Cambium PTP 670 Series User Guide

System Release 670-02-51

Cambium Networks™

Accuracy

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

Copyrights

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

Restrictions

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

License Agreements

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

High Risk Materials

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

Contents

About This User Guide

This guide describes the planning, installation, configuration and operation of the Cambium PTP 670 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 670 product operates in frequency bands between 4.8 GHz and 5.9 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 670 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 670 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 670 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 670. If this is not done, installers and users may be liable to civil and criminal penalties.

Contact the Cambium helpdesk if more guidance is required.

USA specific information

Caution

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

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

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

In order to comply with these FCC requirements, Cambium supplies variants of the PTP 670 for operation in the USA. These variants are only allowed to operate with license keys that comply with FCC rules.

Other variants of the PTP 670 are available for use in the rest of the world, but these variants are not supplied to the USA except under strict controls, when they are needed for export and deployment outside the USA.

Canada specific information

Caution

This device complies with Innovation, Science and Economic Development Canada's licence-exempt RSSs. Operation is subject to the following two conditions:

(1) This device may not cause interference; and

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Innovation, Science and Economic Development Canada (ISEDC) requires manufacturers to implement special features to prevent interference to weather radar systems that operate in the band 5600 MHz to 5650 MHz. These features must be implemented in all products able to operate outdoors in the band 5470 MHz to 5725 MHz.

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

In order to comply with these ISEDC requirements, Cambium supplies variants of the PTP 670 for operation in Canada. These variants are only allowed to operate with license keys that comply with ISEDC rules. In particular, operation of radio channels overlapping the band 5600 MHz to 5650 MHz is not allowed and these channels are permanently barred.

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

Other variants of the PTP 670 are available for use in the rest of the world, but these variants are not supplied to Canada except under strict controls, when they are needed for export and deployment outside Canada.

Renseignements specifiques au Canada

Attention

Le présent appareil est conforme aux CNR d'Innovation, Sciences et Développement Economique Canada applicables aux appareils radio exempts de licence.
L'exploitation est autorisée aux deux conditions suivantes :

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Innovation, Sciences et Développement Economique Canada (ISDEC) a demandé aux fabricants de mettre en œuvre des mécanismes spécifiques pour éviter d'interférer avec des systèmes radar fonctionnant dans la bande 5600 MHz à 5650 MHz. Ces mécanismes doivent être mis en œuvre dans tous les produits capables de fonctionner à l'extérieur dans la bande 5470 MHz à 5725 MHz.

Les fabricants doivent s'assurer que les produits de radiocommunications ne peuvent pas être configurés pour fonctionner en dehors des règles ISDEC, en particulier, il ne doit pas être possible de désactiver ou modifier les fonctions de protection des radars qui ont été démontrés à ISDEC.

Afin de se conformer à ces exigences de ISEDC, Cambium fournit des variantes du PTP 670 exclusivement pour le Canada. Ces variantes ne permettent pas à l'équipement de fonctionner en dehors des règles de ISDEC. En particulier, le fonctionnement des canaux de radio qui chevauchent la bande 5600-5650 MHz est interdite et ces canaux sont définitivement exclus.

EU specific information

	BE	BG	CZ	DK	DE	EE	IE	EL	ES
	FR	HR	IT	CY	LV	LT	LU	HU	MT
	NL	AT	PL	PT	RO	SI	SK	FI	SE
	UK								

PTP 670 can be configured to operate in lightly-licensed frequency bands and unlicensed frequency bands that are permitted in individual countries but not harmonized within the EU. Ensure that the equipment is operated in accordance with applicable regulations for the country of operation. Obtain the necessary licenses or permits before using the equipment in lightly-licensed bands.

EU Declaration of Conformity

Hereby, Cambium Networks declares that the Cambium PTP 670 Series Wireless Ethernet Bridge complies with the essential requirements and other relevant provisions of Directive 1999/5/EC. The declaration of conformity may be consulted at:

http://www.cambiumnetworks.com/support/compliance/

Application firmware

Download the latest PTP 670 Series firmware and install it in the Outdoor Units (ODUs) before deploying the PTP 670 equipment. Instructions for installing firmware are provided in Upgrading software image on page 7-79.

Specific expertise and training for professional installers

To ensure that the PTP 670 is installed and configured in compliance with the requirements of ISEDC and the FCC, installers must have the radio engineering skills and training described in this section. This is particularly important when installing and configuring a PTP 670 system for operation in the 5.1 GHz and 5.4 GHz UNII bands.

External antennas

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

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

Antennas externes

Lorsque vous utilisez une version du produit sans antenne intégrée, il peut être nécessaire de réduire la puissance d'émission pour garantir que la limite réglementaire de puissance isotrope rayonnée équivalente (PIRE) n'est pas dépassée. L'installateur doit avoir une bonne compréhension de la façon de calculer le gain de l'antenne de gain de l'antenne réelle et les pertes dans les câbles de connections.

La plage de valeurs admissibles pour un gain maximal de l'antenne et des pertes de câbles de connections sont inclus dans ce guide d'utilisation avec un exemple de calcul. L'interface utilisateur du produit applique automatiquement la limite de puissance menée correct afin de s'assurer qu'il ne soit pas possible pour l'installation de dépasser la limite PIRE, lorsque les valeurs appropriées pour le gain d'antenne et les pertes de câbles d'alimentation sont entrées dans l’interface utilisateur.

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 670 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 670 should be gained by reading Chapter 5: Installation and Chapter 6: Configuration and alignment and by performing sample set ups at base workshop before live deployments.

Problems and warranty

Reporting problems

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

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

Repair and service

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

Hardware warranty

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

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

Caution

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

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

Security advice

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

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

Warnings, cautions, and notes

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

Warnings

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

Warning

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

Cautions

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

Caution

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

Notes

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

Note

Note text.

Caring for the environment

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

In EU countries

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

Disposal of Cambium equipment

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

Do not dispose of Cambium equipment in landfill sites. For disposal instructions, refer to http://www.cambiumnetworks.com/support/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 670 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 670 Series on page 1-2 introduces the key features, typical uses, product variants and components of the PTP 670 series.
- Wireless operation on page 1-7 describes how the PTP 670 wireless link is operated, including modulation modes, power control and spectrum management.
- Ethernet bridging on page 1-30 describes how the PTP 670 controls Ethernet data, in both the customer data and system management networks.
- TDM bridging on page 1-43 describes how TDM traffic (E1 or T1) may be carried over PTP 670 links.
- System management on page 1-46 introduces the PTP 670 management system, including the web interface, installation, configuration, security, alerts and upgrades.

Overview of the PTP 670 Series

This section introduces the key features, typical uses, product variants and components of the PTP 670 series.

Purpose

Cambium PTP 670 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 4800 MHz and 6050 MHz. Users must ensure that the PTP 670 Series complies with local operating regulations.

The PTP 670 Series acts as a transparent bridge between two segments of the operator's network. In this sense, it can be treated as a virtual wired connection between two points. The PTP 670 Series forwards 802.3 Ethernet frames destined for the other part of the network and filters frames it does not need to forward. The system is transparent to higher-level protocols such as VLANs and Spanning Tree.

Key features

The PTP 670 is a high performance wireless bridge for Ethernet traffic with a maximum throughput of 450 Mbps. It is capable of operating in line-of-sight (LOS), near-LOS and non-LOS propagation condition. Its maximum LOS range is 250 km. The PTP 670 operates in licensed, unlicensed and lightly-licensed frequency bands between 4800 MHz and 6050 MHz. It has a very high spectral efficiency of 10 bps/Hz and supports a channel bandwidth of up to 45 MHz. The PTP 670 Integrated ODU has its own flat plate antenna with antenna gain 23 dBi. The PTP 670 Connectorized ODU is designed for use with an external antenna.

The wireless link uses Time Division Duplex (TDD) and supports both symmetric and asymmetric TDD configurations.

PTP 670 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.

From an Ethernet point-of-view, the PTP 670 wireless link is a transparent Layer 2 bridge. It supports up to three Gigabit Ethernet ports. Two ports support twisted pair Gigabit Ethernet. One of them is capable of providing power via standard 802.3at PoE to an external device such as a video surveillance camera or a wireless access point. The third port accepts either a twisted pair or fibre GE SFP module.

The PTP 670 Series supports an optional TDM adaptor that allows E1 or T1 telecoms circuits to be bridged over the wireless link.

The PTP 670 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 670 supports both synchronous Ethernet and operation as an IEEE 1588-2008 transparent clock.

Table 1 gives a summary of the main PTP 670 characteristics.

Table 1 Main characteristics of the PTP 670 Series

Characteristic	Value
Topology	PTP, HCMP.
Wireless link condition	LOS, near LOS or non-LOS
Range	Up to 250 km
Duplexing	TDD (symmetric and asymmetric)
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	4800 MHz to 5875 MHz (4.8 to 5.9 GHz frequency variant) 4900 MHz to 6050 MHz (4.9 to 6.05 GHz frequency variant)
Channel bandwidth	5, 10, 15, 20, 30, 40 or 45 MHz
High spectral efficiency	Up to 10 bps/Hz
Data rate	Up to 450 Mbps (45 MHz channel BW)
Telecommunications (TDM)	Up to eight E1 or T1 circuits (NIDU required)

Frequency bands

The PTP 670 ODU can be configured by the user to operate in the following bands:

- 4.8 GHz band: 4800 MHz to 4900 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
- 5.9 GHz band: 5825 MHz to 6050 MHz

The PTP 670 frequency variants support the following bands:

Table 2 PTP 670 support for frequency bands

Frequency variant	4.8 GHz	4.9 GHz	5.1 GHz	5.2 GHz	5.4 GHz	5.8 GHz	5.9 GHz
4.8 to 5.9 GHz	Yes	Yes	Yes	Yes	Yes	Yes	-
4.9 to 6.05 GHz	-	Yes	Yes	Yes	Yes	Yes	Yes

Note

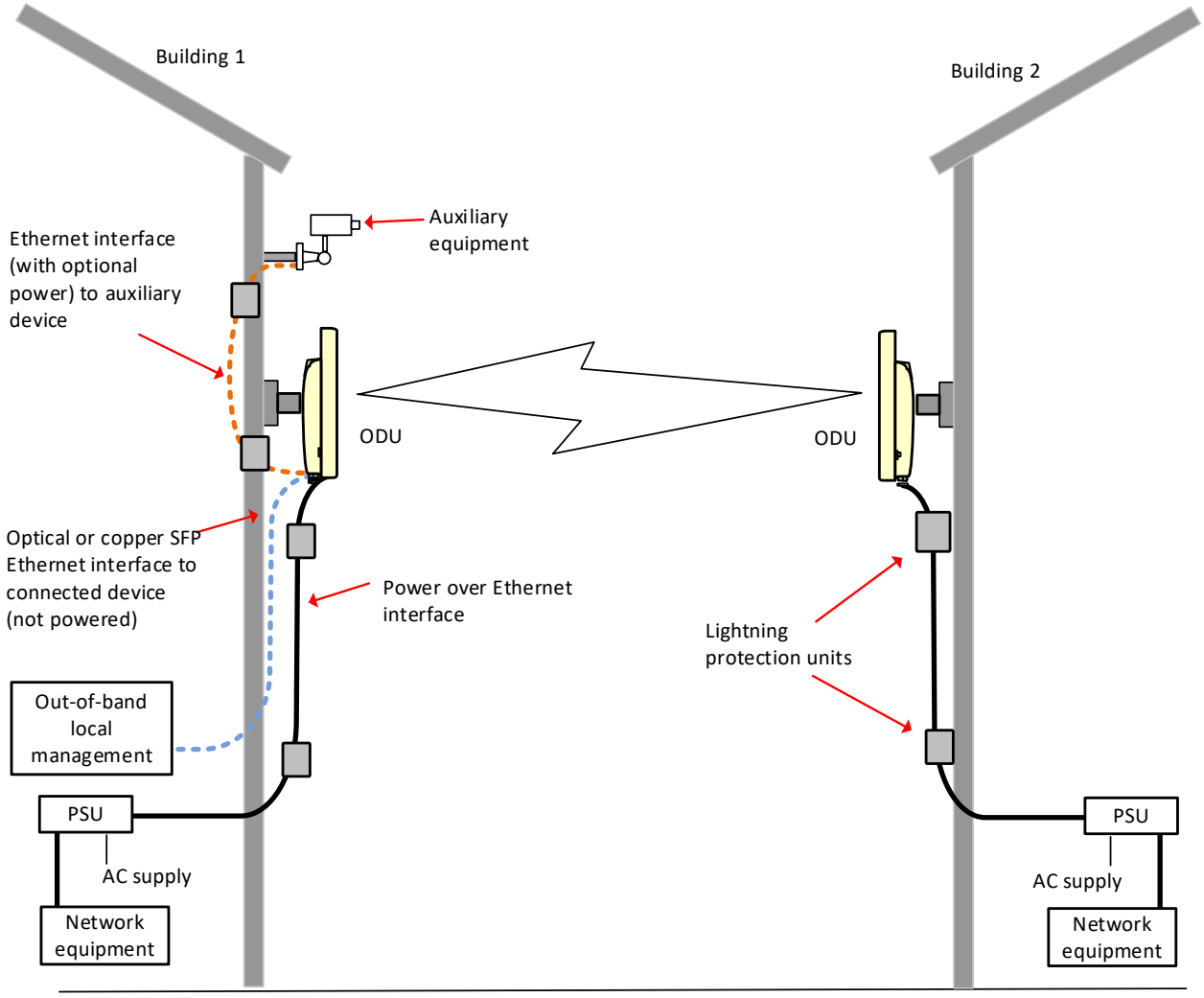
The supported frequency coverage may be further restricted in some country licenses to comply with the applicable regulations.

Typical bridge deployment

The PTP 670 is an "all outdoor" solution consisting of a wireless bridge between two sites. Each site installation consists of a PTP 670 Integrated or PTP 670 Connectorized outdoor unit (ODU), and a power injector (PSU) (Figure 1). The ODU provides the following interfaces:

- PSU port: This provides proprietary power over Ethernet and connection to the management and/or data networks via 100BASE-TX or 1000BASE-T Ethernet. In the basic configuration, this is the only Ethernet connection to the ODU.
- SFP port: This provides an optical or copper Gigabit Ethernet interface for 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 670 typical bridge deployment



Hardware overview

The main hardware components of the PTP 670 are as follows:

- Outdoor unit (ODU): The ODU is a self-contained transceiver unit that houses both radio and networking electronics. The PTP 670 ODU is supplied in two configurations:
  - A PTP 670 Integrated ODU attached to a 23 dBi flat plate antenna
  - A PTP 670 Connectorized ODU intended to work with separately mounted external antennas.
- The ODU is supplied in the following frequency variants:
  - 4.8 to 5.9 GHz
  - 4.9 to 6.05 GHz
- The ODU is supplied in the following regional variants:
  - FCC, intended for deployment in the USA
  - European Union (EU), intended for deployment in countries of the European Union or other countries following ETSI regulations
  - IC, intended for deployment in Canada under the rules of ISEDC.
  - Mexico, intended for use in Mexico
  - RoW, intended for deployment in countries other than USA, Canada and EU countries.
- Power supply unit (PSU): PTP 670 provides three options for PSUs:
  - The AC Power Injector 56V is suitable for powering a single ODU without an auxiliary device. The AC Power Injector 56V is not approved for use with the 4.8 GHz to 5.9 GHz frequency variants of PTP 670.
  - The AC+DC Power Injector 56V is required when powering a single PTP 670 ODU from a DC supply, when powering an auxiliary device, when using PTP-SYNC, or when the PSU is needed to operate at extreme temperatures.
  - 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 670 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.
- Network Indoor Unit (NIDU) (optional): The NIDU allows up to eight TDM channels (E1 or T1) to be bridged over a PTP 670 link.
- Ethernet cabling: All configurations require a copper Ethernet Cat5e connection from the ODU (PSU port) to the PSU. Advanced configurations may also require one or both of the following:
  - A copper or optical Ethernet connection from the ODU (SFP port) to network terminating equipment or another device.

