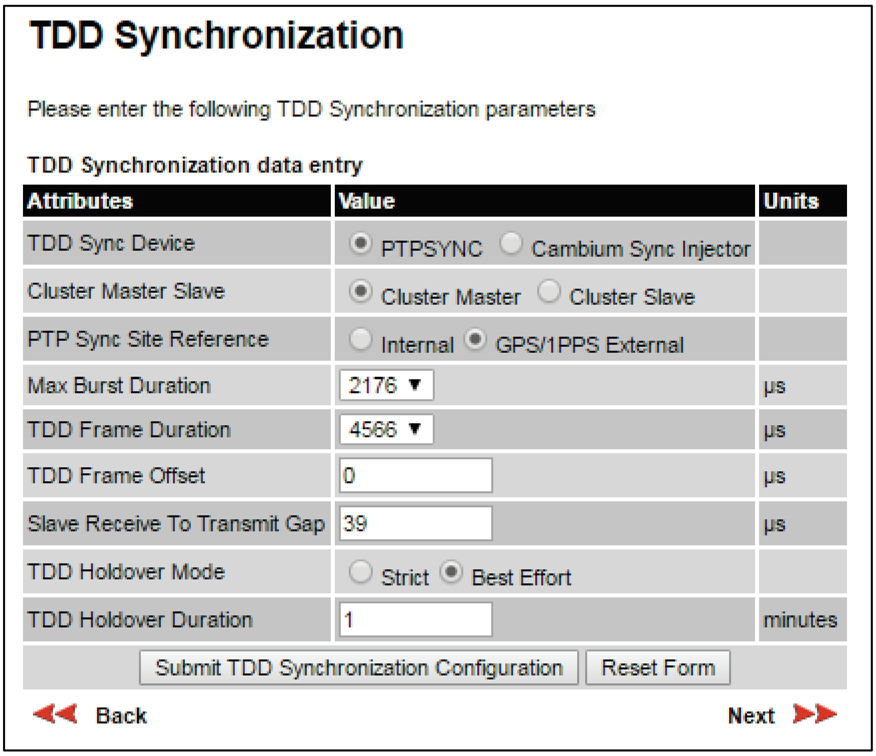


Figure 138 TDD Synchronization page, CMM5 or direct connection, PTP topology

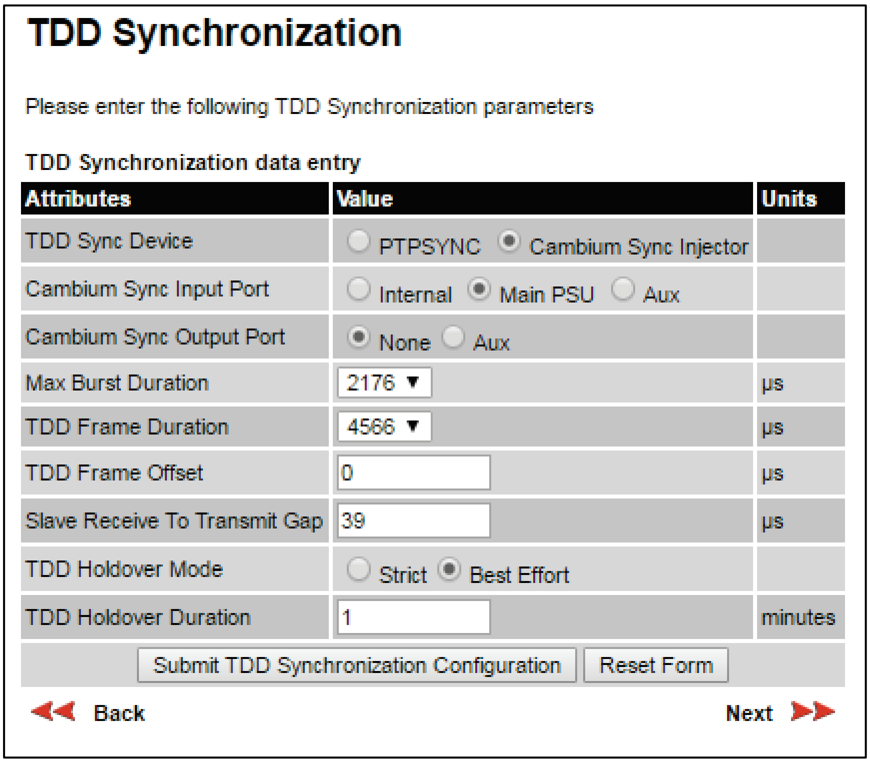


Figure 139 TDD Synchronization page, PTP-SYNC, HCMP topology

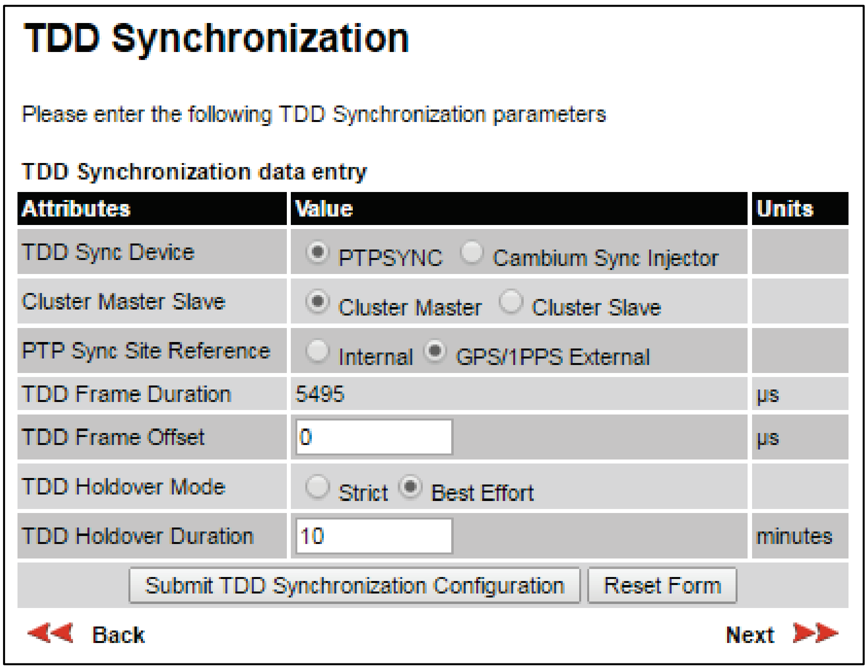


Figure 140 TDD Synchronization page, CMM5 or direct connection, HCMP topology

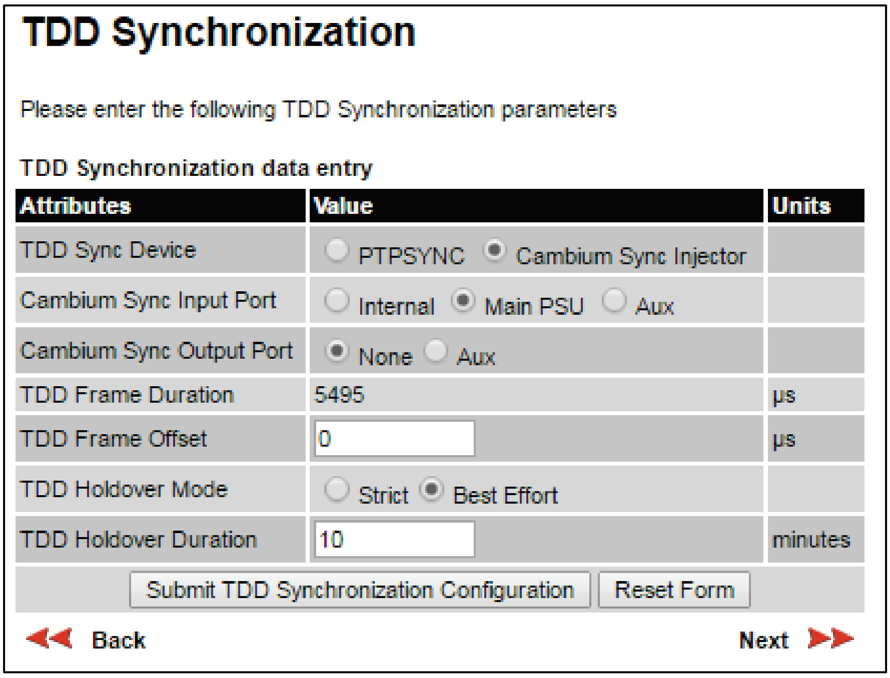
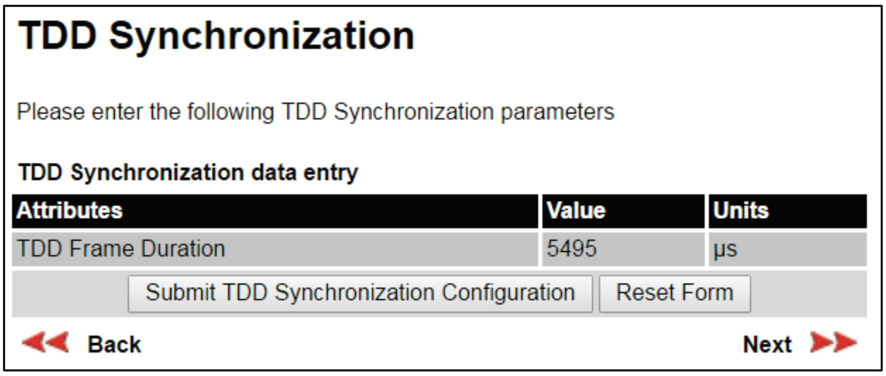


Figure 141 TDD Synchronization page, HCMP Slave



Note For units operating in the PTP topology, obtain the data required to populate this page using the LINKPlanner.

Table 130 TDD Synchronization attributes at a TDD Master or TDD Slave ODU

Attribute	Meaning
Max Burst Duration	Only displayed in PTP topology. The maximum duration of the burst opportunity. For standard frame duration, select a value in the range **544** to **2176** microseconds. For long frame duration (including Hot Standby), select a value in the range **484** to **6528** microseconds.
TDD Frame Duration	Read only in HCMP topology. For PTP with standard frame duration, select a value in the range **1299** to **6410** microseconds. For PTP with long frame duration (including Hot Standby), select a value in the range **1250** to **14286** microseconds.
Slave Receive To Transmit Gap	Only displayed in PTP topology. The duration of the gap between receive and transmit at the slave ODU.

Table 131 TDD Synchronization attributes at a TDD Master ODU

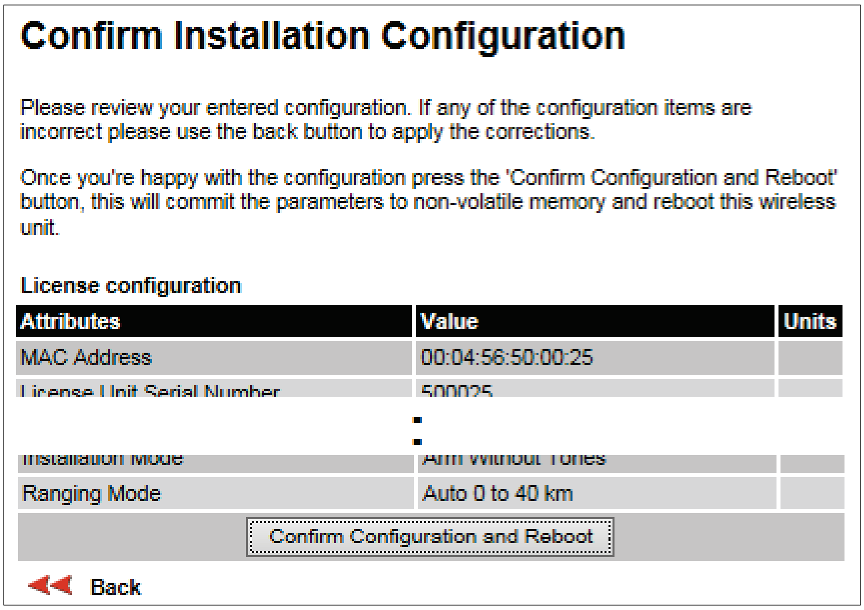
Attribute	Meaning
TDD Sync Device	**PTP-SYNC**: The ODU will synchronize using the connected PTP-SYNC unit **Cambium Sync Injector**: The ODU will synchronize using CMM5, or using a direct connection to another ODU.

Attribute	Meaning
Cluster Master Slave	Only displayed when TDD Sync Device = **PTP SYNC** **Cluster Master**: The first ODU in the synchronization chain. **Cluster Slave**: The second or subsequent ODU in the chain.
PTP-SYNC Site Reference	Only displayed when TDD Sync Device = **PTP SYNC** **Internal**: Standalone operation with no external timing reference. **GPS/1PPS External**: An external GPS receiver will provide a 1 pps timing reference.
Cambium Sync Input Port	Only displayed when TDD Sync Device = **Cambium Sync Injector**. **Internal**: Free-running synchronization is generated internally. **Main PSU**: The ODU will synchronize to a 1PPS signal at the Main PSU port. **Aux**: The ODU will synchronize to a 1PPS signal at the Aux port.
Cambium Sync Output Port	Only displayed when TDD Sync Device = **Cambium Sync Injector**. **None**: The ODU will not output a synchronization signal. **Aux**: The ODU will output a synchronization signal at the Aux port.
TDD Frame Offset	The delay of the start of the TDD frame from the epoch of the external timing reference. This permits the design of synchronized networks in which the phase of the TDD frame is independent of the master/slave function. Enter a value in the range from zero to one microsecond less than the TDD Frame Duration.
TDD Holdover Mode	**Strict**: The unit will not transmit when synchronization is lost. **Best Effort**: The unit will synchronize when there is a reference signal, but otherwise will operate in unsynchronized mode.
TDD Holdover Duration	Specifies duration of holdover period following loss of the external timing reference for TDD synchronization. Default value **10** minutes, maximum **60** minutes.

Confirm Installation Configuration page

Menu option: **Installation** (Figure 142). Use this page to review and confirm the updated wireless configuration of the unit.

Figure 142 Confirm Installation Configuration page (top and bottom of page shown)



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 6-4.
- If IP Address has been changed, use the new IP address to log into the unit.

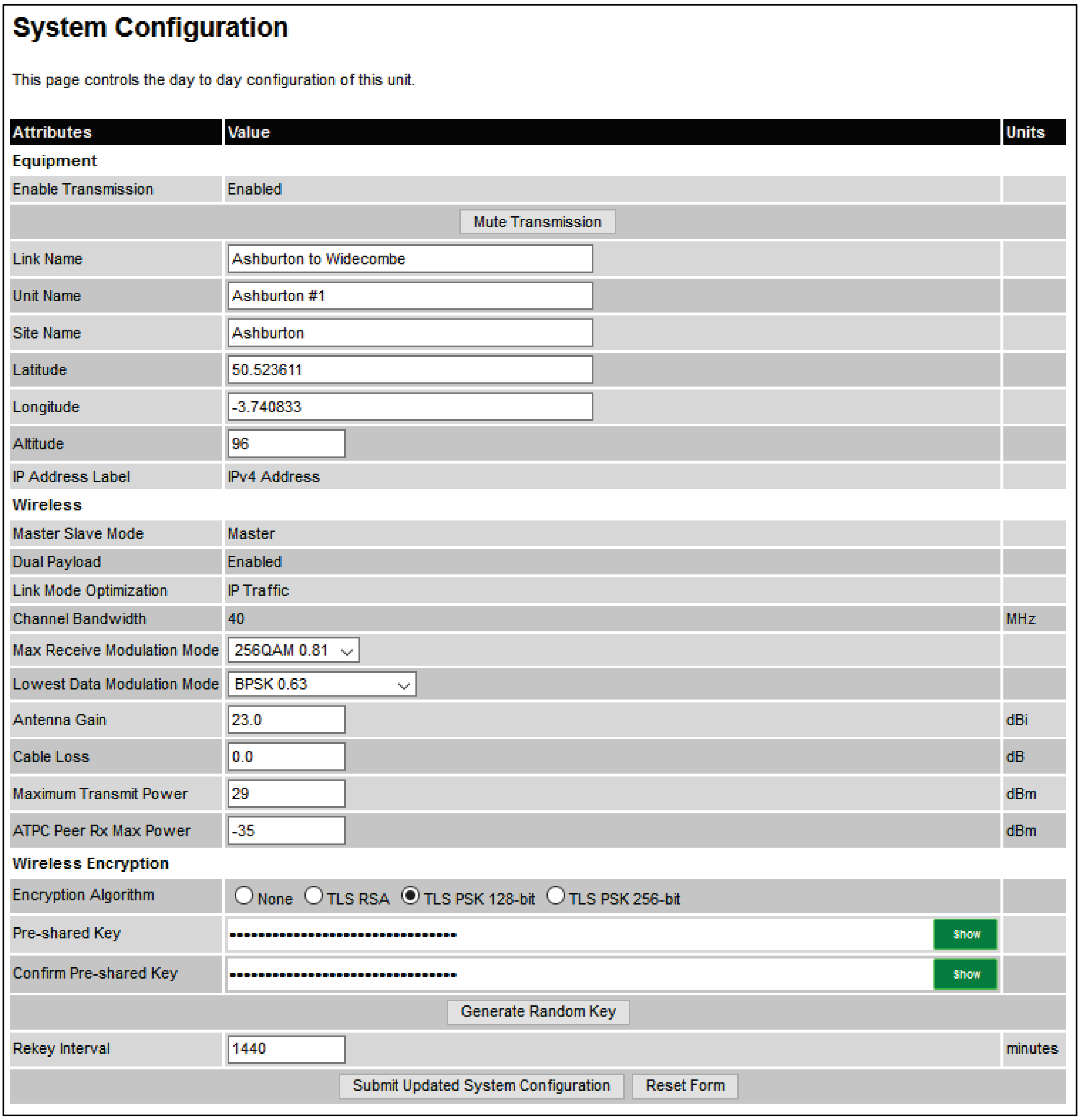
System menu

This section describes how to configure the IP and Ethernet interfaces of the PTP 700 unit.

System Configuration page

Menu option: **System > Configuration** (Figure 143). Use this page to enable AES encryption and to review and update key wireless attributes of the unit.

Figure 143 System Configuration page

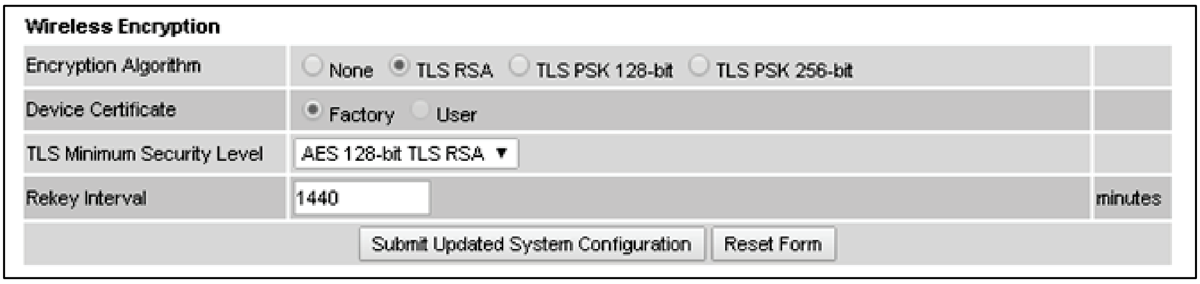


System Configuration

This page controls the day to day configuration of this unit.

Attributes	Value	Units
Equipment		
Enable Transmission	Enabled	
	Mute Transmission	
Link Name	Ashburton to Widecombe	
Unit Name	Ashburton #1	
Site Name	Ashburton	
Latitude	50.523611	
Longitude	-3.740833	
Altitude	96	
IP Address Label	IPv4 Address	
Wireless		
Master Slave Mode	Master	
Dual Payload	Enabled	
Link Mode Optimization	IP Traffic	
Channel Bandwidth	40	MHz
Max Receive Modulation Mode	256QAM 0.81	
Lowest Data Modulation Mode	BPSK 0.63	
Antenna Gain	23.0	dBi
Cable Loss	0.0	dB
Maximum Transmit Power	29	dBm
ATPC Peer Rx Max Power	-35	dBm
Wireless Encryption		
Encryption Algorithm	None TLS RSA TLS PSK 128-bit TLS PSK 256-bit	
Pre-shared Key	•••••••••••••••••••••••••••••••• Show	
Confirm Pre-shared Key	•••••••••••••••••••••••••••••••• Show	
	Generate Random Key	
Rekey Interval	1440	minutes
	Submit Updated System Configuration Reset Form	

Figure 144 System Configuration page, TLS RSA Encryption Algorithm



Attention 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 attribute, or if the Encryption Algorithm attribute provides only the None and TLS RSA 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 6-13).
- Update the attributes (Table 132).
- To save changes, click **Submit Updated System Configuration**.
- If a reboot request is displayed, click **Reboot Wireless Unit** and **OK** to confirm.

Table 132 System Configuration attributes

Attribute	Meaning
Enable Transmission	Only displayed when the ODU is a Master unit and Transmitter Mute Control is enabled (see Webpage Properties page on page 6-76). Use the **Mute Transmission/Enable Transmission** control to toggle between **Muted** and **Enabled**. **Muted:** The ODU will not radiate and will not forward Ethernet frames between the wireless interface and the Ethernet ports. **Enabled**: The ODU is allowed by the user to radiate and will forward Ethernet frames between the wireless interface and the Ethernet ports.
Link Name	This is only visible if the Wireless Topology is set to PTP topology. Link Name may consist of letters (A-Z and a-z), numbers (0-9), spaces, and the following special characters: (),-.,:<=>[]_{}. If Access Method is set to Link Name Access, Link Name must be same at both ends of the link and different to site name.
Unit Name	Unit Name may consist of letters (A-Z and a-z), numbers (0-9), spaces, and the following special characters: (),-.,:<=>[]_{}. Unit name should be unique within the wireless network.
Site Name	User defined name for the site, with additional notes (if required).

Attribute	Meaning
Latitude	The latitude of the ODU, measured in decimal degrees. This attribute has no internal function.
Longitude	The longitude of the ODU, measured in decimal degrees. This attribute has no internal function.
Altitude	The altitude of the ODU, measured in meters. This attribute has no internal function.
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 133).
Master Slave Mode	**Master:** The unit is a Master, that is, it controls the PTP link or HCMP sector. Following startup, the Master transmits continuously, except in the case of radar detection. **Slave:** The unit is a Slave, that is, it listens for its peer and only transmits when the peer has been identified. Read only.
Dual Payload	**Disabled**: The ODU will not request the remote unit to transmit dual payload modulation modes. **Enabled**: The ODU will request the remote unit to transmit single or dual payload modulation modes as determined by the wireless conditions. 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.
Lowest Data Modulation Mode	The lowest modulation mode that must be achieved before the link is allowed to bridge customer data Ethernet frames. This does not affect the bridging of management data: if out-of-band remote management is enabled, this will continue regardless of modulation mode.

Attribute	Meaning
Antenna Gain	Only displayed for a Connectorized ODU, or a Connectorized+Integrated ODU where Anntena Selection is set to **Connectorized**. Gain of the external antenna.
Cable Loss	Only displayed for a Connectorized ODU, or a Connectorized+Integrated ODU where Anntena Selection is set to **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.
Transmitter Channels	Only displayed when the Transmitter Channels Control attribute is enabled (see Webpage Properties page on page 6-76). **H and V:** The ODU transmits on Horizontal and Vertical polarisation **H Only:** The ODU transmits on Horizontal polarisation (or at the H output of a Connectorized unit) only. **V Only:** The ODU transmits on Vertical polarisation (or at the V output of a Connectorized unit) only. **Note** Operation using a single polarisation cannot provide polarisation diversity or polarisation multiplexing. This will reduce availability in non-line-of-sight paths and will reduce capacity in line-of-sight or near-line-of-sight paths.
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 combination of the selected Regulatory Band, Bandwidth and (for connectorized units) Antenna Gain and Cable Loss. Set this attribute to the value specified in the installation report (LINKPlanner). **Note** Maximum Transmit Power is the maximum combined power for the normal case where H and V channels operate together. When Transmitter Channels is set to H Only or V Only, the maximum transmitted power will be 3 dB lower than the configured Maximum Transmit Power.
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.
ATPC Peer Rx Max Power	ATPC maximum receive power level at the remote ODU. In a radar avoidance area this is calculated by the software and cannot be changed. In a non-radar avoidance area this can be set manually.

Attribute	Meaning
Encryption Algorithm	Values are: **None**, **TLS RSA, TLS PSK 128-bit** or **TLS PSK 256-bit**. Use the same setting at both link ends. **TLS PSK 128-bit** and **TLS PSK 256-bit** are only displayed when an AES encryption license key has been generated (Generating license keys on page 6-2) and submitted (Software License Key page on page 6-13). **TLS RSA** cannot be selected if Access Method is set to **Link Name Access**. Encryption Algorithm is not displayed if the only possible value is **None**.
Pre-shared Key	Only displayed when Encryption Algorithm is set to **TLS PSK 128-bit** or **TLS PSK 256-bit**. The key consists of 32 or 64 case-insensitive hexadecimal characters. Use the same key at both link ends.
Confirm Pre-shared Key	Only displayed when encryption algorithm **TLS PSK 128-bit** or **TLS PSK 256-bit** has been selected. Retype the Pre-shared Key.
TLS Minimum Security Level	The minum encryption key size that will be selected in TLS RSA. Values are: **None**, **AES 128-bit TLS RSA** or **AES 256-bit TLS RSA** Only displayed when Encryption Algorithm is set to TLS RSA. **AES 128-bit TLS RSA** or **AES 256-bit TLS RSA** are only available when an AES encryption license key has been generated (Generating license keys on page 6-2) and submitted (Software License Key page on page 6-13). For additional information see TLS RSA on page 1-28
Rekey Interval	The interval (in minutes) between automatic update of the wireless encryption keys. Only displayed when an AES encryption and Over The Air Rekey license key has been generated (Generating license keys on page 6-2) and submitted (Software License Key page on page 6-13). Only displayed at the Master.

LAN Configuration page

Menu option: **System > Configuration > LAN Configuration**. Use this page to control how users connect to the PTP 700 web interface, either from a locally connected computer or from a management network.

The appearance of this page varies depending upon which features have been enabled by license key. For example, Figure 145 shows the attributes that are displayed when Aux Port and Out-of-Band Management Service support are enabled.

Attention Before configuring a VLAN for management interfaces, ensure that the VLAN is accessible, otherwise the unit will be inaccessible after the next reboot.

Attention 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.

Attention 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) 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.

Note Synchronous Ethernet and IEEE 1588 Transparent Clock are only supported in the PTP topology.

Figure 145 LAN Configuration page (Aux, SFP and DNS support)

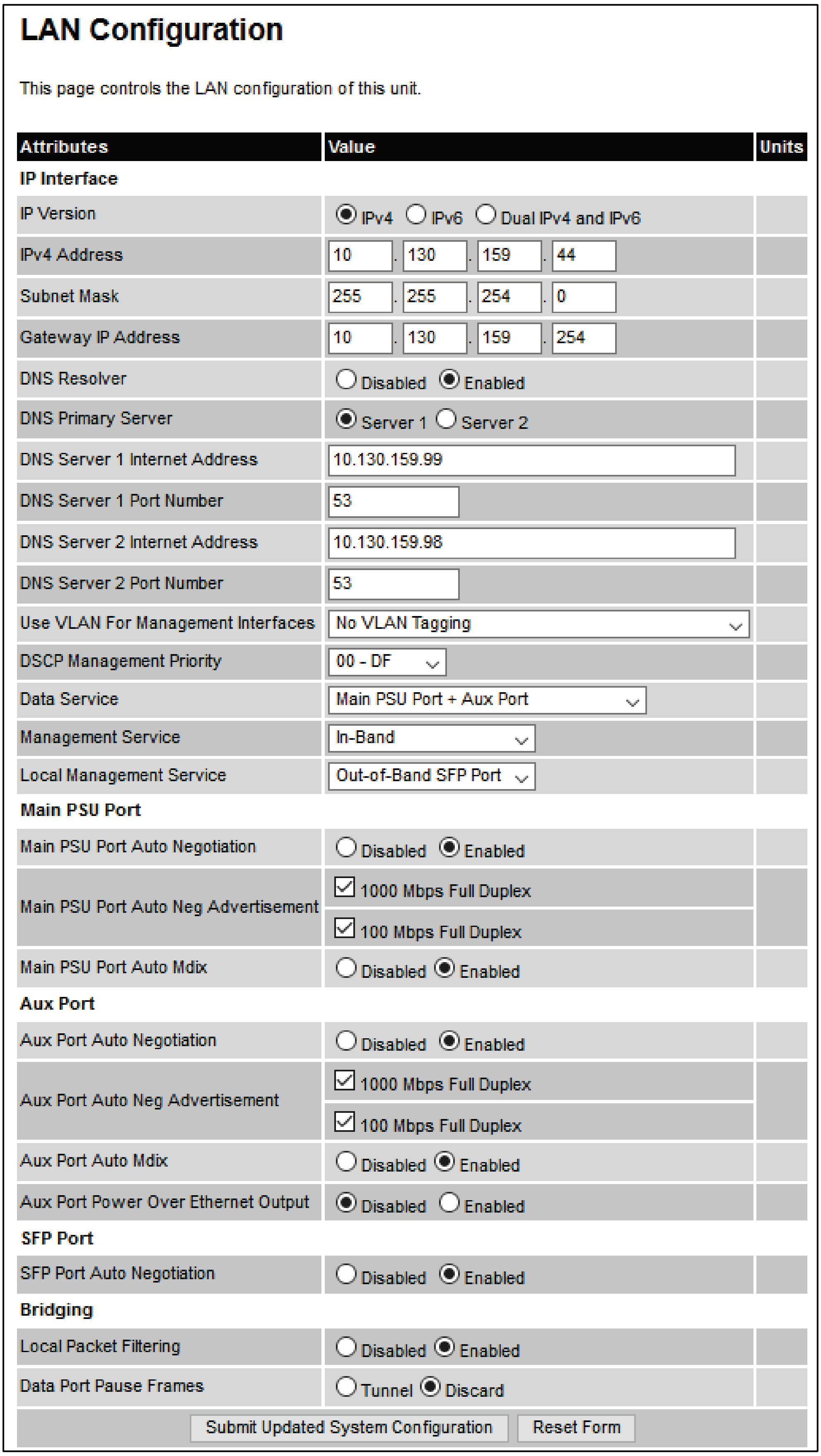
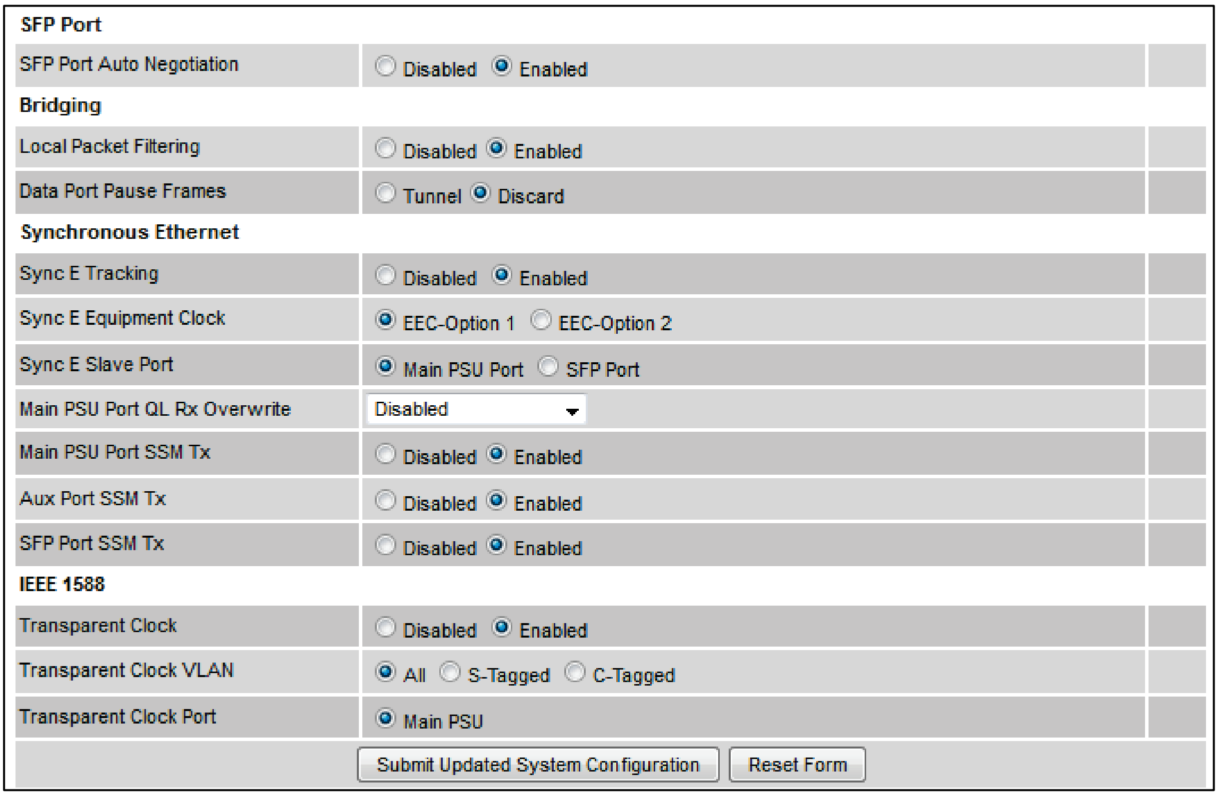


Figure 146 LAN Configuration page (Sync E and IEEE 1588 support)



Procedure:

1 Review and update the attributes: IP Interface (Table 133); Main PSU or Aux Port (Table 134); Bridging (Table 136).

2 To save changes, click **Submit Updated System Configuration**. The system may reboot.

3 If Main PSU Port is selected for **Data Service** only (and not for **Management Service**), connect management PC to the port (Aux or SFP) that was selected for Management or Local Management Service

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 6-4.

5 If IP Address has been changed, use the new IP address to log into the unit.

Table 133 IP interface attributes

Attribute	Meaning
IP Version	Defined in Table 126.
IPv4 Address	
Subnet Mask	
Gateway IP Address	
IPv6 Address	

Attribute	Meaning
IPv6 Prefix Length	
IPv6 Gateway Address	
IPv6 Auto Configured Link Local Address	
DNS Resolver	
DNS Primary Server	
DNS Server 1 Internet Address	
DNS Server 1 Port Number	
DNS Server 2 Internet Address	
DNS Server 2 Port Number	
Use VLAN For Management Interfaces	
VLAN Management VID	
VLAN Management Priority	
DSCP Management Priority	
Data Service	Defined in Table 126. For more help, see Ethernet port allocation on page 3-40.
Management Service	
Local Management Service	
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).

Attribute	Meaning
Management Port Wireless Down Alert	Only displayed when an Out-of-Band Port is selected for Management Service. **Disabled:** The management Ethernet link will not be dropped when the wireless link drops. **Enabled:** The management 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).
Management Network Access Enabled	Only displayed when one of the Port selection attributes (Main PSU, Aux or SFP) is set to **Out-of-Band Management Service**. **Yes:** The local out-of-band management interface can be used to access the remote management network. **No**: The local out-of-band management interface cannot be used to access the remote management network.

Table 134 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. 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 link partner. Use the same setting at both ends.
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 135 SFP Port (connected with copper 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** and SFP port is connected with copper module. 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** and SFP port is connected with copper module. 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	Only displayed when SFP port is connected with copper module. **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.

Table 136 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. If the end station address is unknown, then management traffic is transmitted at the Ethernet port and over the wireless link. In the Local Management Service, 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.

Table 137 Synchronous Ethernet attributes

Attribute	Meaning
Sync E Tracking	**Disabled**: The synchronous Ethernet feature is disabled. Synchronization Status Messages received at the Main PSU port will be discarded. **Enabled**: The synchronous Ethernet feature is enabled.
Sync E Equipment Clock	**EEC-Option 1**: Select this option if the equipment is operating in a 2048 kbit/s synchronisation hierarchy (ITU-T G.813 Option 1) **EEC-Option 2**: Select this option if the equipment is operating in a 1544 kbit/s synchronisation hierarchy (Type IV clock from ITU-T G.812)
Sync E Slave Port	This control configures either the **Main PSU Port** or the **SFP Port** as a candidate for selection as a Sync E Slave port. Only ports that are allocated to one of the standard services (Data Service, Management Service, Local Management Service) are offered as options here.
Main PSU Port QL Rx Overwrite	This control provides the facility to overwrite the Quality Level (QL) of received Synchronisation Status Messages (SSM). It may be useful in a test environment, or for interworking with equipment that does not generate SSMs. **Disabled:** The recommended setting, the QL of received SSMs is unmodified. "**QL-PRC**" or "**QL-SSU A / QL-TNC**" or "**QL-SSU B**" or "**QL-EEC1 / QL-SEC**" or "**QL-DNU / QL-DUS**": The overwritten value of the QL. Where two QLs are given, the QL used is dependent upon the setting of "Sync E Equipment Clock" type.
SFP Port QL Rx Overwrite	This control provides the facility to overwrite the Quality Level (QL) of Synchronisation Status Messages (SSM) received at the SFP port. It may be useful in a test environment, or for interworking with equipment that does not generate SSMs. **Disabled:** The recommended setting, the QL of received SSMs is unmodified. "**QL-PRC**" or "**QL-SSU A / QL-TNC**" or "**QL-SSU B**" or "**QL-EEC1 / QL-SEC**" or "**QL-DNU / QL-DUS**": The overwritten value of the QL. Where two QLs are given, the QL used is dependent upon the setting of "Sync E Equipment Clock" type. This control is hidden if Sync E Slave Port is set to Main PSU Port.
Main PSU Port SSM Tx	**Disabled**: SSMs are not transmitted from the Main PSU port. Disabling SSMs may be useful in a test environment. **Enabled**: SSMs are transmitted from the Main PSU port (normal operation)

Attribute	Meaning
Aux Port SSM Tx	**Disabled**: SSMs are not transmitted from the Aux Port. Disabling SSMs may be useful in a test environment. **Enabled**: SSMs are transmitted from the Aux Port (normal operation)
SFP Port SSM Tx	**Disabled**: SSMs are not transmitted from the SFP port. Disabling SSMs may be useful in a test environment. **Enabled**: SSMs are transmitted from the SFP port (normal operation)

Table 138 IEEE 1588 attributes

Attribute	Meaning
Transparent Clock	**Disabled**: The Transparent Clock function is disabled. IEEE 1588-2008 event frames will be forwarded, but residence time corrections will not be made. **Enabled**: The Transparent Clock function is enabled. Residence time corrections will be made to IEEE 1588-2008 event frames.
Transparent Clock Port	This specifies the transparent clock source port. It can be Main PSU, Aux Port or SFP Fiber. Only the ports allocated for the Data service are available for selection.
Transparent Clock VLAN	**All**: The recommended setting. Residence time corrections will be made to all IEEE 1588-2008 event frames, regardless of any VLAN encapsulation. **S-Tagged**: Residence time corrections are only made to event frames tagged with a service tag equal to “Transparent Clock VID”. **C-Tagged**: Residence time corrections are only made to event frames double tagged and with a customer tag equal to “Transparent Clock VID”.
Transparent Clock VID	The VLAN Identifier (VID) used with “Transparent Clock VLAN” to restrict residence time corrections to IEEE 1588-2008 event frames in a specific VLAN.

QoS Configuration page

Menu option: **System > Configuration > QoS Configuration** (Figure 147 or Figure 148 or Figure 149). 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.

> **Note** In PTP topology, eight QoS levels (Q0 to Q7) are supported, while in HCMP topology, only four QoS levels (Q0 to Q3) are supported for each wireless link.

Figure 147 QoS Configuration page (Ethernet)

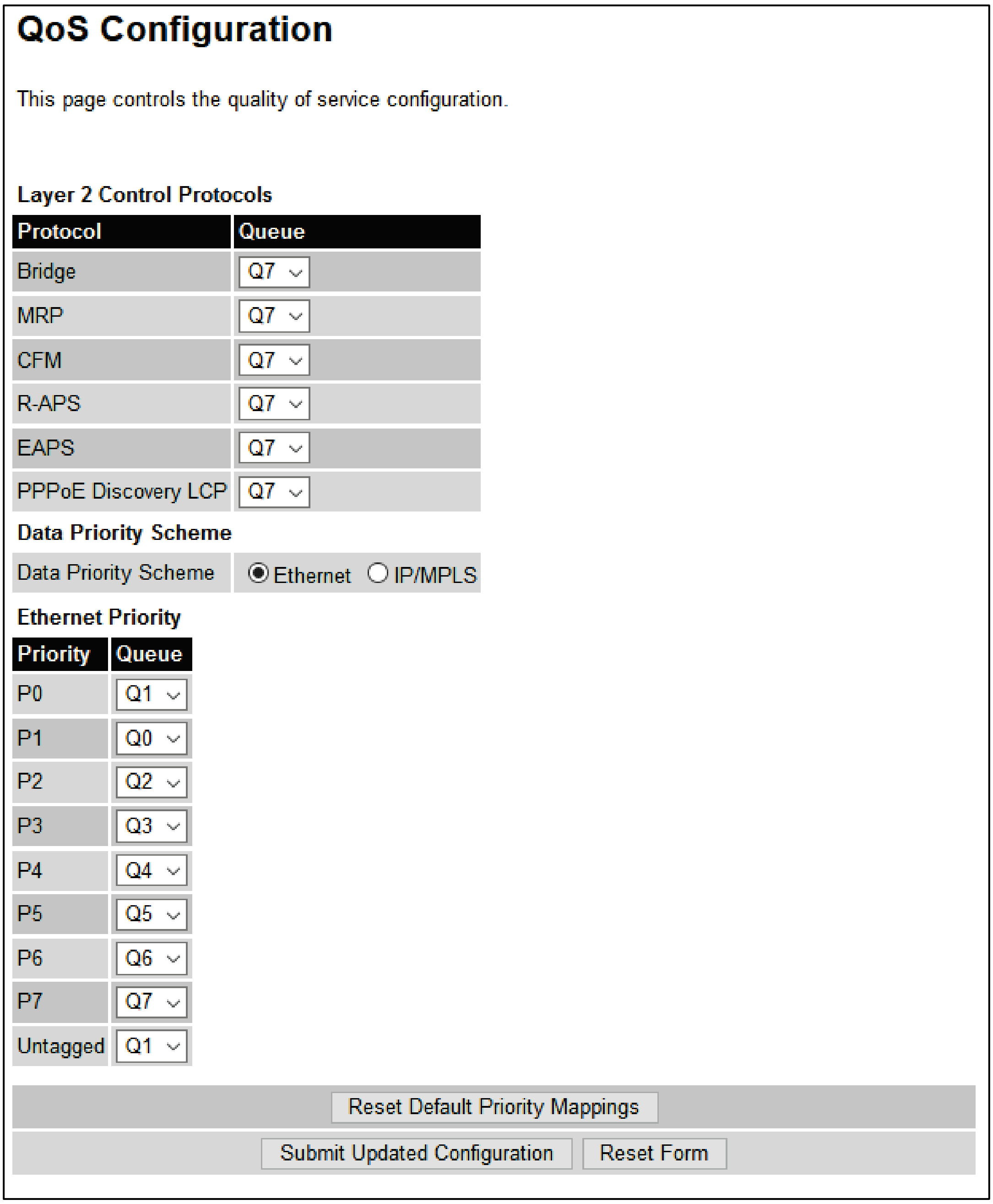


Figure 148 QoS Configuration page (IP/MPLS), Extract

Data Priority Scheme

Data Priority Scheme	○ Ethernet ◉ IP/MPLS

Unknown Network Layer Protocol

Unknown Protocol	Q1

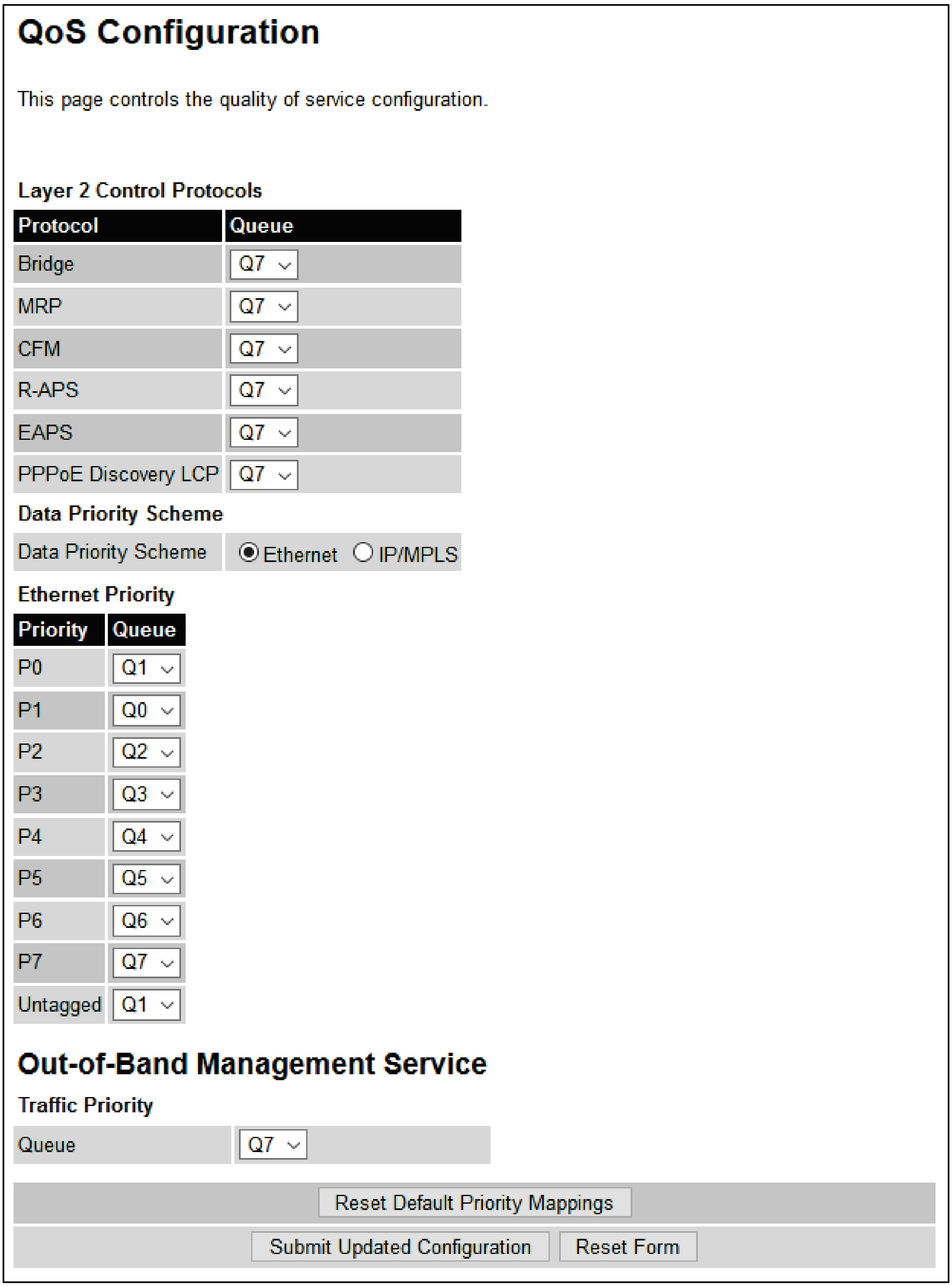
IP DSCP

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

Figure 149 QoS Configuration page showing Out-of-Band Management



Procedures:

- Review and update the attributes (Table 139 and Table 140).
- 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 139 QoS Configuration attributes – Data Service

Attribute	Meaning
Bridge MRP CFM R-APS EAPS PPPoE Discovery LCP	The classification of each layer 2 control protocol (L2CP) to an egress queue at the wireless port.
Data 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.
Ethernet Priority	Ethernet priority mapping to Queue

Table 140 QoS Configuration attributes –Out-of-Band Managment Service

Attribute	Meaning
Queue	Only displayed when one ODU port is allocated to **Out-of-Band Management** (Configuring port allocations on page 6-21). The classification of out-of-band management traffic 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 150) or copper (Figure 151) 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 150 SFP Configuration page (optical 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 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	CA51QA098	
Sfp Date Code	101214	

Figure 151 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	

[Submit Updated System Configuration] [Reset Form]

Procedure (only applies when copper SFP module is installed):

- Update the attributes
    - When optical SFP module is installed (Table 143).
    - When copper SFP module is installed (Table 142)
- To save changes, click **Submit Updated System Configuration**.

