# PTP 300 and PTP 500 Series

## User Guide

## System Release 500-04-00

phn-1115-006v000

## Accuracy

While reasonable efforts have been made to assure the accuracy of this document, Motorola, Inc. assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. Motorola, Inc. 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. Motorola, Inc. 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 Motorola 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 Motorola intends to announce such Motorola products, programming, or services in your country.

## Copyrights



## Restrictions



## License Agreements

The software described in this document is the property of Motorola, Inc 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

Components, units, or 3rd Party products used in the product described herein are NOT fault-tolerant and are NOT designed, manufactured, or intended for use as on-line control equipment in the following hazardous environments requiring fail-safe controls: the operation of Nuclear Facilities, Aircraft Navigation or Aircraft Communication Systems, Air Traffic Control, Life Support, or Weapons Systems (High Risk Activities). Motorola and its supplier(s) specifically disclaim any expressed or implied warranty of fitness for such High Risk Activities.

## Trademarks

MOTOROLA

MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

# Important safety information

This section describes important safety guidelines that must be observed by personnel installing or operating PTP 300 or PTP 500 equipment.

**WARNING**

**To prevent loss of life or physical injury, observe the safety guidelines in this section.**

## Power lines

Exercise extreme care when installing antennas near power lines.

## Working at heights

Exercise extreme care when working at heights.

## Grounding and protective earth

The Outdoor Unit (ODU) must be properly grounded to protect against lightning. It is the user's responsibility to install the equipment in accordance with national regulations. In the USA, follow Section 810 of the *National Electric Code, ANSI/NFPA No.70-1984* (USA). In Canada, follow Section 54 of the *Canadian Electrical Code*. These codes describe correct installation procedures for grounding the outdoor unit, mast, lead-in wire and discharge unit, size of grounding conductors and connection requirements for grounding electrodes. Other regulations may apply in different countries and therefore it is recommended that installation of the outdoor unit be contracted to a professional installer.

## PIDU Plus

The supplied Power Indoor Plus (PIDU Plus PTP 300/500/600 Series) is used to power the ODU. Failure to use the Motorola supplied PIDU could result in equipment damage and will invalidate the safety certification and may cause a safety hazard.

## Powering down before servicing

Always power down and unplug the equipment before servicing.

## Cable measuring card

A cable measuring card must NEVER be used at the ODU end connected to power from the PIDU Plus. It must only be used at the bottom of the mast with a multimeter. This is because the PIDU Plus voltage exceeds the limit allowed in some countries for safe handling in wet conditions and therefore may create a safety hazard.

## Non-Motorola power supply

Safety may be compromised if a different power supply is used than the one supplied by Motorola as part of the system.

## Alternative DC supplies

When using alternative DC supplies (via the PIDU Plus DC in terminals), such as battery-backed DC power source, the supply MUST comply with the following requirements:

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

## Primary disconnect device

The main power supply is the primary disconnect device.

## External cables

Safety may be compromised if outdoor rated cables are not used for connections that will be exposed to the weather.

## Grounding PTP-SYNC

In order to meet the safety requirements for deployment in Australia and New Zealand (AS/NZS 60950-1), the PTP-SYNC unit, if deployed, must be grounded to a Protective Ground in accordance with Local Electrical Regulations.

## RF exposure near the antenna

Strong radio frequency (RF) fields will be present close to the antenna when the transmitter is on. Always mute the transmitter before undertaking maintenance activities in front of the antenna.

## Minimum separation distances

Install the ODUs so as to provide and maintain the minimum separation distances from all persons.

The minimum separation distances for each frequency variant are specified in Calculated distances and power compliance margins on page 4-67.

# Important regulatory information

Operation of the PTP 300 and PTP 500 Series products involves their use as unlicensed devices in frequency bands where they are not allowed to cause interference to licensed services (called primary users of the bands).

## Radar avoidance

In some countries radar systems are the primary users and the regulators have devised special requirements to protect their operation from interference caused by unlicensed devices. The unlicensed devices are required to detect the presence of radar systems and avoid co-channel operation with the radar systems.

The PTP 300 and PTP 500 systems provide detect and avoid functionality for countries and frequency bands requiring protection for radar systems.

Installers and users are reminded that they must follow local regulations with regard to any requirements for radar detection as well as transmitted power level. This can be achieved by using the correct licence key/region code for the product concerned. Failure to follow this could leave the installer and/or user liable to civil and/or criminal penalties.

Contact the Motorola helpdesk if you are unsure about any specific areas where you need guidance.

## USA specific information

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

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

In order to comply with these clear FCC requirements for all manufacturers, Motorola is releasing new versions of PTP 300 and PTP 500 for USA or Canada operation. These new devices will only be allowed to operate with licence keys/region codes which will comply with FCC/IC rules.

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

Installers must follow this procedure when deploying PTP 300 or PTP 500 links in the USA or Canada:

- Check whether either master or slave units are being installed within 35 km of a TDWR system or have a line of sight propagation path to such a system. This can be checked by visiting http://spectrumbridge.com/udrs/home.aspx.
- If a TDWR system is located within 35km or has line of sight propagation to the PTP device, then the installer must:
  - Register the installation on http://spectrumbridge.com/udrs/home.aspx.
  - Use channel barring to ensure a minimum of 30 MHz separation between the TDWR frequency and the operating channel frequency of the PTP system.

# Contents

# List of Figures

# List of Tables

# About This User Guide

This guide describes the planning, installation and operation of the Motorola PTP 300 and PTP 500 Series of Point-to-Point Wireless Ethernet Bridges. It is intended for use by the system designer, system installer and the end-user IT professional. The users of this guide will require expertise in the following areas:

- Outdoor radio equipment installation
- Network configuration
- Use of web browser for system configuration, monitoring and fault finding

# Revision history

## Version information

The following shows the issue status of this document.

| Document issue | Date of issue | Remarks |
|---|---|---|
| 001v000 | Apr 2008 | System release 500-01-00 |
| 002v000 | Jun 2008 | System release 500-02-00 |
| 003v006 | Feb 2009 | System release 500-03-01 |
| 004v000 | Nov 2009 | System release 500-03-02 |
| 005v000 | Feb 2010 | System release 500-03-02 (revised) |
| 006v000 | Sep 2010 | System release 500-04-00 |

# General information

## Purpose

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

Motorola 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.

## Text conventions

The following conventions are used in the Motorola Point-To-Point documents to represent keyboard input text, screen output text and special key sequences.

### Input

**`Characters typed in at the keyboard are shown like this.`**

### Output

```
Messages, prompts, file listings, directories, utilities, and
environmental variables that appear on the screen are shown like this.
```

## Special key sequences

Special key sequences are represented as follows:

| | |
|---|---|
| **CTRL+C** | Press the **Ctrl** and **C** keys at the same time. |
| **CTRL+SHIFT+C** | Press the **Ctrl**, **Shift**, and **C** keys at the same time. |
| **ALT+F** | Press the **Alt** and **F** keys at the same time. |
| **ALT+SHIFT+F11** | Press the **Alt**, **Shift**, and **F11** keys at the same time. |
| **\|** | Press the pipe symbol key. |
| **RETURN** or **ENTER** | Press the **Return** or **Enter** key. |

# Contacting Motorola

## Feedback

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

## Motorola Point-to-Point

Postal address:

Motorola, Inc.,
1303 E. Algonquin Road,
Schaumburg,
Illinois 60196
U.S.A.

URLs:

Main web site: http://www.motorola.com/ptp

Web support: http://www.motorola.com/ptp/support

Email addresses:

Sales enquiries: sales.ptp@motorola.com

Email support: support.ptp@motorola.com

All other enquiries: info.ptp@motorola.com

## Wireless Broadband Technical Support telephone numbers

| Region and country | Support telephone number |
|---|---|
| **North America:** | |
| USA and Canada | 866-961-9288 |
| **Europe, Middle East and Africa:** | |
| Denmark | 043682114 |
| France | 0157323434 |
| Germany | 06950070204 |

| Region and country | Support telephone number |
|---|---|
| Italy | 0291483230 |
| Lithuania | 800 030 828 |
| Netherlands | 0202061404 |
| Norway | 24159815 |
| Portugal | 0217616160 |
| Spain | 912754787 |
| Russia | 810 800 228 41044 |
| Saudi Arabia | 800 844 5345 |
| South Africa | 0800981900 |
| United Kingdom | 0203 0277499 |
| All other countries | +44 203 0277499 |
| **Latin and Central America:** | |
| Argentina | 0800-666-2789 |
| Brazil | 0800-891-4360 |
| Chile | 800-225-288 |
| Columbia | 01-800-912-0557 |
| Mexico | 001-800-942-7721 |
| Peru | 0800-70-086 |
| All other countries | +420 533 336 946 |
| **Asia, Pacific and China:** | |
| Australia | 800 457 439 |
| Singapore | 64 155 110 |
| All other countries | +420 533 336 946 |

## 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 Motorola website at http://www.motorola.com/ptp.
3. Ask for assistance from the Motorola product supplier.
4. Gather information from affected units such as:
    - The IP addresses and MAC addresses
    - The software releases
    - The configuration of software features
    - Any available diagnostic downloads
5. Escalate the problem to Motorola as follows:
    - Either: send e-mail to support.ptp@motorola.com
    - Or: call Wireless Broadband Technical Support.

## Repair and service

If unit failure is suspected, visit http://www.motorola.com/ptp/support for details of the Return Material Authorization (RMA) process.

## Warranty

Motorola's standard hardware warranty is for one (1) year from date of shipment from Motorola or a Motorola Point-to-Point Distributor. Motorola 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. Motorola 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 http://www.motorola.com/ptp/support.

For warranty assistance, contact the reseller or distributor.

**CAUTION**

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

**CAUTION**

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

# Security advice

Motorola systems and equipment provide security parameters that can be configured by the operator based on their particular operating environment. Motorola 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 Motorola 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 this Motorola 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

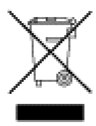
Note text.

# Caring for the environment

The following information describes national or regional requirements for the disposal of Motorola 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 Motorola equipment in EU countries.



### Disposal of Motorola equipment

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

Do not dispose of Motorola equipment in landfill sites. In the EU, Motorola in conjunction with a recycling partner ensures that equipment is collected and recycled according to the requirements of EU environmental law.

### 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 Motorola Networks equipment and all surplus packaging in accordance with national and regional regulations.

# Chapter 1 Product description

This chapter provides a high level description of the PTP 300 and PTP 500 products. It describes in general terms the function of the products, the main product variants and typical deployment. It also describes the main hardware components.

The following topics are described in this chapter:

# Overview

Motorola PTP 300 and PTP 500 Series products are designed for Ethernet bridging over point-to-point microwave links in the unlicensed bands 5.4 GHz (ETSI Band B) and 5.8 GHz (ETSI Band C and FCC ISM band). Users must ensure that the links comply with local operating regulations.

The PTP 300 and PTP 500 Series are used to create a transparent bridge between two segments of the operator’s network. This bridge can be treated as a virtual wired connection between two points. The system is transparent to higher-level protocols such as VLANs and Spanning Tree.

## Key features

The key features of the PTP 300 and PTP 500 Series include:

- True non-line-of-sight (NLOS) operation by using a combination of Orthogonal Frequency Division Multiplexing (OFDM) modulation and Multiple-Input Multiple-Output (MIMO) techniques.
- Wireless connections of up to 250 km (155 miles) in near line-of-sight conditions and up to 100 meters (330 ft) in deep non-line-of-sight conditions.
- Coexistence with other users of the band using a combination of Spectrum Management functionality and Antenna beam shape.
- High link availability, through the use of adaptive modulation techniques that dynamically reduce the data rate in severe or adverse conditions.
- High system gain through high sensitivity antennas for improved signal recovery.
- A radio system that operates using ultra-fast digital signal processors and is controlled by updateable firmware.
- A built-in web server for advanced management capabilities including detailed radio signal diagnosis.
- A range of security features to prevent unauthorized access to data. Optional AES encryption for data transmitted over the wireless, with 128-bit or 256-bit encryption keys. SNMPv3 with optional AES privacy and SHA1 authentication.

### Benefit of the chosen bands

The products operate in bands that offer the dual benefits of high data throughput and good radio propagation characteristics. The wide band of spectrum available is subdivided into several channels such that multiple systems can operate in the vicinity without causing interference to one another.

### Similarity to 802.11a devices

The products are not 802.11a devices. Although similar, they use different encoding and radio transmission systems from 802.11a. In areas where 802.11a systems are operating, the products will detect the 802.11a radio signals and choose a clear channel away from any interference.

### Avoiding interference from nearby devices

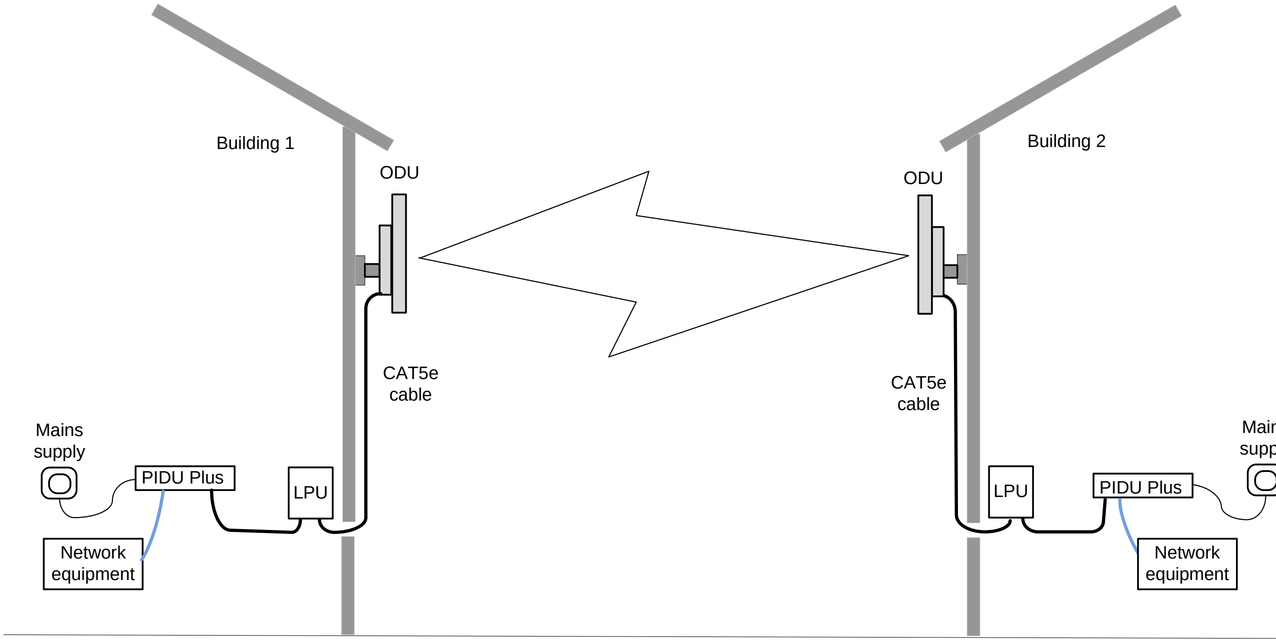
At initialization, the products monitor the available frequency channels to find a channel that is clear of interference. In operation, the products continuously monitor the spectrum to ensure it is operating on the cleanest channel.

## Typical deployment

The PTP 300 or PTP 500 Series Bridge consists of an identical pair of units deployed one at each end of the link. The radio link operates on a single frequency channel in each direction using Time Division Duplex (TDD). One unit is deployed as a master and the other as a slave. The master unit takes responsibility for controlling the link in both directions.

The Bridge is aimed at a wide range of applications. An example application is an enterprise that has a requirement to connect together the Local Area Network (LAN) of two or more buildings as shown in Figure 1-1.

**Figure 1-1** Typical bridge deployment (grounding not shown)




## System components

Each end of the link consists of:

- **Outdoor Unit (ODU):** An integrated (or connectorized) outdoor transceiver unit containing all the radio and networking electronics.
- **PIDU Plus:** An indoor connection box containing a mains power supply, status indicators and network connection port.
- **Cabling and lightning protection:** CAT5e cables, grounding cables, connectors and a lightning protection unit (LPU).

## Product variants

The PTP 300 and PTP 500 Series are available in the following product variants:

- **PTP 300 or PTP 500**: The PTP 300 Series provides lower data throughput rates than the PTP 500 Series. The PTP 300 provides a Line Of Sight (LOS) mode, which is not available in the PTP 500.
- **Frequency variants**: Both products are available in either 5.4 GHz or 5.8 GHz variants, depending upon the chosen license exempt frequency band (Table 1-1). Check that local regulations allow the use of these frequency variants.
- **Lite or Full**: The PTP 500 (but not the PTP 300) is available in either Lite or Full variants. PTP 500 Lite data rates are half those of PTP 500 Full.
- **FCC/IC or ETSI/RoW**: Both products are available in two regional variants: one is for use in regions where FCC or IC licensing restrictions apply (FCC/IC), and the other is for use in ETSI or the rest of the world (ETSI/RoW).
- **Integrated or Connectorized**: Both products are available in either Integrated (with attached antenna) or Connectorized (without an antenna) variants.
- **Link Complete or End Complete**: The Link Complete kit consists of two ODUs and two PIDU Plus units, pre-configured as a link. The End Complete kit consists of one ODU and one PIDU Plus unit.

To identify the available combinations of the above variants, refer to Ordering ODU and PIDU Plus kits on page 4-8.

**Table 1-1** PTP 300 and PTP 500 Series frequency variants

| Variant | Region | Frequency Coverage | Variable Channel Bandwidth | Channel Raster |
|---|---|---|---|---|
| PTP 54300 or PTP 54500 | ETSI 5 GHz Band B<br>FCC UNII Band | 5470-5725 MHz | 5, 10, 15 MHz | 5 MHz |
| PTP 58300 or PTP 58500 | ETSI Band | 5725-5875 MHz | 5, 10, 15 MHz | 5 MHz |
| | FCC ISM Band | 5725-5850 MHz | 5, 10, 15 MHz | 5 MHz |

# Outdoor unit (ODU)

## ODU description

The ODU is a self-contained unit that houses both radio and networking electronics. The ODU is supplied in two configurations: integrated (attached to its own flat plate antenna, Figure 1-2) or connectorized (without an antenna, Figure 1-3).

**Figure 1-2** Integrated ODU (front and rear views)


**Figure 1-3** Connectorized ODU (front and rear views)

### Connectorized variant

The connectorized ODU is designed to work with externally mounted antennas that have higher gains than the integrated antenna. Connectorized units can cope with more difficult radio conditions, as described in When to install connectorized units on page 2-12.

## ODU interfaces

The PIDU Plus interfaces are illustrated in Figure 1-4 and described in Table 1-2.

**Figure 1-4** ODU interfaces

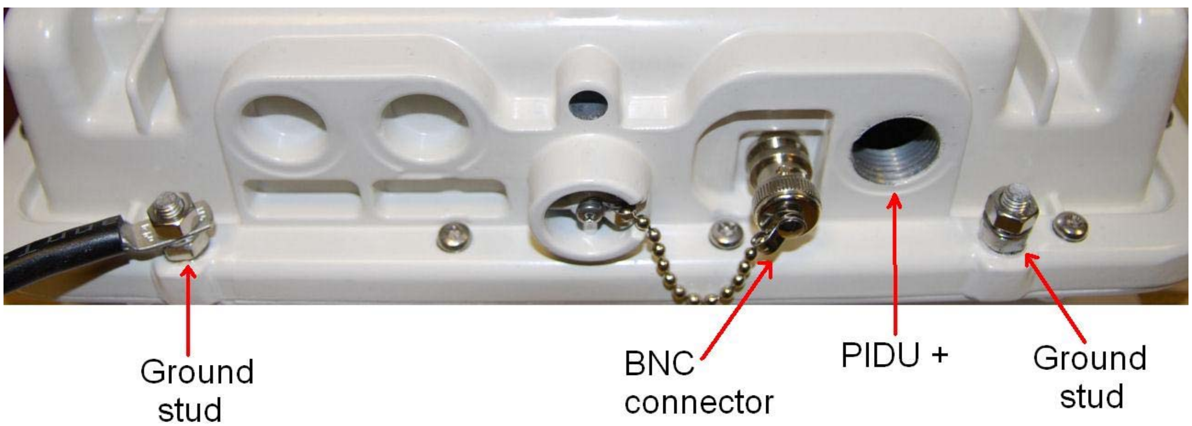



**Table 1-2** ODU interface functions

| Interface | Function |
|---|---|
| Ground studs | For grounding the ODU to the supporting structure. The ground cable (supplied with the ODU) may be connected to either ground stud. |
| BNC connector | Use with a digital voltmeter (DVM) to help with the alignment process. |
| PIDU+ | RJ45 socket for connecting to power supply and network via the PIDU Plus. |

## Connectorized ODU antenna interfaces

The connectorized ODU also has interfaces to connect to an external antenna (Figure 1-5) via a cable of type LMR100, LMR200, LMR300, LMR400 or LMR600. The 'V' interface is for vertical polarization and the 'H interface is for horizontal polarization.

**Figure 1-5** Connectorized ODU antenna interfaces


## Mounting brackets

The ODU is supplied with a bracket for mounting it to a pole of 50mm (2") to 75mm (3") in diameter.

The bracket allows for adjustment in both azimuth and elevation. The bracket may be split to allow the pole mount section of the bracket to be mounted to the pole first. This allows the installer to take the weight of the unit and secure it, one handed, with a single mounting bolt.

## Network connection

The network connection to the ODU is made via a 100BaseT Ethernet connection. Power is provided to the ODU over the 100BaseT Ethernet connection using a patented non-standard powering technique.

# Powered indoor unit (PIDU Plus)

## PIDU Plus description

The PIDU Plus generates the ODU supply voltage from the mains supply (or from an external DC source) and injects this supply voltage into the ODU.

The PIDU Plus is connected to the ODU and network equipment using CAT5e cable with RJ45 connectors. Refer to Cabling and lightning protection on page 1-13.

The ODU should only be deployed using the supplied PIDU Plus PTP 300/500/600 Series.

**CAUTION**

The PIDU Plus ODU port is designed to connect only to PTP 300, PTP 500 or PTP 600 ODUs, LPUs or PTP-SYNC units. Do not connect any other equipment, as damage may occur. The PIDU Plus PTP 300/500/600 Series is not interchangeable with the PIDU Plus PTP 400 Series.

## PIDU Plus interfaces

The PIDU Plus interfaces are illustrated in Figure 1-6 and described in Table 1-3 and Table 1-4.

**Figure 1-6** PIDU Plus interfaces

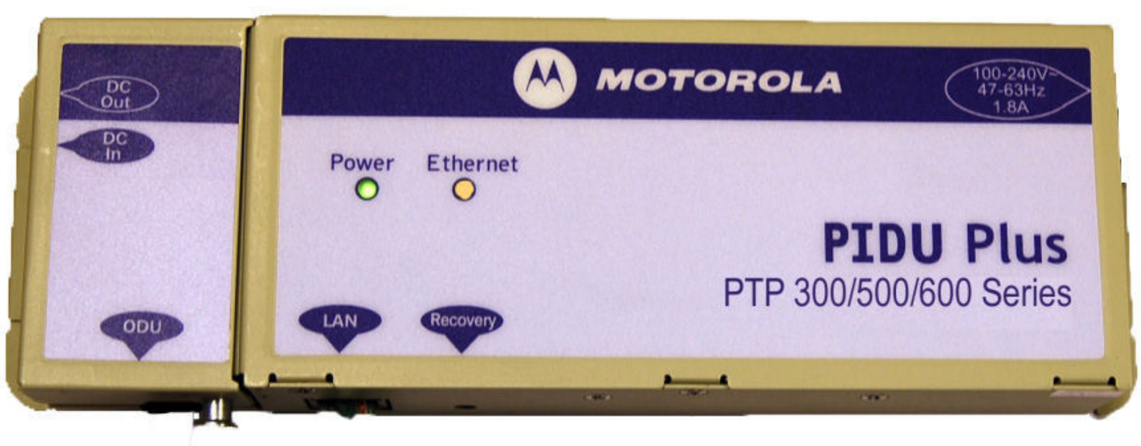


**Table 1-3** PIDU Plus interface functions

| Interface | Function |
|---|---|
| 100-240V 47-63Hz 1.8A | Mains power input (Figure 1-7). |
| DC In | Alternative DC power supply input. Refer to Redundancy and alternative powering configurations on page 1-11. |
| DC Out | DC power output to a second PIDU Plus. Used to provide power supply redundancy. Refer to Redundancy and alternative powering configurations on page 1-11. |
| ODU | RJ45 socket for connecting CAT5e cable to ODU. |
| LAN | RJ45 socket for connecting CAT5e cable to network. |
| Recovery | Used to recover the unit from configuration errors or software image corruption. |

**Table 1-4** PIDU Plus indicator LEDs

| Indicator | Function | Description |
|---|---|---|
| Power | Off | No power. |
| | On | PIDU Plus is receiving power. |
| Ethernet | Off | No Ethernet traffic. |
| | Blink ten times | Correct start up sequence has occurred. |
| | Blink randomly | Normal Ethernet traffic. |

**Figure 1-7** PIDU Plus power input

## Redundancy and alternative powering configurations

The PTP 300 and PTP 500 Series can be powered from an external DC source and can be provided with power supply redundancy as follows:

- External DC supply only (Figure 1-8): This configuration is for use where there is no mains supply.
- External DC supply and AC supply (Figure 1-9): This configuration provides redundancy through the use of mains and DC supply.
- External DC supply and redundant AC Supply (Figure 1-10): This configuration guards against mains failure and failure of the DC output of single PTP 300/500/600 PIDU Plus.

**Figure 1-8** External DC supply only

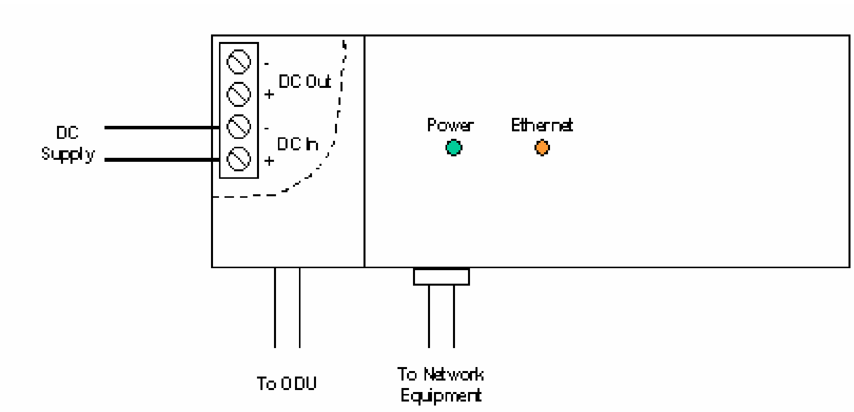



**Figure 1-9** External DC supply and AC supply

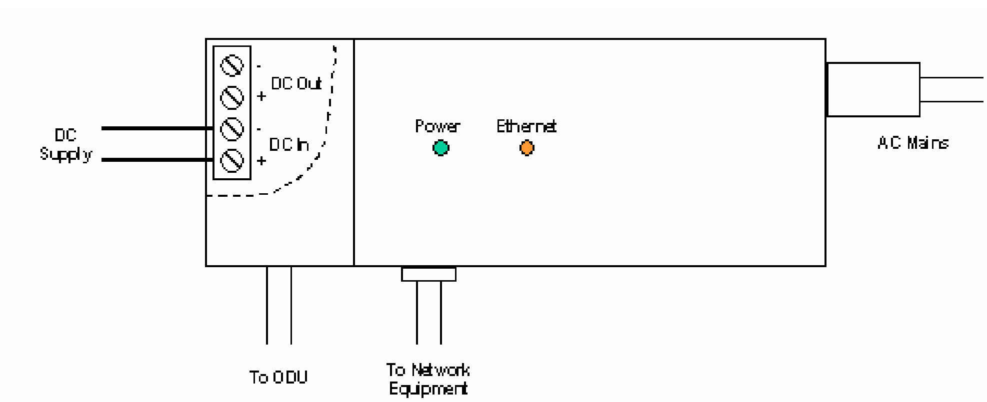
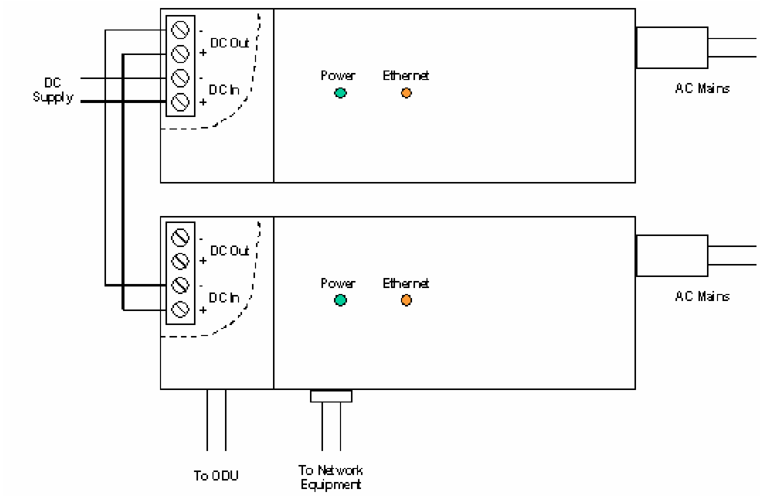


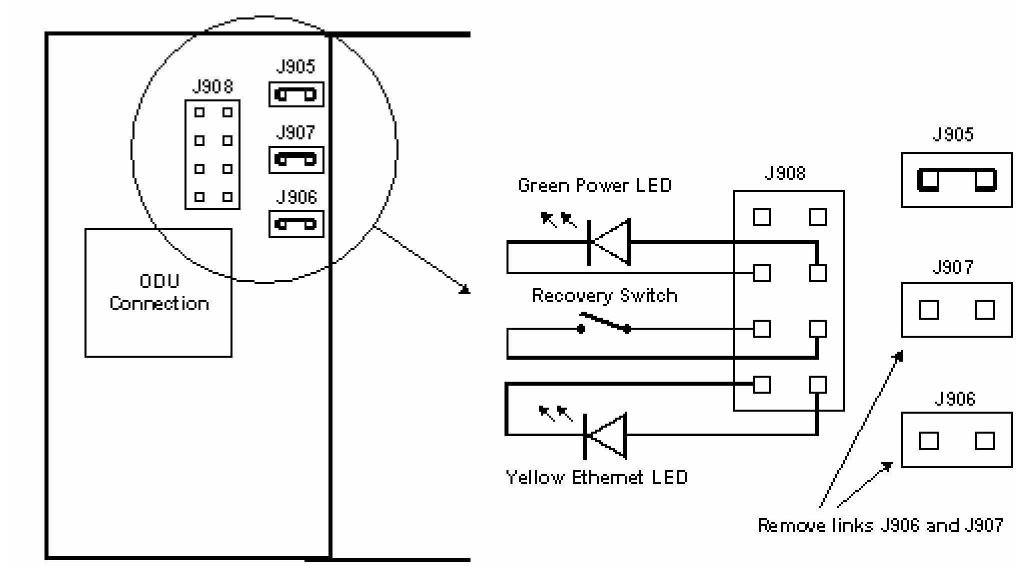
**Figure 1-10** External DC supply and redundant AC supply




## Remote LEDs and recovery switch

The PIDU Plus provides a facility to connect remote LEDs and Recovery switch allowing the PIDU Plus to be mounted inside an enclosure. At the left hand end of the PIDU Plus under the ODU connection cover can be found a PCB header and three jumpers. Jumpers J906 and J907 should be removed and connection to the remote LEDs and Recovery switch made to J908 as shown in Figure 1-11.

**Figure 1-11** Remote LED and recovery switch wiring



# Cabling and lightning protection

The cabling and lightning protection components of a PTP 300 or PTP 500 installation are:

- Outdoor drop cable
- Indoor CAT5e cable
- Grounding cables
- Lightning protection units

## PTP and lightning protection

The PIDU Plus meets the low level static discharge specifications identified in EMC immunity compliance on page 4-58 but does not provide lightning or surge suppression.

The amount of lightning protection is dependent on regulatory requirements and the end user requirements. The standard ODU is fitted with surge limiting circuits and other features to minimize the risk of damage due to nearby lightning strikes. To be fully effective, these standard features require some additional equipment to be configured as part of the system installation.

**CAUTION**

The products are not designed to survive direct lightning strikes. For this reason the units should not be installed as the highest point in a localized area. See Grounding and lightning protection on page 2-14.

## Outdoor connections

The term 'drop cable' refers to the cable that is used for all connections that terminate outside the building, for example, connections between the ODU, LPU (if installed), GPS receiver (if installed) and the ODU port of the PIDU Plus.

**CAUTION**

For outdoor connections, always use Cat5e cable that is gel-filled and shielded with copper-plated steel. This is the only type of outdoor drop cable supported in this application. See Cable and connector specifications on page 4-17.

## Indoor connections

The CAT5e cable that connects the PIDU Plus to the network equipment must meet the screening requirements specified in Cable and connector specifications on page 4-17.

CAUTION

The connected network equipment must feature screened RJ45 connectors and must be connected to ground, otherwise the PIDU Plus will not be grounded, and this may increase the levels of unwanted radiation from the ODU - PIDU Plus cables.

NOTE

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).

## Cable grounding kits

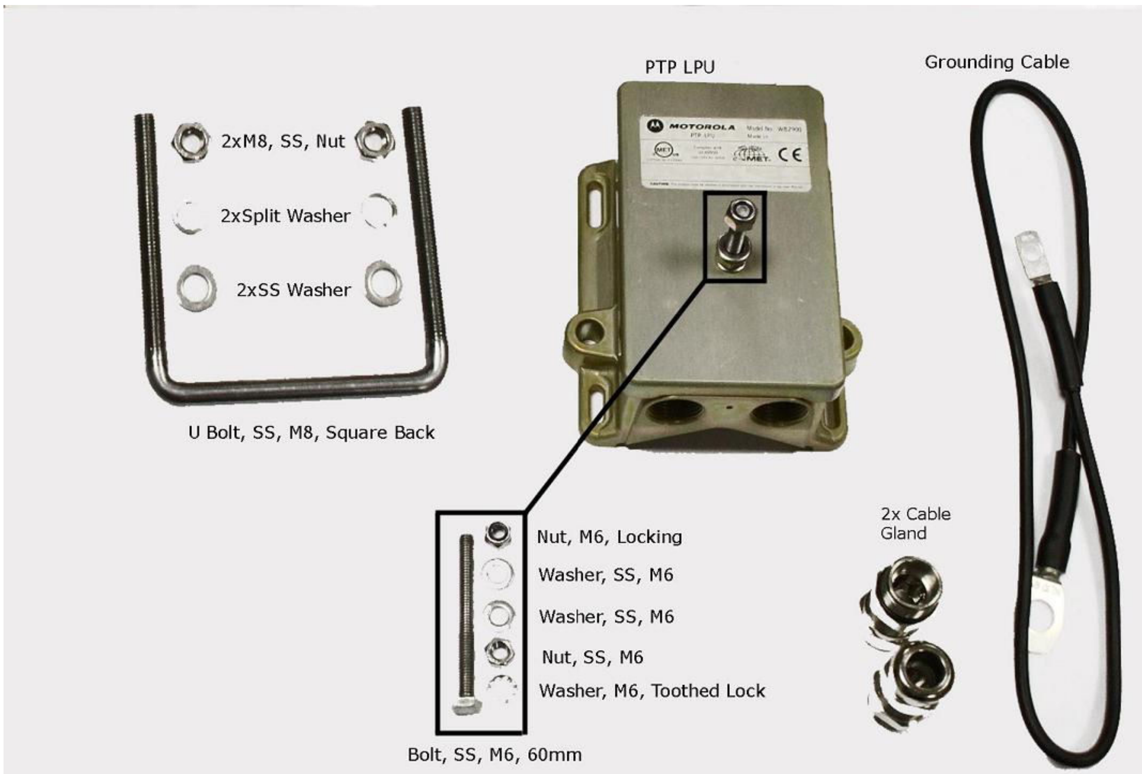
Drop cables must be grounded at the points specified in Grounding and lightning protection on page 2-14. One cable grounding kit (Figure 1-12) is required for each drop cable grounding point.

**Figure 1-12** Cable grounding kit for 1/4” and 3/8” cable

## Lightning protection units (LPUs)

One LPU single end kit (Figure 1-13) is required for each ODU drop cable. If GPS is installed (for PTP-SYNC), one additional LPU kit is required for the GPS drop cable. The LPU is installed near the building entry point.

**Figure 1-13** LPU single end kit



# PTP-SYNC unit

## PTP-SYNC unit description

The PTP-SYNC unit (Figure 1-14) is an optional component for the PTP 500 Series. It is required when TDD synchronization is implemented using PTP-SYNC. It measures the difference between the TDD frame timing and a 1 Hz timing reference, and signals this time difference to the ODU.

For more information on this feature, refer to TDD synchronization on page 1-30.

The PTP-SYNC is a compact indoor unit mounted on a wall or a shelf or (using an optional rack mounting adaptor) in a standard 19 inch rack. It is powered using standard power-over-Ethernet from the PIDU Plus. One PTP-SYNC unit is required for each synchronized link.

**Figure 1-14** PTP-SYNC kit

# PTP-SYNC unit interfaces

The PTP-SYNC front panel is illustrated in Figure 1-15. The annotated interfaces are described in Table 1-5.

**Figure 1-15** PTP-SYNC front panel

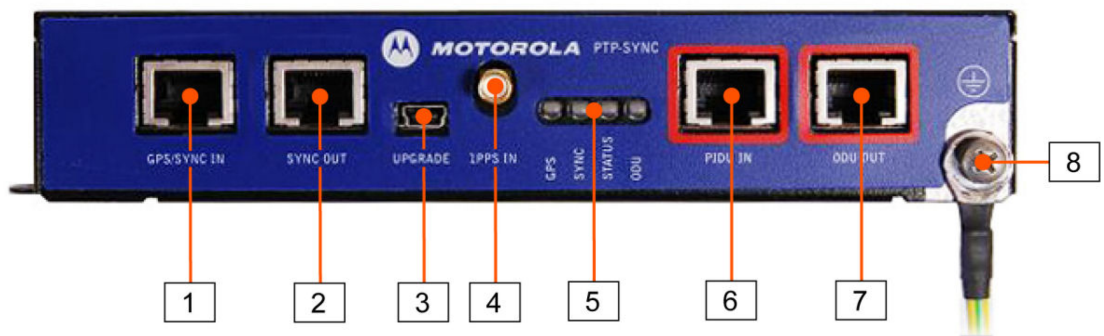



**Table 1-5** PTP-SYNC front panel interfaces

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

**Table 1-6** PTP-SYNC indicator LEDs

| Indicator | Function | Description |
|---|---|---|
| GPS | Off | No GPS satellite data being received at the GPS/SYNC IN port. |
| | On steady or blink | GPS satellite data being received. |
| SYNC | Off | No data being received at the SYNC OUT port. |
| | On steady or blink | Data being received at the SYNC OUT port. |
| STATUS | Off | No power. |
| | On steady | Power but no satellite lock. |
| | Blink | Power and satellite lock at either the GPS/SYNC IN or 1PPS IN port. |
| ODU | Off | No signal being received from the ODU. |
| | On | Communication with the ODU is established. |

# Wireless operation

## Time division duplexing

### TDD cycle

PTP 300 and PTP 500 series 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 1-16. 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 transmits a burst to the master.
5. A delay occurs as the slave-master burst propagates over the link.
6. The master receives the burst from the slave.
7. The master transmits the next burst to the slave.