  - A copper Ethernet Cat5e connection from the ODU (Aux port) to an auxiliary device.
- Lightning protection unit (LPU): LPUs are installed in the PSU and Aux copper drop cables to provide transient voltage surge suppression.
- Ground cables: ODU, LPUs and outdoor copper Ethernet cables are bonded to the site grounding system using ground cables.

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

Wireless operation

This section describes how the PTP 670 wireless link is operated, including topology, modulation modes, power control and security.

Wireless topology

PTP 670 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: 4800 MHz to 5875 MHz, 4900 MHz to 6050 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
- Out-of-band management
- Synchronous Ethernet
- IEEE 1588 Transparent Clock
- TDM: Eight T1/E1 circuits using the Network Indoor Unit (NIDU)

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 time slot of 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: 4800 MHz to 5875 MHz, 4900 MHz to 6050 MHz
- Channel bandwidth: 20 MHz or 40 MHz
- Range: Up to 40 km
- Number of Slaves:
  - 20 MHz: Up to four
  - 40 MHz: Up to eight
- Link symmetry: 4:1, 3:1, 2:1, 1:1, 1:2, 1:3, 1:4, depending on bandwidth and 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

Synchronous Ethernet, IEEE 1588 Transparent Clock and TDM 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 1-21
Capability upgrades for HCMP	Capability upgrades on page 1-60
Configuring encryption in HCMP	Wireless encryption on page 1-21
Configuring the Whitelist	Authorization Control page on page 6-63

Time division duplexing in PTP wireless topology

TDD cycle

PTP 670 links operate using Time Division Duplexing (TDD). They use a TDD cycle in which the ODUs alternately transmit and receive TDD bursts. The TDD cycle is illustrated in Figure 2. The steps in the cycle are as follows:

1 The TDD master transmits a burst to the TDD slave.

2 A delay occurs as the master-slave burst propagates over the link.

3 The slave receives the burst from the master.

4 The slave processes the master-slave burst.

5 The slave transmits a burst to the master.

6 A delay occurs as the slave-master burst propagates over the link.

7 The master receives the burst from the slave.

8 The master transmits the next burst to the slave.

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:

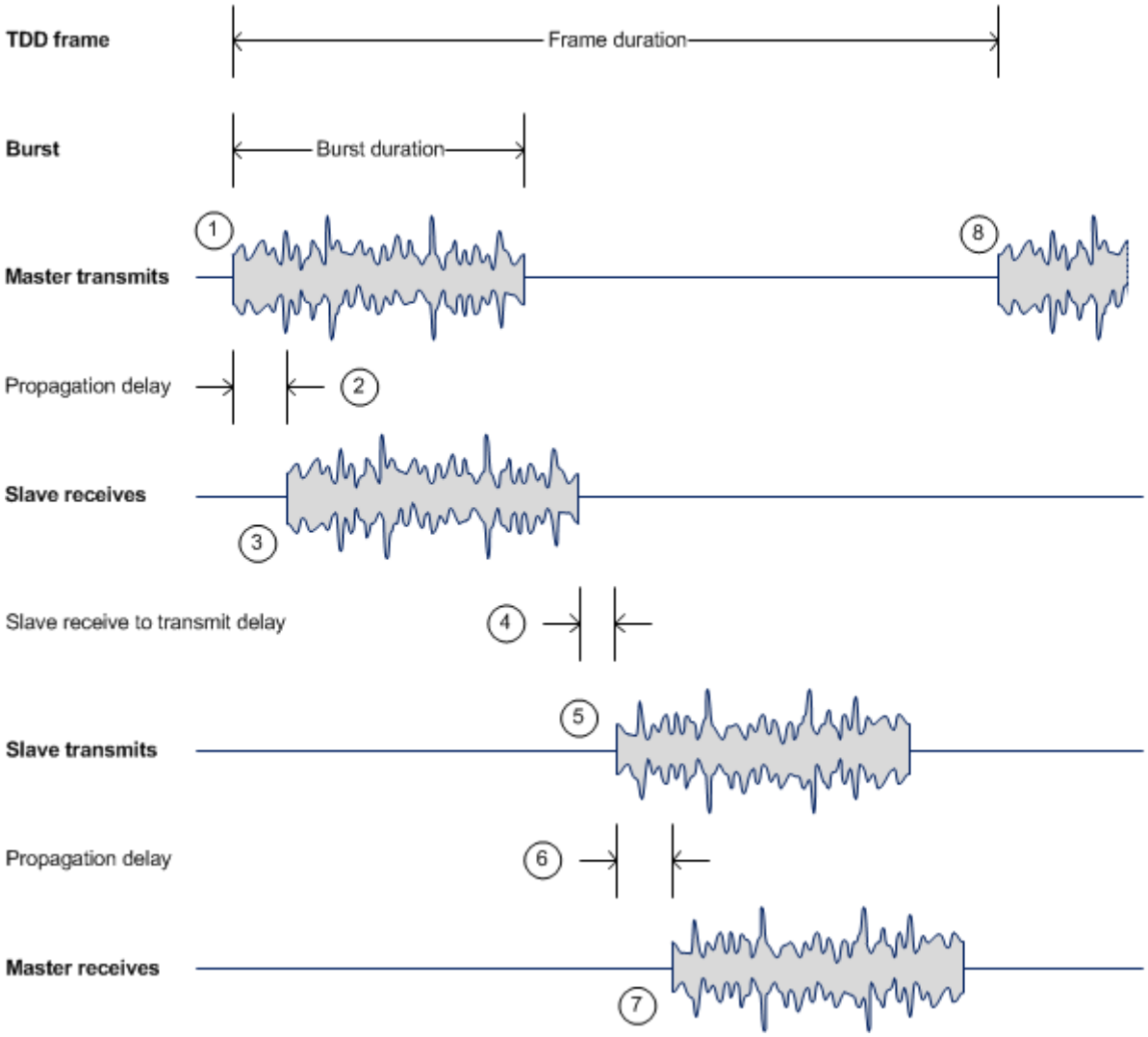
- Channel bandwidth
- Link range
- Link optimization mode
- Link symmetry
- Offered traffic loading.

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. There may be added delays between rx and tx on the master and slave to minimize interference, as set up by the link planner or installer.

Figure 2 TDD cycle



Channel selection

The PTP 670 series links are capable of transmitting and receiving on the same channel or on different channels. In other words, the slave-master direction may use a different channel from the master-slave direction. Independent selection of transmit and receive frequencies can be useful in planned networks or for countering interference.

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

Time division duplexing in HCMP wireless topology

TDD cycle

The TDD cycle in HCMP operation is similar to 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 3. 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

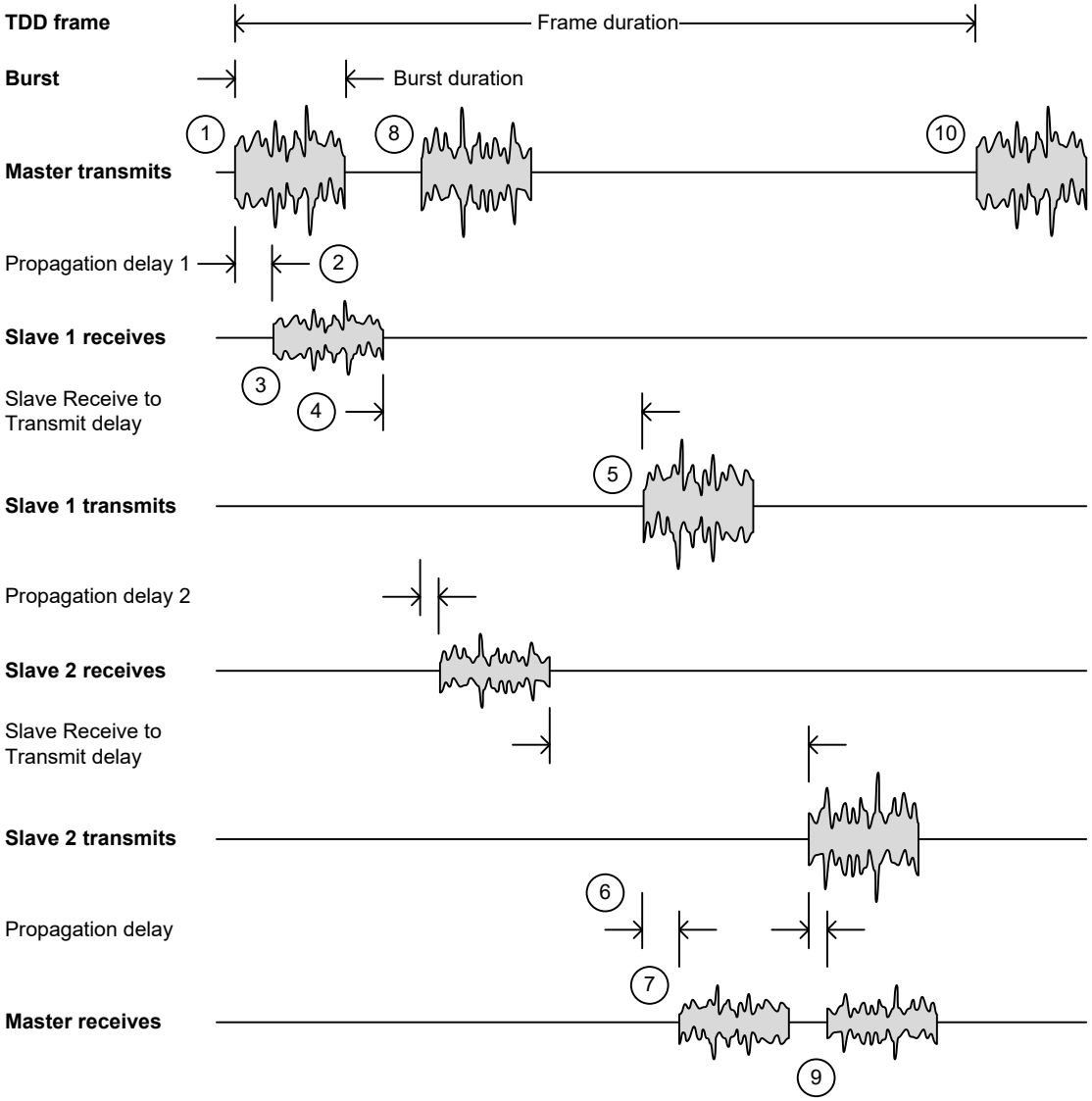
In the HCMP topology, the TDD burst duration is fixed.

The TDD frame duration varies depending on the following:

- Maximum number of Slaves
- Maximum 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. The propagation delay for the second Slave will be different from the delay for the first Slave unless the two Slaves are at exactly the same range.

Figure 3 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 1-26

Link mode optimization

Link mode optimization allows the PTP 670 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 1-13
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 3-86
Effect of IP and TDM modes on system threshold, output power and link loss	System threshold, output power and link loss on page 3-65
How to configure link mode optimization	Wireless Configuration page on page 6-25
Link mode optimization alarms	Alarms on page 7-20

Link symmetry

PTP topology

The PTP 670 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 670 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 670 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 670 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 670 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 670 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 670 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 670 series achieves this by setting the Burst Duration of the Slave to five times that of the Master.
- **Adaptive –** 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 670 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 670 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, or when TDM services are 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 1-12.
- When TDD synchronization is enabled.
- In regions where radar avoidance is operational (see Radar avoidance on page 1-19).

HCMP topology

The PTP 670 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 and the number of Slaves, as shown in Table 3.

Table 3 Link symmetry options in HCMP

Channel Bandwidth	Number of slaves	Supported Link Symmetry options
20 MHz	Two	3:1, 2:1, 1:1, 1:2, 1:3
	Three	2:1, 1:1, 1:2
	Four	1:1
40 MHz	Two, Three	4:1, 3:1, 2:1, 1:1, 1:2, 1:3, 1:4
	Four	3:1, 2:1, 1:1, 1:2, 1:3
	Five, Six	2:1, 1:1, 1:2
	Seven, Eight	1:1

Further reading

For information about...	Refer to...
Link symmetry in synchronized networks	TDD synchronization on page 1-26
Effect of link symmetry on link data throughput capacity	Calculating data rate capacity on page 3-26 Data throughput capacity tables on page 3-86
How to configure link symmetry	Wireless Configuration page on page 6-25

OFDM and channel bandwidth

The PTP 670 series transmits using Orthogonal Frequency Division Multiplexing (OFDM). This wideband signal consists of many equally spaced sub-carriers. Although each sub carrier is modulated at a low rate using conventional modulation schemes, the resultant data rate from the sub-carriers is high. OFDM works exceptionally over a Non-Line-of-Sight (NLoS) channel.

The channel bandwidth of the OFDM signal is configurable to one of the following values: 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.

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

Note

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

Further reading

For information about...	Refer to...
Channel bandwidths per frequency band	General wireless specifications on page 3-20
How to plan for channel bandwidth	Channel bandwidth on page 3-22
Effect of channel bandwidth on link data throughput capacity	Calculating data rate capacity on page 3-26 Data throughput capacity tables on page 3-86
How to configure channel bandwidth	Wireless Configuration page on page 6-25
How to monitor channel bandwidth	Spectrum Management on page 7-29

Spectrum management

The spectrum management feature of the PTP 670 Series monitors the available wireless spectrum and directs both ends of the wireless link to operate on a channel with a minimum level of co-channel and adjacent channel interference.

Spectrum management measurements

The PTP 670 Series performs two mean signal measurements per TDD cycle, per channel. This mean measurement represents the mean received signal power for the 40 microsecond measurement period.

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

Measurement analysis

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

Statistical summary

The display of statistical measurement on the Spectrum 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.

Spectrum management in fixed frequency mode

The transmit and receive frequencies can be fixed in a PTP 670 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.