Table 141 SFP Configuration (Optical 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.

Table 142 SFP Configuration (copper SFP module) attributes

Attribute	Meaning
SFP Port Auto Negotiation	**Disabled:** Configuration of the fiber interface is forced. This is to be used as a last resort only if auto-negotiation fails. **Enabled:** Configuration of the fiber 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.

Authorization Control page

Menu option: **System > Configuration > Authorization Control** (Figure 152).

Authorization control is used when Access Method is configured to **Group Access**, and Encryption Algorithm is configured to **TLS-RSA**. In the HCMP topology, Group Access is the only Access Method supported. In the PTP topology, Group Access is available only with the Group Access license. The Authorization Control page is hidden if it is not applicable.

When Authorization Method is configured to Whitelist, the ODU will connect only if the authenticated MAC address of the remote unit is in the list of authorized ODUs. With the Blacklist option, the ODU will always connect unless the authenticated MAC address has been added to a list of unauthorized ODUs.

The Authorization Control page allows up to 32 MAC addresses to be entered.

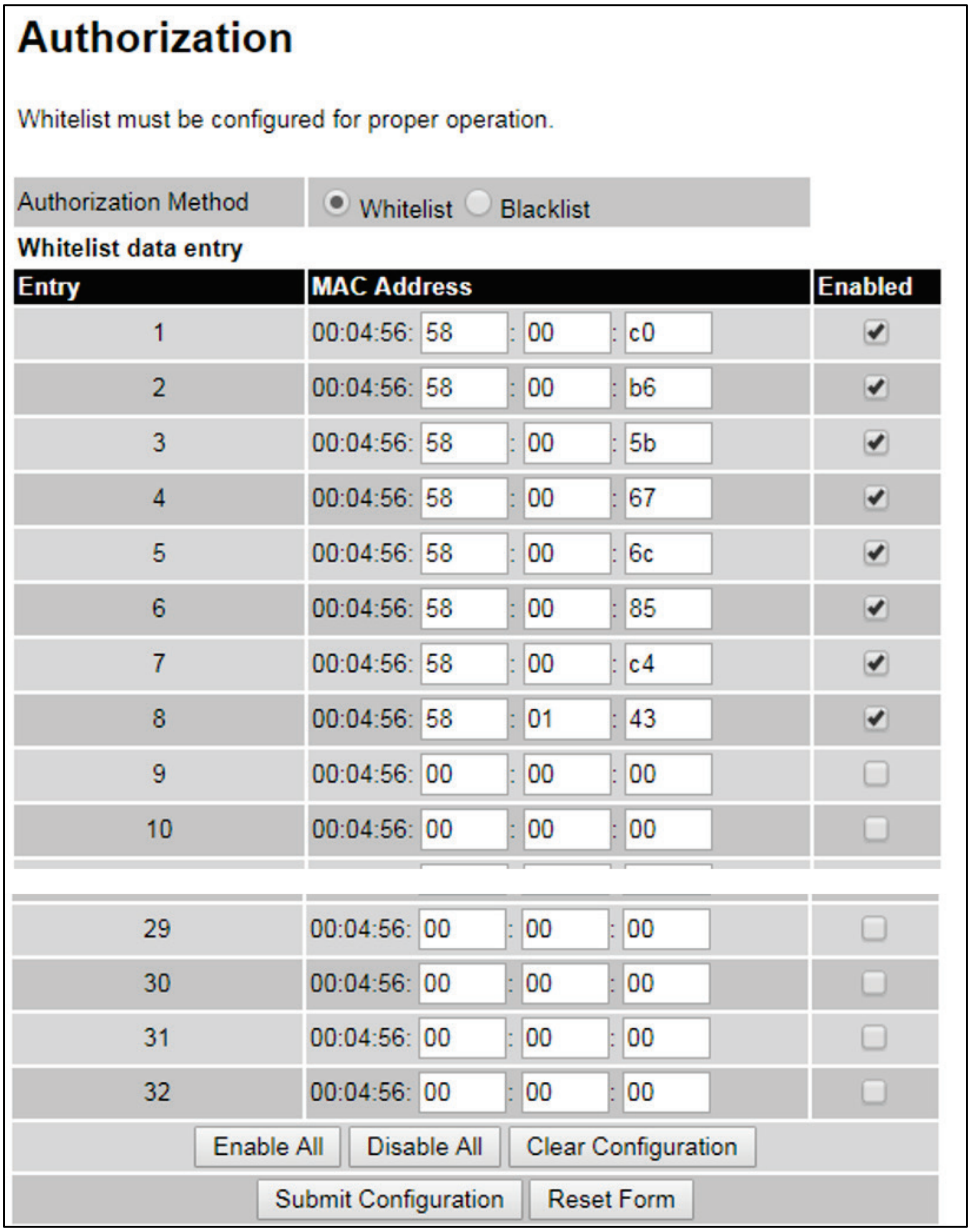
Authorization Control does not require an AES license.

Procedure:

- Select **Whitelist** or **Blacklist**
- Update the MAC Addresses
- To save changes, click **Submit Configuration**.

Note The associated wireless link is automatically dropped if the MAC address of an already-connected ODU is added to the Blacklist or removed from the Whitelist.

Figure 152 Authorization Control page

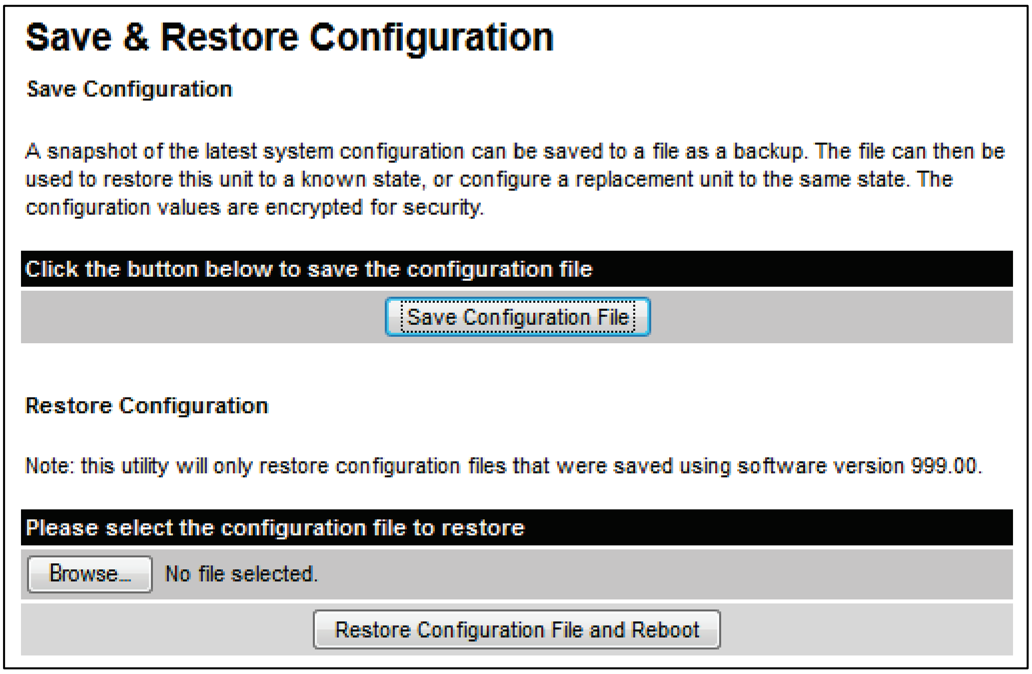


Save and Restore Configuration page

Menu option: **System > Configuration > Save And Restore** (Figure 153).

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 153 Save & Restore Configuration page



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 700 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
- 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
- User-supplied Device Private Key
- User-supplied Device Public Key Certificate
- User-supplied Root CA Certificate
- SNMP Control Of HTTP And Telnet
- SNMP Control of Passwords
- Unit Name

Procedures:

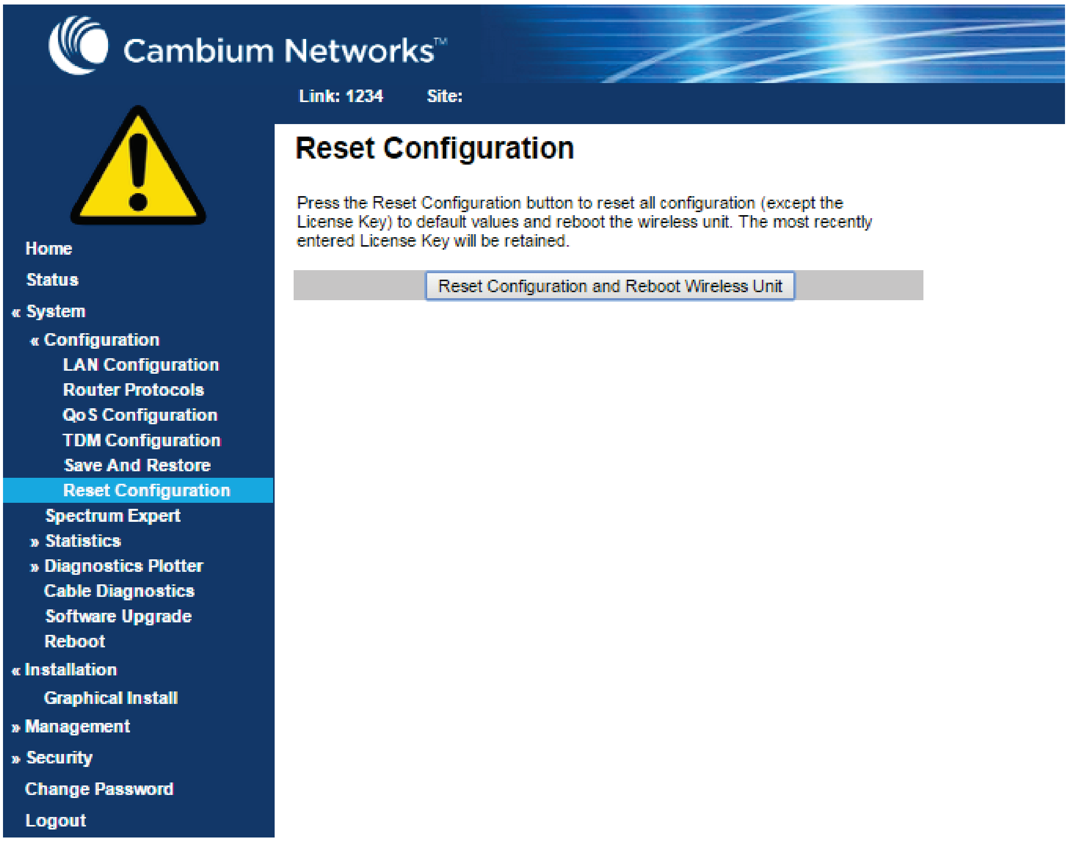
- To save the configuration:
  - Click Save Configuration File.
  - Save the file. The default filename is in the format **MAC-mm-mm-mm_IP-iii-iii-iii-iii.cfg**, where **mm-mm-mm** is MAC address of unit and **iii-iii-iii-iii** is Internet address of unit.
- To restore the configuration:
  - Click **Browse** 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.

Reset Configuration page

Menu option: **System > Configuration > Reset Configuration**. Use this page to reset the ODU configuration to default settings, retaining the most recently entered License Key (Figure 154).

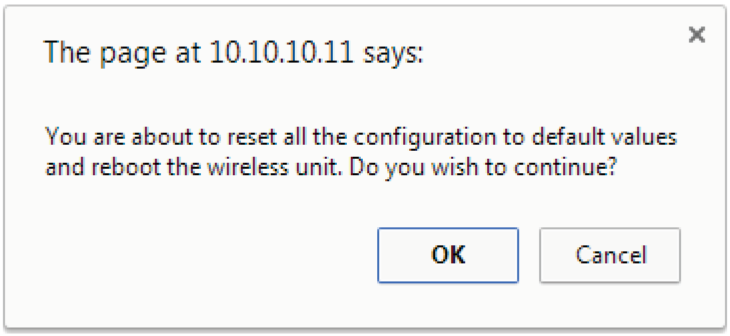
The Reset Configuration page resets the configuration to default settings. After successful execution of Reset Configuration, the ODU reboots and is then accessible via the default IP address (i.e. 169.254.1.1).

Figure 154 Reset Configuration page



Procedure:

- Click **Reset Configuration**. The user pop up box is displayed to reconfirm:



- Click **OK** to restore configuration to the default settings and reboot of unit.

Further reading

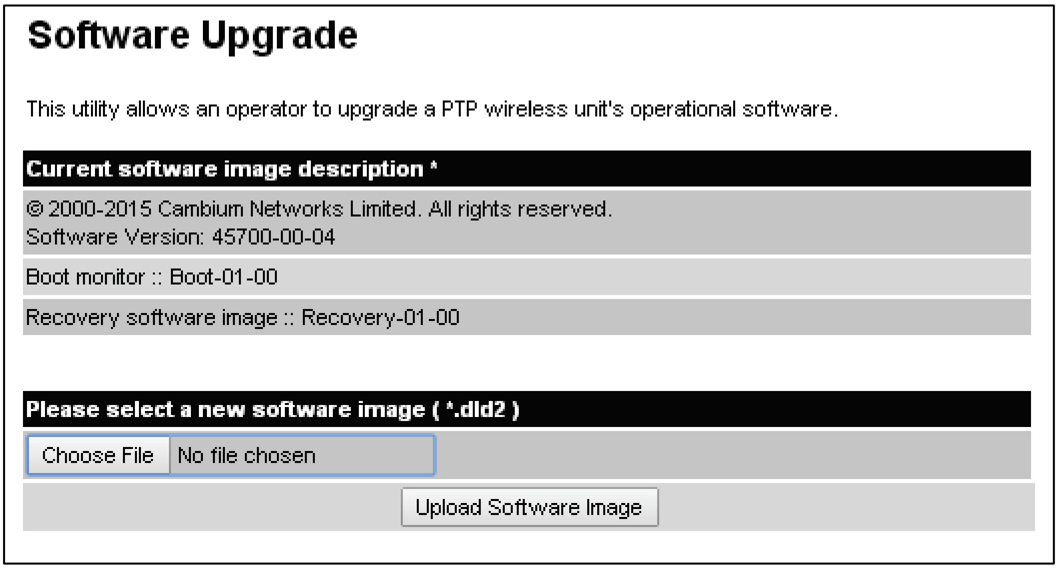
For information about…	Refer to…
Erase Configuration	Use this option to erase the entire configuration of the unit. Refer to Resetting all configuration data on page 7-78.

Software Upgrade page

Menu option: **System > Software Upgrade** (Figure 155).

Use this page to upgrade the unit to a new version of PTP 700 operational software.

Figure 155 Software Upgrade page



Attention Ensure that the correct units are upgraded, as units cannot easily be downgraded afterwards.

Attention 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.

Attention 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 700 Series**.
- If the support web page contains a later Software Version than that installed on the PTP 700 unit, perform the procedure below.

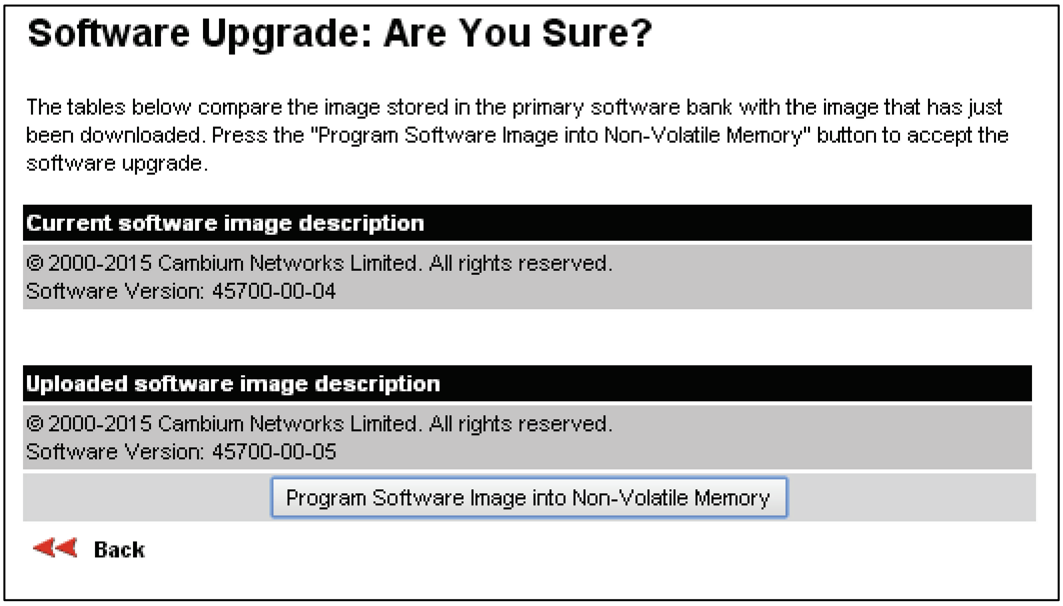
Procedure:

1 Save the system configuration; see Save and Restore Configuration page on page 6-62.

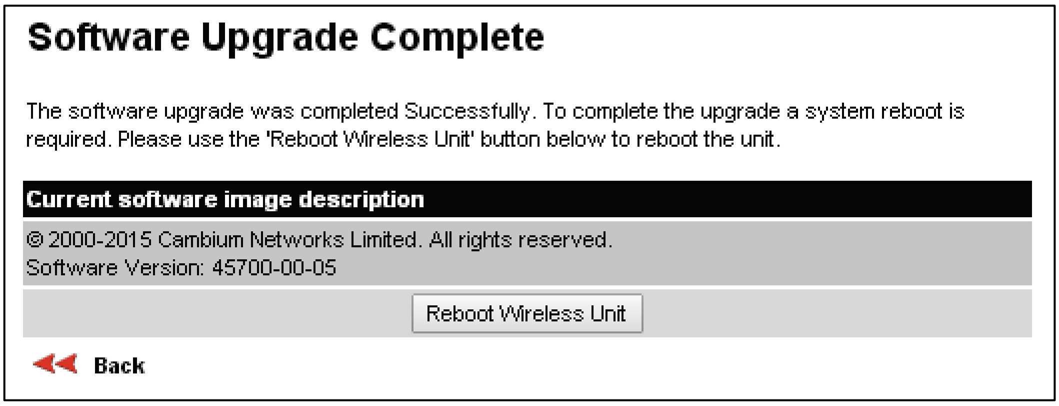
2 On the Cambium Support web page, select the latest PTP 700 software image (dld2 file) and save it to the local management PC.

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:



5 Click **Program Software Image into Non-Volatile Memor**y. The Progress Tracker page is displayed. On completion, the Software Upgrade Complete page is displayed:



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 and Restore Configuration page on page 6-62.

Note The unit will not upload FIPS versions of the software unless the unit has the AES encryption and FIPS licenses installed.

Note CSPs are automatically zeroized if FIPS software is loaded in a unit to replace standard (non-FIPS) software, or standard (non-FIPS) software is loaded in a unit to replace FIPS software.

Management menu

This section describes how to configure web-based management of the PTP 700 unit.

Web-Based Management page

Menu option: **Management > Web** (Figure 156).

Use this page to configure web-based management of the unit.

Figure 156 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	
Submit Updated Configuration	Reset Form	

Attention 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. (see Planning for HTTPS/TLS operation on page 3-57).

Procedure:

- Review and update the attributes (Table 143).
- To save changes, click **Submit Updated Configuration**.

Table 143 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**.
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 6-128.

Attribute	Meaning
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

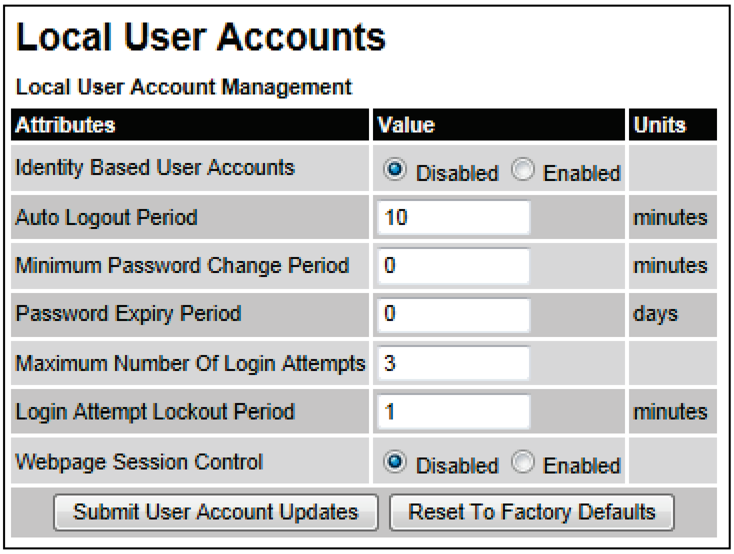
Menu option: **Management > Web > Local User Accounts**.

The contents of this page depend upon the setting of Identity Based User Accounts: **Disabled** (Figure 157) or **Enabled** (Figure 158).

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 6-115.

Figure 157 Local User Accounts page (Identity Based User Accounts disabled)



Local User Accounts

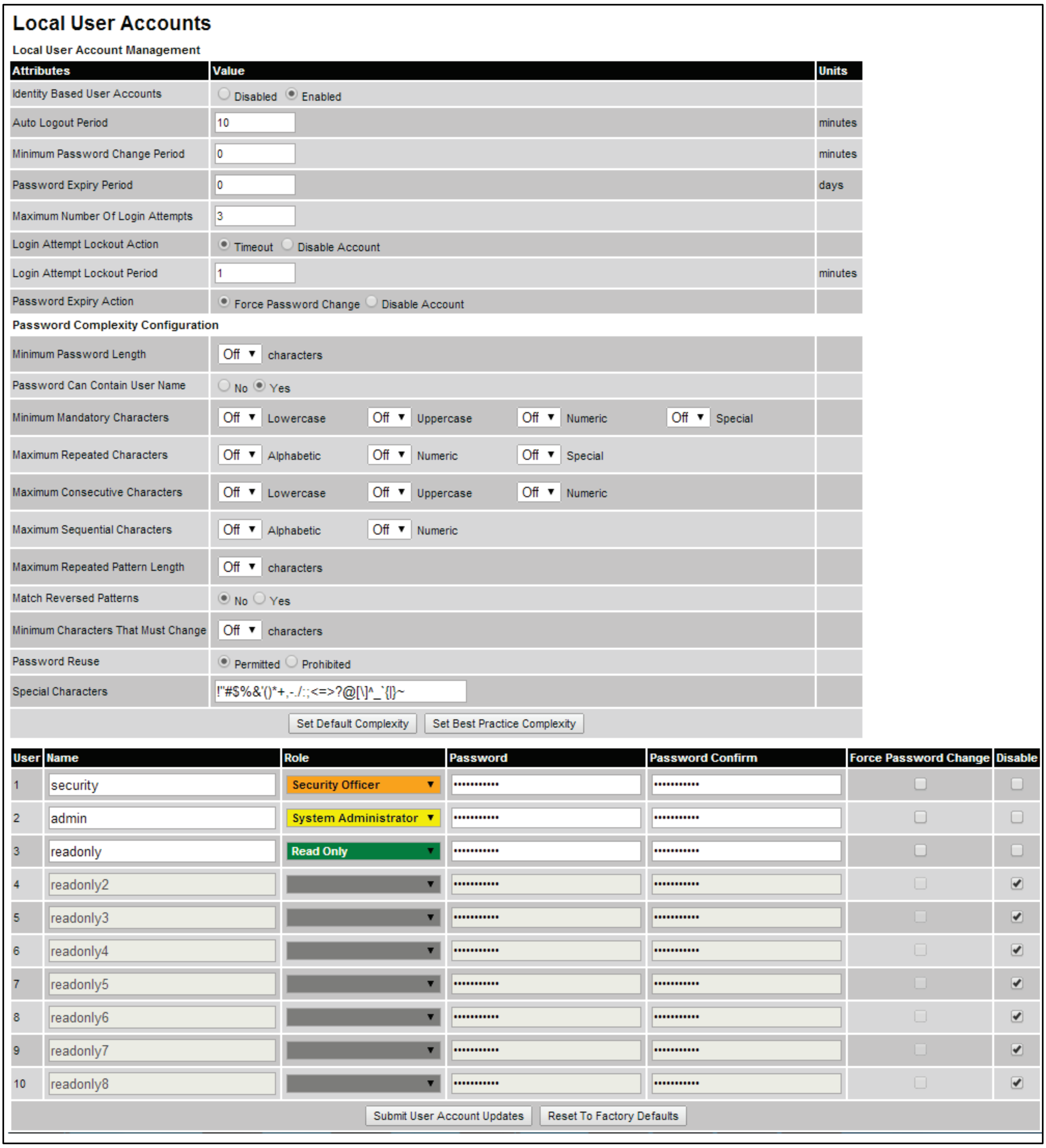
Local User Account Management

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	

Submit User Account Updates | Reset To Factory Defaults

Note Identity Based User Accounts is automatically set to **Enabled** in the FIPS 140-2 secure mode.

Figure 158 Local User Accounts page (Identity Based User Accounts enabled)



Procedure:

- Choose whether to set Identity Based User Accounts to **Disabled** or **Enabled**.
- Review and update the Local User Account Management attributes (Table 144).
- If Identity Based User Accounts is set to **Enabled:**
  - Review and update the Password Complexity Configuration attributes (Table 145). 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 146).
- If any attributes have been updated, click **Submit User Account Updates**.

Table 144 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**.
Password Expiry Action	Only displayed when Identity Based User Accounts is **Enabled**. The action to be taken by the PTP 700 when a password expires.

Table 145 Password Complexity Configuration attributes

Attribute	Meaning	Best practice
Minimum Password Length	The minimum number of characters required in passwords.	8
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.	Off
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.	Off
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
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

Attribute	Meaning	Best practice
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 146 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 145).
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.

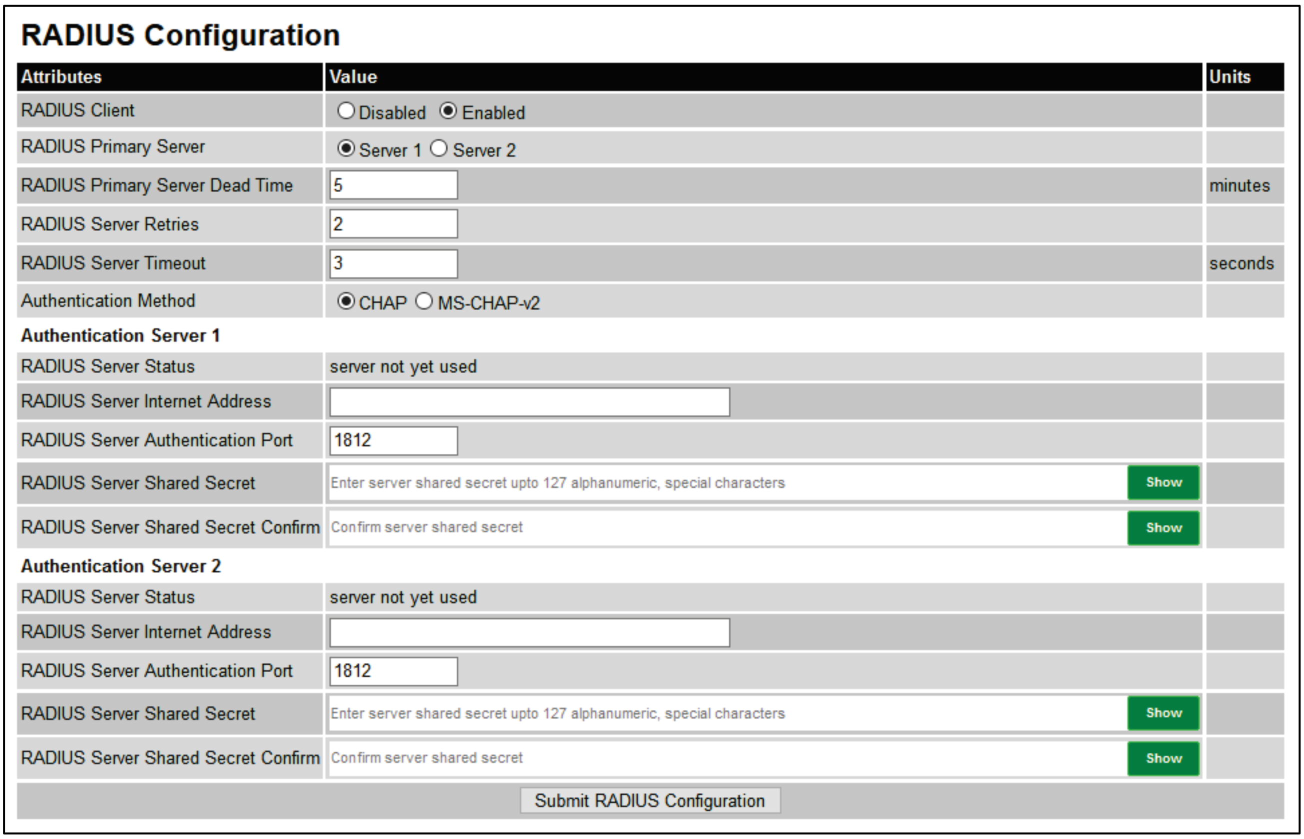
Note At least one user must be assigned the Security Officer role. If RADIUS is enabled, then this rule is relaxed, in which case the RADIUS server(s) SHOULD be configured with at least one user with **Security Officer** privileges.

RADIUS Configuration page

Menu option: **Management** > **Web** > **Radius Configuration** (Figure 159).

Use this page to configure RADIUS authentication. RADIUS authentication is only available when PTP 700 is configured for Identity-based User Accounts and when RADIUS servers are connected to the network.

Figure 159 RADIUS Configuration page



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.

Note RADIUS is disabled in the FIPS 140-2 Approved Mode.

Procedure:

- Update the attributes (Table 147).
- Click **Submit RADIUS Configuration**.

Table 147 RADIUS Authentication attributes

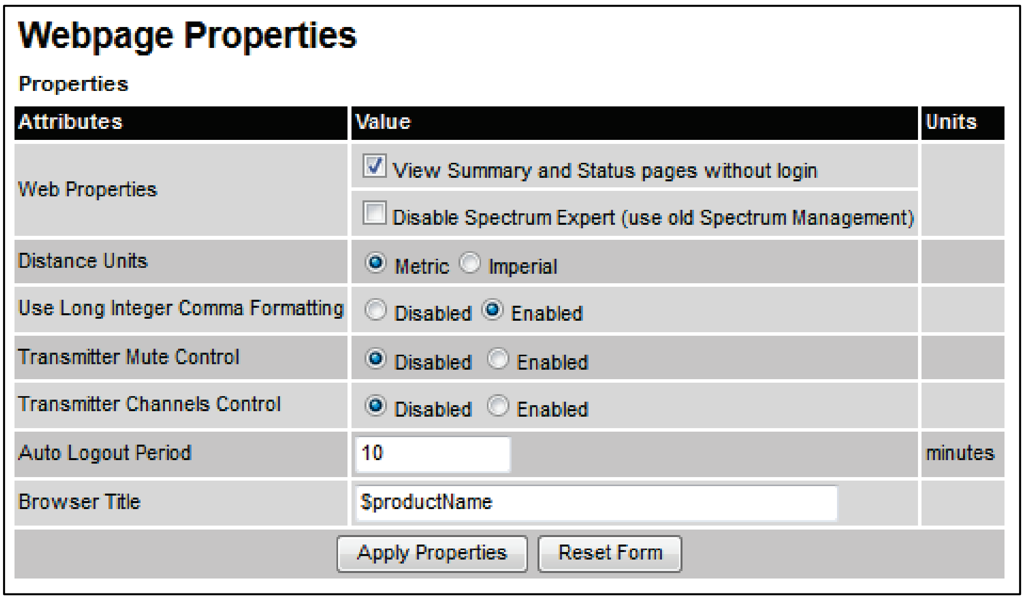
Attribute	Meaning
RADIUS Client Enabled	**Enabled:** PTP 700 users may be authenticated via the RADIUS servers. **Disabled**: RADIUS authentication is not used. This may only be selected if at least one user with Security Officer privileges exists.
RADIUS Primary Server	Specifies the primary server, 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 700 will retry after a RADIUS server fails to respond to an initial request.
RADIUS Server Timeout	Time (in seconds) the PTP 700 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	FQDN, 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.
RADIUS Server Shared Secret Confirm	Shared secret confirmation.

Webpage Properties page

Menu option: **Management > Web > Web Properties** (Figure 160).

Use this page to control the display of the web interface.

Figure 160 Webpage Properties page



Procedure:

- Update the attributes (Table 148).
- Click Apply Properties.

Table 148 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 7-17. **Disable Spectrum Expert (use old Spectrum Management):** • If not ticked (the default setting), the System Menu includes Spectrum Expert (not Spectrum Management). • If ticked, the System Menu includes Spectrum Management (not Spectrum Expert).
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.
Transmitter Mute Control	**Disabled:** Hides the Enable Transmission attribute. **Enabled:** Shows the Enable Transmission attribute (System Configuration page on page 6-42).

Attribute	Meaning
Transmitter Channels Control	**Disabled:** Hides the Transmitter Channels attribute. **Enabled:** Shows the Transmitter Channels attribute (Wireless Configuration page on page 6-24 and System Configuration page on page 6-42).
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, web browser tab titles display PTP 700 model, page title and IP address in the following format: “Cambium PTP 45700 – “ & pageName & “ (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 149.

Table 149 Browser Title attribute variables

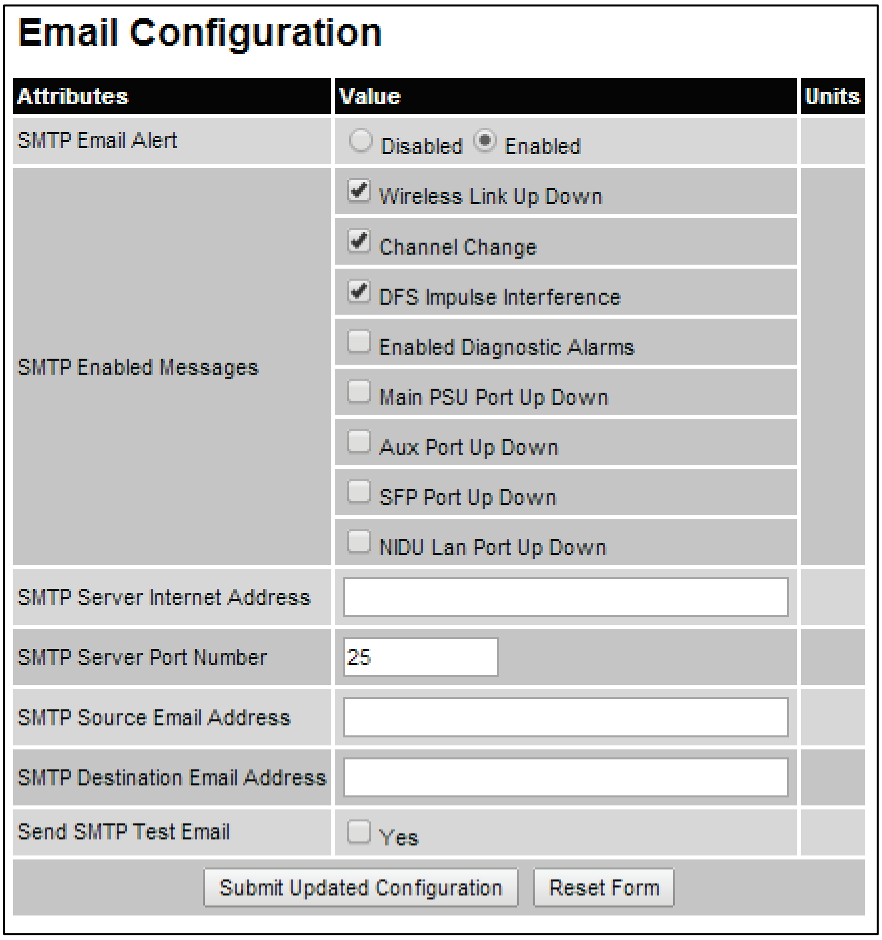
Variable	Meaning
$groupID	
$ipAddress	IP Address currently used to identify the ODU, either IPv4 or IPv6 Address, depending upon the setting of IP Address Label in the System Configuration page (Table 132): • **IPv4**: $ipAddress = $ipv4Address • **IPv6**: $ipAddress = $ipv6Address (if not blank) or $ipv6LinkLocalAddress
$ipv4Address	IPv4 Address of the ODU, as set in the LAN Configuration page (Table 133).
$ipv6Address	IPv6 Address of the ODU, as set in the LAN Configuration page (Table 133).
$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 133).
$linkName	Link Name, as set in the System Configuration page (Table 132).

Variable	Meaning
$masterSlaveMode	Master Slave Mode, as set in the Step 2: Wireless Configuration page (Table 128).
$productName	The product variant, for example **Cambium PTP 700**. Not updateable.
$pageName	Name of the page currently being browsed.
$protectionMode	Role and status of the ODU in a Hot Standby link. For example, “Primary Master, Standby”.
$siteName	Site Name, as set in the System Configuration page (Table 132).
$sysName	Sys Name for this SNMP managed node, as set in the Step 2: SNMP MIB-II System Objects page (Table 155).
$unitName	

Email Configuration page

Menu option: **Management** > **Email** (Figure 161). Use this page to enable the PTP 700 to generate Simple Mail Transfer Protocol (SMTP) email messages to notify the system administrator when certain events occur.

Figure 161 Email Configuration page



Procedure:

- Update the attributes (Table 150).
- 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 150 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 FQDN, 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 700 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 700 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.

Instant Messaging page

Menu option: **Management** > **Instant Messaging** (Figure 162).

Use this page to send text-based messages to an operator at the remote end of the wireless link. Type the message (maximum 180 characters) in the edit box and press the **Send** button. The message is added to the message history when it has been received at the remote end of the link.

Instant Messaging is available in PTP and HCMP topologies. At an HCMP Master ODU, select the destination Slave ODU from a list of connected ODUs. HCMP Slaves can exchange messages with the associated Master ODU through this service but HCMP Slaves cannot message each other.

The ODU provides an alert in the Status Bar (Figure 163) if messages are received when the Instant Messaging page is not displayed.

Figure 162 Instant Messaging page

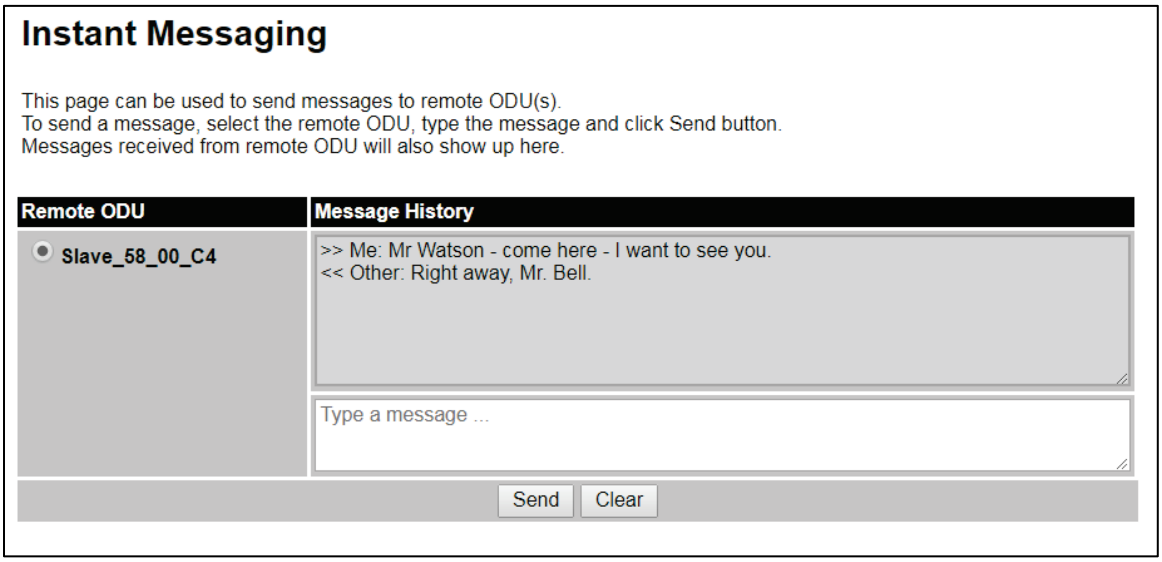


Figure 163 Unread messages

Diagnostic Alarms page

Menu option: **Management** > **Diagnostic Alarms** (Figure 164).

Use this page to select which diagnostic alarms will be notified to the system administrator.

Figure 164 Diagnostic Alarms page

Diagnostic Alarms

Attributes	Value	Units
Enabled Diagnostic Alarms	Regulatory Band	
	Install Status	
	Install Arm State	
	Unit Out Of Calibration	
	Maximum Link Range Exceeded	
	Incompatible Regulatory Bands	
	Incompatible Master And Slave	
	Port State	
	No Wireless Channel Available	
	SNTP Synchronization Failed	
	Wireless Link Disabled Warning	
	TDD Synchronization Alarm	
	Link Mode Optimization Mismatch	
	Syslog Disabled Warning	
	Syslog Local Nearly Full	
	Syslog Local Wrapped	
	Syslog Client Disabled Warning	
	Data Bridging Status	
	Remaining Full Capacity Trial Time	
	Capacity Variant Mismatch	
	TDM Alarms	

Procedure:

- Tick the required alarms. These alarms are described in Alarms on page 7-18.
- Click **Submit Updated Configuration**.

Time Configuration page

Menu option: **Management > Time** (Figure 165 and Figure 166). Use this page to set the real-time clock of the PTP 700.

Setting the real-time clock manually

Use this procedure to keep time without connecting to a networked time server.

If SNTP is disabled, it will be necessary to reset the time manually after each system reboot.

Procedure:

- Set SNTP State to **Disabled** (Figure 165).
- Review and update the manual clock attributes (Table 151).
- Click **Submit Updated Configuration**.

Figure 165 Time Configuration page (SNTP disabled)

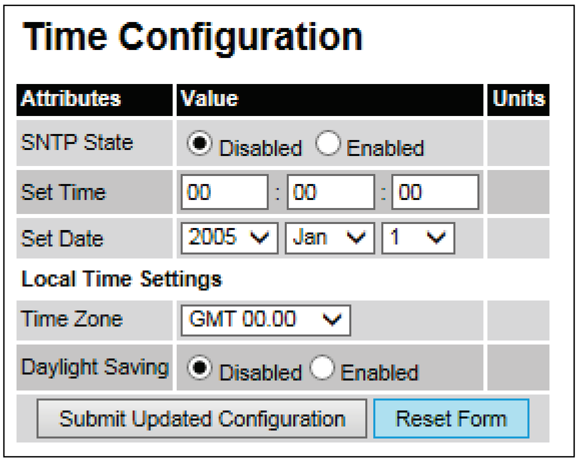


Table 151 Manual clock attributes

Attribute	Meaning
SNTP State	**Disabled:** the PTP 700 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** (Figure 166).
- Review and update the SNTP clock attributes (Table 152).
- Click **Submit Updated Configuration**.

Figure 166 Time Configuration page (SNTP enabled)

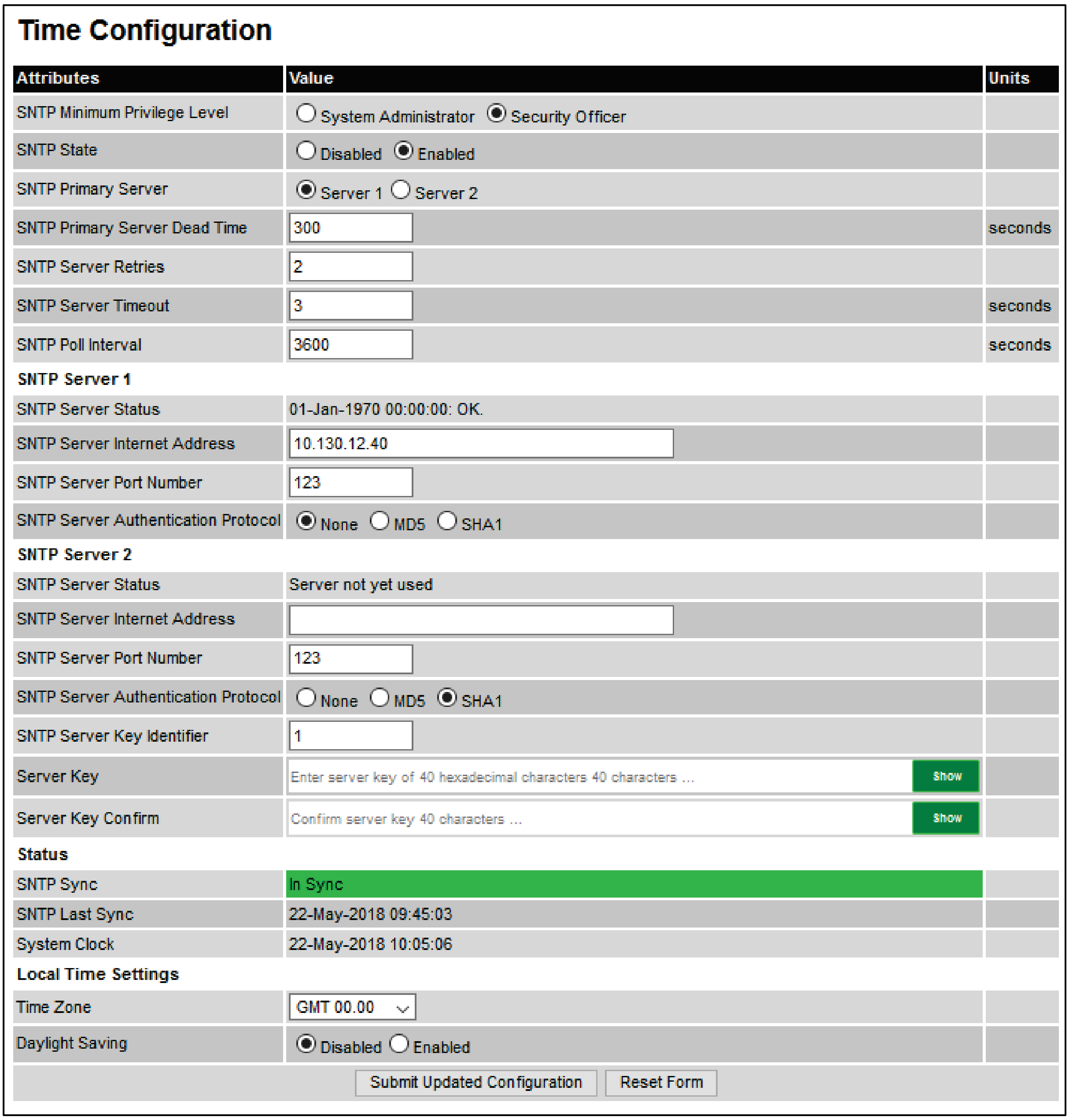


Table 152 SNTP clock attributes

Attribute	Meaning
SNTP Minimum Privilege Level	Minimum security level which is permitted to administer SNTP security settings. Only displayed when Identity Based User Accounts are **Enabled** on the User Accounts page (Table 144).
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.