### TDD frame parameters

The TDD burst duration varies depending on the following:

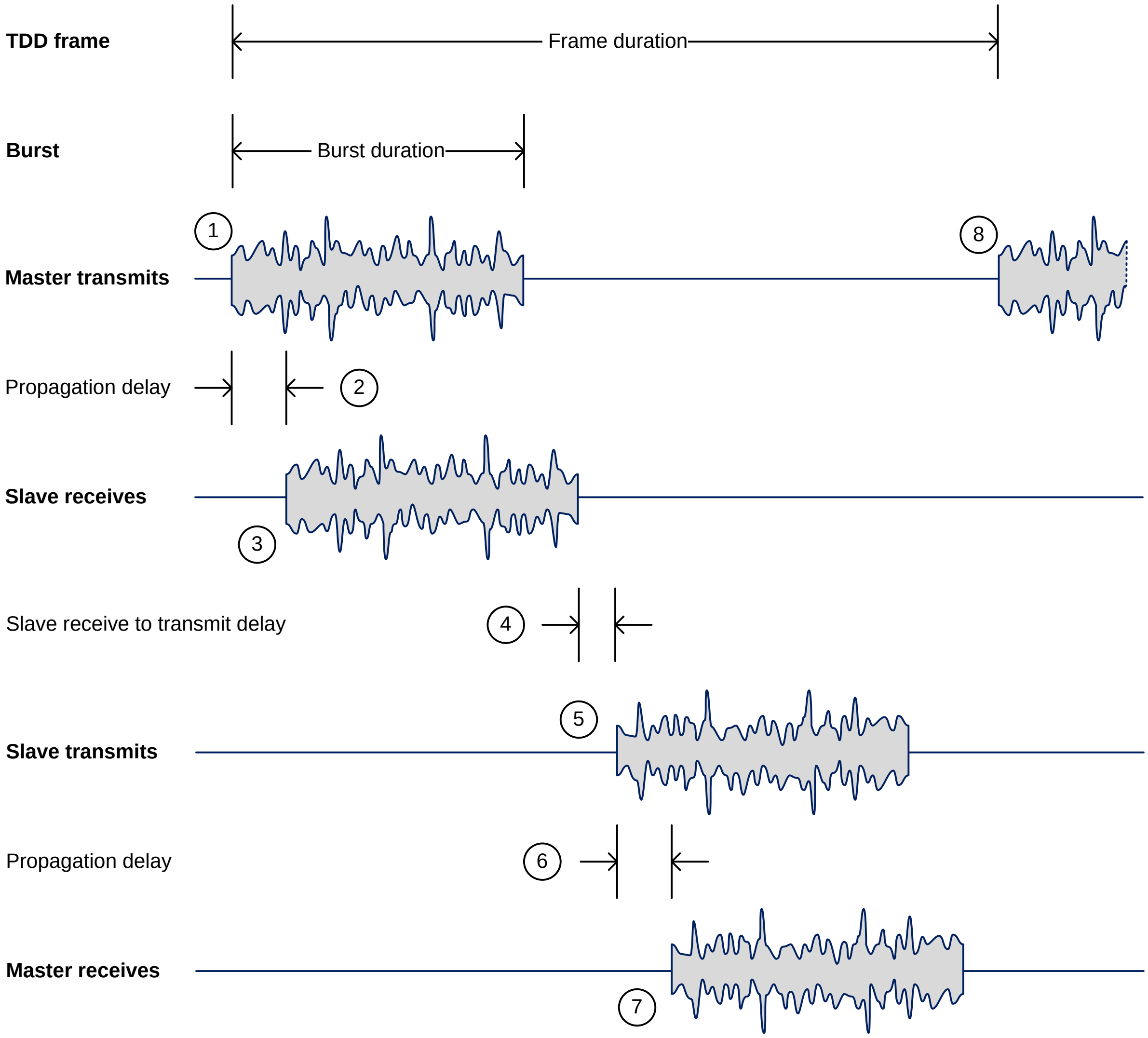
- Channel bandwidth
- Link range
- Link optimization mode
- Link symmetry
- Offered traffic loading.

The TDD frame duration varies depending on the following:

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

The propagation delay in Step 2 is necessarily equal to the propagation delay in Step 5, and is determined solely by the link range. There will be added delays between rx and tx on the master and slave to minimise interference.

**Figure 1-16** TDD cycle




## Channel selection

The PTP 300 and PTP 500 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 must monitor its transmit channel for the presence of radar signals, and thus transmit and receive channels are always identical.

# Link mode optimization

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

## IP traffic

IP Traffic mode is optimized to provide the maximum possible link capacity. IP Traffic mode is an appropriate choice where applications in the bridged networks provide some measure of reliable transmission, and where very low latency is not critical. IP mode supports both fixed and adaptive link symmetry (see Link symmetry on page 1-21).

## TDM traffic

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

# Link symmetry

The PTP 300 and PTP 500 Series provide four configuration options for apportioning the available capacity between the two link directions.

- **Symmetric:** The Master and Slave have equal capacity. The system achieves this by allocating an equal Burst Duration for the Master and the Slave.
- **3:1** The capacity in the direction Master to Slave is three times that of the direction Slave to Master. The system series achieves this by setting the Burst Duration of the Master to three times that of the Slave.
- **1:3** The capacity in the direction Slave to Master is three times that of the direction Master to Slave. The system achieves this by setting the Burst Duration of the Slave to three times that of the Master.

**NOTE**

The 3:1 and 1:3 modes are not available when TDD synchronization is enabled or when 5 MHz bandwidth is selected.

- **Adaptive:** The capacity allocated to a given link direction is dependant 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 system 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 system 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**

  Adaptive mode is not available in the following configurations :

  - When link mode optimization is set to TDM Traffic see Link mode optimization on page 1-21).
  - When TDD synchronization is enabled.
  - In regions where radar avoidance is operational (see Radar avoidance on page 1-27).
  - When 5 MHz bandwidth is selected.

## Non Line Of Sight (NLOS) and Line Of Sight (LOS)

### PTP 300

The PTP 300 Series Bridge is designed to operate by default in both Non Line Of Sight (NLOS) and Line Of Sight (LOS) environments. However, the PTP 300 web interface includes a Line Of Sight mode control. When this control is enabled, the bridge can operate at higher data throughput rates over a short unobstructed path.

LOS mode is available only where license key enables the capability, the mode is enabled in the Installation Wizard, and the link range is less than 10 km (6.2 miles). A PTP 300 bridge operating in LOS mode has the same throughput capacity as a PTP 500 Lite bridge.

### PTP 500

The PTP 500 Series Bridge is designed to operate in both Non Line Of Sight (NLOS) and Line Of Sight (LOS) environments. The LOS mode feature is not available in the PTP 500.

# OFDM and channel bandwidth

The PTP 300 and PTP 500 Series transmit 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 all the sub-carriers is high. OFDM works exceptionally well over a Non-Line-of-Sight (NLoS) channel.

The channel bandwidth of the OFDM signal is configurable to one of three values: 5 MHz, 10 MHz and 15 MHz. Higher bandwidths provide greater link capacity at the expense of using more spectrum. Systems configured for a narrower channel bandwidth provide better receiver sensitivity and can also be an appropriate choice in deployments where the amount of free spectrum is limited.

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

**NOTE**

The Channel Bandwidth must be configured to the same value at both ends of the link.

# Spectrum management

The spectrum management feature of the PTP 300 and PTP 500 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 system performs two mean signal measurements per TDD cycle, per channel. This mean measurement represents the mean received signal power for the 40 microseconds measurement period.

The Spectrum Management algorithm collects measurements equally from all channels. This process is called the Channel Availability Check (hereafter referred to by the acronym 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. The analysis produces three key metrics for each channel:

- Peak of Means
- 99.9% Percentile of the Means
- Mean of Means

These metrics are defined in Interpreting the spectrum management plots on page 7-25.

## Statistical summary

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

## Spectrum management in fixed frequency mode

The transmit and receive frequencies can be fixed in a PTP 300 or PTP 500 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 (see Step 2: Wireless configuration on page 6-31). Care must also be taken to ensure that the frequency allocations at each end of the link are compatible.

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

# Adaptive modulation

The PTP 300 and PTP 500 Series can transport data over the wireless link using a number of different modulation modes ranging from 64QAM 0.83 to BPSK 0.50. For a given channel bandwidth and TDD frame structure, each modulation mode transports data at a fixed rate. Also, the receiver requires a given signal to noise ratio in order to successfully demodulate a given modulation mode. Although the more complex modulations such as 64QAM 0.83 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 system 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 system to operate in challenging none line of sight radio channels.

Specifications of capacity for all channel bandwidths, modulation modes and configurations are provided in Data throughput capacity on page 4-80.

Specifications of receive level thresholds for each modulation mode (assuming no interference) are provided in the various system threshold tables in Chapter 4 Reference information.

**NOTE**

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

# MIMO

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

The PTP 300 and PTP 500 transmit two signals on the same radio frequency, one of which is vertically polarized and the other horizontally polarized. The system also has the ability to adapt between two modes of operation:

- **Dual Payload**: When the radio channel conditions allow, the system 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 system.
- **Single Payload**: As the radio channel becomes more challenging, the system 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 system to operate in challenging non- line of sight radio channels.

The two modes have been implemented by the introduction of two sets of modulation modes. The lower order modulations (BPSK 0.50 up to QPSK 0.50) are only available as single payload modes. Each of the higher order modulations (QPSK 0.75 to 64QAM 0.83) 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 1-25.

**NOTE**

The system automatically chooses between dual and single payload to try to increase the capacity of a link. However the user may choose 'single payload only' at installation time, forcing this more robust option.

## Intelligent dynamic frequency selection

The PTP 300 and PTP 500 Series use an interference mitigation technique known as Intelligent Dynamic Frequency Selection (i-DFS). 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 system can continually move channels in response to changes in interference. Two modes of operation are available:

- The first mode is where the two link directions are forced to select the same frequency. This is determined by the Master.
- The second mode is where the frequency of operation can be determined independently for each direction. This uses the CAC measurements. It enables the system to operate successfully in areas where other radio equipments are operating within the same band. It is not permitted in radar regions.

# Radar avoidance

In regions where protection of radars is part of the local regulations, the PTP 300 and PTP 500 must detect interference from radar-like systems and avoid co-channel operation with these systems.

To meet this requirement, the PTP 300 and PTP 500 implement the following features:

- The equipment can only transmit on available channels, of which there are none at initial power up. 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 there is found to be no radar on the channel
- When operating on a channel, the spectrum management algorithm implements a radar detection function which looks for impulsive interference on the operating channel. If impulsive interference is detected, spectrum management will mark the current operating channel as having detected radar (unavailable channel) and initiate a channel hop to an available channel. The previous operating channel will remain in the unavailable state for thirty minutes after the impulsive interference pulse was detected.
- After the thirty minutes have expired the channel will be returned to the usable channel pool.

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

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

**NOTE**

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

## Security

The PTP 300 and PTP 500 Series support optional encryption for data transmitted over the wireless link. The encryption algorithm used is the Advanced Encryption Standard (AES) with 128-bit and 256-bit key size. AES is a symmetric encryption algorithm approved by U.S. Government organizations (and others) to protect sensitive information. The AES implementation in PTP 300 and PTP 500 is approved to FIPS-197.

Encryption is enabled through the purchase of an upgrade.

## Region codes

Some aspects of wireless operation are controlled, enforced or restricted according to a region code. Region codes represent individual countries (for example Denmark) or regulatory regions (for example FCC or ETSI).

Region codes affect the following aspects of wireless operation:

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

A region code is encoded in the license key. The region code can be changed by generating and entering a new license key.

**NOTE**

Some units are supplied with two alternative license keys for different region codes, one of which is factory configured.

**CAUTION**

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

# PTP networks

## Using Intelligent Dynamic Frequency Selection

The Intelligent Dynamic Frequency Selection (i-DFS) feature allows a PTP 300 or PTP 500 unit to select wireless channels for a lower level of radio frequency (RF) interference. This approach is appropriate where the network consists of a small number of PTP links, or where the RF interference is predominantly from equipment belonging to other operators.

## Using frequency planning

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

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

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

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

For help with planning networks, refer to Chapter 2 Planning considerations, or contact your Motorola distributor or re-seller.

### Synchronized networks

TDD synchronization can be used to relax constraints on the frequency planning of PTP 500 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.

**NOTE**

TDD synchronization is not supported in the PTP 300 Series.

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.

## TDD synchronization

### Additional hardware

To synchronize PTP 500 links, one PTP-SYNC unit is required for each master ODU. The PTP-SYNC unit is connected in line in the drop cable between the PIDU Plus and the ODU, and is collocated with the PIDU Plus.

**NOTE**

TDD synchronization is not supported in the PTP 300 Series.

## Timing references for use with PTP-SYNC

PTP-SYNC requires an external timing reference in all but the simplest networks. Up to ten PTP-SYNCs can be connected in a chain to share the timing signal from one timing reference. In the majority of applications, one reference is required for each site that contains master ODUs.

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 following GPS timing receivers:

- Trimble Acutime™ Gold GPS receiver

In simple networks where all master ODUs are at a single site, the external reference can be omitted. In this case, one ODU acts as a reference for other collocated units.

## 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.

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

Link symmetry is always 1:1 in synchronized networks.

## 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.

## Advantages of PTP-SYNC

The advantages of PTP-SYNC over alternative technologies are:

- PTP-SYNC does not require individual GPS receivers, nor must they be located close to the ODUs. This reduces the complexity and the cost of the installation on the mast.
- The GPS receiver can be located anywhere with a clear view of the sky, offering additional flexibility in the installation.
- The PTP-SYNC solution is compatible with standard 1 Hz interfaces, allowing an operator to take advantage of alternative timing references that may be already present at the site.
- The recommended GPS receiver continues to provide accurate timing even after the number of received satellites has dropped down to one, leading to significantly better availability of the reference signal.
- The PTP-SYNC offers the possibility of creating synchronized single-hub networks where no GPS receiver is required.

# Ethernet bridging

## Customer network

### Transparent Ethernet service

The PTP 300 and PTP 500 Series provide an Ethernet service between the Ethernet port at a local ODU and the Ethernet port 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, 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 is 2000 octets.

### Layer two control protocols

The PTP 300 and PTP 500 Series are 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 system does not generate or respond to any L2CP traffic.

### Quality of service for bridged Ethernet traffic

The PTP 300 and PTP 500 Series support eight traffic classes for Ethernet frames queued for transmission over the wireless link. Ethernet frames are classified by inspection of the Ethernet priority code point in the outermost VLAN tag.

The system provides a configurable mapping between Ethernet priority and traffic class, together with a simple way to restore a default mapping based on the recommended default in IEEE 802.1Q-2005. Untagged frames can be classified into any one of the eight classes.

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 300 and PTP 500 Series minimize 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.

## Management network

### IP interface

The PTP 300 and PTP 500 ODU contains an embedded management agent with a single IP interface. Network management communication is exclusively based on IP and associated higher layer transport and application protocols. The default IP address of the management agent is 169.254.1.1 in the master ODU and 169.254.1.2 in the slave ODU. The products do not require use of supplementary serial interfaces.

### MAC address

The management agent end-station MAC address is recorded on the enclosure. The MAC address is not configurable by the user.

### VLAN membership

The management agent can be configured to transmit and receive either untagged, priority-tagged, C-tagged (IEEE 802.1Q) or S-tagged (IEEE 801.ad) frames. S-tagged frames must be single tagged, in other words, an S-tag with no encapsulated C-tag. The VLAN ID can be 0 (priority tagged) or in the range 1 to 4094.

### In-band management

In the in-band management mode, the management agent can be reached from the Ethernet port at the local ODU, and (assuming that the wireless link is established) the Ethernet port at the remote ODU.

Management frames in the customer network are processed by the management agent if (a) destination MAC address in the frame matches the CMU 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 network.

### In-band quality of service

Frames generated within the management agent may be assigned a configured Ethernet priority. Management frames are multiplexed with customer frames of the same priority for transmission at the wireless port.

### Source address learning

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

### Wireless link down alert

The PTP 300 and PTP 500 Series provide an optional indication of failure of the wireless link by means of a brief disconnection of the data port. The Wireless link down alert can be used to trigger protection switching by Spanning Tree Protocol (STP) or Ethernet Automatic Protection Switching (EAPS) in a redundant network.

## Back-to-back links

PTP 300 and PTP 500 will not operate correctly if a direct cabled connection is made between two PIDUs. Where two or more links are deployed in a chain, always use an Ethernet switch or router to interconnect the links at the relay points.

# Protocol model

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

- Ethernet Port
- Wireless Port

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

Protocol layers involved in bridging between Ethernet and wireless interfaces are shown in Figure 1-17. Protocol layers involved in bridging between external interfaces and the management agent are shown in Figure 1-18. In these figures, the layers have the meanings defined in IEEE 802.1Q-2005.

**Figure 1-17** Protocol layers between Ethernet and wireless interfaces

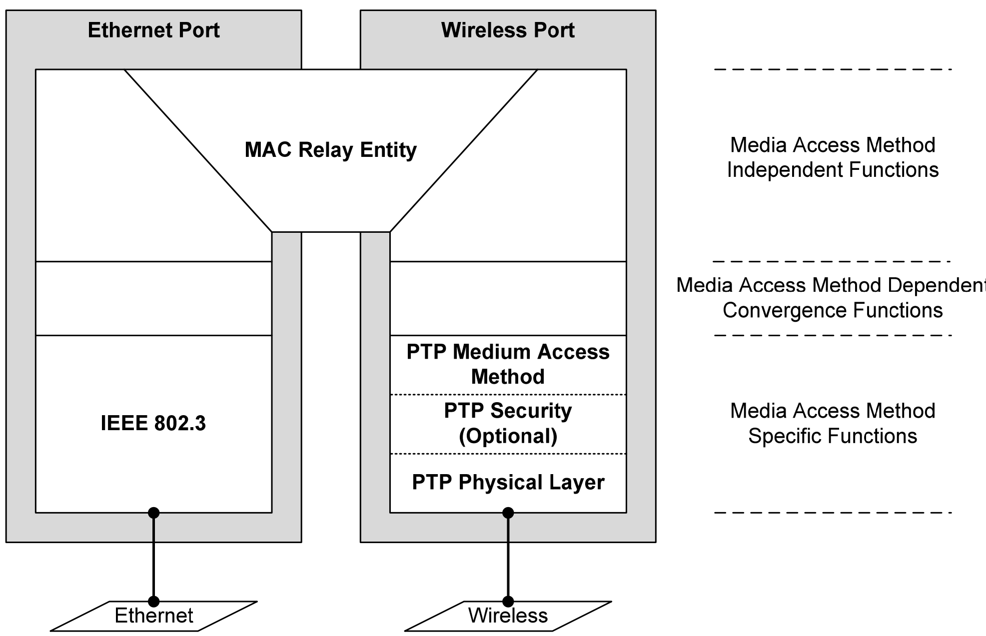
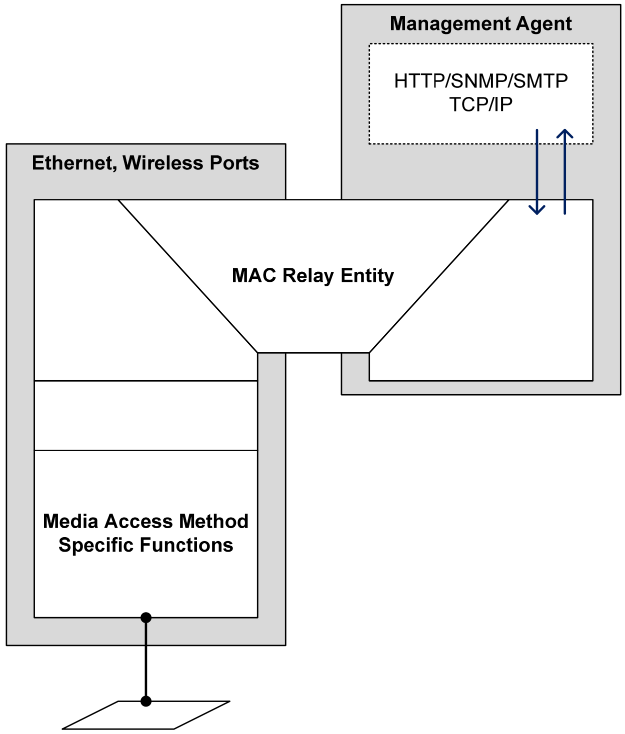


**Figure 1-18** Protocol layers between external interfaces and the management agent



# Telecoms circuits

The PTP 300 and PTP 500 provide native support for one E1 link, or one T1 link. The link relays unstructured E1 or T1 data and provides accurate timing transfer.

## Lowest telecoms modulation mode

In narrow channel bandwidth 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 telecoms 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 Telecoms Modulation Mode" during installation. Appropriate settings for this control may be determined by using the PTP LINKPlanner tool. The reduction in latency is achieved by disabling the relay of telecoms data in lower modulation modes, and this necessarily results in somewhat lower availability for the telecoms circuit. The loss of availability can be estimated using the PTP LINKPlanner.

The unit will override the user setting of Lowest Telecoms Modulation Mode if the selected mode has insufficient capacity to carry the telecoms data, or if the mode demands very high latency and requires more buffering than the link can provide. When the effective mode differs for Single and Dual Payload operation two modes will be displayed: "Lowest Dual Payload Modulation Mode" and "Lowest Single Payload Modulation Mode".

## Fixed frequency operation

In a PTP 300 or PTP 500 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 Telecoms traffic by preventing channel changes initiated by i-DFS. This can be achieved by barring all channels except one in the Spectrum Management page, or alternately 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.

## Further reading

Installation is described in Installing an E1 or T1 interface on page 5-41.

Configuration is described in Task 8: Configuring wireless and telecoms interfaces on page 6-26.

Testing is described in Performing a telecoms loopback test on page 8-19.

# System management

## Management agent

PTP 300 and PTP 500 equipment is managed through an embedded management agent. Management workstations, network management systems or PCs can be connected to this agent using standard management protocols multiplexed with user traffic at the Ethernet data port.

The management agent supports the following interfaces:

- Hyper text transfer protocol (HTTP)
- TELNET
- Simple network management protocol (SNMP)
- Simple mail transfer protocol (SMTP)
- Simple network time protocol (SNTP)

## Web server

The PTP 300 and PTP 500 management agent contains a web server. The web server supports the HTTP interface.

Web-based management offers a convenient way to manage the 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 system installation, and for the majority of configuration management tasks.

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 system.
- **System:** These web-pages are used for configuration management, including IP and Ethernet, AES encryption keys, quality of service, software upgrade and installation of license keys. The System pages additionally provide detailed counters and diagnostic measurements used for performance management.
- **Installation:** The Installation Wizard is used in the initial configuration of the system and arming the unit ready for alignment.
- **Management:** These web-pages are used to configure the network management interfaces.
- **Change Password**: The Change Password web-page changes the web-interface password of the active user. Users use this screen to change their own password.
- **Logout:** Allows a user to log out from the web-based interface.

## 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.
- PTP 300 and PTP 500 Series proprietary MIB.

# SNMPv3 security

## SNMP Engine ID

PTP 300 and PTP 500 support three different formats for SNMP Engine ID:

- MAC address
- IP address
- Configurable text string

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

## User-based security model

PTP 300 and PTP 500 support 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 AES upgrade described in AES license on page 1-46. The ODU will allow the creation of users configured with AES privacy protocol, regardless of license key. However, a user configured to use AES privacy protocol will not be able to transmit and receive encrypted messages unless the license key enables the AES capability.

## View-based access control model

PTP 300 and PTP 500 support 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). It is not possible to read or modify AES keys used to encrypt data transmitted at the wireless interface.

## MIB-based management of SNMPv3 security

PTP 300 and PTP 500 support 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.

The system 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 IP Address AND the IP 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 4-55.

The system 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 1-42. 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 300 and PTP 500 support 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 IP Address and the IP 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 license key so as to disable the AES capability when SNMPv3 users are configured with AES privacy and VACM is configured to require privacy. In this case, recovery is by either (a) restoring the correct license key, or (b) using recovery mode to erase all configuration and entering new configuration.

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

## AES license

PTP 300 and PTP 500 provide optional encryption using the Advanced Encryption Standard (AES). Encryption is not available in the standard system.

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

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

AES encryption may be used in the following ways:

- At the wireless port to encrypt data transmitted over the wireless link.
- At the SNMP management interface in the SNMPv3 mode.

Two levels of encryption are available to purchase:

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

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

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

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

For more information, see:

- Task 4: Installing license keys on page 6-14
- Task 6: Configuring security on page 6-22

## Critical security parameters

Critical security parameters (CSPs) are as follows:

- AES encryption keys for the wireless interface.
- User account password for the web-based interface.

## Capacity upgrades

Capacity upgrades are supplied as an access key purchased from your Motorola Point-to-Point distributor or solutions provider. The upgrade is applied by entering an access key together with the MAC address of the target ODU into the PTP License Key Generator web page, which may be accessed from http://www.motorola.com/ptp/support.

The License Key Generator creates a new license key delivered by email. The license key must be installed on the ODU as described in reference to Task 4: Installing license keys on page 6-14. Once applied, the capacity upgrade is bound to a single ODU and is not transferrable.

## Software upgrade

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

PTP 300 and PTP 500 software images are digitally signed, and the ODU will accept only images that contain a valid Motorola PTP digital signature. The ODU always requires a reboot to complete a software upgrade.

**NOTE**

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

**NOTE**

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 Motorola.

The management process for software upgrade is described in detail in Task 5: Upgrading software version on page 6-17.

Software can be downgraded using Recovery mode as described in Recovery mode on page 1-48.

# Recovery mode

The PTP 300 and PTP 500 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 the PIDU Plus recovery button is pressed at the same time as the ODU is rebooted or power cycled.

## Recovery mode options

Options in recovery mode are as follows:

- Load new main application software.
- Reset all configuration data to factory default. This option resets IP and Ethernet configuration.
- Reset IP and Ethernet configuration to factory default.
- Reboot with existing software and configuration.

**NOTE**

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

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

For detailed instructions on using the recovery mode, see Using recovery mode on page 7-53.

# Chapter 2 Planning considerations

This chapter provides information to help the user to plan a PTP 300 or PTP 500 link.

The following topics are described in this chapter:



To calculate the data throughput capacity of a planned link, see Data rate calculations on page 4-77.

# Spectrum planning

Each frequency variant has specific regulatory restrictions that affect frequency range, radar avoidance  and channel bandwidth usage.

## Conformance to regulations

Ensure the link is configured to conform to local regulatory requirements by installing license keys for the correct region code.

**CAUTION**

For the connectorized model, when using external antennas of higher gain than the appropriate integrated antenna, the regulations may require the maximum Tx power to be reduced. To ensure that regulatory requirements are met for connectorized installations, refer to Regulatory issues with connectorized units on page 4-62.

The license and region codes for each frequency variant are listed in Licenses and region codes on page 4-32.

## Frequency selection

Choose a method of frequency selection. The choice depends upon whether or not the region mandates DFS (radar detection).

### Regions without mandatory radar detection

In regions that do not mandate DFS, choose 'i-DFS' or 'Fixed Frequency':

- **Intelligent Dynamic Frequency Selection (i-DFS)**: In this mode, the unit continually continually monitors the spectrum looking for the channel with the lowest level of interference. Statistical techniques are used to select the most appropriate transmit and receive channels. The unit can be configured such that it operates in i-DFS mode, but does not operate on selected channels. This allows a frequency plan to be implemented in cases where multiple links are installed in close proximity.

- **Fixed Frequency**: In this mode, the unit must be configured with a single fixed transmit frequency and a single fixed receive frequency. These may set to the same value or to different values. This mode should only be considered in exceptional circumstances, for example where it is known that are no sources of interference on the selected channels.

## Regions with mandatory radar detection

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

**NOTE**

The PTP 300 and PTP 500 fully conform to regional regulatory requirements for radar avoidance.

In DFS regions, choose ‘DFS’ or ‘DFS with i-DFS’:

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

**NOTE**

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

- For the EU: in specification EN 301-893 version V1.5.1.
- For the US: in the specification FCC part 15.407 plus the later requirements covered in **Important Regulatory Inofrmation** in this User Guide.
- For Canada: in the specification RSS210 Annex 9 (Issue 7).

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

## Available spectrum

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

Of particular note, is that certain regulations have allocated certain channels as unavailable for use:

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

For details of these restrictions, refer to Licenses and region codes on page 4-32.

Where regulatory restrictions apply to certain channels, these channels are barred automatically by the use of the correct licence key and region code. For example, at 5.8 GHz in the UK and some other European countries, the RTTT band 5795 MHz to 5815 MHz is barred. With the appropriate license key installed for this region, the PTP 500 will not operate on channels within this band.

The number and identity of channels barred by the licence key and region code is dependent on the channel bandwidth and channel raster selected.

Barred channels are indicated by a ‘No Entry’ symbol displayed on the Spectrum Management web page, see Spectrum management in radar avoidance mode on page 7-29.

## Avoidance of weather radars (USA only)

To comply with FCC rules, units which are installed within 35 km of a Terminal Doppler Weather Radar (TDWR) system (or have a line of sight propagation path to such a system) must be configured to avoid any frequency within +30 MHz or –30 MHz of the frequency of the TDWR device.

When planning a link in the USA, visit http://spectrumbridge.com/udrs/home.aspx, enter the location of the planned link and search for TDWR radars. If the search result lists one or more TDWR radars within 35 km (22 miles), perform the following tasks:

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

⚠ CAUTION

To comply with FCC rules, the affected channels must be barred during staging, before the units are allowed to radiate on site, as described in Chapter 6 Configuration and alignment.

## Channel bandwidth

Select the required channel bandwidth for the link.

The channel bandwidth may be set to 5 MHz, 10 MHz or 15 MHz. The wider the channel bandwidth, the greater the capacity.

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

NOTE

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

# Site planning

This section describes factors to be taken into account when choosing sites for the ODU, PIDU Plus and PTP-SYNC unit (if installed).

## ODU site selection

When selecting a site for the ODU, consider the following factors:

- Height and location to ensure that people are kept away from the antenna; see Calculated distances and power compliance margins on page 4-67.
- Height and location to achieve the best radio path.
- Height in relation to other objects with regard to lightning strikes.
- Aesthetics and planning permission issues.
- Cable lengths; see Maximum cable lengths on page 2-7.
- The effect of strong winds on the installation; see Wind loading on page 2-7.

## PIDU Plus site selection

When selecting a site for the PIDU Plus, consider the following factors:

- Indoor location with no possibility of condensation.
- Availability of a mains electricity supply.
- Accessibility for viewing status indicators and pressing Recovery switch.
- Cable lengths; see Maximum cable lengths on page 2-7.

## PTP-SYNC site selection

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

- Indoor location, or outdoor in a weatherproofed cabinet, with no possibility of condensation.
- Accessibility for viewing status indicators.
- Cable lengths; see Maximum cable lengths on page 2-7.

A rack mounting adaptor is available for the PTP-SYNC unit.

# Maximum cable lengths

The maximum permitted lengths of interface cables in PTP 300 or PTP 500 installations are specified in Table 2-1.

**Table 2-1** Maximum cable lengths

| Interface type | Maximum length | Comment |
|---|---|---|
| Copper Ethernet | 100 m (330 ft) | ODU to network terminating equipment |
| E1 | 100 m (330 ft) | ODU to network terminating equipment |
| T1 | 100 m (330 ft) | ODU to network terminating equipment |

# Wind loading

Ensure that the site will not be prone to excessive wind loading.

Antennas and equipment mounted on towers or buildings will subject the mounting structure to significant lateral forces when there is appreciable wind. Antennas are normally specified by the amount of force (in pounds) for specific wind strengths. The magnitude of the force depends on both the wind strength and size of the antenna.

## Calculation of lateral force

The ODU, with or without the integral antenna, is essentially a flat structure and so the magnitude of the lateral force can be estimated from:

Force (in pounds) = 0.0042 . A . $v^2$

Where A is the surface area in square feet and v is the wind speed in miles per hour.

The lateral force produced by a single PTP 300 or PTP 500 ODU (integrated or connectorized model) at different wind speeds is shown in Table 2-2 and Table 2-3.

**Table 2-2** Lateral force – metric

| | Largest Surface Area (sq m) | Lateral Force (Kg) at wind speed (m/s) | | | | |
|---|---|---|---|---|---|---|
| | | 30 | 40 | 50 | 60 | 70 |
| **Integrated ODU** | 0.130 | 12 | 22 | 34 | 49 | 66 |
| **Connectorized ODU** | 0.093 | 9 | 16 | 24 | 35 | 48 |

**Table 2-3** Lateral force – US

| | Largest Surface Area (sq ft) | Lateral Force (lb) at wind speed (mph) | | | | |
|---|---|---|---|---|---|---|
| | | 80 | 100 | 120 | 140 | 150 |
| **Integrated ODU** | 1.36 | 36.6 | 57.1 | 82.3 | 146.2 | 228.5 |
| **Connectorized ODU** | 1.00 | 26.9 | 42 | 60.5 | 107.5 | 168.0 |

**NOTE**

When the connectorized ODU is used with external antennas, the figures from the antenna manufacturer for lateral force should be included to calculate to total loading on the mounting structure.

## Capabilities of the PTP 300 and PTP 500 Series

The structure and mounting brackets of the ODU are capable of withstanding wind speeds up to 242 kph (151 mph). Ensure that the structure to which the ODU is fixed to is also capable of withstanding the prevalent wind speeds and loads.

## Wind speed statistics

Contact the national meteorological office for the country concerned to identify the likely wind speeds prevalent at the proposed location.  Use this data to estimate the total wind loading on the support structures. Sources of information:

- US National Weather Service, http://www.nws.noaa.gov/
- UK Meteorological Office, www.meto.gov.uk

# Link planning

Link planning must take account of range, obstructions and path loss.

## Range and obstacles

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

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

The PTP 300 and PTP 500 Series are designed to operate in Non-Line-of-Sight (NLoS) and Line-of-Sight (LoS) environments. An NLOS environment is one in which there is no optical line-of-sight, that is, there are obstructions between the antennas.

The bridge operates at ranges from 100 m (330 ft) to 250 km (155 miles). Operation of the system will depend on obstacles in the path between the units. Operation at 40 km (25 miles) or above requires a near line of sight path. Operation at 100m (330 ft) may be achieved with one unit totally obscured from the other unit, but with the penalty of transmitting at higher power in a non-optimal direction, thereby increasing interference in the band.

**NOTE**

In radar detection regions, the minimum LoS operating range with integrated antennas is 300 meters (990 ft). When higher gain connectorized antennas are used, operation with a predicted receiver signal level of 45 dBm or higher is not recommended.

## PTP LINKPlanner

The Motorola PTP LINKPlanner software and user guide may be downloaded from http://www.motorola.com/ptp/support.

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

## PTP LINKPlanner for synchronized networks (PTP 500 only)

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

## Using Line Of Sight Mode (PTP 300 only)

To permit higher data throughput rates over links of range 10 km (6.2 miles) or less, the PTP 300 Series Bridge can be configured to operate with Line Of Site mode enabled.

The line of sight capability must be enabled in the license key. This requires purchase of an upgrade access key.

Line Of Site mode may be used only when the path is completely unobstructed and the link range is less than 10 km (6 miles). An unobstructed path is one in which the first Fresnel zone is clear of obstructions and there is zero excess path loss. The PTP LINKPlanner provides capabilities to check for obstructions in the path.

**⚠ CAUTION**

The link may suffer severely reduced data rate and availability if the LOS mode is enabled in a link with an obstructed path.

The Line Of Sight mode control is in the Installation Wizard. If the user selects LOS mode and the link range clearly exceeds 10 km (6.2 miles), the unit automatically disables LOS mode and data rates, and raises a "Line Of Sight Mode Inactive" front panel alarm and email alert.

## Path loss considerations

Path loss is the amount of attenuation the radio signal undergoes between the two ends of the link.

### Calculating path loss

The path loss is the sum of the attenuation of the path if there were no obstacles in the way (Free Space Path Loss), the attenuation caused by obstacles (Excess Path Loss) and a margin to allow for possible fading of the radio signal (Fade Margin). The calculation of Equation 2-1 needs to be performed to judge whether a particular link can be installed.

**Equation 2-1** Path loss

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

Where is

| | |
|---|---|
| $L_{free\_space}$ | Free Space Path Loss (dB) |
| $L_{excess}$ | Excess Path Loss (dB) |
| $L_{fade}$ | Fade Margin Required (dB) |
| $L_{seasonal}$ | Seasonal Fading (dB) |
| $L_{capability}$ | Equipment Capability (dB) |

## Adaptive modulation

Adaptive modulation ensures that the highest throughput that can be achieved instantaneously will be obtained, taking account of propagation and interference. When the link has been installed, web pages provide information about the link loss currently measured by the equipment, both instantaneously and averaged. The averaged value will require maximum seasonal fading to be added, and then the radio reliability of the link can be computed.

For minimum error rates on TDM links, the maximum modulation mode should be limited to 64QAM 0.75.

The values for (BPSK) are static receive sensitivity measurements. The other values are static receive sensitivity measurements with an AMOD threshold applied. The AMOD threshold applied is for a benign radio channel.

When selecting a modulation mode, the system is influenced by the parameters listed in Table 2-4.

**Table 2-4** Parameters that influence modulation mode selection

| Parameter | Meaning |
|---|---|
| Sensitivity | The combined receive input signal level on both horizontal and vertical inputs that produces a Null BER Error ratio of $3 \times 10^{-7}$. |
| Output Power | Defaults to the region code limit selected for the link in question. The output power will be reduced on the edge channels and may vary if different region codes are selected. |

| Parameter | Meaning |
|---|---|
| AMOD Threshold | The combined receive input signal level on both horizontal and vertical inputs that results in the link consistently entering the receive modulation mode under consideration as the signal level is increased. |
| System Threshold | Thresholds for all modes except BPSK are for the relevant link optimization AMOD thresholds. System threshold for BPSK is the RPSK receive sensitivity. |
| Max Link Loss | The maximum link loss for each modulation mode is derived from the AMOD threshold for that mode (sensitivity threshold for BPSK) and the maximum region 1 center channel output power. The figures assume integral antennas are used, with gain 23 dBi (5.8 GHz and 5.4 GHz). |

## When to install connectorized units

The majority of radio links can be successfully deployed with the integrated PTP 300 or PTP 500 Series. However the integrated units may not be sufficient in some areas, for example:

- Where the path is heavily obscured by dense woodland on an NLOS link.
- Where long LOS links (>80 km or >50 miles) extend over water.
- Where there are known to be high levels of interference.