Further reading

For information about...	Refer to...
How to perform spectrum management	Spectrum Management on page 7-29

Adaptive modulation

The PTP 670 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 670 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 670 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 1-33
Lowest TDM modulation mode	Lowest TDM modulation mode on page 1-44
Planning for adaptive modulation	Adaptive modulation on page 3-25
Effect of modulation mode on link data throughput capacity	Calculating data rate capacity on page 3-26 Data throughput capacity tables on page 3-86

For information about...	Refer to...
Effect of modulation mode on system threshold, output power and link loss	System threshold, output power and link loss on page 3-65
How to configure modulation modes	Interface Configuration page on page 6-16 Wireless Configuration page on page 6-25 System Configuration page on page 6-39
Modulation mode when the ODU is armed	Checking that the units are armed on page 6-118
How to view the transmit and receive modulation modes	System Status page on page 7-3 System counters (PTP topology) on page 7-57

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 670 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 670 will adapt between two modes of operation:

- **Dual Payload**: When the radio channel conditions allow, the PTP 670 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 670.
- **Single Payload**: As the radio channel becomes more challenging, the PTP 670 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 670 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 1-17.

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 6-25

For information about...	Refer to...
Single and dual payload modulation modes	System threshold, output power and link loss on page 3-65
TDM single payload lock feature	TDM on page 7-15

Dynamic spectrum optimization

The PTP 670 series uses an interference mitigation technique known as Dynamic Spectrum Optimization (DSO). Both the Master and Slave continually monitor for interference on all channels and then select the best frequency of operation. This is a dynamic process where the PTP 670 can continually move channels in response to changes in interference. Two modes of operation are available:

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

Note

PTP 670 does not support Dynamic Spectrum Optimization in the HCMP topology.

Further reading

For information about...	Refer to...
Using DSO in PTP networks	Using Dynamic Spectrum Optimization on page 1-25
Planning to use DSO	Frequency selection on page 3-22
How to configure DSO	Wireless Configuration page on page 6-25
Asymmetric DSO in non-radar regions	Spectrum Management Settings on page 7-35

Radar avoidance

In regions where protection of radars is part of the local regulations, the PTP 670 must detect interference from radar-like systems and avoid co-channel operation with these systems.

To meet this requirement, the PTP 670 implements the following features:

- The radar detection algorithm will always scan a usable channel for 60 seconds for radar interference before making the channel an available channel.
- This compulsory channel scan will mean that there is at least 60 seconds service outage every time radar is detected and that the installation time is extended by at least 60 seconds even if no radar is found.

- When operating on a channel, the spectrum management algorithm implements a radar detection function which looks for impulsive interference on the operating channel. If impulsive interference is detected, spectrum management will mark the current operating channel as having detected radar (unavailable channel) and initiate a channel hop to an available channel. The previous operating channel will remain in the unavailable state for thirty minutes after the impulsive interference pulse was detected.
- After the thirty minutes have expired the channel will be returned to the usable channel pool.

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

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

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 670 does not support Radar Avoidance in the HCMP topology.

Further reading

For information about...	Refer to...
Radar avoidance in the country of operation	License keys and regulatory bands on page 1-24
Planning for mandatory radar detection	Frequency selection on page 3-22
Radar avoidance when aligning antennas	ODU installation tones on page 6-121
Effect of radar detection on spectrum management	Spectrum Expert page in radar avoidance mode on page 7-41

Access method

PTP topology

PTP 670 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 670 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...
General description of Wireless encryption	Wireless encryption on page 1-21
Configuring Access Method	Wireless Configuration page on page 6-25
Configuring Target MAC Address	Wireless Configuration page on page 6-25
Authorization Control page	Authorization Control page on page 6-63

Wireless encryption

The PTP 670 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 670 is approved to FIPS 197.

The use of AES encryption in PTP 670 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 670 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.

User-supplied device certificates are 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 670 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 670 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 670 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 670 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 1-20
Authentication of the remote ODU	Wireless encryption on page 1-21
Licensing AES encryption	AES license on page 1-57 Capability upgrades on page 1-60
How to generate AES license keys	Generating license keys on page 6-3
How to configure AES encryption	System Configuration page on page 6-39
Configuring the Whitelist of approved ODUs for an HCMP sector.	Authorization Control page on page 6-63

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. Both 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 1-20
Authentication of the remote ODU	Wireless encryption on page 1-21
Licensing AES encryption	AES license on page 1-57 Capability upgrades on page 1-60
How to generate AES license keys	Generating license keys on page 6-3
How to configure AES encryption	System Configuration page on page 6-39

Over the air rekeying

PTP 670 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 1-22
General description of TLS-PSK	TLS PSK 128-bit and TLS PSK 256-bit on page 1-23
Upgrading for Over the Air Rekey	Capability upgrades on page 1-60
Configuring Rekey Interval	System Configuration page on page 6-39

License keys and regulatory bands

The PTP 670 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 670 provides a choice between the available bands. In each regulatory band, PTP 670 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.

Caution

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

Attention

Pour éviter une éventuelle sanction par le régulateur du pays, utiliser toujours nos liaisons radiofréquences conformément à la réglementation locale.

Further reading

For information about...	Refer to...
Planning PTP 670 links to conform to the regulatory band restrictions	Radio spectrum planning on page 3-20
Radio regulations in the country of operation	Compliance with radio regulations on page 4-26
How to generate a license key for the country of operation	Generating license keys on page 6-3
How to configure the regulatory band	Wireless Configuration page on page 6-25
How to view the regulatory band	System Status page on page 7-3
Regulatory band alarms	Alarms on page 7-20

Designing PTP networks

Using Dynamic Spectrum Optimization

The Dynamic Spectrum Optimization (DSO) feature allows a PTP 670 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 670 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 670 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.

Caution

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 (1 pps) 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 1 pps output on its Aux port, and one ODU configured to receive the 1 pps 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.

Further reading

For information about...	Refer to...
The PTP-SYNC unit	PTP-SYNC unit on page 2-39
Trimble GPS and UGPS receivers	GPS receivers on page 2-45
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 GPS receivers	GPS receiver location on page 3-15
Use of LINKPlanner for TDD synchronization	LINKPlanner for synchronized networks on page 3-25
TDD synchronization methods that may be implemented using PTP-SYNC	Configuration options for TDD synchronization on page 3-31
TDD frame duration in HCMP topology	Data capacity in HCMP topology on page 3-120
How to install a PTP-SYNC unit	Installing a PTP-SYNC unit on page 5-25

For information about...	Refer to...
How to install the Trimble GPS receiver	Installing the Trimble Accutime GPS receiver on page 5-29
How to enable TDD synchronization	Wireless Configuration page on page 6-25
How to configure TDD synchronization	TDD synchronization page (optional) on page 6-33
How to view TDD synchronization status	System Status page on page 7-3
TDD synchronization alarms	Alarms on page 7-20
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 670 ODU processes Ethernet data, and how Ethernet ports are allocated to the Data Service, Second Data Service, Management Service and Local Management Service.

Ethernet ports

The PTP 670 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 Power Injector 56V, 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 670 Series ODU supports four 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. In the HCMP topology, the Data Service additionally provides bridging between Ethernet ports at the same ODU.
- **Second Data Service**: This optional point-to-point transparent service offers a second virtual circuit for customer's data between one of the Ethernet ports at the local ODU and one of the Ethernet ports at an associated remote ODU. The Data Service and Second Data Service are always mapped to different ports at an ODU. The Data traffic of the two services are distinct and are separately bridged to the appropriate configured remote ODU port. The Second Data Service is not supported in the HCMP topology.
- **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 1-32.
A more detailed description of the Second Data Service	Second Data Service on page 1-34.
A more detailed description of the Out-of-Band Management Service	Out-of-Band Management Service on page 1-36.
SFP optical or copper module kits	SFP module kits on page 2-36
The PSU, AUX and SFP ports of the ODU	ODU interfaces on page 2-9
Diagrams showing Ethernet connections	Typical deployment on page 3-2
How to plan the use of Ethernet ports for customer and management traffic	Ethernet interfaces on page 3-36
How to install the Ethernet interfaces to the ODU	Installing the copper Cat5e Ethernet interface on page 5-14 Installing an SFP Ethernet interface on page 5-25 Installing an Aux Ethernet interface on page 5-54
How to configure the ODU Ethernet ports	Interface Configuration page on page 6-16 LAN Configuration page on page 6-43
Ethernet port status attributes	Ethernet / Internet on page 7-8
Ethernet port alarms	Alarms on page 7-20

Ethernet switching

PTP topology

When configured for the PTP topology, the ODU provides flexible interconnection of customer data and network management using several Ethernet ports, but it does not provide Ethernet bridging between the wired Ethernet ports of the same ODU.

One Ethernet port must be allocated to the Data Service. If the Management Service is configured for In-Band Management, then these two services share the same Ethernet Port.

If the Second Data Service or Out of Band Management are configured, one Ethernet port must be allocated to these services.

Up to two ports can be allocated to the Local Management Service.

HCMP topology

When configured for the HCMP topology, the ODU provides conventional Ethernet bridging between wired Ethernet ports configured for the same service, using an embedded Ethernet switch.

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 670 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 Aux port to the customer data network at the other end of the link.

In the HCMP topology, more than one port may be allocated to the Data Service.

Layer two control protocols

The Data Service in the PTP 670 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 670 Series does not generate or respond to any L2CP traffic.

Quality of service for bridged Ethernet traffic

In the PTP wireless topology, the PTP 670 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 670 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 670 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 670 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 670 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 670 does not support Data port wireless link down alert in the HCMP topology.

Lowest Data Modulation Mode

The PTP 670 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 670 customer data networks	Data network planning on page 3-36
How to configure the Ethernet service	LAN Configuration page on page 6-43
How to configure Ethernet quality of service	QoS Configuration page on page 6-56
How to monitor Ethernet performance	System statistics on page 7-54

Second Data Service

Note

PTP 670 does not support the Second Data Service in the HCMP topology.

Transparent Ethernet service

The PTP 670 Series provides an optional second Ethernet data service between one of the Ethernet ports at a local ODU and one of the Ethernet ports at an associated remote ODU. The Ethernet service is based on conventional layer two transparent bridging. The PTP 670 maintains complete separation between Ethernet traffic in the data service and the second data 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 second data service is 2000 bytes.

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

Layer two control protocols

The Second Data Service in the PTP 670 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 670 Series does not generate or respond to any L2CP traffic.

Quality of service for bridged Ethernet traffic

The PTP 670 Series supports a single traffic queue in the Second Data 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 670 Series Second Data Service are always fragmented for transmission over the wireless link, even when the single queue for the Second Data Service has higher priority than all of the data service queues.

Second Data port wireless link down alert

The PTP 670 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 Second Data Service. 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 Second Data Modulation Mode

The PTP 670 ODU can be configured to discard Ethernet frames in the Second Data Service when the modulation mode is lower than the configured Lowest Second 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 Second 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 Second 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 670 customer data networks	Data network planning on page 3-36
How to configure the Ethernet Second Data Service	LAN Configuration page on page 6-43

For information about...	Refer to...
How to configure Ethernet quality of service	QoS Configuration page on page 6-56
How to monitor Ethernet performance	System statistics on page 7-54

Out-of-Band Management Service

Transparent Ethernet service

The PTP 670 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 670 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 670 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 670 Series does not generate or respond to any L2CP traffic.

Quality of service for bridged Ethernet traffic

The PTP 670 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 670 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 670 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 1-33.

Further reading

For information about...	Refer to...
Factors to be considered when planning PTP 670 management data networks	Data network planning on page 3-36
How to configure the Ethernet service	LAN Configuration page on page 6-43
How to configure Ethernet quality of service	QoS Configuration page on page 6-56
How to monitor Ethernet performance	System statistics on page 7-54

Ethernet loopback mode

Note

PTP 670 does not support the Ethernet loopback mode in the HCMP topology.

PTP 670 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 670 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 670 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 6-43

Protocol model for PTP topology

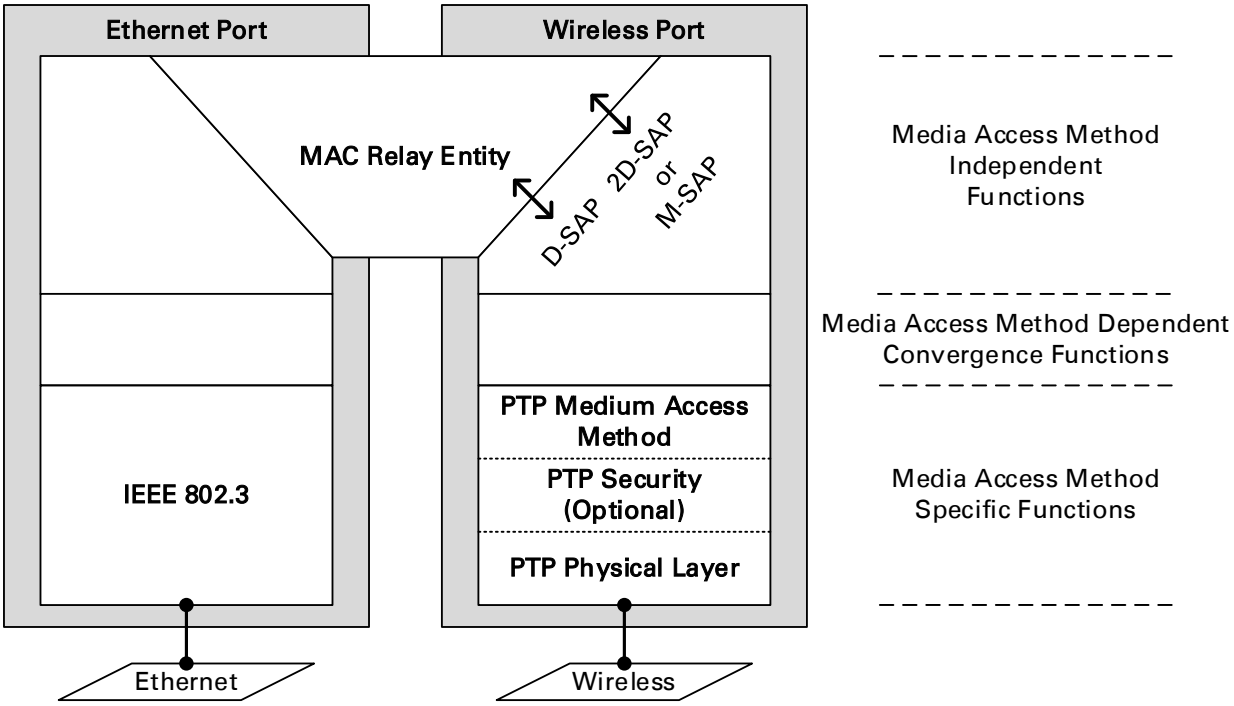
Ethernet bridging behavior at each end of the wireless link is equivalent to a two-port, managed, transparent MAC bridge where the two ports are a wired Ethernet port allocated to the Data Service, Second Data Service, Out-of-Band Management Service, and the Wireless port.