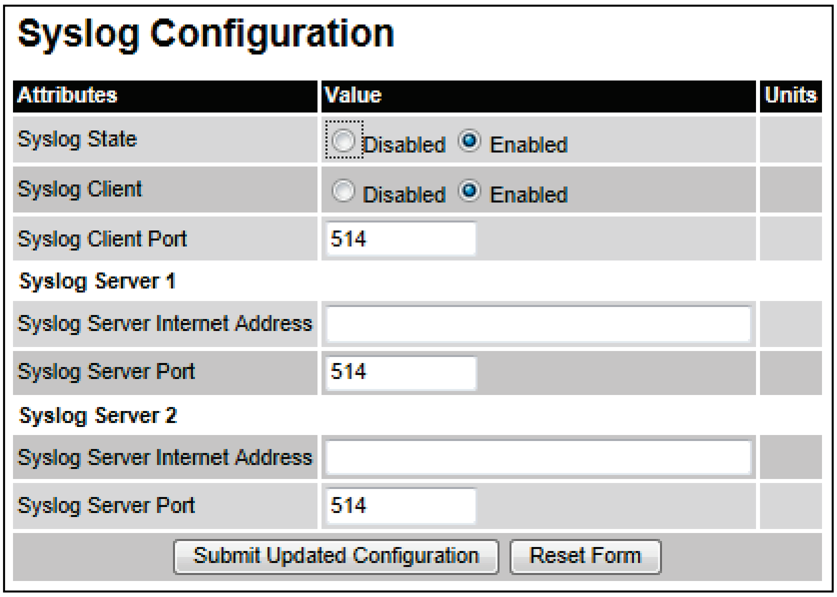
Attribute	Meaning
SNTP Primary Server Dead Time	Time (in seconds) to wait before retrying communications with an unresponsive primary SNTP server. Setting the value to zero disables the timer.
SNTP Server Retries	Number of times the PTP will retry after an SNTP server fails to respond.
SNTP Server Timeout	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 FQDN, 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, MD5 or SHA1).
SNTP Server Key Identifier	SNTP key identifier. A key of zeros is reserved for testing.
Server Key	Key used to authenticate SNTP communications. For SHA1, the key must be exactly 40 hexadecimal characters.
Server Key Confirm	Must match the Server Key.
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.
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 167).

Use this page to configure system logging. Only users with **Security Officer** role are permitted to configure the syslog client.

Figure 167 Syslog Configuration page



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 6-82).

Procedure:

- Update the attributes (Table 153).
- Click **Submit Updated Configuration**.

Table 153 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 FQDN, IPv4 or IPv6 Address of the syslog server. Delete the Internet address to disable logging on the syslog server.
Syslog Server Port	The server port at which syslog messages are received.

SNMP pages (for SNMPv3)

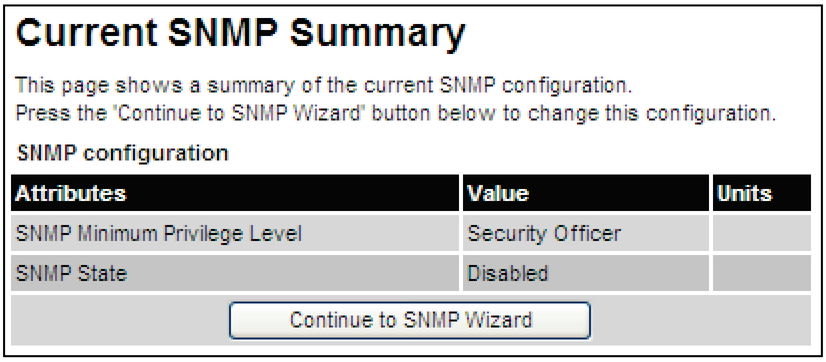
This section describes how to configure Simple Network Management Protocol version 3 (SNMPv3) traps using the SNMP Wizard.

Current SNMP Summary (for SNMPv3)

Menu option: **Management > SNMP** (Figure 168).

Use this page to review the current SNMP configuration and start the SNMP Wizard.

Figure 168 Current SNMP Summary page (when SNMP is disabled)



Procedure:

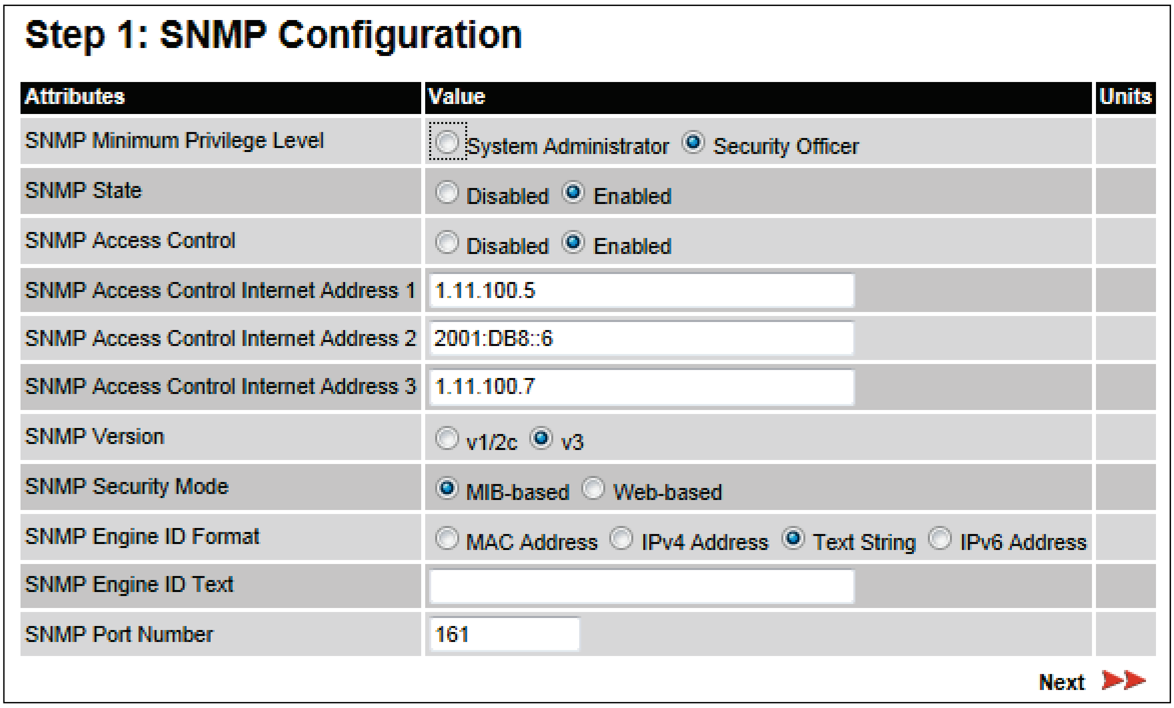
- Review the summary.
- If any updates are required, click **Continue to SNMP Wizard**.

Step 1: SNMP Configuration (for SNMPv3)

Menu option: **Management** > **SNMP**. Part of the SNMP Wizard (Figure 169).

Use this page to enable SNMP, select SNMPv3 and configure access to the SNMP server.

Figure 169 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	

Next

Procedure:

- Set SNMP State to **Enabled**.
- Set SNMP Version to **v3**. The page is redisplayed with SNMPv3 attributes.
- Update the attributes (Table 154).
- Click **Next**.

Table 154 Step 1: SNMP Configuration attributes (for SNMPv3)

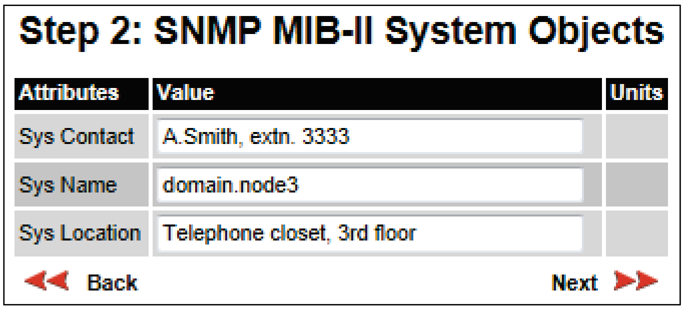
Attribute	Meaning
SNMP Minimum Privilege Level	Minimum security level which is permitted to administer SNMP security settings. Only displayed when Identity Based User Accounts are **Enabled** on the User Accounts page (Table 144).
SNMP State	Enables or disables SNMP.
SNMP Access Control	Enables or disables 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 6-92.
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 170).

Use this page to enter details of the SNMP managed node.

Figure 170 Step 2: SNMP MIB-II System Objects page (for SNMPv3)



Procedure:

- Update the attributes (Table 155).
- 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 6-92.
  - If **MIB-based**, go to Confirm SNMP Configuration (for SNMPv3) on page 6-96.

Table 155 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 171).

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 156).
- Click **Next**.

Figure 171 Step 3: SNMP User Policy Configuration page (for SNMPv3)

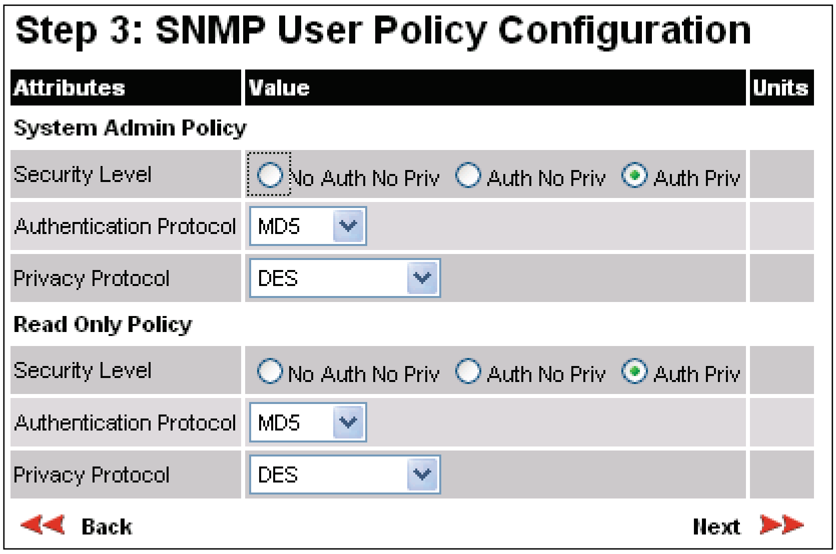


Table 156 Step 3: SNMP User Policy Configuration attributes (for SNMPv3)

Attribute	Meaning
Security Level	Defines the security level and associated protocols that are required to allow SNMP users to access the PTP 700. **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.
Authentication Protocol	The authentication protocol to be used to access the PTP 700 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.

Attribute	Meaning
Privacy Protocol	The privacy protocol to be used to access the PTP 700 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.

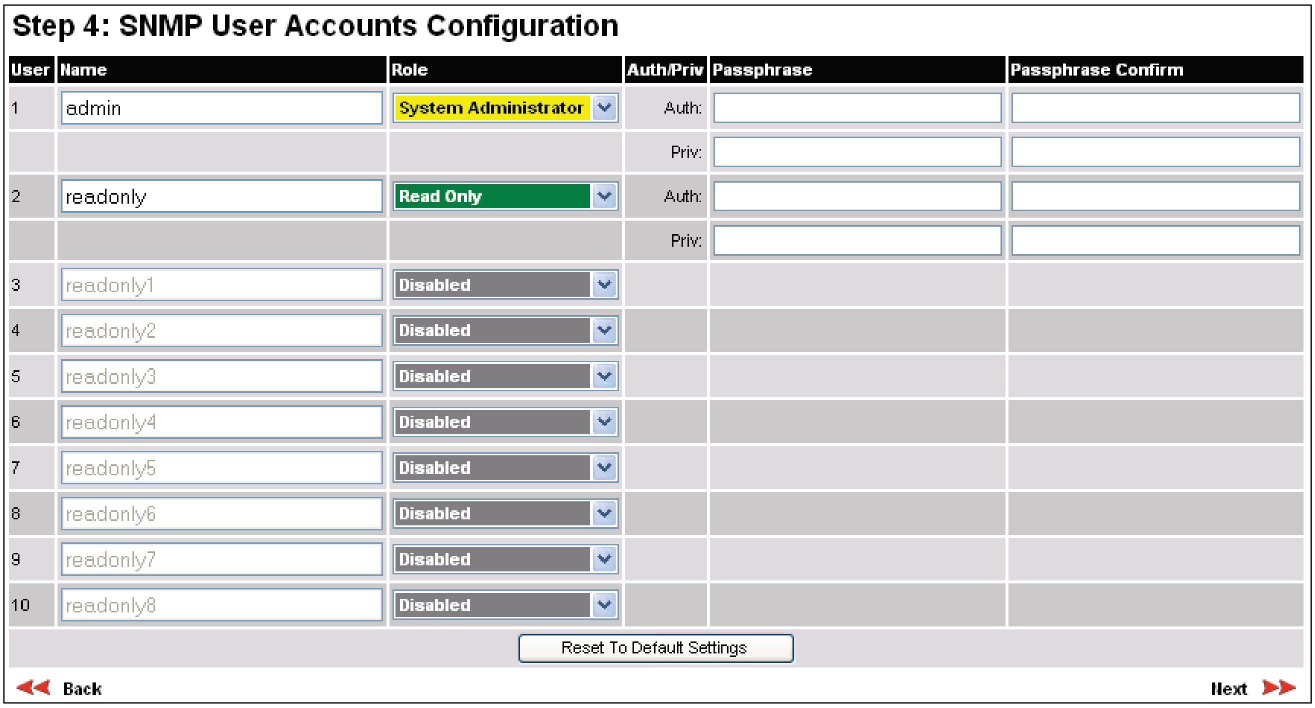
Note A user configured to use AES privacy protocol will not be able to transmit and receive encrypted messages unless the license key enables the AES capability.

Step 4: SNMP User Accounts Configuration (for SNMPv3)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 172).

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 172 Step 4: SNMP User Accounts Configuration page (for SNMPv3)



Procedure:

- Update the individual user attributes (Table 157) for up to 10 SNMP users.
- Click **Next**.

Table 157 Step 4: SNMP User Accounts Configuration attributes (for SNMPv3)

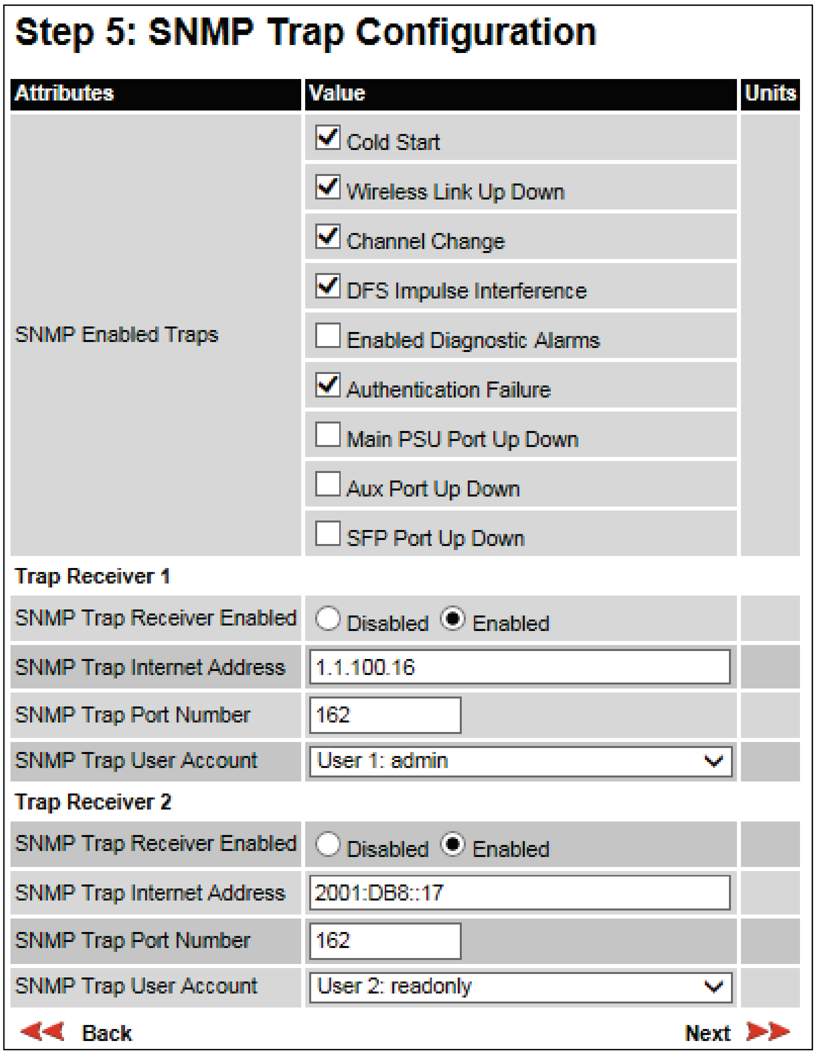
Attribute	Meaning
Name	Name to be used by the SNMP user to access the system.
Role	Selects which of the two web-based security profiles are applied to this user: **System administrator** or **Read only**. Select **Disabled** to disable the SNMP account.
Auth/Priv	Indicates whether the Passphrase applies to authentication or privacy protocols.
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 173).

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 173 Step 5: SNMP Trap Configuration page (for SNMPv3)



Procedure:

- Update the attributes (Table 158).
- Click **Next**.

Table 158 Step 5: SNMP Trap Configuration attributes (for SNMPv3)

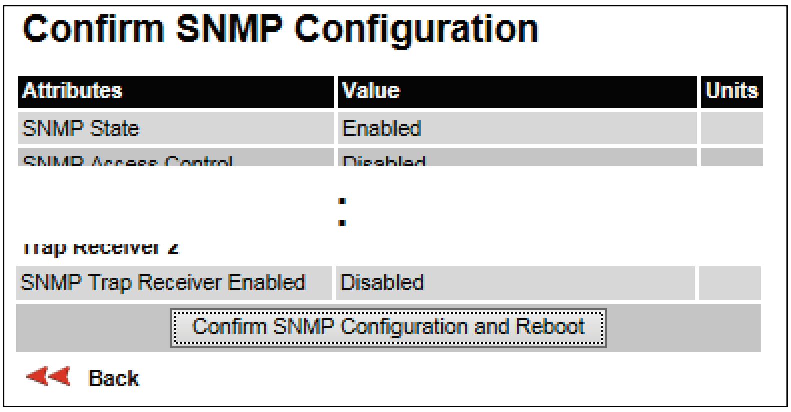
Attribute	Meaning
SNMP Enabled Traps	Select the events that will generate SNMP traps.
SNMP Trap Receiver 1 and SNMP Trap Receiver 2:	
SNMP Trap Receiver Enabled	**Disabled**: SNMP traps are not sent to the corresponding SNMP Trap Receiver (1 or 2). **Enabled**: SNMP traps are sent to the corresponding SNMP Trap Receiver (1 or 2).
SNMP Trap Internet Address	The FQDN, 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 174).

Use this page to review and confirm the updated SNMPv3 configuration of the unit.

Figure 174 Confirm SNMP Configuration page (for SNMPv3) (top and bottom of page shown)



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 168).

Use this page to review the current SNMP configuration and start the SNMP Wizard.

Procedure:

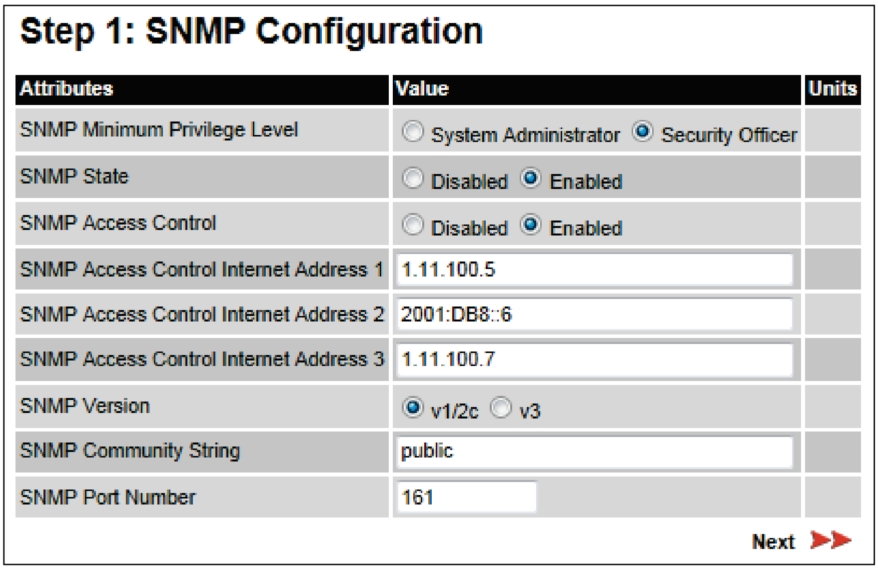
- Review the summary.
- If any updates are required, click **Continue to SNMP Wizard**.

Step 1: SNMP Configuration (for SNMPv1/2c)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 175).

Use this page to enable SNMP, select SNMPv1/2c and configure access to the SNMP server.

Figure 175 Step 1: SNMP Configuration page (for SNMPv1/2c)



Step 1: SNMP Configuration

Attributes	Value	Units
SNMP Minimum Privilege Level	System Administrator / Security Officer (selected)	
SNMP State	Disabled / Enabled (selected)	
SNMP Access Control	Disabled / Enabled (selected)	
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 (selected) / v3	
SNMP Community String	public	
SNMP Port Number	161	

Next

Procedure:

- Set SNMP State to **Enabled**.
- Set SNMP Version to **v1/2c**. The page is redisplayed with SNMPv1/2c attributes.
- Update the attributes (Table 159).
- Click **Next**.

Table 159 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 144).
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 700 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.

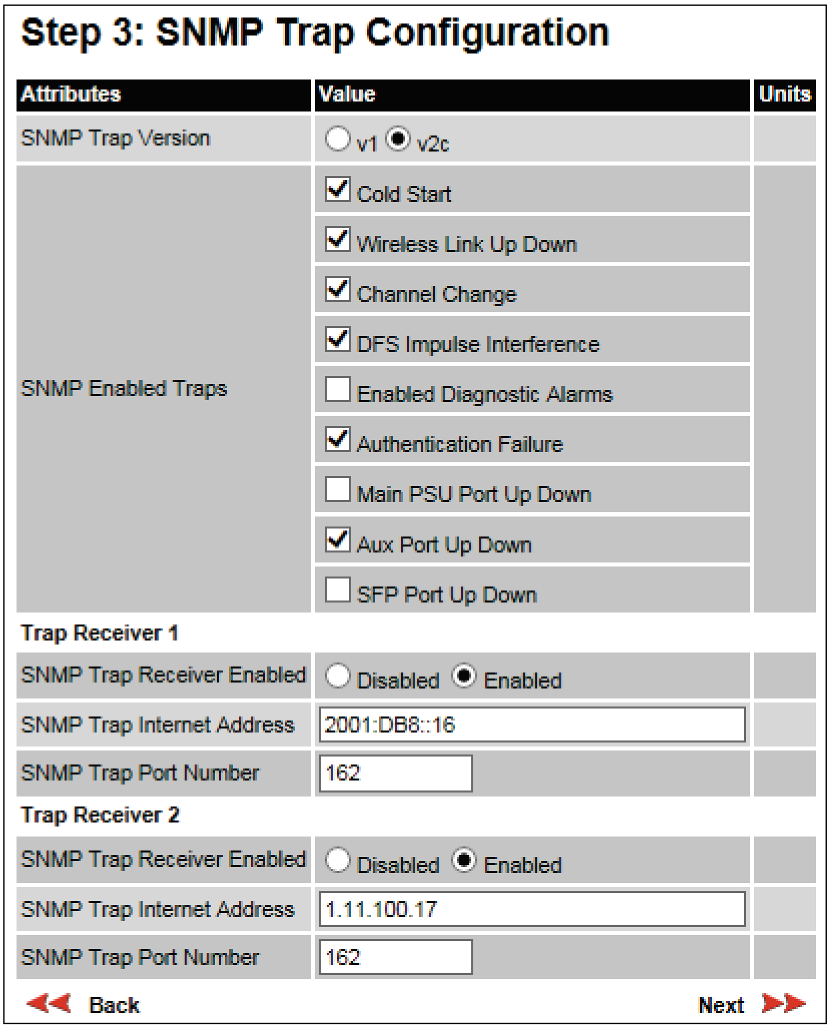
Step 2: SNMP MIB-II System Objects (for SNMPv1/2c)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 170). Use this page to enter details of the SNMP managed node. Update the attributes (Table 155) and click **Next**.

Step 3: SNMP Trap Configuration (for SNMPv1/2c)

Menu option: **Management** > **SNMP**. Part of the SNMP Wizard (Figure 176).

Figure 176 Step 3: SNMP Trap Configuration page (for SNMPv1/2c)



Procedure:

- Update the attributes (Table 160).
- Click **Next**.

Table 160 Step 3: SNMP Trap Configuration attributes (for SNMPv1/2c)

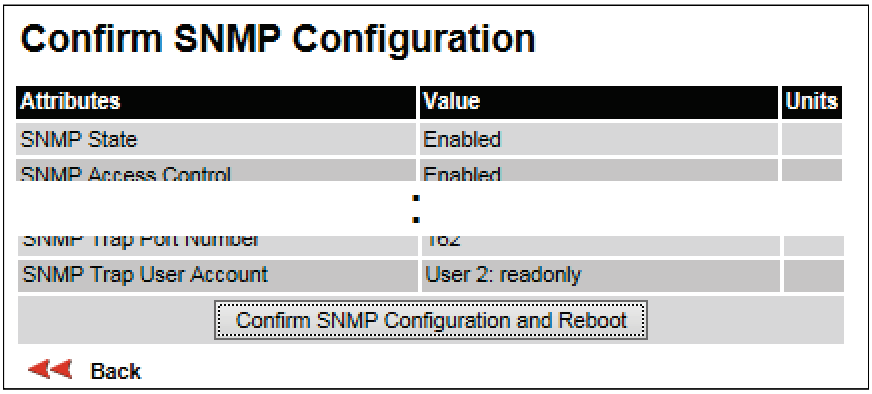
Attribute	Meaning
SNMP Trap Version	Select the SNMP protocol version to use for SNMP traps: **v1** or **v2c**.
SNMP Enabled Traps	Select the events that will generate SNMP traps.
SNMP Trap Receiver Enabled	**Disabled**: SNMP traps are not sent to the corresponding SNMP Trap Receiver (1 or 2). **Enabled**: SNMP traps are sent to the corresponding SNMP Trap Receiver (1 or 2).
SNMP Trap Internet Address	The FQDN, 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 177).

Use this page to review and confirm the updated SNMPv1/2c configuration of the unit.

Figure 177 Confirm SNMP Configuration page (for SNMPv1/2c) (top and bottom of page shown)



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 security options using the Security Wizard.

To configure security for the FIPS 140-2 approved mode, read this section and additionally read Configuring security for FIPS 140-2 applications on page 6-116.

Attention Ensure that the operator's security requirements are configured before connecting the PTP 700 to the network. Otherwise, security may be compromised.

Preparation

Obtain the necessary cryptographic material as described in:

- Using the Security Wizard on page 3-54.
- Planning for wireless encryption on page 3-55.
- Planning for HTTPS/TLS operation on page 3-57.
- Planning for protocols and ports on page 3-57.

Ensure that the ODU has the AES license. If necessary, order the necessary AES capability upgrade, generate a license key (Generating license keys on page 6-2) and enter it on the Software License Key page (Software License Key page on page 6-13).

On the Local User Accounts page (Local User Accounts page on page 6-70), 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 178). Use this page to review the current security configuration of the unit.

Figure 178 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	Not configured	
DRNG Entropy	Not configured	
User Defined Security Banner		
Require Acknowledgement Of Notices	No	
Display Login Information	No	
HTTPS Access Enabled	No	
Encryption Algorithm	TLS RSA	
TLS Minimum Security Level	None	
Device Certificate	Factory	
Authorization Method	Blacklist	
HTTP Access Enabled	Yes	
HTTP Port Number	80	
Telnet Access Enabled	No	
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	

Continue to Security Wizard

To continue with the Security Wizard, click **Continue to Security Wizard**.

Security options

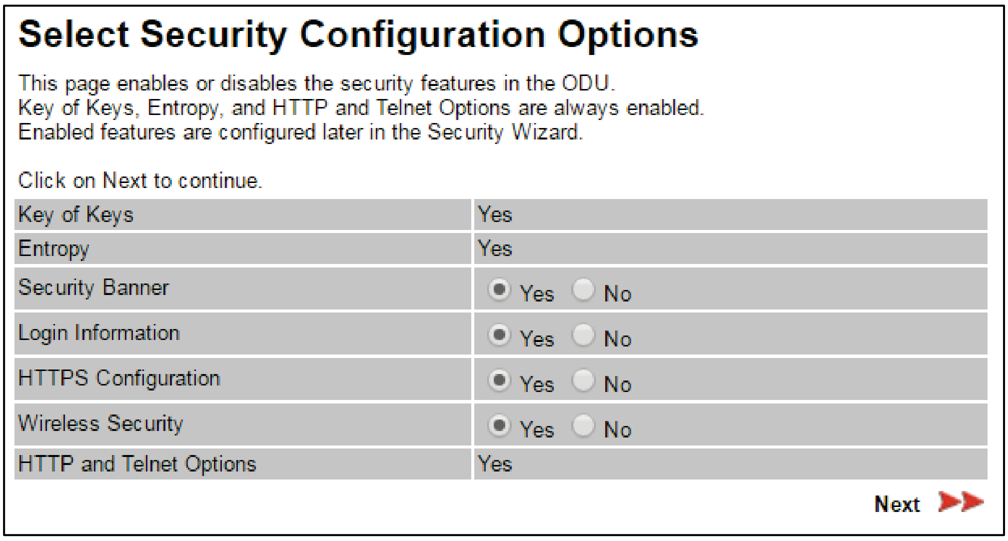
Menu option: **Security**. Part of the Security Wizard (Figure 179).

Select optional security features.

Keys of Keys, Entropy, and HTTP and Telnet Options are always enabled.

Set the remaining options to **No** to disable the associated feature, or set to **Yes** to enable the associated feature. Enabled features are configured in the remaining pages of the Security Wizard.

Figure 179 Security Options page

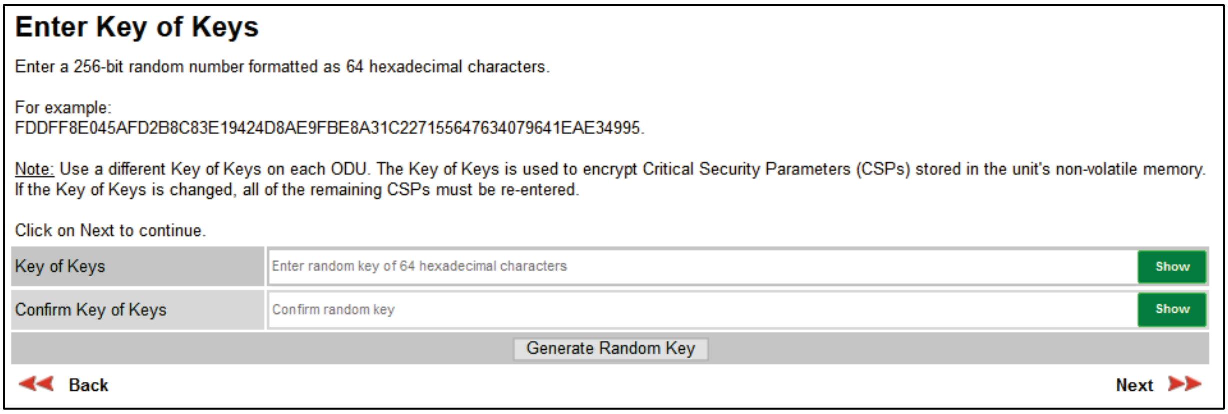


Key of Keys

Menu option: **Security**. Part of the Security Wizard (Figure 180 to Figure 182).

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 180 Key of Keys page



Click on the **Show** button to display the entered value as standard text.

Figure 181 Key of Keys page showing entered value

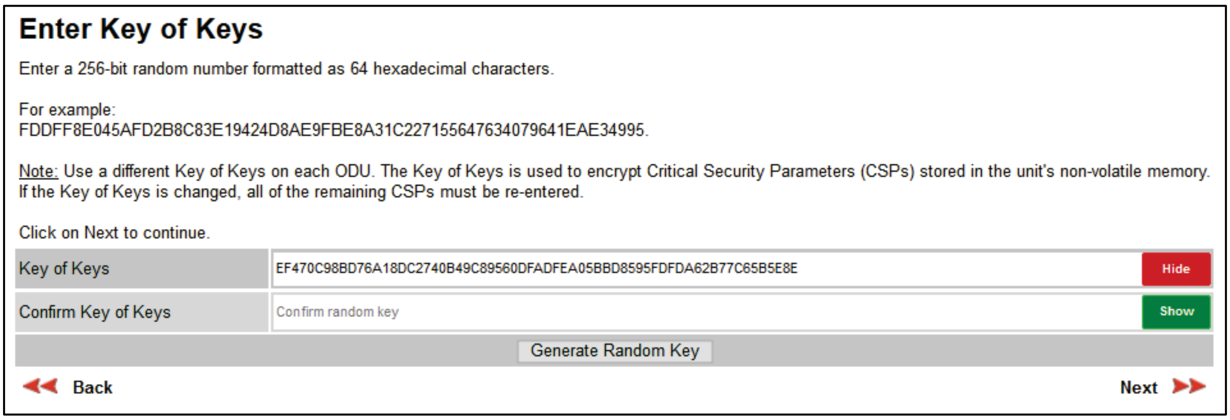
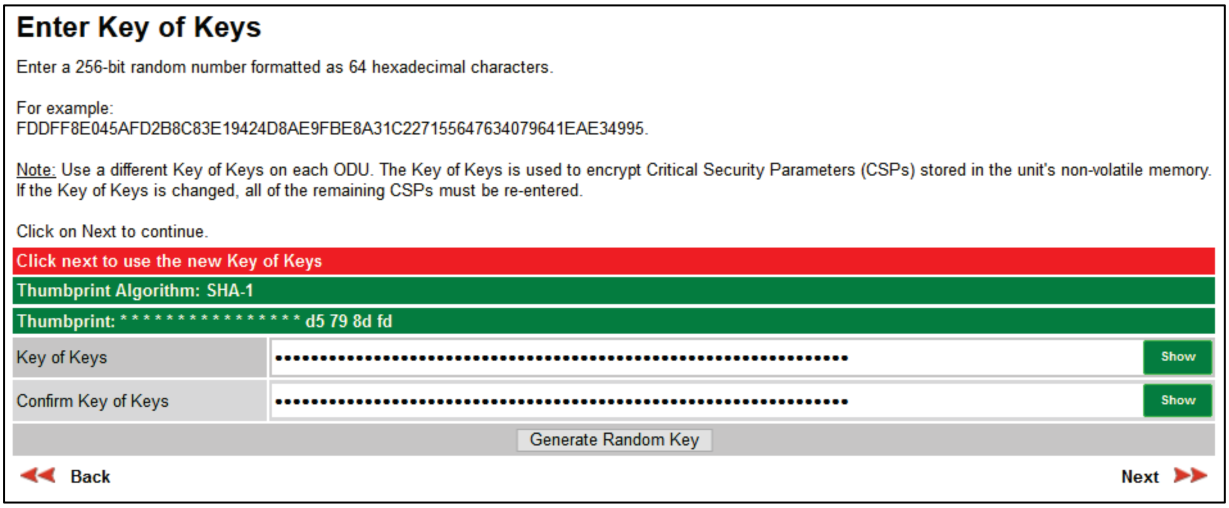


Figure 182 Key of Keys page with configured value



Note The Key of Keys attribute can be configured using the Security Wizard. It cannot be updated after the Security Wizard is submitted, except by first zeroizing CSPs.

Procedure:

- Enter and confirm the generated Key of Keys.
- Click **Generate Random Key** to enter an internally-generated random key
- Click **Next**.

Entropy

Menu option: **Security**. Part of the Security Wizard (Figure 183 and Figure 184).

Use this page to enter entropy input to seed the internal random number algorithm.

Figure 183 Entropy page

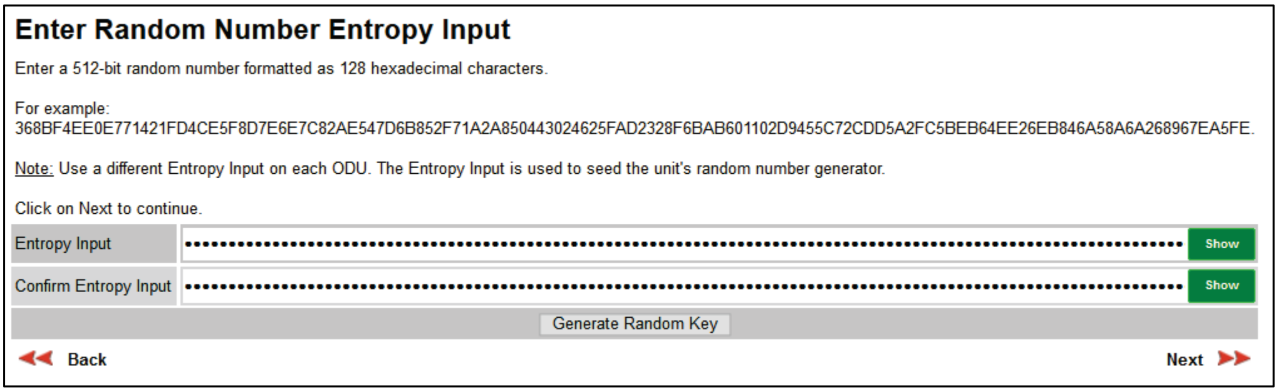
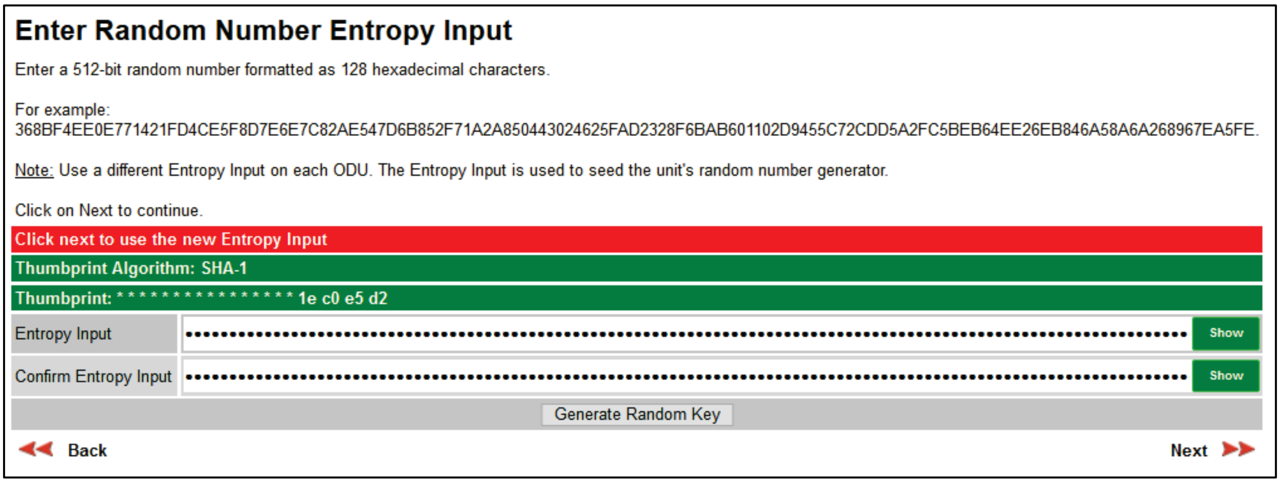


Figure 184 Entropy page with configured value



Procedure:

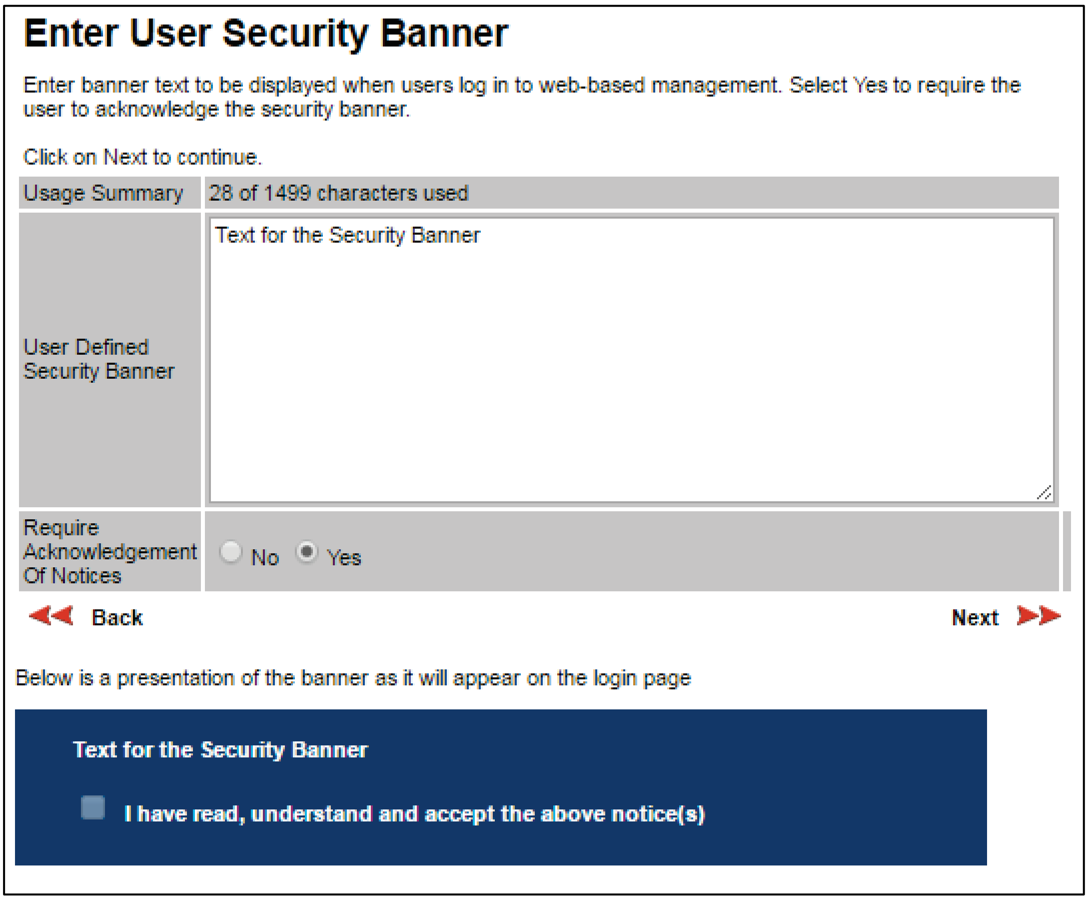
- If valid entropy input exists, then an SHA-1 thumbprint of the input is displayed. If this input is correct, then take no action. Otherwise, enter the generated input in the Entropy Input and Confirm Entropy Input fields.
- Click **Generate Random Key** to enter an internally-generated random key
- Click **Next**.

Enter User Security Banner

Menu option: **Security**. Part of the Security Wizard (Figure 185).

Use this page to enter a banner that will be displayed every time a user attempts to login to the wireless unit.

Figure 185 Enter User Security Banner page



Procedure:

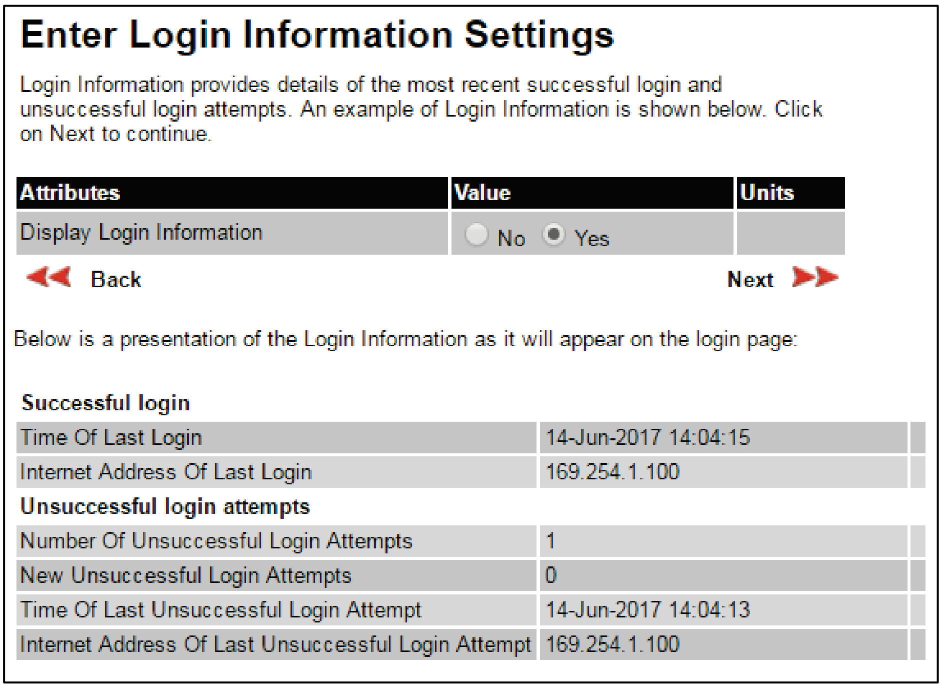
- Update the User Defined Security Banner (optional).
- Set the Acknowledgement to **No** or **Yes**.
- Click **Next**.

Enter Login Information Settings

Menu option: **Security**. Part of the Security Wizard (Figure 186).

Use this page to choose whether or not to display information about previous login attempts when the user logs into the web interface.

Figure 186 Enter Login Information Settings page



Procedure:

- Set Display Login Information to **No** or **Yes**.
- Click **Next**.

Enter HTTPS Configuration

Menu option: **Security**. Part of the Security Wizard (Figure 187 and Figure 188).

Use this page to select and upload the HTTPS/TLS Private Key and Public Certificate files.