**NOTE**

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

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

The external antennas can be either dual-polarization (as the integrated antenna) or two single polarized antennas can be used in a spatially diverse configuration. It is expected that the dual-polarization antennas would normally be used to simplify the installation process; spatially diverse antennas may provide additional fade margin on very long LOS links where there is evidence of correlation of the fading characteristics on Vertical and Horizontal polarizations.

## System threshold, output power and link loss

For details of the system threshold, output power and link loss for each frequency variant in all modulation modes for all available channel bandwidths, refer to System threshold, output power and link loss on page 4-41.

# Grounding and lightning protection

Structures, equipment and people must be protected against power surges (typically caused by lightning) by conducting the surge current to ground via a separate preferential solid path.

The actual degree of protection required depends on local conditions and applicable local regulations.

Motorola recommends that PTP 300 and PTP 500 installation is contracted to a professional installer.

WARNING

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

## Standards

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

## Lightning protection zones

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

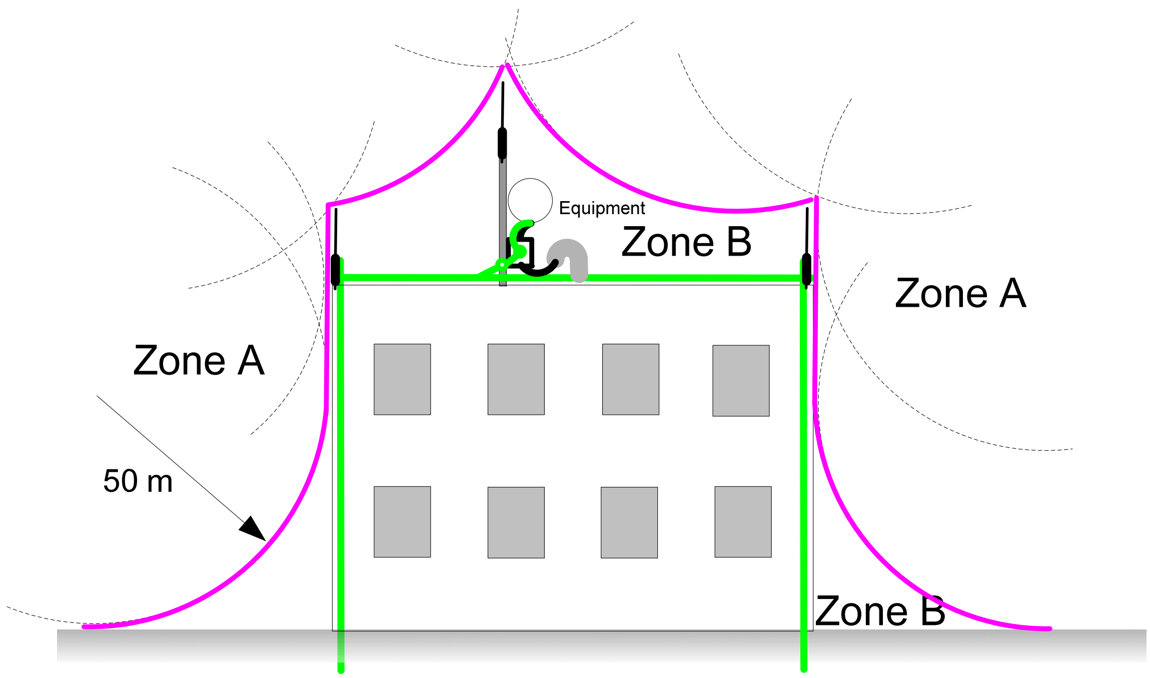
Assess locations on masts, towers and buildings to determine if the location is in Zone A or Zone B:

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

**WARNING**

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

**Figure 2-1** Rolling sphere method to determine the lightning protection zones




## General protection requirements

To adequately protect a PTP 300 or PTP 500 installation, both ground bonding and transient voltage surge suppression are required.

**NOTE**

Where an installation already has, or requires the use of a Master Ground Bar then the requirements of Motorola specification *R56: Standards And Guidelines For Communication Sites (68P81089E50)* take precedence over those in this guide.

## Basic requirements

The following basic protection requirements must be implemented:

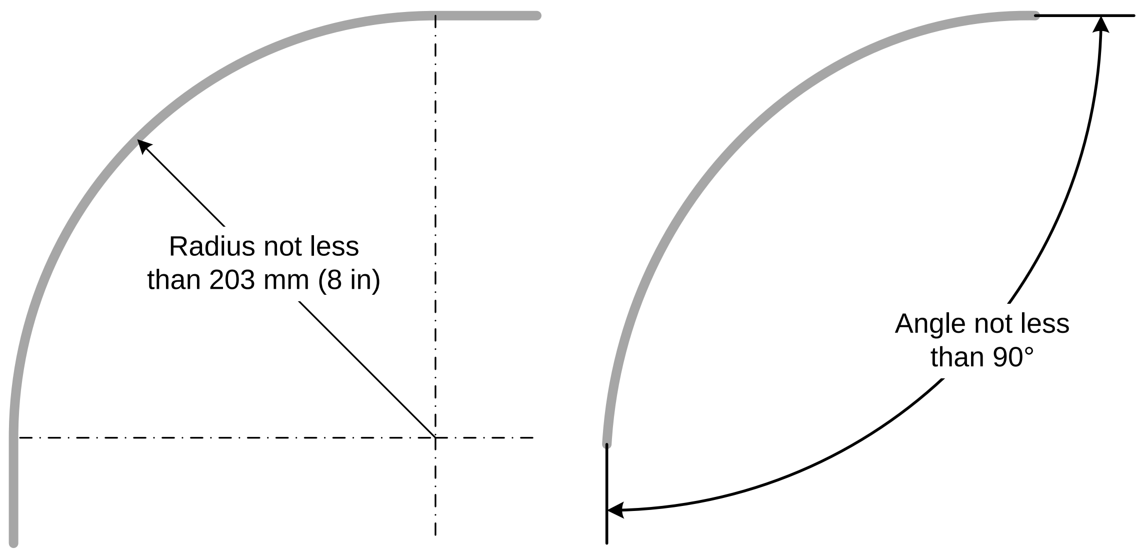
- The equipment (ODU or GPS receiver for PTP-SYNC) must be in ‘Zone B’ (see Lightning protection zones on page 2-14).
- A lightning protection unit (LPU) must be installed within 600 mm (24 in) of the point at which the drop cable enters the building or equipment room.
- The drop cable must be bonded to the supporting structure in order to prevent lightning creating a potential between the structure and cable, which could cause arcing, resulting in fire risk and damage to equipment.
- The drop cable must be grounded at the building entry point.
- The drop cable must not be laid alongside a lightning air terminal.
- 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).

## Grounding cable requirements

When routing, fastening and connecting grounding cables, the following requirements must be implemented:

- Grounding conductors must be run as short, straight, and smoothly as possible, with the fewest possible number of bends and curves.
- Grounding cables must not be installed with drip loops.
- All bends must have a minimum radius of 203 mm (8 in) and a minimum angle of 90° (Figure 2-2). A diagonal run is preferable to a bend, even though it does not follow the contour or run parallel to the supporting structure.
- All bends, curves and connections must be routed towards the grounding electrode system, ground rod, or ground bar.
- Grounding conductors must be securely fastened.
- Braided grounding conductors must not be used.
- Approved bonding techniques must be used for the connection of dissimilar metals.

**Figure 2-2** Grounding cable minimum bend radius and angle




### ODU requirements

The following ODU protection requirements must be implemented:

- The ODU must be grounded to the supporting structure.

## Protection requirements for a mast or tower installation

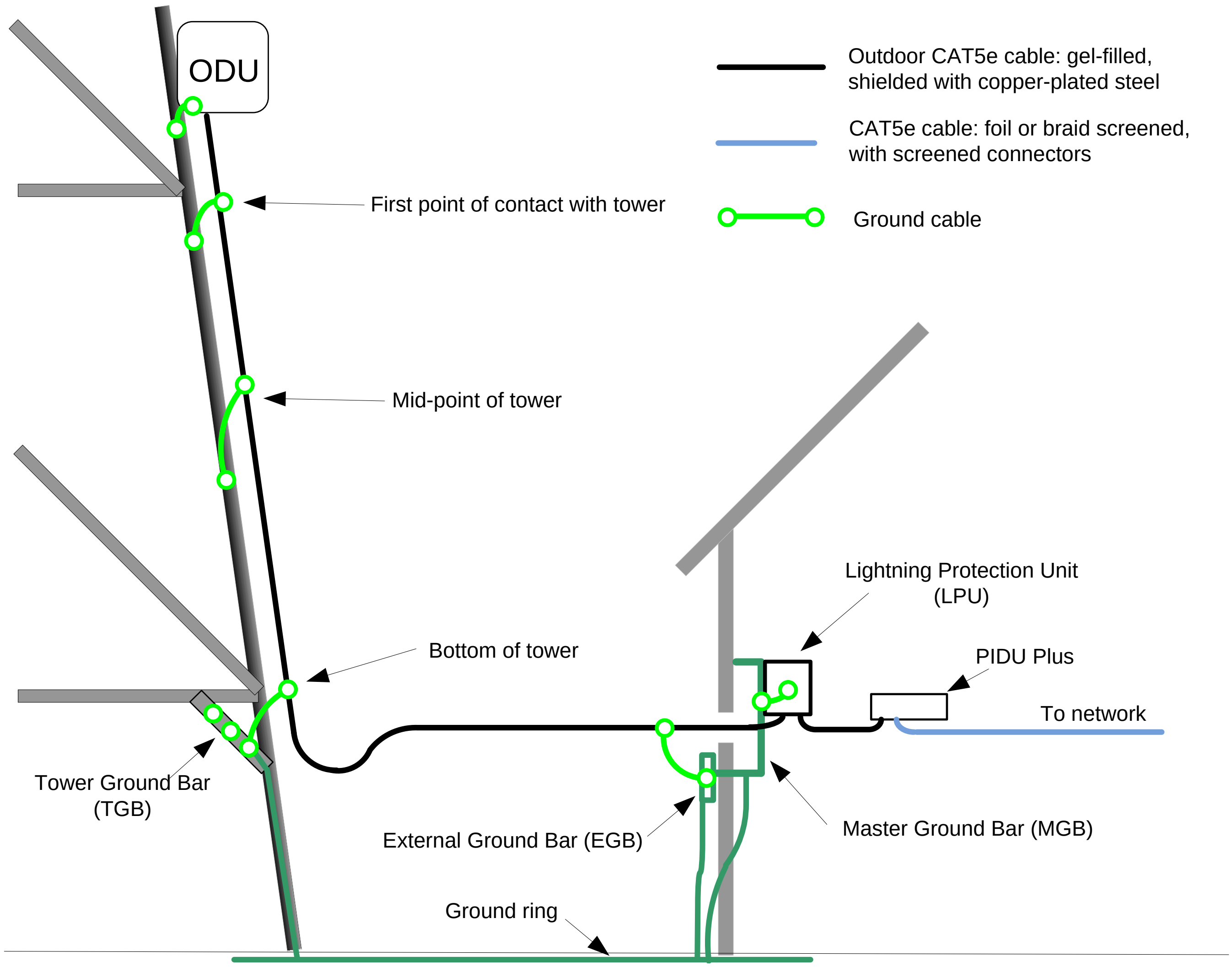
If the ODU is to be mounted on a metal tower or mast, then in addition to the general protection requirements (above), the following requirements must be observed:

- The equipment must be lower than the top of the tower or its lightning air terminal.
- The metal tower or mast must be correctly grounded.
- A grounding kit must be installed at the first point of contact between the drop cable and the tower, near the top.
- A grounding kit must be installed at the bottom of the tower, near the vertical to horizontal transition point. This grounding kit must be bonded to the tower or tower ground bus bar (TGB), if installed.
- If the tower is greater than 61 m (200 ft) in height, an additional grounding kit must be installed at the tower midpoint. Additional ground kits must be installed as necessary to reduce the distance between ground kits to 61 m (200 ft) or less.

- In high lightning prone geographical areas, additional ground kits should be installed at spacing between 15 to 22 m (50 to 75 ft). This is especially important on towers taller than 45 m (150 ft).

Schematic examples of mast or tower installations are shown in Figure 2-3.

**Figure 2-3** Grounding and lightning protection on mast or tower



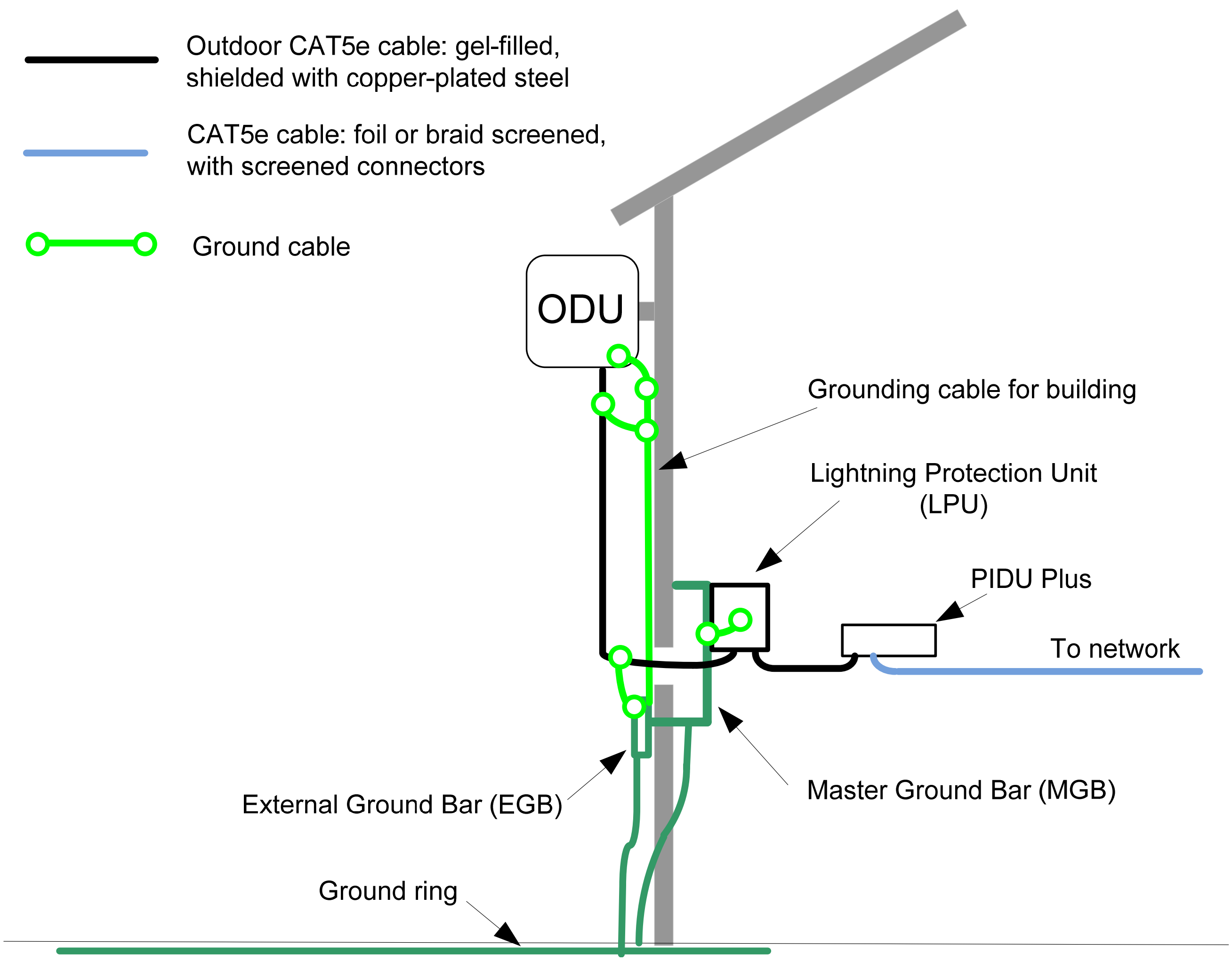
## Protection requirements for a wall installation

If the ODU is to be mounted on the wall of a building, then in addition to the general protection requirements (above), the following requirements must be observed:

- The equipment must be lower than the top of the building or its lightning air terminal.
- The building must be correctly grounded.

Schematic examples of wall installations are shown in Figure 2-4.

**Figure 2-4** Grounding and lightning protection on wall

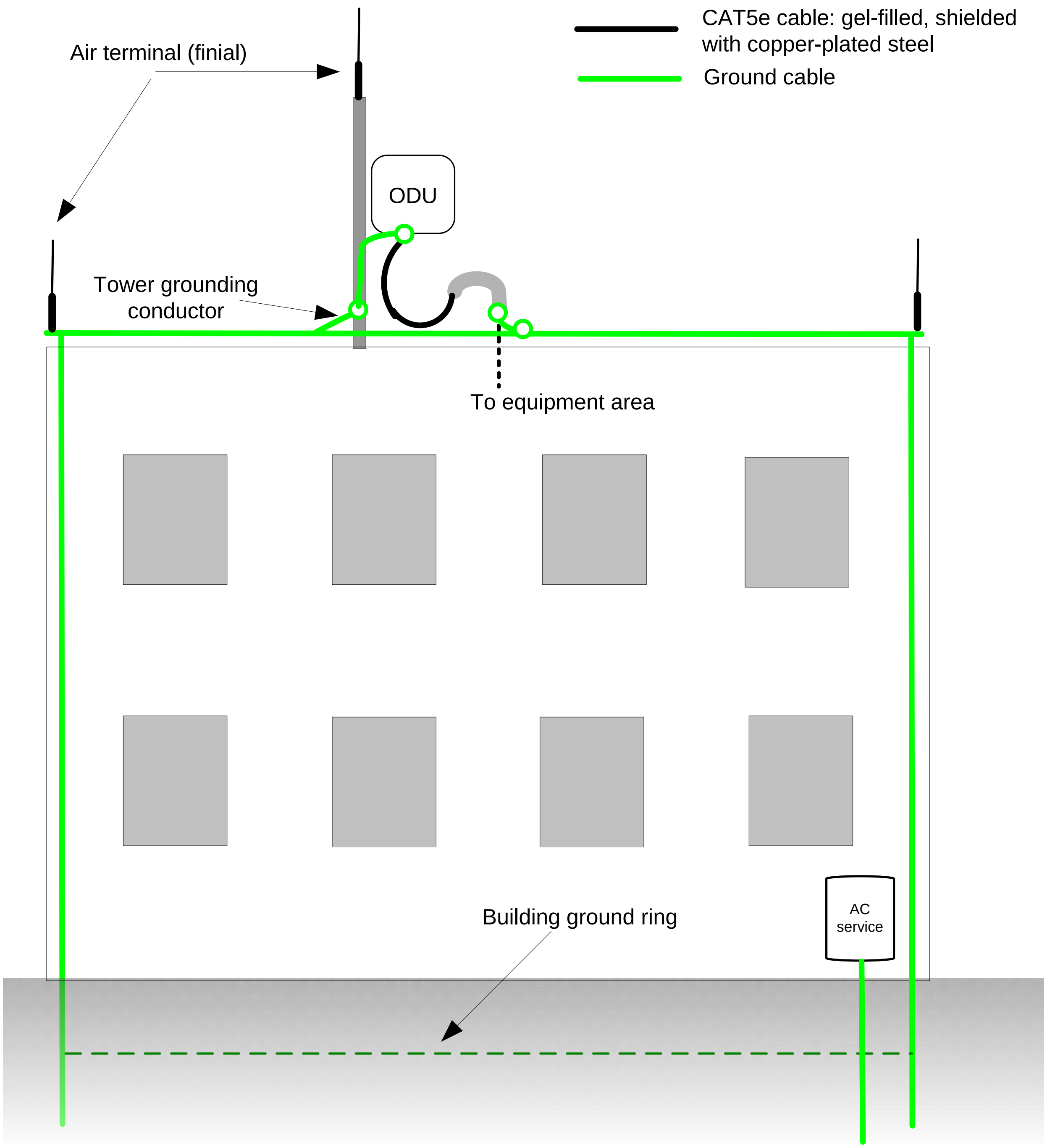


## Protection requirements on a high rise building

If the ODU is to be mounted on a high rise building, it is likely that cable entry is at roof level (Figure 2-5) and the equipment room is several floors below (Figure 2-6). In addition to the general protection requirements (above), the following requirements must be observed:

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

**Figure 2-5** Grounding and lightning protection on building

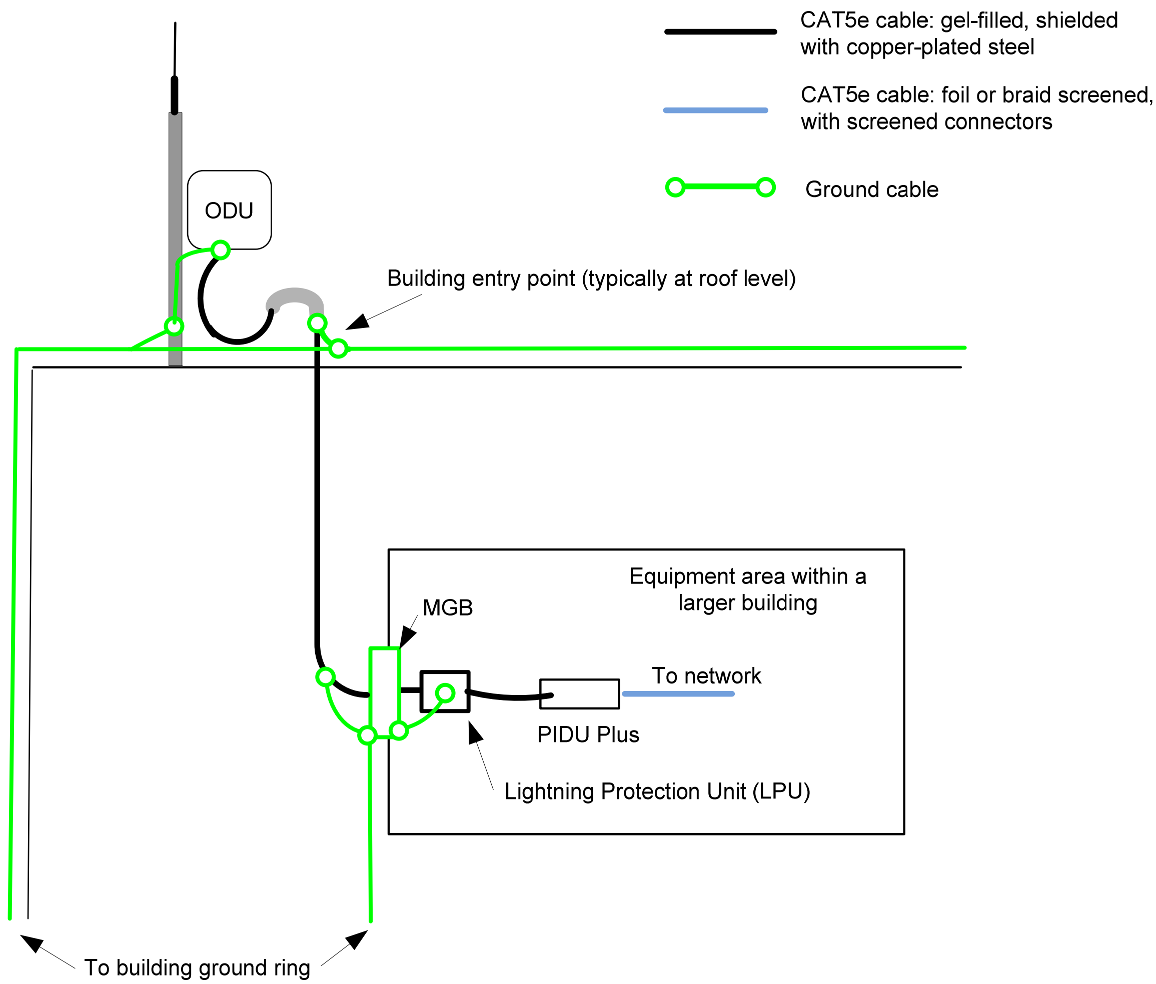


## Protection inside a high rise building

The following protection requirements must be observed inside multi-story or high rise buildings (Figure 2-6):

- The drop cable shield must be bonded to the building grounding system at the entry point to the building.
- The drop cable shield must be bonded to the building grounding system at the entry point to the equipment area.
- An LPU must be installed within 600 mm (24 in) of the entry point to the equipment area.

**Figure 2-6** Grounding and lightning protection inside high building



## Connecting to the grounding conductor

Figure 2-7 and Figure 2-8 illustrate the techniques employed to provide equipment grounding in high rise buildings. A steel component of the building can be used as a grounding conductor, provided it is part of the structural building steel and is effectively grounded.

**Figure 2-7** Grounding in a high rise building – building steel not available

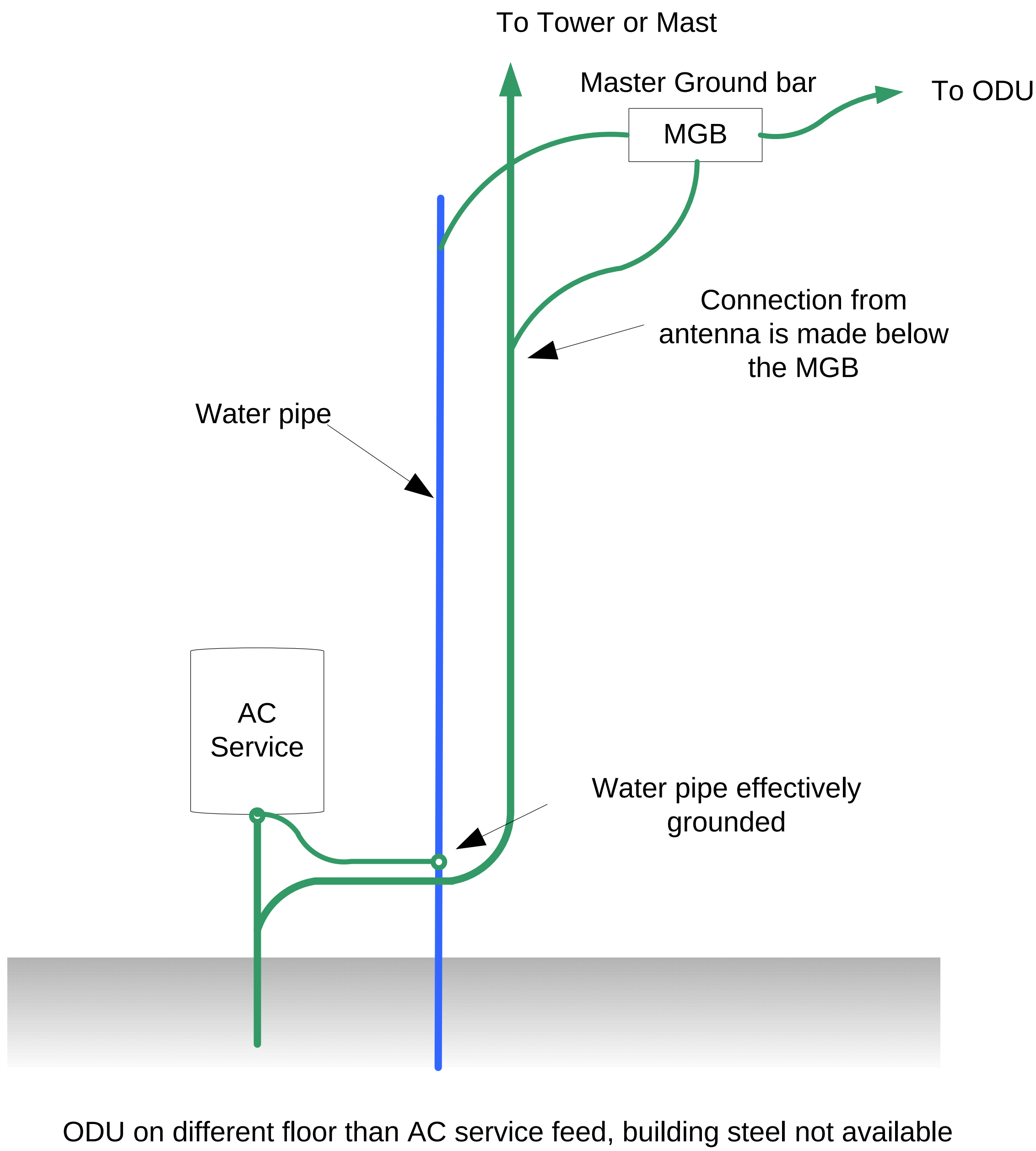
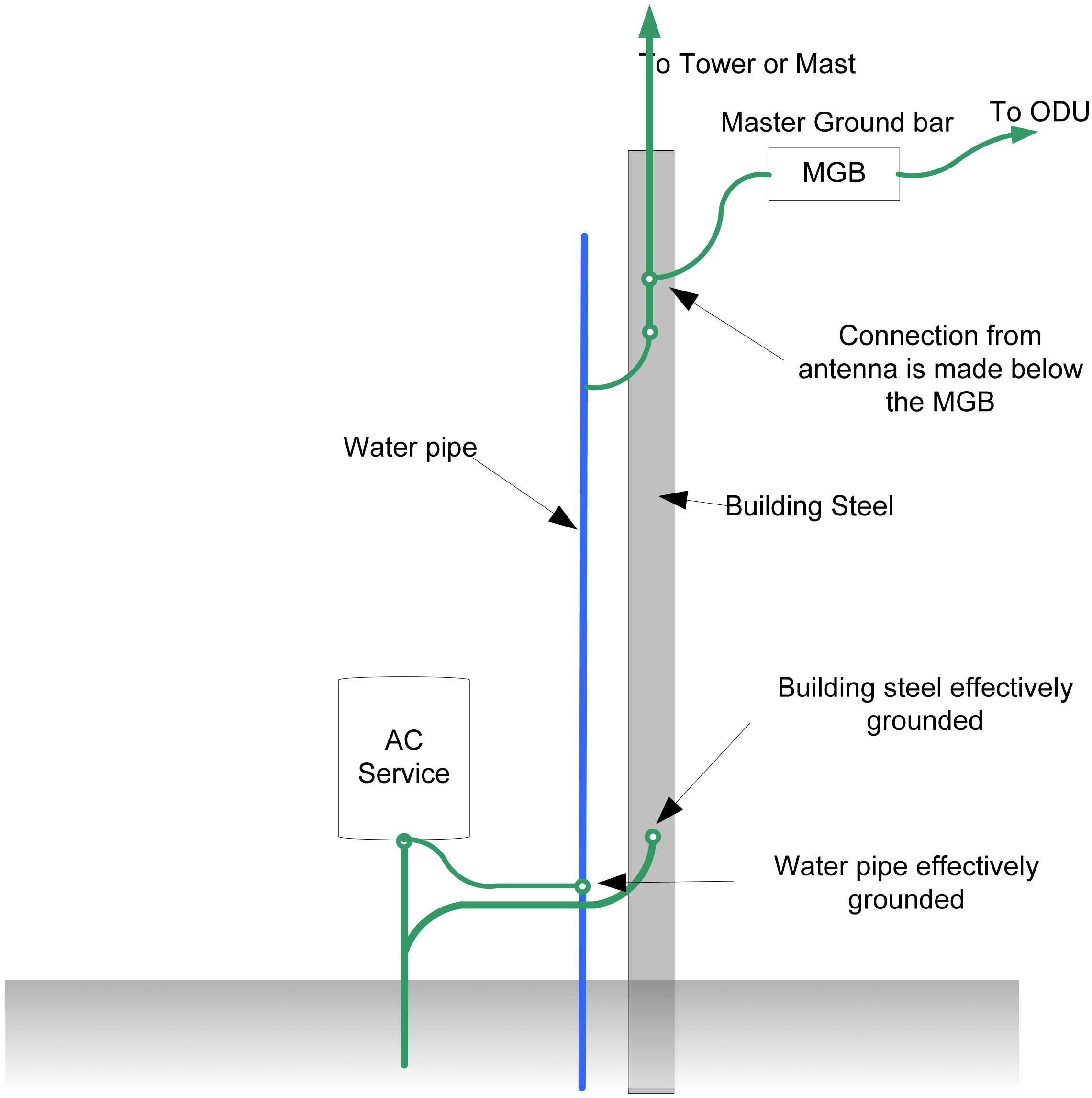


**Figure 2-8** Grounding in a high rise building – building steel available




ODU on different floor than AC service feed, building steel available

# Configuration options for TDD synchronization

This section describes the different configuration options that may be used for implementing TDD synchronization in the PTP 500 Series. Schematic diagrams are included.

**NOTE**

TDD synchronization is not supported in the PTP 300 Series.

## TDD synchronization configurations supported

The PTP 500 series supports the following TDD synchronization configurations:

- Single link configuration with PTP-SYNC.
- Cluster with PTP-SYNC and GPS receiver.
- Cluster with PTP-SYNC and no GPS receiver.

**NOTE**

If PTP-SYNC is the selected TDD synchronization method, select a 1 Hz timing reference for the system. This will normally be a GPS receiver module.

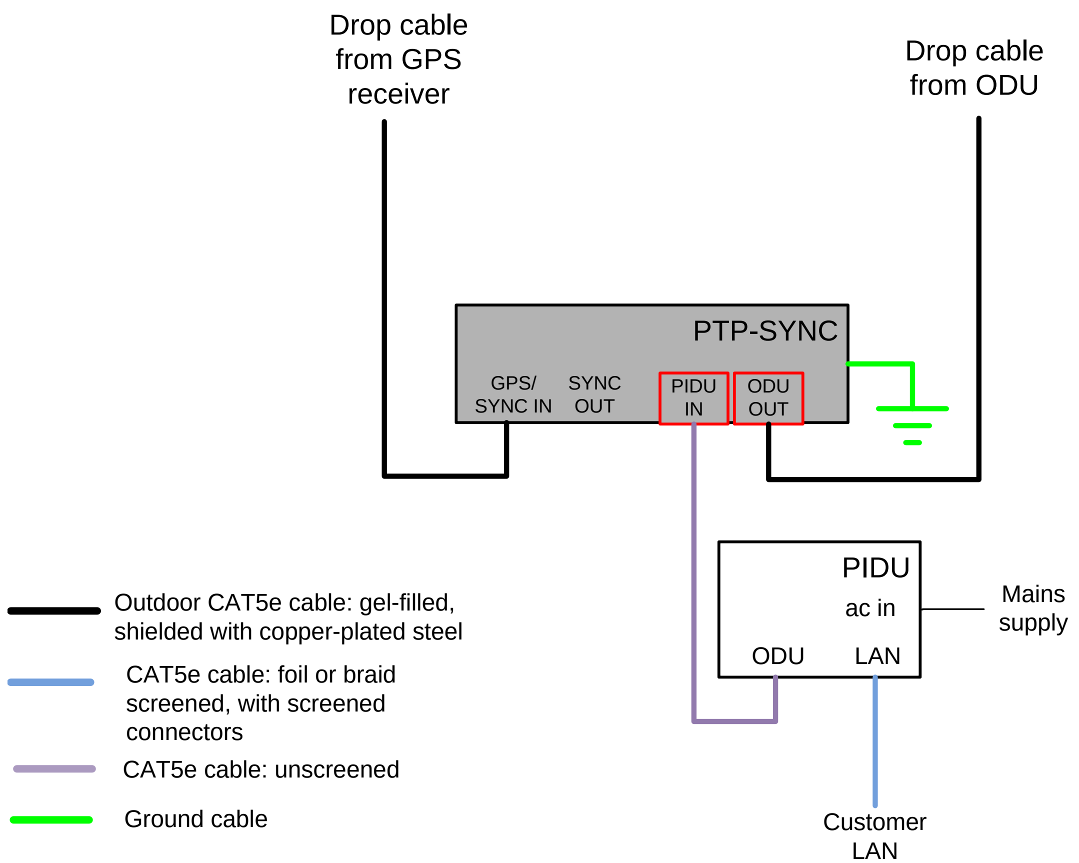
## Single link configuration with PTP-SYNC

Each link requires one PTP-SYNC unit connected to the master ODU and one compatible GPS receiver. Use this configuration where a site contains only one TDD master ODU. The GPS receiver can be replaced by an alternative compatible 1 Hz timing reference (Figure 2-9).

The wireless configuration settings are:

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

**Figure 2-9** TDD synchronization configuration – single link with PTP-SYNC




phn-1115_006v000

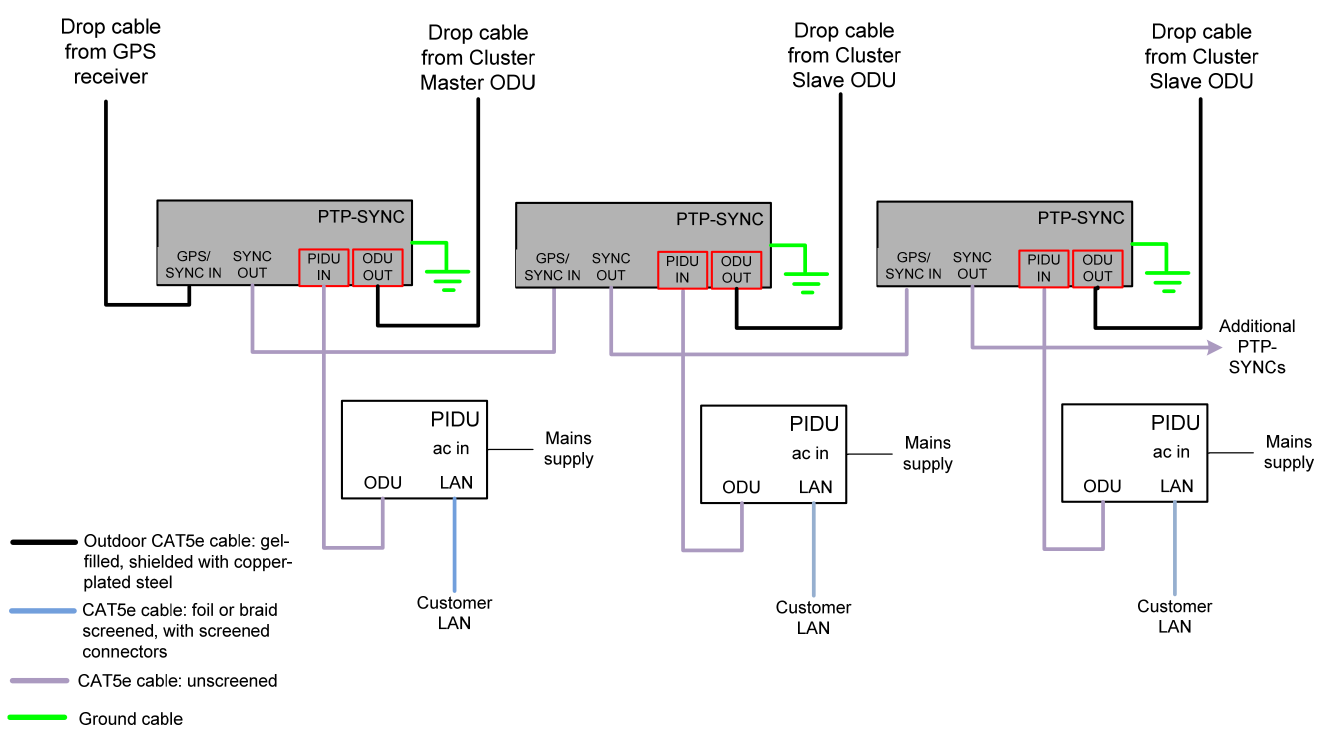
## Cluster with PTP-SYNC and GPS receiver

Each link requires one PTP-SYNC unit. Each site requires one compatible GPS receiver. Collocated PTP-SYNC units are connected together in a daisy-chain. Between two and ten PTP-SYNCs may be chained in this way. Use this configuration where a site contains collocated TDD master ODUs in an extended network and where multiple sites have TDD master ODUs (Figure 2-10).