Frames are transmitted at the Wireless port over a proprietary point-to-point circuit-mode link layer between ends of the PTP 670 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 either the Second Data Service or 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.

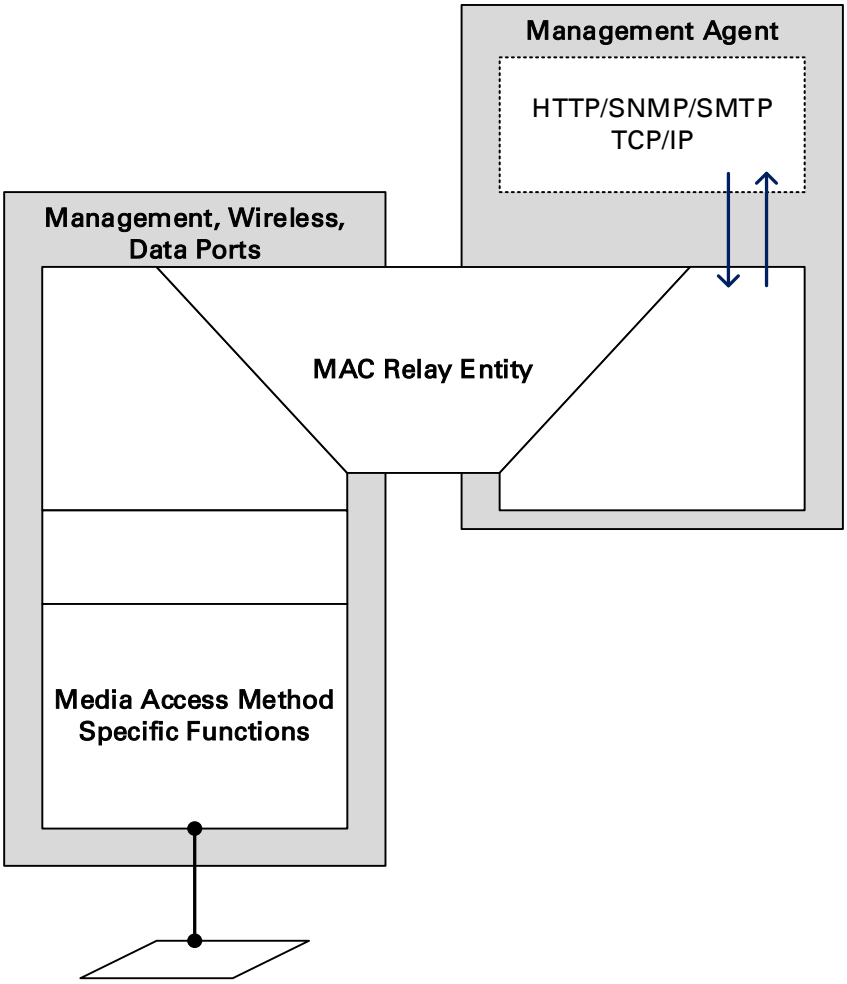
Protocol layers involved in bridging between Ethernet and wireless interfaces are shown in Figure 4. Protocol layers involved in bridging between external interfaces and the management agent are shown in Figure 5. In these figures, the layers have the meanings defined in IEEE 802.1Q-2005.

Figure 4 Protocol layers between Ethernet and wireless interfaces



D-SAP = Data Service Access Point
2D-SAP = Second Data Service Access Point
M-SAP = Management Service Access Point

Figure 5 Protocol layers between external interfaces and the management agent



Further reading

For information about...	Refer to...
Layer two control protocols (L2CPs) identified by PTP 670	Layer two control protocols on page 3-36

Synchronous Ethernet

Note

PTP 670 does not support Synchronous Ethernet in the HCMP topology.

PTP 670 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 670 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 670 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 670 does not support Synchronous Ethernet on a copper SFP module.

Further reading

For information about...	Refer to...
Relationship between synchronous Ethernet and TDM	TDM description on page 1-43
Availability of synchronous Ethernet	Capability upgrades on page 1-60
Relationship between synchronous Ethernet and Ethernet port allocation	Additional port allocation rules on page 3-45
How to configure synchronous Ethernet	LAN Configuration page on page 6-43
Upgrading to synchronous Ethernet	Generating license keys on page 6-3
Synchronous Ethernet status indicators	Synchronous Ethernet on page 7-12
Synchronous Ethernet alarms	Alarms on page 7-20
Synchronous Ethernet status	SyncE Status page on page 7-70

IEEE 1588-2008 Transparent Clock

Note

PTP 670 does not support IEEE 1588-2008 Transparent Clock in the HCMP topology.

PTP 670 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 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 670 uses the Synchronous Ethernet clock to increase the accuracy of 1588 residence time measurements.

Note

PTP 670 does not support IEEE 1588 Transparent Clock on a copper SFP module.

Further reading

For information about...	Refer to...
Relationship between IEEE 1588-2008 Transparent Clock and TDM	TDM description on page 1-43
Availability of IEEE 1588-2008 Transparent Clock	Capability upgrades on page 1-60
Relationship between IEEE 1588-2008 Transparent Clock and Ethernet port allocation	Additional port allocation rules on page 3-45
Relationship between IEEE 1588-2008 Transparent Clock and VLAN membership	VLAN membership on page 3-50
Upgrading to IEEE 1588-2008	Generating license keys on page 6-3
How to configure IEEE 1588-2008 Transparent Clock	LAN Configuration page on page 6-43
IEEE 1588-2008 Transparent Clock status indicators	Synchronous Ethernet on page 7-12
IEEE 1588-2008 Transparent Clock alarms	Alarms on page 7-20

TDM bridging

Note

PTP 670 does not support TDM bridging in the HCMP topology.

This section describes how TDM traffic (E1 or T1) may be carried over PTP 670 links.

If a NIDU is installed at each link end, the PTP 670 link supports up to eight E1 channels or up to eight T1 channels. The link relays unstructured E1 or T1 data and provides accurate timing transfer.

TDM description

PTP 670 Series bridges up to eight E1 or T1 telecoms circuits over a single-hop PTP 670 wireless link using the optional Network Indoor Unit (NIDU). The NIDU provides the eight TDM interfaces on individual RJ45/RJ48 connectors, together with an Ethernet interface to the operator's data network and a separate Ethernet interface to the PTP 670 Series ODU. One NIDU is required at each end of the link. It operates from a 48 V DC power supply.

TDM circuits established using the NIDUs are structure agnostic, meaning that the circuits can bridge framed or unframed data.

The NIDUs are tightly integrated with associated ODUs providing for simple configuration, accurate timing transfer, low and predictable latency, high efficiency, quick settling time, and a timing-only mode that maintains timing transfer when the wireless link has insufficient capacity to bridge the configured TDM data.

Through timing

TDM bridging in the PTP 670 series uses the "through timing" model. In other words, the clock frequency used for transmitting TDM data is, on average, exactly the same as the clock frequency received at the corresponding TDM port at the remote end of the link. The wander and jitter in the transmit clock complies with applicable requirements of ITU-T G.823 and G.824 without additional external frequency references. Timing transfer is independent between individual circuits, and between transmit and receive directions of the same circuit.

NIDUs and TDM

TDM circuits in PTP 670 span a single wireless link. To transmit TDM data across a network segment consisting of several wireless links, use one pair of NIDUs for each wireless link, and interconnect the TDM ports at relay sites.

The NIDU is not a general-purpose TDM multiplexer, and will not interwork with standards-based products from other manufacturers. The NIDU does not support (and does not need to support) internal, external or loop timing modes. The NIDU does not accept (or need) an external frequency reference.

The NIDU is not separately managed, and it does not have an IP address. Instead, the ODU is used to configure and monitor the associated NIDU through the standard HTTP/HTTPS, SNMP, SMTP and syslog interfaces already used by the ODU.

The NIDU always connects to the ODU using the Main PSU port of the ODU. This constrains the flexible allocation of ports to services somewhat.

Timing transfer for TDM circuits

Accurate timing transfer for TDM circuits in the PTP 670 Series is based on the same underlying technology as the IEEE 1588 Transparent Clock and Synchronous Ethernet features. Consequently, the IEEE 588 and Synchronous Ethernet features are not available when TDM bridging is enabled. Similarly, TDM bridging is not available if either IEEE 1588 or Sync E is in use. The Adaptive setting for Link Symmetry is not compatible with TDM bridging.

TDM bridging is a licensed feature, and may require an optional upgrade for the ODU firmware.

Lowest TDM modulation mode

In narrow channel bandwidths and lower modulation modes, the link may have insufficient capacity to relay the E1/T1 payload; in this case, the wireless link continues to carry timing information in order to maintain accurate clock synchronization. The relay of TDM data resumes automatically when the link reaches a suitable modulation mode.

Links that are able to operate consistently in a high modulation mode can take advantage of lower link latency. This option is configured by setting the "Lowest TDM Modulation Mode" during installation. Appropriate settings for this control may be determined by using the LINKPlanner tool. The reduction in latency is achieved by disabling the relay of TDM data in lower modulation modes, and this necessarily results in somewhat lower availability for the TDM circuit. The loss of availability can be estimated using the LINKPlanner.

The unit will override the user setting of Lowest TDM Modulation Mode if the selected mode has insufficient capacity to carry the TDM data, or if the mode demands very high latency and requires more buffering than the link can provide.

Fixed frequency operation

In the PTP 670 link, data errors may occur during channel changes on an operational link. It may be appropriate to minimize channel-change-related errors in a link carrying TDM traffic by preventing channel changes initiated by DSO. This can be achieved by barring all channels except one in the Spectrum Expert or Spectrum Management pages, or alternatively by selecting Fixed Frequency mode. These steps unavoidably disable interference avoidance mechanisms, and should not be taken if the risk of errors due to interference is more severe than the risk due to channel changes.

Fixed frequency operation is not available when radar detection requirements exist in the frequency band. Channel barring is allowed in radar regions, but it is unwise to bar all channels except one, as any radar signals detected on that channel will drop the link for up to 30 minutes.

Ethernet cables for TDM

The Ethernet cables from the ODU via the PSU to the NIDU must be capable of supporting operation at 1000BASE-T. If the ODU port has negotiated a link at 100BASE-T, the NIDU will not send or receive TDM data and will not bridge customer data traffic.

Further reading

For information about...	Refer to...
The hardware required to implement TDM	Network indoor unit (NIDU) on page 2-47
A typical E1 or T1 site deployment	E1 or T1 interfaces on page 3-5
Where to locate the NIDU	NIDU location on page 3-16
TDM interface specifications	Ethernet interfaces on page 3-36
The effect of TDM on data throughput	TDM traffic load on page 3-127
How to install TDM hardware	Installing a NIDU on page 5-39
How to generate TDM (E1 or T1) license keys	Generating license keys on page 6-3
How to install TDM license keys (part of the Installation Wizard)	Software License Key page on page 6-13
How to enable E1 or T1 and configure TDM channels (part of the Installation Wizard)	Interface Configuration page on page 6-16
How to configure NIDU LAN port auto-negotiation	LAN Configuration page on page 6-43
How to configure TDM channels and initiate loopback tests (after installation)	TDM Configuration page on page 6-62
How to enable TDM alarms	Diagnostic Alarms page on page 6-83
The meaning of TDM status attributes	System Status page on page 7-3
The meaning of TDM alarms	Alarms on page 7-20
How to check the NIDU LEDs, perform a TDM loopback test, and check for 1000BASE-T	Testing a TDM link on page 8-18
To find the latency of a TDM link	System Status page, TDM Latency attribute (Table 205) Alternatively, use LINKPlanner

System management

This section introduces the PTP 670 management system, including the web interface, installation, configuration, alerts and upgrades.

Management agent

PTP 670 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 1-47.

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

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

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

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

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

Note

PTP 670 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 670 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 670 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 670 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 3-50
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 6-25
Planning VLAN membership	VLAN membership on page 3-50
How to configure VLAN for the management interface	Interface Configuration page on page 6-16 LAN Configuration page on page 6-43
Planning the Ethernet and IP (DSCP) priority	Priority for management traffic on page 3-50
Planning the use of Ethernet ports for customer and management traffic	Additional port allocation rules on page 3-45

IPv6

The PTP 670 management agent supports the following IPv6 features:

Neighbor discovery

PTP 670 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 670 sends router solicitations, but does not process router advertisements.

Path MTU discovery and packet size

PTP 670 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 670 supports ICMPv6 as specified in RFC 4443. PTP 670 does not support RFC 4884 (multi-part messages).

Addressing

The PTP 670 management agent is compatible with the IPv6 addressing architecture specified in RFC 4291. PTP 670 allows static configuration of the following:

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

PTP 670 additionally assigns an automatically configured Link Local address using stateless address auto-configuration (SLAAC) as specified in RFC 4862. PTP 670 does not assign a global unicast IP address using SLAAC.

PTP 670 responds on the standard management agent interfaces (HTTP, HTTPS, syslog, Telnet, SNMP, SMTP, SNTP) using the global unicast address.

Privacy extensions

PTP 670 does not support the privacy extensions specified in RFC 4941.

DHCPv6

PTP 670 does not support address assignment using DHCPv6. The address of the management agent must be configured statically.

Multicast listener discovery for IPv6

The PTP 670 management agent supports Multicast Listener Discovery version 1 (MLDv1) as specified in RFC 2710.

PTP 670 does not support Multicast Listener Discovery version 2 (MLDv2).

Textual representation of IPv6 addresses

PTP 670 allows users to input text-based IP addresses in any valid format defined in RFC 5952. IPv6 addresses are automatically converted by PTP 670 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 670 does not support IP security (IPsec).

Further reading

For information about...	Refer to...
Planning the IPv6 interface	IP interface on page 3-50
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 6-43

Web server

The PTP 670 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 670 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 670.

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 670.
- **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 670 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 670 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 670 unit. PTP 670 supports certificates with 2048-bit key size.

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

Note

The PTP 670 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 670 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 670 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 670 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 670 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 670 allows the role-based and identity-based passwords for the web-based interface to be updated using the proprietary SNMP MIB. This capability is controlled by the SNMP Control of Passwords, and is disabled by default.

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

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 3-56
How to configure user accounts	Local User Accounts page on page 6-72

RADIUS authentication

PTP 670 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 670 supports connections to primary and secondary RADIUS servers. The RADIUS interface is configured through the RADIUS Authentication page of the web-based interfaces.

PTP 670 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 670 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 670 is configured for Identity-based User Accounts.

Further reading

For information about...	Refer to...
How to plan the use of RADIUS	Planning for RADIUS operation on page 3-63
How to configure RADIUS.	RADIUS Configuration page on page 6-77

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 670 Series proprietary MIB.