Figure 187 Enter HTTPS Configuration page

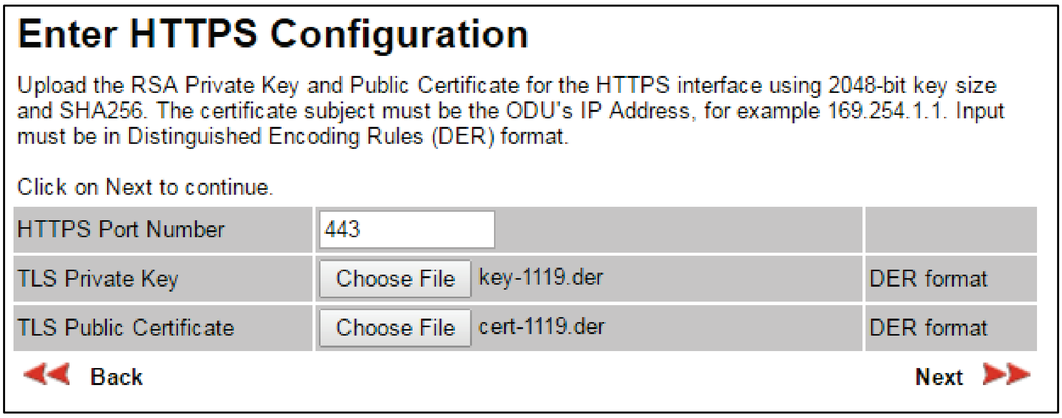
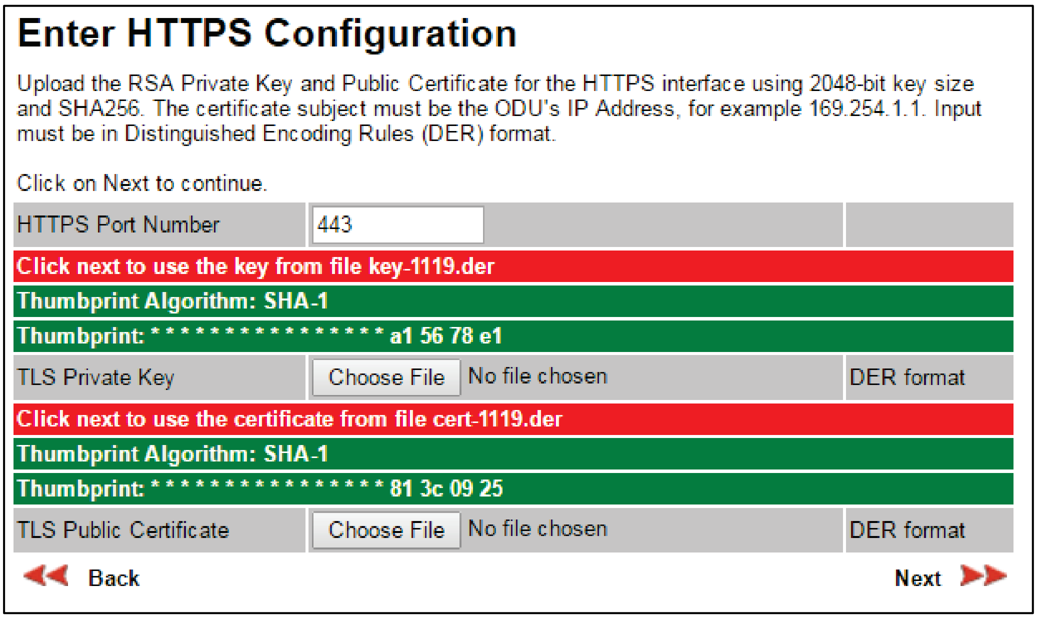


Figure 188 Configured HTTPS Configuration page



Attention If the certificates expire, your web browser will display security warnings. Always investigate the cause of security warnings and rectify errors in the content or expiry of certificates where necessary. Do not accept or ignore web browser security warnings.

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.**

Configure Wireless Security

Menu option: **Security**. Part of the Security Wizard (Figure 189 to Figure 193).

Use this page to enable device authentication and authorization, and AES encryption of the wireless link. Wireless link encryption key is used to encrypt all traffic over the PTP 700 wireless link.

Figure 189 Wireless Link Encryption Settings, TLS-RSA

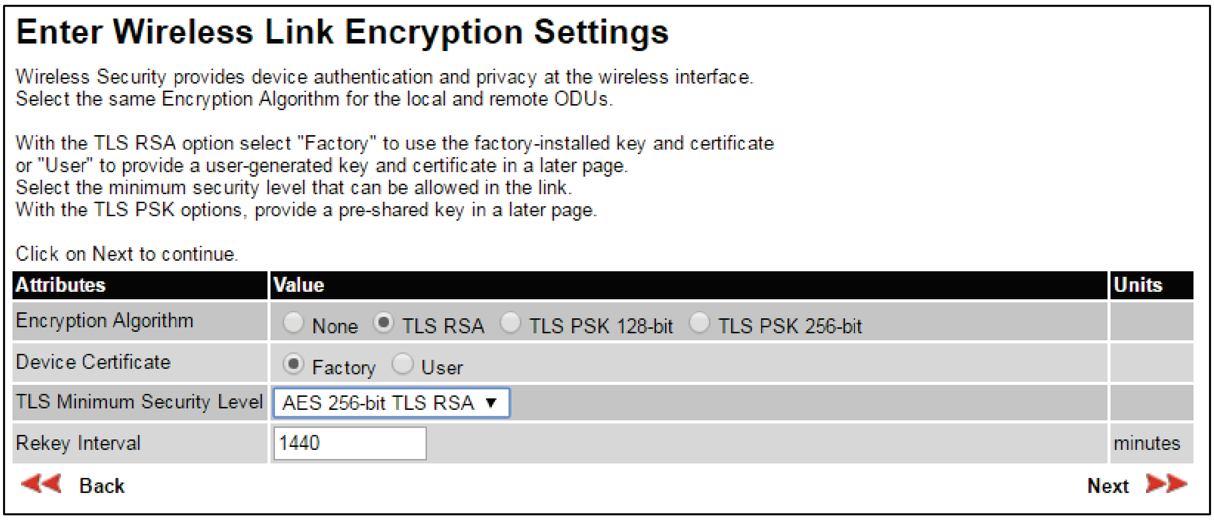


Figure 190 Wireless Link Encryption Settings, User-supplied device certificates

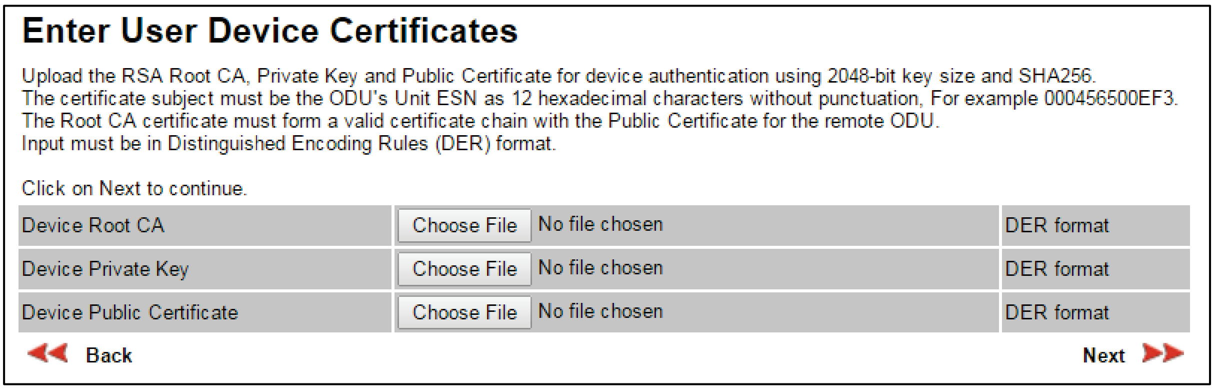


Figure 191 Wireless Link Encryption Settings, Authorization Control

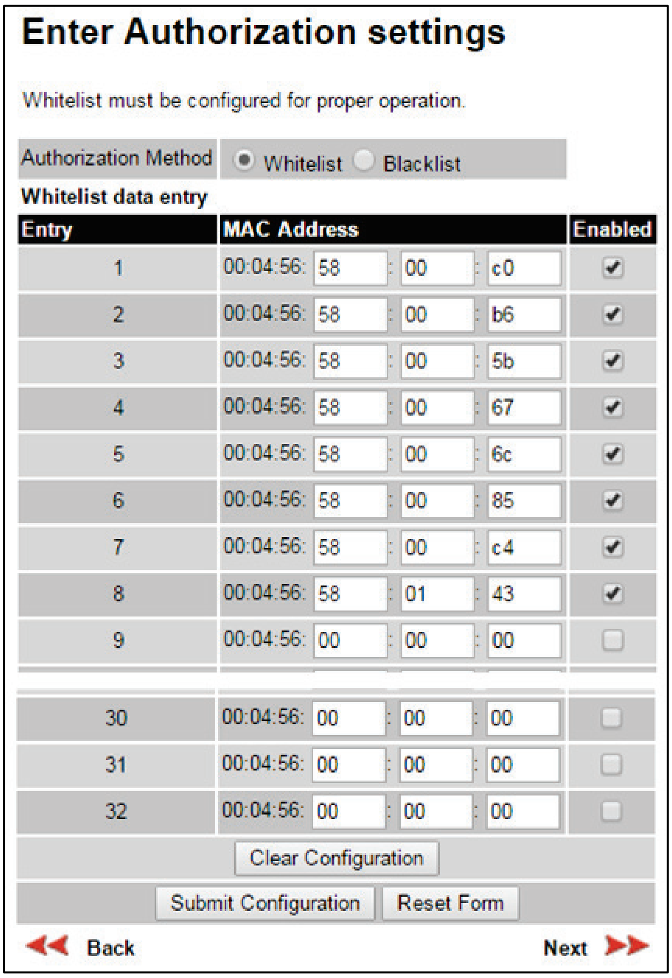


Figure 192 Wireless Link Encryption Settings, TLS-PSK

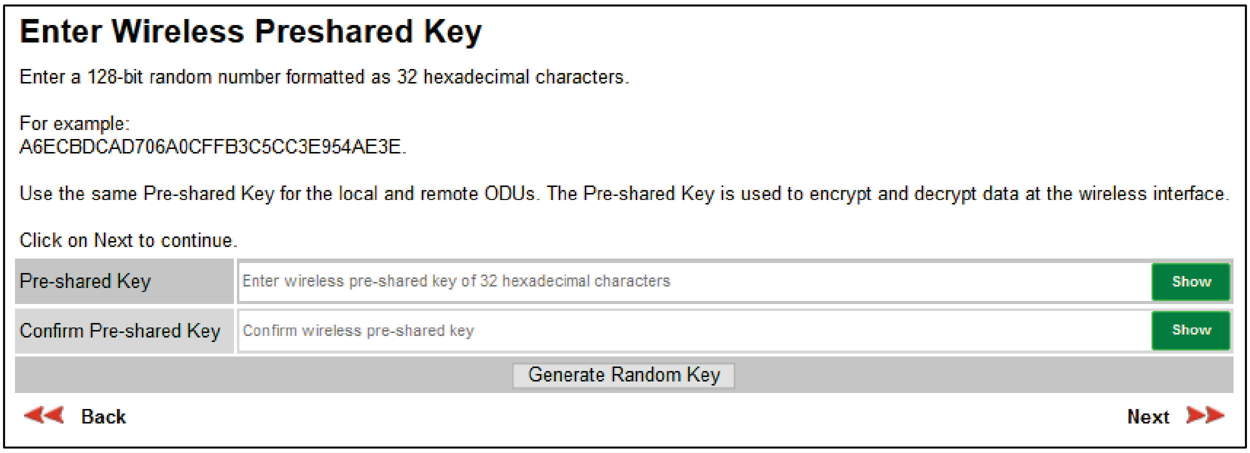
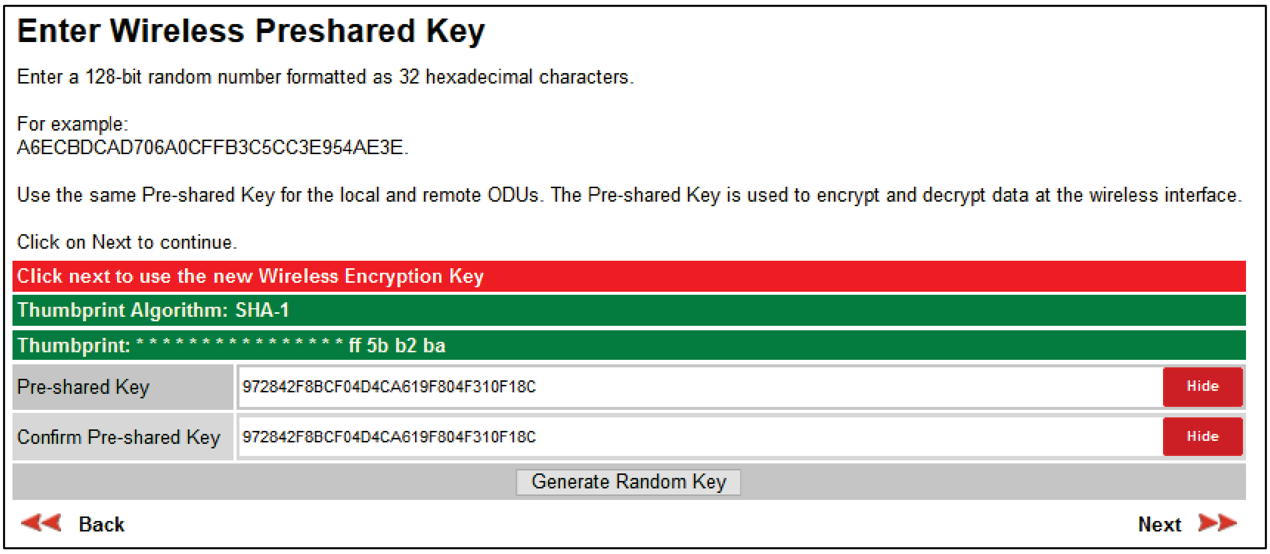


Figure 193 Wireless Link Encryption Settings, TLS-PSK with configured value



Procedure:

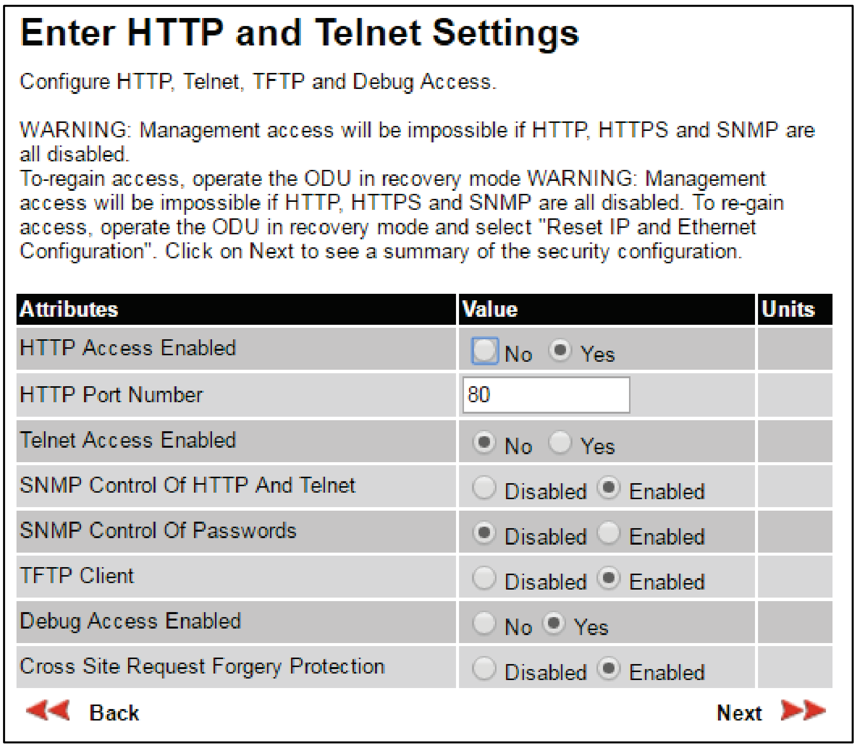
- Select the applicable value in the Encryption Algorithm field.
- For TLS-RSA, select Factory or User device certificates.
- For User device certificates, install Private Key, Public Certificate and Root CA certificate.
- For TLS-RSA and Group Access, configure the Whitelist or Blacklist
- For TLS-PSK, configure the pre-shared key. 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.
- For TLS-PSK, click **Generate Random Key** to enter an internally-generated random key
- Click **Next**.

HTTP and Telnet options

Menu option: **Security**. Part of the Security Wizard (Figure 194).

Use this page to configure network management of the PTP 700 using one or more of the following methods: HTTPS, HTTP, Telnet or SNMP.

Figure 194 HTTP and Telnet Settings page



Enter HTTP and Telnet Settings

Configure HTTP, Telnet, TFTP and Debug Access.

WARNING: Management access will be impossible if HTTP, HTTPS and SNMP are all disabled.
To-regain access, operate the ODU in recovery mode WARNING: Management access will be impossible if HTTP, HTTPS and SNMP are all disabled. To re-gain access, operate the ODU in recovery mode and select "Reset IP and Ethernet Configuration". Click on Next to see a summary of the security configuration.

Attributes	Value	Units
HTTP Access Enabled	No Yes	
HTTP Port Number	80	
Telnet Access Enabled	No Yes	
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	

Back Next

Attention 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).

Review and update the HTTP and Telnet attributes (Table 161) and click **Next**.

Table 161 HTTP and Telnet attributes

Attribute	Meaning
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.

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. 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.

Confirm Security Configuration

Menu option: **Security**. Part of the Security Wizard (Figure 195).

Use this page to review and confirm the updated security configuration of the unit.

Figure 195 Confirm Security Configuration page

Confirm Security Configuration

Press the button to confirm the security configuration and reboot the ODU.

Attributes	Value	Units
Key of Keys	Modified	
DRNG Entropy	Modified	
User Defined Security Banner		
Require Acknowledgement Of Notices	No	
Display Login Information	Yes	
HTTPS Access Enabled	Yes	
HTTPS Port Number	443	
Private Key	Modified	
Public Certificate	Modified	
Encryption Algorithm	TLS PSK 128-bit	
Wireless Encryption Key	Modified	
HTTP Access Enabled	Yes	
HTTP Port Number	80	
Telnet Access Enabled	No	
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	

Confirm Security Configuration and Reboot

Back

Procedure:

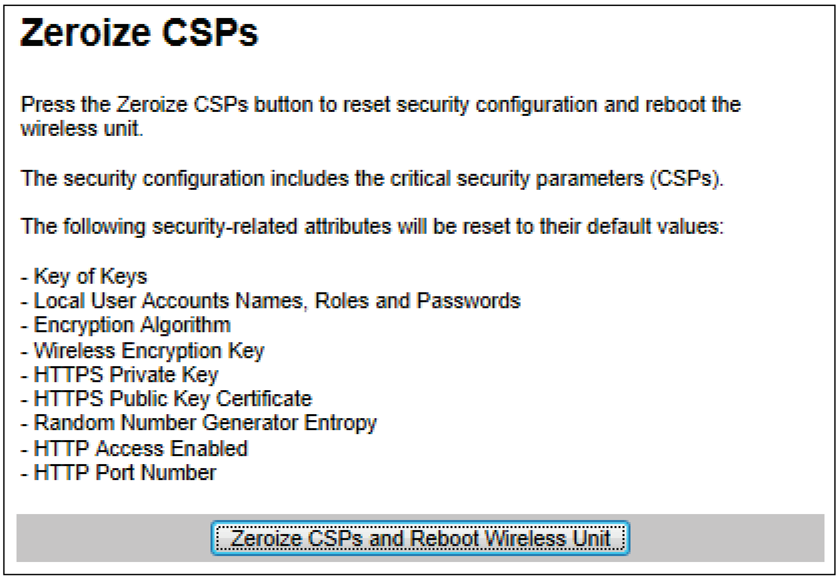
- Review all changes that have been made in the Security Wizard.
- To ensure that the changes take effect, click **Commit Security Configuration and Reboot**. The unit reboots and the changes take effect.

Zeroize CSPs page

Menu option: **Security** > **Zeroize CSPs** (Figure 196).

Use this page if it is necessary to reset the security configuration to default values.

Figure 196 Zeroize CSPs page



Procedure:

- Click **Zeroize CSPs and Reboot Wireless Unit**.
- Confirm the reboot.

Configuring security for FIPS 140-2 applications

This is a summary of all the configuration tasks that are necessary if the unit is to operate in FIPS 140-2 approved mode. For more information, refer to FIPS 140-2 mode on page 1-67 and Security planning on page 3-53.

The common steps for configuring security are described in Security menu on page 6-101.

Prerequisites for FIPS 140-2 configuration

Use this procedure to confirm that all prerequisites for FIPS 140-2 are ready.

Procedure:

1 Ensure that the following cryptographic material has been generated using a FIPS-approved cryptographic generator:
   - Key Of Keys
   - TLS Private Key and Public Certificates (for the correct IP address) with 2048-bit key size, and signed using the SHA-256 Secure Hash Algorithm.
   - Entropy Input
   - Wireless Link Encryption Key for AES

2 Identify the Port number for HTTPS.

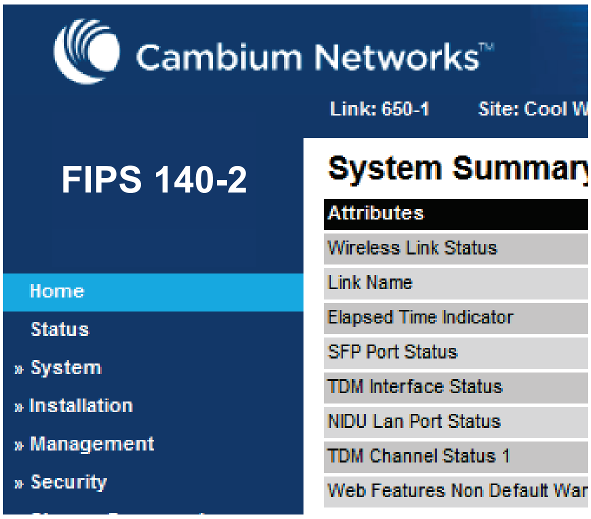
3 Ensure that the web browsers used are enabled for HTTPS/TLS operation using FIPS-approved cipher specifications.

4 On the **Management, Web** menu, click **Local User Accounts** and check that the current user's role is **Security Officer**.

5 Ensure that the installed license key meets all requirements including FIPS 140-2 compatibility:
   - Check that Security Level is “`FIPS`”.
   - Check that Encryption Algorithm is “`AES….`”.
   - If necessary, generate and enter a new license key with the above settings and install as described in Software License Key page on page 6-13.

6 Ensure that the installed software version is prefixed “`FIPS-`”. If necessary, upgrade to the latest FIPS validated image as described in Software Upgrade page on page 6-65.

7 To confirm that the above steps have been completed, check that the FIPS 140-2 logo is displayed in the Navigation Bar:



Configuration procedures for FIPS 140-2

To operate the ODU in FIPS 140-2 secure mode:

- Perform the steps in Local User Accounts page on page 6-70, taking care to configure appropriate identity-based user names and passwords.
- Perform the steps described in Security menu on page 6-101.

Checking that the unit is in the FIPS 140-2 operational state

Use this procedure to confirm that the unit is now in the FIPS 140-2 operational state:

Procedure:

1 On the menu, click **Security** and check the Secure Mode Alarm value.

2 If the alarm is “`Secure mode is active`”, the unit is in FIPS 140-2 secure mode and no further action is needed.

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
Secure Mode Alarm	Secure Mode Is Active	
Key of Keys	Configured	
Private Key	Configured	
Public Certificate	Configured	

If the alarm is “`Secure mode is not configured`”, return to Security menu on page 6-101 and check that all Security Wizard settings are correct for FIPS 140-2.

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
Secure Mode Alarm	Secure Mode Is Not Configured	
Key of Keys	Not configured	
Private Key	Not configured	
Public Certificate	Not configured	

If this alarm is displayed, it is also displayed in the System Summary page.

4 If the alarm is “`Secure mode is configured, but not active`”, return to HTTP and Telnet options on page 6-111 and check that HTTP Access Enabled is set to No.

If this alarm is displayed, it is also displayed in the System Summary page.

Note If it is necessary to exit from FIPS 140 2 mode, refer to Managing security on page 7-51.

Aligning antennas

This section describes how to align the antennas for Master and Slave ODUs in the PTP topology, and Slave ODUs in the HCMP topology, using the web interface to assist with alignment, and checking 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 6-4.

4 Power up the remote unit.

5 Log into the local unit as described in Logging into the web interface on page 6-6.

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 6-9.

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.

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 6-121 before starting alignment.

Note For improved radio performance, mount the integrated ODU at 45 degrees to the vertical; this ensures that side-lobe levels are minimized for interference transmitted or received at zero elevation.

To achieve best results, make small incremental changes to elevation and azimuth.

Attention 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 6-122
   - Graphical Install page on page 6-124

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 6-124) 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 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 6-120.
2. Connect the vertical polarization antenna to the ODU, disconnect the horizontal polarization antenna, then perform Aligning antennas on page 6-120.
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 5-77.

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 162. 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 162 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

Attention 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 700 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.

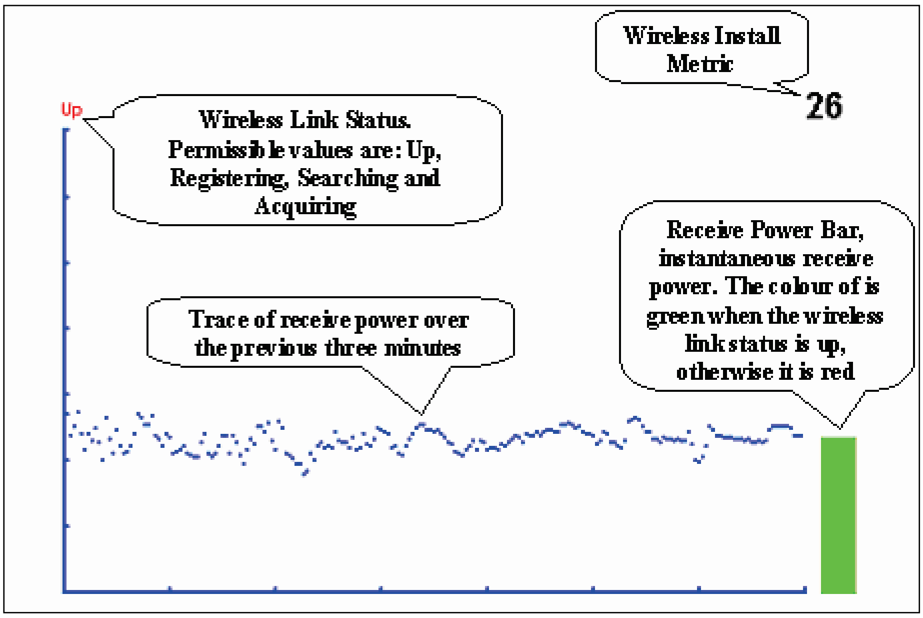
  The Slave unit does not have a ranging process. The slave unit will change to the Synchronized state as soon as the wanted signal is demodulated.
- Retrying same channel: If, at the end of the ranging period, the Registered state is not achieved due to interference or other reasons, the Master unit will 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 197).

This is the second of two methods that may be used to monitor receive signal level during antenna alignment.

Figure 197 Graphical Install page



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 6 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 116).
- Click **Disarm Installation Agent**. The confirmation page is displayed (Figure 198).

Figure 198 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. LINKPlanner provides the prediction in the form of an installation report.

Procedure:

- Select menu option **System > Statistics**. The System Statistic page is displayed (Figure 199).
- Monitor the following attributes:
  - Link Loss
  - Transmit Data Rate
  - Receive Data Rate

Figure 199 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	

Reset System Histogram Measurement Period

For more information on the System Statistics page, refer to System Statistics page on page 7-52.

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 700, 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 is not allocated to the Data or Management services, 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 6-68.
2. Set tFTP attributes as described in Table 163.
3. Monitor tFTP attributes as described in Table 164.
4. Reboot the ODU as described in Rebooting the unit on page 7-81.

Table 163 Setting tFTP attributes

Attribute	Meaning
tFTPServerInternetAddress	The FQDN, 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 164 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**
tFTPSoftwareUpgradeStatus Text	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**
tFTPSoftwareUpgradeStatus AdditionalText	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 700 wireless Ethernet bridge.

The following topics are described in this chapter:

System summary and status

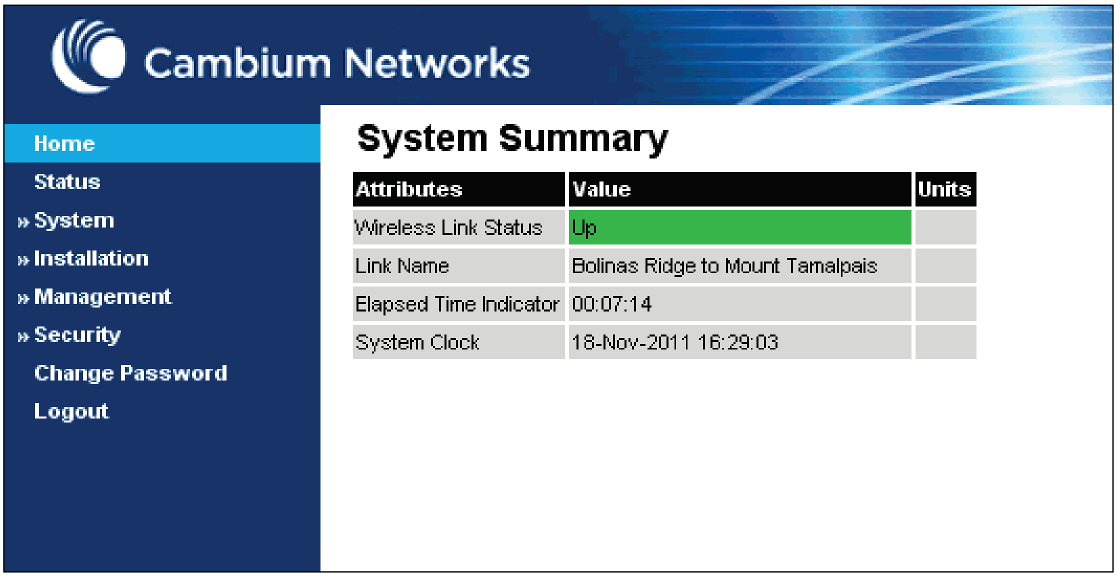
This section describes how to use the summary and status pages to monitor the status of the Ethernet ports and wireless link.

System Summary page

Menu option: **Home** (Figure 200).

This page contains a high-level summary of the status of the wireless link and associated equipment.

Figure 200 System Summary page



Procedure:

- Review the attributes (Table 165).
- 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. For more information, refer to Alarms on page 7-18.

Table 165 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.
Link Name	The name of the PTP link, as set in the System Configuration page.

Attribute	Meaning
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

PTP topology

Menu option: **Status** (Figure 201). This page provides a detailed view of the operation of the PTP 700 link from both the wireless and network perspectives.

Figure 201 System Status page (PTP topology)

System Status - Point To Point - Master

Attributes	Value	Units
Equipment		
Link Name	Ashburton to Widecombe	
Unit Name	Ashburton 01	
Site Name	Ashburton	
Software Version	50670-G7PFP-B73+ wdog	
Hardware Version	B0P01.00-C-FPS	
Unit ESN	00045658076A	
Unit MSN	U9TD000ZSB5R	
Regulatory Band	1 - 5.8 GHz - United States	
Elapsed Time Indicator	00:06:03	
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	Down	
SFP Port Speed And Duplex		
MAC Address	00:04:56:58:07:6a	
Management		
cnMaestro Server	cnMaestro On-Premises	
cnMaestro Connection Status	Connected	
Remote Identification		
Remote Unit Name	Slave_58_07_6B	
Remote MAC Address	00:04:56:58:07:6b	
Remote Internet Address	http://169.254.1.40	
Status Page Refresh Period	3600	Seconds

Attributes	Value	Units
Wireless		
Wireless Link Status	Up	
Wireless Link Up Time	00:05:30	
Wireless Encryption	None	
Maximum Transmit Power	10	dBm
EIRP	33.0	dBm
Remote Maximum Transmit Power	10	dBm
Transmit Power	10.0, 9.6, -15.0, 10.0	dBm
Receive Power	-49.4, -51.6, -110.0, -50.0	dBm
Vector Error	7.2, -28.9, -34.9, -31.7	dB
Link Loss	106.1, 98.7, 0.0, 106.0	dB
Signal Strength Ratio	-0.7, -1.5, -2.2, -1.5	dB
Transmit Data Rate	225.56, 208.75, 0.00, 225.56	Mbps
Receive Data Rate	319.59, 209.97, 0.00, 225.56	Mbps
Aggregate Data Rate	451.12, 418.72, 0.00, 451.12	Mbps
Link Capacity Variant	Full	
Link Capacity	451.11	Mbps
Wireless Link Availability	100.0000	%
Data Bridging Availability	100.0000	%
Transmit Modulation Mode	256QAM 0.81 (Dual) (45 MHz)	
Receive Modulation Mode	256QAM 0.81 (Dual) (45 MHz)	
Link Symmetry	1 to 1	
Receive Modulation Mode Detail	Running At Maximum Receive Mode	
Range	0.2	km
TDD Synchronization		
TDD Synchronization Interface	Disabled	
	Update Page Refresh Period / Reset form	

In the PTP topology, the two PTP 700 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.

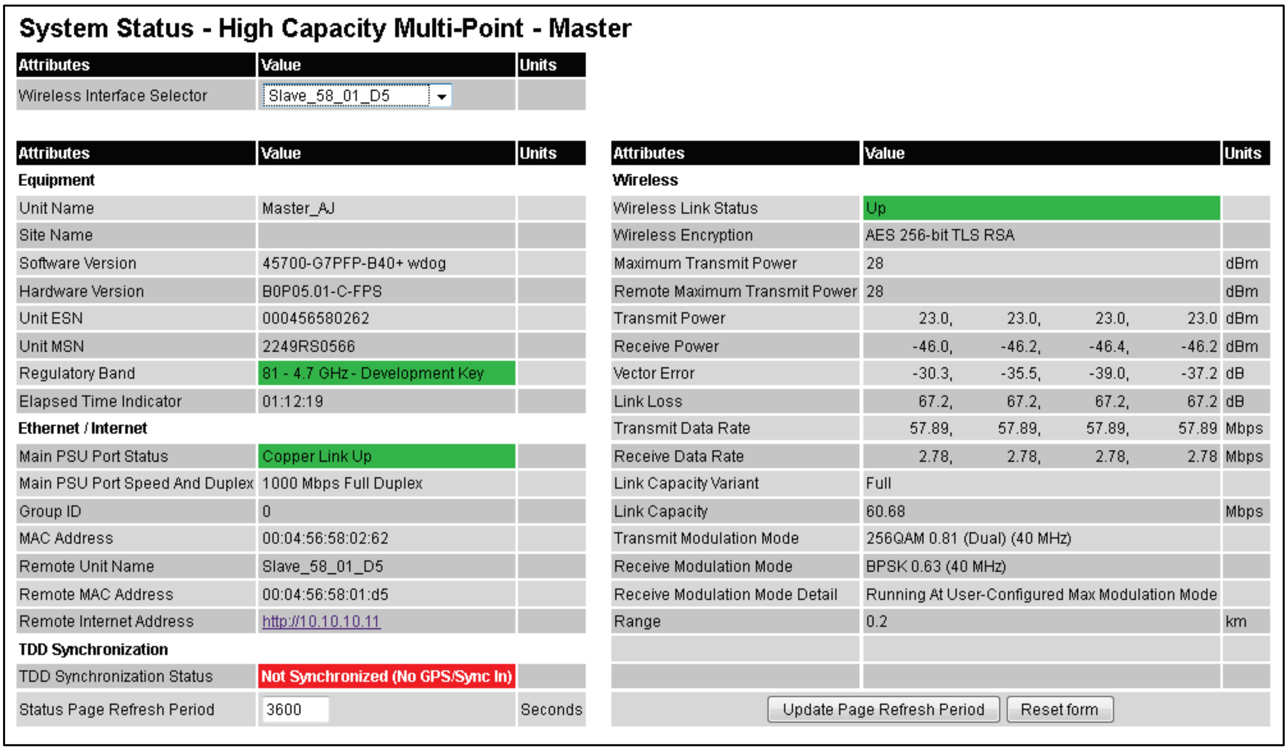
Procedures:

- Confirm that the Ethernet Link Status attributes are green and set to **Copper Link Up** or **Fiber Link Up**.

HCMP topology

Menu option: **Status** (Figure 202 to Figure 204). This page provides a detailed view of the operation of the PTP 700 link from both the wireless and network perspectives.

Figure 202 System Status page (Master, HCMP topology, Wireless Interface set to a single link)



System Status - High Capacity Multi-Point - Master

Attributes	Value	Units
Wireless Interface Selector	Slave_58_01_D5	

Attributes	Value	Units
Equipment		
Unit Name	Master_AJ	
Site Name		
Software Version	45700-G7PFP-B40+ wdog	
Hardware Version	B0P05.01-C-FPS	
Unit ESN	000456580262	
Unit MSN	2249RS0566	
Regulatory Band	81 - 4.7 GHz - Development Key	
Elapsed Time Indicator	01:12:19	
Ethernet / Internet		
Main PSU Port Status	Copper Link Up	
Main PSU Port Speed And Duplex	1000 Mbps Full Duplex	
Group ID	0	
MAC Address	00:04:56:58:02:62	
Remote Unit Name	Slave_58_01_D5	
Remote MAC Address	00:04:56:58:01:d5	
Remote Internet Address	http://10.10.10.11	
TDD Synchronization		
TDD Synchronization Status	Not Synchronized (No GPS/Sync In)	
Status Page Refresh Period	3600	Seconds

Attributes	Value	Units
Wireless		
Wireless Link Status	Up	
Wireless Encryption	AES 256-bit TLS RSA	
Maximum Transmit Power	28	dBm
Remote Maximum Transmit Power	28	dBm
Transmit Power	23.0, 23.0, 23.0, 23.0	dBm
Receive Power	-46.0, -46.2, -46.4, -46.2	dBm
Vector Error	-30.3, -35.5, -39.0, -37.2	dB
Link Loss	67.2, 67.2, 67.2, 67.2	dB
Transmit Data Rate	57.89, 57.89, 57.89, 57.89	Mbps
Receive Data Rate	2.78, 2.78, 2.78, 2.78	Mbps
Link Capacity Variant	Full	
Link Capacity	60.68	Mbps
Transmit Modulation Mode	256QAM 0.81 (Dual) (40 MHz)	
Receive Modulation Mode	BPSK 0.63 (40 MHz)	
Receive Modulation Mode Detail	Running At User-Configured Max Modulation Mode	
Range	0.2	km

Update Page Refresh Period | Reset form

Figure 203 System Status page (Master, HCMP topology, Wireless Interface set to “All Wireless Interfaces”)

System Status - High Capacity Multi-Point - Master

Attributes	Value	Units
Wireless Interface Selector	All Wireless Interfaces	

Attributes	Value	Value	Value	Units
Equipment				
Unit Name	Master_AJ			
Site Name				
Software Version	45700-G7PFP-B40+ wdog			
Hardware Version	B0P05.01-C-FPS			
Unit ESN	000456580262			
Unit MSN	2249RS0566			
Regulatory Band	81 - 4.7 GHz - Development Key			
Elapsed Time Indicator	01:13:47			
TDD Synchronization				
TDD Synchronization Status	Not Synchronized (No GPS/Sync In)			
Ethernet / Internet				
Main PSU Port Status	Copper Link Up			
Main PSU Port Speed And Duplex	1000 Mbps Full Duplex			
Group ID	0			
MAC Address	00:04:56:58:02:62			
Remote MAC Address	00:04:56:58:01:d5	Not Available	Not Available	
Remote Internet Address	http://10.10.10.11	Not Available	Not Available	
Wireless				
Remote Unit Name	Slave_58_01_D5	Not Available	Not Available	
Wireless Link Status	Up	Initialising	Searching	
Wireless Encryption	AES 256-bit TLS RSA	None	None	
Maximum Transmit Power	28			dBm
Remote Maximum Transmit Power	28	Not Available	Not Available	dBm
Transmit Power	23.0, 23.0	28.0, 28.0	0.0, 0.0	dBm
Receive Power	-46.2, -46.2	-109.9, -110.0	0.0, 0.0	dBm
Vector Error	-35.5, -36.6	0.0, 0.0	0.0, 0.0	dB
Link Loss	67.2, 67.2	0.0, 0.0	0.0, 0.0	dB
Transmit Data Rate	57.89, 57.89	0.00, 0.00	0.00, 0.00	Mbps
Receive Data Rate	2.78, 2.78	0.00, 0.00	0.00, 0.00	Mbps
Link Capacity	60.68	0.00	0.00	Mbps
Transmit Modulation Mode	256QAM 0.81 (Dual)	Acquisition	Acquisition	
Receive Modulation Mode	BPSK 0.63	Acquisition	Acquisition	
Channel Bandwidth	40 MHz			
Range	0.2	Not Available	0.0	km
Status Page Refresh Period	3600			seconds

Updated Page Refresh Period | Reset Form

Figure 204 System Status page (Slave, HCMP topology)

System Status - High Capacity Multi-Point - Slave

Equipment

Attributes	Value	Units
Link Name		
Site Name	AJ bench	
Software Version	45700-G7PFP-B471+ !wdog	
Hardware Version	B0P05.01-C-FPS	
Unit ESN	000456580186	
Unit MSN	2249RS0201	
Regulatory Band	95 - 4.5 GHz - Development Key	
Elapsed Time Indicator	00:02:15	
Ethernet / Internet		
Main PSU Port Status	Copper Link Up	
Main PSU Port Speed And Duplex	1000 Mbps Full Duplex	
Group ID	123	
MAC Address	00:04:56:58:01:86	
Remote MAC Address	00:04:56:58:02:62	
Remote Internet Address	http://10.10.10.10	
Status Page Refresh Period	3600	Seconds

Wireless

Attributes	Value	Units
Wireless Link Status	Up	
Wireless Encryption	AES 256-bit TLS RSA	
Maximum Transmit Power	17	dBm
Remote Maximum Transmit Power	24	dBm
Transmit Power	17.0, 12.3, -15.0, 17.0	dBm
Receive Power	-55.7, -62.8, -110.0, -57.9	dBm
Vector Error	7.2, -12.1, -39.0, -25.5	dB
Link Loss	111.9, 34.0, 0.0, 80.9	dB
Transmit Data Rate	5.18, 1.24, 0.00, 1.90	Mbps
Receive Data Rate	15.45, 3.38, 0.00, 15.45	Mbps
Link Capacity Variant	Full	
Link Capacity	17.21	Mbps
Wireless Link Availability	100.0000	%
Data Bridging Availability	97.4709	%
Transmit Modulation Mode	QPSK 0.63 (Single) (20 MHz)	
Receive Modulation Mode	64QAM 0.92 (Dual) (20 MHz)	
Dual Payload	Enabled	
Receive Modulation Mode Detail	Limited By The Wireless Conditions	
Range	12.1	km

Update Page Refresh Period Reset form

In the HCMP topology, one PTP 700 Series unit is the Master and up to eight PTP 700 Series units are configured as Slaves. The roles of the units in this relationship are displayed in the page title. The master unit will always have the title " - High Capacity MultiPoint - Master", and the slave will always have "- High Capacity MultiPoint - Slave" appended to the "Systems Status" page title.

Procedures:

- Only on a device configured as in HCMP mode as a Master, set the Wireless Interface Selector to the Wireless Interface the diagnostic data needs to be displayed for. Note the Remote MAC Address indicates the MAC address of the unit currently connected, if any, to the selected wireless interface.

Equipment

The Equipment section of the System Status page contains the attributes described in Table 166.

Table 166 System Status attributes - Equipment

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 700 software installed on the equipment.

Attribute	Meaning
Hardware Version	The PTP 700 hardware version. Formatted as "vvvv-C" or "vvvv-C+I" where vvvv is the version of the printed circuit card. The "-C" suffix indicates a PTP 700 Connectorized unit. The "-C+I" suffix indicates a PTP 700 Connectorized+Integrated unit.
Unit ESN	The Electronic Serial Number of the ODU.
Unit MSN	The Mechanical Serial Number of the ODU.
Unit SKU	The Cambium Part Number of the ODU
Unit Color	**White**, **Green**, **Desert Tan** The color of the external paint finish of the ODU.
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.

Ethernet / Internet

The Ethernet / Internet section of the System Status page contains the attributes described in Table 167.

Table 167 System Status attributes – Ethernet / Internet

Attribute	Meaning
Main PSU Port Status	The current status of the Ethernet link to the PSU port: • Green "`Copper Link Up`": The Ethernet link is established. • Red "`Down`": 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.
Aux Port Status	The current status of the Ethernet link to the Aux port: • Green "`Copper Link Up`": The Ethernet link is established. • Red "`Down`": 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	The current status of the Ethernet link to the SFP port: • Green "`Fiber Link Up`": The Ethernet link is established. • Red "`Down`": The Ethernet link is not established.

Attribute	Meaning
SFP Port Speed and Duplex	The negotiated speed and duplex setting of the Ethernet link to the SFP port. The speed setting is specified in Mbps.
MAC Address	The MAC Address of this unit.

Management

The Management section of the System Status page contains the attributes described in Table 168.

Table 168 System Status attributes – Management

Attribute	Meaning
cnMaestro Server	**cnMaestro On-Premises**: The ODU will connect to the On Premises server. **cnMaestro Cloud**: The ODU will connect to the Cloud server.
cnMaestro Connection Status	The status of the connection between the ODU and the cnMaestro server. **Connected**: The ODU is connected to the cnMaestro Server. **Not Connected**: The ODU is not connected to the cnMaestro Server. This is default state in which transactions begin. **DNS Failed**: The ODU could not resolve the supplied cnMaestro Server Internet Address. **Error returned by Server**: An error occurred on the server. The cnMaestro Connection Status Message attribute will display the details. **Connecting**: Connection is in progress. The ODU is communicating with the cnMaestro Server. **Approval Pending**: A connection has been established. The ODU is in cnMaestro Server's On-boarding queue, waiting for a cnMaestro user to approve the ODU as a new device. After the device is approved, the ODU should transition to the Connected state. **Ownership Error**: The cnMaestro server is unable to match the supplied Cambium ID or Onboarding Key with its configured data.
cnMaestro Connection Status Message	Error text generated by the cnMaestro server when an error is returned.

Remote Identification

The Remote Identification section of the System Status page contains the attributes described in Table 169.

Table 169 System Status attributes – Remote Identification

Attribute	Meaning
Remote Unit Name	The configured Unit Name of the peer unit. If the link is down, this is set to “`Not available`”.
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 133) and IP Address Label (Table 132), this may be either an IPv4 or an IPv6 address.

Protection

The Protection section of the System Status page contains the attributes described in Table 170.

Table 170 System Status attributes – Protection

Attribute	Meaning
Protection State	**Unprotected:** The Primary and/or Seocndary link is not available, and so the Hot Standby system is not protecting the end-to-end connection.
Hot Standby Link State	**Standby**: The ODU is part of a wireless link in the Standby state. This may be because the link has a fault and is therefore unavailable, or because the link is fault-free, but neighbor link is in the Active state. **Active**: The ODU is in a wireless link in the Active state. The link is fault-free and is forwarding traffic in the Data and Management services.

Wireless

The Wireless section of the System Status page contains the attributes described in Table 171.