The wireless configuration settings are:

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

**Figure 2-10** TDD synchronization configuration – cluster with PTP-SYNC and GPS



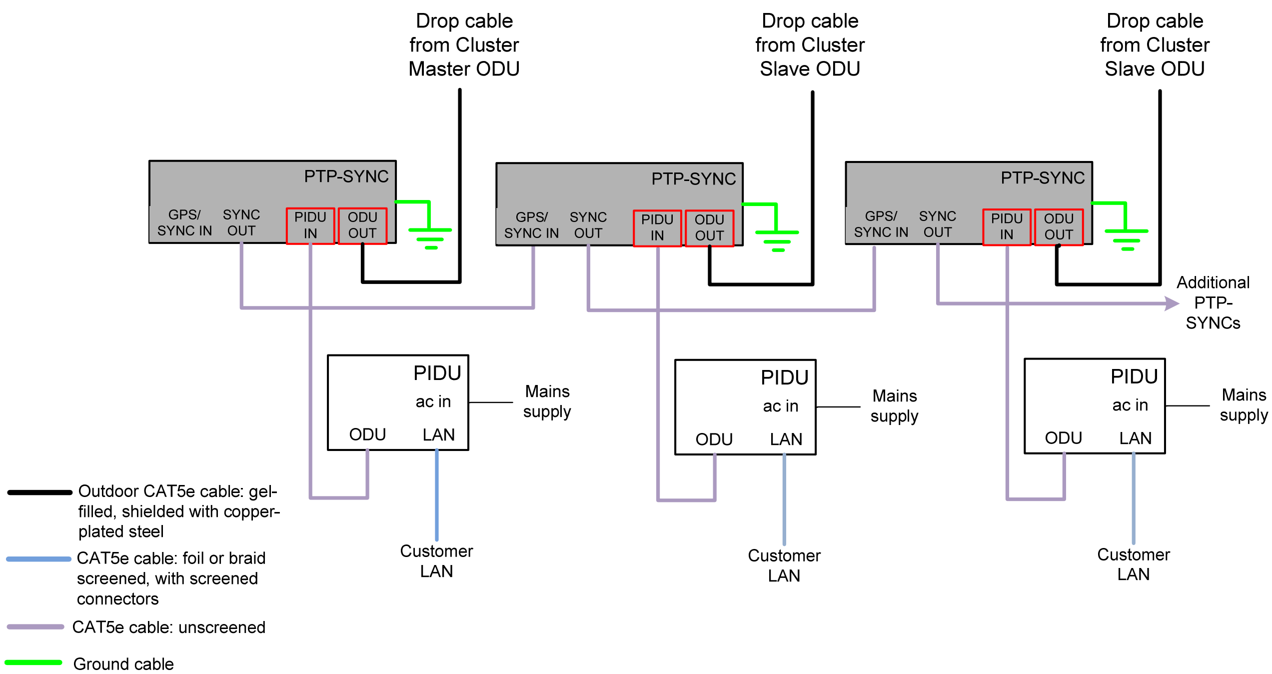
# Cluster with PTP-SYNC and no GPS receiver

Each link requires one PTP-SYNC unit. PTP-SYNC units are connected together in a daisy-chain. Between two and ten PTP-SYNCs may be chained in this way. One ODU is designated as a cluster timing master. Use this configuration where all master ODUs are collocated at a single site. As this configuration does not require a GPS receiver, it provides additional flexibility, particularly in applications requiring rapid deployment (Figure 2-11).

The wireless configuration settings are:

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

**Figure 2-11** TDD synchronization configuration – cluster with PTP-SYNC and no GPS



# Mounting options for the PTP-SYNC GPS receiver

If PTP-SYNC is the selected TDD synchronization method for PTP 500, with a GPS receiver as the timing reference source, then the GPS receiver must be mounted as described in this section.

**CAUTION**

Ensure that the GPS receiver module is mounted in a position where all protection requirements can be met.

## GPS receiver location requirements

The GPS receiver for PTP-SYNC must be mounted at a location that meets the following requirements:

- It must be possible to protect the installation as described in General protection requirements on page 2-15.
- It must have an un-interrupted view of the sky.
- It must receive an adequate signal from at least four GPS satellites.
- It must be mounted at least 1 m (3 ft), preferably 2 m (6 ft), away from other GPS receiving equipment.
- It must not be sited in the field of radiation of co-located radio communications equipment and should be positioned at a distance of at least 3 m (10 ft) away.

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

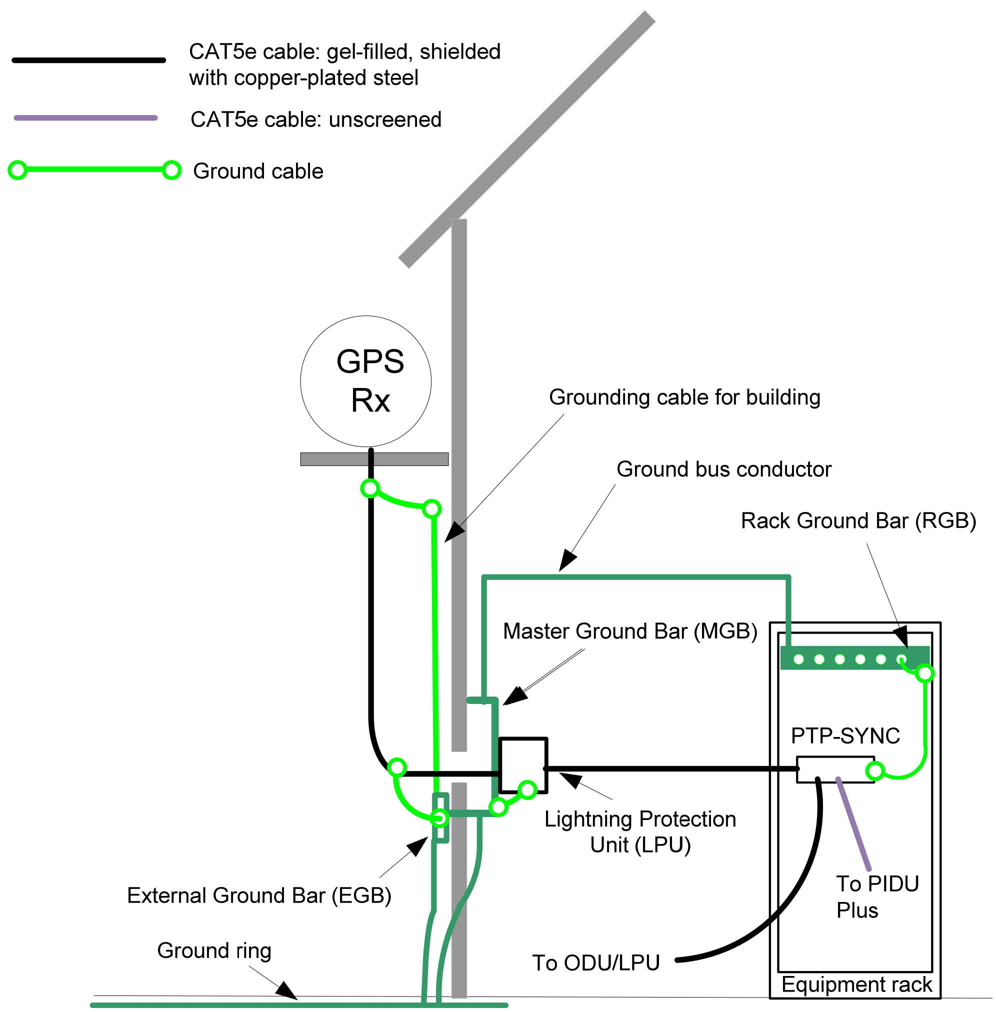
## Mounting the GPS receiver module on the equipment building

If mounting the GPS receiver for PTP-SYNC on the equipment building (Figure 2-12), select a position on the wall that meets the following requirements:

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

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

**Figure 2-12** Grounding and lightning protection for GPS receiver on building

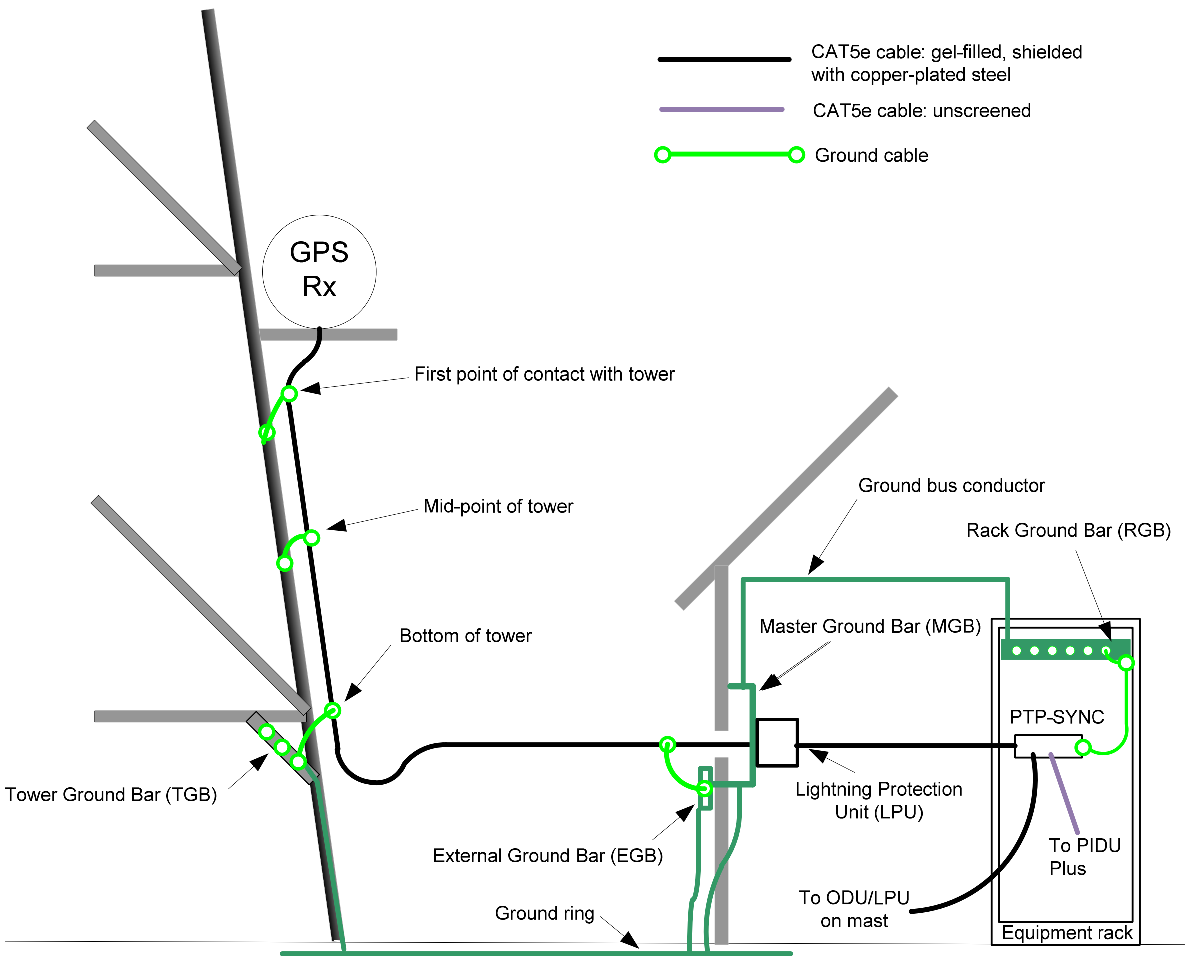


## Mounting the GPS receiver module on a metal tower or mast

If mounting the GPS receiver module on a metal tower or mast (Figure 2-13), select a position that meets the following requirements:

- It must not be mounted any higher than is necessary to receive an adequate signal from four GPS satellites.
- It must be protected by a nearby lightning air terminal that projects further out from the tower than the GPS receiver module.
- It must meet all the requirements stated in Protection requirements for a mast or tower installation on page 2-17.

**Figure 2-13** Grounding and lightning protection for GPS receiver on tower or mast



# Data network planning

## VLAN membership

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

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

## Priority for management traffic

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

## IP interface

Choose an IP address for the IP interface of the ODU management agent. The IP address must be unique and valid for the connected network segment and VLAN.

Find out the correct subnet mask and gateway IP address for this network segment and VLAN.

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

## Quality of service for bridged Ethernet traffic

Choose an appropriate assignment between the priority code point in bridged Ethernet frames and traffic classes. This assignment should be consistent with quality of service policy in the rest of the customer data network.

The user interface provides a convenient shortcut to select the assignment recommended in IEEE 802.1Q-2005.

**NOTE**

Ethernet priority information is coded in the Ethernet VLAN tag and differentiated quality of service is therefore not available in a network based on untagged Ethernet frames.

## Back to back links

Avoid the use of direct cabled connections between two PIDUs. Where two or more links are deployed in a chain, always use an Ethernet switch or router to interconnect the links at a relay point.

## ‘Green Ethernet’ switches

Do not connect PTP 300 or PTP 500 units to Ethernet networking products that control the level of the transmitted Ethernet signal based on the measured length of the Ethernet link, for example Green Ethernet products manufactured by D-Link Corporation. The Ethernet interfaces in these networking products do not work correctly when connected directly to the PIDU.

# Network management planning

## Planning for SNMP operation

### Supported notifications

The supported notifications are as follows:

- Cold start
- Wireless Link Up/Down
- DFS Channel Change
- DFS Impulse Interference
- Authentication Failure
- Ethernet Link Up/Down

### Supported MIBs

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

- RFC-1493. BRIDGE-MIB
- RFC-2233. IF-MIB
- RFC-3411. SNMP-FRAMEWORK-MIB
- RFC-3412. SNMP-MPD-MIB
- RFC-3413. SNMP-TARGET-MIB
- RFC-3414. SNMP-USER-BASED-SM-MIB
- RFC-3415. SNMP-VIEW-BASED-ACM-MIB
- RFC-3418. SNMPv2-MIB
- RFC-3826. SNMP-USM-AES-MIB
- PTP 300 and PTP 500 Series proprietary MIBs

**NOTE**

The proprietary MIBs are provided in the PTP 300 or PTP 500 Series software download files in http://www.motorola.com/ptp/support.

## Supported alarms

PTP 300 and PTP 500 support the following diagnostic alarms:

- Region Code
- Install Status
- Install Arm State
- Unit Out Of Calibration
- Incompatible Region Codes
- Incompatible Master And Slave
- Ethernet Configuration Mismatch
- No Wireless Channel Available
- SNTP Synchronization Failed
- Wireless Link Disabled Warning
- Ethernet Link Disabled Warning
- Ethernet Link Status
- Telecoms Channel A Status
- Telecoms Channel B Status
- Telecoms Channel A Loopback
- Telecoms Channel B Loopback
- TDD Synchronization Alarm
- Link Mode Optimization Mismatch

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

## Enabling SNMP

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

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

When the SNMP Version is set to SNMPv1/2c the interface must be additionally configured by entering the following attributes:

- SNMP Trap IP Address
- SNMP Trap Port Number
- SNMP Community String

# Security planning

## Planning for SNMPv3 operation

### SNMP security mode

Decide how SNMPv3 security will be configured.

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

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

## Web-based management of SNMPv3 security

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

- MAC address (default)
- IP address
- Text string

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

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

- Read Only
- System Administrator

Identify the security level for each of the security roles. Three security levels are available:

- No authentication, no privacy
- Authentication, no privacy
- Authentication, privacy

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

- MD5
- SHA

If privacy will be used, identify the protocol. Two privacy protocols are available:

- DES
- AES

AES link encryption is only available to users who have purchased an appropriate license key.

If authentication or authentication and privacy protocols are required, identify passphrases for each protocol for each SNMP user. It is considered good practice to use different passphrases for authentication and privacy. Passphrases must have length between 8 and 32 characters, and may contain any of the characters listed in Table 2-5.

**Table 2-5** Permitted character set for SNMPv3 passphrases

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

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

# Chapter 3 Legal information

This chapter provides legal notices including software license agreements.

**CAUTION**

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

The following topics are described in this chapter:

# Motorola Inc. end user license agreement

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

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

## Definitions

In this Agreement, the word "Software" refers to the set of instructions for computers, in executable form and in any media, (which may include diskette, CD-ROM, downloadable internet, hardware, or firmware) licensed to you. The word "Documentation" refers to electronic or printed manuals and accompanying instructional aids licensed to you. The word "Product" refers to Motorola's MOTOwi4™ fixed wireless broadband devices for which the Software and Documentation is licensed for use.

## Grant of license

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

## Conditions of use

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

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

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

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

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

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

## Title and restrictions

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

## Confidentiality

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

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

## Right to use Motorola's name

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

## Transfer

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

## Updates

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

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

## Maintenance

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

## Disclaimer

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

## Limitation of liability

THE TOTAL LIABILITY OF MOTOROLA UNDER THIS AGREEMENT FOR DAMAGES WILL NOT EXCEED THE TOTAL AMOUNT PAID BY YOU FOR THE PRODUCT LICENSED UNDER THIS AGREEMENT. IN NO EVENT WILL MOTOROLA BE LIABLE IN ANY WAY FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL OR PUNITIVE DAMAGES OF ANY NATURE, INCLUDING WITHOUT LIMITATION, LOST BUSINESS PROFITS, OR LIABILITY OR INJURY TO THIRD PERSONS, WHETHER FORESEEABLE OR NOT, REGARDLESS OF WHETHER MOTOROLA HAS BEEN ADVISED OF THE POSSIBLITY OF SUCH DAMAGES. Some jurisdictions do not permit limitations of liability for incidental or consequential damages, so the above exclusions may not apply to you.

## U.S. government

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

## Term of license

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

## Governing law

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

## Assignment

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

## Survival of provisions

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

## Entire agreement

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

## Third party software

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

### Trademarks

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

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

### Net SNMP

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

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

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

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

All Rights Reserved

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

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

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

Copyright © 2001-2003, Networks Associates Technology, Inc

All rights reserved.

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

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

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

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



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

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

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

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



Use is subject to license terms below.

This distribution may include materials developed by third parties.

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

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

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

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

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

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

Copyright © 2003-2008, Sparta, Inc

All rights reserved.

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

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

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,

PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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



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

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

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

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

Author: Bernhard Penz

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

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

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

## OpenSSL

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

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

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

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

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

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

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

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

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

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

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

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

Original SSLeay License

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

All rights reserved.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Zlib



## Libpng

particular purposes or needs. This library is provided with all faults, and the entire risk of satisfactory quality, performance, accuracy, and effort is with the user.

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

Tom Lane

Glenn Randers-Pehrson

Willem van Schaik

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

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

John Bowler

Kevin Bracey

Sam Bushell

Magnus Holmgren

Greg Roelofs

Tom Tanner

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

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

Andreas Dilger

Dave Martindale

Guy Eric Schalnat

Paul Schmidt

Tim Wegner

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

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

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

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

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

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

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

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

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

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

Glenn Randers-Pehrson

glennrp at users.sourceforge.net

February 14, 2009

## Bzip2

This program, "bzip2", the associated library "libbzip2", and all documentation, are copyright (C) 1996-2007 Julian R Seward. All rights reserved.

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

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

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

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

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

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

Julian Seward, jseward@bzip.org

## USB library functions

Atmel Corporation

2325 Orchard Parkway
San Jose, Ca 95131

Copyright (c) 2004 Atmel

## FreeRADIUS

Copyright (c) 1998 The NetBSD Foundation, Inc.

All rights reserved.

This code is derived from software contributed to The NetBSD Foundation by Christos Zoulas.

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

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   This product includes software developed by the NetBSD

Foundation, Inc. and its contributors.

4. Neither the name of The NetBSD Foundation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

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

-----------------------------------------------------------------------------

Copyright (c) 2003 Maxim Sobolev <sobomax@FreeBSD.org> All rights reserved.

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

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

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

# Hardware warranty

Motorola's standard hardware warranty is for one (1) year from date of shipment from Motorola or a Motorola Point-to-Point Distributor. Motorola 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. Motorola 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.

# Limit of liability

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

# Chapter 4 Reference information

This chapter describes the reference information and regulatory notices that are common to all PTP 300 and PTP 500 products and those that are specific to each frequency variant.

The following topics are described in this chapter:

# Installation inventories

This section contains inventories of the components required, both for standard bridge installations and for the main installation options, such as connectorized ODUs, PTP-SYNC, GPS and E1 or T1.

The following tables contain inventories for PTP 300 or PTP 500 installations:

- Table 4-1 - Inventory for standard installations
- Table 4-2 - Additional inventory for connectorized bridges
- Table 4-3 - Additional inventory for PTP-SYNC installations
- Table 4-4 - Additional inventory for GPS receiver installations
- Table 4-5 - Additional inventory for E1 or T1 installations

**Table 4-1** Inventory for standard installations

| Item | Notes |
|---|---|
| ODU and PIDU Plus kits: 'Link Complete' or 'End Complete'<br> <br><br> | 'Link Complete' kit contents: two ODUs, two PIDU Plus units, mounting brackets and mains leads.<br>'End Complete' kit contents: one ODU, one PIDU Plus unit, mounting bracket and mains lead.<br>May be Integrated or Connectorized.<br>Refer to Ordering ODU and PIDU Plus kits on page 4-8. |

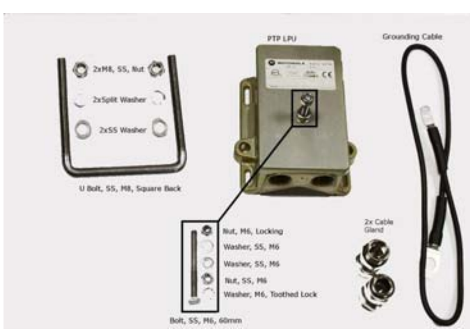
| Item | Notes |
|---|---|
| Outdoor drop cable<br> | **CAUTION**<br>Always use Cat5e cable that is gel-filled and shielded with copper-plated steel. Alternative types of drop cable are not supported by Motorola.<br>Superior Essex BBDGe is suitable. Refer to Cable and connector specifications on page 4-17. |
| Outdoor connectors and glands | Refer to Cable and connector specifications on page 4-17. |
| Indoor CAT5e cable | Refer to Cable and connector specifications on page 4-17. |
| Cable grounding kits for 1/4” and 3/8” cable<br> | Motorola part number 01010419001.<br>One per drop cable grounding point.<br>Kit contents: grounding cable, self-amalgamating tape, PVC tape, tie-wraps, bolts, washers and nuts. |
| Lightning Protection Unit (LPU) single end kit<br> | Motorola part number WB2978B.<br>Two kits required per standard link.<br>Kit contents: LPU, grounding cable, nuts, bolts and glands. |
| Cable ties, cable cleats | Purchase separately. |

**Table 4-2** Additional inventory for connectorized bridges

| Item | Notes |
|---|---|
| Antenna | Purchase separately.<br>Refer to Antenna specifications on page 4-19. |
| RF cable | Purchase separately.<br>For connecting the ODU to the antenna.<br>May be cable of type LMR100, LMR200, LMR300, LMR400 or LMR600. Cable losses are specified in Table 4-56.<br>**NOTE**<br>A cable of a type similar to LMR400 is a lot more difficult to handle and route than a cable of a type similar to LMR100. |
| RF cable connectors<br> | Purchase separately.<br>N type male connectors are required for connecting the RF cable to the ODU.<br>For the antenna end of the RF cable, refer to the antenna manufacturer's instructions.<br>Use weatherproof connectors, preferably ones that are supplied with adhesive lined heat shrink sleeves that are fitted over the cable/connector interface. |
| Cable ties, cable cleats | Purchase separately. |
| Self-amalgamating and PVC tape<br> | Purchase separately.<br>To weatherproof the RF connectors. |

**Table 4-3** Additional inventory for PTP-SYNC installations

| Item | Notes |
|---|---|
| PTP-SYNC kit<br> | Motorola part number WB3665.<br>Kit contents:<br>1 x PTP-SYNC unit<br>1 x M4 pan screw<br>2 x M4 washers<br>2 x M3 (6mm) torx drive screws<br>1 x lug for unit ground (cable not supplied)<br>Installation guide |
| Indoor CAT5e cable | To connect the PTP-SYNC to the PIDU Plus.<br>Can be any standard screened or unscreened CAT5e cable. |
| PTP800 CMU / PTP-SYNC 19” rack mount installation kit<br> | Motorola part number WB3486.<br>Required for rack-mounted PTP-SYNC units.<br>Kit contents:<br>1 x rack bracket<br>8 x M3 washers<br>8 x M3 screws<br>1 x rack mount blank plate<br>8 x M5 nuts<br>8 x M5 washers<br>2 x rack handles |

**Table 4-4** Additional inventory for GPS receiver installations

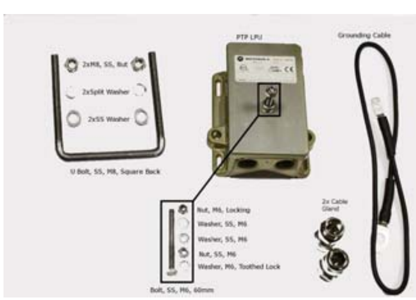
| Item | Notes |
|---|---|
| Trimble Acutime™ Gold GPS receiver | Motorola part number STLN6594. |
| Outdoor drop cable | ⚠ CAUTION<br>Always use Cat5e cable that is gel-filled and shielded with copper-plated steel. Alternative types of drop cable are not supported by Motorola.<br>Superior Essex BBDGe is suitable. Refer to Cable and connector specifications on page 4-17. |
| Connectors and glands for LPU | Use the recommended connectors and glands to connect the drop cable to the LPU. Refer to Outdoor connectors and glands on page 4-17. |
| Connectors and glands for GPS | Use the recommended connectors and glands to connect the drop cable to the Trimble GPS receiver. Refer to Outdoor connectors and glands – Trimble GPS on page 4-18. |
| Cable grounding kits for 1/4” and 3/8” cable<br> | Motorola part number 01010419001.<br>One per drop cable grounding point.<br>Kit contents: grounding cable, self-amalgamating tape, PVC tape, tie-wraps, bolts, washers and nuts. |
| Lightning Protection Unit (LPU) single end kit<br> | Motorola part number WB2978B.<br>For protecting the connection to the GPS receiver.<br>Kit contents: LPU, grounding cable, nuts, bolts and glands. |

**Table 4-5** Additional inventory for E1 or T1 installations

| Item | Notes |
|---|---|
| PTP 300/500 Series E1/T1 Splitter   | Motorola part number WB3476. |
| E1 or T1 network cable | Purchase separately. |

# Ordering ODU and PIDU Plus kits

This section contains the information needed to order kits for PTP 300 or PTP 500 links.

## Kit contents

The Link Complete kit consists of two ODUs and two PIDU Plus units.

The End Complete kit consists of one ODU and one PIDU Plus unit.

All ODUs are pre-fitted with a mounting bracket and earth bonding lead.

All PIDU Plus units are supplied with a mains power lead.

## Regional variants

PTP 300 and PTP 500 kits are supplied in two regional variants: one is for use in regions where FCC or IC licensing restrictions apply (FCC/IC), and the other is for use in ETSI or the rest of the world (ETSI/RoW). Table 4-6 identifies the regional variant that is required for each combination of frequency band and region.

**Table 4-6** ODU regional variants

| Frequency band | Region | Regional variant |
|---|---|---|
| 5.4 GHz | Australia | ETSI/RoW |
| 5.4 GHz | Canada | FCC/IC |
| 5.4 GHz | ETSI | ETSI/RoW |
| 5.4 GHz | FCC | FCC/IC |
| 5.4 GHz | Full Power | ETSI/RoW |
| 5.4 GHz | Full Power + Radar | ETSI/RoW |
| 5.4 GHz | Korea | ETSI/RoW |
| 5.4 GHz | Thailand | ETSI/RoW |
| 5.8 GHz | Australia, Hong Kong | ETSI/RoW |
| 5.8 GHz | Bahrain | ETSI/RoW |
| 5.8 GHz | China | ETSI/RoW |

| Frequency band | Region | Regional variant |
|---|---|---|
| 5.8 GHz | Denmark | ETSI/RoW |
| 5.8 GHz | ETSI | ETSI/RoW |
| 5.8 GHz | Eire | ETSI/RoW |
| 5.8 GHz | FCC USA, Canada, Taiwan, Brazil | FCC/IC |
| 5.8 GHz | Full Power | ETSI/RoW |
| 5.8 GHz | Full Power + Radar + RTTT | ETSI/RoW |
| 5.8 GHz | Germany | ETSI/RoW |
| 5.8 GHz | India | ETSI/RoW |
| 5.8 GHz | Korea | ETSI/RoW |
| 5.8 GHz | Norway | ETSI/RoW |
| 5.8 GHz | Singapore | ETSI/RoW |
| 5.8 GHz | Spain | ETSI/RoW |
| 5.8 GHz | Thailand | ETSI/RoW |
| 5.8 GHz | UK | ETSI/RoW |

## ODU and PIDU Plus kit part numbers

The following tables contain part numbers for all kit variants:

- Table 4-7: PTP 54300.
- Table 4-8: PTP 58300.
- Table 4-9: PTP 54500.
- Table 4-10: PTP 58500.

**NOTE**

Units manufactured before the introduction of regional variants have the same part numbers as corresponding ETSI/RoW units, but are identified by an earlier part number suffix.

**Table 4-7** PTP 54300 kit part numbers

| Frequency variant | Regional variant | Integrated or Connectorized | Link or End Complete | Part number |
|---|---|---|---|---|
| PTP 54300 | ETSI/RoW | Integrated | Link Complete | WB3150CC |
| PTP 54300 | ETSI/RoW | Integrated | End Complete | WB3151CC |
| PTP 54300 | ETSI/RoW | Connectorized | Link Complete | WB3152CC |
| PTP 54300 | ETSI/RoW | Connectorized | End Complete | WB3153CC |
| PTP 54300 | FCC/IC | Integrated | Link Complete | WB3856AA |
| PTP 54300 | FCC/IC | Integrated | End Complete | WB3857AA |
| PTP 54300 | FCC/IC | Connectorized | Link Complete | WB3858AA |
| PTP 54300 | FCC/IC | Connectorized | End Complete | WB3859AA |

**Table 4-8** PTP 58300 kit part numbers

| Frequency variant | Regional variant | Integrated or Connectorized | Link or End Complete | Part number |
|---|---|---|---|---|
| PTP 58300 | ETSI/RoW | Integrated | Link Complete | WB3146BB |
| PTP 58300 | ETSI/RoW | Integrated | End Complete | WB3147BB |
| PTP 58300 | ETSI/RoW | Connectorized | Link Complete | WB3148BB |
| PTP 58300 | ETSI/RoW | Connectorized | End Complete | WB3149BB |
| PTP 58300 | FCC/IC | Integrated | Link Complete | WB3852AA |
| PTP 58300 | FCC/IC | Integrated | End Complete | WB3853AA |
| PTP 58300 | FCC/IC | Connectorized | Link Complete | WB3854AA |
| PTP 58300 | FCC/IC | Connectorized | End Complete | WB3855AA |

**Table 4-9** PTP 54500 kit part numbers

| Frequency variant | Lite or Full | Regional variant | Integrated or Connectorized | Link or End Complete | Part number |
|---|---|---|---|---|---|
| PTP 54500 | Lite | ETSI/RoW | Integrated | Link Complete | WB2876CC |
| PTP 54500 | Lite | ETSI/RoW | Integrated | End Complete | WB2880CC |
| PTP 54500 | Lite | ETSI/RoW | Connectorized | Link Complete | WB2877CC |
| PTP 54500 | Lite | ETSI/RoW | Connectorized | End Complete | WB2881CC |
| PTP 54500 | Lite | FCC/IC | Integrated | Link Complete | WB3840AA |
| PTP 54500 | Lite | FCC/IC | Integrated | End Complete | WB3841AA |
| PTP 54500 | Lite | FCC/IC | Connectorized | Link Complete | WB3842AA |
| PTP 54500 | Lite | FCC/IC | Connectorized | End Complete | WB3843AA |
| PTP 54500 | Full | ETSI/RoW | Integrated | Link Complete | WB2874CC |
| PTP 54500 | Full | ETSI/RoW | Integrated | End Complete | WB2878CC |
| PTP 54500 | Full | ETSI/RoW | Connectorized | Link Complete | WB2875CC |
| PTP 54500 | Full | ETSI/RoW | Connectorized | End Complete | WB2879CC |
| PTP 54500 | Full | FCC/IC | Integrated | Link Complete | WB3836AA |
| PTP 54500 | Full | FCC/IC | Integrated | End Complete | WB3837AA |
| PTP 54500 | Full | FCC/IC | Connectorized | Link Complete | WB3838AA |
| PTP 54500 | Full | FCC/IC | Connectorized | End Complete | WB3839AA |

**Table 4-10** PTP 58500 kit part numbers

| Frequency variant | Lite or Full | Regional variant | Integrated or Connectorized | Link or End Complete | Part number |
|---|---|---|---|---|---|
| PTP 58500 | Lite | ETSI/RoW | Integrated | Link Complete | WB2859BB |
| PTP 58500 | Lite | ETSI/RoW | Integrated | End Complete | WB2863BB |
| PTP 58500 | Lite | ETSI/RoW | Connectorized | Link Complete | WB2860BB |
| PTP 58500 | Lite | ETSI/RoW | Connectorized | End Complete | WB2864BB |
| PTP 58500 | Lite | FCC/IC | Integrated | Link Complete | WB3848AA |
| PTP 58500 | Lite | FCC/IC | Integrated | End Complete | WB3849AA |
| PTP 58500 | Lite | FCC/IC | Connectorized | Link Complete | WB3850AA |
| PTP 58500 | Lite | FCC/IC | Connectorized | End Complete | WB3851AA |
| PTP 58500 | Full | ETSI/RoW | Integrated | Link Complete | WB2857BB |
| PTP 58500 | Full | ETSI/RoW | Integrated | End Complete | WB2861BB |
| PTP 58500 | Full | ETSI/RoW | Connectorized | Link Complete | WB2858BB |
| PTP 58500 | Full | ETSI/RoW | Connectorized | End Complete | WB2862BB |
| PTP 58500 | Full | FCC/IC | Integrated | Link Complete | WB3844AA |
| PTP 58500 | Full | FCC/IC | Integrated | End Complete | WB3845AA |
| PTP 58500 | Full | FCC/IC | Connectorized | Link Complete | WB3846AA |
| PTP 58500 | Full | FCC/IC | Connectorized | End Complete | WB3847AA |

# ODU specifications

This section contains specifications of the outdoor unit (ODU) that is supplied by Motorola for PTP 300 and PTP 500 installations. These specifications apply to all product variants.

## ODU dimensions and weight

The integrated ODU conforms to the physical specifications listed in Table 4-11.

**Table 4-11** Integrated ODU physical specifications

| Category | Specification |
|---|---|
| Dimensions | Width 370 mm (14.5 in), Height 370 mm (14.5 in), Depth 95 mm (3.75 in) |
| Weight | 5.35 Kg (11.8 lbs) including bracket |

The connectorized ODU conforms to the physical specifications listed in Table 4-12.

**Table 4-12** Connectorized ODU physical specifications

| Category | Specification |
|---|---|
| Dimensions | Width 309 mm (12.2 in), Height 309 mm (12.2 in), Depth 105 mm (4.01 in) |
| Weight | 4.7 Kg (10.4 lbs) including bracket |

## ODU environmental

The ODU conform to the environmental specifications listed in Table 4-16.

**Table 4-13** ODU environmental specifications

| Category | Specification |
|---|---|
| Temperature | -40°C (40°F) to +60°C (140°F) |
| Wind loading | 150 mph (242 kph) maximum. See Wind loading on page 2-7 for a full description. |
| Humidity | 100% condensing |
| Waterproof | IP66 |
| UV exposure | 10 year operational life (UL746C test evidence) |

# PIDU Plus specifications

This section contains specifications of the powered indoor unit (PIDU Plus) that is supplied by Motorola for PTP 300 and PTP 500 installations. These specifications apply to all PTP 300 and PTP 500 product variants.

## PIDU Plus dimensions and weight

The PIDU Plus conforms to the physical specifications listed in Table 4-14.

**Table 4-14** PIDU Plus physical specifications

| Category | Specification |
|---|---|
| Dimensions | Width 250 mm (9.75 in), Height 40 mm (1.5 in), Depth 80 mm (3 in) |
| Weight | 0.864 Kg (1.9 lbs) |

## PIDU Plus environmental

The PIDU Plus conforms to the environmental specifications listed in Table 4-15.

**Table 4-15** PIDU Plus environmental specifications

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

## PIDU Plus electrical

The PIDU Plus conforms to the electrical specifications listed in Table 4-16.

**Table 4-16** PIDU Plus electrical specifications

| Category | Specification |
|---|---|
| AC Input | 90 – 264 V AC, 47 – 60 Hz |
| Alternative DC Input | 36 – 60 V DC |
| DC Output Voltage | For mains input: 55 V, +2V, -0V<br>For DC input: Output voltage at maximum rated output current, not more than 1.5 V below the DC input voltage |
| AC Input connector | IEC 320-C8, (figure of eight) |
| DC Output current | 1.4A |
| 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 |

# Cable and connector specifications

This section contains specifications of the CAT5e cables, connectors and glands that are required for PTP 300 and PTP 500 installations.

## Outdoor CAT5e cable (drop cable)

⚠ CAUTION

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

A suitable make of outdoor drop cable is Superior Essex BBDGe, with part numbers as specified in Table 4-17.

**Table 4-17** Superior Essex cable - available lengths and part numbers

| Length (on plywood reel) | Part number |
|---|---|
| 304 m (1000 ft) | BBDGe 04-001-55 |
| 762 m (2500 ft) | BBDGe 04-002-55 |
| 1524 m (5000 ft) | BBDGe 04-003-55 |
| Cut to length | BBDGe 04-601-55 |

## Outdoor connectors and glands – ODU or LPU

The recommended connectors and glands to be used for connecting the supported drop cable to the ODU or LPU are specified in Table 4-18.