Further reading

For information about...	Refer to...
How to plan for SNMPv1/2c	Planning for SNMP operation on page 3-54
How to enable SNMP control of HTTP, Telnet and passwords	Web-Based Management page on page 6-70 HTTP and Telnet options on page 6-113
How to configure SNMPv1 or SNMPv2c	SNMP pages (for SNMPv1/2c) on page 6-99
How to upgrade software remotely using Trivial FTP (TFTP) triggered by SNMP	Upgrading software using TFTP on page 6-127

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 670 can be configured to authenticate received NTP messages using an MD5 signature.

Further reading

For information about...	Refer to...
How to plan for SNTP operation	Planning for SNTP operation on page 3-56
How to configure SNTP	Time Configuration page on page 6-84

SNMPv3 security

SNMP Engine ID

PTP 670 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 670 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 670 AES upgrade described in AES license on page 1-57.

View-based access control model

PTP 670 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 670. It is not possible to read or modify AES keys used to encrypt data transmitted at the wireless interface. Neither is it possible to read or modify security parameters associated with TLS protection of the web-based management interface. The recovery mode option to zeroize CSPs does not affect SNMPv3 configuration.

MIB-based management of SNMPv3 security

PTP 670 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 670 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 3-62.

PTP 670 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 1-54. 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 670 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 670 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 rest 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 3-60
How to configure SNMPv3	SNMP pages (for SNMPv3) on page 6-90

System logging (syslog)

PTP 670 supports the standard syslog protocol to log important configuration changes, status changes and events. The protocol complies with RFC 3164.

PTP 670 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 670 additionally creates syslog messages for changes in any status variable displayed in the web-based interface.

PTP 670 creates syslog messages on a number of events (for example successful and unsuccessful attempts to log in to the web-based interface).

PTP 670 can be configured to send syslog messages to one or two standard syslog servers.

Additionally, PTP 670 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 6-88
Syslog alarms	Alarms on page 7-20
How to view the local log of event messages	Syslog page on page 7-25
How to interpret syslog messages	Format of syslog server messages on page 7-25

AES license

PTP 670 provides optional encryption using the Advanced Encryption Standard (AES). Encryption is not available in the standard PTP 670 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 670 license key.

Further reading

For information about...	Refer to...
General description of wireless encryption in PTP 670	Wireless encryption on page 1-21
Capability upgrades for AES	Capability upgrades on page 1-60
AES and HTTPS/TLS operation	Planning for HTTPS/TLS operation on page 3-59
AES and SNMPv3 operation	Planning for SNMPv3 operation on page 3-60
How to generate an AES license key	Generating license keys on page 6-3
How to enable AES capability	Software License Key page on page 6-13
How to configure AES encryption	System Configuration page on page 6-39
How to configure security with AES	Security menu on page 6-103

Critical security parameters

The critical security parameters (CSPs) are as follows:

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

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 6-117
How to zeroize CSPs (recovery mode)	Zeroize Critical Security Parameters on page 7-83

Software upgrade

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

PTP 670 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.

Caution

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

Caution

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 6-68
How to upgrade software remotely using Trivial FTP (TFTP) triggered by SNMP	Upgrading software using TFTP on page 6-127

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 670 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 670 Connectorized ODU	PTP 670 Connectorized ODU on page 2-5
Capabilities of the PTP 670 Integrated ODU	PTP 670 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 6-3
How to install capability upgrades	Software License Key page on page 6-13

Recovery mode

The PTP 670 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 7-77

Chapter 2: System hardware

This chapter describes the hardware components of a PTP 670 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.

Hardware platform variants

PTP 670 ODUs are available in two different hardware platform variants:

- PTP 670 Integrated ODU
- PTP 670 Connectorized ODU

Regional variants

Each of the PTP 670 hardware platform variants is available in five different regional variants. The regional variants are supplied with default country licenses as follows:

- FCC: “USA” country license with regulatory bands:
  - 1 “5.8 GHz FCC”
  - 9 “5.4 GHz USA (New Rules)”
  - 14 “4.9 GHz Public Safety, USA/Canada”
  - 38 “5.2 GHz FCC U-NII 2A”
  - 84 “5.1 GHz FCC U-NII 1”
- RoW: “Other” country license with regulatory bands:
  - 8 “5.4 GHz unrestricted”
  - 35 “5.8 GHz unrestricted”
  - 61 “4.9 GHz unrestricted”
  - 62 “5.2 GHz unrestricted”
- EU: “EU” country license with regulatory band:
  - 26 “5.4 GHz ETSI”
- IC: “Canada” country license with regulatory bands:
  - 1 “5.8 GHz FCC”
  - 13 “5.4 GHz FCC U-NII 2C”
  - 14 “4.9 GHz Public Safety, USA/Canada”
  - 38 “5.2 GHz FCC U-NII 2A”
  - 84 “5.1 GHz FCC U-NII 1”
- Mexico: “Mexico” country license:
  - 13 “5.4 GHz Canada”
  - 59 “5.8 GHz Mexico”
  - 65 “5.1 GHz Colombia/Denmark/Kenya/Mexico”
  - 68 “5.2 GHz Colombia/Mexico”

- 96 “4.8 GHz Mexico” (4.8 to 5.9 GHz frequency variant only)

For details of how to configure the ODUs to operate with other country licenses, refer to Generating license keys on page 6-3 and Software License Key page on page 6-13. The list of available countries depends upon the regional variant. The list of available regulatory bands depends on the country.

PTP 670 Integrated ODU

The PTP 670 Integrated ODU is attached to a 23 dBi flat plate antenna (Figure 6 and Figure 7) and is intended for medium to long-range difficult links and traditional backhaul requirements where high capacity and high link budget are required. The integrated antenna offers a convenient and easily-deployed solution where the additional gain of external antennas is not needed.

Figure 6 PTP 670 (4.8 to 5.9 GHz) Integrated ODU (front and rear views)

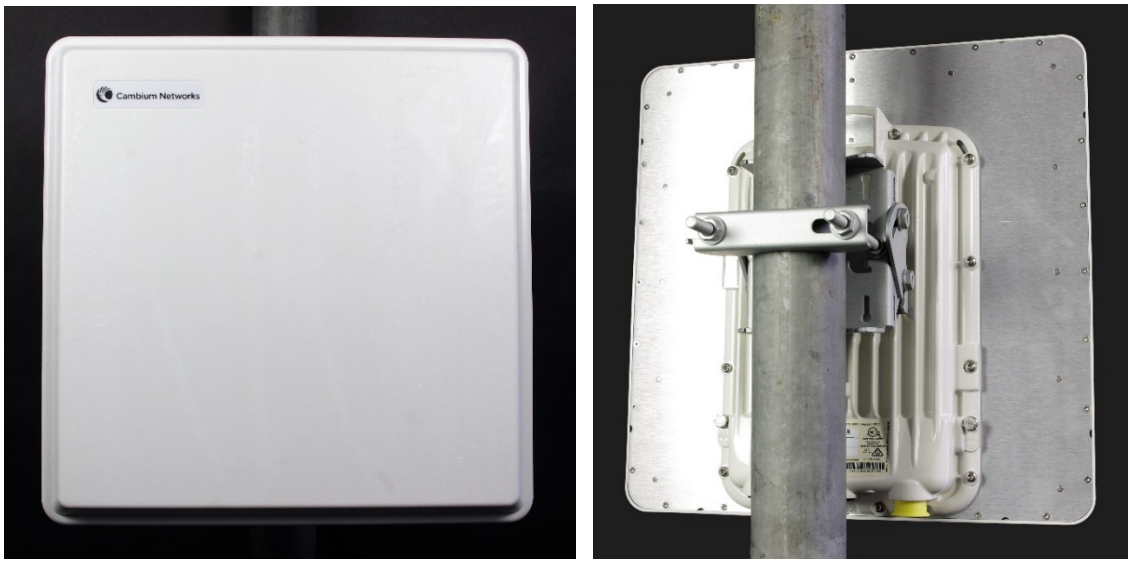


Figure 7 PTP 670 (4.9 to 6.05 GHz) Integrated ODU (front and rear views)

Capability licensing

PTP 670 ODUs support the following capability upgrades (see ODU capability upgrades on page 2-7):

- SFP port operation
- AES encryption
- Synchronous Ethernet and 1588 Transparent Clock
- TDM (E1 or T1) operation
- High Capacity Multipoint (HCMP) Master
- Over-the-air rekeying

Individual ODU part numbers

Order PTP 670 Integrated ODUs from Cambium Networks (Table 4). ODUs are supplied without mounting brackets.

Table 4 PTP 670 Integrated individual ODU part numbers

Cambium description	Cambium part number
PTP 670 (4.9 to 6.05 GHz) Integrated 23 dBi ODU (FCC)	C050067B001A
PTP 670 (4.9 to 6.05 GHz) Integrated 23 dBi ODU (ROW)	C050067B004A
PTP 670 (4.9 to 6.05 GHz) Integrated 23 dBi ODU (EU)	C050067B007A
PTP 670 (4.9 to 6.05 GHz) Integrated 23 dBi ODU (IC)	C050067B010A
PTP 670 (4.8 to 5.9 GHz) Integrated 23 dBi ODU (Mexico)	C050067B021A

ODU kit part numbers

Order PTP 670 Integrated ODU kits from Cambium Networks (Table 5).

Each of the parts listed in Table 5 includes the following items:

- One Integrated ODU
- One AC Power Injector 56V or one AC+DC Enhanced Power Injector 56V PSU.
- One line cord, either US or EU as indicated.
- One Tilt Bracket Assembly (Figure 9).

Table 5 ODU kit part numbers for Integrated ODUs

Cambium description	Cambium part number
PTP 670 Integrated 23dBi END with AC Supply (FCC)	C050067H003A
PTP 670 Integrated 23dBi END with AC+DC Enhanced Supply (FCC)	C050067H004A
PTP 670 Integrated 23dBi END with AC Supply (ROW - U.S. Line Cord)	C050067H009A

Cambium description	Cambium part number
PTP 670 Integrated 23dBi END with AC+DC Enhanced Supply (ROW - U.S. Line Cord)	C050067H010A
PTP 670 Integrated 23dBi END with AC Supply (ROW - EU Line Cord)	C050067H015A
PTP 670 Integrated 23dBi END with AC+DC Enhanced Supply (ROW - EU Line Cord)	C050067H016A
PTP 670 Integrated 23dBi END with AC Supply (EU)	C050067H021A
PTP 670 Integrated 23dBi END with AC+DC Enhanced Supply (EU)	C050067H022A
PTP 670 Integrated 23dBi END with AC Supply (IC)	C050067H027A
PTP 670 Integrated 23dBi END with AC+DC Enhanced Supply (IC)	C050067H028A

PTP 670 Connectorized ODU

The PTP 670 Connectorized ODU is intended to work with separately mounted external antennas (Figure 8). External antennas generally have higher gains than the integrated antennas, allowing the PTP 670 to cope with more difficult radio conditions.

Figure 8 PTP 670 Connectorized ODU (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 3-29.

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

Attention

Pour déterminer si il est nécessaire d'installer une liaison radiofréquence avec des antennes externes et pour calculer leur impact sur les performances de la liaison et les limites réglementaires, voir Planning for connectorized units page 3-29.

Pour sélectionner les antennes, câbles et connecteurs RF pour les liaisons radiofréquence sans antenne intégrée, voir Antennas and antenna cabling page 2-21.

Capability licensing

PTP 670 ODUs support the following capability upgrades (see ODU capability upgrades on page 2-7):

- SFP port operation
- AES encryption
- Synchronous Ethernet and 1588 Transparent Clock
- TDM (E1 or T1) operation
- High-Capacity Multipoint (HCMP) Master
- Over-the air rekeying

Individual ODU part numbers

Order PTP 670 Connectorized ODUs from Cambium Networks (Table 6). ODUs are supplied without mounting brackets.

Table 6 PTP 670 Connectorized individual ODU part numbers

Cambium description	Cambium part number
PTP 670 (4.9 to 6.05 GHz) Connectorized ODU (FCC)	C050067B003A
PTP 670 (4.9 to 6.05 GHz) Connectorized ODU (ROW)	C050067B006A
PTP 670 (4.9 to 6.05 GHz) Connectorized ODU (EU)	C050067B009A
PTP 670 (4.9 to 6.05 GHz) Connectorized ODU (IC)	C050067B012A
PTP 670 (4.8 to 5.9 GHz) Connectorized ODU (Mexico)	C050067B022A

ODU kit part numbers

Order PTP 670 Connectorized ODU kits from Cambium Networks (Table 7).

Each of the parts listed in Table 7 includes the following items:

- One Connectorized ODU.

- One AC Power Injector 56V or one AC+DC Enhanced Power Injector 56V PSU.
- One line cord, either US or EU as indicated.
- One Tilt Bracket Assembly (Figure 9).

Table 7 ODU kit part numbers for Connectorized ODUs

Cambium description	Cambium part number
PTP 670 Connectorized END with AC Supply (FCC)	C050067H001A
PTP 670 Connectorized END with AC+DC Enhanced Supply (FCC)	C050067H002A
PTP 670 Connectorized END with AC Supply (ROW - U.S. Line Cord)	C050067H007A
PTP 670 Connectorized END with AC+DC Enhanced Supply (ROW - U.S. Line Cord)	C050067H008A
PTP 670 Connectorized END with AC Supply (ROW - EU Line Cord)	C050067H013A
PTP 670 Connectorized END with AC+DC Enhanced Supply (ROW - EU Line Cord)	C050067H014A
PTP 670 Connectorized END with AC Supply (EU)	C050067H019A
PTP 670 Connectorized END with AC+DC Enhanced Supply (EU)	C050067H020A
PTP 670 Connectorized END with AC Supply (IC)	C050067H025A
PTP 670 Connectorized END with AC+DC Enhanced Supply (IC)	C050067H026A

ODU capability upgrades

To upgrade a PTP 670 ODU to one or more new capabilities, order the necessary upgrades from Cambium Networks (Table 8). For details of how to install the capability upgrades, refer to Generating license keys on page 6-3 and Software License Key page on page 6-13.

Table 8 Capability upgrades available for PTP 670 Series ODUs

Cambium description (*1)	Part number
8-Port T1/E1 Software License (per END).	C000065K049A
PTP 650/670 128-bit AES Encryption – per ODU (*2)	C000065K018A
PTP 650/670 256-bit AES Encryption – per ODU (*2)	C000065K019A
PTP 650/670 Precise Network Timing Software License (per END)	C000065K040A
PTP 670 Basic High-Capacity Multipoint – per Access Point	C000067K001A
PTP 670 OTAR support – per END (*3)	C000067K002A

(*1) Order two upgrades per link.

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

(*3) Order one upgrade for every ODU that will be used as a TDD Master.

ODU accessories

Spare ODU port blanking plugs are available from Cambium Networks (Table 9).

Table 9 ODU accessory part numbers

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

ODU mounting brackets

The Tilt Bracket Assembly (Figure 10) and Mounting Bracket (Integrated) bracket (Figure 9) are used to mount a PTP 670 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 10).