Table 171 System Status attributes – Wireless

Attribute	Meaning
Wireless Link Status	The current status of the wireless link: • Green “`Up`”: The wireless link is established. • Red “`Down`”: The wireless link is not established.
Wireless Link Up Time	The time in hours, minutes, seconds that the present wireless link has been established.

Attribute	Meaning
Wireless Encryption	For the HCMP topology only, the encryption algorithm used for the wireless link: • **None**: The wireless link in not encrypted. • **AES 128-bit TLS RSA**: The wireless link in encrypted using the AES TLS RSA algorithm with a 128-bit key. • **AES 256-bit TLS RSA**: The wireless link in encrypted using the AES TLS RSA algorithm with a 256-bit key.
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 7-52.
Receive Power	The maximum, mean, minimum and latest measurements of Receive Power (dBm). See System histograms on page 7-52.
Vector Error	The maximum, mean, minimum and latest measurements of Vector Error (dB). See System histograms on page 7-52. 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 7-52. The link loss is the total attenuation of the wireless signal between the two point-to-point units. The link loss calculation is: $$P_{ll} = P_{T_x} - P_{R_x} + g_{T_x} + g_{R_x} - c_{T_x} - c_{R_x}$$ 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). This is the gain of the integrated or connectorized antenna. c_{T_x}, c_{R_x} = Cable loss at the remote and local units respectively (dB). It is RF cable loss which connects ODU to Connectorized antenna. For connectorized ODUs, the link loss calculation is modified to allow for the increased antenna gains at each end of the link.

Attribute	Meaning
Transmit Data Rate	The maximum, mean, minimum and latest measurements of Transmit Data Rate (Mbps). See System histograms on page 7-52.
Receive Data Rate	The maximum, mean, minimum and latest measurements of Receive Data Rate (Mbps). See System histograms on page 7-52.
Link Capacity Variant	Indicates whether the installed license key is Lite 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.
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 172.
Range	The range between the PTP 700 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 6-76.

Table 172 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.

Value	Meaning
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.
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.

Synchronous Ethernet

Note Synchronous Ethernet is available in the PTP topology.

The Synchronous Ethernet section of the System Status page contains the attributes described in Table 173.

Table 173 System Status attributes – Synchronous Ethernet

Attribute	Meaning
Sync E Tracking State	The state of frequency tracking in Synchronous Ethernet. For a list of values and their meanings, see Table 174. In normal operation, with the Synchronous Ethernet feature enabled and a valid timing source present, one end of the link should be in the "`Locked Local, Holdover Acquired State`", the other end should be in the "`Locked Remote, Holdover Acquired`" state. Further status information for the Synchronous Ethernet features is available in the Sync E Status page. See SyncE Status page on page 7-67.

Table 174 Sync E Tracking State values and meanings

Value	Meaning
Disabled	The synchronous Ethernet feature is disabled.
Acquiring Wireless Lock	Synchronous Ethernet is not operational because the wireless link is establishing.

Value	Meaning
Free Running	Synchronous Ethernet is operational, but with no timing source or history. This is a temporary state.
Locked Local, Acquiring Holdover	Sync E tracking has locked to a synchronisation signal from a cabled Ethernet port on the local ODU. This is a temporary state until the unit has acquired holdover history.
Locked Local, Holdover Acquired	Sync E tracking has locked to a synchronisation signal from a cabled Ethernet port on the local ODU and has acquired holdover history.
Holdover	There is currently no source for the tracking loop, but previously the tracking loop was in a Locked, Holdover Acquired state. The system is using the last known good frequency.
Locked Remote, Acquiring Holdover	The tracking loop has locked to a synchronisation signal from the remote ODU. This is a temporary state until the unit has acquired holdover history.
Locked Remote, Holdover Acquired	The tracking loop has locked to a synchronisation signal form the remote ODU and has acquired holdover history.

TDD Synchronization

The TDD Synchronization section of the System Status page contains the attributes described in Table 175.

Table 175 System Status attributes – TDD Synchronization

Attribute	Meaning
TDD Synchronization Status	The status of TDD synchronization. Displayed at a TDD Master if TDD synchronization is active. For a list of values and their meanings, see Table 176 and Table 177.

Table 176 TDD Synchronization Status values and meanings for PTP-SYNC

Value	Meaning
Inactive	TDD Synchronization has been administratively disabled. This value is not displayed in the System Status page, but can be determined from the SNMP MIB. TDD Synchronization Status is always in the Inactive state at a TDD Slave unit.
Cluster Timing Master	The ODU has been configured as a Cluster Master with an internal reference, and is communicating correctly with the PTP SYNC unit.

Value	Meaning
Initialising	The wireless link is down, and the master ODU is attempting to synchronize the TDD frame structure with an external 1 pps reference. Synchronization proceeds more rapidly in this state than in the Acquiring Lock state, because the TDD master does not need to consider the ability of the TDD slave to track changes in frame timing.
PTP-SYNC Not Connected	The ODU is not able to communicate with the PTP SYNC unit.
Locked	The master ODU has locked the TDD frame structure to the 1 pps reference received at the input of the PTP-SYNC unit. The ODU may be a Cluster Master or a Cluster Slave. The ODU is transmitting.
Holdover (No GPS Sync In)	The 1 pps reference has been lost at the input to the PTP-SYNC unit, and the ODU in a free running state. The ODU is transmitting. If the reference input is not restored, the Holdover state will terminate automatically after a period set by TDD Holdover Duration.
Holdover	The ODU is a Cluster Slave and the 1 pps reference has been lost at the input to an upstream PTP-SYNC unit. The ODU is locked to an upstream ODU that is in the Holdover (No GPS Sync In) state. The ODU is transmitting. If the reference input is not restored at the upstream PTP-SYNC unit, the Holdover state will terminate automatically after a period set by TDD Holdover Duration.
Not Synchronized (No GPS Sync In)	The 1 pps reference has been lost at the input to the PTP-SYNC unit and the holdover period has expired. If the ODU is configured for TDD Holdover Mode = Best Effort then the ODU will be transmitting, otherwise it will be muted.
Not Synchronized	The ODU is a Cluster Slave and the 1 pps reference has been lost at the input to an upstream PTP-SYNC unit. The holdover period has expired. If the ODU is configured for TDD Holdover Mode = Best Effort then the ODU will be transmitting, otherwise it will be muted.
Acquiring Lock	The wireless link is up and the master ODU is attempting to synchronize the TDD frame structure with an external 1 pps reference. Frame timing changes at the TDD master are constrained to allow for tracking by the TDD slave. This state is not allowed when TDD Holdover Mode = Strict.

Table 177 TDD Synchronization Status values and meanings for CMM5 or direct connection

Value	Meaning
Inactive	TDD Synchronization has been administratively disabled. This value is not displayed in the System Status page, but can be determined from the SNMP MIB. TDD Synchronization Status is always in the Inactive state at a TDD Slave unit.
Initialising	The wireless link is down, and the master ODU is attempting to synchronize the TDD frame structure with an external 1 pps reference. Synchronization proceeds rapidly in this state because the TDD master does not need to consider the ability of the TDD slave to track changes in frame timing.
Locked	The TDD frame structure is locked to a 1 pps reference from the CMM5 or from the directly-connected partner ODU. The ODU is transmitting.
Holdover	The ODU is transmitting. If the reference input is not restored, the Holdover state will terminate automatically after a period set by TDD Holdover Duration.
Not Synchronized	The holdover period has expired. If the ODU is configured for TDD Holdover Mode = Best Effort then the ODU will be transmitting, otherwise it will be muted.

IEEE 1588 Transparent Clock

Note IEEE 1588 Transparent Clock is available in the PTP topology.

The IEEE 1588 Transparent Clock section of the System Status page contains the attributes described in Table 178.

Table 178 System Status attributes – IEEE 1588 Transparent Clock

Attribute	Meaning
Transparent Clock	Indicates if the IEEE 1588 transparent clock feature is enabled.

Rebooting and logging out

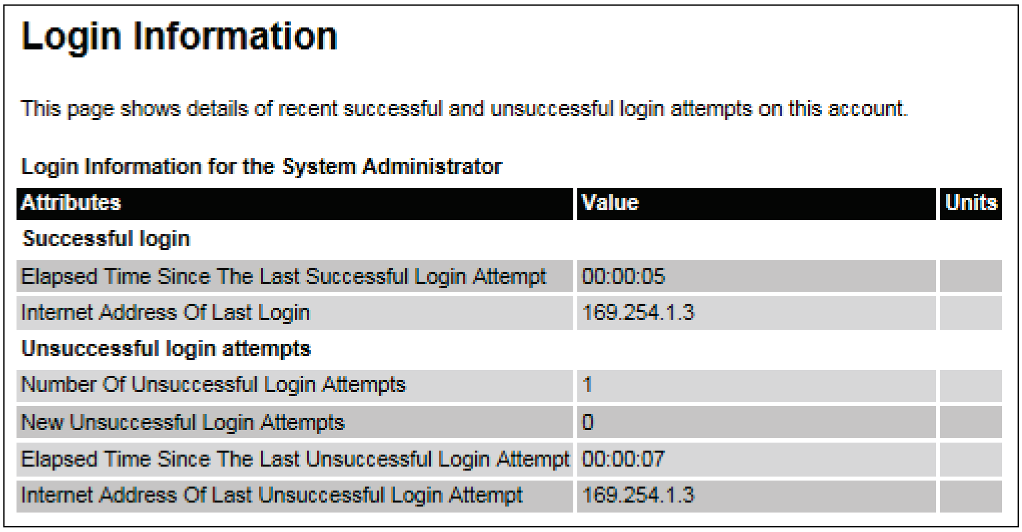
This section describes how to reboot the unit and log out of the web interface.

Login Information page

Menu option: **Management > Web > Login Information** (Figure 205).

Use this page to show recent successful and unsuccessful login attempts on this account.

Figure 205 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

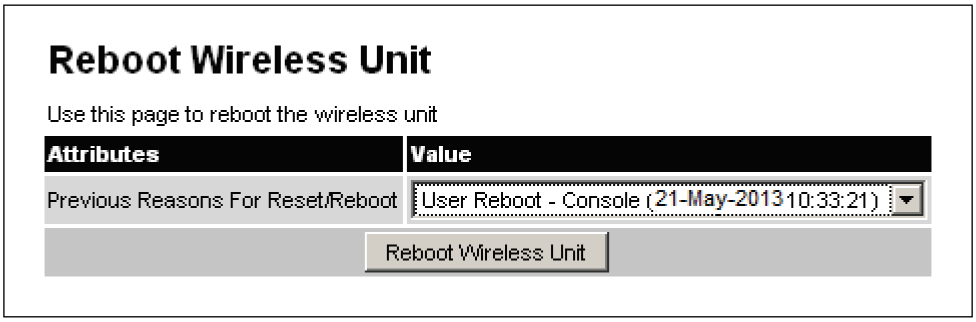
Attributes	Value	Units
Successful login		
Elapsed Time Since The Last Successful Login Attempt	00:00:05	
Internet Address Of Last Login	169.254.1.3	
Unsuccessful login attempts		
Number Of Unsuccessful Login Attempts	1	
New Unsuccessful Login Attempts	0	
Elapsed Time Since The Last Unsuccessful Login Attempt	00:00:07	
Internet Address Of Last Unsuccessful Login Attempt	169.254.1.3	

Reboot Wireless Unit page

Menu option: **System > Reboot** (Figure 206).

Use this page to reboot the ODU or view a list of previous reboot reasons.

Figure 206 Reboot Wireless Unit page



Reboot Wireless Unit

Use this page to reboot the wireless unit

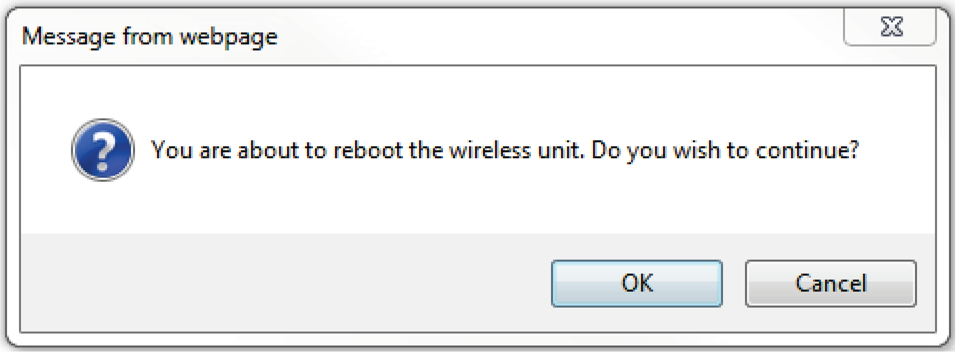
Attributes	Value
Previous Reasons For Reset/Reboot	User Reboot - Console (21-May-2013 10:33:21)
	Reboot Wireless Unit

Procedure:

- Use the drop-down list to view the Previous Reasons For Reset/Reboot.
- If a reboot is required:
  - Click **Reboot Wireless Unit**. The Reboot Confirmation dialog is displayed (Figure 207).

- Click **OK**. The reboot progress message is displayed. On completion, the unit restarts.

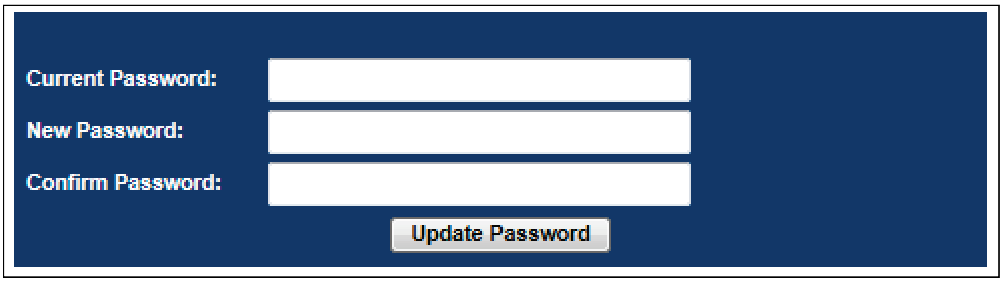
Figure 207 Reboot confirmation pop up



Change Password page

Menu option: **Change Password** (Figure 208). Use this page to change a personal password.

Figure 208 Change Password page (System Administration example)



A security officer can change the passwords of other users using the User Accounts page, as described in Local User Accounts page on page 6-70.

Procedure:

- Enter and confirm the new password (the default is blank). The new password must comply with the complexity rules (Table 145).

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 160).

Alarms, alerts and messages

This section describes how to use alarms, alerts and syslog messages to monitor the status of a PTP 700 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 the menu option **Alarms** to navigate to the Alarms page. The warning triangle and the Alarms menu item are hidden if there are no active alarms.

The example in Figure 209 shows the warning triangle in the navigation bar and an alarm displayed in the Alarms page. The alarms are defined in Table 179.

A change of state in most alarms generates an SNMP trap or an SMTP email alert.

Figure 209 Alarms page

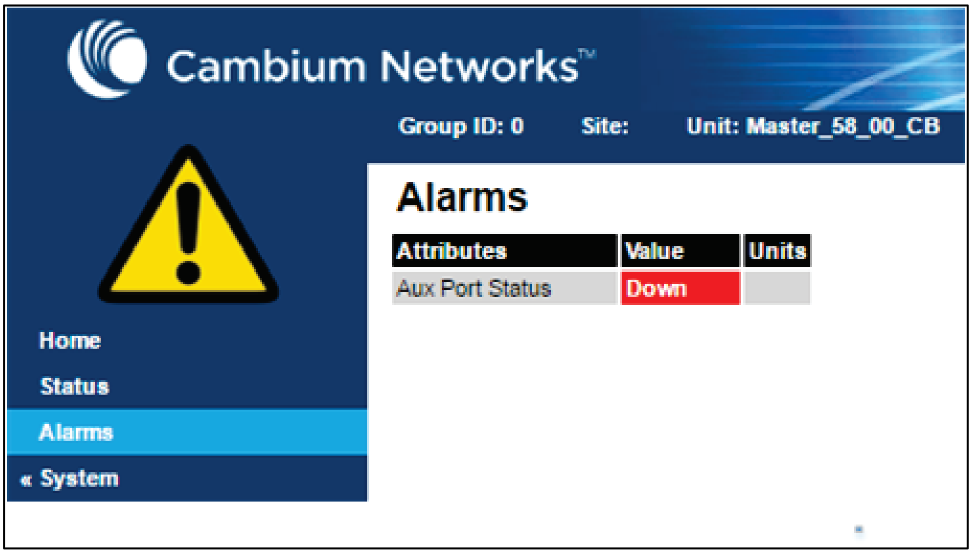


Table 179 System alarms

Alarm	Meaning
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.
Aux Port Disabled Warning	The Aux port link has been administratively disabled via the SNMP Interface.
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.

Alarm	Meaning
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.
Cable Diagnostics Warning	“Test In Progress“ means that the Cable Diagnostics test has been initiated on one or more ports and is in progress.
Capacity Variant Mismatch	The link ends are different capability variants, for example, one is Full and the other is Med.
Data Bridging Status	This alarm depends on Lowest Data Modulation Mode. “Disabled” means that the link has stopped bridging Ethernet frames because the Lowest Data Modulation Mode is not being achieved.
Device Certificate Status	Please contact customer support if this error is displayed.
Hot Standby Configuration Check	The configuration of the ODU is not compatible with the configuration of a Hot Standby neighbor.
Hot Standby Neighbor Link Status	The neighbor link in a Hot Standby configuration has a fault, or its status is unknown. Possible values are “Unknown”, “Wireless Link Down”, “Master Data Port Down”, “Slave Data Port Down”.
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 6-125.
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.
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).

Alarm	Meaning
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.
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.
No Wireless Channel Available	Spectrum Management was unable to locate a suitable wireless channel to operate on.
Port Allocation Mismatch	The local and remote ODUs have different services configured. The following alarms are raised on the port configuration mismatch: • **Mismatch in Out of Band Remote Management Service**: The Out of Band Management Service is configured at the local unit but it is not configured at the remote unit or vice versa.
Regulatory Band	The installed license key contains an invalid Regulatory Band. The wireless unit is prohibited from operating outside the regulated limits.
Remaining Full Capacity Time Trial	Time remaining on the full capability trial period. Activated when seven days or less of the trial period remain.
Remote Transparent Clock Compatibility	The local and remote units have different IEEE 1588 transparent clock configurations. Both units must have the same configuration for the feature to work correctly.
Secure Mode Alarm	The unit is operating in the FIPS secure mode, but is not in the operational state. To clear an alarm value of **Secure mode is not configured** ensure that all settings are correct for FIPS 140-2 in the Security Wizard. To clear an alarm value of **Secure mode is configured, but not active** ensure that HTTP Access Enabled is set to **No**.
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.

Alarm	Meaning
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.
SNTP Synchronization failed	SNTP has been enabled but the unit is unable to synchronize with the specified SNTP server.
Sync E tracking state	The state of the Synchronous Ethernet feature, if there is a problem.
Syslog Client Enabled/Disabled Warning	The local syslog client has been enabled or disabled.
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.
Syslog Local Wrapped	The local log of event messages is full and is now being overwritten by new messages.
TDD Synchronization Alarm	The reference signal for TDD Synchronization is absent and the ODU is now in holdover with more than 80% of the holdover period elapsed (**Reference Signal Lost**) or the ODU has reached the end of the configured holdover period and may not be correctly synchronized with the remaining units in the wireless network (**Synchronization Lost**). If TDD Synchronization Alarm = Synchronization Lost and TDD Holdover Mode = Strict, the ODU will be muted and the wireless link will be down.
Transparent Clock Source Port Alarm	If SFP was the selected transparent clock source port but the media did not negotiate to Fiber.
Unit Out Of Calibration	The unit is out of calibration and must be returned to the factory using the RMA process for re-calibration.
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**.

Email alerts

The management agent can be configured to generate alerts by electronic mail when certain events occur. The alerts are defined in Table 180.

Table 180 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 210).

Use this page to view the local log of event messages.

Figure 210 Syslog local log


Previous Page Refresh

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 1-59 describes the system logging feature.

Syslog Configuration page on page 6-86 describes how to enable system logging.

Format of syslog server messages

PTP 700 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 = "PTP700" 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:

PTP700: configuration; IP Address; Web user; was=10.10.10.10; now=169.254.1.1;

This is an example of a status message:

PTP700: status; Data Port Status; was=Down; now=Up;

Event messages

Event messages are listed in Table 181. Definition of abbreviations:

SC = ";"
SP = " "

This is an example of an event message:

PTP700: event; auth_login; web user=MarkT; from=169.254.1.1; port=80; connection=HTTP; authentication=local;

Table 181 Event messages

Facility	Severity	Identifier	Message content
security(4)	warning(4)	auth_idle	
security(4)	info(6)	auth_login	

Facility	Severity	Identifier	Message content
security(4)	warning(4)	auth_login_failed	"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)	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
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

Facility	Severity	Identifier	Message content
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
security(4)	info(6)	eap_tls_auth	"MAC=" MAC-address SC "Authentication success" SC "Cipher=" cipher SC cipher = "None" | "AES 128-bit TLS RSA" | "AES 256-bit TLS RSA"
security(4)	warning(4)	eap_tls_auth_failure	"MAC=" MAC-address SC "reason=" eap-tls-auth-reason SC eap-tls-auth-reason = "Authentication timeout" | "Authentication error" | "Certificates not installed" | "Installed certificate has a common name mismatch" | "Invalid certificate Root CA" | "Installed certificate has invalid key length"| "Certificate common name does not match with any entry in whitelist" | "TLS handshake failed."
security(4)	info(6)	eap_tls_rekey	"MAC=" MAC-address SC "Rekey success" SC "Cipher=" cipher SC
security(4)	warning(4)	eap_tls_rekey_failure	"MAC=" MAC-address SC "reason=" eap-tls-rekey-reason SC eap-tls-rekey-reason = "Rekey timeout" | "Rekey error" | "Certificate common name does not match with any entry in whitelist" | "TLS handshake failed."

Spectrum Management

This section describes how to use the Spectrum Management pages to monitor the radio spectrum usage of the PTP 700 link.

Spectrum Expert and Spectrum Management pages

There are two alternative web pages providing access the spectrum monitoring information:

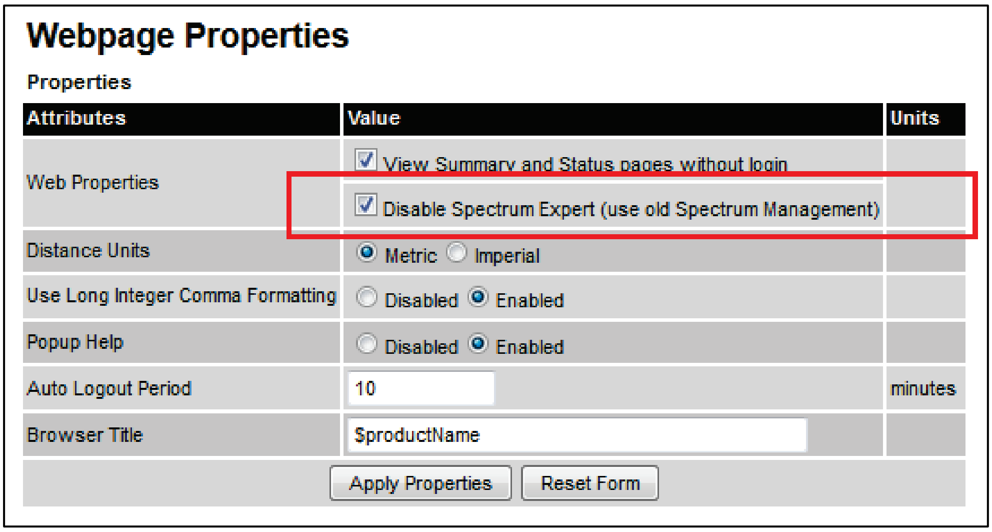
- the Spectrum Expert page, and
- the Spectrum Management page.

The Spectrum Expert page is the default as it is effectively a superset of the Spectrum Management page. However, it makes use of features only available in the most recent web browsers. It also requires additional data to be sent across the wireless link, thus reducing the capacity available for other types of traffic when the page is displayed.

Note Internet Explorer versions up to and including IE8 do not support the HTTP features used in the Spectrum Expert page.

For these reasons, the PTP 700 Series may be configured to use the Spectrum Management page instead of the Spectrum Expert page. This is done by checking the **Disable Spectrum Expert (use old Spectrum Management)** control in the **Web Property** attribute under the **Management > Web > Web Properties** menu, as shown in Figure 211.

Figure 211 Disabling Spectrum Management page advanced web page



Note When configured to use the Spectrum Expert page, the PTP 700 is capable of automatically detecting whether the browser accessing the unit supports the required features. If it does not, the Spectrum Management page will be returned instead of the spectrum Expert page. Internet Explorer 8 is not compatible with the Spectrum Expert page.

Spectrum Expert page

Menu option: **System > Spectrum Expert**

This page is used to view and configure spectrum usage.

The Spectrum Expert page displays the following plots:

- The Local Receive Spectrum for PTP or HCMP wireless topology, and
- The Peer Receive Spectrum for PTP wireless topology.

The Spectrum Expert page has two display modes:

- Standard Display mode – The 'Standard' Display mode is the mode which displays only the operational subband channels (shown in Figure 212). In this mode, the Extended Spectrum Scanning attribute could be Enabled but the Extended display box could be un-checked.

  It has further two types of plot:

  - Standard Display mode without realtime line
  - Standard Display mode with realtime line

- Extended Display mode – The 'Extended' Display Mode shows the entire DSO Full Band range of channels along with highlighted operational channels (shown in Figure 213). In this mode, the Extended Spectrum Scanning attribute is Enabled.

  This mode also has two types of plot:

  - Extended Display mode without realtime line
  - Extended Display mode with realtime line

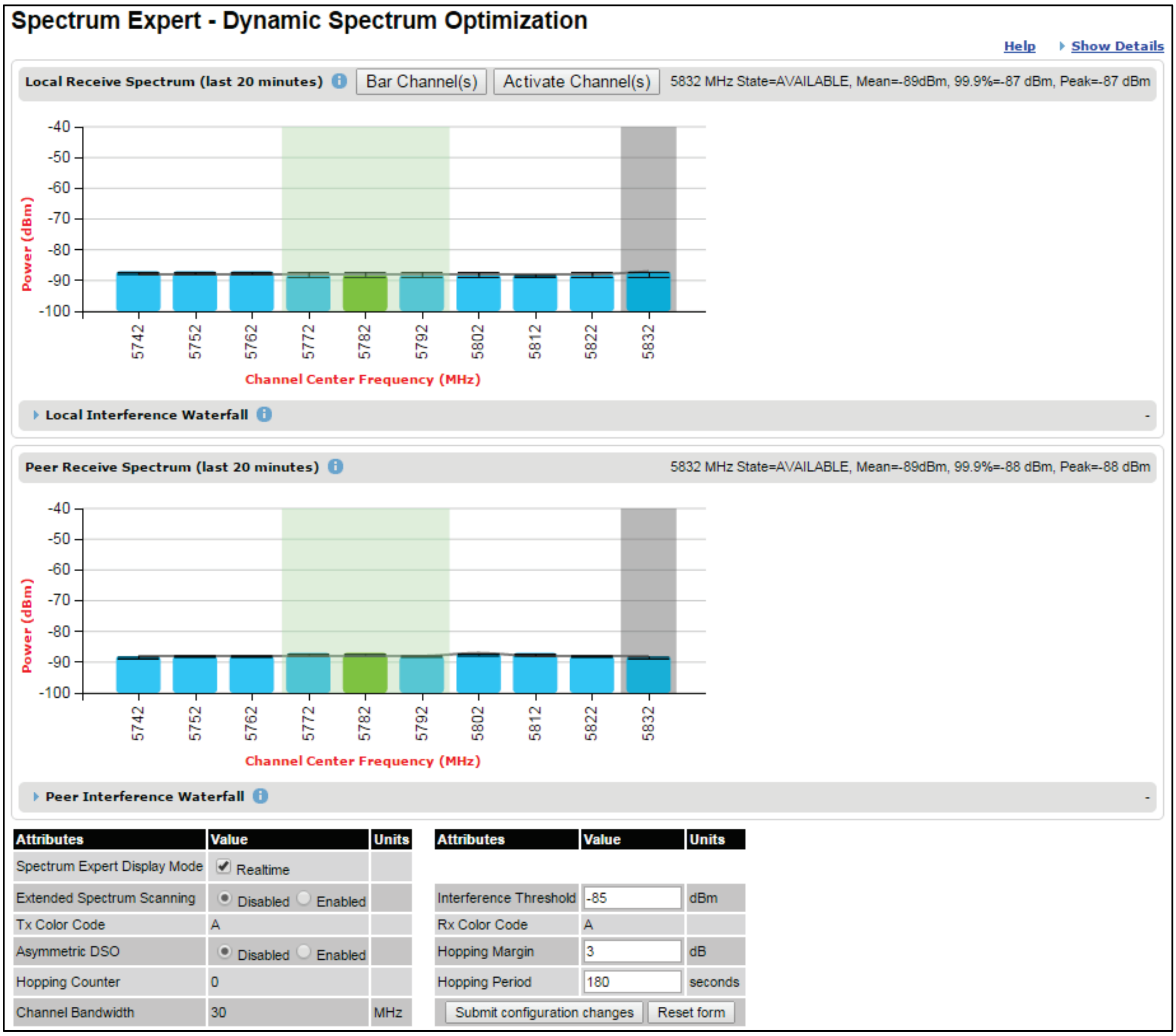
The Extended display mode selection checkbox appears when the Extended Spectrum Scanning attribute is set to Enabled.

See Interpreting the receive spectrum plot on page 7-35 for details on the how to interpret these plots.

Attention Do not leave the ODU with Extended Spectrum Scanning enabled during normal operation because this adversely affects the DSO response in the operating band.

Standard Display mode

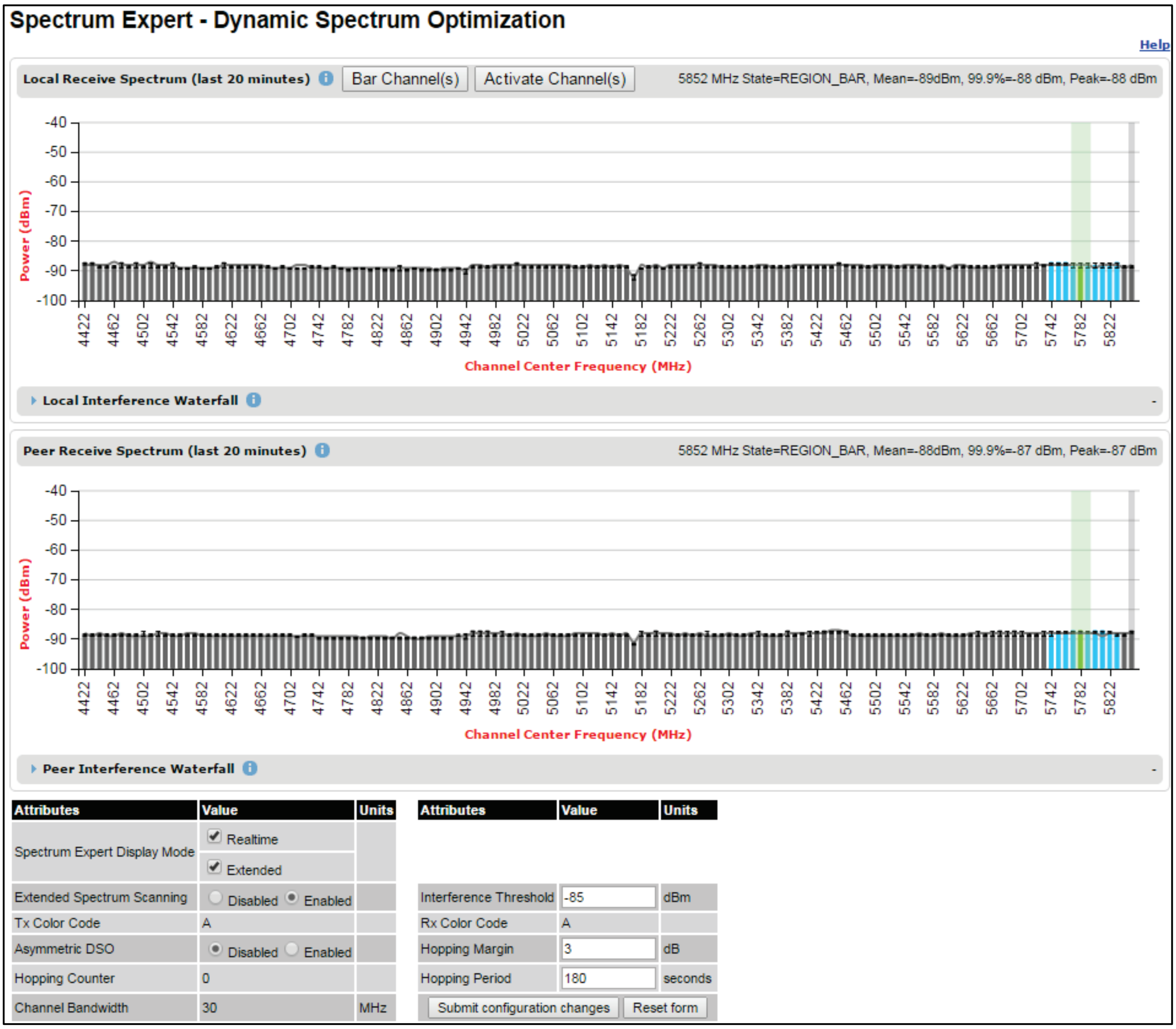
Figure 212 Spectrum Expert page – Standard Display mode



Note When Wireless Network Topology is set to HCMP, only the Local Receive Spectrum is shown on both the Master and the Slaves.

Extended Display Mode

Figure 213 Spectrum Expert page – Extended Display mode



Note Figure 212 shows the default layout for a unit configured as a Master. On a unit configured as Slave, some of the controls at the bottom of the page are not available. In the remainder of this section, the screen shots shown are for the Master Unit.

Note For Spectrum Expert Extended Display mode, Extended Spectrum Scanning is Enabled and Display mode is set to Extended.

Note When Wireless Network Topology is set to HCMP, only the Local Receive Spectrum is shown on both the Master and the Slaves.

Standard Display with extended layout

The page layout may be changed from the compact layout to the extended layout by clicking on the **Show Details** hyperlink on the top right of the page shown in Figure 212.

This hyperlink is only visible when the Extended Display checkbox in Spectrum Expert Display Mode is not selected.

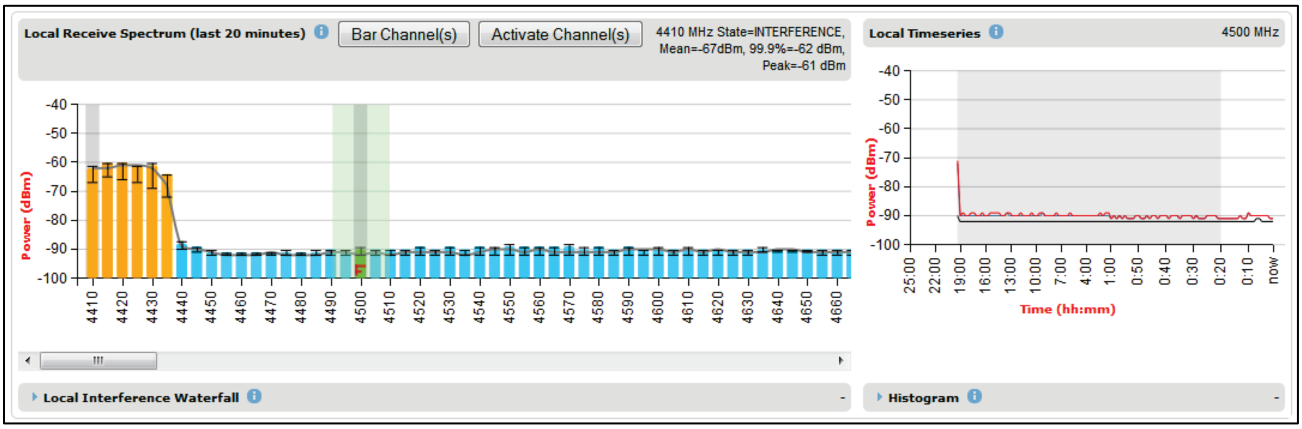
A screen shot of the Spectrum Expert page in the extended layout is shown in Figure 214. It displays the following additional plots:

- The Local Timeseries, and
- The Peer Timeseries.

These plots are on the right of the corresponding Receive Spectrum plots. See Selecting a Channel and a Time period on page 7-43 for details on the timeseries plots.

Clicking on the **Hide Details** hyperlink returns to the compact layout.

Figure 214 Spectrum Expert page with Receive Spectrum and Timeseries for the Local unit



Full layout

The page layout may be extended further to give access to more information on either or both the local and the peer interference spectra.

For the local interference spectrum, clicking on the **Local Interference Waterfall** hyperlink below the Local Receive Spectrum plot shows:

- The Local Interference Waterfall plot, if the Local TimeSeries was not shown (Figure 215), or
- The Local Interference Waterfall and the Histogram plots otherwise (Figure 216).

The same can be done for the peer section of the page.

Details on how to interpret the Interference Waterfall and Histogram plots are provided in sections Interpreting the Interference Waterfall plot on page 7-45 and Interpreting the histogram plot on page 7-47 respectively.

Figure 215 Spectrum Expert page showing the Receive Spectrum and Interference Waterfall for the Local unit

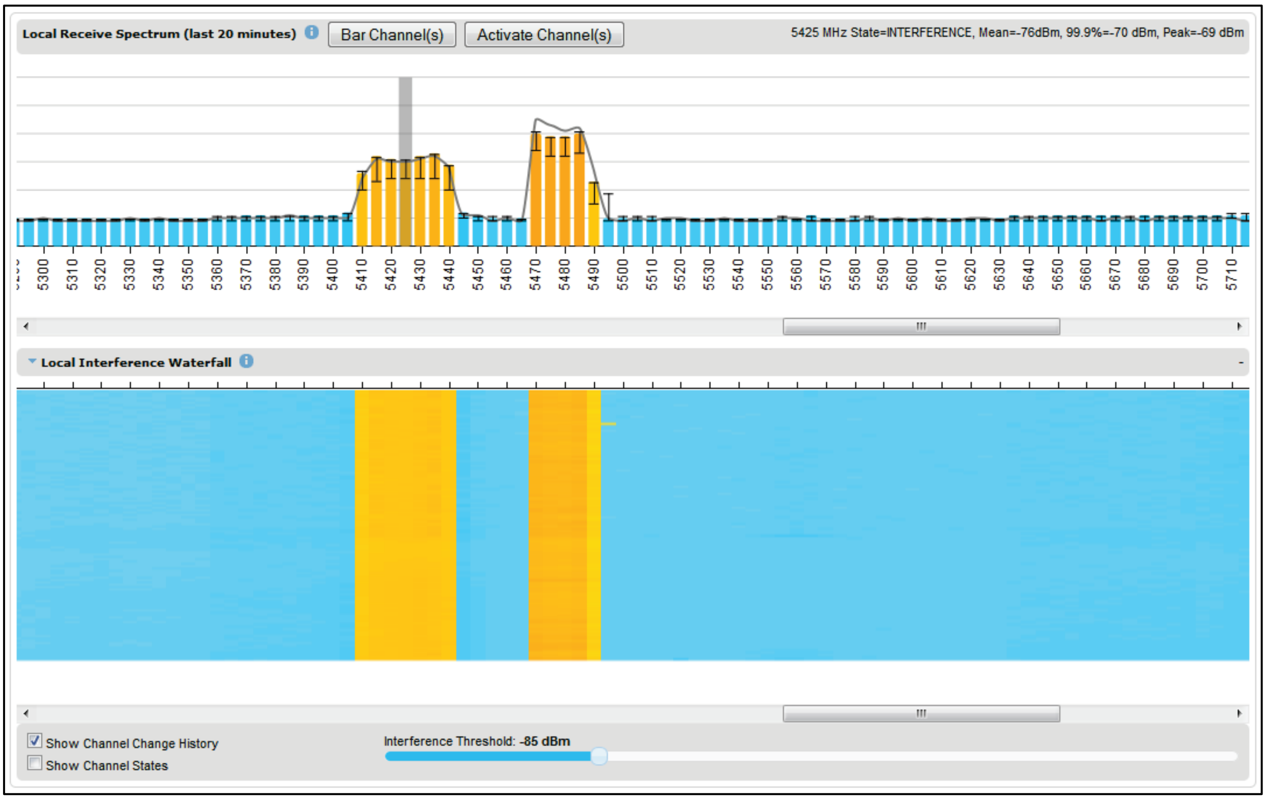
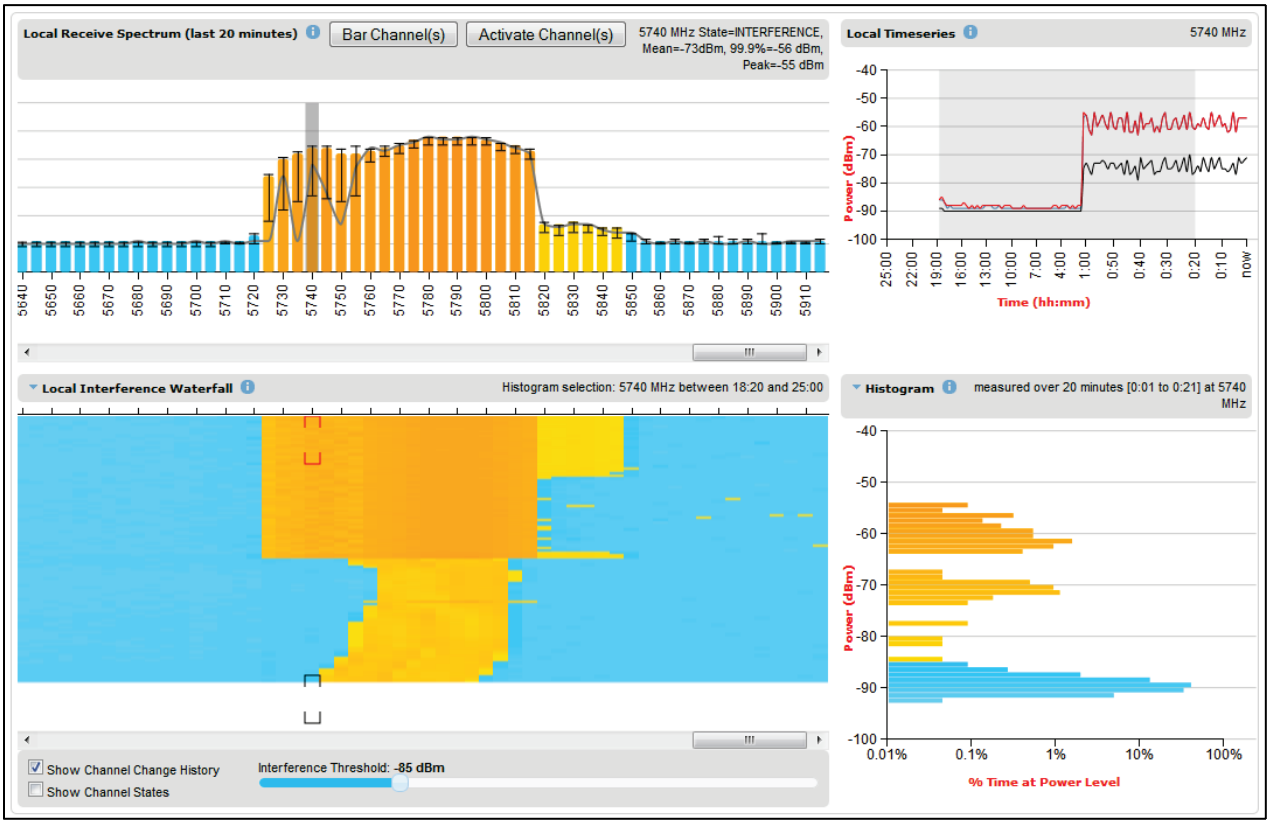


Figure 216 Spectrum Expert page showing the Receive Spectrum, Timeseries, Interference Waterfall and Histogram for the Local unit



Spectrum Expert page with Slave Scan

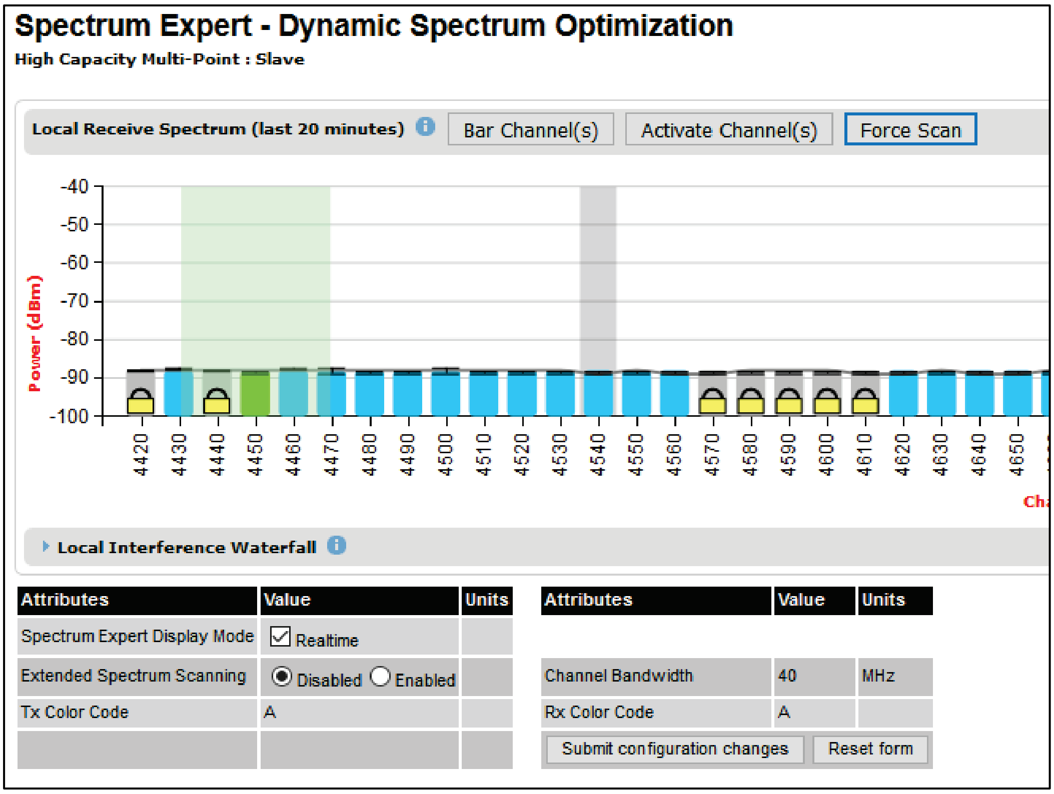
The page layout in an HCMP Slave with Slave Scan is shown in Figure 217.

When Slave Scan is configured at a Slave ODU, the Spectrum Expert page allows channels to be administratively barred using the **Bar Channel(s)** and **Activate Channel(s)** buttons. Bar unused channels to reduce the scan time.

The Slave Scan channel scan can be monitored by observing progress of the green colored channel marker.

Restart the channel scan on the lowest channel using the **Force Scan** button. This option is useful if physical installation (for example, antenna alignment) is changed whilst a scan is in progress.