**Table 4-18** Recommended outdoor connectors for ODU and LPU

| Item | Manufacturer | Part number |
|---|---|---|
| Connector | Tyco (AMP) | 5-569278 |
| Crimp tool | Tyco (AMP) | 2-231652 |
| Die set | Tyco (AMP) | 1-8534400-0 |
| Gland | Motorola | WB1811 |

**NOTE**

The connector, crimp tool and die set listed in Table 4-18 are specific to Superior Essex BBDGe cable. They may not work with other makes of cable.

## Outdoor connectors and glands – Trimble GPS

The recommended connectors and glands to be used for connecting the supported drop cable to the Trimble GPS receiver are specified in Table 4-19.

**Table 4-19** Recommended outdoor connectors for Trimble GPS receiver

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

## Indoor CAT5e cable

The CAT5e cable that connects the PIDU Plus to the network equipment should be purchased separately and must meet the following requirements:

- It must be either foil screen (FTP) or braided screen (STP) cable.
- It must use screened RJ45 connectors with metal shells at both ends.
- There must be a continuous electrical connection between both screened connectors.

**CAUTION**

The connected network equipment must feature screened RJ45 connectors and must be connected to ground, otherwise the PIDU Plus will not be grounded.

# Antenna specifications

This section contains specifications of the antennas that are approved for use with the connectorized ODUs.

For more information on antenna restrictions, refer to Regulatory issues with connectorized units on page 4-62.

## Antenna selection criteria

The main selection criterion is the required antenna gain. The secondary criterion is the ease of mounting and alignment. For example, the Radio Waves Parabolic dishes are supplied with a mount that allows adjustment for alignment independent of the actual antenna mounting. This type of antenna is much easier to align than those that have to be rotated around the mounting pole for alignment.

## Non-FCC regions

In non-FCC regions, antenna choice is not restricted, but any region specific EIRP limit must be obeyed by reducing the maximum Transmit power, see Conformance to regulations on page 2-2.

## FCC regions

In FCC regions, antenna choice is restricted as described in FCC antenna restrictions (5.4 GHz) on page 4-20 and FCC antenna restrictions (5.8 GHz) on page 4-23.

## FCC antenna restrictions (5.4 GHz)

In FCC regions, external antennas from the list in Table 4-20 can be used with the Connectorized version of the PTP 54300 and PTP 54500. These are approved by the FCC for use with the product and are constrained by the following limit for Single/Dual Polarization Parabolic Dish Antennas: up to 34.9 dBi (33.4 dBi for 5 MHz bandwidth) per polarization or antenna.

However, the Maximum Transmit Power must be reduced to avoid exceeding the EIRP limits.

In FCC regions when using external antennas, cable loss between the connectorized ODU and the antenna ports must not be less than 1.2 dB.

**CAUTION**

Antennas not included in this table, or those having a gain greater than the specified maximum, are strictly prohibited for use with the PTP 54300 and PTP 54500. The required antenna impedance is 50 ohms.

**Table 4-20** Allowed antennas for deployment in USA/Canada – 5.4 GHz

| Manufacturer | Antenna Type | Gain (dBi) | Parabolic Dish |
|---|---|---|---|
| Andrew | Andrew 2-foot Parabolic, P2F-52 (29.4 dBi) | 29.4 | Y |
| Andrew | Andrew 2-foot Dual-Pol Parabolic, PX2F-52 (29.4 dBi) | 29.4 | Y |
| Andrew | Andrew 3-foot Parabolic, P3F-52 (33.4 dBi) | 33.4 | Y |
| Andrew | Andrew 3-foot Dual-Pol Parabolic, PX3F-52 (33.4 dBi) | 33.4 | Y |
| Andrew | Andrew 4-foot Parabolic, P4F-52 (34.9 dBi) | 34.9 | Y |
| Andrew | Andrew 4-foot Dual-Pol Parabolic, PX4F-52 (34.9 dBi) | 34.9 | Y |
| Gabriel | Gabriel 2-foot High Performance QuickFire Parabolic, HQF2-52-N | 28.2 | Y |

| Manufacturer | Antenna Type | Gain (dBi) | Parabolic Dish |
|---|---|---|---|
| Gabriel | Gabriel 4-foot High Performance QuickFire Parabolic, HQF4-52-N | 34.4 | Y |
| Gabriel | Gabriel 2-foot High Performance Dual QuickFire Parabolic, HQFD2-52-N | 28.1 | Y |
| Gabriel | Gabriel 4-foot High Performance Dual QuickFire Parabolic, HQFD4-52-N | 34.3 | Y |
| Gabriel | Gabriel 2-foot Standard QuickFire Parabolic, QF2-52-N | 28.5 | Y |
| Gabriel | Gabriel 2-foot Standard QuickFire Parabolic, QF2-52-N-RK | 28.5 | Y |
| Gabriel | Gabriel 2.5-foot Standard QuickFire Parabolic, QF2.5-52-N | 31.2 | Y |
| Gabriel | Gabriel 4-foot Standard QuickFire Parabolic, QF4-52-N | 34.8 | Y |
| Gabriel | Gabriel 4-foot Standard QuickFire Parabolic, QF4-52-N-RK | 34.8 | Y |
| Gabriel | Gabriel 2-foot Standard Dual QuickFire Parabolic, QFD2-52-N | 28.4 | Y |
| Gabriel | Gabriel 2.5-foot Standard Dual QuickFire Parabolic, QFD2.5-52-N | 31.1 | Y |
| Gabriel | Gabriel 2-foot Standard Dual QuickFire Parabolic, QFD2-52-N-RK | 28.4 | Y |
| Gabriel | Gabriel 4-foot Standard Dual QuickFire Parabolic, QFD4-52-N | 34.7 | Y |
| Gabriel | Gabriel 4-foot Standard Dual QuickFire Parabolic, QFD4-52-N-RK | 34.7 | Y |
| RadioWaves | Radio Waves 2-foot Dual-Pol Parabolic, SPD2-5.2 (28.1 dBi) | 28.1 | Y |

| Manufacturer | Antenna Type | Gain (dBi) | Parabolic Dish |
|---|---|---|---|
| RadioWaves | Radio Waves 2-foot Parabolic, SP2-5.2 (29.0 dBi) | 29 | Y |
| RadioWaves | Radio Waves 3-foot Dual-Pol Parabolic, SPD3-5.2 (31.1 dBi) | 31.1 | Y |
| RadioWaves | Radio Waves 3-foot Parabolic, SP3-5.2 (31.4 dBi) | 31.4 | Y |
| RadioWaves | Radio Waves 4-foot Dual-Pol Parabolic, SPD4-5.2 (34.4 dBi) | 34.4 | Y |
| RadioWaves | Radio Waves 4-foot Parabolic, SP4-5.2 (34.8 dBi) | 34.8 | Y |
| RadioWaves | Radio Waves 2-foot Parabolic, SP2-2/5 (28.3 dBi) | 28.3 | Y |
| RadioWaves | Radio Waves 3-foot Parabolic, SP3-2/5 (31.4 dBi) | 31.4 | Y |
| RadioWaves | Radio Waves 4-foot Parabolic, SP4-2/5 (34.6 dBi) | 34.6 | Y |
| RFS | RFS 2-foot Parabolic, SPF2-52AN or SPFX2-52AN (27.9 dBi) | 27.9 | Y |
| RFS | RFS 3-foot Parabolic, SPF3-52AN or SPFX3-52AN(31.4 dBi) | 31.4 | Y |
| RFS | RFS 4-foot Parabolic, SPF4-52AN or SPFX4-52AN(33.9 dBi) | 33.9 | Y |
| RFS | RFS 2-foot HP Parabolic, SDF2-52AN or SDFX2-52AN (31.4 dBi) | 31.4 | Y |
| RFS | RFS 4-foot HP Parabolic, SDF4-52AN or SDFX4-52AN (33.9 dBi) | 33.9 | Y |

## FCC antenna restrictions (5.8 GHz)

In FCC regions, external antennas from the lists in Table 4-21 and Table 4-22 can be used with the Connectorized version of the PTP 58300 and PTP 58500. These are approved by the FCC for use with the product and are constrained by the following limit for Single/Dual Polarization Parabolic Dish Antennas: up to 37.7 dBi per polarization or antenna.

In FCC regions when using external antennas, cable loss between the connectorized ODU and the antenna ports must not be less than 1.2 dB.

**NOTE**

When operating PTP 58300 and PTP 58500 with a 5 MHz channel bandwidth and with dish antennas larger than 1.2 meters (4 ft) diameter, the maximum operating power must be reduced to 24 dBm (3 dB reduction) to ensure that FCC requirements are met.

**CAUTION**

Antennas not included in this table, or those having a gain greater than the specified maximum, are strictly prohibited for use with the PTP 58300 and PTP 58500. The required antenna impedance is 50 ohms.

**Table 4-21** Allowed antennas for deployment in USA/Canada – 5.8 GHz

| Manufacturer | Antenna Type | Gain (dBi) | Flat Plate | Parabolic Dish |
|---|---|---|---|---|
| Andrew | Andrew 2-foot Parabolic, P2F-52 (29.4 dBi) | 29.4 | | Y |
| Andrew | Andrew 2-foot Dual-Pol Parabolic, PX2F-52 (29.4 dBi) | 29.4 | | Y |
| Andrew | Andrew 3-foot Parabolic, P3F-52 (33.4 dBi) | 33.4 | | Y |
| Andrew | Andrew 3-foot Dual-Pol Parabolic, PX3F-52 (33.4 dBi) | 33.4 | | Y |
| Andrew | Andrew 4-foot Parabolic, P4F-52 (34.9 dBi) | 34.9 | | Y |
| Andrew | Andrew 4-foot Dual-Pol Parabolic, PX4F-52 (34.9 dBi) | 34.9 | | Y |

| Manufacturer | Antenna Type | Gain (dBi) | Flat Plate | Parabolic Dish |
|---|---|---|---|---|
| Andrew | Andrew 6-foot Parabolic, P6F-52 (37.6 dBi) | 37.6 | | Y |
| Andrew | Andrew 6-foot Dual-Pol Parabolic, PX6F-52 (37.6 dBi) | 37.6 | | Y |
| Gabriel | Gabriel 2-foot High Performance QuickFire Parabolic, HQF2-52-N | 28.2 | | Y |
| Gabriel | Gabriel 4-foot High Performance QuickFire Parabolic, HQF4-52-N | 34.4 | | Y |
| Gabriel | Gabriel 6-foot High Performance QuickFire Parabolic, HQF6-52-N | 37.4 | | Y |
| Gabriel | Gabriel 2-foot High Performance Dual QuickFire Parabolic, HQFD2-52-N | 28.1 | | Y |
| Gabriel | Gabriel 4-foot High Performance Dual QuickFire Parabolic, HQFD4-52-N | 34.3 | | Y |
| Gabriel | Gabriel 6-foot High Performance Dual QuickFire Parabolic, HQFD6-52-N | 37.3 | | Y |
| Gabriel | Gabriel 2-foot Standard QuickFire Parabolic, QF2-52-N | 28.5 | | Y |
| Gabriel | Gabriel 2-foot Standard QuickFire Parabolic, QF2-52-N-RK | 28.5 | | Y |
| Gabriel | Gabriel 2.5-foot Standard QuickFire Parabolic, QF2.5-52-N | 31.2 | | Y |
| Gabriel | Gabriel 4-foot Standard QuickFire Parabolic, QF4-52-N | 34.8 | | Y |
| Gabriel | Gabriel 4-foot Standard QuickFire Parabolic, QF4-52-N-RK | 34.8 | | Y |
| Gabriel | Gabriel 6-foot Standard QuickFire Parabolic, QF6-52-N | 37.7 | | Y |

| Manufacturer | Antenna Type | Gain (dBi) | Flat Plate | Parabolic Dish |
|---|---|---|---|---|
| Gabriel | Gabriel 2-foot Standard Dual QuickFire Parabolic, QFD2-52-N | 28.4 | | Y |
| Gabriel | Gabriel 2.5-foot Standard Dual QuickFire Parabolic, QFD2.5-52-N | 31.1 | | Y |
| Gabriel | Gabriel 2-foot Standard Dual QuickFire Parabolic, QFD2-52-N-RK | 28.4 | | Y |
| Gabriel | Gabriel 4-foot Standard Dual QuickFire Parabolic, QFD4-52-N | 34.7 | | Y |
| Gabriel | Gabriel 4-foot Standard Dual QuickFire Parabolic, QFD4-52-N-RK | 34.7 | | Y |
| Gabriel | Gabriel 6-foot Standard Dual QuickFire Parabolic, QFD6-52-N | 37.7 | | Y |
| RadioWaves | Radio Waves 2-foot Dual-Pol Parabolic, SPD2-5.2 (28.1 dBi) | 28.1 | | Y |
| RadioWaves | Radio Waves 2-foot Parabolic, SP2-5.2 (29.0 dBi) | 29 | | Y |
| RadioWaves | Radio Waves 3-foot Dual-Pol Parabolic, SPD3-5.2 (31.1 dBi) | 31.1 | | Y |
| RadioWaves | Radio Waves 3-foot Parabolic, SP3-5.2 (31.4 dBi) | 31.4 | | Y |
| RadioWaves | Radio Waves 4-foot Dual-Pol Parabolic, SPD4-5.2 (34.4 dBi) | 34.4 | | Y |
| RadioWaves | Radio Waves 4-foot Parabolic, SP4-5.2 (34.8 dBi) | 34.8 | | Y |
| RadioWaves | Radio Waves 6-foot Dual-Pol Parabolic, SPD6-5.2 (37.5 dBi) | 37.5 | | Y |
| RadioWaves | Radio Waves 6-foot Parabolic, SP6-5.2 (37.7 dBi) | 37.7 | | Y |
| RadioWaves | Radio Waves 2-foot Parabolic, SP2-2/5 (28.3 dBi) | 28.3 | | Y |
| RadioWaves | Radio Waves 3-foot Parabolic, SP3-2/5 (31.4 dBi) | 31.4 | | Y |

| Manufacturer | Antenna Type | Gain (dBi) | Flat Plate | Parabolic Dish |
|---|---|---|---|---|
| RadioWaves | Radio Waves 4-foot Parabolic, SP4-2/5 (34.6 dBi) | 34.6 | | Y |
| RadioWaves | Radio Waves 6-foot Parabolic, SP6-2/5 (37.7 dBi) | 37.7 | | Y |
| RFS | RFS 2-foot Parabolic, SPF2-52AN or SPFX2-52AN (27.9 dBi) | 27.9 | | Y |
| RFS | RFS 3-foot Parabolic, SPF3-52AN or SPFX3-52AN(31.4 dBi) | 31.4 | | Y |
| RFS | RFS 4-foot Parabolic, SPF4-52AN or SPFX4-52AN(33.9 dBi) | 33.9 | | Y |
| RFS | RFS 6-foot Parabolic, SPF6-52AN or SPFX6-52AN (37.4 dBi) | 37.4 | | Y |
| RFS | RFS 2-foot HP Parabolic, SDF2-52AN or SDFX2-52AN (31.4 dBi) | 31.4 | | Y |
| RFS | RFS 4-foot HP Parabolic, SDF4-52AN or SDFX4-52AN (33.9 dBi) | 33.9 | | Y |
| RFS | RFS 6-foot HP Parabolic, SDF6-52AN or SDFX6-52AN (37.4 dBi) | 37.4 | | Y |
| StellaDoradus | StellaDoradus 45 inch Parabolic Antenna, 58PSD113 | 33.8 | | Y |

**Table 4-22** Sectored antennas for deployment in USA/Canada – 5.8 GHz

| Manufacturer | Antenna Type | Gain (dBi) | Beamwidth |
|---|---|---|---|
| RadioWaves | SEC-55V-60-17<br>SEC-55H-60-17<br>SEC-55D-60-17 | 17 | 60° |
| RadioWaves | SEC-55V-90-16<br>SEC-55H-90-16<br>SEC-55D-90-16 | 16 | 90° |

# PTP-SYNC specifications

This section contains specifications of the PTP-SYNC unit that is supplied by Motorola for PTP 500 installations that require TDD synchronization via PTP-SYNC (optional).

## PTP-SYNC dimensions and weight

The PTP-SYNC unit conforms to the physical specifications listed in Table 4-23.

**Table 4-23** PTP-SYNC unit physical specifications

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

## PTP-SYNC environmental

The PTP-SYNC unit conforms to the environmental specifications listed in Table 4-24.

**Table 4-24** PTP-SYNC unit environmental specifications

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

## PTP-SYNC electrical

The PTP-SYNC unit conforms to the electrical specifications listed in Table 4-25.

**Table 4-25** PTP-SYNC unit electrical specifications

| Category | Specification |
|---|---|
| Power supply | Integrated with PIDU Plus |
| Power consumption | 1.5 W max<br>(extra power is required to supply a GPS receiver) |

## Timing inputs

There are two timing inputs to the PTP-SYNC unit: GPS/SYNC IN (RJ-45) (Table 4-26) and 1PPS IN (SMA) (Table 4-27).

**Table 4-26** PTP-SYNC unit timing specifications - GPS/SYNC IN (RJ-45)

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

**Table 4-27** PTP-SYNC unit timing specifications - 1PPS IN (SMA)

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

## GPS/SYNC IN pinout description

The pinouts of the PTP-SYNC unit GPS/SYNC IN port are specified in Table 4-28.

**Table 4-28** GPS/SYNC IN port pinouts

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

**NOTE**

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

# Wireless specifications

## General wireless specifications

Table 4-29 contains radio system specifications for the PTP 54300 and PTP 54500.

Table 4-30 contains radio system specifications for the PTP 58300 and PTP 58500.

**Table 4-29** PTP 54300 and PTP 54500 RF specifications

| Radio Technology | Specification |
|---|---|
| RF Band | 5.470-5.725 GHz |
| Channel Selection | By dynamic frequency control and manual intervention<br>Automatic detection on start-up and continual adaptation to avoid interference. |
| Dynamic Frequency Control | Initial capture 10-15 sec. Out of service on interference 100 ms. |
| Channel size | 5, 10 and 15 MHz |
| Manual Power Control | Maximum power can be controlled lower than the power limits shown above in order to control interference to other users of the band. |
| Receiver Noise Figure | Typically 6 dB |
| Integrated Antenna Type/Gain | Integrated flat plate antenna; 23dBi |
| External Antenna Gain | Depends on feeder losses, see Regulatory issues with connectorized units on page 4-62. |
| Antenna Beamwidth | 8 Degrees |
| Max Path Loss (5 MHz channel, integrated antenna) | 169 dB |
| Duplex Scheme | Symmetric fixed, asymmetric fixed or adaptive TDD |
| Range | 250 km (155 miles) optical line-of-sight<br>10 km (6 miles) non-line-of-sight |
| Over-the-Air Encryption | Proprietary scrambling mechanism. |

| Radio Technology | Specification |
|---|---|
| Weather Sensitivity | Sensitivity at higher modes may be reduced during high winds through trees due to Adaptive Modulation Threshold changes |
| Error Correction | FEC |

**Table 4-30** PTP 58300 and PTP 58500 RF specifications

| Radio Technology | Specification |
|---|---|
| RF Band | 5.725-5.850 GHz |
| Channel Selection | By dynamic frequency control and manual intervention<br>Automatic detection on start-up and continual adaptation to avoid interference. |
| Dynamic Frequency Control | Initial capture 10-15 sec. Out of service on interference 100 ms. |
| Channel size | 5, 10 and 15 MHz |
| Manual Power Control | Maximum power can be controlled lower than the power limits shown above in order to control interference to other users of the band. |
| Receiver Noise Figure | Typically 6 dB |
| Antenna Type (Integrated) | Flat plate antenna; 23 dBi |
| Antenna Type (External) | Parabolic dish, maximum permitted gain: 37.7 dBi<br>Flat plate; maximum permitted gain: 28.0 dBi<br>Sectored antennas up to 17 dBi |
| Antenna Beamwidth (Integrated) | 8 degrees |
| Max Path Loss (5 MHz Channel) | 166 dB |
| Duplex Scheme | Symmetric fixed, asymmetric fixed or adaptive TDD; same or split frequency Tx/Rx where regulations permit |
| Range | 250 km (155 miles) optical line-of-sight<br>6 miles (10km) non-line-of-sight |

| Radio Technology | Specification |
|---|---|
| Over-the-Air Encryption | Proprietary scrambling mechanism. |
| Weather Sensitivity | Sensitivity at higher modes may be reduced during high winds through trees due to Adaptive Modulation Threshold changes |
| Error Correction | FEC |

## Licenses and region codes

This section specifies the licenses and region codes that are available for each frequency variant and regional variant (RoW means rest of world):

- Table 4-31 - PTP 54300 and PTP 54500, FCC/IC regional variants
- Table 4-32 - PTP 54300 and PTP 54500, ETSI/RoW regional variants
- Table 4-33 - PTP 58300 and PTP 58500, FCC/IC regional variants
- Table 4-34 - PTP 58300 and PTP 58500, ETSI/RoW regional variants

These tables indicate the default and alternative region codes as follows:

- (Def) indicates the default region code, already installed when shipped.
- (Alt) indicates the alternative license key region code, provided in the documentation supplied with the unit.

If the link is to be installed in any other permitted region, the user must obtain a new license key from the reseller or distributor.

**CAUTION**

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

**Table 4-31** Licenses and region codes for 5.4 GHz FCC/IC variants

| Region code | License or regulation | Frequencies | DFS | Channel bandwidth | Max transmit power |
|---|---|---|---|---|---|
| 12 (Alt) | FCC USA | 5470 - 5725 MHz | Yes | 5 MHz | 23 dBm EIRP |
| | | | | 10 MHz | 26 dBm EIRP |
| | | | | 15 MHz | 28 dBm EIRP |
| 13 (Def) | Canada | 5470 - 5600 MHz<br>5650 - 5725 MHz<br>(*1) | Yes | 5 MHz | 23 dBm EIRP |
| | | | | 10 MHz | 26 dBm EIRP |
| | | | | 15 MHz | 28 dBm EIRP |

(*1) Region code 13: the band 5600 MHz to 5650 MHz is reserved for the use of weather radars.

**Table 4-32** Licenses and region codes for 5.4 GHz ETSI/RoW variants

| Region code | License or regulation | Frequencies | DFS | Channel bandwidth | Max transmit power |
|---|---|---|---|---|---|
| 7 | Full Power + Radar | 5470 - 5725 MHz | Yes | 5, 10, 15 MHz | 27 dBm |
| 8 | Full Power | 5470 - 5725 MHz | | 5, 10, 15 MHz | 27 dBm |
| 13 (Alt) | Australia | 5470 - 5600 MHz<br>5650 - 5725 MHz<br>(*1) | Yes | 5 MHz | 23 dBm EIRP |
| | | | | 10 MHz | 26 dBm EIRP |
| | | | | 15 MHz | 28 dBm EIRP |
| 20 | Thailand | 5470 - 5725 MHz | | 5, 10, 15 MHz | 30 dBm EIRP |
| 21 | Korea | 5470 - 5650 MHz | | 5 MHz | 23 dBm EIRP |
| | | | | 10 MHz | 26 dBm EIRP |
| | | | | 15 MHz | 28 dBm EIRP |
| 26 (Def) | ETSI | 5470 - 5600 MHz<br>5650 - 5725 MHz<br>(*1) | Yes | 5 MHz | 23 dBm EIRP |
| | | | | 10 MHz | 26 dBm EIRP |
| | | | | 15 MHz | 28 dBm EIRP |

(*1) Region codes 13 and 26: the band 5600 MHz to 5650 MHz is reserved for the use of weather radars.

**Table 4-33** Licenses and region codes for 5.8 GHz FCC/IC variants

| region code | License or regulation | Frequencies | DFS | Channel bandwidth | Max transmit power |
|---|---|---|---|---|---|
| 1 (Def) | FCC USA, Canada, Taiwan, Brazil | 5725 - 5850 MHz (*1) | | 5, 10, 15 MHz | 27 dBm |

(*1) Region code 1: reduced TX power at band edges.

**Table 4-34** Licenses and region codes for 5.8 GHz ETSI/RoW variants

| region code | License or regulation | Frequencies | DFS | Channel bandwidth | Max transmit power |
|---|---|---|---|---|---|
| 2 | China | 5725 - 5850 MHz | | 5 MHz | 26 dBm EIRP |
| | | | | 10 MHz | 29 dBm EIRP |
| | | | | 15 MHz | 31 dBm EIRP |
| 3 | Australia, Hong Kong | 5725 - 5850 MHz | | 5, 10, 15 MHz | 36 dBm EIRP |
| 4 (Alt) | UK | 5725 - 5795 MHz 5815 - 5850 MHz (*1) | Yes | 5 MHz | 29 dBm EIRP |
| | | | | 10 MHz | 32 dBm EIRP |
| | | | | 15 MHz | 33 dBm EIRP |
| 5 | Singapore | 5725 - 5850 MHz | | 5, 10, 15 MHz | 30 dBm EIRP (*2) |
| 6 | Eire | 5725 - 5875 MHz | | 5 MHz | 26 dBm EIRP |
| | | | | 10 MHz | 29 dBm EIRP |
| | | | | 15 MHz | 31 dBm EIRP |
| 7 | Norway | 5725 - 5795 MHz 5815 - 5850 MHz | Yes | 5 MHz | 47 dBm EIRP |
| | | | | 10 MHz | 50 dBm EIRP |
| | | | | 15 MHz | 51 dBm EIRP |
| 8 | Full Power | 5725 - 5875 MHz | | 5, 10, 15 MHz | 27 dBm |

| region code | License or regulation | Frequencies | DFS | Channel bandwidth | Max transmit power |
|---|---|---|---|---|---|
| 10 | Spain | 5725 - 5795 MHz<br>5815 - 5855 MHz | Yes | 5 MHz | 29 dBm EIRP |
| | | | | 10 MHz | 32 dBm EIRP |
| | | | | 15 MHz | 33 dBm EIRP |
| 11 | Korea | 5725 - 5825 MHz | | 15 MHz | 30 dBm EIRP |
| 19 | India | 5825 - 5875 MHz | | 5 MHz | 33 dBm EIRP |
| | | | | 10 MHz | 36 dBm EIRP |
| | | | | 15 MHz | 36 dBm EIRP |
| 20 | Thailand | 5725 - 5850 MHz | | 5, 10, 15 MHz | 30 dBm EIRP |
| 22 | Germany | 5755 - 5875 MHz | Yes | 5 MHz | 29 dBm EIRP |
| | | | | 10 MHz | 32 dBm EIRP |
| | | | | 15 MHz | 33 dBm EIRP |
| 24 | Bahrain | 5725 - 5850 MHz | Yes | 5 MHz | 26 dBm EIRP |
| | | | | 10 MHz | 29 dBm EIRP |
| | | | | 15 MHz | 31 dBm EIRP |
| 25 | ETSI | 5725 - 5875 MHz | Yes | 5 MHz | 29 dBm EIRP |
| (Def) | | | | 10 MHz | 32 dBm EIRP |
| | | | | 15 MHz | 33 dBm EIRP |
| 27 | Denmark | 5725 - 5795<br>5815 - 5875 MHz<br>(*1) | Yes | 5 MHz | 29 dBm EIRP |
| | | | | 10 MHz | 32 dBm EIRP |
| | | | | 15 MHz | 33 dBm EIRP |

(*1) Region codes 4 and 27: the 5795 MHz to 5815 MHz band is assigned for Road Transport and Traffic Telematics (RTTT).

(*2) Region code 5: maximum transmit power is limited to 20 dBm EIRP in links that were installed before system release 500-04-00. This limit still applies when these units are upgraded to system release 500-04-00 or later.

# Available spectrum settings

## PTP 54300 and PTP 54500 available spectrum settings

The available spectrum settings for the PTP 54300 and PTP 54500 are illustrated in this section.

Adjustment of the lower center frequency allows the operator to slide the available frequency settings up and down the 5.4 GHz band in steps of 2 MHz.

In the 15 MHz (Figure 4-1), 10 MHz (Figure 4-2) and 5 MHz (Figure 4-3) channel bandwidths, the PTP 54300 and PTP 54500 variants operate on a 5 MHz channel raster. The channel raster is set to even center frequencies. The PTP 54300 and PTP 54500 product variants do not apply any band edge power reduction.

**NOTE**

These tables contain data for one typical region code. The specified channel center frequencies may not be available in other region codes.

**Figure 4-1** PTP 54300 and PTP 54500 available spectrum in 15 MHz channel bandwidth

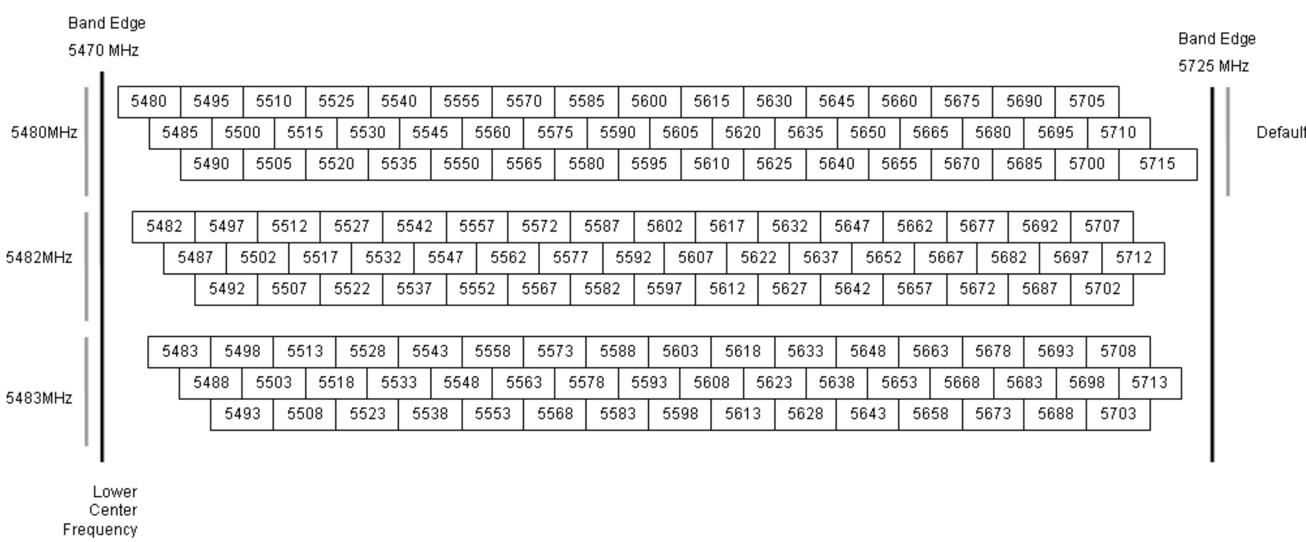


**Figure 4-2** PTP 54300 and PTP 54500 available spectrum in 10 MHz channel bandwidth

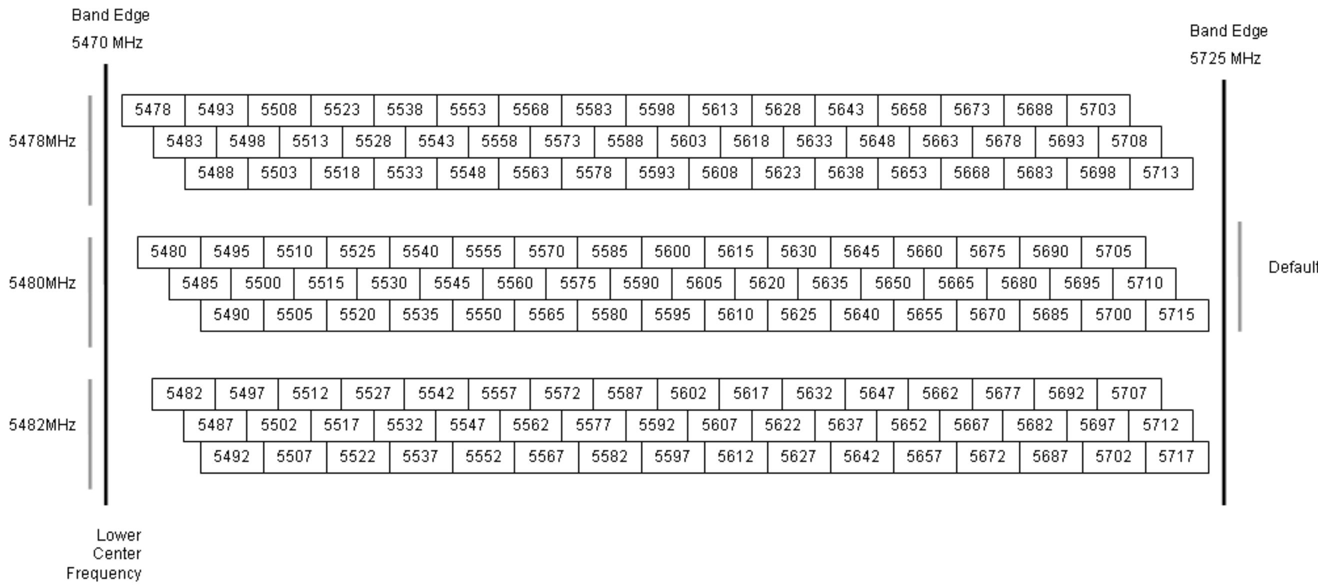
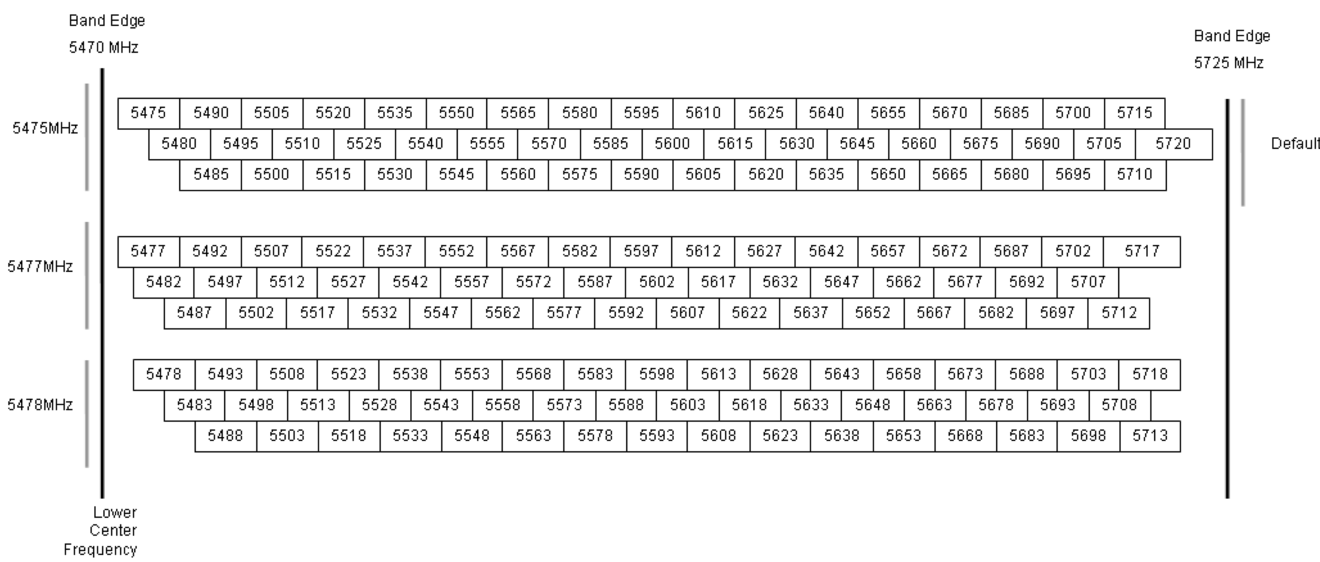



**Figure 4-3** PTP 54300 and PTP 54500 available spectrum in 5 MHz channel bandwidth



## PTP 58300 and PTP 58500 available spectrum settings

The available spectrum settings for the PTP 58300 and PTP 58500 are illustrated in this section.

Adjustment of the lower center frequency allows the operator to slide the available frequency settings up and down the 5.8 GHz band in steps of 2 MHz.

In the 15 MHz (Figure 4-4), 10 MHz (Figure 4-5) and 5 MHz (Figure 4-6) channel bandwidths, the PTP 58300 and PTP 58500 variants operate on a 5 MHz channel raster. The channel raster is set to even center frequencies.

**NOTE**

These tables contain data for one typical region code. The specified channel center frequencies may not be available in other region codes.