Figure 9 ODU Tilt Bracket Assembly

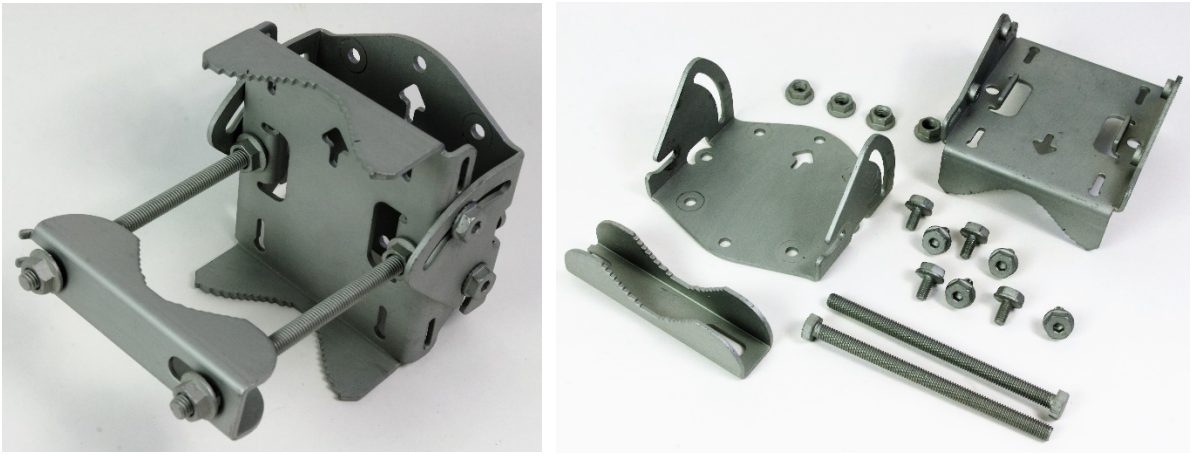


Figure 10 ODU Mounting Bracket (Integrated)

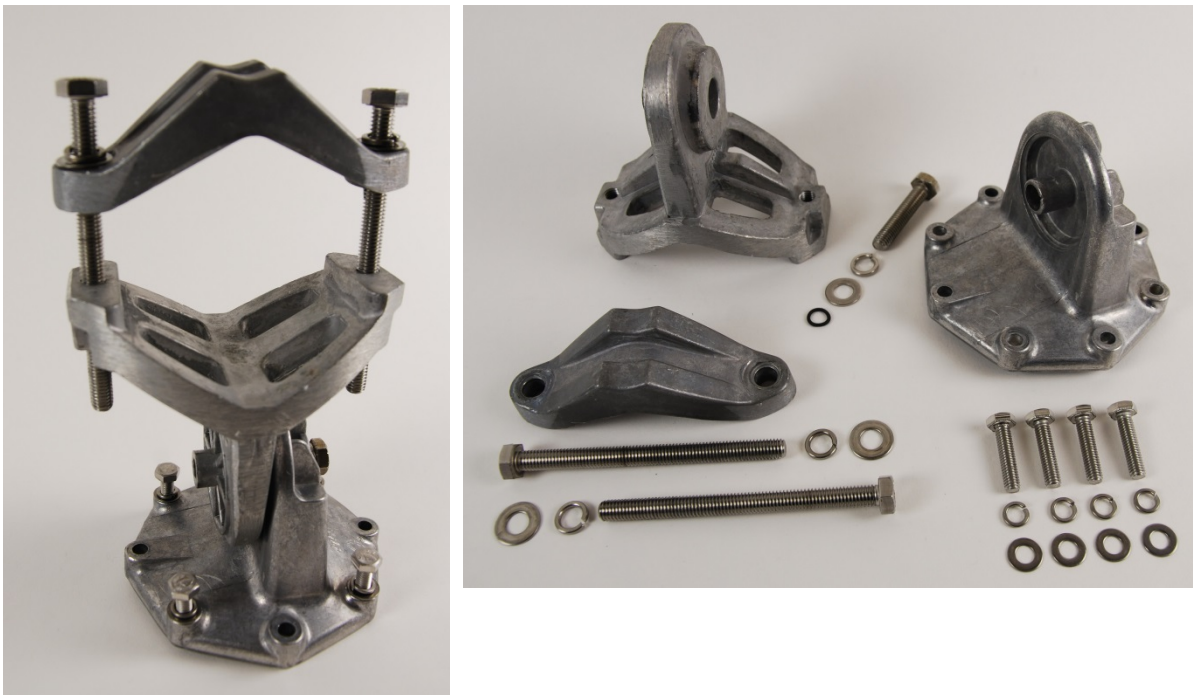


Table 10 ODU mounting bracket part numbers

Bracket	ODU variants	Bracket part number
Tilt Bracket Assembly	PTP 670 Integrated PTP 670 Connectorized	N000045L002A
Mounting Bracket (Integrated)	PTP 670 Integrated	N000065L031A

ODU interfaces

The PSU, AUX and SFP ports are on the rear of the ODUs (Figure 11). These interfaces are described in Table 11. 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
- Second Data Service
- Management Service
- Local Management Service

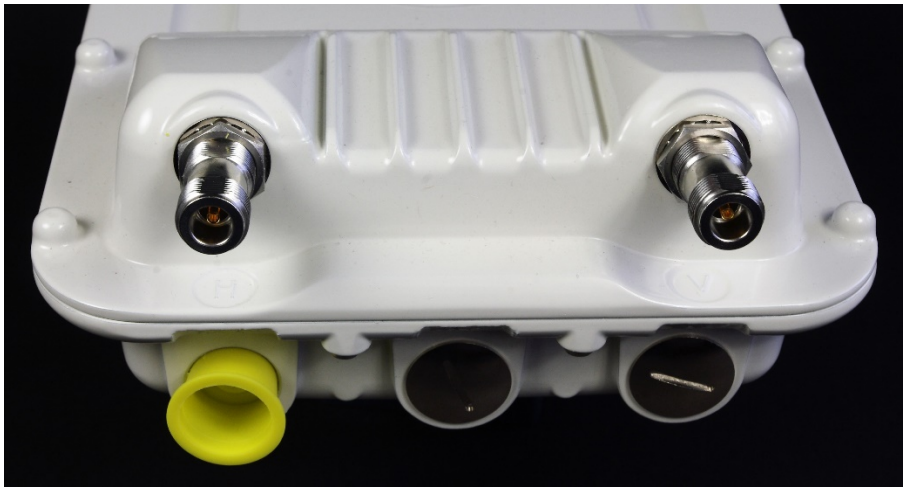
Figure 11 ODU rear interfaces

Table 11 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 12) provides N type female connectors for RF cable interfaces to antennas with horizontal (H) and vertical (V) polarization.

Figure 12 Connectorized ODU antenna interfaces



ODU specifications

The PTP 670 ODU conforms to the specifications listed in Table 12.

Table 12 ODU specifications

Category	Specification
Dimensions	Integrated: 371 mm (14.6 in) x 371 mm (14.6 in) x 81 mm (3.2 in) Connectorized: 204 mm (8.0 in) x 318 mm (12.5 in) x 98 mm (3.9 in)
Weight	Integrated: 4.1 kg (9.0 lbs) including 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 Power Injector 56V (Figure 13) supplies a single ODU, accepts an AC input supply only. The AC Power Injector 56V is approved for use only with the 4.9 GHz to 6.05 GHz frequency variant of the ODU.
- The AC+DC Enhanced Power Injector 56V (Figure 14) supplies a single ODU, accepts both AC and DC input, tolerates a greater temperature range, and allows the ODU to support a device on the Aux port, such as a video camera or wireless access point. It also allows the ODU to provide DC power output. 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 15, Figure 16 and Figure 17) 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 670 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 670 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 670.

Figure 13 AC Power Injector 56V

Figure 14 AC+DC Power Injector 56V

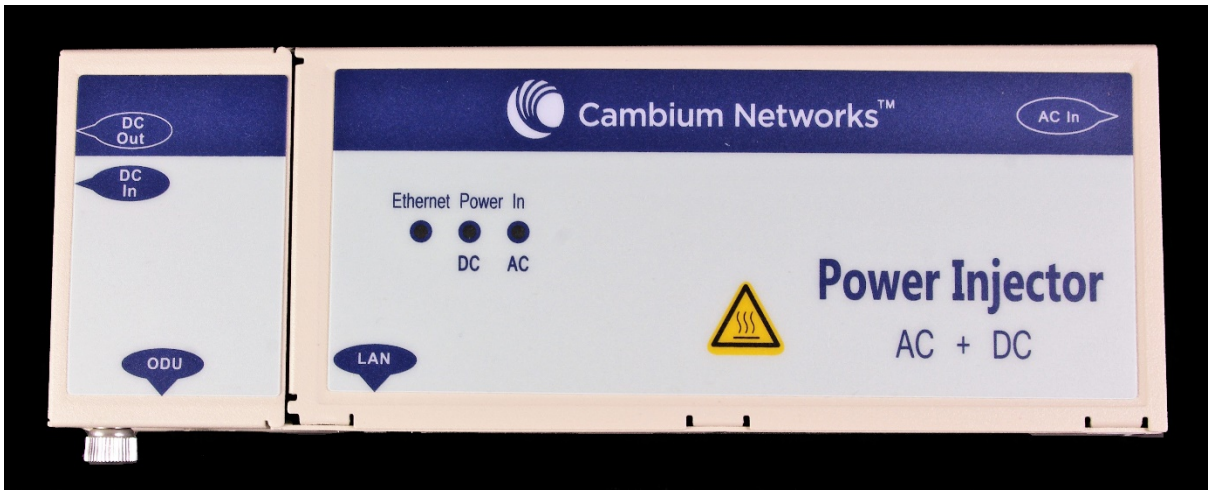


Figure 15 CMM5 Power and Sync Injector

Figure 16 CMM5 Controller

Figure 17 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.

Caution

The PSU ODU ports are designed to connect only to PTP 670 ODUs, PTP-SYNC units, NIDUs 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 670 ODU or LPU.

Note

The AC Power Injector 56V is not approved for use with the 4.8 GHz to 5.9 GHz frequency variant ODUs.

Further reading

For information about...	Refer to...
General description of TDD Synchronization	TDD synchronization on page 1-26
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 13).

Table 13 Power supply component part numbers

Cambium description	Cambium part number
AC+DC Enhanced Power Injector 56V	C000065L002C

Cambium description	Cambium part number
AC Power Injector 56V	N000065L001C
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 Power Injector 56V interfaces

The AC Power Injector 56V interfaces are shown in Figure 18 and described in Table 14.

Figure 18 AC Power Injector 56V interfaces

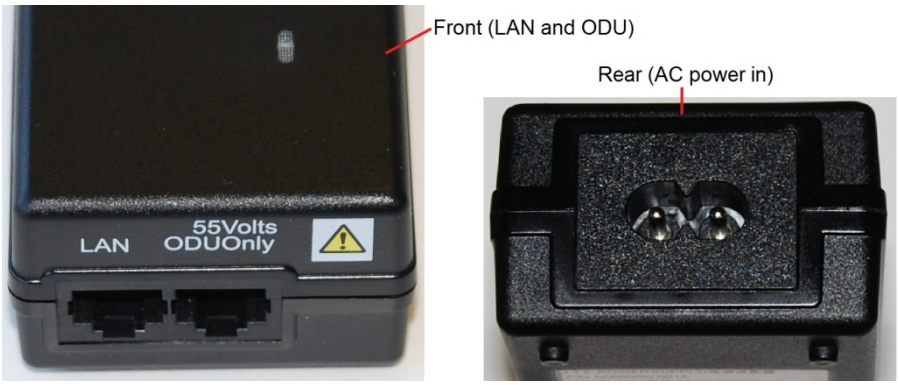


Table 14 AC Power Injector 56V interface functions

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

AC+DC Enhanced Power Injector 56V interfaces

The AC+DC Enhanced Power Injector 56V interfaces are shown in Figure 19 and described in Table 15.

Figure 19 AC+DC Enhanced Power Injector 56V interfaces

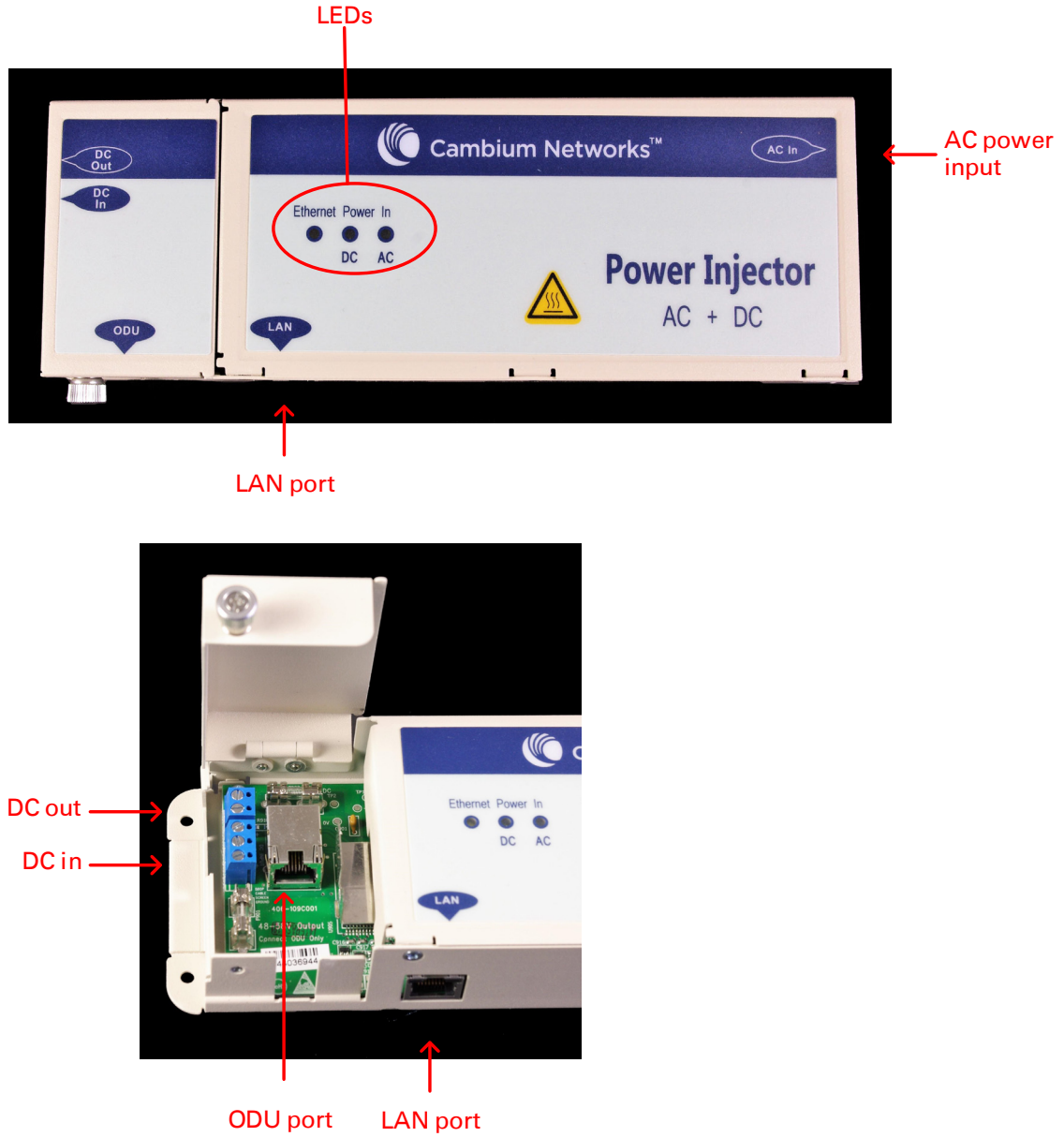


Table 15 AC+DC Enhanced Power Injector 56V interface functions

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) or to a NIDU.