Figure 217 Spectrum Expert page with Slave Scan



Spectrum Management page

Menu option: **System > Spectrum Management**

Note that this page is only shown when the Spectrum Expert page has been disabled, as explained in Spectrum Expert and Spectrum Management pages on page 7-26.

Use this page to view and configure spectrum usage. The width of the vertical green bar represents the channel width (10 MHz illustrated).

Note The extended view is available only in Spectrum Expert, and not in Spectrum Management.

Note When Wireless Network Topology is set to HCMP, only the Local Receive Spectrum is shown on both the Master and the Slaves.

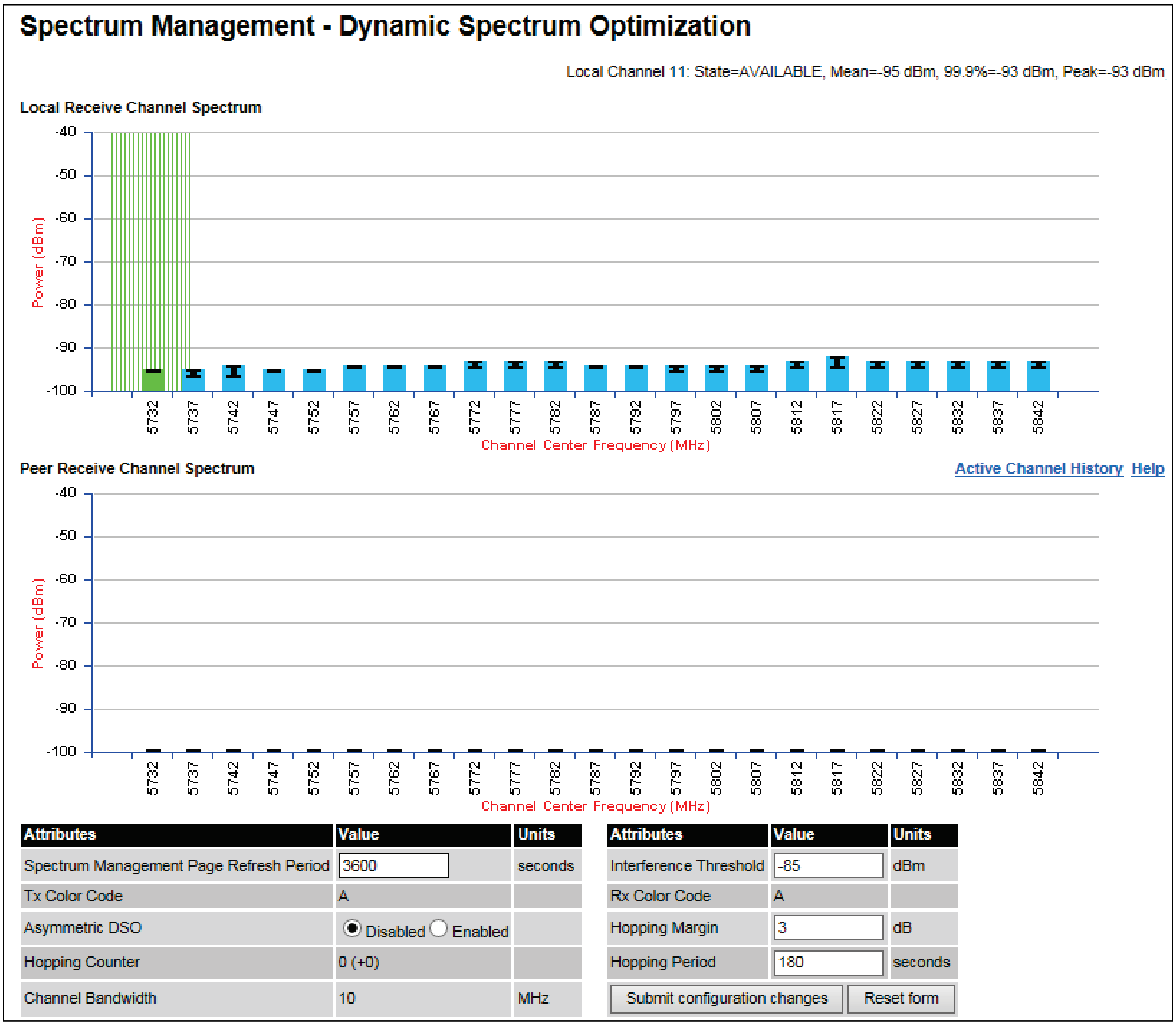


Figure 218 Spectrum Management page (Master unit)

Figure 218 shows the Spectrum Management page layout for a unit configured as a Master. On a unit configured as Slave, some of the controls at the bottom of the page are not available.

Spectrum Management Settings

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 700 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 6-24.

> **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 182)
- Update the attributes as required. At the slave unit, only Page Refresh Period can be updated.
- To save changes, click Submit configuration changes.

Table 182 Spectrum Management attributes

Attribute	Meaning
Spectrum Expert Display Mode	**Realtime:** When set to Realtime, an additional line appears on the Receive Spectrum plots showing the most recent measurements of interference level for every channel **Extended:** Extended Display mode is visible only when Extended Scanning is enabled. This control is available in the Spectrum Expert page only.
Extended Spectrum Scanning	**Enabled:** Enables scanning of entire DSO full band channels. **Disabled:** Only the operational subband channels are scanned. This control is available in the Spectrum Expert page only.
Spectrum Management Page Refresh Period	The page refreshes automatically according to the setting entered here (in seconds). This control is available in the Spectrum Management page only.
Hopping Margin	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.

Attribute	Meaning
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	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 (not configurable)	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.
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 700 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.
Tx Color Code (not configurable)	This shows the Tx Color Code selected during Installation.
Rx Color Code (not configurable)	This shows the Rx Color Code selected during Installation.

Interpreting the receive spectrum plot

The Spectrum Expert page has two graphical plots:

- Local Receive Spectrum
- Peer Receive Spectrum

A more detailed example of one of these plots is shown in Figure 212.

For more information, select the **Help** hyperlink at the top right of the Spectrum Expert page and follow the instructions.

X axis and Y axis

The X-axis shows a stylized view of the selectable wireless channels. Note that the distance between adjacent channels may be smaller than the channel bandwidth. If this is the case, adjacent channels 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 9 in Figure 212) is always marked using hatched green and white lines on the Spectrum Management page or solid green on the Spectrum Expert page. The width of the hatching is directly proportional the channel bandwidth or 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 183).

Table 183 Channel states represented in the Spectrum Expert plot

Color	State	Meaning
Green	Active	The channel is currently in use, hosting the 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.
Light 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 but The lock is not shown in Extended view.
Red	Radar Detected	A radar signal has been detected and operation on this channel is currently not allowed.
Dark Grey	Region Barred	Extended scanned channels outside the range of configured operational subband channels

Key metrics

The "I" bar and top of the colored bar represent three key metrics (Table 184). The vertical part of the "I" bar represents the statistical spread between the peak and the mean of the statistical distribution.

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.

Table 184 Key metrics represented in the Spectrum Expert 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.
Realtime interference level	The arithmetic mean of the power measured during the last quantization period. The quantization period is two seconds.	Countinuous line.

Spectrum Expert page in fixed frequency mode

When the link is operating in fixed frequency mode, the Spectrum Expert page uses two visual cues (Figure 219). The main page title has the “Fixed Frequency Mode” suffix and the selected channels are identified by a red capital “F”.

Figure 219 Spectrum Expert page for Fixed Frequency – Standard display mode

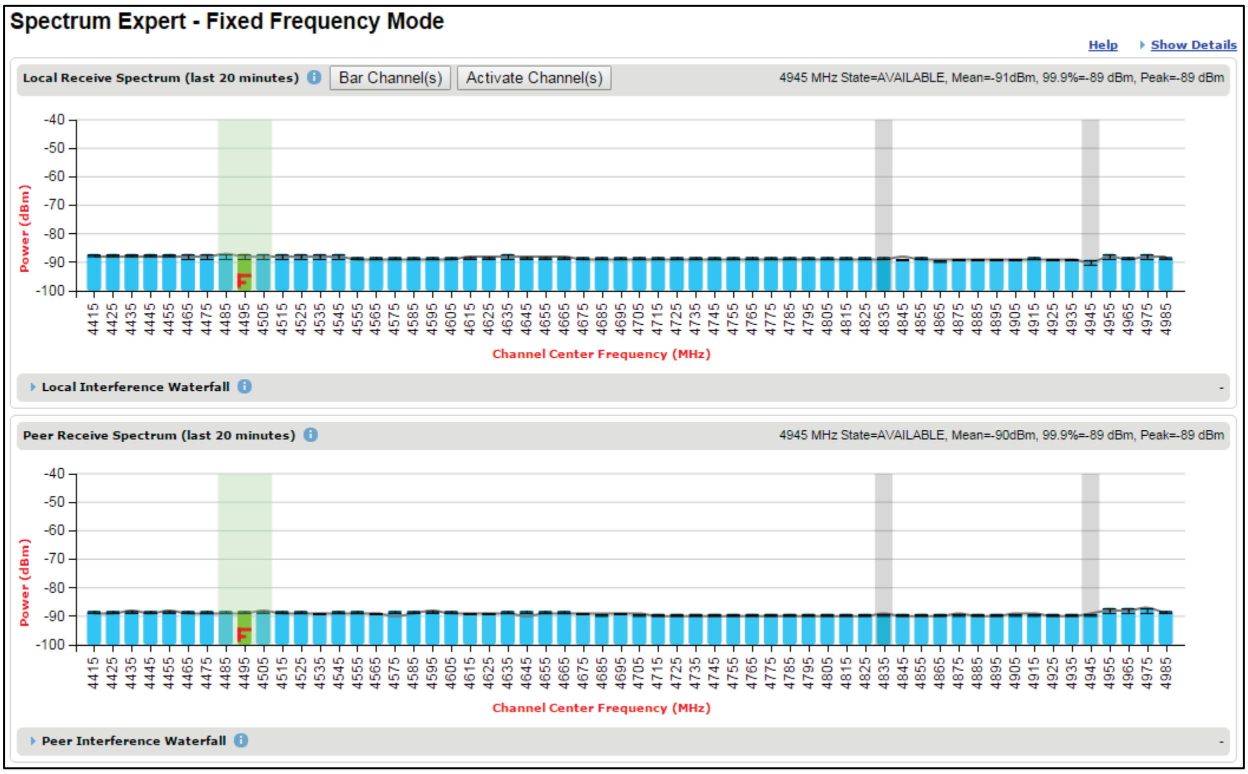
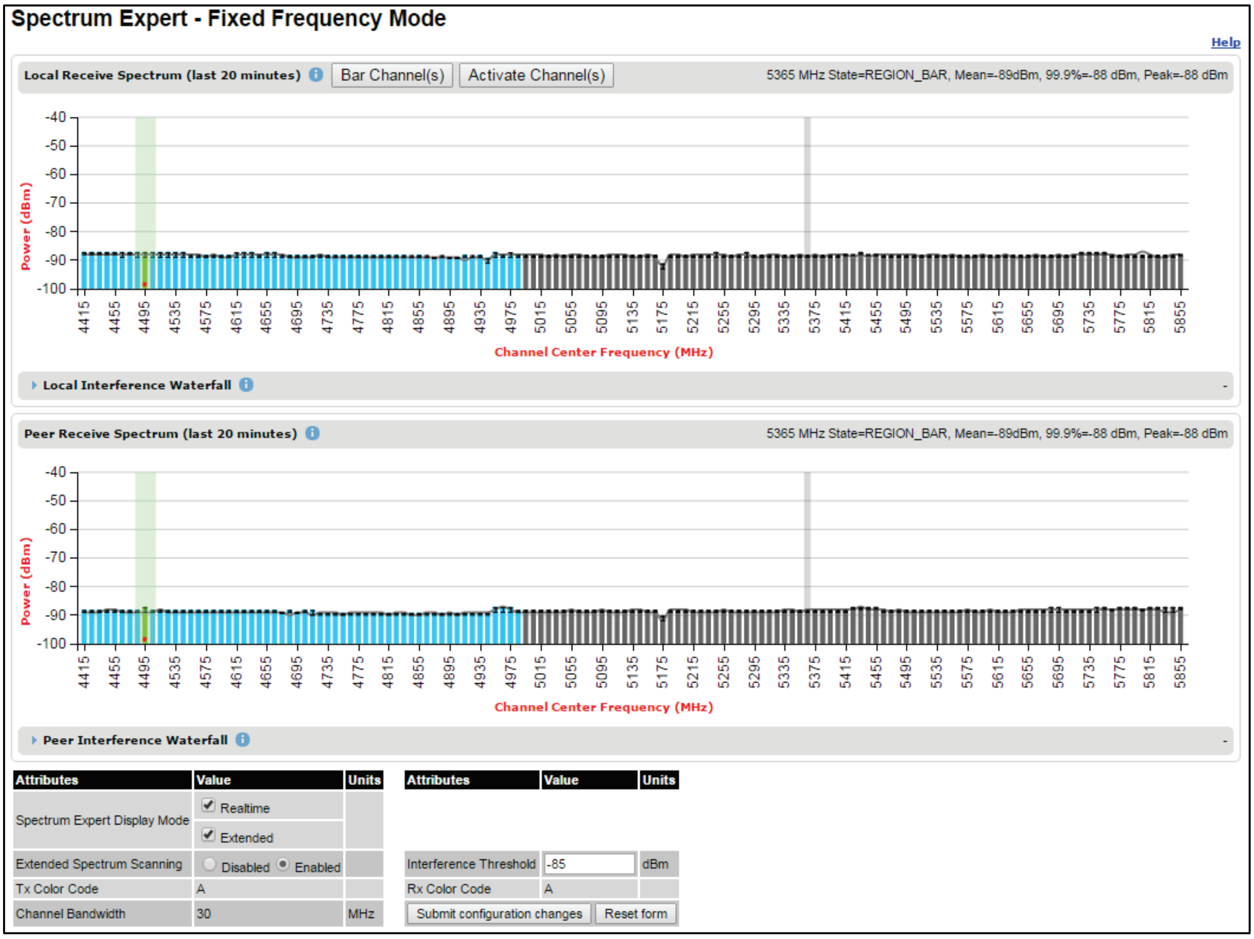


Figure 220 Spectrum Expert page for Fixed Frequency – Extended display mode



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 Spectrum Expert Display Mode 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.

Spectrum Expert page in radar avoidance mode

When the link is operating in radar avoidance mode, the Spectrum Expert page (Figure 221) 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 185).

Figure 221 Spectrum Expert page with radar avoidance – Standard Display

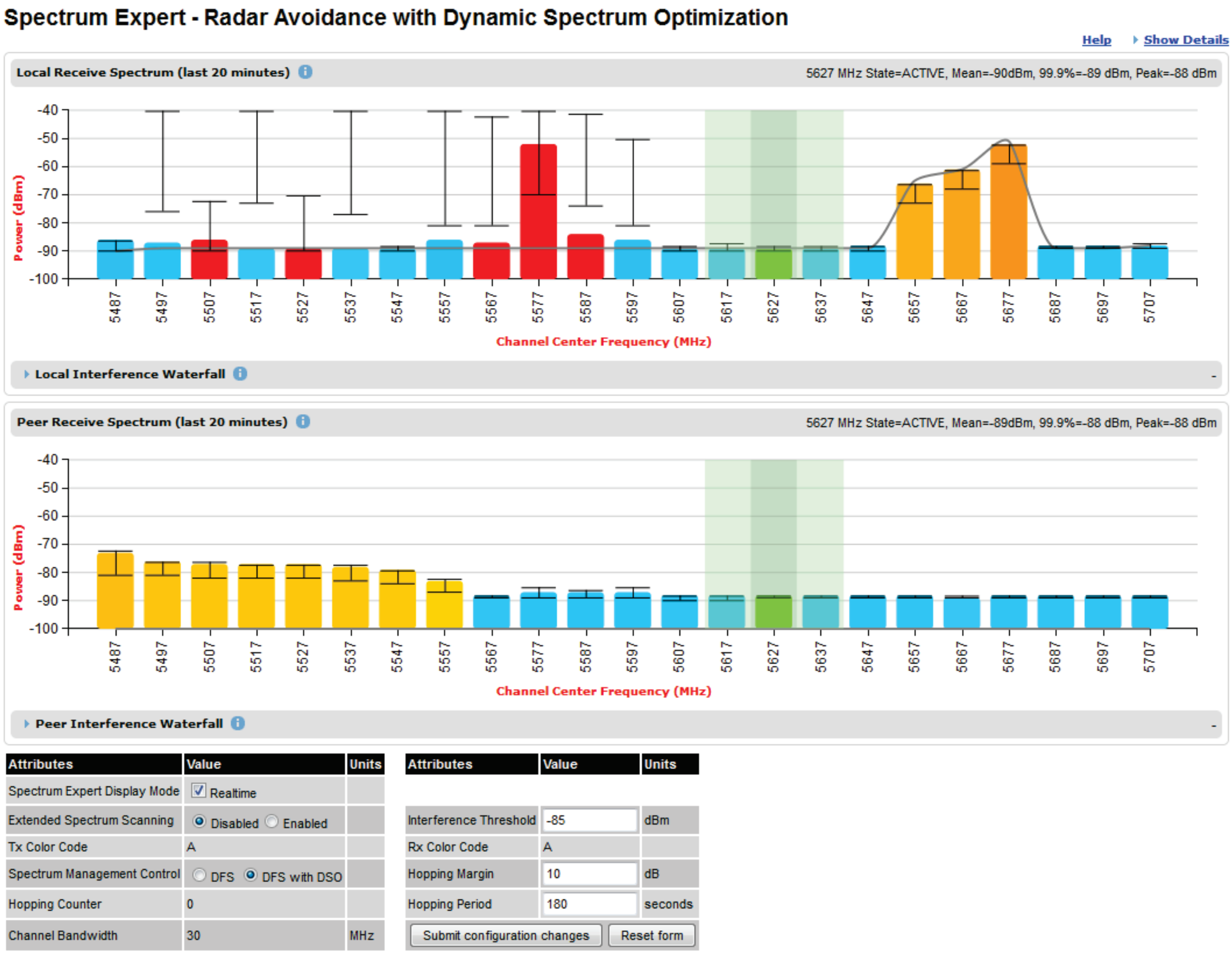
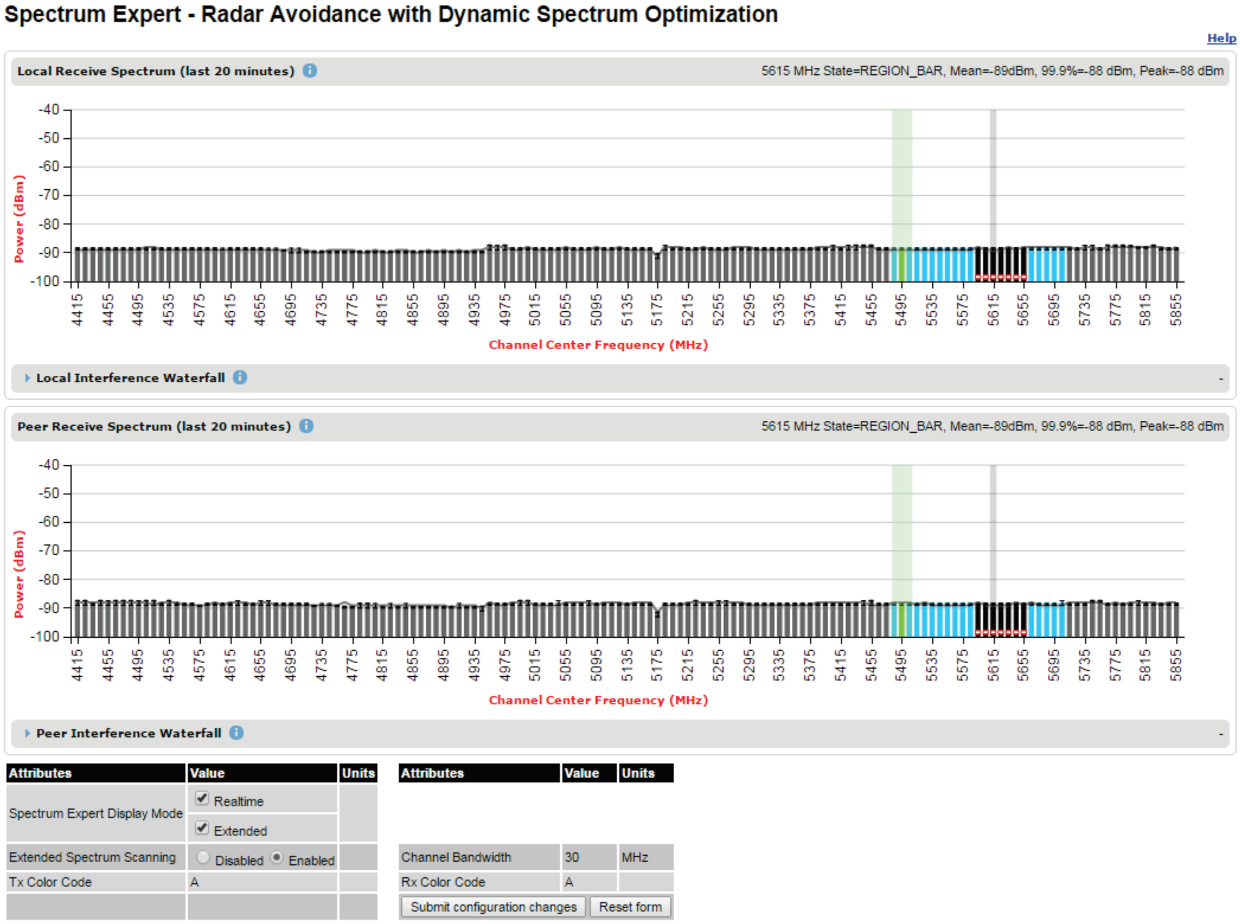


Figure 222 Spectrum Expert page with radar avoidance – Extended Display



When operating with RTTT (Road transport and Traffic Telematics) Avoidance enabled or other regulatory restrictions on channel usage, 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.

Table 185 Channel states in the Spectrum Expert 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

Color	State and color	Meaning
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.
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

Barring channels

Procedure:

- Log into the Master unit.
- Select menu option **System > Spectrum Expert**. The Spectrum Expert page is displayed.
- Select one channel by clicking on the graphical display. If required, select additional channels using control clicking, or select a range of channels using shift clicking. The example in Figure 223 shows three channels selected at 4965 MHz, 4970 MHz and 4975 MHz.
- Click on the **Bar Channel(s)** button. A confirmation dialogue is displayed as shown in Figure 224. Click **OK**.
- Barred channels are indicated by the lock symbol as shown in Figure 225 on page 7-43.

To activate previously barred channels, select the barred channels and click on **Activate Channel(s)**.

Note The **Bar Channel(s)** and **Activate Channel(s)** buttons are available on the Master unit, but not on the Slave unit.

Figure 223 Selecting channels for barring

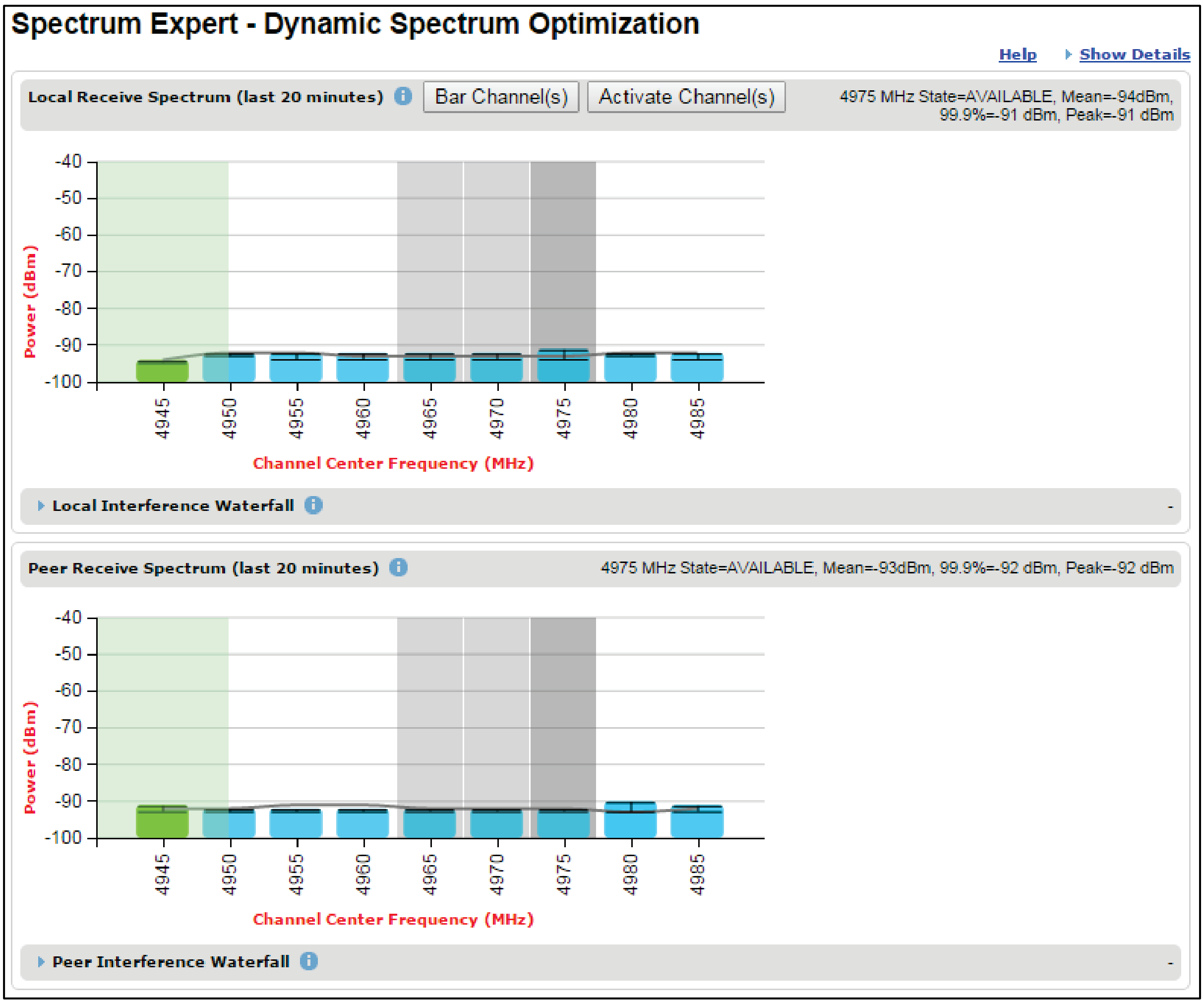


Figure 224 Channel barring confirmation

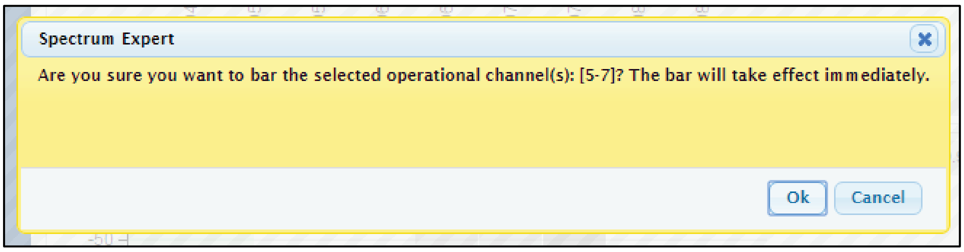
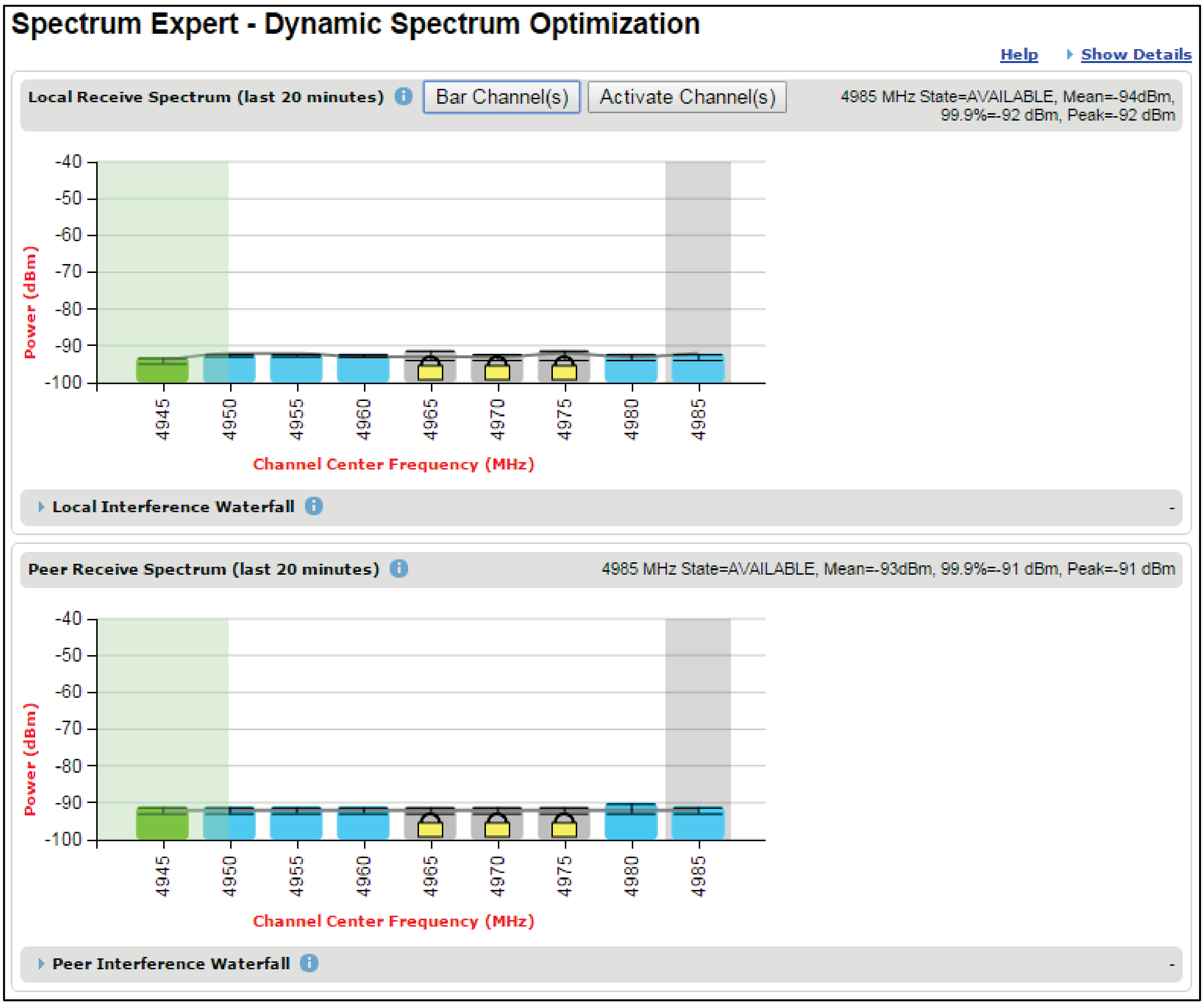


Figure 225 Barred channels



Selecting a Channel and a Time period

The Timeseries plot uses measurements for the selected channel. The Histogram plot uses measurements for the selected channel and the selected measurement period.

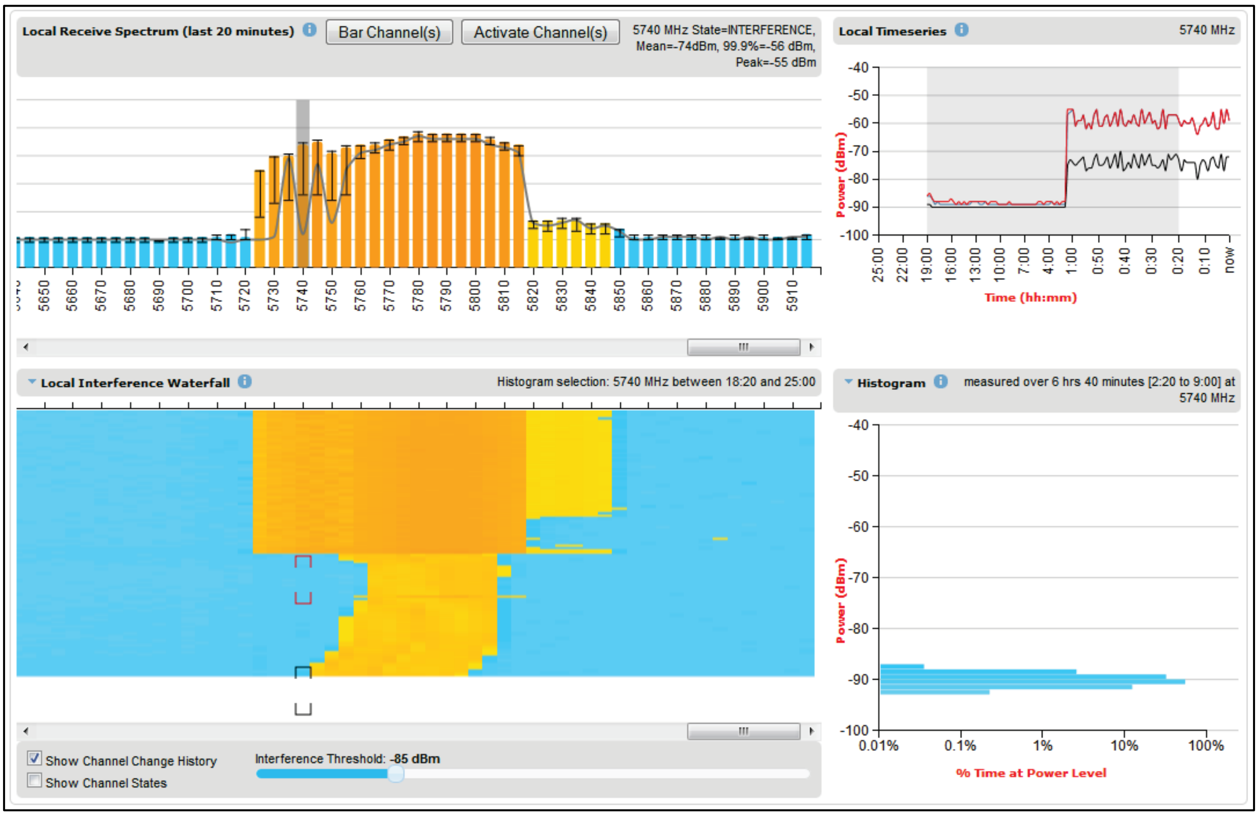
To select a channel, place the cursor in the Receive Spectrum display or the Interference Waterfall display. The Timeseries plot updates automatically to show the data for the selected channel. To select a combination of channel and time period, place the cursor in the Interference Waterfall display. The Histogram plot automatically updates to show data for the selected channel and time period.

The selected channel is shown with a grey background in the Receive Spectrum display and by the horizontal position of square brackets in the Interference Waterfall display. The selected time period is shown by the vertical position of the square brackets.

The Selected Channel is centred on 5740 MHz, and the time period is from 2:20 to 9:00 in the example in Figure 226.

The selected frequency and time period are also displayed in the heading for the Timeseries and Histogram plots.

Figure 226 Selecting a channel on the Receive Spectrum



To freeze the selection of channel and time period, click on the cursor position. The frequency and time period are now fixed until a new combination is selected by clicking in a different location. The frozen time period is shown by red brackets in the Interference Waterfall display.

Interpreting the timeseries plot

This plot displays the interference measurements of all previous measurement quantization periods for the selected channel, up to a maximum of 25 h (Figure 227).

The channel is selected as described in Selecting a Channel and a Time period. The center frequency of the selected channel is indicated in MHz at the top right of the Timeseries plot.

The colored lines represent interference measurements, with the color map provided in Table 186.

A white background indicates the measurement period which is used to generate the Receive Spectrum plot. Typically, only the last 20 min are used, although any period of time where the wireless link has been down is excluded.

Figure 227 Spectrum Expert, Timeseries plot

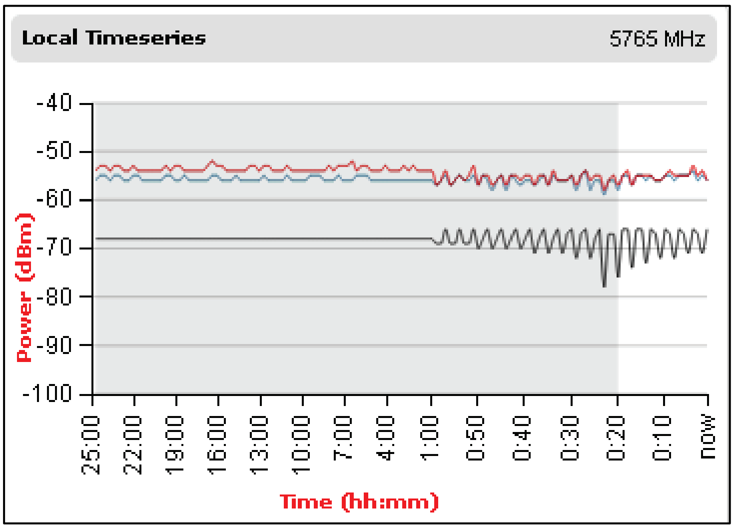


Table 186 Interference represented in the time series plot

Color	Meaning
RED	Peak of Means interference measurement
BLACK	99.9% percentile of means interference measurement
BLUE	Mean of Means interference measurement

Interpreting the Interference Waterfall plot

The Interference Waterfall indicates the level of interference for all the channels in the band over the last 25 h. Figure 228 shows a screen capture example.

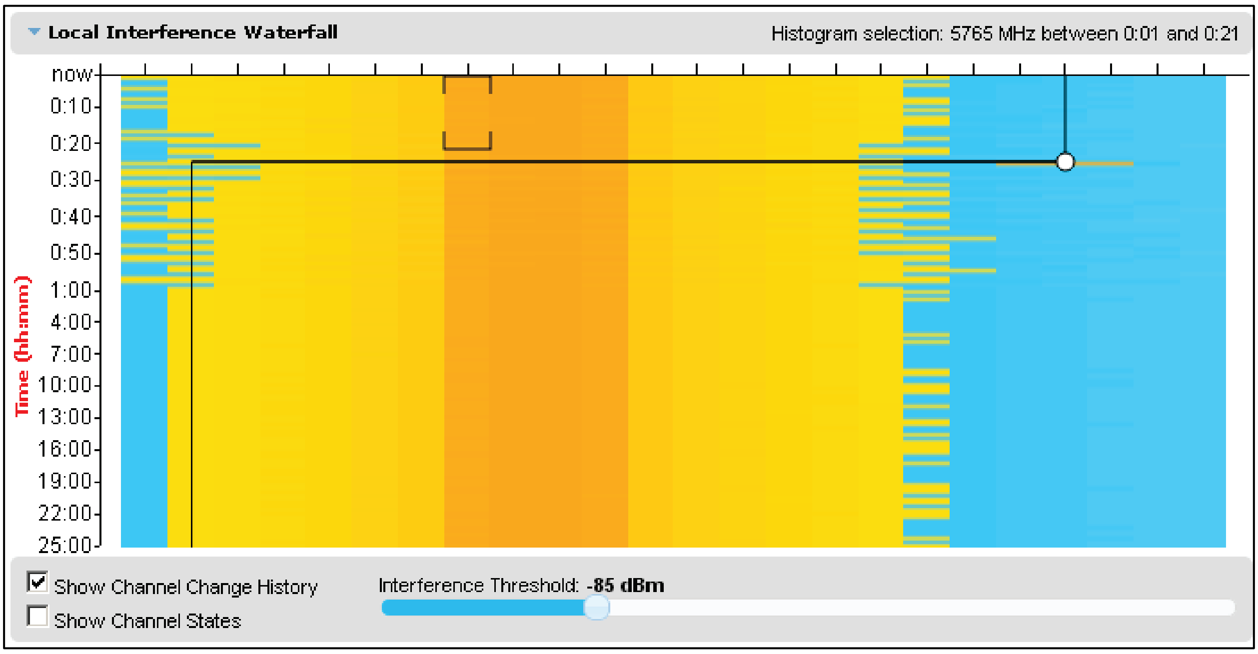
The channel and measurement period are selected as described in Selecting a Channel and a Time period on page 7-43 The center frequency of the selected channel and the time period are indicated at the top right of the Interference Waterfall plot.

The X-axis corresponds to the channel center frequency and is horizontally aligned with the Receive Spectrum plot.

The Y-axis corresponds to the time in the past in hours and minutes, with the most recent period being at the top of the plot.

Each channel and measurement period is indicated using the color scale given in Table 183.

Figure 228 Spectrum Expert, Interference Waterfall plot



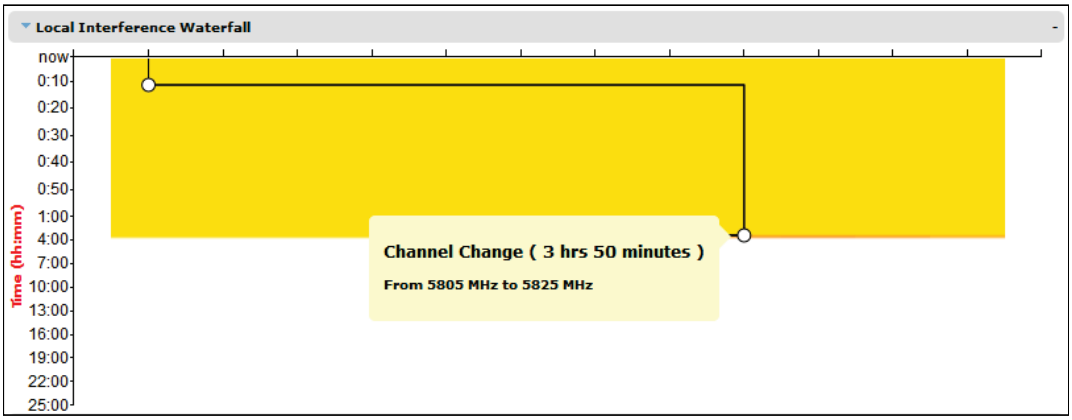
Setting the interference threshold

The interference threshold may be set using the sliding control located directly below the Interference Waterfall plot. This is an alternative to the method described in Spectrum Management Settings on page 7-32. For either method, the change to the Interference Threshold is not taken into account until the Submit button is clicked.

Viewing the active channel history

To display the active channel history, tick the Show Channel Change History control right below the Interference Waterfall plot. The active channel history over the last 25 hours is plotted as a black line overlay on the Interference Waterfall plot. A circle is displayed every time the active channel has changed. By hovering above the circle, the reason for the channel change is indicted, as shown in Figure 229.

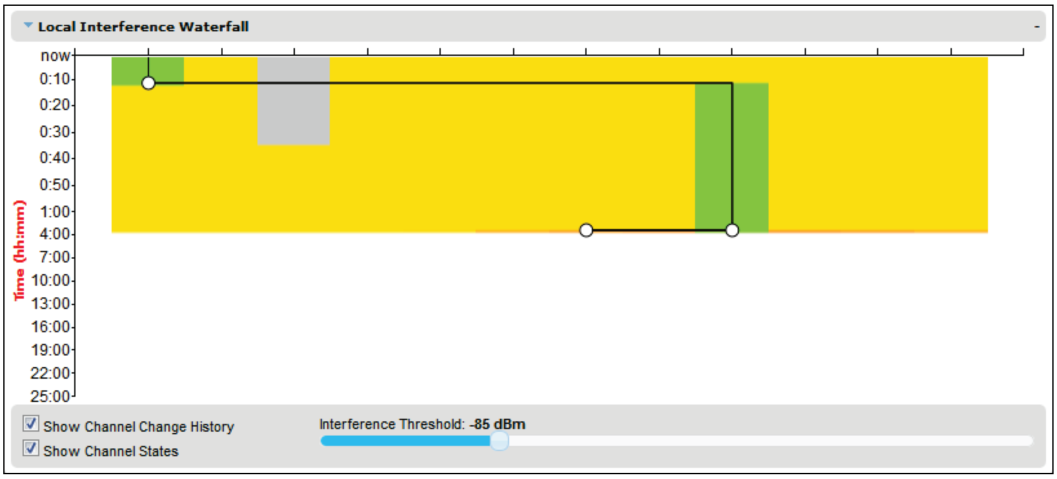
Figure 229 Spectrum Expert, Interference Waterfall with active channel history



Viewing the channel states

To display the Channel States, tick the Show Channel State control right below the Interference Waterfall plot. Figure 230 shows an example of the Interference Waterfall when the Channel States are displayed. The colors used are defined in Channel states on page 7-36.

Figure 230 Spectrum Expert page, Interference Waterfall plot with channel states



Interpreting the histogram plot

The histogram plot indicates the percentage of the measurements in the selected measurement period where the interference level for the selected channel is at a given level (Figure 231).

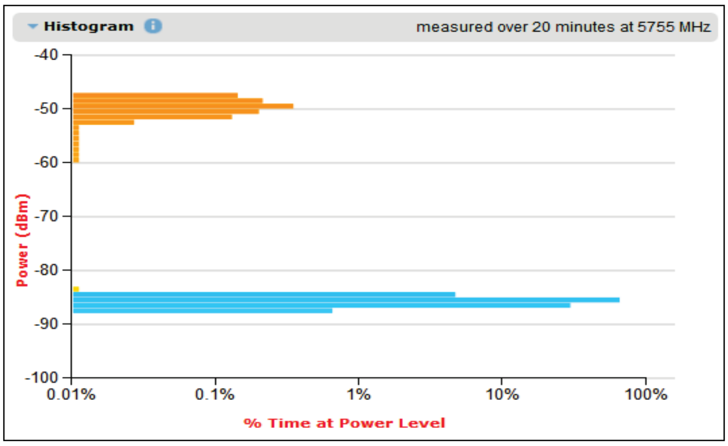
The channel and measurement period are selected as described in Selecting a Channel and a Time period on page 7-43 The combined selection is indicated graphically by a pair of brackets in the Waterfall plot, and in text form on the top right of the Histogram plot, as shown in Figure 230.

The X-axis corresponds to a percentage of the measurements in the measurement period on a logarithmic scale.

The Y-axis corresponds to actual interference level in dBm.

The bar for each each power level is of the same color as in the Interference Waterfall plot.

Figure 231 Spectrum Expert page, histogram plot



Spectrum Expert example

In this example from a real-world link, shown in Figure 232, the channel at 5740 MHz has been selected for analysis.