**Figure 4-4** PTP 58300 and PTP 58500 available spectrum in 15 MHz channel bandwidth

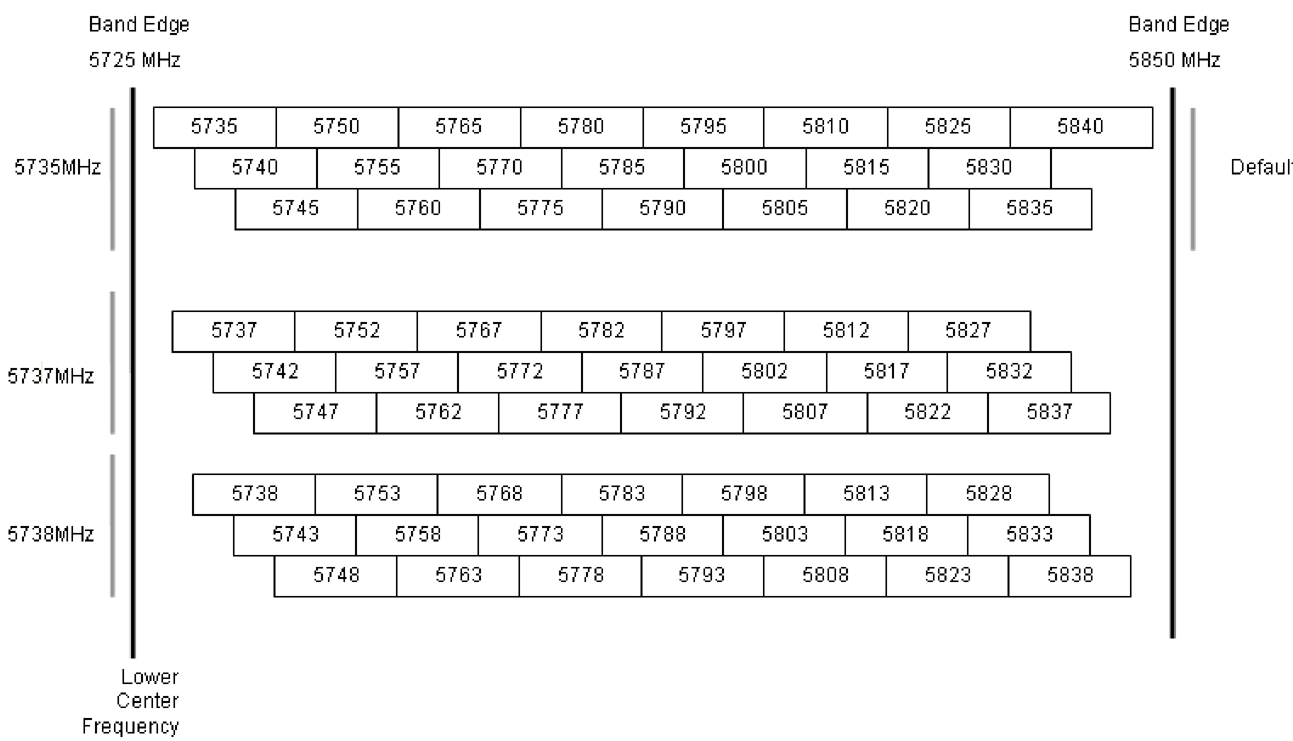


**Figure 4-5** PTP 58300 and PTP 58500 available spectrum in the 10 MHz channel bandwidth

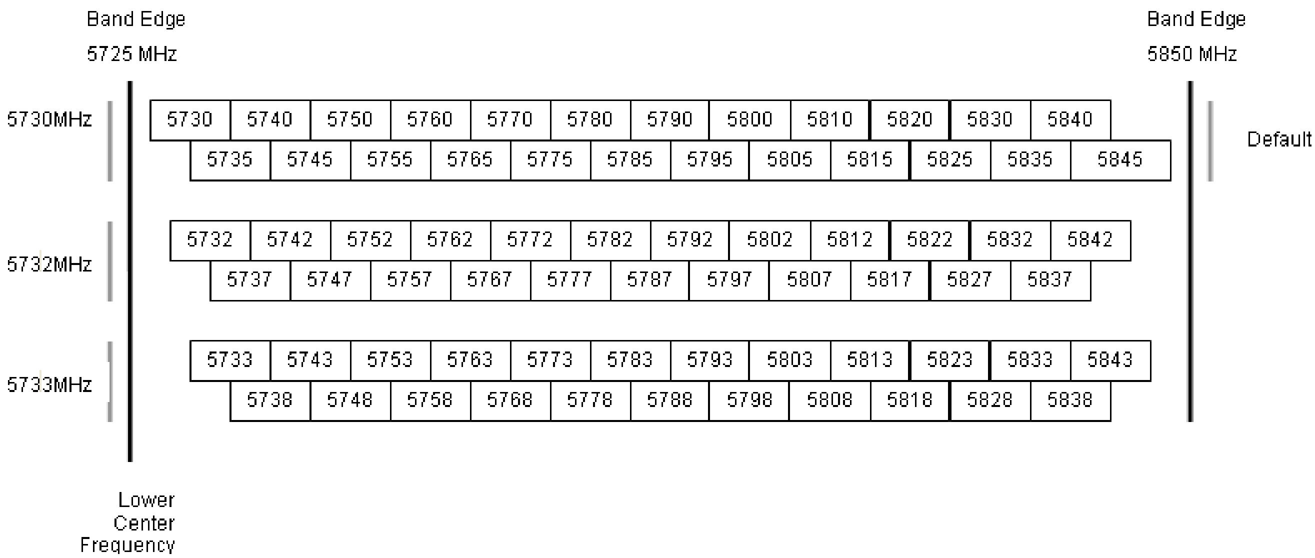
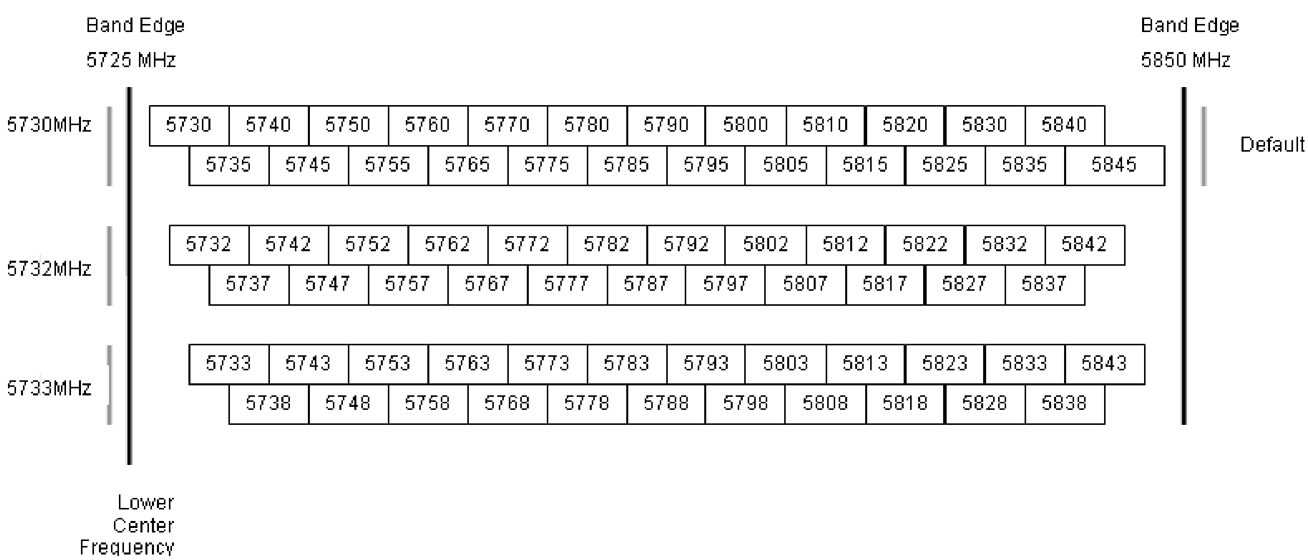



**Figure 4-6** PTP 58300 and PTP 58500 available spectrum in 5 MHz channel bandwidth



## Transmit power reduction at the band edges

Operation at or near the 5.8 GHz band edges can results in a lower maximum transmit power. In some configurations the system reduces the power when operating at the edge channels. The amount of reduction, if any, is dependant on the region code of the region of operation. This currently only affects systems configured with region code 1. The maximum powers at the edge channels for 5 MHz, 10 MHz and 15 MHz are presented in Table 4-35 (for region code 1 ONLY).

**Table 4-35** PTP 58300 and PTP 58500 maximum transmit power at the edge channels (FCC)

| Channel | Channel width (MHz) | | |
|---|---|---|---|
| | 5 | 10 | 15 |
| 5730 | 26 | N/A | N/A |
| 5731 | 27 | N/A | N/A |
| 5732 | 27 | N/A | N/A |
| 5733 | 27 | 26 | N/A |
| 5734 | 27 | 27 | N/A |
| 5735 | 27 | 27 | 25 |
| 5736 | 27 | 27 | 25 |
| 5737 | 27 | 27 | 25 |
| 5738 | 27 | 27 | 25 |
| 5739 | 27 | 27 | 25 |
| 5740 - 5838 | 27 | 27 | 27 |
| 5839 | 27 | 27 | 26 |
| 5840 | 27 | 27 | 26 |
| 5841 | 27 | 27 | N/A |
| 5842 | 27 | 26 | N/A |
| 5843 | 27 | N/A | N/A |
| 5844 | 27 | N/A | N/A |
| 5845 | 26 | N/A | N/A |

## System threshold, output power and link loss

PTP 54300 and PTP 54500 system threshold, output power and maximum link loss are given in the following tables:

- Table 4-36 - IP Mode (15 MHz bandwidth)
- Table 4-37 - TDM Mode (15 MHz bandwidth)
- Table 4-38 - IP Mode (10 MHz bandwidth)
- Table 4-39 - TDM Mode (10 MHz bandwidth)
- Table 4-40 - IP Mode (5 MHz bandwidth)
- Table 4-41 - TDM Mode (5 MHz bandwidth)

PTP 58300 and PTP 58500 system threshold, output power and maximum link loss are given in the following tables:

- Table 4-42 - IP Mode (15 MHz bandwidth)
- Table 4-43 - TDM Mode (15 MHz bandwidth)
- Table 4-44 - IP Mode (10 MHz bandwidth)
- Table 4-45 - TDM Mode (10 MHz bandwidth)
- Table 4-46 - IP Mode (5 MHz bandwidth)
- Table 4-47 - TDM Mode (5 MHz bandwidth)

These figures assume that antenna gain is 23 dBi.

**Table 4-36** PTP 54300 and PTP 54500 thresholds - IP mode (15 MHz bandwidth)

| Modulation mode | System threshold (dBm) | Vector error (dB) | Output power (dBm) | Max link loss (dB) |
|---|---|---|---|---|
| 64QAM 0.83 dual | -70.2 | -21.1 | +21.0 | 137.2 |
| 64QAM 0.67 dual | -74.0 | -18.8 | +22.0 | 142.0 |
| 16QAM 0.75 dual | -76.7 | -14.7 | +23.0 | 145.6 |
| 16QAM 0.50 dual | -81.2 | -12.1 | +24.0 | 151.2 |
| QPSK 0.75 dual | -82.6 | -8.3 | +25.0 | 153.6 |
| 64QAM 0.83 single | -73.6 | -21.1 | +21.0 | 140.5 |
| 64QAM 0.67 single | -77.0 | -18.8 | +22.0 | 145.0 |
| 16QAM 0.75 single | -79.9 | -14.7 | +23.0 | 148.9 |
| 16QAM 0.50 single | -84.8 | -12.0 | +24.0 | 154.8 |
| QPSK 0.75 single | -86.4 | -8.2 | +25.0 | 157.4 |
| QPSK 0.50 single | -88.8 | -6.5 | +26.0 | 160.8 |
| BPSK 0.50 single | -94.1 | -1.9 | +27.0 | 167.1 |

**Table 4-37** PTP 54300 and PTP 54500 thresholds - TDM mode (15 MHz bandwidth)

| Modulation mode | System threshold (dBm) | Vector error (dB) | Output power (dBm) | Max link loss (dB) |
|---|---|---|---|---|
| 64QAM 0.83 dual | -65.9 | -24.2 | +21.0 | 132.9 |
| 64QAM 0.67 dual | -69.3 | -21.9 | +22.0 | 137.3 |
| 16QAM 0.75 dual | -73.6 | -17.8 | +23.0 | 142.6 |
| 16QAM 0.50 dual | -76.3 | -15.1 | +24.0 | 146.3 |
| QPSK 0.75 dual | -79.1 | -11.5 | +25.0 | 150.1 |
| 64QAM 0.83 single | -69.7 | -24.2 | +21.0 | 136.7 |
| 64QAM 0.67 single | -72.5 | -22.0 | +22.0 | 140.5 |
| 16QAM 0.75 single | -76.5 | -17.8 | +23.0 | 145.5 |
| 16QAM 0.50 single | -79.3 | -15.1 | +24.0 | 149.3 |
| QPSK 0.75 single | -82.5 | -11.5 | +25.0 | 153.5 |
| QPSK 0.50 single | -84.9 | -9.7 | +26.0 | 156.9 |
| BPSK 0.50 single | -94.1 | -1.9 | +27.0 | 167.1 |

**Table 4-38** PTP 54300 and PTP 54500 thresholds - IP mode (10 MHz bandwidth)

| Modulation mode | System threshold (dBm) | Vector error (dB) | Output power (dBm) | Max link loss (dB) |
|---|---|---|---|---|
| 64QAM 0.83 dual | -72.7 | -21.1 | +21.0 | 139.7 |
| 64QAM 0.67 dual | -76.2 | -18.8 | +22.0 | 144.2 |
| 16QAM 0.75 dual | -79.2 | -14.7 | +23.0 | 148.2 |
| 16QAM 0.50 dual | -83.8 | -12.1 | +24.0 | 153.8 |
| QPSK 0.75 dual | -84.7 | -8.5 | +25.0 | 155.7 |
| 64QAM 0.83 single | -75.2 | -21.1 | +21.0 | 142.2 |
| 64QAM 0.67 single | -78.7 | -18.8 | +22.0 | 146.7 |
| 16QAM 0.75 single | -81.8 | -14.7 | +23.0 | 150.7 |
| 16QAM 0.50 single | -86.8 | -12.0 | +24.0 | 156.8 |
| QPSK 0.75 single | -88.5 | -8.1 | +25.0 | 159.5 |
| QPSK 0.50 single | -90.7 | -6.5 | +26.0 | 162.7 |
| BPSK 0.50 single | -95.5 | -2.0 | +27.0 | 168.5 |

**Table 4-39** PTP 54300 and PTP 54500 thresholds - TDM mode (10 MHz bandwidth)

| Modulation mode | System threshold (dBm) | Vector error (dB) | Output power (dBm) | Max link loss (dB) |
|---|---|---|---|---|
| 64QAM 0.83 dual | -67.4 | -24.2 | +21.0 | 134.4 |
| 64QAM 0.67 dual | -70.8 | -21.9 | +22.0 | 138.8 |
| 16QAM 0.75 dual | -75.0 | -17.8 | +23.0 | 144.0 |
| 16QAM 0.50 dual | -77.8 | -15.1 | +24.0 | 147.8 |
| QPSK 0.75 dual | -80.7 | -11.6 | +25.0 | 151.7 |
| 64QAM 0.83 single | -71.2 | -24.2 | +21.0 | 138.2 |
| 64QAM 0.67 single | -73.9 | -22.0 | +22.0 | 141.9 |
| 16QAM 0.75 single | -78.0 | -17.8 | +23.0 | 147.0 |
| 16QAM 0.50 single | -81.0 | -15.1 | +24.0 | 151.0 |
| QPSK 0.75 single | -84.7 | -11.2 | +25.0 | 155.7 |
| QPSK 0.50 single | -86.6 | -9.7 | +26.0 | 158.6 |
| BPSK 0.50 single | -95.5 | -2.0 | +27.0 | 168.5 |

**Table 4-40** PTP 54300 and PTP 54500 thresholds - IP mode (5 MHz bandwidth)

| Modulation mode | System threshold (dBm) | Vector error (dB) | Output power (dBm) | Max link loss (dB) |
|---|---|---|---|---|
| 64QAM 0.83 dual | -74.8 | -21.1 | +21.0 | 141.8 |
| 64QAM 0.67 dual | -78.3 | -18.8 | +22.0 | 146.3 |
| 16QAM 0.75 dual | -81.4 | -14.7 | +23.0 | 150.4 |
| 16QAM 0.50 dual | -86.4 | -12.1 | +24.0 | 156.4 |
| QPSK 0.75 dual | -87.3 | -8.7 | +25.0 | 158.3 |
| 64QAM 0.83 single | -77.7 | -21.2 | +21.0 | 144.7 |
| 64QAM 0.67 single | -81.5 | -18.8 | +22.0 | 149.5 |
| 16QAM 0.75 single | -84.8 | -14.7 | +23.0 | 153.8 |
| 16QAM 0.50 single | -88.8 | -12.2 | +24.0 | 158.8 |
| QPSK 0.75 single | -90.4 | -9.0 | +25.0 | 161.4 |
| QPSK 0.50 single | -92.3 | -7.5 | +26.0 | 164.3 |
| BPSK 0.50 single | -99.0 | -1.9 | +27.0 | 172.0 |

**Table 4-41** PTP 54300 and PTP 54500 thresholds - TDM mode (5 MHz bandwidth)

| Modulation mode | System threshold (dBm) | Vector error (dB) | Output power (dBm) | Max link loss (dB) |
|---|---|---|---|---|
| 64QAM 0.83 dual | -70.4 | -24.2 | +21.0 | 137.4 |
| 64QAM 0.67 dual | -73.4 | -22.0 | +22.0 | 141.4 |
| 16QAM 0.75 dual | -77.5 | -17.8 | +23.0 | 146.5 |
| 16QAM 0.50 dual | -80.5 | -15.1 | +24.0 | 150.5 |
| QPSK 0.75 dual | -83.8 | -11.4 | +25.0 | 154.8 |
| 64QAM 0.83 single | -74.0 | -24.2 | +21.0 | 141.0 |
| 64QAM 0.67 single | -76.5 | -22.0 | +22.0 | 144.5 |
| 16QAM 0.75 single | -80.8 | -17.8 | +23.0 | 149.8 |
| 16QAM 0.50 single | -84.1 | -15.2 | +24.0 | 154.1 |
| QPSK 0.75 single | -87.8 | -11.1 | +25.0 | 158.8 |
| QPSK 0.50 single | -89.7 | -9.5 | +26.0 | 161.7 |
| BPSK 0.50 single | -99.0 | -1.9 | +27.0 | 172.0 |

**Table 4-42** PTP 58300 and PTP 58500 thresholds - IP mode (15 MHz bandwidth)

| Modulation mode | System threshold (dBm) | Vector error (dB) | Output power (dBm) | Max link loss (dB) |
|---|---|---|---|---|
| 64QAM 0.83 dual | -70.2 | -21.1 | +21.0 | 137.2 |
| 64QAM 0.67 dual | -74.0 | -18.8 | +22.0 | 142.0 |
| 16QAM 0.75 dual | -76.7 | -14.7 | +23.0 | 145.7 |
| 16QAM 0.50 dual | -81.3 | -12.1 | +24.0 | 151.3 |
| QPSK 0.75 dual | -82.6 | -8.4 | +25.0 | 153.6 |
| 64QAM 0.83 single | -73.7 | -21.1 | +21.0 | 140.7 |
| 64QAM 0.67 single | -77.1 | -18.8 | +22.0 | 145.1 |
| 16QAM 0.75 single | -79.9 | -14.7 | +23.0 | 148.9 |
| 16QAM 0.50 single | -84.9 | -12.0 | +24.0 | 154.9 |
| QPSK 0.75 single | -86.5 | -8.2 | +25.0 | 157.4 |
| QPSK 0.50 single | -89.0 | -6.4 | +26.0 | 161.0 |
| BPSK 0.50 single | -94.4 | -2.0 | +27.0 | 167.4 |

**Table 4-43** PTP 58300 and PTP 58500 thresholds - TDM mode (15 MHz bandwidth)

| Modulation mode | System threshold (dBm) | Vector error (dB) | Output power (dBm) | Max link loss (dB) |
|---|---|---|---|---|
| 64QAM 0.83 dual | -66.4 | -24.1 | +21.0 | 133.4 |
| 64QAM 0.67 dual | -69.6 | -21.9 | +22.0 | 137.6 |
| 16QAM 0.75 dual | -73.7 | -17.8 | +23.0 | 142.7 |
| 16QAM 0.50 dual | -76.3 | -15.1 | +24.0 | 146.3 |
| QPSK 0.75 dual | -79.8 | -11.5 | +25.0 | 150.2 |
| 64QAM 0.83 single | -69.9 | -24.2 | +21.0 | 136.9 |
| 64QAM 0.67 single | -72.6 | -22.0 | +22.0 | 140.6 |
| 16QAM 0.75 single | -76.5 | -17.8 | +23.0 | 145.5 |
| 16QAM 0.50 single | -79.3 | -15.1 | +24.0 | 149.3 |
| QPSK 0.75 single | -82.9 | -11.2 | +25.0 | 153.9 |
| QPSK 0.50 single | -85.0 | -9.6 | +26.0 | 157.0 |
| BPSK 0.50 single | -94.4 | -2.0 | +27.0 | 167.4 |

**Table 4-44** PTP 58300 and PTP 58500 thresholds - IP mode (10 MHz bandwidth)

| Modulation mode | System threshold (dBm) | Vector error (dB) | Output power (dBm) | Max link loss (dB) |
|---|---|---|---|---|
| 64QAM 0.83 dual | -72.8 | -21.1 | +21.0 | 139.8 |
| 64QAM 0.67 dual | -76.2 | -18.7 | +22.0 | 144.2 |
| 16QAM 0.75 dual | -79.2 | -14.7 | +23.0 | 148.2 |
| 16QAM 0.50 dual | -83.7 | -12.1 | +24.0 | 153.7 |
| QPSK 0.75 dual | -84.7 | -8.5 | +25.0 | 155.7 |
| 64QAM 0.83 single | -75.3 | -21.2 | +21.0 | 142.3 |
| 64QAM 0.67 single | -78.8 | -18.7 | +22.0 | 146.8 |
| 16QAM 0.75 single | -81.8 | -14.7 | +23.0 | 150.8 |
| 16QAM 0.50 single | -86.8 | -12.1 | +24.0 | 156.8 |
| QPSK 0.75 single | -88.5 | -8.1 | +25.0 | 159.5 |
| QPSK 0.50 single | -90.7 | -6.5 | +26.0 | 162.7 |
| BPSK 0.50 single | -96.4 | -2.0 | +27.0 | 169.4 |

**Table 4-45** PTP 58300 and PTP 58500 thresholds - TDM mode (10 MHz bandwidth)

| Modulation mode | System threshold (dBm) | Vector error (dB) | Output power (dBm) | Max link loss (dB) |
|---|---|---|---|---|
| 64QAM 0.83 dual | -68.0 | -24.1 | +21.0 | 135.0 |
| 64QAM 0.67 dual | -71.0 | -21.9 | +22.0 | 139.0 |
| 16QAM 0.75 dual | -75.0 | -17.8 | +23.0 | 144.0 |
| 16QAM 0.50 dual | -77.8 | -15.1 | +24.0 | 147.8 |
| QPSK 0.75 dual | -80.7 | -11.6 | +25.0 | 151.7 |
| 64QAM 0.83 single | -71.7 | -24.2 | +21.0 | 138.7 |
| 64QAM 0.67 single | -74.1 | -22.0 | +22.0 | 142.1 |
| 16QAM 0.75 single | -78.1 | -17.8 | +23.0 | 147.1 |
| 16QAM 0.50 single | -81.0 | -15.1 | +24.0 | 151.0 |
| QPSK 0.75 single | -84.8 | -11.2 | +25.0 | 155.7 |
| QPSK 0.50 single | -86.6 | -9.7 | +26.0 | 158.6 |
| BPSK 0.50 single | -96.4 | -2.0 | +27.0 | 169.4 |

**Table 4-46** PTP 58300 and PTP 58500 thresholds - IP mode (5 MHz bandwidth)

| Modulation mode | System threshold (dBm) | Vector error (dB) | Output power (dBm) | Max link loss (dB) |
|---|---|---|---|---|
| 64QAM 0.83 dual | -75.0 | -21.1 | +21.0 | 142.0 |
| 64QAM 0.67 dual | -78.5 | -18.8 | +22.0 | 146.5 |
| 16QAM 0.75 dual | -81.5 | -14.7 | +23.0 | 150.5 |
| 16QAM 0.50 dual | -86.5 | -12.1 | +24.0 | 156.5 |
| QPSK 0.75 dual | -87.3 | -8.8 | +25.0 | 158.3 |
| 64QAM 0.83 single | -77.9 | -21.2 | +21.0 | 144.9 |
| 64QAM 0.67 single | -81.7 | -18.8 | +22.0 | 149.6 |
| 16QAM 0.75 single | -84.9 | -14.7 | +23.0 | 153.9 |
| 16QAM 0.50 single | -88.7 | -12.2 | +24.0 | 158.7 |
| QPSK 0.75 single | -90.5 | -9.0 | +25.0 | 161.4 |
| QPSK 0.50 single | -92.4 | -7.5 | +26.0 | 164.4 |
| BPSK 0.50 single | -99.0 | -1.9 | +27.0 | 172.0 |

**Table 4-47** PTP 58300 and PTP 58500 thresholds - TDM mode (5 MHz bandwidth)

| Modulation mode | System threshold (dBm) | Vector error (dB) | Output power (dBm) | Max link loss (dB) |
|---|---|---|---|---|
| 64QAM 0.83 dual | -71.0 | -24.1 | +21.0 | 138.0 |
| 64QAM 0.67 dual | -73.6 | -22.0 | +22.0 | 141.6 |
| 16QAM 0.75 dual | -77.7 | -17.8 | +23.0 | 146.7 |
| 16QAM 0.50 dual | -80.6 | -15.1 | +24.0 | 150.6 |
| QPSK 0.75 dual | -83.9 | -11.4 | +25.0 | 154.9 |
| 64QAM 0.83 single | -74.4 | -24.2 | +21.0 | 141.4 |
| 64QAM 0.67 single | -76.7 | -22.0 | +22.0 | 144.7 |
| 16QAM 0.75 single | -81.0 | -17.8 | +23.0 | 150.0 |
| 16QAM 0.50 single | -84.8 | -14.5 | +24.0 | 154.8 |
| QPSK 0.75 single | -88.0 | -11.0 | +25.0 | 159.0 |
| QPSK 0.50 single | -89.8 | -9.5 | +26.0 | 161.8 |
| BPSK 0.50 single | -99.0 | -1.9 | +27.0 | 172.0 |

# Data network specifications

## Ethernet interfaces

The PTP 300 and PTP 500 Ethernet ports conform to the specifications listed in Table 4-48 and Table 4-49.

**Table 4-48** Ethernet bridging specifications

| Ethernet Bridging | Specification |
|---|---|
| Protocol | IEEE802.1; IEEE802.1p; IEEE802.3 compatible |
| QoS | IEEE 802.1p (eight levels), IEEE 802.1Q, IEEE 802.1ad |
| Interface | 100BaseT (RJ-45), Supports MDI/MDIX Auto Crossover |
| Data Rates | See Data rate calculations on page 4-77. |
| Maximum Ethernet Frame Size | 2000 bytes |

**NOTE**

Practical Ethernet rates will depend on network configuration, higher layer protocols and platforms used.

Over the air throughput will be capped to the rate of the Ethernet interface at the receiving end of the link.

**Table 4-49** Telecoms interface specifications

| Telecoms | Specification |
|---|---|
| Interfaces | E1 balanced 120R or T1 balanced 100R over a CAT5 screened twisted pair cable |
| Jitter and Wander | Compliant with G.823/ G.824. |
| Surge Protection and Power Cross | Compliant with GR1089, EN60950. |

# System management data

## SNMPv3 default configuration (MIB-based)

When SNMPv3 MIB-based Security Mode is enabled, the default configuration for the `usmUserTable` table is based on one initial user and four template users as listed in Table 4-50.

**Table 4-50** Default SNMPv3 users

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

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

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

## Email alerts

The management agent can be configured to generate alerts by electronic mail when any of the following events occur:

- Wireless Link Up/Down
- DFS Channel Change
- DFS Impulse Interference
- Enabled Diagnostic Alarms
- Data Port Up/Down

# Safety compliance

## Electrical safety compliance

The PTP 300 and PTP 500 hardware has been tested for compliance to the electrical safety specifications listed in Table 4-51.

**Table 4-51** Safety compliance specifications

| Region | Specification |
|---|---|
| USA | UL 60950 |
| Canada | CSA C22.2 No.60950 |
| International | CB certified & certificate to IEC 60950 |

# Electromagnetic compliance

## EMC immunity compliance

The PTP 300 and PTP 500 comply with European EMC Specification EN301 489-1 with testing carried out to the detailed requirements of EN301 489-4.

**NOTE**

For EN 61000-4-2: 1995 Electro Static Discharge (ESD), Class 2, 8 kV air, 4 kV contact discharge, the PTP 300 and PTP 500 have been tested to ensure immunity to 15 kV air and 8 kV contact.

Table 4-52 lists the EMC specification type approvals that have been granted for the PTP 300 and PTP 500.

**Table 4-52** EMC emissions compliance

| Region | Specification (Type Approvals) |
|---|---|
| USA | FCC Part 15 Class B |
| Canada | CSA Std C108.8, 1993 Class B |
| Europe | EN55022 CISPR 22 |

## Radio certifications

Table 4-53 lists the radio specification type approvals that have been granted for PTP 300 and PTP 500 frequency variants.

**Table 4-53** Radio certifications

| Variant | Region | Specification (Type Approvals) |
|---|---|---|
| PTP 54300 and PTP 54500 | USA | FCC Part 15 E |
| | Canada | RSS 210 Issue 7, Annex 9 |
| | Europe | EN301 893 V1.5.1 |
| PTP 58300 and PTP 58500 | USA | FCC Part 15.247 |
| | CANADA | RSS 210 Issue 7, Annex 8 |
| | UK | IR 2007 |
| | Eire | ComReg 06/47R |
| | Germany | Order No 47/2007 |
| | EU | EN302 502 v 1.2.1 |
| | Spain | CNAF-2010-BOE |
| | Norway | REG 2009-06-02 no. 580 |
| | Denmark | Danish radio interface 00 007 |

# Compliance with regulations

Changes or modifications not expressly approved by Motorola could void the user's authority to operate the system.

This system has achieved Type Approval in various countries around the world. This means that the system has been tested against various local technical regulations and found to comply. The frequency bands in which the system operates may be 'unlicensed' and, in these bands, the system can be used provided it does not cause interference. Further, it is not guaranteed protection against interference from other products and installations.

**CAUTION**

When planning a link that will use Connectorized PTP 300 or PTP 500 Series (with external antennas), ensure that regulatory requirements are met for the installation, as described in Regulatory issues with connectorized units on page 4-62.

## FCC and ETSI compliance testing (without PTP-SYNC)

Without PTP-SYNC installed, the system has been tested for compliance to both US (FCC) and European (ETSI) specifications. It has been shown to comply with the limits for emitted spurious radiation for a Class B digital device, pursuant to Part 15 of the FCC Rules in the USA and appropriate European ENs. These limits have been designed to provide reasonable protection against harmful interference. However the equipment can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to other radio communications. There is no guarantee that interference will not occur in a particular installation.

**NOTE**

A Class B Digital Device is a device that is marketed for use in a residential environment, notwithstanding use in commercial, business and industrial environments.

**NOTE**

Notwithstanding that Motorola has designed (and qualified) the PTP 300 and PTP 500 products to generally meet the Class B requirement to minimize the potential for interference, the PTP 300 and PTP 500 product ranges are not marketed for use in a residential environment.

## FCC and ETSI compliance testing (with PTP-SYNC)

With PTP-SYNC installed, this equipment has been tested and found to comply with the limits for a Class B digital device, provided that the PIDU Plus is correctly grounded as described in Indoor CAT5e cable on page 4-18.

## Radio and television interference

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the Outdoor Unit (ODU).
- Increase the separation between the affected equipment and ODU.
- Connect the ODU and PIDU Plus into a power outlet on a circuit different from that to which the receiver is connected.
- Consult your installer or supplier for help.

## Deployment and operation

The Radio Regulations of various countries' limits constrain the operation of radio products generally. In particular the local regulator may limit the amount of conducted or radiated transmitter power and may require registration of the radio link.

The power transmitted by the PTP 300 and PTP 500 Series is controlled by the use of region-specific license keys. Contact your supplier/installer to ensure that your product is set for the correct license key for your country and region and to ensure that you have fulfilled all the local regulatory requirements, especially if you are intending to use a link with external antennas.

## Registration of links

UK Registration of Links – OfCom, The application form may be found at:

http://www.ofcom.org.uk/radiocomms/isu

Eire Registration of Links – Commission for Communication Regulation, The application form may be found at:

http://www.comreg.ie/licensing_and_services

# Regulatory issues with connectorized units

## Maximum EIRP for connectorized units

In most regions (including USA, Canada, Europe and Australia) operation of products in the band 5470 MHz to 5725 MHz is constrained by an EIRP limit. The constraint is that the EIRP must not exceed 30 dBm or (17 + 10 x Log Bandwidth) dBm.

In some regions (including Europe) operation of products in the band 5725 MHz to 5850/5875 MHz is constrained by an EIRP limit. The constraint is that the EIRP must not exceed 36 dBm or (23 + 10 x Log Bandwidth) dBm.

As the products have an operating bandwidth from approximately 5 MHz to approximately 15 MHz, then the maximum allowed EIRP depends on the operating bandwidth of the radio as shown in Table 4-54.

**Table 4-54** Normal EIRP limits with operating channel bandwidth

| Operating bandwidth (MHz) | Allowed EIRP (dBm) at 5.4 GHz | Allowed EIRP (dBm) at 5.8 GHz |
|---|---|---|
| 5 | 24 | 30 |
| 10 | 27 | 33 |
| 15 | 28.8 | 34.8 |

## Calculating EIRP for connectorized units

When operating with external antennas, the installer or operator has to set the maximum transmit power to ensure that the EIRP limit is not exceeded. The EIRP may be calculated from:

Allowed EIRP(dBm) =

Max_Transmit_Power (dBm) + Antenna Gain (dBi) – Feeder Losses (dB)

and hence:

Max_Transmit_Power (dBm) =

Allowed EIRP(dBm) – Antenna Gain (dBi) + Feeder Losses (dB)

## The Set_Max_Transmit_Power parameter for connectorized units

As the actual maximum transmit power can only be adjusted in 1 dB steps, then the installer or operator must configure the system to have a Set_Max_Transmit_Power parameter as calculated below:

> Set_Max_Transmit_Power = [Max_Transmit_Power] rounded down to nearest lower dB step

In order to simplify matters, the settings to be used for regions with the EIRP limits in Table 4-54 (assuming short feeder cables) are shown in Table 4-55.

**Table 4-55** Setting maximum transmit power to meet general EIRP limits

| Antenna size | Maximum available antenna gain (dBi) | Operating bandwidth (MHz) | Set_Max_Transmit_Power parameter setting (dBm) | |
|---|---|---|---|---|
| | | | 5.4 GHz | 5.8 GHz |
| 2ft dish | 29.4 | 5 | -6 | 0 |
| | | 10 | -3 | 3 |
| | | 15 | -2 | 4 |
| 2.5ft dish | 31.2 | 5 | -8 | -2 |
| | | 10 | -5 | 1 |
| | | 15 | -3 | 3 |
| 3ft dish | 33.4 | 5 | -10 | -4 |
| | | 10 | -7 | -1 |
| | | 15 | -5 | 0 |
| 4ft dish | 34.8 | 5 | -11 | -6 |
| | | 10 | -8 | -3 |
| | | 15 | -7 | -1 |

**NOTE**

Table 4-55 has been calculated on the basis of 0.5 dB cable loss and the highest gain antennas per size of which Motorola are aware. At these operating frequencies, feeder losses even with short cables are unlikely ever to be below 0.5 dB for practical installations and cable diameters.

## Cable losses (FCC regions only) for connectorized units

The FCC approval for the product is based on tests with a cable loss between the units of not less than 1.2 dB at 5.8 GHz. The use of lower cable losses would result in the installation being outside the FCC rules. As an indication, 1.2 dB of cable loss corresponds to the following cable lengths excluding connector losses (source: Times Microwave).

**Table 4-56** Cable losses per length

| Cable | Length for 1.2dB Cable Loss at 5.8 GHz | |
|---|---|---|
| | (ft) | (m) |
| LMR100 | 1.9 | 0.6 |
| LMR200 | 4.6 | 1.4 |
| LMR300 | 7.25 | 2.2 |
| LMR400 | 11.1 | 3.4 |
| LMR600 | 16.5 | 5.0 |

# Electromagnetic energy

## Standards

Relevant standards (USA and EC) applicable when working with RF equipment are:

- *ANSI IEEE C95.1-1991, IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz.*
- Council recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz) (1999/519/EC) and respective national regulations.
- *Directive 2004/40/EC of the European Parliament and of the Council of 29 April 2004* on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) (18th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC).
- US FCC limits for the general population. See the FCC web site at http://www.fcc.gov, and the policies, guidelines, and requirements in Part 1 of Title 47 of the Code of Federal Regulations, as well as the guidelines and suggestions for evaluating compliance in FCC OET Bulletin 65.
- Health Canada limits for the general population. See the Health Canada web site at http://www.hc-sc.gc.ca/ewh-semt/pubs/radiation/99ehd-dhm237/limits-limites_e.html and Safety Code 6.
- EN 50383:2002 Basic standard for the calculation and measurement of electromagnetic field strength and SAR related to human exposure from radio base stations and fixed terminal stations for wireless telecommunication systems (110 MHz - 40 GHz).
- BS EN 50385:2002 Product standard to demonstrate the compliances of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields (110 MHz – 40 GHz) – general public.
- ICNIRP (International Commission on Non-Ionizing Radiation Protection) guidelines for the general public. See the ICNIRP web site at http://www.icnirp.de/ and Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields.

## Power density exposure limit

Install the radios for the PTP 300 and PTP 500 families of PTP wireless solutions so as to provide and maintain the minimum separation distances from all persons.

The applicable power density exposure limit from the standards (see Electromagnetic energy on page 4-65 ) is:

**10 W/m²** for RF energy in the 5.4 GHz and 5.8 GHz frequency bands.

## Calculation of power density

**NOTE**

The following calculation is based on the ANSI IEEE C95.1-1991 method. as that provides a worst case analysis. Details of the assessment to EN50383:2002 can be provided, if required.

Peak power density in the far field of a radio frequency point source is calculated as follows:

$$S = \frac{P.G}{4\pi d^2}$$

| Where: | Is: |
|---|---|
| S | power density in $W/m^2$ |
| P | maximum average transmit power capability of the radio, in W |
| G | total Tx gain as a factor, converted from dB |
| d | distance from point source, in m |

Rearranging terms to solve for distance yields:

$$d = \sqrt{\frac{P.G}{4\pi.S}}$$

## Calculated distances and power compliance margins

Table 4-57 shows calculated minimum separation distances, recommended distances and resulting margins for each frequency band and antenna combination. These are conservative distances that include compliance margins. At these and greater separation distances, the power density from the RF field is below generally accepted limits for the general population.

Explanation of terms used in Table 4-57:

Tx burst – maximum average transmit power in burst (Watt)

P – maximum average transmit power capability of the radio (Watt)

G – total transmit gain as a factor, converted from dB

S – power density (W/m$^2$)

d – minimum distance from point source (meters)

R – recommended distances (meters)

C – compliance factor

**Table 4-57** Power compliance margins

| Band | Antenna | Tx burst (W) | P (W) | G | S (W/m$^2$) | d (m) | R (m) | C |
|---|---|---|---|---|---|---|---|---|
| 5.4 GHz | Integrated | 0.005 | 0.004 | 200 | 10 | 0.07 | 1 | 14 |
| | External 4ft Dish | 0.00035 | 0.00028 | 2884 | 10 | 0.07 | | |
| ETSI 5.8 GHz | Integrated | 0.02 | 0.016 | 200 | 10 | 0.14 | 1 | 7 |
| | External 4ft Dish | 0.0014 | 0.000112 | 2884 | 10 | 0.14 | | |
| FCC 5.8 GHz | Integrated | 0.5 | 0.256 | 200 | 10 | 0.71 | 2 | 3 |
| | External 2ft Flat Plate | 0.5 | 0.4 | 631 | 10 | 1.26 | 5 | 4 |
| | External 6ft Dish | 0.5 | 0.4 | 6310 | 10 | 4.00 | 10 | 2.5 |
| | External sectored antenna (60°) | 0.5 | 0.4 | 50.1 | 10 | 0.36 | 1 | 2.8 |

**NOTE**

Gain of antenna in dBi = 10*log(G).

The regulations require that the power used for the calculations is the maximum power in the transmit burst subject to allowance for source-based time-averaging.

At 5.4 GHz and EU 5.8 GHz, the products are generally limited to a fixed EIRP which can be achieved with the Integrated Antenna. The calculations above assume that the maximum EIRP allowed by the regulations is being transmitted.

**NOTE**

If there are no EIRP limits in the country of deployment, use the distance calculations for FCC 5.8 GHz for all frequency bands.

At FCC 5.8 GHz, for antennas between 0.6m (2ft) and 1.8m (6ft), alter the distance proportionally to the antenna gain.

# Examples of regulatory limits

## PTP 54300 and PTP 54500

Table 4-58 shows how the regulatory limits currently apply in specific countries. Operators should note that regulations are subject to change.