Interface	Function
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
Ethernet (yellow) LED	Ethernet traffic detection

CMM5 Power and Sync Injector interfaces

The CMM5 Power and Sync Injector interfaces are shown in Figure 20 and described in Table 16.

Figure 20 CMM5 Power and Sync Injector interfaces

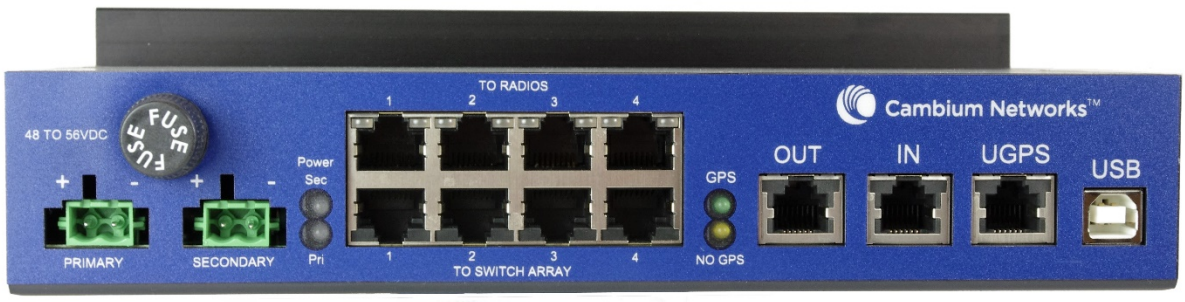


Table 16 CMM5 Power and Sync Injector interface functions

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 Power Injector 56V conforms to the specifications listed in Table 17.

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 17 AC Power Injector 56V specifications

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

Table 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

Category	Specification
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
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. These antennas are not supplied by Cambium Networks.

For connectorized units operating in the USA 4.9 GHz, 5.1 GHz, 5.2 GHz, 5.4 GHz or 5.8 GHz bands, choose external antennas from those listed in FCC approved antennas on page 2-22. Do not install any other antennas.

For connectorized units operating in the Canada 4.9 GHz, 5.1 GHz, 5.2 GHz, 5.4 GHz or 5.8 GHz bands, choose external antennas from those listed in ISEDC approved antennas on page 2-25. Do not install any other antennas.

For links in other countries, the listed antennas are advisory, not mandatory.

Note

To determine when to install connectorized units and to calculate their impact on link performance and regulatory limits, see Planning for connectorized units on page 3-29.

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 2-33 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 670 LPUs) are required for protecting the antenna RF cables at building entry. One arrestor is required per antenna cable. One example of a compatible lightning arrestor is the Polyphaser LSXL-ME or LSXL (not supplied by Cambium Networks).

FCC approved antennas

For connectorized units operating in the USA, choose external antennas from Table 21 (4.9 GHz), Table 22 (5.1 GHz), Table 23 (5.2 GHz), Table 24 (5.4 GHz) or Table 25 (5.8 GHz). These are approved by the FCC for use with the product and are constrained by the following limits for single- or dual-polarization parabolic dish antennas:

- 4.9 GHz – 36.0 dBi per polarization or antenna.
- 5.1 GHz – 34.5 dBi per polarization or antenna.
- 5.2 GHz – 34.5 dBi per polarization or antenna.
- 5.4 GHz – 34.5 dBi per polarization or antenna.
- 5.8 GHz – 38.1 dBi per polarization or antenna.

Caution

Antennas not included in these tables are strictly prohibited for use with the PTP 670 in the specified bands.

Table 21 Antennas permitted for deployment in USA – 4.9 GHz

Manufacturer	Antenna type	Nominal gain (dBi)	Cambium part number
Cambium	6-foot Dual-Pol Parabolic, SPD6-4.7	36.0	RDH4502A
Cambium	6-foot Dual-Pol Parabolic, HPD6-4.7	35.8	RDH4515A
Cambium	4-foot Dual-Pol Parabolic, SPD4-4.7	33.0	RDH4501A
Cambium	4-foot Parabolic, SP4-4.7	33.0	N000000D002A
Cambium	4-foot Dual-Pol Parabolic, HPD4-4.7	32.8	RDH4516A
Cambium	3-foot Dual-Pol Parabolic, SPD3-4.7	30.4	RDH4500A
Cambium	3-foot Dual-Pol Parabolic, HPD3-4.7	30.2	RDH4517A
Cambium	2-foot Dual-Pol Parabolic, SPD2-4.7	27.0	RDH4499A
Cambium	2-foot Parabolic, SP2-4.7	26.9	N000000D001A

Manufacturer	Antenna type	Nominal gain (dBi)	Cambium part number
Cambium	2-foot Dual-Pol Parabolic, HPD2-4.7	26.8	RDH4518A
MARS	MA-WS54-50R Flat Plate (Dual-Pol)	23.0	Integrated
MARS	MA-WA56-DP23G7CM Flat Plate (Dual-Pol)	23.0	Integrated
Cambium	1-foot Dual-Pol Parabolic, HPLPD1-4.7	20.8	RDH4519A
Cambium	90 4.9 - 6 GHz, 90/120 deg Sector Antenna	17.0	C050000D004A
Cambium	90 Sectorized (Dual-Pol), SEC-47D-90-16	16.4	N000000D003A

Table 22 Antennas permitted for deployment in USA – 5.1 GHz

Manufacturer	Antenna type	Nominal gain (dBi)	Cambium part number
Andrew	4-foot Dual-Pol Parabolic, PX4F-52	34.5	RDG4453B
Cambium	4FT 5GHz Single-Pol Parabolic PTP Antenna	33.9	N050067D014A
Cambium	4FT 5GHz Dual-Pol Parabolic PTP Antenna	33.6	N050067D004A
Cambium	3FT 5GHz Single-Pol Parabolic PTP Antenna	31.3	N050067D013A
Cambium	3FT 5GHz Dual-Pol Parabolic PTP Antenna	31.0	N050067D003A
Cambium	2FT 5GHz Single-Pol Parabolic PTP Antenna	27.8	N050067D012A
Cambium	2FT 5GHz Dual-Pol Parabolic PTP Antenna	27.5	N050067D002A
MARS	MA-WS54-50R Flat Plate (Dual-Pol)	23.0	Integrated
MARS	MA-WA56-DP23G7CM Flat Plate (Dual-Pol)	23.0	Integrated
Cambium	90 4.9 - 6 GHz, 90/120 deg Sector Antenna	17.0	C050000D004A
KPPA	KPPA-5.7-DPOMA Omni (Dual-Pol)	13.0	

Table 23 Antennas permitted for deployment in USA – 5.2 GHz

Manufacturer	Antenna type	Nominal gain (dBi)	Cambium part number
Andrew	4-foot Dual-Pol Parabolic, PX4F-52	34.5	RDG4453B
Cambium	4FT 5GHz Single-Pol Parabolic PTP Antenna	34.4	N050067D014A
Cambium	4FT 5GHz Dual-Pol Parabolic PTP Antenna	34.1	N050067D004A
Cambium	3FT 5GHz Single-Pol Parabolic PTP Antenna	32.0	N050067D013A
Cambium	3FT 5GHz Dual-Pol Parabolic PTP Antenna	31.7	N050067D003A
Cambium	2FT 5GHz Single-Pol Parabolic PTP Antenna	28.5	N050067D012A
Cambium	2FT 5GHz Dual-Pol Parabolic PTP Antenna	28.2	N050067D002A

Manufacturer	Antenna type	Nominal gain (dBi)	Cambium part number
MARS	MA-WS54-50R Flat Plate (Dual-Pol)	23.0	Integrated
MARS	MA-WA56-DP23G7CM Flat Plate (Dual-Pol)	23.0	Integrated
Cambium	90 4.9 - 6 GHz, 90/120 deg Sector Antenna	17.0	C050000D004A
KPPA	KPPA-5.7-DPOMA Omni (Dual-Pol)	13.0	

Table 24 Antennas permitted for deployment in USA – 5.4 GHz

Manufacturer	Antenna type	Nominal gain (dBi)	Cambium part number
Andrew	4-foot Dual-Pol Parabolic, PX4F-52	34.5	RDG4453B
Cambium	4FT 5GHz Single-Pol Parabolic PTP Antenna	34.4	N050067D014A
Cambium	4FT 5GHz Dual-Pol Parabolic PTP Antenna	34.1	N050067D004A
Cambium	3FT 5GHz Single-Pol Parabolic PTP Antenna	32.0	N050067D013A
Cambium	3FT 5GHz Dual-Pol Parabolic PTP Antenna	31.7	N050067D003A
Cambium	2FT 5GHz Single-Pol Parabolic PTP Antenna	28.5	N050067D012A
Cambium	2FT 5GHz Dual-Pol Parabolic PTP Antenna	28.2	N050067D002A
MARS	MA-WS54-50R Flat Plate (Dual-Pol)	23.0	Integrated
MARS	MA-WA56-DP23G7CM Flat Plate (Dual-Pol)	23.0	Integrated
Cambium	90 4.9 - 6 GHz, 90/120 deg Sector Antenna	17.0	C050000D004A
Cambium	60 5 GHz Sector Antenna	17.0	85009325001
KPPA	KPPA-5.7-DPOMA Omni (Dual-Pol)	13.0	

Table 25 Antennas permitted for deployment in USA – 5.8 GHz

Manufacturer	Antenna type	Nominal gain (dBi)	Cambium part number
Andrew	6-foot Dual-Pol Parabolic, PX6F-52	38.1	
Cambium	6FT 5GHz Single-Pol Parabolic PTP Antenna	38.4	N050067D019A
Cambium	6FT 5GHz Dual-Pol Parabolic PTP Antenna	37.9	RDH4506B
Andrew	4-foot Dual-Pol Parabolic, PX4F-52	35.3	RDG4453
Cambium	4FT 5GHz Single-Pol Parabolic PTP Antenna	34.9	N050067D018A
Cambium	4FT 5GHz Dual-Pol Parabolic PTP Antenna	34.9	RDH4505B

Cambium	3FT 5GHz Single-Pol Parabolic PTP Antenna	32.5	RDH4513B
Cambium	3FT 5GHz Dual-Pol Parabolic PTP Antenna	32.3	RDH4504B
Cambium	2FT 5GHz Single-Pol Parabolic PTP Antenna	29	N050067D017A
Cambium	2FT 5GHz Dual-Pol Parabolic PTP Antenna	28.8	RDH4503B
MARS	MA-WS54-50R Flat Plate (Dual-Pol)	23	Integrated
MARS	MA-WA56-DP23G7CM Flat Plate (Dual-Pol)	23	Integrated
Cambium	90 4.9 - 6 GHz, 90/120 deg Sector Antenna	17	A005365
Cambium	90 5 GHz Sector Antenna	17	85009324001
KPPA	KPPA-5.7-DPOMA Omni (Dual-Pol)	13	

ISEDC approved antennas

For connectorized units operating in Canada, choose external antennas from Table 26 (4.9 GHz), Table 27 (5.1 GHz), Table 28 (5.2 GHz), Table 29 (5.4 GHz) or Table 30 (5.8 GHz). These are approved by ISEDC for use with the product and are constrained by the following limits for single- or dual-polarization parabolic dish antennas:

- 4.9 GHz – 36.0 dBi per polarization or antenna.
- 5.1 GHz – 34.5 dBi per polarization or antenna.
- 5.2 GHz – 34.5 dBi per polarization or antenna.
- 5.4 GHz – 34.5 dBi per polarization or antenna.
- 5.8 GHz – 35.3 dBi per polarization or antenna.

Caution

Antennas not included in these tables are strictly prohibited for use with the PTP 670 in the specified bands.

Caution

This radio transmitter (ISEDC certification number 109AO-45700) has been approved by ISEDC to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Antennes approuvées par ISDEC

Pour les unités sans antenne intégrée destinées au Canada, choisissez des antennes externes dans la list ci-dessous. Ces antennes paraboliques a polarisation simple ou double sont approuvées par ISDEC pour une utilisation avec le produit comme suit:

- 4.9 GHz – 36.0 dBi par polarisation maximum.
- 5.1 GHz – 34.5 dBi par polarisation maximum.
- 5.2 GHz – 34.5 dBi par polarisation maximum.
- 5.4 GHz – 34.5 dBi par polarisation maximum.
- 5.8 GHz – 35.3 dBi par polarisation maximum.

Attention

Les antennes qui ne sont pas listées dans ces tableaux sont strictement interdites d'utilisation avec le PTP 670 dans les bandes spécifiées

Attention

Le présent émetteur radio (Numéro de certification ISDEC 109AO-45700) a été approuvé par ISDEC pour fonctionner avec les types d'antenne énumérés ci-dessous et ayant un gain admissible maximal et l'impédance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est supérieur au gain maximal indiqué, sont strictement interdits pour l'exploitation de l'émetteur.