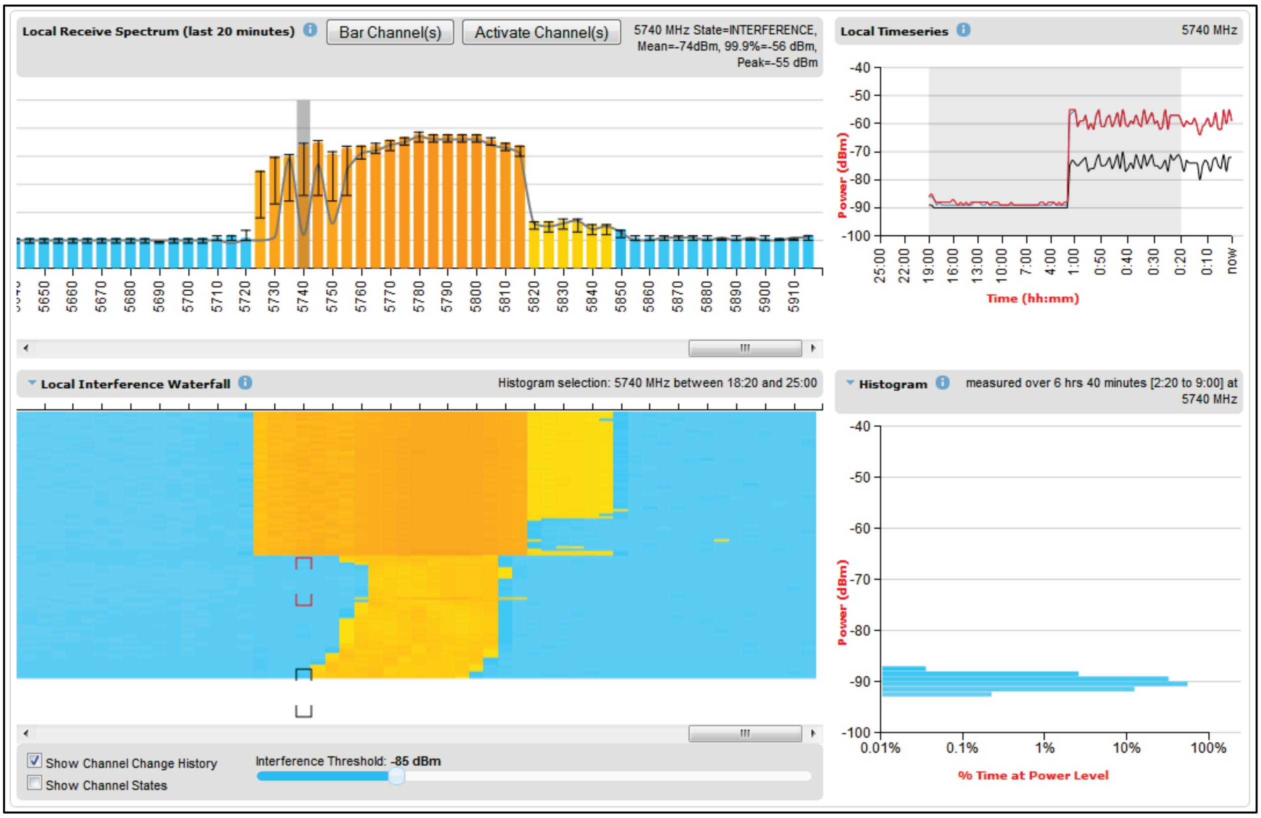
The Spectrum display is based in the most recent 20 minute period. The height of the colored bar in the selected channel shows that the 99.9th percentile of the interference is at about -66 dBm. The orange color of the bar is a reminder that this level is above the interference threshold of -85 dBm.

The upper bar of the “I” bar indicates the peak level of the interference. The lower bar of the “I” bar indicates the mean level of the interference. The height of the “I” bar represents the peak to mean ratio. In this channel, the peak to mean ratio is about 15 dB.

The red and black traces in the Timeseries plot show that the peak and mean interference levels have been maintained at approximately constant levels over a period of about two hours. Before that period, the interference level was considerably lower, at about -90 dBm.

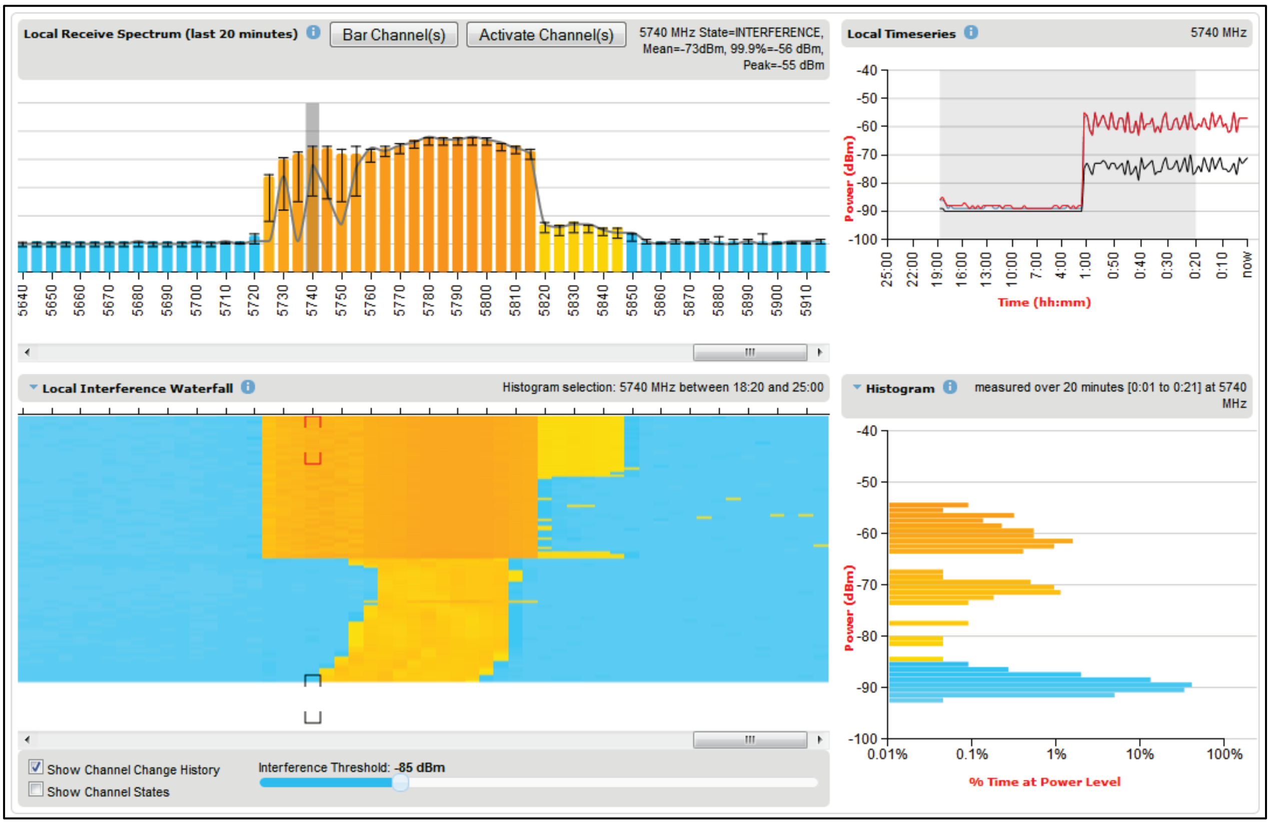
In the Interference Waterfall plot, the selected time period is from 2 hours 20 minutes to 9 hours ago. The plot shows that interference occurred suddenly, across a broad band of channels, shortly after the selected period, or about two hours ago, and that it has been maintained at an approximately constant level since then. The Histogram plot shows that, prior to the onset of interference, the interference level was consistently close to -90 dBm, corresponding to the earlier part of the Timeseries plot.

Figure 232 Spectrum Expert, example 1



In Figure 233, the time period for the Histogram plot has been set to the most recent 20 minutes. The histogram shows that interference levels are distributed over the range of approximately -74 dBm to approximately -54 dBm.

Figure 233 Spectrum Expert, example 2



The interference observed in Figure 233 for the channel at 5740 MHz during the recent two hour period is not compatible with satisfactory operation a PTP 700 link.

The situation is, if anything, even worse in the channel at 5780 MHz, as shown in Figure 234, where the interference level was historically worse, and in the recent period was consistently in the range -52 dBm to -58 dBm.

Figure 235 shows the recent history of the channel at 5835 MHz. In this case, the peak interference is less than -80 dBm. This channel is likely to support satisfactory operation at a receive signal level of -60 dBm or greater.

Figure 234 Spectrum Expert, example 3

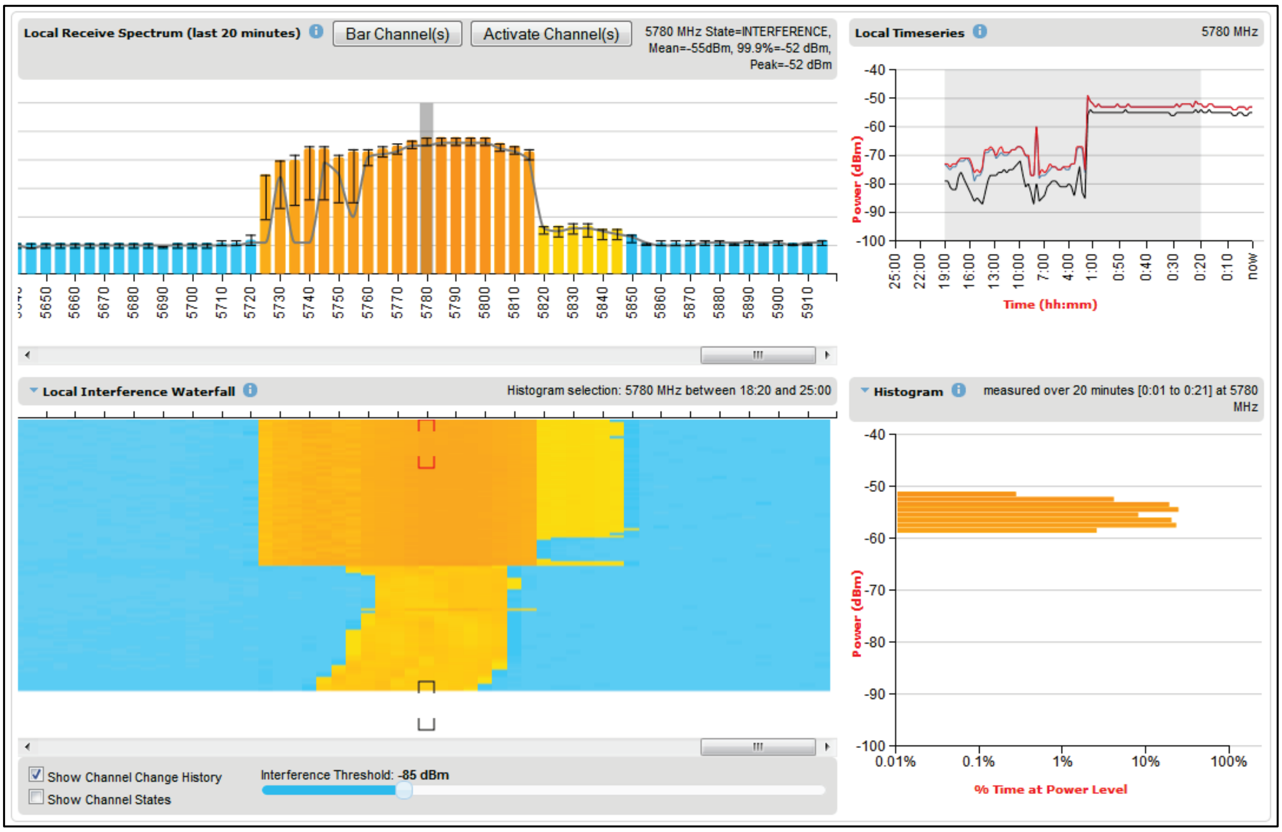
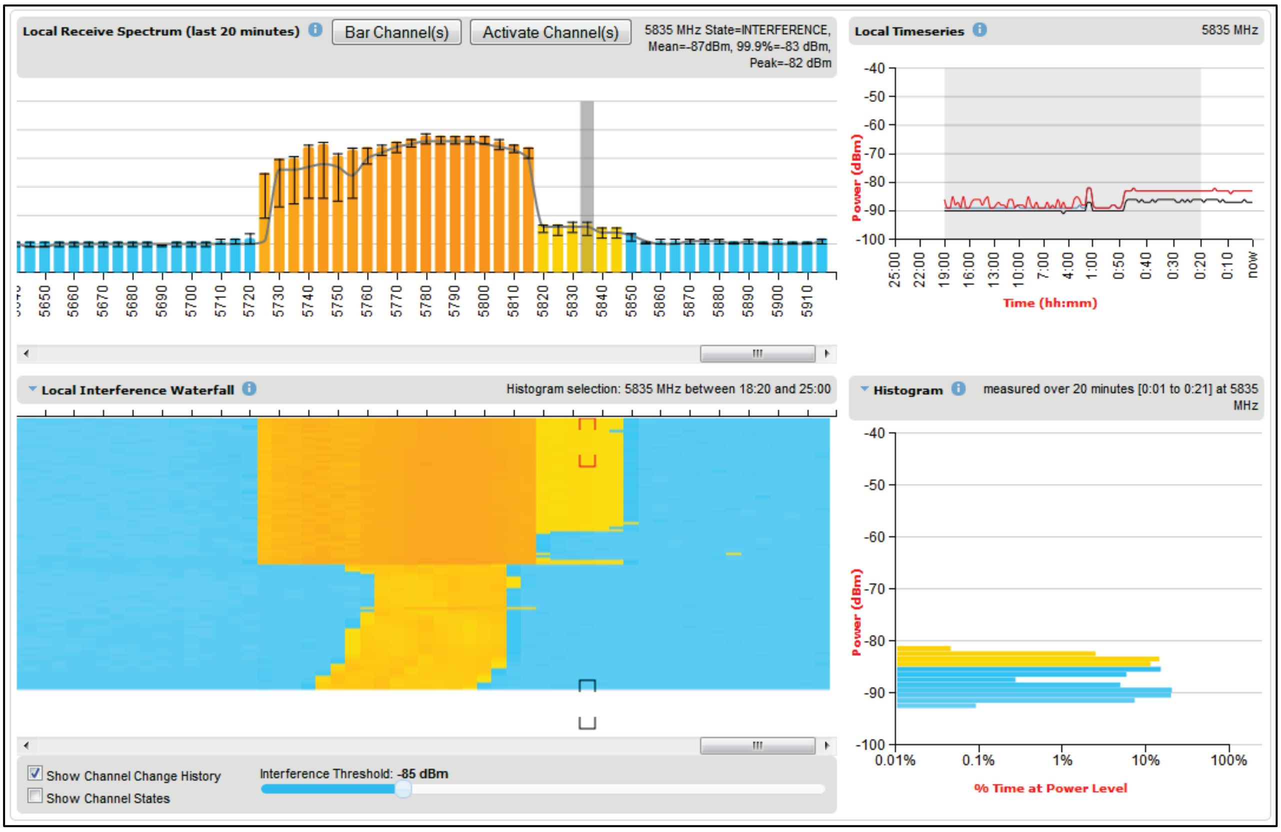


Figure 235 Spectrum Expert, example 4



Managing security

This section describes the following procedures:

- Exiting FIPS 140-2 approved mode
- Zeroising critical security parameters

Other security configuration procedures are described in Security menu on page 6-101.

Exiting FIPS 140-2 approved mode

To exit from the FIPS 140-2 approved mode, install standard (non-FIPS) PTP 700 software.

Note The critical security parameters (CSPs) are zeroized when the unit exits from the FIPS 140-2 approved mode.

Zeroizing critical security parameters

Use this procedure to zeroize Critical security parameters (CSPs) 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.
- Private key for the User-supplied Device Certificate.
- User account passwords for the web-based interface.
- SNTP server keys for SHA1
- SNMPv3 USM authentication keys
- SNMPv3 USM privacy keys

Procedure:

- On the Security menu, click Zeroize CSPs.
- Click Select Zeroize CSPs and Reboot Wireless Unit.
- Confirm the reboot.

Note Alternatively, select the Zeroize CSPs option in Recovery mode as described in Zeroize Critical Security Parameters on page 7-79

System statistics

This section describes how to use the system statistics pages to manage the performance of the PTP 700 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 236 and Figure 237) contains eight diagnostic attributes that are presented as arrays of four elements (Table 187).

Figure 236 System Histograms section of the System Statistics page (PTP Topology)

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	

Reset System Histogram Measurement Period

Figure 237 System Histograms section of the System Statistics page (HCMP Topology, Wireless Interface Selector set to "All Wireless Interfaces")

System Statistics

Attributes	Value	Units
Wireless Interface Selector	All Wireless Interfaces	

Attributes	Value	Value	Value	Units
Remote Unit Name	Slave_58_01_D5	Not Available	Not Available	
System Histograms				
Transmit Power	23.0, 23.0	28.0, 28.0	0.0, 0.0	dBm
Receive Power	-46.2, -46.2	-109.9, -110.0	0.0, 0.0	dBm
Vector Error	-35.5, -33.7	0.0, 0.0	0.0, 0.0	dB
Link Loss	67.2, 67.2	0.0, 0.0	0.0, 0.0	dB
Signal Strength Ratio	3.1, 3.2	0.0, 0.0	0.0, 0.0	dB
Transmit Data Rate	57.89, 57.89	0.00, 0.00	0.00, 0.00	Mbps
Receive Data Rate	2.78, 2.78	0.00, 0.00	0.00, 0.00	Mbps
Aggregate Data Rate	60.67, 60.67	0.00, 0.00	0.00, 0.00	Mbps
Histogram Measurement Period	01:00:00			
Reset System Histogram Measurement Period				

Attributes	Value	Units
Elapsed Time Indicator	01:21:18	
Statistics Page Refresh Period	3600	seconds
Submit Page Refresh Period		

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.

Use the Diagnostics Plotter page on page 7-70 to plot these attributes against time. Use the Generate Downloadable Diagnostics page on page 7-71 to extract historical data for these attributes to a CSV file.

Procedure:

- To reset and restart measurement, click **Reset System Histograms and Measurement Period**.

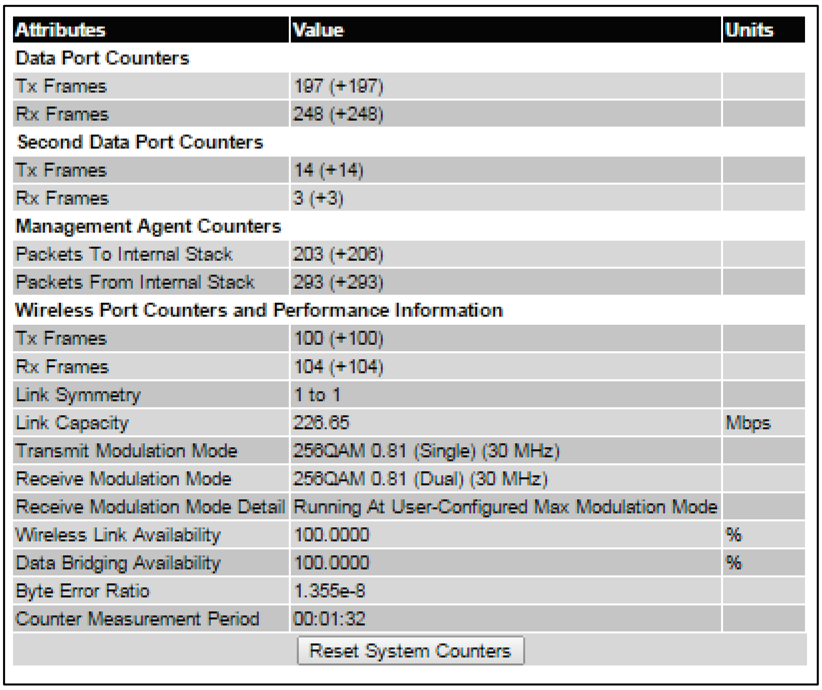
Table 187 System Histogram attributes in the System Statistics page

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.
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.

Wireless Port Counters (PTP topology)

The System Counters section of the System Statistics page (Figure 238) contains Data Port Counters (Table 188), Management Agent Counters (Table 189) and Wireless Port Counters and Performance Information (Table 190).

Figure 238 System Counters section of the System Statistics page



Attributes	Value	Units
Data Port Counters		
Tx Frames	197 (+197)	
Rx Frames	248 (+248)	
Second Data Port Counters		
Tx Frames	14 (+14)	
Rx Frames	3 (+3)	
Management Agent Counters		
Packets To Internal Stack	203 (+206)	
Packets From Internal Stack	293 (+293)	
Wireless Port Counters and Performance Information		
Tx Frames	100 (+100)	
Rx Frames	104 (+104)	
Link Symmetry	1 to 1	
Link Capacity	226.65	Mbps
Transmit Modulation Mode	256QAM 0.81 (Single) (30 MHz)	
Receive Modulation Mode	256QAM 0.81 (Dual) (30 MHz)	
Receive Modulation Mode Detail	Running At User-Configured Max Modulation Mode	
Wireless Link Availability	100.0000	%
Data Bridging Availability	100.0000	%
Byte Error Ratio	1.355e-8	
Counter Measurement Period	00:01:32	
	Reset System Counters	

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 188 Data Port Counters

Attribute	Meaning
Tx Frames	The total number of good frames the bridge has sent for transmission through the port selected for Data Service
Rx Frames	The total number of good frames the bridge has received through the port selected for Data Service

Table 189 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 190 Wireless Port Counters and Performance Information

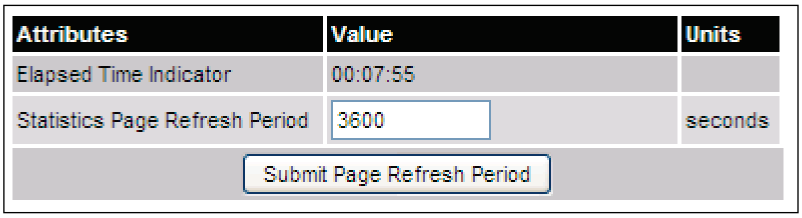
Attribute	Meaning
Tx Frames	Total number of good frames on the Data path, the bridge has sent for transmission through the wireless interface.
Rx Frames	Total number of good frames on the Data path, the bridge has received from the wireless interface.
Tx Frame Management	Total number of good managment frames, the bridge has sent for transmission through 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.
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 172.
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.

Attribute	Meaning
Counter Measurement Period	The time over which the system counters were collected.

Other attributes

The bottom section of the System Statistics page (Figure 239) contains two attributes (Table 191).

Figure 239 Other attributes section of the System Statistics page



Procedure:

- After updating the Statistics Page Refresh Period field, click **Submit Page Refresh Period**.

Table 191 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

PTP topology

Menu option: **System > Statistics > Wireless Port Counters** (Figure 240).

Use this page to check the Ethernet performance of the wireless bridge.

Figure 240 Wireless Port Counters page (PTP topology)

Wireless Port Counters

Attributes	Value	Units	Attributes	Value	Units
Tx Frames	132 (+32)		Rx Frames	491 (+387)	
			Rx Frames With Crc Error	0 (+0)	
Tx Frames Q0	0 (+0)		Rx Frames Q0	0 (+0)	
Tx Frames Q1	125 (+125)		Rx Frames Q1	160 (+160)	
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	7 (+7)		Rx Frames Q7	331 (+331)	
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)				
Tx Frames Second Data	3 (+3)		Rx Frames Second Data	198 (+198)	
Tx Drops Second Data	0 (+0)				

Attributes	Value	Units	Attributes	Value	Units
Counter Page Refresh Period	3600	seconds	Counter Measurement Period	00:05:36	
Submit Page Refresh Period			Reset System Counters		

Procedure:

- Review the attributes (Table 192).
- 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 192 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.

HCMP topology

Menu option: **System > Statistics > Wireless Port Counters** (Figure 241 to Figure 243).

Use this page to check the Ethernet performance of the wireless bridge.

Figure 241 Wireless Port Counters page (Master, HCMP topology, Wireless Interface Selector set to a single link)

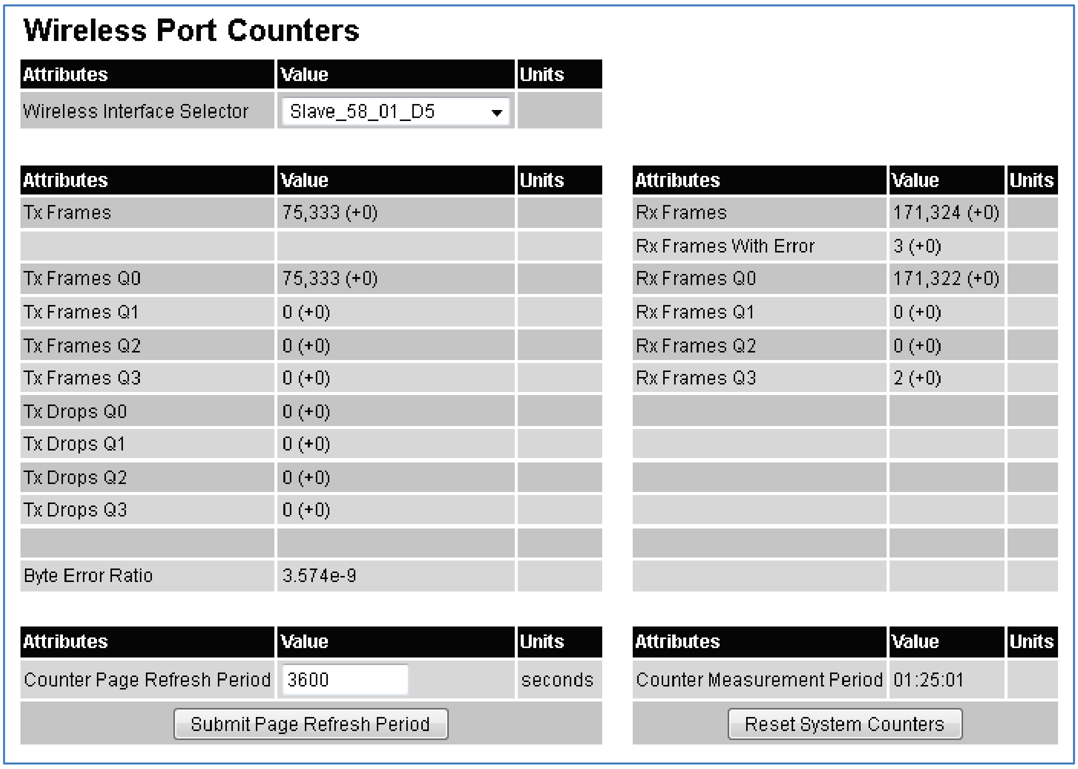


Figure 242 Wireless Port Counters page (Master, HCMP topology, Wireless Interface Selector set to All Wireless Links)

Wireless Port Counters

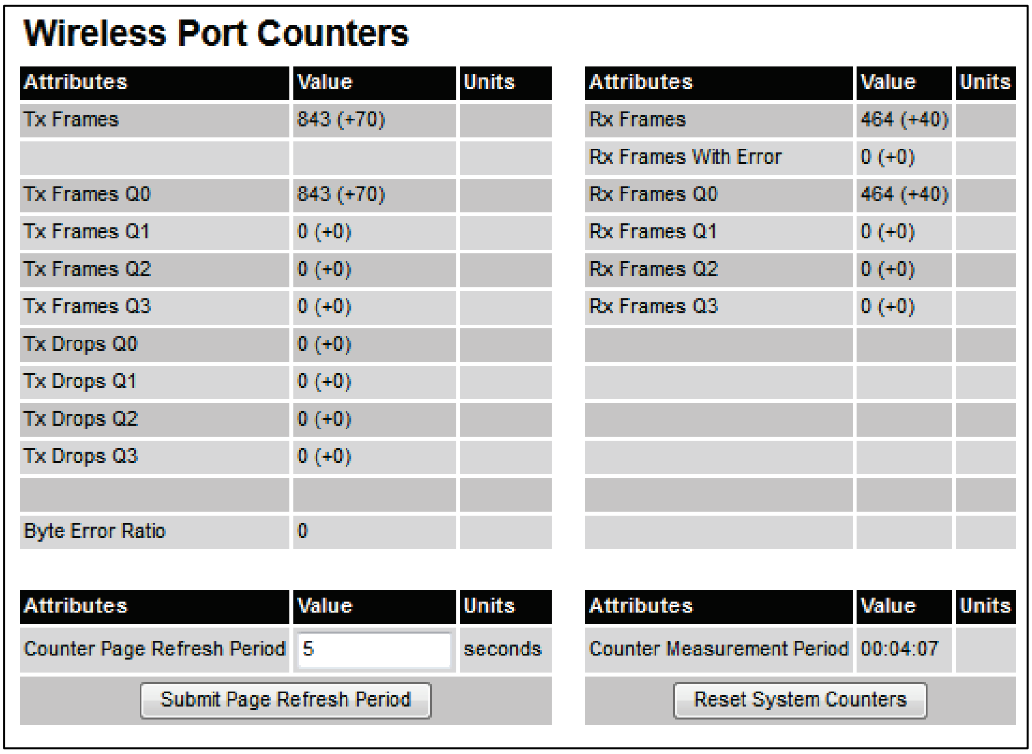
Attributes	Value	Units
Wireless Interface Selector	All Wireless Interfaces	

Attributes	Value	Value	Value	Units
Remote Unit Name	Slave_58_01_D5	Not Available	Not Available	
Tx Frames	75,333 (+0)	0 (+0)	0 (+0)	
Rx Frames	171,324 (+0)	0 (+0)	0 (+0)	
Rx Frames With Error	3 (+0)	0 (+0)	0 (+0)	
Tx Frames Q0	75,333 (+0)	0 (+0)	0 (+0)	
Tx Frames Q1	0 (+0)	0 (+0)	0 (+0)	
Tx Frames Q2	0 (+0)	0 (+0)	0 (+0)	
Tx Frames Q3	0 (+0)	0 (+0)	0 (+0)	
Tx Drops Q0	0 (+0)	0 (+0)	0 (+0)	
Tx Drops Q1	0 (+0)	0 (+0)	0 (+0)	
Tx Drops Q2	0 (+0)	0 (+0)	0 (+0)	
Tx Drops Q3	0 (+0)	0 (+0)	0 (+0)	
Rx Frames Q0	171,322 (+0)	0 (+0)	0 (+0)	
Rx Frames Q1	0 (+0)	0 (+0)	0 (+0)	
Rx Frames Q2	0 (+0)	0 (+0)	0 (+0)	
Rx Frames Q3	2 (+0)	0 (+0)	0 (+0)	
Byte Error Ratio	3.533e-9	0	0	

Attributes	Value	Units
Counter Page Refresh Period	3600	seconds
Counter Measurement Period	01:25:58	

Submit Page Refresh Period | Reset System Counters

Figure 243 Wireless Port Counters page (Slave, HCMP topology)



Wireless Port Counters

Attributes	Value	Units	Attributes	Value	Units
Tx Frames	843 (+70)		Rx Frames	464 (+40)	
			Rx Frames With Error	0 (+0)	
Tx Frames Q0	843 (+70)		Rx Frames Q0	464 (+40)	
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 Drops Q0	0 (+0)				
Tx Drops Q1	0 (+0)				
Tx Drops Q2	0 (+0)				
Tx Drops Q3	0 (+0)				
Byte Error Ratio	0				

Attributes	Value	Units	Attributes	Value	Units
Counter Page Refresh Period	5	seconds	Counter Measurement Period	00:04:07	
Submit Page Refresh Period			Reset System Counters		

Procedure:

- Only on a device configured as in HCMP topology as a Master, select one interface using the Wireless Interface Selector. Note the Remote MAC Address indicates the MAC address of the unit currently connected, if any, to the selected wireless interface.
- Review the attributes (Table 193).
- 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 193 Wireless Port Counters attributes, HCMP mode

Attribute	Meaning
Tx/Rx Frames	Number of frames transmitted and received over the wireless link.
Rx Frames With Error	Number of received frames with errors.
Tx/Rx Frames Q0...Q3	Number of transmitted and received frames for each Traffic Class.
Tx Drops Q0...Q3	Number of frames discarded for each Traffic Class by taildrop.

Main Port Counters page (PTP topology only)

Menu option: **System > Statistics > Main Port Counters** (Figure 244). 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 244 Main Port Counters page (when main port is bridging traffic)

Main Port Counters

Attributes	Value	Units	Attributes	Value	Units
Tx Octets	684,506 (+684,506)		Rx Octets	398,584 (+398,584)	
Tx Frames	6,177 (+2)		Rx Frames	6,044 (+2)	
Tx Drops	0 (+0)		Rx Frames With Crc Error	0 (+0)	
Tx Broadcasts	5,368 (+5,368)		Rx Broadcasts	5,554 (+5,554)	
Tx IEEE1588 Event Frames	0 (+0)		Rx IEEE1588 Event Frames	0 (+0)	
			Rx Frames Undersize	0 (+0)	
Tx Frames 64 Bytes	5,912 (+5,912)		Rx Frames 64 Bytes	5,968 (+5,968)	
Tx Frames 65 To 127 Bytes	41 (+41)		Rx Frames 65 To 127 Bytes	57 (+57)	
Tx Frames 128 To 255 Bytes	17 (+17)		Rx Frames 128 To 255 Bytes	2 (+2)	
Tx Frames 256 To 511 Bytes	6 (+6)		Rx Frames 256 To 511 Bytes	11 (+11)	
Tx Frames 512 To 1023 Bytes	4 (+4)		Rx Frames 512 To 1023 Bytes	2 (+2)	
Tx Frames 1024 To 1600 Bytes	197 (+197)		Rx Frames 1024 To 1600 Bytes	4 (+4)	
Tx Frames 1601 To Max Bytes	0 (+0)		Rx Frames 1601 To Max Bytes	0 (+0)	
			Rx Frames Oversize	0 (+0)	
			Rx Pause Frames	0 (+0)	

Attributes	Value	Units	Attributes	Value	Units
Counter Page Refresh Period	3600	seconds	Counter Measurement Period	00:08:09	
Submit Page Refresh Period			Reset System Counters		

Procedure:

- Review the attributes (Table 194).
- 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 194 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.
Tx/Rx IEEE1588 Event Frames	Only displayed when IEEE 1588 Transparent Clock is enabled.

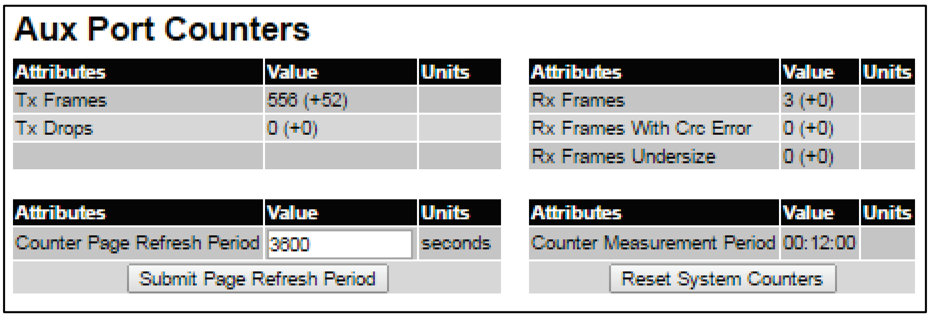
Attribute	Meaning
	Total number of transmitted or received IEEE 1588 Event frames
Rx Frames Undersize	Total number of frames received that are less than 64 bytes.
Tx/Rx Frames 64 Bytes	Total number 64 byte frames transmitted and received.
Tx/Rx Frames xxxx to yyyy Bytes	Total number of frames transmitted 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 (PTP topology only)

Menu option: System > Statistics > **Aux Port Counters** (Figure 245).

Use this page to check the Ethernet performance of the Aux port.

Figure 245 Aux Port Counters page (when Aux port is is allocated to the Local Management Service)



Procedure:

- Review the attributes (Table 195).
- 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 195 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.

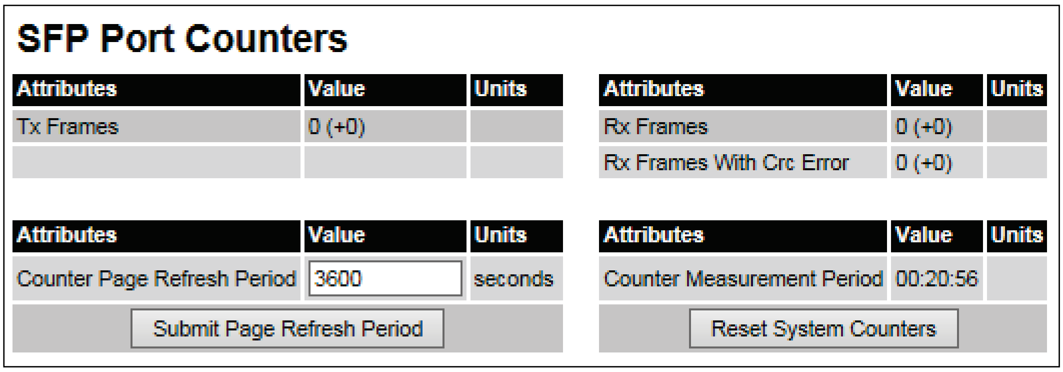
Attribute	Meaning
Rx Frames With Crc Error	Total number of received frames with CRC errors.
Tx Drops	Number of frames dropped due to excessive collision, late collision or frame ageing
Rx Frames Undersize	Number of short frames (<64 Bytes) with or without a valid CRC

SFP Port Counters page (PTP topology only)

Menu option: System > Statistics > **SFP Port Counters** (Figure 246).

Use this page to check the Ethernet performance of the SFP port.

Figure 246 SFP Port Counters page (when SFP port is allocated to the Local Management Service)



Procedure:

- Update the attributes (Table 196).
- 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 196 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.

Ethernet Port Counters page (HCMP topology only)

Menu option: **System > Statistics > Ethernet Port Counters** (Figure 247). Use this page to check the performance of all Ethernet. The displayed counters vary depending on which port is being used to bridge the traffic.

Figure 247 Ethernet Port Counters page (HCMP topology)

Ethernet Port Counters

Main Port Counters

Attributes	Value	Units	Attributes	Value	Units
Tx Octets	3,465,824 (+0)		Rx Octets	113,761 (+0)	
Tx Frames	2,638 (+0)		Rx Frames	1,464 (+0)	
Tx Broadcasts	0 (+0)		Rx Frames With Error	0 (+0)	
			Rx Broadcasts	0 (+0)	
			Rx Frames Undersize	0 (+0)	
			Rx Frames Oversize	0 (+0)	

Aux Port Counters

Attributes	Value	Units	Attributes	Value	Units
Tx Octets	0 (+0)		Rx Octets	0 (+0)	
Tx Frames	0 (+0)		Rx Frames	0 (+0)	
Tx Broadcasts	0 (+0)		Rx Frames With Error	0 (+0)	
			Rx Broadcasts	0 (+0)	
			Rx Frames Undersize	0 (+0)	
			Rx Frames Oversize	0 (+0)	

SFP Port Counters

Attributes	Value	Units	Attributes	Value	Units
Tx Octets	0 (+0)		Rx Octets	0 (+0)	
Tx Frames	0 (+0)		Rx Frames	0 (+0)	
Tx Broadcasts	0 (+0)		Rx Frames With Error	0 (+0)	
			Rx Broadcasts	0 (+0)	
			Rx Frames Undersize	0 (+0)	
			Rx Frames Oversize	0 (+0)	

Attributes	Value	Units	Attributes	Value	Units
Counter Page Refresh Period	5	seconds	Counter Measurement Period	01:52:50	
Submit Page Refresh Period			Reset System Counters		

Procedure:

- Review the attributes (Table 197).
- 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**.

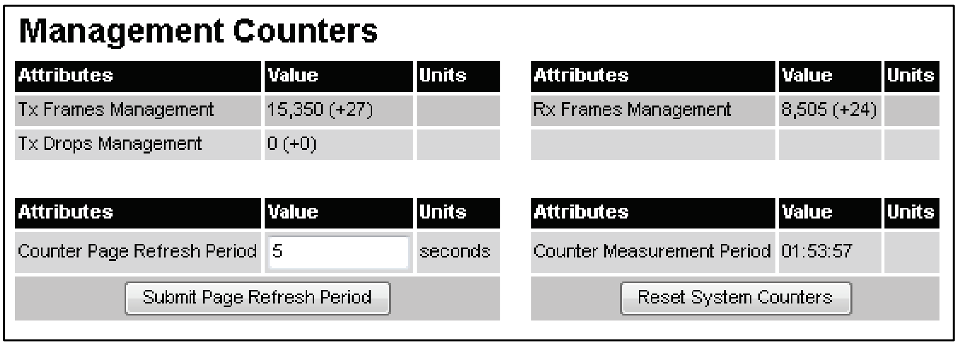
Table 197 Ethernet Port Counters attributes (HCMP topology)

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.
Rx Frames With 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.
Rx Frames Oversize	Total number of frames received that are greater than the maximum number of bytes.

Management Counters page (HCMP topology only)

Menu option: **System** > **Statistics** > **Management Counters** (Figure 248). Use this page to check the performance of all Ethernet. The displayed counters vary depending on which port is being used to bridge the traffic.

Figure 248 Management Counters page (HCMP topology)



Procedure:

- Review the attributes (Table 198).
- 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 198 Management Counters attributes (HCMP topology)

Attribute	Meaning
Tx Frames Management	Total number of frames transmitted over the management interface.
Tx Drops Management	Total number of transmit frames dropped over the management interface.

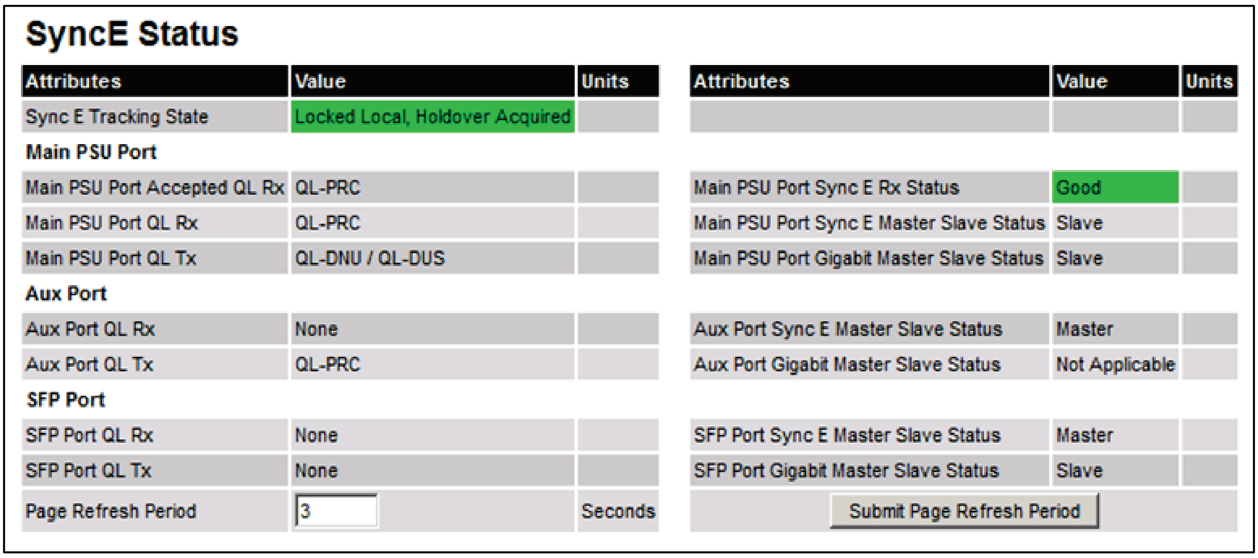
Attribute	Meaning
Rx Frames Management	Total number of frames received over the management interface.

SyncE Status page

Menu option: System > Statistics > **SyncE Status**

Use this page to monitor the state of the Synchronous Ethernet function.

Figure 249 SyncE Status page



Procedure:

- Review the attributes
- To change the refresh period, update the Page Refresh Period attribute and click **Submit Page Refresh Period**

Table 199 Sync E Status attributes

Attribute	Meaning
Sync E Tracking State	The state of the Synchronous Ethernet state machine. See Table 200 for further details.
Main PSU Port Accepted QL Rx	The "accepted" QL received by the Main PSU Port. This should be the same as Main PSU Port QL Rx, unless: • an "Overwrite" has been configured • the system is starting up or recovering from an exception
Main PSU Port QL Rx	The QL currently being received at the Main PSU Port
Main PSU Port QL Tx	The QL currently being transmitted at the Main PSU Port

Attribute	Meaning
Main PSU Port SyncE Rx Status	The overall status of the incoming synchronous Ethernet signal on the Main PSU port. This port is available as a valid synchronization source if the status is Good. The port may potentially be a valid source in the near future if the status is Wait-to-Restore.
Main PSU Port Sync E Master Slave Status	This attribute indicates if the Main PSU Port is operating as a Synchronous Ethernet master (providing a source of timing for downstream devices) or slave (receiving a source of timing from an upstream device).
Main PSU Port Gigabit Master Slave Status	This attribute indicates if the Main PSU Port's Gigabit Ethernet physical interface is operating as a master (generating a clock) or slave (locking to a clock generated at the other end of the Ethernet link).
Aux Port QL Rx	The QL currently being received on the Aux Port
Aux Port Accepted QL Rx	The "accepted" QL received by the Aux Port. This should be the same as Aux Port QL Rx, unless the system is starting up or recovering from an exception
Aux Port QL Tx	The QL currently being transmitted at the Aux Port
Aux Port Sync E Master Slave Status	The Aux Port operates as a Synchronous Ethernet master (providing a source of timing for downstream devices).
Aux Port Gigabit Master Slave Status	This attribute indicates if the Aux Port's Gigabit Ethernet physical interface is operating as a master (generating a clock) or slave (locking to a clock generated at the other end of the Ethernet link).
SFP Port QL Rx	The QL currently being received on the SFP Port
SFP Port Accepted QL Rx	The "accepted" QL received by the SFP Port. This should be the same as SFP Port QL Rx, unless: • an "Overwrite" has been configured • the system is starting up or recovering from an exception The ODU synchronizes to the best frequency reference as determined by the Port Accepted QL Rx values at the nominated Sync E Slave Ports of local and remote ODUs.
SFP Port QL Tx	The QL currently being transmitted at the SFP Port
SFP Port Sync E Master Slave Status	This attribute indicates if the SFP Port is operating as a Synchronous Ethernet master (providing a source of timing for downstream devices) or slave (receiving a source of timing from an upstream device).

Attribute	Meaning
SFP Port Gigabit Master Slave Status	This attribute indicates if the SFP Port's Gigabit Ethernet physical interface is operating as a master (generating a clock) or slave (locking to a clock generated at the other end of the Ethernet link). The Master Slave Status is **Not Applicable** unless a Copper SFP module is present.

The "Sync E Tracking State" attribute can take the following values:

Table 200 Sync E Tracking State

Value	Meaning
Disabled	The synchronous Ethernet feature is disabled.
Acquiring Wireless Lock	Synchronous Ethernet is not operational because real-time clocks have not completed alignment.
Free Running	Synchronous Ethernet is operational, but with no timing source or history. This is a temporary state.
Locked Local, Acquiring Holdover	Sync E tracking has locked to a synchronisation signal from a cabled Ethernet port on the local ODU. This is a temporary state until the unit has acquired holdover history.
Locked Local, Holdover Acquired	Sync E tracking has locked to a synchronisation signal from a cabled Ethernet port on the local ODU and has acquired holdover history.
Holdover	There is currently no source for the tracking loop, but previously the tracking loop was in a Locked, Holdover Acquired state. The system is using the last known good frequency.
Locked Remote, Acquiring Holdover	The tracking loop has locked to a synchronisation signal from the remote ODU. This is a temporary state until the unit has acquired holdover history.
Locked Remote, Holdover Acquired	The tracking loop has locked to a synchronisation signal form the remote ODU and has acquired holdover history.

In normal operation, with the Synchronous Ethernet feature enabled and a valid timing source present, one end of the link should be in the "Locked Local, Holdover Acquired State", the other end should be in the "Locked Remote, Holdover Acquired" state.