**Table 4-58** PTP 54300 and PTP 54500 examples of regulatory limits

| Region | Examples of Regulatory Limits at 5.4GHz |
|---|---|
| FCC | Under FCC Regulations, operation of this product is only allowed with a license key for region 12. This implements Radar Detection in accordance with FCC Regulations and limits the EIRP to the regulatory limits below:<br>EIRP ≤ Max of [(17 +10 x Log(Channel BW)) and 30] dBm |
| ETSI | Under ETSI Regulations, operation of this product is only allowed with a license key for region 26. This implements Radar Detection in accordance with ETSI Regulations, including barring of the band from 5600 MHz to 5650 MHz and limits the EIRP to the regulatory limits below:<br>EIRP ≤ Max of [(17 +10 x Log(Channel BW)) and 30] dBm |
| Canada | Under Industry Canada Regulations, operation of this product is only allowed with a license key for region 13. This implements Radar Detection in accordance with Canadian Regulations, including barring of the band from 5600 MHz to 5650 MHz and limits the EIRP to the regulatory limits below:<br>EIRP ≤ Max of [(17 +10 x Log(Channel BW)) and 30] dBm |

| General Notice Applicable to Europe – 5.4 GHz |
|---|
| This equipment complies with the essential requirements for the EU R&E Directive 1999/5/EC. |

**NOTE**

In regions other than EU/USA, specific local regulations may apply. It is the responsibility of the installer/user to check that the equipment as deployed meets local regulatory requirements.

## PTP 58300 and PTP 58500

Table 4-59 shows how the regulatory limits currently apply in specific countries. Operators should note that regulations are subject to change.

**Table 4-59** PTP 58300 and PTP 58500 examples of regulatory limits

| Region | Examples of regulatory limits |
|---|---|
| USA/ Canada/ Taiwan | Equipment can be operated in any mode, best results will be obtained using region 1 settings. There are some limitations on the use of antennas above 4ft diameter plus a 1 dB band edge power reduction. |
| UK | Under UK Regulations, operation of this product is allowed with a license key for region 4 .  This implements Radar Detection with barring of the band from 5795 MHz to 5815 MHz and above 5850 MHz.  It limits the EIRP to the Regulatory Limits below:<br>EIRP ≤ Max of [(23 +10 x Log(Channel BW)) and 36] dBm |
| Eire | Under Eire Regulations, operation of this product is only allowed with a license key for region 6. This limits the EIRP to the Regulatory Limits below:<br>EIRP ≤ Max of [(20 +10 x Log(Channel BW)) and 33] dBm |
| Norway | Under Norway Regulations, operation of this product is only allowed with a license key for region 7. This implements Radar Detection and limits the EIRP to the Regulatory Limits below:<br>EIRP ≤ Max of [(40 +10 x Log(Channel BW)) and 53] dBm |
| Germany | Operation of this product is only allowed with a license key for region 22. This implements Radar Detection. It limits the band of operation to 5755 MHz to 5875 MHz and limits the EIRP to the Regulatory Limits below:<br>EIRP ≤ Max of [(23 +10 x Log(Channel BW)) and 36] dBm |
| Denmark | Operation of this product is only allowed with a license key for region 27.  This implements Radar Detection with barring of the band from 5795 MHz to 5815 MHz.  It limits the EIRP to the Regulatory Limits below:<br>EIRP ≤ Max of [(23 +10 x Log(Channel BW)) and 36] dBm |

| Region | Examples of regulatory limits |
|---|---|
| Spain | Operation of this product is allowed with a license key for region 10 . This implements Radar Detection with barring of the band from 5795 MHz to 5815 MHz and above 5850 MHz. It limits the EIRP to the Regulatory Limits below:<br>EIRP ≤ Max of [(23 +10 x Log(Channel BW)) and 36] dBm |

| General Notice Applicable to Europe – 5.8 GHz |
|---|
| This equipment complies with the essential requirements for the EU R&E Directive 1999/5/EC. |
| The use of 5.8 GHz for Point to Point radio links is not harmonized across the EU and currently the product may only be deployed in the UK, Eire (IRL), Germany, Denmark, Norway and Spain. |
| However, the regulatory situation in Europe is changing and the radio spectrum may become available in other countries in the near future. Please contact Motorola for the latest situation. |

# Notifications

The PTP 300 and PTP 500 comply with the regulations that are in force in the USA, Canada and Europe. The relevant notifications are specified in this section.

## PTP 54300 and PTP 54500 FCC and IC notification

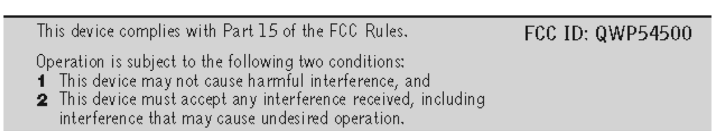
U.S. Federal Communication Commission (FCC) and Industry Canada (IC) Notification.

This device complies with part 15.407 of the US FCC Rules and Regulations and with RSS-210 Issue 7 of Industry Canada.  Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation. In Canada, users should be cautioned to take note that high power radars are allocated as primary users (meaning they have priority) of the 5250 – 5350 MHz and 5470 – 5725 MHz and these radars could cause interference and/or damage to license-exempt local area networks (LELAN).

For the connectorized version of the product and in order to reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that permitted by the regulations.  The transmitted power must be reduced to achieve this requirement.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the US FCC Rules and with RSS-210 of Industry Canada.  These limits are designed to provide reasonable protection against harmful interference in a residential installation.  This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference by one or more of the following measures:

- Increase the separation between the affected equipment and the unit;
- Connect the affected equipment to a power outlet on a different circuit from that which the receiver is connected to;
- Consult the dealer and/or experienced radio/TV technician for help.
- FCC IDs and Industry Canada Certification Numbers are listed below:




Where necessary, the end user is responsible for obtaining any National licenses required to operate this product and these must be obtained before using the product in any particular country. Contact the appropriate national administrations for details on the conditions of use for the bands in question and any exceptions that might apply.

## PTP 54300 and PTP 54500 European Union notification

The PTP 54300 and PTP 54500 products are two-way radio transceivers suitable for use in Broadband Wireless Access System (WAS), Radio Local Area Network (RLAN), or Fixed Wireless Access (FWA) systems. They are a Class 1 devices and use operating frequencies that are harmonized throughout the EU member states. The operator is responsible for obtaining any national licenses required to operate these products and these must be obtained before using the products in any particular country.

Hereby, Motorola declares that the PTP 54300 and PTP 54500 products comply with the essential requirements and other relevant provisions of Directive 1999/5/EC. The declaration of conformity may be consulted at http://www.motorola.com/ptp/support.

This equipment is marked to show compliance with the European R&TTE directive 1999/5/EC.



.

**European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive** The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases). As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste. Customers or end-users in EU countries should contact their local equipment supplier representative or service center for information about the waste collection system in their country.

## PTP 58300 and PTP 58500 FCC and IC notification

U.S. Federal Communication Commission (FCC) and Industry Canada (IC) Notification.

This system has achieved Type Approval in various countries around the world. This means that the system has been tested against various local technical regulations and found to comply. The frequency band in which the system operates is ‘license exempt’ and the system is allowed to be used provided it does not cause interference. Further, the licensing authority does not guaranteed protection against interference from other products and installations.

This device complies with part 15 of the US FCC Rules and Regulations and with RSS-210 of Industry Canada. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation. In Canada, users should be cautioned to take note that high power radars are allocated as primary users (meaning they have priority) of the 5650 – 5850 MHz spectrum and these radars could cause interference and/or damage to license-exempt local area networks (LELAN).

For the connectorized version of the product and in order to reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the Effective Isotropically Radiated Power (EIRP) is not more than that permitted for successful communication.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the US FCC Rules and with RSS-210 of Industry Canada. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with these instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment on and off, the user is encouraged to correct the interference by one or more of the following measures:

- Increase the separation between the affected equipment and the unit;
- Connect the affected equipment to a power outlet on a different circuit from that which the receiver is connected to;
- Consult the dealer and/or experienced radio/TV technician for help.

FCC IDs and Industry Canada Certification Numbers are listed below:

This device complies with Part 15 of the FCC Rules.

FCC ID: QWP58500

Operation is subject to the following two conditions:

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

IC:109AO-58500

Where necessary, the end user is responsible for obtaining any National licenses required to operate this product and these must be obtained before using the product in any particular country. Contact the appropriate national administrations for details on the conditions of use for the bands in question and any exceptions that might apply.

## PTP 58300 and PTP 58500 European Union notification

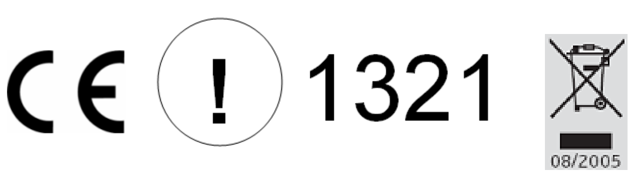
The PTP 58300 and PTP 58500 are Class 2 devices as they operate on frequencies that are not harmonized across the EU. Currently the products may only be operated in Denmark, Germany, Eire (IRL), Norway, Spain and the UK. However, the regulatory situation in Europe is changing and the radio spectrum may become available in other countries in future. See www.ero.dk for further information. The operator is responsible for obtaining any national licenses required to operate these products and these must be obtained before using the products in any particular country.

**NOTE**

Norway regulation is FOR2007-04-20 Nr 439 regarding border PFD limit.

Hereby, Motorola declares that the PTP 58300 and PTP 58500 products comply with the essential requirements and other relevant provisions of Directive 1999/5/EC. The declaration of conformity may be consulted at http://www.motorola.com/ptp/support.

This equipment is marked to show compliance with the European R&TTE directive 1999/5/EC.



**European Union (EU) Waste of Electrical and Electronic Equipment (WEEE) directive:**

The European Union's WEEE directive requires that products sold into EU countries must have the crossed out trash bin label on the product (or the package in some cases). As defined by the WEEE directive, this cross-out trash bin label means that customers and end-users in EU countries should not dispose of electronic and electrical equipment or accessories in household waste. Customers or end-users in EU countries should contact their local equipment supplier representative or service center for information about the waste collection system in their country.

## PTP 58300 and PTP 58500 EU notification

The PTP 58300 and PTP 58500 connectorized products have been notified for operation in the EU countries listed in Table 4-59.

**CAUTION**

This equipment operates as a secondary application, so it has no rights against harmful interference, even if generated by similar equipment, and must not cause harmful interference on systems operating as primary applications.

# Data rate calculations

This section provides instructions, tables and graphs to allow calculation of the data rate capacity that can be provided by alternative PTP 300 and PTP 500 configurations.

The following topics are described in this section:



## Data rate defined

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

- Product (PTP 300 or PTP 500)
- Link Symmetry
- Link Mode Optimization (IP or TDM)
- Modulation Mode
- Channel Bandwidth
- Link Range

# Calculation procedure and example

## Procedure

To calculate the data rate capacity of a PTP 300 or PTP 500 link, perform Procedure 4-1.

**Procedure 4-1** Calculating data rate capacity

| | |
|---|---|
| **1** | Use the tables in Data throughput capacity on page 4-80 to look up the data throughput capacity rates (Tx, Rx and Both) for the required combination of:<br>Product (PTP 300 or PTP 500)<br>Link Symmetry<br>Link Mode Optimization<br>Modulation Mode<br>Channel Bandwidth |
| **2** | The tables contain data rates for links of zero range. Use the curves in Range adjustment curves on page 4-87 to look up the Throughput Factor that must be applied to adjust the data rates for the actual range of the link. |
| **3** | Multiply the data rates by the Throughput Factor to give the throughput capacity of the link. |

**NOTE**

There is a small difference between the rates for IP and TDM because there is fragmentation in TDM (for low priority traffic) which causes the throughput to be reduced buy approximately 1% compared to the IP mode.

## Example

Suppose that the link characteristics are:

- Product = PTP 500
- Link Symmetry = 1:1
- Link Mode Optimization = TDM
- Modulation Mode = 64QAM 0.83 Dual
- Channel Bandwidth = 10 MHz
- Link Range = 55 km

To calculate the throughput capacity of the link, proceed as follows:

**Procedure 4-2** Example of data rate capacity calculation

| | |
|---|---|
| **1** | Use Table 4-65 to look up the data throughput capacity rates:<br>Tx = 32.78<br>Rx = 32.78<br>Both = 65.56 |
| **2** | Use Figure 4-8 to look up the Throughput Factor for 1:1, TDM and Link Range 55 km. The factor is 0.7. |
| **3** | Multiply the rates from Step 2 by the Throughput Factor from Step 3 to give the throughput capacity of the link:<br>Tx = 22.95<br>Rx = 22.95<br>Both = 45.89<br>If the product is a PTP 500 Lite, divide these figures by 2. |

## Data throughput capacity

The following tables show the data throughput rates (Mbits/s) that are achieved when the link distance (range) is 0 km:

- Table 4-60 - PTP 300, link symmetry = adaptive or 3:1
- Table 4-61 - PTP 300, link symmetry 1:1, link optimization IP
- Table 4-62 - PTP 300, link symmetry 1:1, link optimization TDM
- Table 4-63 - PTP 500 Full, link symmetry = adaptive or 3:1
- Table 4-64 - PTP 500 Full, link symmetry 1:1, link optimization IP
- Table 4-65 - PTP 500 Full, link symmetry 1:1, link optimization TDM

Use the curves in Range adjustment curves on page 4-87 to adjust these figures to allow for link range

**NOTE**

When using these tables, be aware of the factors that affect data throughput, as listed below.

Data throughput capacity is restricted by the following factors:

- Throughput for Link Symmetry 3:1 is the same as that for 1:3, but the Tx and Rx data rates are swapped.
- The data rates for Adaptive symmetry apply to the most asymmetric case where the link has significant offered traffic in one direction only. The data rates for Adaptive symmetry with bidirectional offered traffic are the same as those for Link Symmetry = 1:1 with Link Optimization = IP.
- PTP 500 Lite data rates are half the quoted PTP 500 Full rates.

**Table 4-60** Throughput for PTP 300, link symmetry = adaptive or 3:1 (Mbit/s)

| LOS disabled: | 15 MHz | | | 10 MHz | | | 5 MHz | | |
|---|---|---|---|---|---|---|---|---|---|
| **Modulation mode** | **Tx** | **Rx** | **Both** | **Tx** | **Rx** | **Both** | **Tx** | **Rx** | **Both** |
| 64QAM 0.83 Dual | 19.37 | 6.40 | 25.77 | 19.44 | 6.30 | 25.74 | Not supported | | |
| 64QAM 0.67 Dual | 15.50 | 5.05 | 20.55 | 15.40 | 5.05 | 20.45 | | | |
| 16QAM 0.75 Dual | 11.62 | 3.87 | 15.49 | 11.62 | 3.78 | 15.39 | | | |
| 16QAM 0.50 Dual | 7.75 | 2.52 | 10.27 | 7.58 | 2.52 | 10.10 | | | |
| QPSK 0.75 Dual | 5.73 | 1.85 | 7.57 | 5.80 | 1.76 | 7.55 | | | |
| 64QAM 0.83 Single | 9.60 | 3.19 | 12.79 | 9.60 | 3.03 | 12.62 | | | |
| 64QAM 0.67 Single | 7.75 | 2.52 | 10.27 | 7.58 | 2.52 | 10.10 | | | |
| 16QAM 0.75 Single | 5.73 | 1.85 | 7.57 | 5.80 | 1.76 | 7.55 | | | |
| 16QAM 0.50 Single | 3.87 | 1.17 | 5.04 | 3.78 | 1.25 | 5.03 | | | |
| QPSK 0.75 Single | 2.86 | 0.84 | 3.69 | 2.77 | 0.75 | 3.51 | | | |
| QPSK 0.50 Single | 1.85 | 0.50 | 2.34 | 1.76 | 0.50 | 2.26 | | | |
| BPSK 0.50 Single | 0.84 | 0.16 | 1.00 | 0.75 | 0.24 | 0.99 | | | |
| **LOS enabled:** | **15 MHz** | | | **10 MHz** | | | **5 MHz** | | |
| **Modulation mode** | **Tx** | **Rx** | **Both** | **Tx** | **Rx** | **Both** | **Tx** | **Rx** | **Both** |
| 64QAM 0.83 Dual | 38.74 | 12.80 | 51.54 | 25.92 | 8.41 | 34.33 | Not supported | | |
| 64QAM 0.67 Dual | 31.00 | 10.11 | 41.11 | 20.54 | 6.73 | 27.27 | | | |
| 16QAM 0.75 Dual | 23.24 | 7.74 | 30.97 | 15.49 | 5.04 | 20.53 | | | |
| 16QAM 0.50 Dual | 15.50 | 5.04 | 20.54 | 10.10 | 3.36 | 13.46 | | | |
| QPSK 0.75 Dual | 11.45 | 3.69 | 15.14 | 7.73 | 2.34 | 10.07 | | | |
| Not supported: 64QAM 0.83 Single, 64QAM 0.67 Single, 16QAM 0.75 Single and 16QAM 0.50 Single. | | | | | | | | | |
| QPSK 0.75 Single | 0.84 | 0.16 | 1.00 | 0.75 | 0.24 | 0.99 | | | |
| QPSK 0.50 Single | 0.84 | 0.16 | 1.00 | 0.75 | 0.24 | 0.99 | | | |
| BPSK 0.50 Single | 0.84 | 0.16 | 1.00 | 0.75 | 0.24 | 0.99 | | | |

**Table 4-61** Throughput for PTP 300, link symmetry 1:1, link optimization IP (Mbit/s)

| LOS disabled: | 15 MHz | | | 10 MHz | | | 5 MHz | | |
|---|---|---|---|---|---|---|---|---|---|
| **Modulation mode** | **Tx** | **Rx** | **Both** | **Tx** | **Rx** | **Both** | **Tx** | **Rx** | **Both** |
| 64QAM 0.83 Dual | 12.97 | 12.97 | 25.93 | 12.87 | 12.87 | 25.75 | 6.30 | 6.30 | 12.59 |
| 64QAM 0.67 Dual | 10.27 | 10.27 | 20.54 | 10.34 | 10.34 | 20.69 | 5.04 | 5.04 | 10.09 |
| 16QAM 0.75 Dual | 7.75 | 7.75 | 15.50 | 7.58 | 7.58 | 15.15 | 3.77 | 3.77 | 7.55 |
| 16QAM 0.50 Dual | 5.05 | 5.05 | 10.11 | 5.05 | 5.05 | 10.10 | 2.52 | 2.52 | 5.04 |
| QPSK 0.75 Dual | 3.87 | 3.87 | 7.74 | 3.78 | 3.78 | 7.55 | 1.75 | 1.75 | 3.50 |
| 64QAM 0.83 Single | 6.40 | 6.40 | 12.80 | 6.30 | 6.30 | 12.61 | 3.02 | 3.02 | 6.05 |
| 64QAM 0.67 Single | 5.05 | 5.05 | 10.11 | 5.05 | 5.05 | 10.10 | 2.52 | 2.52 | 5.04 |
| 16QAM 0.75 Single | 3.87 | 3.87 | 7.74 | 3.78 | 3.78 | 7.55 | 1.75 | 1.75 | 3.50 |
| 16QAM 0.50 Single | 2.52 | 2.52 | 5.04 | 2.52 | 2.52 | 5.04 | 1.25 | 1.25 | 2.50 |
| QPSK 0.75 Single | 1.85 | 1.85 | 3.69 | 1.76 | 1.76 | 3.51 | 0.75 | 0.75 | 1.49 |
| QPSK 0.50 Single | 1.17 | 1.17 | 2.34 | 1.25 | 1.25 | 2.51 | 0.50 | 0.50 | 1.01 |
| BPSK 0.50 Single | 0.50 | 0.50 | 1.00 | 0.50 | 0.50 | 1.01 | 0.24 | 0.24 | 0.48 |
| **LOS enabled:** | **15 MHz** | | | **10 MHz** | | | **5 MHz** | | |
| **Modulation mode** | **Tx** | **Rx** | **Both** | **Tx** | **Rx** | **Both** | **Tx** | **Rx** | **Both** |
| 64QAM 0.83 Dual | 25.93 | 25.93 | 51.86 | 17.17 | 17.17 | 34.33 | 8.40 | 8.40 | 16.79 |
| 64QAM 0.67 Dual | 20.54 | 20.54 | 41.08 | 13.79 | 13.79 | 27.58 | 6.73 | 6.73 | 13.45 |
| 16QAM 0.75 Dual | 15.50 | 15.50 | 30.99 | 10.10 | 10.10 | 20.20 | 5.03 | 5.03 | 10.06 |
| 16QAM 0.50 Dual | 10.11 | 10.11 | 20.21 | 6.73 | 6.73 | 13.46 | 3.36 | 3.36 | 6.72 |
| QPSK 0.75 Dual | 7.74 | 7.74 | 15.47 | 5.04 | 5.04 | 10.07 | 2.34 | 2.34 | 4.67 |
| Not supported: 64QAM 0.83 Single, 64QAM 0.67 Single, 16QAM 0.75 Single and 16QAM 0.50 Single. | | | | | | | | | |
| QPSK 0.75 Single | 0.50 | 0.50 | 1.00 | 0.50 | 0.50 | 1.01 | 0.24 | 0.24 | 0.48 |
| QPSK 0.50 Single | 0.50 | 0.50 | 1.00 | 0.50 | 0.50 | 1.01 | 0.24 | 0.24 | 0.48 |
| BPSK 0.50 Single | 0.50 | 0.50 | 1.00 | 0.50 | 0.50 | 1.01 | 0.24 | 0.24 | 0.48 |

**Table 4-62** Throughput for PTP 300, link symmetry 1:1, link optimization TDM (Mbit/s)

| LOS disabled: | 15 MHz | | | 10 MHz | | | 5 MHz | | |
|---|---|---|---|---|---|---|---|---|---|
| Modulation mode | Tx | Rx | Both | Tx | Rx | Both | Tx | Rx | Both |
| 64QAM 0.83 Dual | 12.39 | 12.39 | 24.78 | 12.29 | 12.29 | 24.59 | 6.30 | 6.30 | 12.59 |
| 64QAM 0.67 Dual | 9.81 | 9.81 | 19.63 | 9.88 | 9.88 | 19.76 | 5.04 | 5.04 | 10.09 |
| 16QAM 0.75 Dual | 7.40 | 7.40 | 14.81 | 7.23 | 7.23 | 14.46 | 3.77 | 3.77 | 7.55 |
| 16QAM 0.50 Dual | 4.83 | 4.83 | 9.66 | 4.82 | 4.82 | 9.64 | 2.52 | 2.52 | 5.04 |
| QPSK 0.75 Dual | 3.70 | 3.70 | 7.39 | 3.61 | 3.61 | 7.22 | 1.75 | 1.75 | 3.50 |
| 64QAM 0.83 Single | 6.12 | 6.12 | 12.23 | 6.02 | 6.02 | 12.04 | 3.02 | 3.02 | 6.05 |
| 64QAM 0.67 Single | 4.83 | 4.83 | 9.66 | 4.82 | 4.82 | 9.64 | 2.52 | 2.52 | 5.04 |
| 16QAM 0.75 Single | 3.70 | 3.70 | 7.39 | 3.61 | 3.61 | 7.22 | 1.75 | 1.75 | 3.50 |
| 16QAM 0.50 Single | 2.41 | 2.41 | 4.82 | 2.41 | 2.41 | 4.82 | 1.25 | 1.25 | 2.50 |
| QPSK 0.75 Single | 1.76 | 1.76 | 3.53 | 1.68 | 1.68 | 3.35 | 0.75 | 0.75 | 1.49 |
| QPSK 0.50 Single | 1.12 | 1.12 | 2.24 | 1.20 | 1.20 | 2.39 | 0.50 | 0.50 | 1.01 |
| BPSK 0.50 Single | 0.48 | 0.48 | 0.95 | 0.48 | 0.48 | 0.96 | 0.24 | 0.24 | 0.48 |
| **LOS enabled:** | **15 MHz** | | | **10 MHz** | | | **5 MHz** | | |
| **Modulation mode** | **Tx** | **Rx** | **Both** | **Tx** | **Rx** | **Both** | **Tx** | **Rx** | **Both** |
| 64QAM 0.83 Dual | 24.78 | 24.78 | 49.56 | 16.39 | 16.39 | 32.78 | 8.40 | 8.40 | 16.79 |
| 64QAM 0.67 Dual | 19.63 | 19.63 | 39.25 | 13.17 | 13.17 | 26.34 | 6.73 | 6.73 | 13.45 |
| 16QAM 0.75 Dual | 14.81 | 14.81 | 29.61 | 9.64 | 9.64 | 19.28 | 5.03 | 5.03 | 10.06 |
| 16QAM 0.50 Dual | 9.66 | 9.66 | 19.31 | 6.43 | 6.43 | 12.85 | 3.36 | 3.36 | 6.72 |
| QPSK 0.75 Dual | 7.39 | 7.39 | 14.78 | 4.81 | 4.81 | 9.62 | 2.34 | 2.34 | 4.67 |
| Not supported: 64QAM 0.83 Single, 64QAM 0.67 Single, 16QAM 0.75 Single and 16QAM 0.50 Single. | | | | | | | | | |
| QPSK 0.75 Single | 0.48 | 0.48 | 0.95 | 0.48 | 0.48 | 0.96 | 0.24 | 0.24 | 0.48 |
| QPSK 0.50 Single | 0.48 | 0.48 | 0.95 | 0.48 | 0.48 | 0.96 | 0.24 | 0.24 | 0.48 |
| BPSK 0.50 Single | 0.48 | 0.48 | 0.95 | 0.48 | 0.48 | 0.96 | 0.24 | 0.24 | 0.48 |

**Table 4-63** Throughput for PTP 500 Full, link symmetry = adaptive or 3:1 (Mbit/s)

| Modulation mode | 15 MHz | | | 10 MHz | | | 5 MHz | | |
|---|---|---|---|---|---|---|---|---|---|
| | Tx | Rx | Both | Tx | Rx | Both | Tx | Rx | Both |
| 64QAM 0.83 Dual | 77.48 | 25.60 | 103.08 | 51.84 | 16.81 | 68.65 | Not supported | | |
| 64QAM 0.67 Dual | 62.00 | 20.21 | 82.21 | 41.07 | 13.46 | 54.53 | | | |
| 16QAM 0.75 Dual | 46.47 | 15.47 | 61.94 | 30.98 | 10.07 | 41.05 | | | |
| 16QAM 0.50 Dual | 30.99 | 10.08 | 41.07 | 20.20 | 6.72 | 26.92 | | | |
| QPSK 0.75 Dual | 22.90 | 7.38 | 30.28 | 15.46 | 4.68 | 20.14 | | | |
| 64QAM 0.83 Single | 38.38 | 12.77 | 51.15 | 25.59 | 8.07 | 33.66 | | | |
| 64QAM 0.67 Single | 30.99 | 10.08 | 41.07 | 20.20 | 6.72 | 26.92 | | | |
| 16QAM 0.75 Single | 22.90 | 7.38 | 30.28 | 15.46 | 4.68 | 20.14 | | | |
| 16QAM 0.50 Single | 15.47 | 4.68 | 20.15 | 10.07 | 3.34 | 13.41 | | | |
| QPSK 0.75 Single | 11.43 | 3.34 | 14.77 | 7.38 | 1.99 | 9.37 | | | |
| QPSK 0.50 Single | 7.38 | 1.99 | 9.37 | 4.68 | 1.34 | 6.02 | | | |
| BPSK 0.50 Single | 3.34 | 0.64 | 3.98 | 1.99 | 0.64 | 2.63 | | | |

**Table 4-64** Throughput for PTP 500 Full, link symmetry 1:1, link optimization IP (Mbit/s)

| Modulation mode | 15 MHz | | | 10 MHz | | | 5 MHz | | |
|---|---|---|---|---|---|---|---|---|---|
| | Tx | Rx | Both | Tx | Rx | Both | Tx | Rx | Both |
| 64QAM 0.83 Dual | 51.86 | 51.86 | 103.72 | 34.33 | 34.33 | 68.66 | 16.79 | 16.79 | 33.58 |
| 64QAM 0.67 Dual | 41.08 | 41.08 | 82.16 | 27.58 | 27.58 | 55.16 | 13.45 | 13.45 | 26.90 |
| 16QAM 0.75 Dual | 30.99 | 30.99 | 61.98 | 20.20 | 20.20 | 40.40 | 10.06 | 10.06 | 20.12 |
| 16QAM 0.50 Dual | 20.21 | 20.21 | 40.42 | 13.46 | 13.46 | 26.92 | 6.72 | 6.72 | 13.44 |
| QPSK 0.75 Dual | 15.47 | 15.47 | 30.94 | 10.07 | 10.07 | 20.14 | 4.67 | 4.67 | 9.34 |
| 64QAM 0.83 Single | 25.60 | 25.60 | 51.20 | 16.81 | 16.81 | 33.62 | 8.06 | 8.06 | 16.12 |
| 64QAM 0.67 Single | 20.21 | 20.21 | 40.42 | 13.46 | 13.46 | 26.92 | 6.72 | 6.72 | 13.44 |
| 16QAM 0.75 Single | 15.47 | 15.47 | 30.94 | 10.07 | 10.07 | 20.14 | 4.67 | 4.67 | 9.34 |
| 16QAM 0.50 Single | 10.08 | 10.08 | 20.16 | 6.72 | 6.72 | 13.44 | 3.33 | 3.33 | 6.66 |
| QPSK 0.75 Single | 7.38 | 7.38 | 14.76 | 4.68 | 4.68 | 9.36 | 1.99 | 1.99 | 3.98 |
| QPSK 0.50 Single | 4.68 | 4.68 | 9.36 | 3.34 | 3.34 | 6.68 | 1.34 | 1.34 | 2.68 |
| BPSK 0.50 Single | 1.99 | 1.99 | 3.98 | 1.34 | 1.34 | 2.68 | 0.64 | 0.64 | 1.28 |

**Table 4-65** Throughput for PTP 500 Full, link symmetry 1:1, link optimization TDM (Mbit/s)

| Modulation Mode | 15 MHz | | | 10 MHz | | | 5 MHz | | |
|---|---|---|---|---|---|---|---|---|---|
| | Tx | Rx | Both | Tx | Rx | Both | Tx | Rx | Both |
| 64QAM 0.83 Dual | 49.56 | 49.56 | 99.12 | 32.78 | 32.78 | 65.56 | 16.79 | 16.79 | 33.58 |
| 64QAM 0.67 Dual | 39.25 | 39.25 | 78.50 | 26.34 | 26.34 | 52.68 | 13.45 | 13.45 | 26.90 |
| 16QAM 0.75 Dual | 29.61 | 29.61 | 59.22 | 19.28 | 19.28 | 38.56 | 10.06 | 10.06 | 20.12 |
| 16QAM 0.50 Dual | 19.31 | 19.31 | 38.62 | 12.85 | 12.85 | 25.70 | 6.72 | 6.72 | 13.44 |
| QPSK 0.75 Dual | 14.78 | 14.78 | 29.56 | 9.62 | 9.62 | 19.24 | 4.67 | 4.67 | 9.34 |
| 64QAM 0.83 Single | 24.46 | 24.46 | 48.92 | 16.05 | 16.05 | 32.10 | 8.06 | 8.06 | 16.12 |
| 64QAM 0.67 Single | 19.31 | 19.31 | 38.62 | 12.85 | 12.85 | 25.70 | 6.72 | 6.72 | 13.44 |
| 16QAM 0.75 Single | 14.78 | 14.78 | 29.56 | 9.62 | 9.62 | 19.24 | 4.67 | 4.67 | 9.34 |
| 16QAM 0.50 Single | 9.63 | 9.63 | 19.26 | 6.42 | 6.42 | 12.84 | 3.33 | 3.33 | 6.66 |
| QPSK 0.75 Single | 7.05 | 7.05 | 14.10 | 4.47 | 4.47 | 8.94 | 1.99 | 1.99 | 3.98 |
| QPSK 0.50 Single | 4.47 | 4.47 | 8.94 | 3.19 | 3.19 | 6.38 | 1.34 | 1.34 | 2.68 |
| BPSK 0.50 Single | 1.90 | 1.90 | 3.80 | 1.28 | 1.28 | 2.56 | 0.64 | 0.64 | 1.28 |

# Range adjustment curves

Use these curves to look up the link Range and find the Throughput Factor that must be applied to adjust the 0 km data throughput rates for the required combination of Link Symmetry, Link Optimization and Link Range (km).

Curve A (Figure 4-7) is used when one of the following conditions applies:

- Link Symmetry = 3:1
- Link Symmetry = 1:1 and Link Optimization = IP
- Link Symmetry = 1:3

Curve B (Figure 4-8) is used only when Link Symmetry = 1:1 and Link Optimization = TDM.

**Figure 4-7** PTP 300 and PTP 500 range adjustment for data rates, curve A

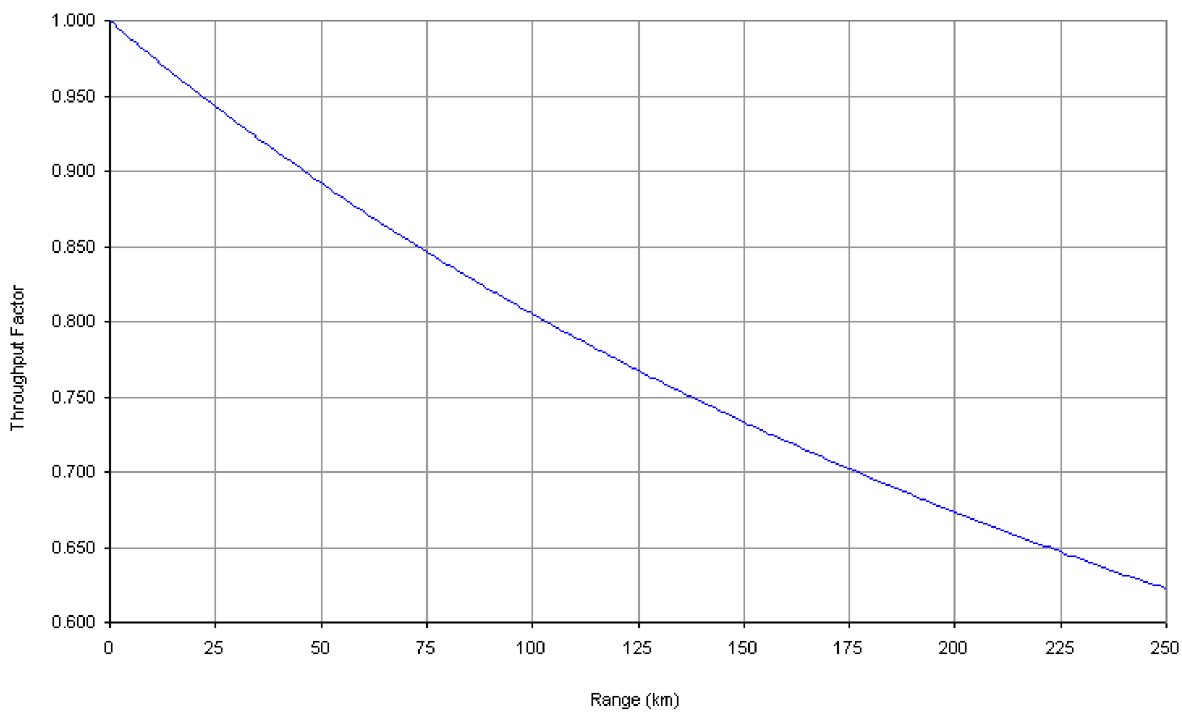
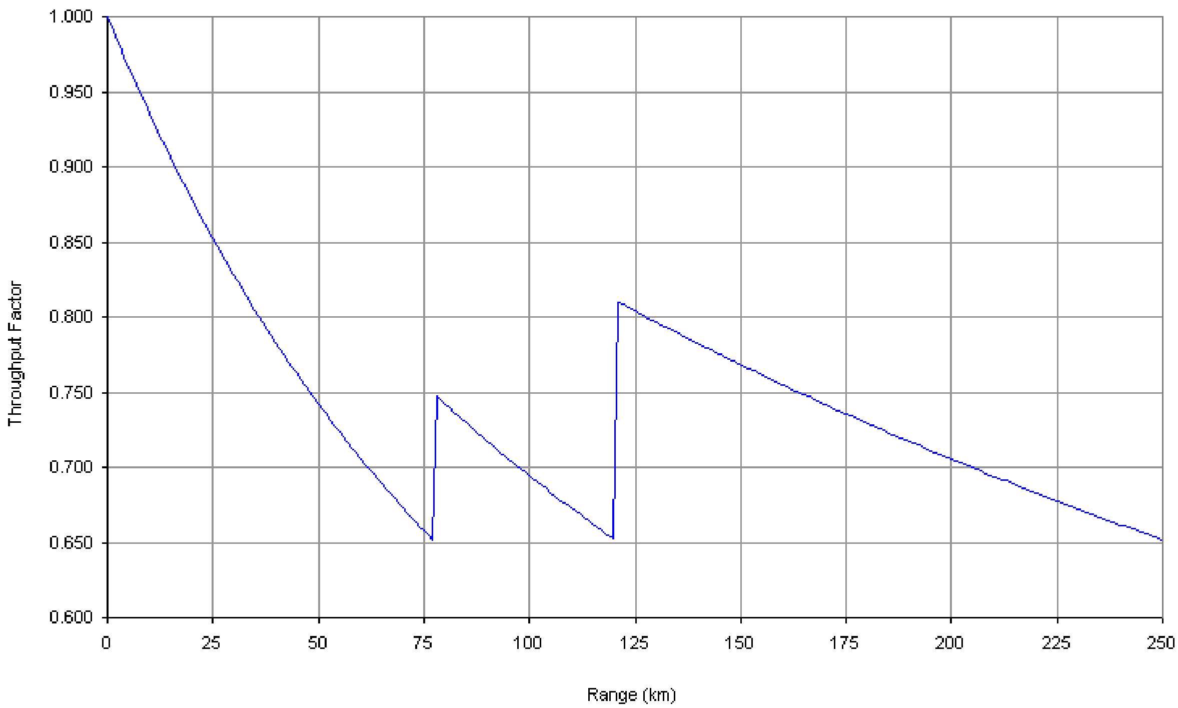


**Figure 4-8** PTP 300 and PTP 500 range adjustment for data rates, curve B



# Chapter 5 Installation

This chapter provides instructions for installing a PTP 300 or PTP 500 link.

A standard PTP 300 or PTP 500 Series installation process consists of the following tasks:



The following tasks may also be required for installation options:

# Preparing for installation

This section describes the checks to be performed before proceeding with the installation.

**NOTE**

It is common practise to pre-configure the ODUs during staging before site installation, as described in Chapter 6 Configuration and alignment.

## Precautions before installation

**CAUTION**

Apply the practices and procedures detailed in manual *R56 STANDARDS AND GUIDELINES FOR COMMUNICATION SITES (68P81089E50)* to all new site build activities.

## Preparing personnel

IN NO EVENT SHALL MOTOROLA, INC. BE LIABLE FOR ANY INJURY TO ANY PERSONS OR ANY DAMAGE CAUSED DURING THE INSTALLATION OF THE MOTOROLA PTP 500 SERIES PRODUCT.