Table 26 Antennas permitted for deployment in Canada – 4.9 GHz

Manufacturer	Antenna type	Nominal gain (dBi)	Cambium part number
Cambium	6-foot Dual-Pol Parabolic, SPD6-4.7	36.0	RDH4502A
Cambium	6-foot Dual-Pol Parabolic, HPD6-4.7	35.8	RDH4515A
Cambium	4-foot Dual-Pol Parabolic, SPD4-4.7	33.0	RDH4501A
Cambium	4-foot Parabolic, SP4-4.7	33.0	N000000D002A
Cambium	4-foot Dual-Pol Parabolic, HPD4-4.7	32.8	RDH4516A
Cambium	3-foot Dual-Pol Parabolic, SPD3-4.7	30.4	RDH4500A
Cambium	3-foot Dual-Pol Parabolic, HPD3-4.7	30.2	RDH4517A
Cambium	2-foot Dual-Pol Parabolic, SPD2-4.7	27.0	RDH4499A
Cambium	2-foot Parabolic, SP2-4.7	26.9	N000000D001A
Cambium	2-foot Dual-Pol Parabolic, HPD2-4.7	26.8	RDH4518A
MARS	MA-WS54-50R Flat Plate (Dual-Pol)	23.0	Integrated
MARS	MA-WA56-DP23G7CM Flat Plate (Dual-Pol)	23.0	Integrated
Cambium	1-foot Dual-Pol Parabolic, HPLPD1-4.7	20.8	RDH4519A

Manufacturer	Antenna type	Nominal gain (dBi)	Cambium part number
Cambium	90 4.9 - 6 GHz, 90/120 deg Sector Antenna	17.0	C050000D004A
Cambium	90 Sectorized (Dual-Pol), SEC-47D-90-16	16.4	N000000D003A

Table 27 Antennas permitted for deployment in Canada – 5.1 GHz

Manufacturer	Antenna type	Nominal gain (dBi)	Cambium part number
Andrew	4-foot Dual-Pol Parabolic, PX4F-52	34.5	RDG4453B
Cambium	4FT 5GHz Single-Pol Parabolic PTP Antenna	33.9	N050067D014A
Cambium	4FT 5GHz Dual-Pol Parabolic PTP Antenna	33.6	N050067D004A
Cambium	3FT 5GHz Single-Pol Parabolic PTP Antenna	31.3	N050067D013A
Cambium	3FT 5GHz Dual-Pol Parabolic PTP Antenna	31.0	N050067D003A
Cambium	2FT 5GHz Single-Pol Parabolic PTP Antenna	27.8	N050067D012A
Cambium	2FT 5GHz Dual-Pol Parabolic PTP Antenna	27.5	N050067D002A
MARS	MA-WS54-50R Flat Plate (Dual-Pol)	23.0	Integrated
MARS	MA-WA56-DP23G7CM Flat Plate (Dual-Pol)	23.0	Integrated
Cambium	90 4.9 - 6 GHz, 90/120 deg Sector Antenna	17.0	C050000D004A
Cambium	60 5 GHz Sector Antenna	17.0	85009325001
KPPA	KPPA-5.7-DPOMA Omni (Dual-Pol)	13.0	

Table 28 Antennas permitted for deployment in Canada – 5.2 GHz

Manufacturer	Antenna type	Nominal gain (dBi)	Cambium part number
Andrew	4-foot Dual-Pol Parabolic, PX4F-52	34.5	RDG4453B
Cambium	4FT 5GHz Single-Pol Parabolic PTP Antenna	34.4	N050067D014A
Cambium	4FT 5GHz Dual-Pol Parabolic PTP Antenna	34.1	N050067D004A
Cambium	3FT 5GHz Single-Pol Parabolic PTP Antenna	32.0	N050067D013A
Cambium	3FT 5GHz Dual-Pol Parabolic PTP Antenna	31.7	N050067D003A
Cambium	2FT 5GHz Single-Pol Parabolic PTP Antenna	28.5	N050067D012A
Cambium	2FT 5GHz Dual-Pol Parabolic PTP Antenna	28.2	N050067D002A
MARS	MA-WS54-50R Flat Plate (Dual-Pol)	23.0	Integrated
MARS	MA-WA56-DP23G7CM Flat Plate (Dual-Pol)	23.0	Integrated
Cambium	90 4.9 - 6 GHz, 90/120 deg Sector Antenna	17.0	C050000D004A

Manufacturer	Antenna type	Nominal gain (dBi)	Cambium part number
Cambium	60 5 GHz Sector Antenna	17.0	85009325001
KPPA	KPPA-5.7-DPOMA Omni (Dual-Pol)	13.0	

Table 29 Antennas permitted for deployment in Canada – 5.4 GHz

Manufacturer	Antenna type	Nominal gain (dBi)	Cambium part number
Andrew	4-foot Dual-Pol Parabolic, PX4F-52	34.5	RDG4453B
Cambium	4FT 5GHz Single-Pol Parabolic PTP Antenna	34.4	N050067D014A
Cambium	4FT 5GHz Dual-Pol Parabolic PTP Antenna	34.1	N050067D004A
Cambium	3FT 5GHz Single-Pol Parabolic PTP Antenna	32.0	N050067D013A
Cambium	3FT 5GHz Dual-Pol Parabolic PTP Antenna	31.7	N050067D003A
Cambium	2FT 5GHz Single-Pol Parabolic PTP Antenna	28.5	N050067D012A
Cambium	2FT 5GHz Dual-Pol Parabolic PTP Antenna	28.2	N050067D002A
MARS	MA-WS54-50R Flat Plate (Dual-Pol)	23.0	Integrated
MARS	MA-WA56-DP23G7CM Flat Plate (Dual-Pol)	23.0	Integrated
Cambium	90 4.9 - 6 GHz, 90/120 deg Sector Antenna	17.0	C050000D004A
Cambium	60 5 GHz Sector Antenna	17.0	85009325001
KPPA	KPPA-5.7-DPOMA Omni (Dual-Pol)	13.0	

Table 30 Antennas permitted for deployment in Canada – 5.8 GHz

Manufacturer	Antenna type	Nominal gain (dBi)	Cambium part number
Andrew	4-foot Dual-Pol Parabolic, PX4F-52	35.3	RDG4453
Cambium	4FT 5GHz Single-Pol Parabolic PTP Antenna	34.9	N050067D018A
Cambium	4FT 5GHz Dual-Pol Parabolic PTP Antenna	34.9	RDH4505B
Cambium	3FT 5GHz Single-Pol Parabolic PTP Antenna	32.5	RDH4513B
Cambium	3FT 5GHz Dual-Pol Parabolic PTP Antenna	32.3	RDH4504B
Cambium	2FT 5GHz Single-Pol Parabolic PTP Antenna	29	N050067D017A
Cambium	2FT 5GHz Dual-Pol Parabolic PTP Antenna	28.8	RDH4503B

MARS	MA-WS54-50R Flat Plate (Dual-Pol)	23	Integrated
MARS	MA-WA56-DP23G7CM Flat Plate (Dual-Pol)	23	Integrated
Cambium	90 4.9 - 6 GHz, 90/120 deg Sector Antenna	17	A005365
Cambium	90 5 GHz Sector Antenna	17	85009324001
KPPA	KPPA-5.7-DPOMA Omni (Dual-Pol)	13	

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

Table 32 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 2-36 for details of the Ethernet standards supported and maximum permitted cable lengths.

Table 31 PSU drop cable length restrictions

Type of PSU installed	Power supply to PSU	Ethernet supported (*1)	Power output to auxiliary device	Maximum cable length (*2)
AC Power Injector 56V	AC mains	100BASE-TX 1000BASE-T	No	100 m (330 ft)
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 670.

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

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

Table 32 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 670.

(*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 21).

Caution

Always use Cat5e cable that is gel-filled and shielded with copper-plated steel. Alternative types of drop cable are not supported by Cambium Networks for the PTP 670.

Order Superior Essex type BBDGe cable from Cambium Networks (Table 33). Other lengths of this cable are available from Superior Essex.

Figure 21 Outdoor drop cable

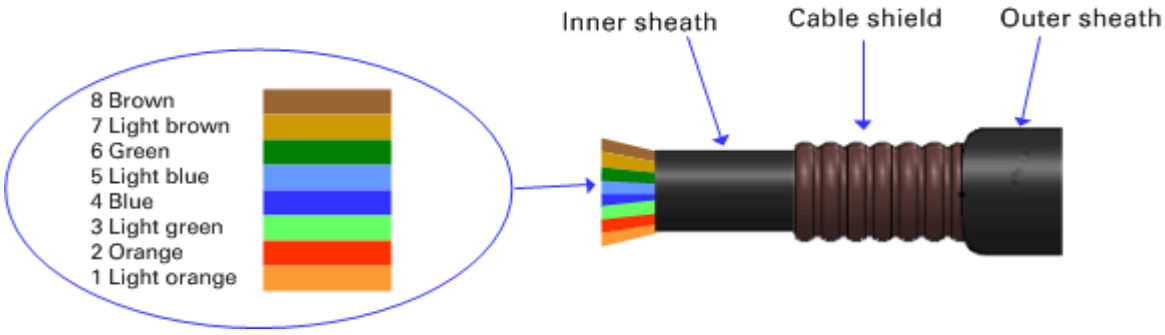


Table 33 Drop cable part numbers

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 22) is required for each grounding point on the PSU, Aux and copper SFP drop cables. Order cable grounding kits from Cambium Networks (Figure 30).

Caution

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

Figure 22 Cable grounding kit

Table 34 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

LPUs provide transient voltage surge suppression for PTP 670 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 35).

Table 35 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 35) 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 36).

Table 36 LPU and grounding kit part number

Cambium description	Cambium part number
LPU and Grounding Kit (One Kit Per End)	C000065L007A

Note

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 (C000065L007A) (Table 35) is suitable. Alternatively, the single LPU kit for PTP 250/300/500 (Figure 23) could be used.

Figure 23 LPU kit used for GPS receiver drop cables

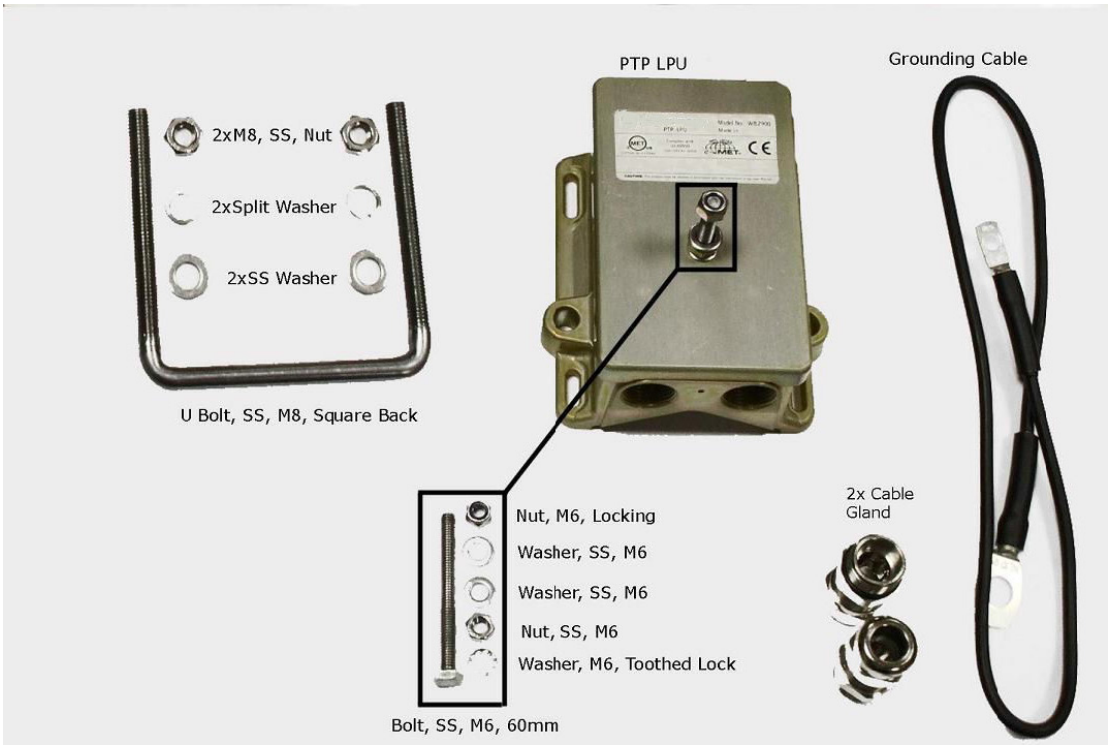


Table 37 LPU and grounding kit part number – Use with GPS receiver drop cable only

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 38).

Note

The RJ45 connectors and crimp tool listed in Table 38 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 24). These are identified with a black sealing nut. If extra glands are required, order them from Cambium Networks (in packs of 10) (Table 38).

One long EMC strain relief gland (Figure 27) 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 24 Cable gland

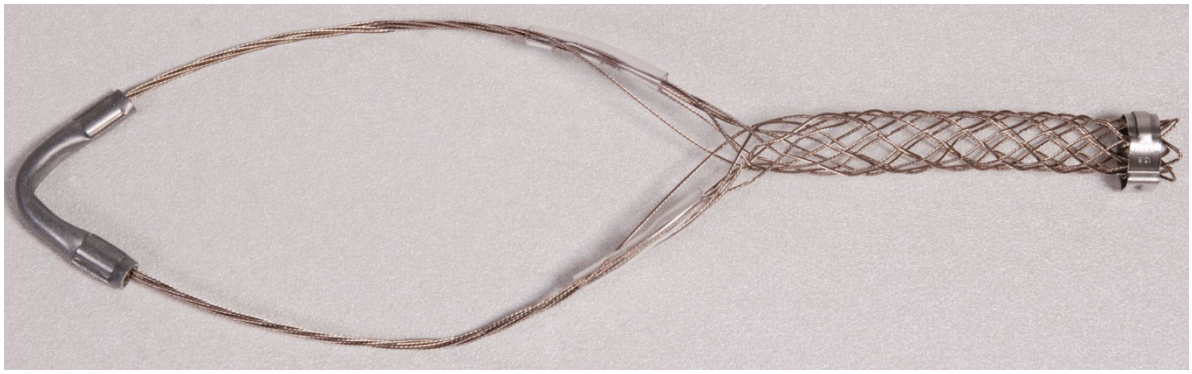
Table 38 RJ45 connector and spare gland part numbers

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 25). They are not supplied by Cambium Networks.

Figure 25 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 670 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 39).

Table 39 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 40 and Table 41.

Table 40 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 41 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 26)
- Long EMC strain relief cable gland (Figure 27)
- The *Ethernet SFP Module Installation Guide*
- License key instructions and unique Access Key

Figure 26 Optical or copper SFP transceiver module

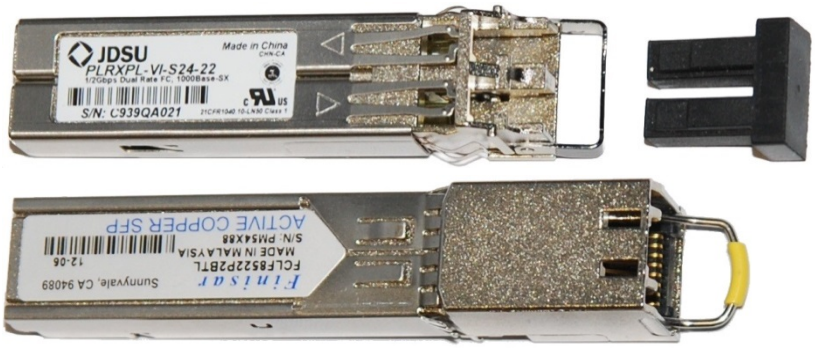


Figure 27 Long cable gland

Note

PTP 670 does not support the Synchronous Ethernet or 1588 Transparent Clock features using copper SFP transceivers.