The Sync E Tracking State attribute remains in the Acquiring Wireless Lock state for a period of time after the wireless link has established whilst the two ODUs establish precise synchronization. The duration of this period depends on channel bandwidth, varying from less than one minute at 45 MHz, up to two minutes for 5 MHz.

Diagnostics Plotter page

Menu option: **System** > **Diagnostics Plotter** (Figure 250 and Figure 251).

Use this page to monitor the performance of an operational PTP 700 link over time.

Figure 250 Diagnostic Plotter page (PTP topology)

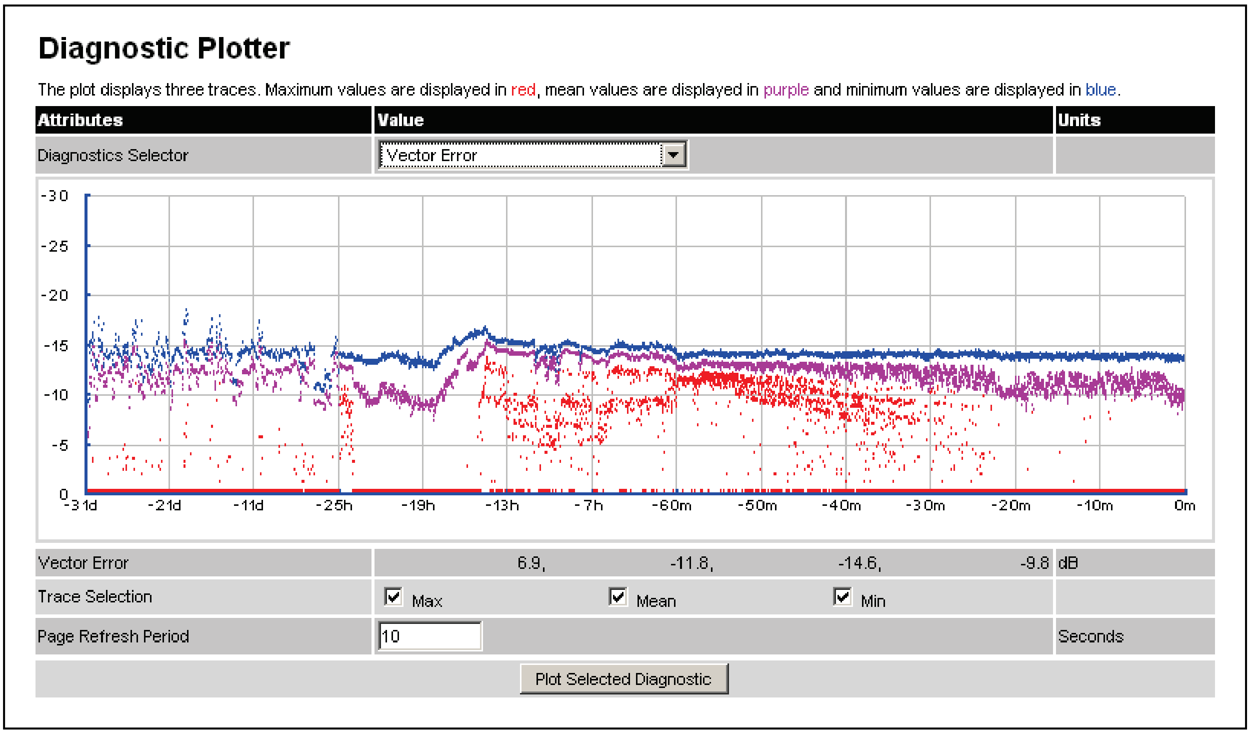
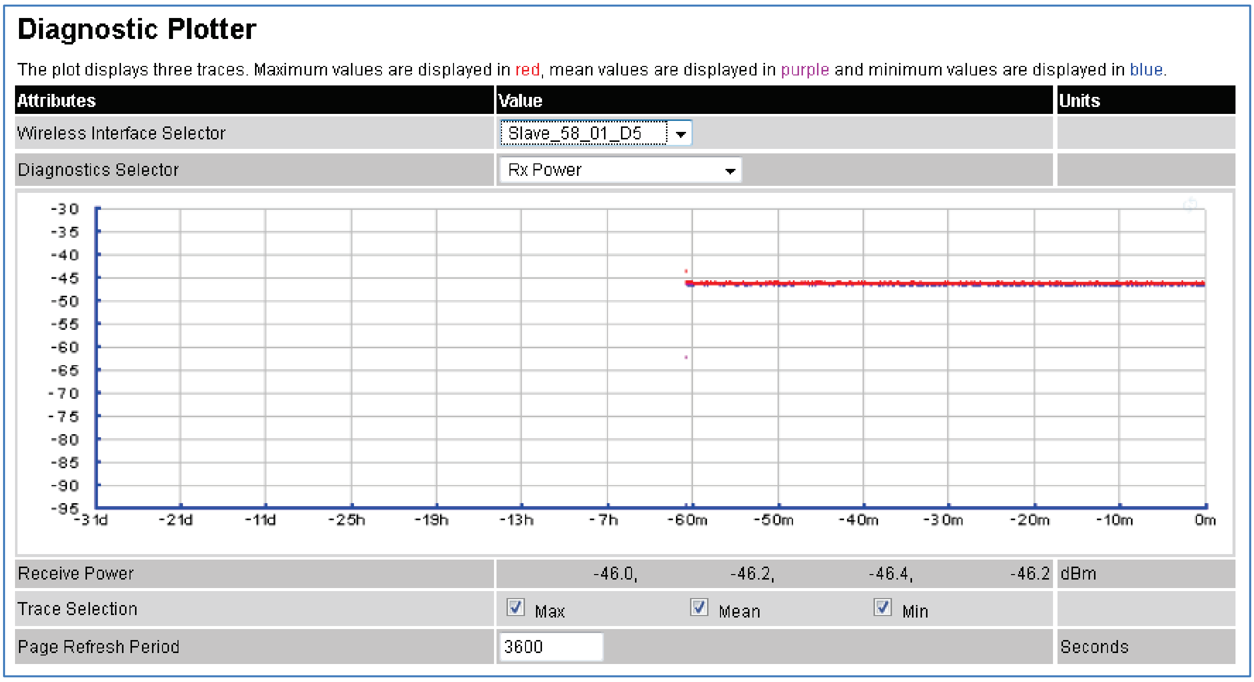


Figure 251 Diagnostic Plotter page (HCMP topology)



Procedure:

- Only on a device configured as in HCMP topology as a Master, set the Wireless Interface Selector to the Wireless Interface the diagnostic data needs to be displayed for. Note the Remote MAC Address indicated the MAC address of the unit currently connected, I any, to the selected wireless interface.
- 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 187) plus those listed in Table 201.
- 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.

Table 201 Diagnostic Plotter specific System Histogram attributes

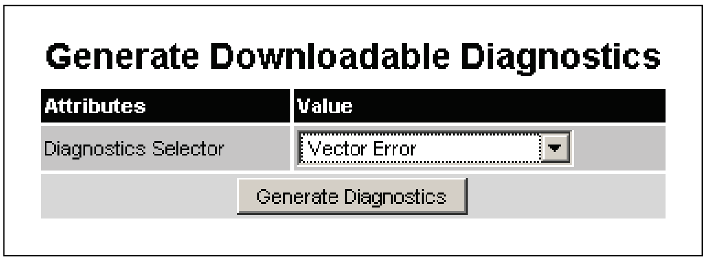
Attribute	Meaning
PCB Temperature	The temperature in degrees Celsius measured by a sensor on the printed circuit board of the ODU. The PCB temperature will normally be higher than the ambient temperature.
Tx Link Capacity Utilization	The Tx Link Capacity Utilization measures the percentage of the instantaneous transmit capacity actually uses to carry traffic. Note that this percentage is relative to the instantaneous capacity of the link in the transmit direction and that this capacity is dependent over time of the modulation the link operates in.

Generate Downloadable Diagnostics page

Menu option: **System > Diagnostics Plotter > CSV Download (**Figure 252**).**

Use this page to download diagnostics data to a CSV file.

Figure 252 Generate Downloadable Diagnostics page



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 700 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 two 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:

5 Click on the warning page image. The Recovery Option Page is displayed (Figure 253).

6 Review the Software Version and Recovery Reason (Table 202).

7 Select a recovery option (Table 203).

Figure 253 Recovery Options page

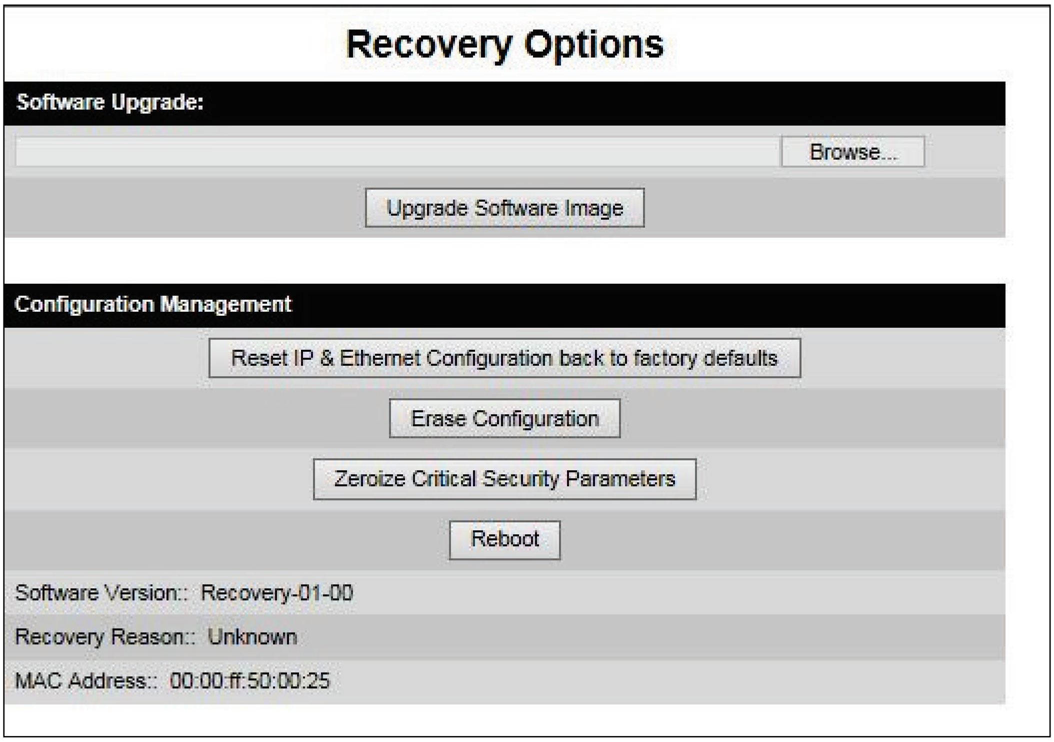


Table 202 Recovery Options attributes

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 203 Recovery Options buttons

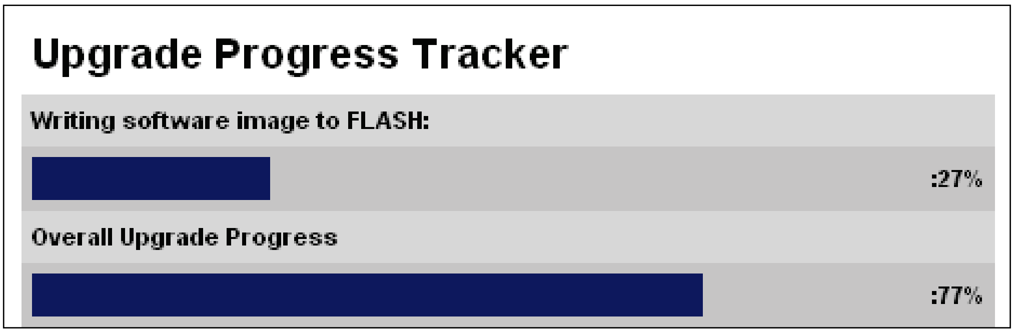
Button	Purpose
Upgrade Software Image	Use this option to restore a working software version when software corruption is suspected, or when an incorrect software image has been loaded. Refer to Upgrading software image on page 7-75.
Reset IP & Ethernet Configuration back to factory defaults	Use this option to reset the IP and Ethernet attributes to factory defaults. Refer to Resetting IP & Ethernet configuration on page 7-76.
Erase Configuration	Use this option to reset the entire configuration of the unit to factory defaults. Refer to Resetting all configuration data on page 7-78.
Zeroize Critical Security Parameters	Use this option to reset the security configuration to default values. Refer to Zeroize Critical Security Parameters on page 7-79.
Reboot	Use this option to reboot the unit. Refer to Rebooting the unit on page 7-81.

Upgrading software image

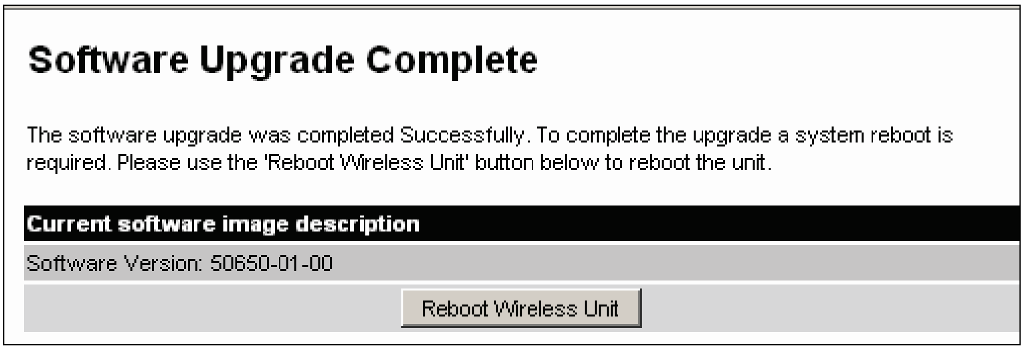
Use this option to restore a working software image from the Recovery Options page (Figure 253).

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:



4. When the Software Upgrade Complete page is displayed, check that the correct image has been downloaded:



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 8-7.

Note The unit will not upload FIPS versions of the software unless the unit has the AES encryption and FIPS licenses installed.

Note CSPs are automatically zeroized if FIPS software is loaded in a unit to replace standard (non-FIPS) software, or standard (non-FIPS) software is loaded in a unit to replace FIPS software.

Resetting IP & Ethernet configuration

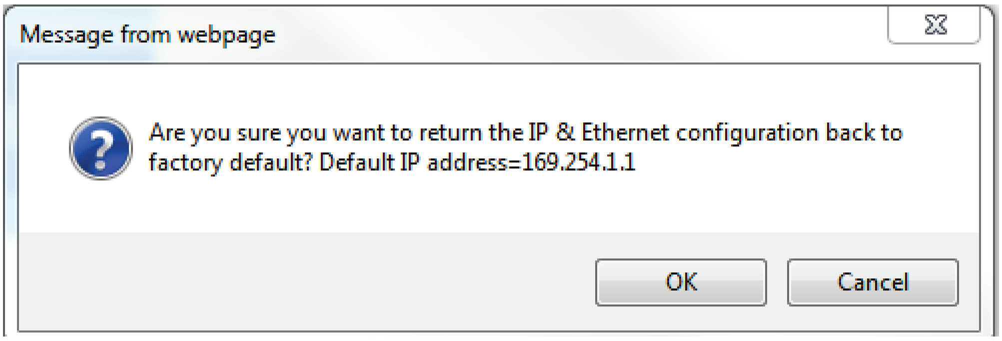
Use this option in the Recovery Options page to reset IPv4, IPv6 and Ethernet configuration to default values (Figure 253). This procedure resets the IP Version attribute to **IPv4**. It also resets the IPv6 configuration. The reset action affects the following attributes:

- IP Version
- IPv4 Address
- Subnet Mask
- Gateway IP Address
- use VLAN For Management Interfaces
- VLAN Management VID
- VLAN Management Priority
- IPv6 Address
- IPv6 Prefix Length
- IPv6 Gateway Address
- Data Service
- Management Service
- Local Management Service
- Data Port Wireless Down Alert

- Management Port Wireless Down Alert
- Main PSU Port Auto Negotiation
- Main PSU Port Auto Neg Advertisement
- Main PSU Port Auto Mdix
- Aux Port Auto Negotiation
- Aux Port Auto Neg Advertisement
- Aux Port Auto Mdix
- Aux Port Power Over Ethernet Output
- SFP Port Auto Negotiation
- SFP Port Auto Neg Advertisement
- SFP Port Auto Mdix
- Local Packet Filtering
- SNMP Access Control
- Access Control
- IP Address Label

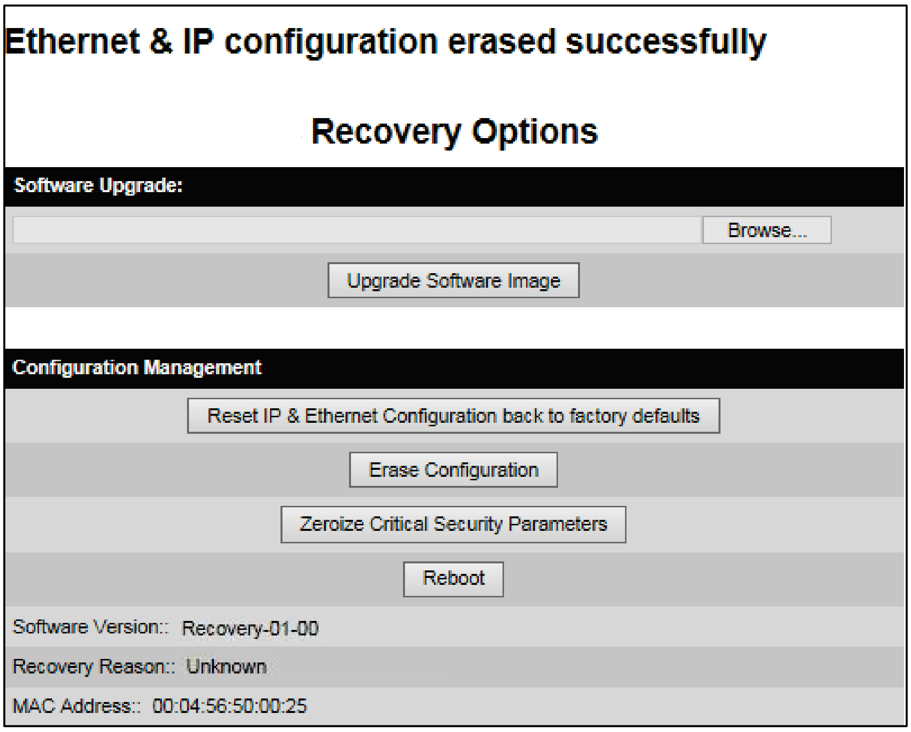
Procedure:

1 Click **Reset IP & Ethernet Configuration back to factory defaults**. The reset pop up box is displayed:



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:



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 8-7 and Cable Diagnostics on page 8-2.

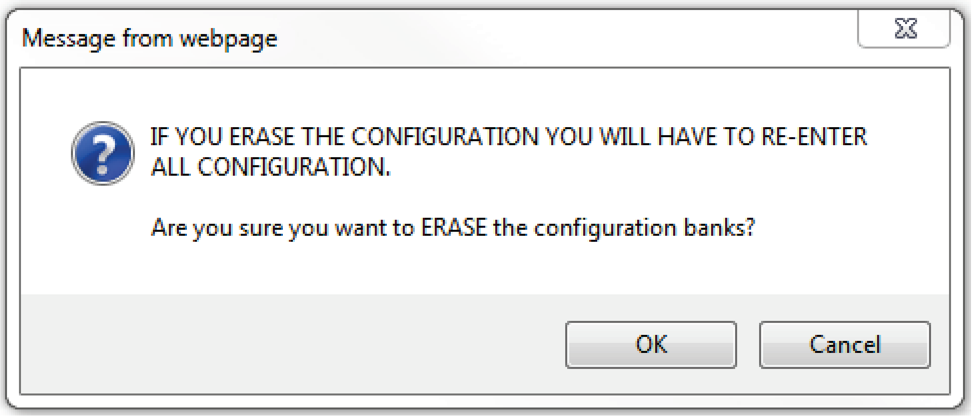
Resetting all configuration data

Note Wireless Topology is not reset by this procedure.

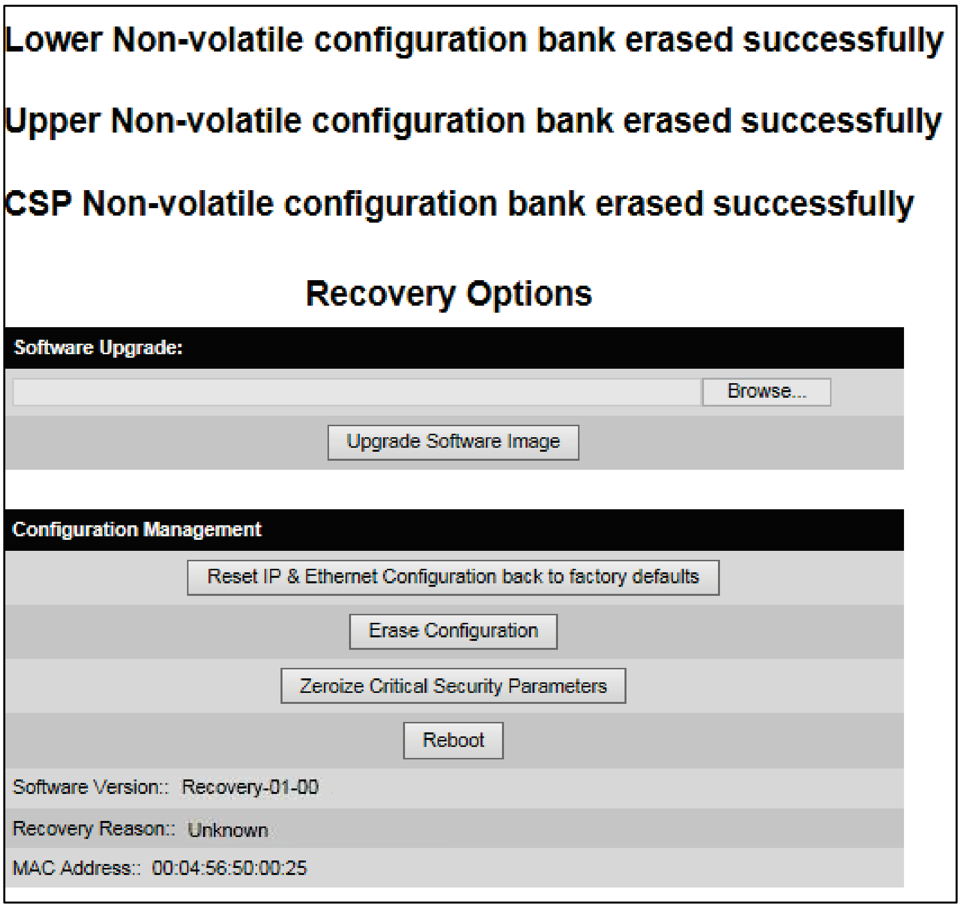
Use this option in the Recovery Options page to reset the entire configuration of the unit (including IP, Ethernet and CSPs) to default values (Figure 253).

Procedure:

1 Click **Erase Configuration**. The erase pop up box is displayed:



2 Click **OK**. The erase confirmation page is displayed:



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 reset to default values. If the unit fails to start up, refer to Testing link end hardware on page 8-7 and Cable Diagnostics on page 8-2.

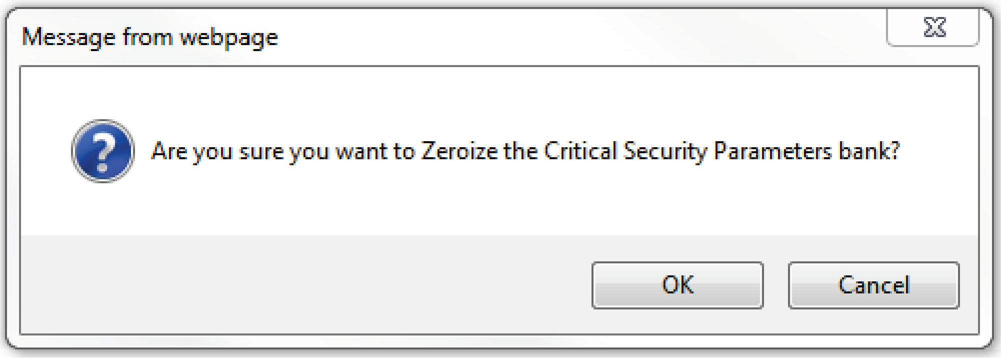
Zeroize Critical Security Parameters

Use this option in the Recovery Options page to reset the security configuration of the unit to default values (Figure 253). This action includes the following attributes:

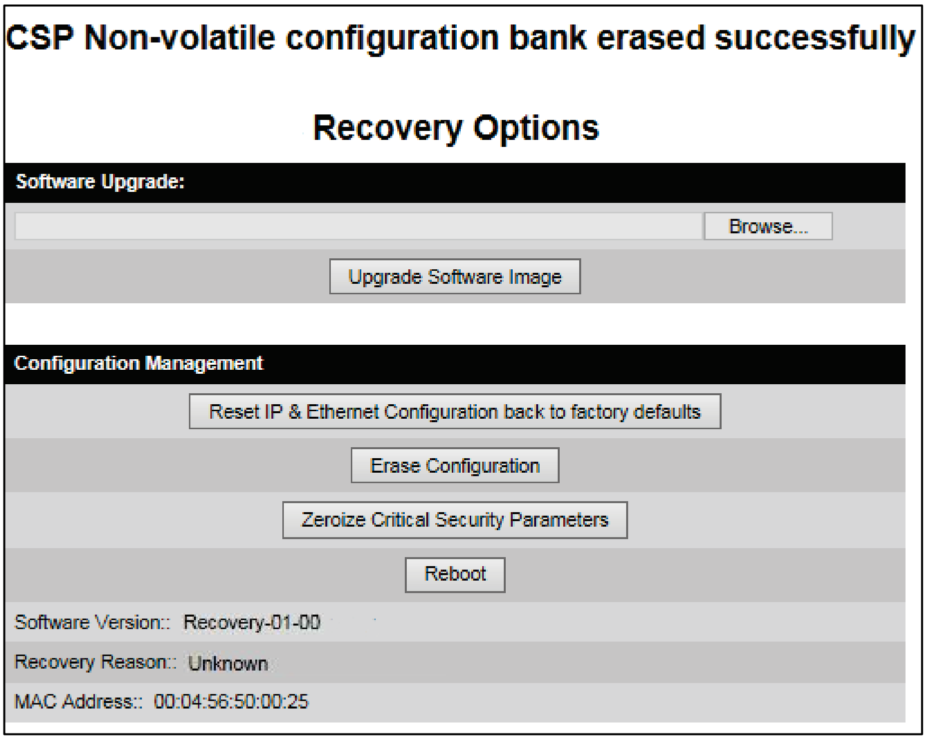
- Key of Keys
- Local User Accounts Names, Roles and Passwords
- Encryption Algorithm
- Wireless Encryption Key
- HTTPS Private Key
- HTTPS Public Key Certificate
- Random Number Generator Entropy
- User-supplied Device Private Key
- HTTP Access Enabled
- HTTP Port Number
- SNTP server keys for SHA1
- SNTP server authentication protocol
- SNTP server key identifier
- SNMPv3 USM authentication keys
- SNMPv3 USM privacy keys

Procedure:

1. Click **Zeroize Critical Security Parameters**. The confirmation pop up box is displayed:



2. Click **OK**. The zeroize CSPs confirmation page is displayed:



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 security configuration reset to default values. If the unit fails to recover, refer to Testing link end hardware on page 8-7 and Cable Diagnostics on page 8-2.

Rebooting the unit

Use this option to reboot the unit from the Recovery Options page (Figure 253).

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 8-7.

Chapter 8: Troubleshooting

This chapter contains procedures for identifying and correcting faults in a PTP 700 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:

- Cable Diagnostics on page 8-2 describes how to perform cable diagnostics test to detect cabling related faults.
- Testing link end hardware on page 8-7 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 8-13 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 PTP-SYNC on page 8-15 describes how to test the PTP-SYNC unit and its connections when the PTP-SYNC LEDs do not illuminate correctly, or when a synchronization fault is suspected.

Cable Diagnostics

This section describes how to diagnose cable faults.

The Cable Diagnostics feature may be used to test Ethernet cables connected to the Main PSU port and the Aux port. The feature uses Time Domain Reflectometry (TDR) technology to test individual twisted pairs in the cable, to identify open circuit and short circuit faults, and indicate the approximate location of the fault:

- Open circuit – An open circuit is detected when the impedance is greater than 300 ohms.
- Short circuit – A short circuit is detected when the impedance is less than 33 ohms.
- Approximate location of the fault - The fault location is reported as a distance from the ODU along the cable, and is accurate to +/- 2 meters (6.5 feet).

Note

- The cable diagnostics results are provided only as a guide.
- The feature reliably detects all open circuit and short circuit faults in cable pairs, but it is not possible to reliably detect short circuit faults between wires in different cable pairs. Except for that specific circumstance, an OK result for all pairs means the cable is good.
- The presence of LPUs can affect the accuracy and reliability of the results.

Before initiating the test, confirm that all outdoor drop cables (that is those that connect the ODU to equipment inside the building) are specified as supported, as defined in Outdoor copper Cat5e Ethernet cable on page 2-24.

Test scenarios

The Cable Diagnostics test may be performed in following scenarios:

Scenarios	Actions
Main PSU port “Down”	Check for physical Ethernet cable connectivity between Power over Ethernet (PoE) and Customer Data Network (or LAN). If the cable connectivity is OK, Perform Cable Diagnostics test.
Aux port “Down”	Check for physical Ethernet cable connectivity between ODU and Customer Data Network or Management Agent. If the cable connectivity is OK, Perform Cable Diagnostics test.
Main PSU or Aux port is “Up” but the Ethernet speed is noticed slow	There is a possibility that one or more cable pairs have intermittent contact with the RJ45 connector pin. This could result in intermittent communication errors. Follow procedure Ethernet packet test.

	If Ethernet Rx Crc and Align counter is greater than ten (>10), Perform Cable Diagnostics test. If Packet Error Rate is greater than 1 in 1 million, Perform Cable Diagnostics test. If Number of lost packets are less than two (<2) after performing Test ping packet loss, perform Cable Diagnostics test. Otherwise check the ODU's parameter configurations.

Cable Diagnostics test

Menu option: **System > Cable Diagnostics**

The Cable Diagnostics feature determines a fault in a cable and its approximate location based on Time Domain Reflectometry (TDR).

When the test is initiated for the selected port(s), the ODU sends a known signal (+1V) over the twisted pair cable. The transmitted signal will travel down the cable until it reflects off a fault. The magnitude of the reflection and the time it takes for the reflection to come back can be used to calculate the distance to the fault on the cable. For example, a +1V reflection will indicate an open close to the PHY and a -1V reflection will indicate a short close to the PHY.

Based on the returned signal, the radio identifies the cable status and estimates the distance of the fault. The result of the cable test will be displayed.

The cable diagnostics test can be carried out for Main PSU and AUX ports. This test is not supported for SFP port.

Attention

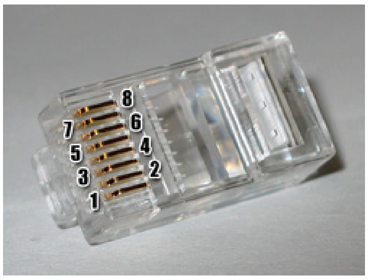
- On the Main PSU port, the presence of LPUs can affect the accuracy of the cable diagnostics results for some cable configurations. When a fault is detected, the feature reports the distance corresponding to the final TDR signal reflection. In configurations where there is a short cable from the ODU to the first LPU (< 2m), and a moderately long cable to the second LPU (30m), the final TDR signal reflection may come from one of the LPUs itself, rather than the fault. For example, a fault in the first short cable may be reported at or near the second LPU.
- On the Aux port, the presence of LPUs can affect the reliability of the cable diagnostics results for many cable configurations. Frequently, open circuit faults may be reported when the cable is OK, and fault distances may be reported corresponding to the LPU locations. Cable diagnostics tests on the Aux port should be repeated a number of times to establish a pattern.

Note All cable diagnostics results should be verified with an external cable tester before remedial action is taken.

All four twisted pairs of the cable are tested separately, and results are displayed for each pair.

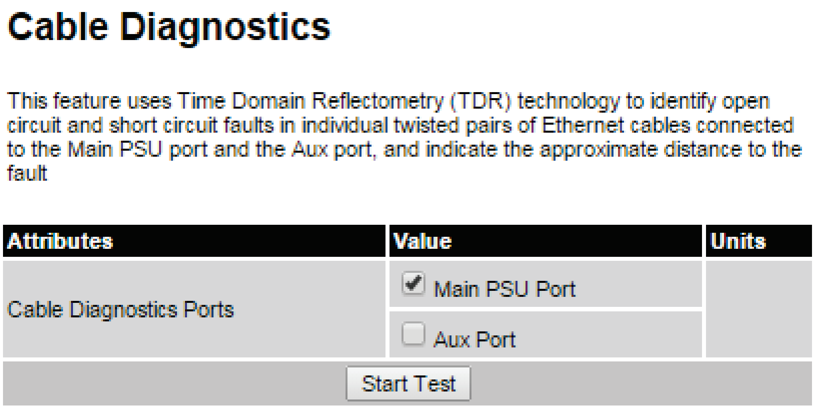
The pin to pair mapping of a cable is shown in Table 204.

Table 204 Pin to pair mapping of a cable (T568B termination)

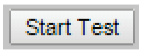
Pin	Pair	Wire	Color (Supplied cable)	Color (Conventional)	Pins on plug face
1	2	1	Light Orange	White/Orange	
2	2	2	Orange	Orange	
3	3	1	Light Green	White/Green	
4	1	2	Blue	Blue	
5	1	1	Light Blue	White/Blue	
6	3	2	Green	Green	
7	4	1	Light Brown	White/Brown	
8	4	2	Brown	Brown	

Procedure

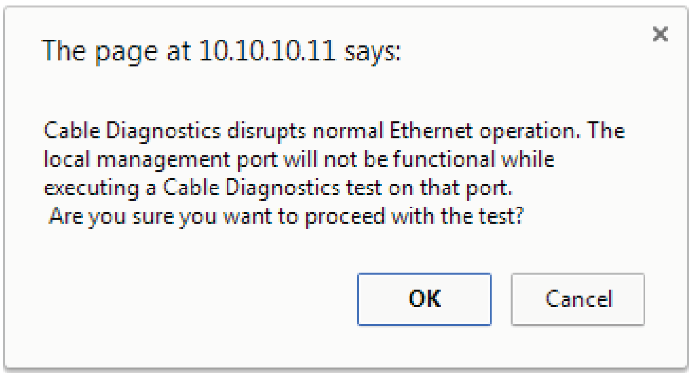
1 Select ports for cable diagnostics test:



2 Click “Start Test” button to begin the test:



3 The confirmation pop up box is displayed. Click the “OK” button to proceed with the test:



Note The Local Management port connection will be lost when the local management port is under test. However, the management port will be accessible when the other ports are under test.

4 On completion of the test, the web page is refreshed automatically, and the results are displayed:

Cable Diagnostics Results

The cable diagnostics results are provided only as a guide.
The presence of LPUs can affect the accuracy and reliability of the results (see the User Guide for more details).

All cable diagnostics results should be verified with an external cable tester before remedial action is taken.

Main PSU Port

Attributes	Value	Units
Last Test Time	01-Jan-1970 00:06:53	

Cable Pair	Results	Distance to Fault	Units
Pair 1	Short Circuit	6	meters
Pair 2	OK		
Pair 3	OK		
Pair 4	Short Circuit	6	meters

Aux Port

Attributes	Value	Units
Last Test Time		

Cable Pair	Results	Distance to Fault	Units
Pair 1	Not Tested		
Pair 2	Not Tested		
Pair 3	Not Tested		
Pair 4	Not Tested		

Note The last test performed results are shown for user reference purpose.

Table 205 Cable Diagnostics attributes

Attribute	Meaning
Cable Diagnostics Ports	Select ports on which Cable Diagnostics must be executed.
Last Test Time	The date and time when a Cable Diagnostics test was last executed successfully.

Attribute	Meaning
Cable Pair	The result of the most recent execution of cable diagnostics on a cable pair. There are four twisted pairs in each Cat5 cable. The cable diagnostics test is performed on each pair of the cable.
Results	OK: Reported when the test is passed for a respective cable pair. Open Circuit: Reported when the impedance is greater than 330 ohms. Short Circuit: Reported when impedance is less than 33 ohms.
Distance	The estimate of the distance from the ODU to the fault detected on the cable pair during the most recent execution of Cable Diagnostics. Fault in cables longer than 160 meters (525 feet) may not be detected. The error margin is +/- 2 meters (6.5 feet).
Units	Unit of cable length in meters.

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 2-24.

AC+DC Enhanced Power Injector 56V LED sequence

For the AC+DC Enhanced Power Injector 56V, 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 8-7
- Power LED is blinking on page 8-7
- Ethernet LED did not blink 10 times on page 8-8
- Ethernet LED blinks ten times then stays off on page 8-8
- Ethernet LED blinks irregularly on page 8-9 (for example a short blink followed by a long blink)
- Power LED is on, Ethernet LED blinks randomly on page 8-9

If a fault is suspected in the ODU-PSU drop cable, perform Test resistance in the drop cable on page 5-45.

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 5-45.

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.

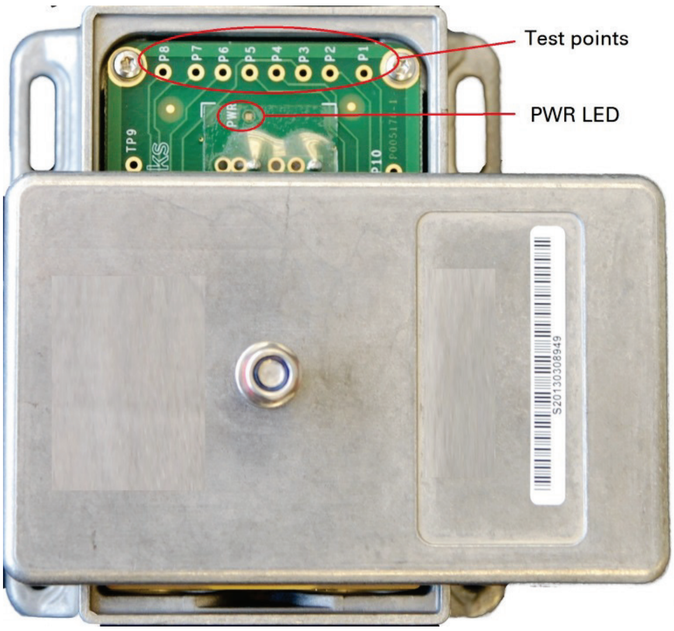
Ethernet LED did not blink 10 times

Meaning: The ODU flashes the LED on the AC+DC Enhanced Power Injector 56V 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 5-45. 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 56V 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 5-45.

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 7-73.

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.

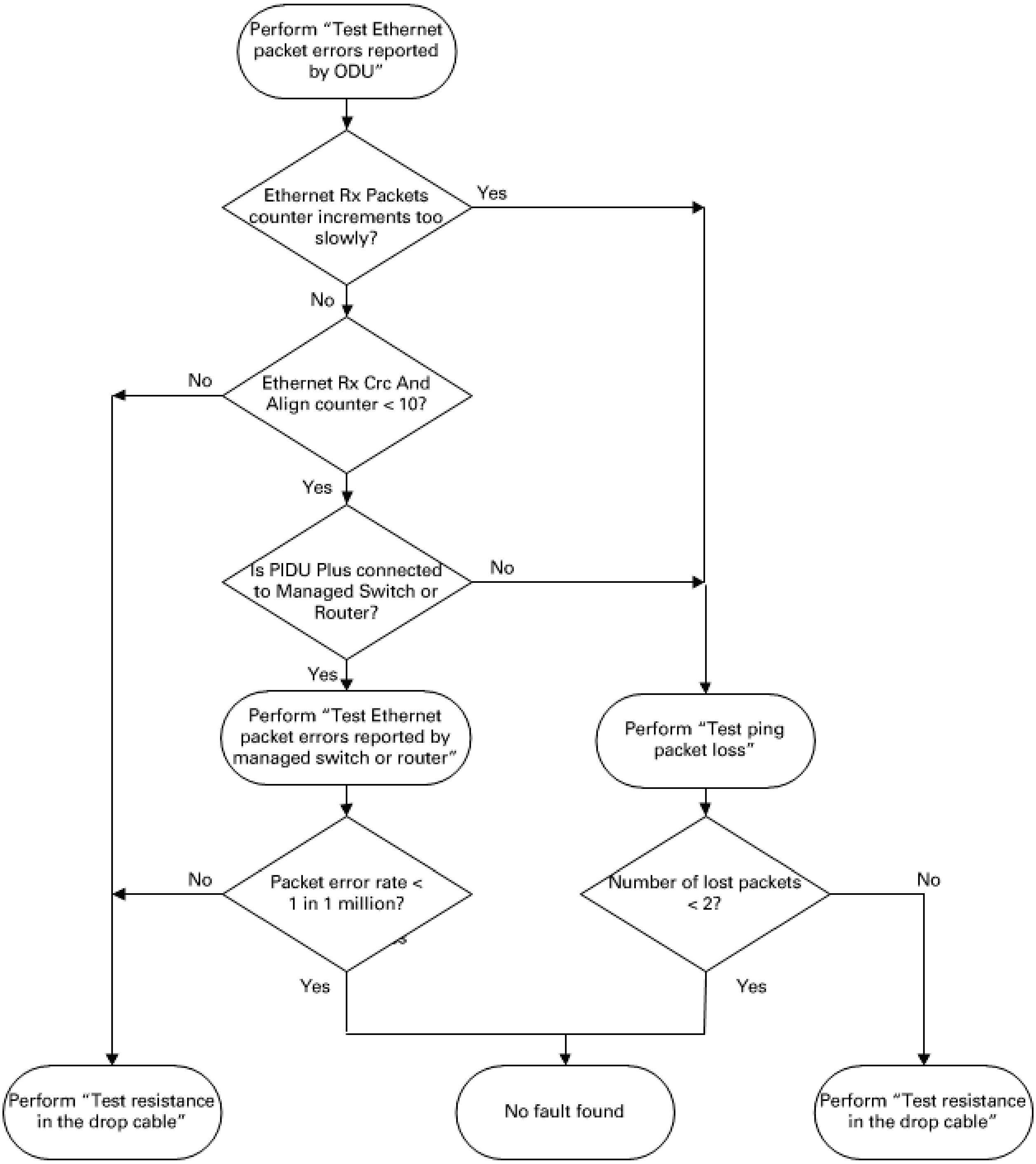
Action: If, in spite of this, a fault is suspected in the link end hardware:

- 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 8-10.

Ethernet packet test

Follow the Ethernet packet test flowchart (Figure 254) and procedures below.

Figure 254 Ethernet packet test flowchart



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 700 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 8-11.

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.

Attention This procedure disrupts network traffic carried by the PTP 700 under test:

Procedure:

1 Ensure that the IP address of the computer is configured appropriately for connection to the PTP 700 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 700 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 700 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 700 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.

Testing PTP-SYNC

This section describes how to test the PTP-SYNC unit and its connections when the PTP-SYNC LEDs do not illuminate correctly, or when a synchronization fault is suspected.

Checking the PTP-SYNC LEDs

If a fault is suspected in the PTP-SYNC or GPS hardware, check the PTP-SYNC LED states and use Table 206 to choose the correct test procedure.

Table 206 PTP-SYNC indicator LED states

LED	State	Description and test procedure
GPS	Off	No GPS satellite data being received at the GPS/SYNC IN port. Refer to GPS LED does not illuminate or blink on clustered units on page 8-16.
	On steady or blink	GPS satellite data being received.
SYNC	Off	No data being received at the SYNC OUT port.
	On steady or blink	Data being received at the SYNC OUT port. The SYNC LED does not normally illuminate, even in cluster configurations.
STATUS	Off	No power. Refer to LEDs do not illuminate on page 8-15.
	On steady	Power but no satellite lock. Refer to STATUS LED is on steady on page 8-16.
	Blink	Power and satellite lock at either the GPS/SYNC IN or 1PPS IN port.
	Double blink	Possible fault in GPS/SYNC IN or 1PPS IN cables. Refer to STATUS LED double-blinks on page 8-16.
ODU	Off	No signal being received from the ODU. Refer to ODU LED does not illuminate within 90 seconds on page 8-16.
	On	Communication with the ODU is established.
	Blink red	Error in communication with ODU. Refer to ODU LED blinks red on page 8-16,

LEDs do not illuminate

Meaning: The PTP-SYNC unit is not powered up.

Action: Ensure that there is a cable connection between the PSU ODU interface and the PIDU IN interface of the PTP-SYNC unit. Confirm that the PSU is powered up.

STATUS LED is on steady

Meaning: There is power but no satellite lock. This probably indicates that a 1PPS synchronization pulse is not detected by the PTP-SYNC unit.

Action: Depending on system configuration, take one of the following actions:

- System using a GPS receiver module - Ensure that there is a cable connection between the PTP-SYNC GPS/SYNC IN interface and the LPU, also that there is a cable connection between the LPU and the GPS receiver module. Check that the GPS receiver module has an uninterrupted view of the sky.
- System using an alternative 1PPS timing source - Ensure that there is a cable connection between the PTP-SYNC GPS/SYNC IN or 1PPS IN interface and the 1PPS timing source.
- On cluster slave units – Ensure that there is a cable connection between the slave GPS/SYNC IN interface and the SYNC OUT interface of the preceding unit in the chain.

STATUS LED double-blinks

Meaning: There may be a fault in the GPS/SYNC IN or 1PPS IN cables.

Action: Check the GPS wiring in accordance with Table 40.

ODU LED does not illuminate within 90 seconds

Meaning: There may be no communication between PTP-SYNC and ODU.

Action: Ensure that the PTP-SYNC ODU OUT interface is connected to the ODU (and LPUs if installed) via the drop cable.

ODU LED blinks red

Meaning: Error in communication with ODU. Possible causes are: fault in the ODU or PSU cable, maximum recommended cable lengths exceeded, or TDD synchronization is not enabled at the ODU.

Action: Confirm that the ODU and PSU cables are not too long: see Ethernet standards and cable lengths on page 2-23. Check the ODU cable wiring by following the procedure described in Test resistance in the drop cable on page 5-45.

GPS LED does not illuminate or blink on clustered units

Meaning: This indicates a fault only when the timing source is a GPS receiver.

Action: Table 207 describes the action to be taken depending upon the behavior of the GPS LEDs at the master and slave(s).

Table 207 Clustered PTP-SYNC units - GPS LEDs Fault-finding

Cluster timing source	GPS LED on master	GPS LED on slave(s)	Diagnosis
GPS receiver providing NMEA data	Blink	Blink	OK
	Off	Any	Fault in GPS unit or GPS cable

Cluster timing source	GPS LED on master	GPS LED on slave(s)	Diagnosis
	Blink	Off	Fault in daisy chain cable
Alternative 1PPS source, no NMEA data	Off	Off	OK
	Off	On	Fault in alternative 1PPS source
One ODU is cluster timing master	Off	Off	OK

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
FCC	Federal Communications Commission

Term	Definition
FIPS	Federal Information Processing Standards
FQDN	Fully Qualified Domain Name
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
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
SFP	Small Form-factor Pluggable

Term	Definition
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