Ensure that only qualified personnel undertake the installation of a PTP 500 Series link.

Ensure that all safety precautions can be observed.

## Preparing inventory

Perform the following inventory checks:

- Check that an installation report is available and that it is based on the principles described in Chapter 2 Planning considerations.
- Check that the correct components are available, as described in Installation inventories on page 4-2.
- Check the contents of all packages against the parts lists shown in their packing lists.

## Preparing tools

Check that following specific tools are available, in addition to general tools:

- 13mm wrench and 22 mm wrench for use with the glands.
- RJ45 crimp tool (it must be the correct tool for the type of RJ45 being used).
- Personal Computer (PC) with 100 BaseT Ethernet.
- Either Internet Explorer 7, Internet Explorer 8, Firefox 3 or Firefox 3.5.
- Ethernet patch cables.

# Preparing and using drop cable

The following procedures may be performed several times during the installation process:

- Assembling an RJ45 connector and gland on page 5-4
- Connecting an RJ45 and gland to a unit on page 5-6
- Disconnecting an RJ45 and gland from a unit on page 5-8
- Making a drop cable ground point on page 5-9

Refer back to these procedures as appropriate.

## Assembling an RJ45 connector and gland

Perform this task to prepare the outdoor CAT5e cable with connectors and glands.

The maximum permitted lengths of CAT5e cables are specified in Maximum cable lengths on page 2-7.

For details of supported cables and recommended connectors, refer to Cable and connector specifications on page 4-17.

### Safety precautions

**WARNING**

**The metal screen of the drop cable is very sharp and may cause personal injury.**

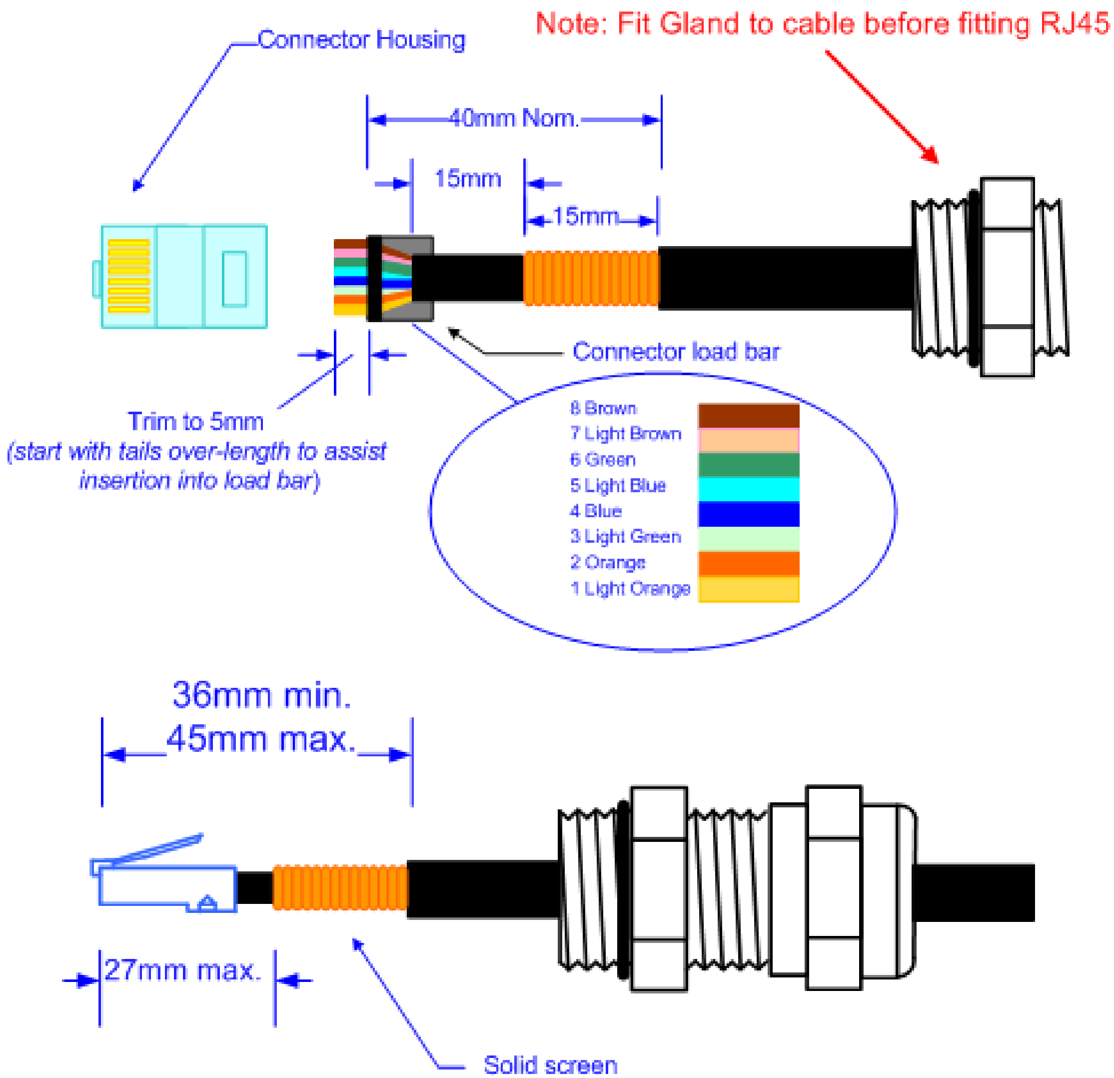
When preparing the drop cable, take the following safety precautions:

- ALWAYS wear cut resistant gloves (check the label to ensure they are cut resistant).
- ALWAYS wear protective eyewear.
- ALWAYS use a rotary blade tool to strip the cable (DO NOT use a bladed knife). To use the rotary blade tool, fit it around the outer cable sheath and rotate the cutter around the cable once or twice. The stripped outer section can then be removed.

## Assembly

Assemble the drop cable as shown in Figure 5-1. The gland is only required for outdoor connections, that it, at the ODU or LPU. The connection to the PIDU Plus requires the RJ45 plug but no gland.

**Figure 5-1** Correct cable preparation for drop cable of the supported type




**CAUTION**

Check that the crimp tool matches the RJ45 connector being used, otherwise the cable or connector may be damaged.

**CAUTION**

The cable inner sheath must be located correctly under the connector housing tang. If this is not done correctly, there is no strain relief on the cable terminations.

Figure 5-2 shows the end of a drop cable fitted with an RJ45 plug and a gland.

**Figure 5-2** Drop cable with RJ45 and gland

## Connecting an RJ45 and gland to a unit

Perform this task to connect the drop cable to an ODU or LPU. This procedure contains illustrations of an ODU, but it applies in principle to both the ODU and the LPU.

To connect the drop cable with a gland to a unit (LPU or ODU), proceed as follows:

**Procedure 5-1** Connect the drop cable with a gland to a unit (LPU or ODU)

| | |
|---|---|
| **1** | Insert the RJ45 plug into the socket in the unit, making sure that the locking tab snaps home.  |

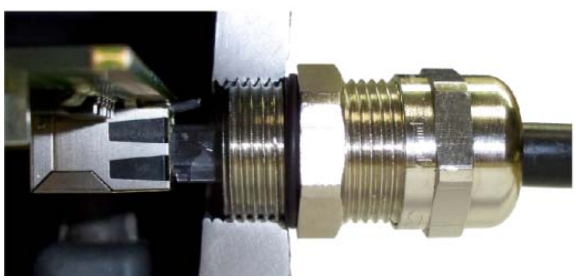
| | |
|---|---|
| **2** | Support the drop cable and gently hand screw the gland body into the unit until the O ring seal is flush to the unit body.<br><br>**NOTE**<br>Do not fit the back shell prior to securing the gland body. |
| **3** | Once the gland is fully hand screwed into the unit, tighten it with a spanner to torque 10 Nm (7.4 ftlbs).<br> |
| **4** | When the gland body has been fitted, tighten the gland back shell.<br><br>**CAUTION**<br>Do not over-tighten the gland back shell, as the internal seal and structure may be damaged. Figure 5-3 shows correctly tightened and over-tightened gland back shells. |

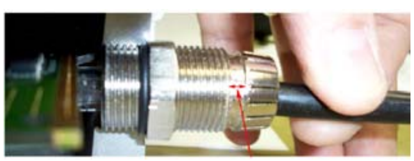
**Figure 5-3** Correct and incorrect tightening of cable gland back shell

## Disconnecting an RJ45 and gland from a unit

Perform this task to disconnect the drop cable from an ODU or LPU. This procedure contains illustrations of an ODU, but it applies in principle to both the ODU and the LPU.

To disconnect the drop cable with a gland from a unit (LPU or ODU), proceed as follows:

**Procedure 5-2** Disconnect the drop cable with a gland from a unit (LPU or ODU)

| | |
|---|---|
| **1** | Remove the gland back shell. |
| **2** | Wiggle the drop cable to release the tension of the gland body.<br><br>When the tension in the glad body is released, a gap opens at the point shown in red in the above photograph. |
| **3** | Unscrew the gland body. |

| | |
|---|---|
| **4** | Use a small screwdriver to depress the RJ45 locking cap<br> |
| **5** | Unplug the RJ45. |

## Making a drop cable ground point

Perform this task to connect the screen of the drop cable to the metal of the supporting structure using a cable grounding kit.

The cable grounding kit for 1/4” and 3/8” cable (Figure 1-12) contains the following components:

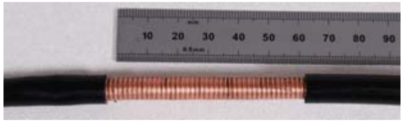
- 1 x grounding cable with grounding 2 hole lug fitted (M10)
- 1 x self Amalgamating tape
- 1 x PVC tape
- 3 x tie wraps
- 2 x bolt, washer and nut

**⚠ CAUTION**

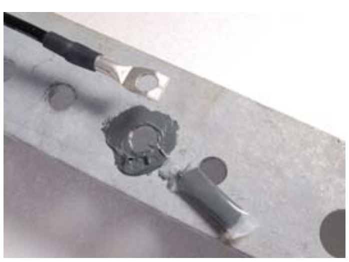
Ground cables must be installed without drip loops and pointing down towards the ground, otherwise they may not be effective.

To ground the drop cable to a metal structure, proceed as follows:

**Procedure 5-3** Ground the drop cable

| | |
|---|---|
| **1** | Remove 60mm (2.5inches) of the drop cable outer jacket.  |
| **2** | Cut 38mm (1.5 inches) of rubber tape (self amalgamating) and fit to the ground cable lug. Wrap the tape completely around the lug and cable.  |
| **3** | Fold the ground wire strap around the drop cable screen. Fit cable ties and tighten with pliers.  |

| | |
|---|---|
| **4** | Cut the surplus from the cable ties. Cut a 38mm (1.5 inches) section of self-amalgamating tape and fit to the ground cable lug. Wrap the self-amalgamating tape completely around the lug and cable.<br> |
| **5** | Use the remainder of the self-amalgamating tape to wrap the complete assembly. Press the tape edges together so that there are no gaps.<br> |
| **6** | Wrap a layer of PVC tape, starting from 25mm (1 inch) above the outer jacket and finishing 25mm (1 inch) below the self-amalgamating tape, over lapping at half width.<br> |

| | |
|---|---|
| **7** | Repeat with a further four layers of PVC tape.<br>Start the second layer 25mm (1 inch) above the first layer tape, start the third layer below the finish of the second layer. Continue until five layers have been applied, always over lapping at half width.<br> |
| **8** | If a single hole tag is required at the mast end, modify the two hole tag as shown.<br> |
| **9** | Apply the anti-oxidant compound liberally applied between the two metals.<br>If paint is present, remove it to provide a good electrical contact.<br> |

# Installing the ODU

Perform this task to install the ODU (integrated or connectorized) on the supporting structure.

This task consists of the following procedures:


- Checks and safety precautions on page 5-13
- Selecting a position for the ODU (connectorized) on page 5-15
- Mounting the ODU on page 5-15


If a connectorized ODU is being installed, see also:


- Installing connectorized antennas on page 5-17


## Checks and safety precautions

**WARNING**

**To prevent failure of the assembly, do not remove the mounting bracket, and do not mount the ODU on a pole that is too narrow or too wide.**

**WARNING**

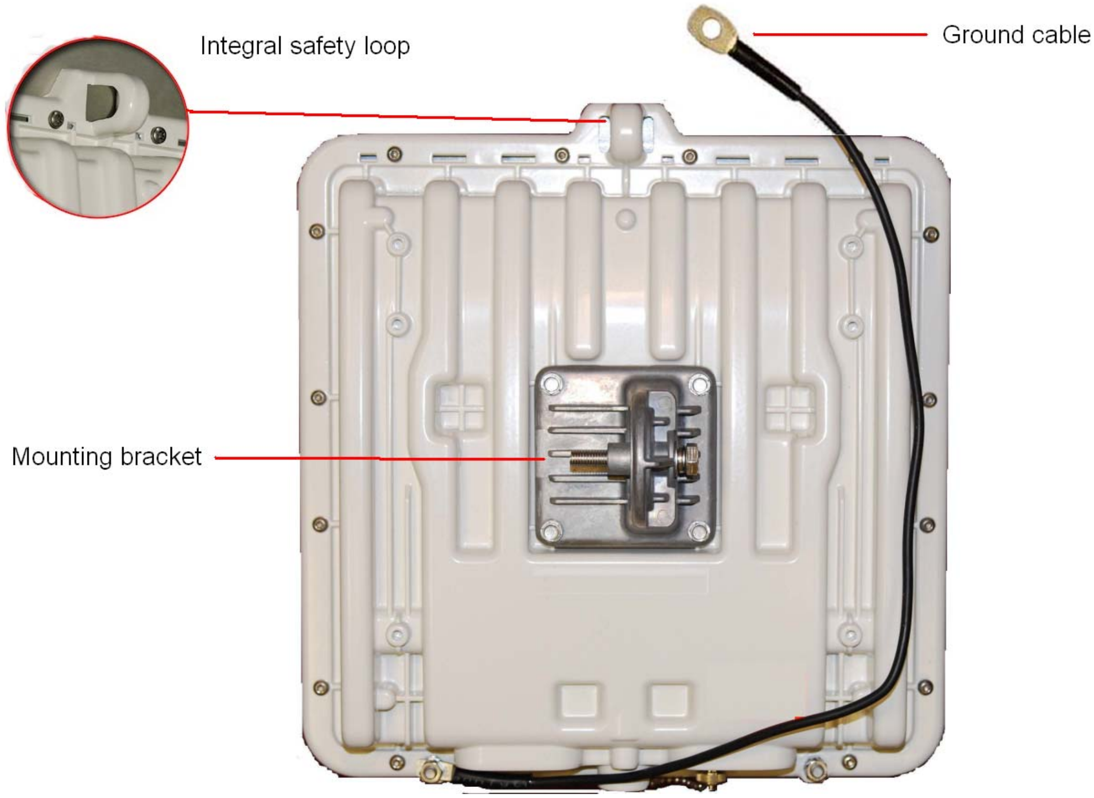
**To minimize the risk of injury, do not attempt to hoist the ODU until the necessary precautions have been taken.**

**WARNING**

**To prevent failure of the assembly, do not over-tighten the bolts.**

Check that the ODU is pre-fitted with a mounting bracket (designed to ease installation) and with a ground cable (Figure 5-4).

**Figure 5-4** Checking the ODU before mounting




Do not mount the ODU on poles with diameter less than 50mm (2”) or greater than 75mm (3”). The ODU mounting bracket is designed to work only with poles with diameter in the 50 mm (2”) to 75 mm (3”) range.

Before hoisting the ODU, take the following precautions:

- Check that the safety loop (Figure 5-4) and its fixing are not damaged in any way and have not been exposed to a shock loading due to a fall.
- Check that the safety lanyard does not exceed 1m (approx 3 ft) in length.
- Check that the safety lanyard is made from a material that does not degrade in an outdoor environment.
- Check that the safety lanyard is fixed to a separate point that is not part of the direct mounting system for the ODU.

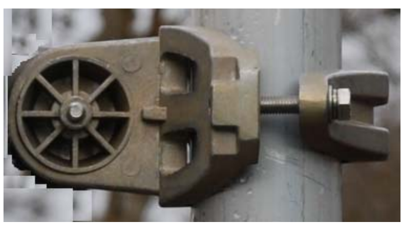
## Selecting a position for the ODU (connectorized)

If the ODU is connectorized, select a mounting position that gives it maximum protection from the elements, but still allows easy access for connecting and weatherproofing the cables. To minimize cable losses, select a position where the antenna cable lengths can be minimized. If separate antennas are being deployed, it is not necessary to mount the ODU at the mid point between the antennas.

## Mounting the ODU

To mount the ODU, proceed as follows:

**Procedure 5-4** Mounting the ODU

| | |
|---|---|
| **1** | Attach the ODU bracket strap to the pole using M8 x 70 mm bolts, M8 flat washers and M8 coil washers.  Tighten to ensure the assembly grips, but can be adjusted on the pole. |
| **2** | Use the integral safety loop (Figure 5-4) to hoist the ODU up to the bracket, observing the precautions described in Checks and safety precautions on page 5-13. |
| **3** | When the ODU is in position, use the safety loop as a fixing point to secure a permanent lanyard from the supporting structure to the ODU, as a precaution against mounting failure. |

| | |
|---|---|
| **4** | Offer the ODU (with pre-fitted mounting bracket) to the bracket strap and affix using the captive M8 bolt. Tighten to ensure the assembly grips, but can be adjusted on the pole.<br> |
| **5** | Adjust the elevation and azimuth of the unit to achieve an approximate visual alignment (does not apply to connectorized ODUs). Tighten both nuts to the required torque settings of 14 Nm (11 lb ft). |
| **6** | Connect the ODU ground cable to the to the supporting structure grounding point, within 0.3 meters (1 ft) of the ODU bracket and on the same metal (if necessary, remove paint and apply anti-oxidant compound first).<br>**CAUTION**<br>Do not attach grounding cables to the ODU mounting bracket bolts, as this arrangement will not provide full protection. |
| **7** | To prevent corrosion and possible loss of ground continuity, weatherproof the grounding point. |

# Installing connectorized antennas

If the ODU is connectorized, perform this task to install separate antenna(s).

## Preparing for connectorized installations

Before proceeding with the installation, perform the following checks:

- Check that the correct components are available, as described in Installation inventories on page 4-2.
- Check that the selected antenna conforms to the applicable regulatory restrictions, as described in Antenna specifications on page 4-19 and Electromagnetic compliance on page 4-58.
- Check that the correct tools are available. The tools required for mounting the antennas are specific to the antenna chosen. Refer to the antenna manufacturer's instructions.

## Mounting and connecting antennas

To mount and connect the antenna(s), proceed as follows:

**Procedure 5-5** Mount and connect antenna(s)

| | |
|---|---|
| **1** | Mount the antenna(s) according to manufacturer's instructions. When using separate antennas to achieve spatial diversity, mount one with Horizontal polarization and the other with Vertical polarization. |
| **2** | Connect the ODU to the antenna with cables of type LMR100, LMR200, LMR300, LMR400 or LMR600. Use the ODU 'V' interface for vertical polarization and the 'H interface for horizontal polarization (Figure 1-5).<br>**NOTE**<br>When using separate antennas to achieve spatial diversity, the antenna cables will be disconnected from the ODU during the alignment procedure. Therefore, do not weatherproof the ODU joints until antenna alignment is complete. |
| **3** | Where the ODU is mounted indoors, install lightning arrestors at the building entry point (Figure 5-5). Assemble the Polyphaser LSXL-ME or LSXL as shown in Figure 5-6. Connect the lighting arrestors to the master ground bar of the building. |

| | |
|---|---|
| **4** | When dressing the antenna cables, form drip loops near the lower ends (Figure 5-7). These ensure that water is not constantly channeled towards the connectors. |
| **5** | Weatherproof the ODU joints using self-amalgamating tape under a layer of PVC tape (Figure 5-8). Weatherproof the antenna joints in the same way (unless the antenna manufacturer specifies a different method). |
| **6** | Ground the antenna cables to the supporting structure at the correct points (Figure 5-9).<br>**NOTE**<br>A mast or tower may require additional grounding points, as specified in Protection requirements for a mast or tower installation on page 2-17. |
| **7** | Dress the antenna cables and fix them using cable ties, cleats or PVC tape.<br>**CAUTION**<br>Ensure that no undue strain is placed on the ODU or antenna connectors. Ensure that the cables do not flap in the wind, as flapping cables are prone to damage and induce unwanted vibrations in the supporting structure. |

**Figure 5-5** Lightning arrestor mounting

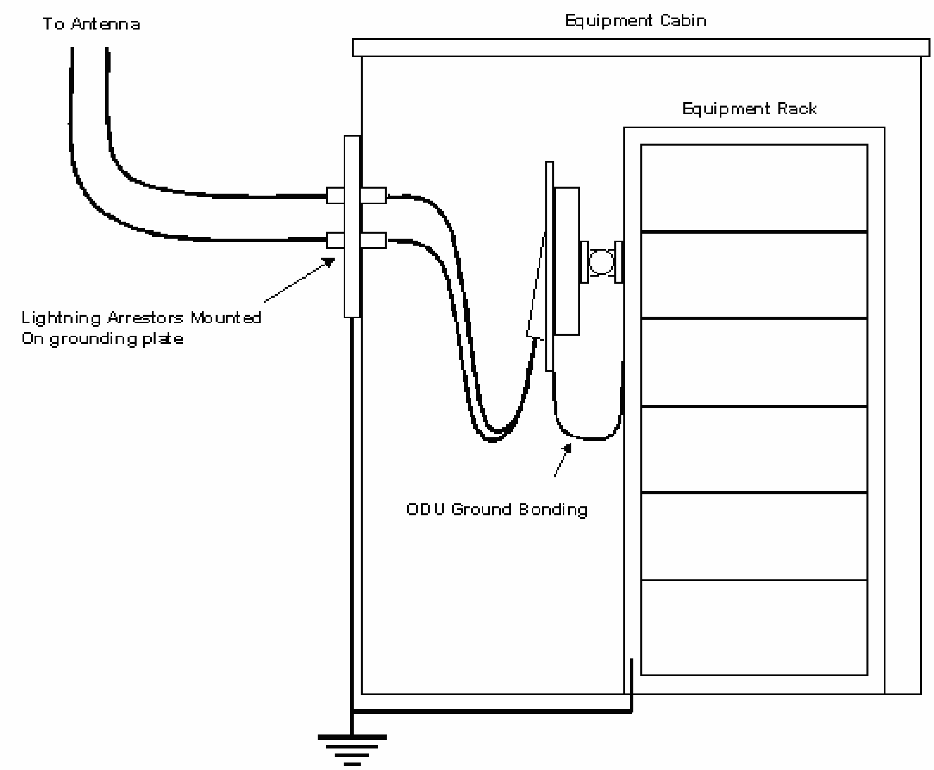



**Figure 5-6** Polyphaser assembly

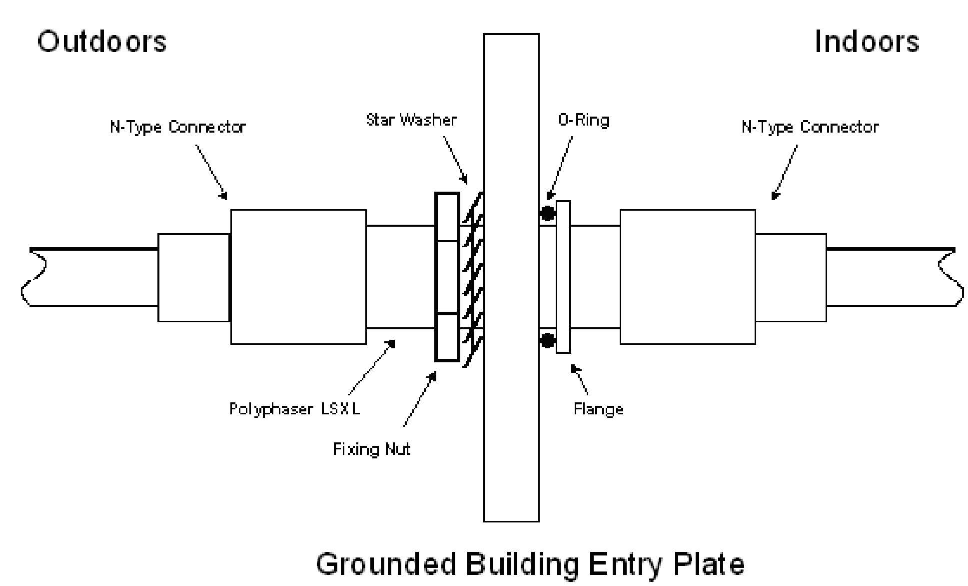


**Figure 5-7** Forming a drip loop

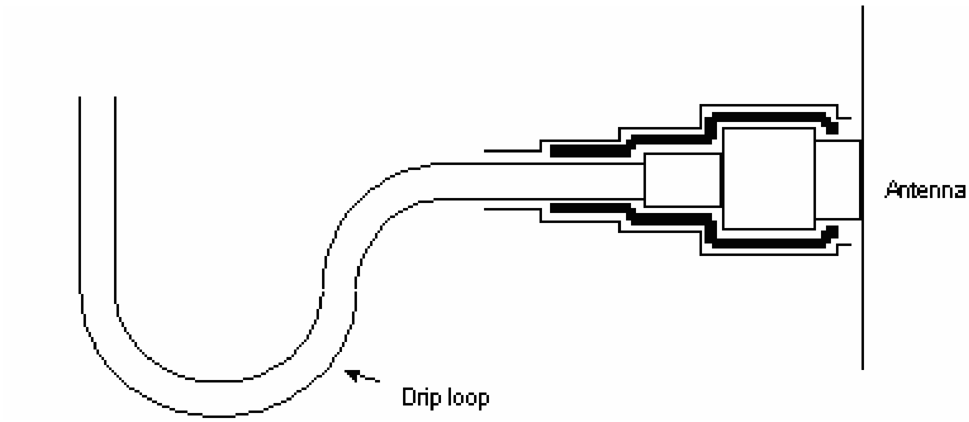



**Figure 5-8** Weatherproofing the antenna connections

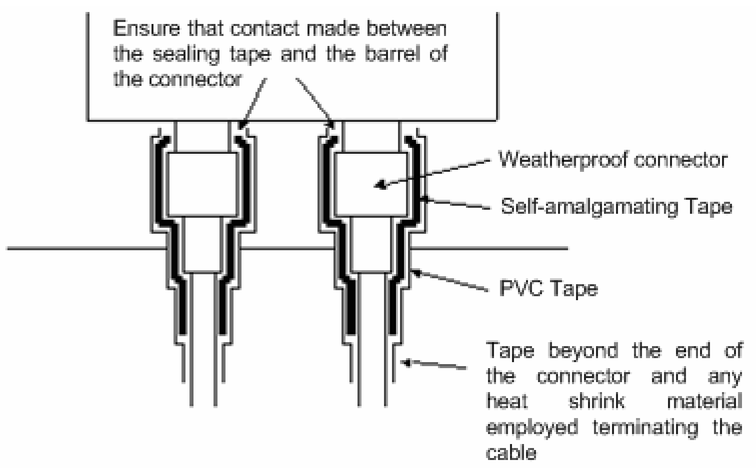
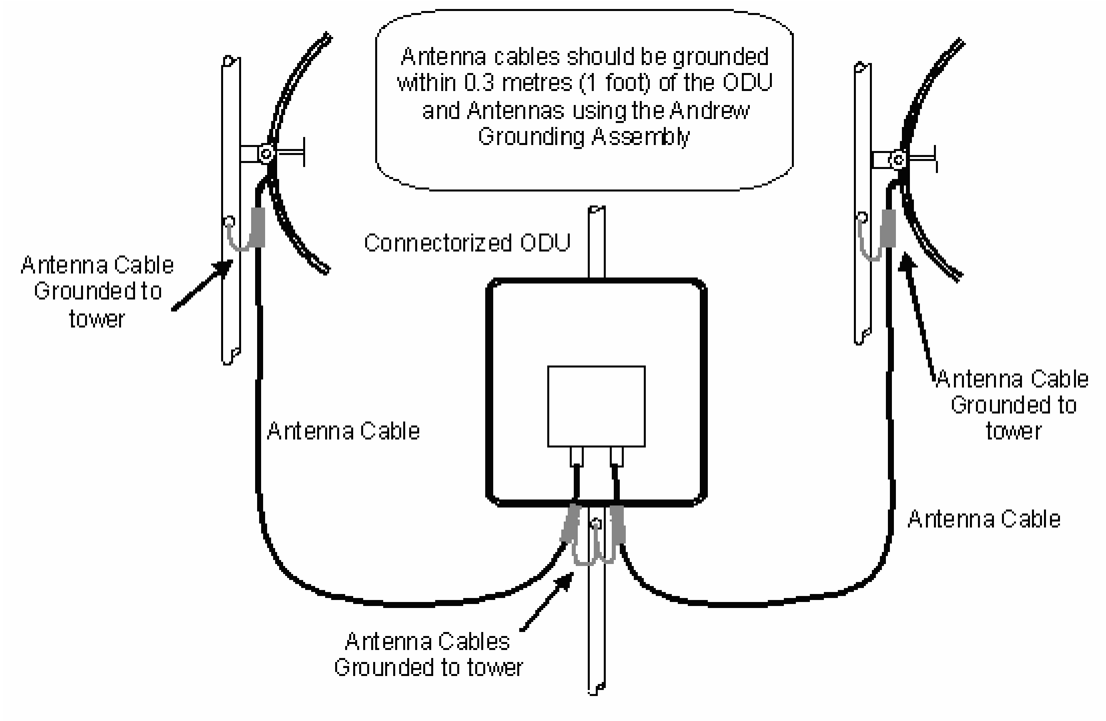


**Figure 5-9** Grounding points for antenna cables



# Installing the drop cable and LPU

Perform this task to install the drop cable from the ODU to the PIDU Plus, and to provide grounding and lightning protection for the installation.

This task consists of the following procedures:

- Installing the long drop cable on page 5-23.
- Installing and connecting the LPU on page 5-24.

**CAUTION**

The drop cable and ground cable installation must meet the requirements defined in Grounding and lightning protection on page 2-14.

**CAUTION**

To provide effective protection against lightning induced surges, grounding cables must be installed without drip loops and pointing down towards the ground.

**CAUTION**

To avoid damage to the installation, do not connect or disconnect the drop cable when power is applied to the PIDU Plus.

# Installing the long drop cable

Perform this procedure to install the long drop cable, connect it to the ODU, and ground it to the supporting structure.

To install the long drop cable, proceed as follows:

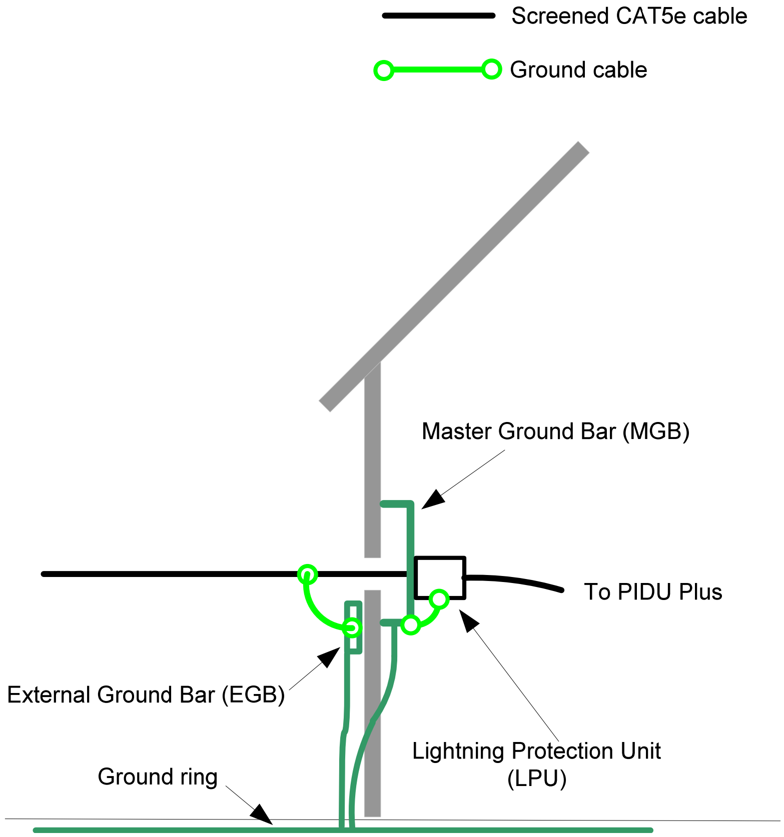
**Procedure 5-6** Install long drop cable

| | |
|---|---|
| **1** | Cut a section of drop cable long enough to run from the ODU down the supporting structure to the site of the LPU at building entry point. |
| **2** | Fit a connector and gland to the top end of the long drop cable, as described in Assembling an RJ45 connector and gland on page 5-4. |
| **3** | Connect the top end of the long drop cable to the ODU (PIDU+ port), as described in Connecting an RJ45 and gland to a unit on page 5-6.  |
| **4** | Lay the long drop cable down the supporting structure, through the building entry point to the site of the LPU. |
| **5** | Ground the drop cable to the supporting structure at the points shown in Figure 2-3 (mast or tower installation) or Figure 2-4 (wall installation), as described in Making a drop cable ground point on page 5-9. **NOTE** A mast or tower may require additional grounding points, as specified in Protection requirements for a mast or tower installation on page 2-17. |
| **6** | Ground the drop cable to the external ground bar outside the building entry point, as described in Making a drop cable ground point on page 5-9. |
| **7** | Secure the drop cable to the supporting structure using cable ties or cleats. |

# Installing and connecting the LPU

Perform this procedure to install and ground the LPU and connect it to the drop cables at the building (or cabinet) entry point (Figure 5-10).

**Figure 5-10** Grounding at building entry



To install and connect the LPU, proceed as follows:

**Procedure 5-7** Install the LPU at building entry

| | |
|---|---|
| **1** | Install the LPU inside the building entry point. Mount the LPU vertically with cable glands facing downwards. |
| **2** | Ground the LPU to the master ground bar. |
| **3** | Fit a connector and gland to the bottom end of the long drop cable, as described in Assembling an RJ45 connector and gland on page 5-4. |
| **4** | Connect the long drop cable to the LPU, as described in Connecting an RJ45 and gland to a unit on page 5-6. |
| **5** | Cut a section of drop cable long enough to run from the LPU to the PIDU Plus (or PTP-SYNC if installed). |
| **6** | Fit a connector and gland to the LPU end of the short drop cable, as described in Assembling an RJ45 connector and gland on page 5-4. Fit a connector (but no gland) to the PIDU Plus (or PTP-SYNC) end. |
| **7** | Connect the short drop cable to the LPU and run it to the site of the PIDU Plus or PTP-SYNC (if installed). |

**NOTE**

If it is necessary to disconnect the drop cable, refer to Disconnecting an RJ45 and gland from a unit on page 5-8.

# Installing the PIDU Plus

Perform this task to install the PIDU Plus and connect it to the ODU and network cables.

This task consists of the following procedures:

- Mounting the PIDU Plus on page 5-26
- Connecting the PIDU Plus to the ODU cable on page 5-26
- Preparing the PIDU Plus to LAN cable on page 5-28

## Mounting the PIDU Plus

Mount the PIDU Plus on a wall or other suitable mounting surface, at a height that protects it from flooding or rising damp.

Mount it using the lugs provided, as this prevents the unit from being knocked or kicked and can help maintain link availability.

Ensure that the Recovery switch can be accessed when mounting the unit.

**⚠ CAUTION**

The PIDU Plus is not waterproof and should be mounted away from sources of moisture. If mounted outdoors, the unit should be mounted in a rain proof enclosure, preferably ventilated.

## Connecting the PIDU Plus to the ODU cable

The cable from the ODU is connected to the PIDU Plus by means of a concealed RJ45 socket.

**⚠ CAUTION**

Plugging other equipment into the ODU RJ45 socket may damage the equipment due to the non-standard techniques employed to inject DC power into the 100BaseT connection between the PIDU Plus and the ODU. Plugging the ODU into other equipment may damage the ODU and/or the other equipment.

**⚠ CAUTION**

Do not dress the PIDU Plus cables too tightly, as this may make the connections unreliable.

**⚠ CAUTION**

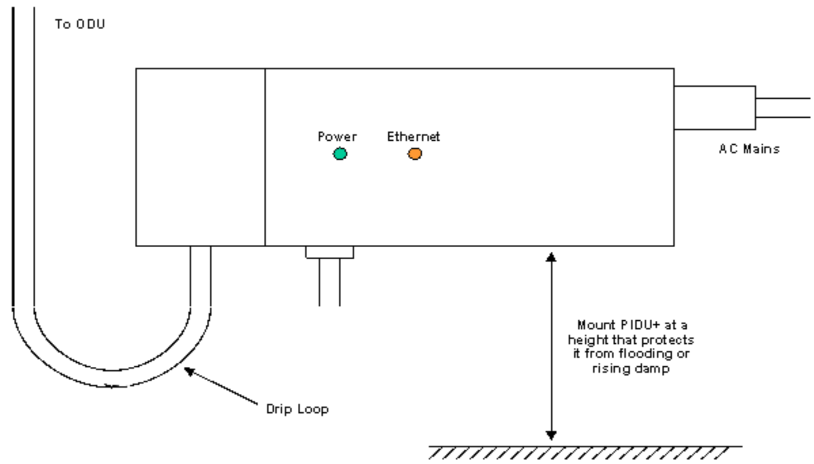
The connected network equipment must feature screened RJ45 connectors and must be connected to ground, otherwise the PIDU Plus will not be grounded.

To connect the PIDU Plus to the cable from the ODU, proceed as follows:

**Procedure 5-8** Connecting the PIDU Plus to the ODU

| | |
|---|---|
| **1** | Undo the retaining screw and hinge back the cover.   |
| **2** | Plug in the cable from the LPU (or PTP-SYNC if installed), ensuring that it snaps home.   |
| **3** | Replace the cover and secure with the retaining screw.   |

| | |
|---|---|
| **4** | Form a drip loop on the cable from the LPU. This ensures that any moisture that runs down the cable into the cabinet or enclosure cannot enter the PIDU Plus. The network connection and mains cable should be treated in the same way if there is a risk that they can carry moisture to the PIDU Plus. |




## Preparing the PIDU Plus to LAN cable

Prepare the CAT5e cable that will connect the PIDU Plus to the network equipment. This cable must meet the following requirements:

- Use either foil screen (FTP) or braided screen (STP) cable.
- Use screened RJ45 connectors with metal shells at both ends.
- Ensure there is a continuous electrical connection between both screened connectors.

The PIDU Plus is not normally connected to the network equipment until antenna alignment is complete. See Task 13: Connecting link to the network on page 6-56.

# Installing a PTP-SYNC unit

If the chosen TDD synchronization method for PTP 500 requires PTP-SYNC (see TDD synchronization configurations supported on page 2-25), then perform this task to install a PTP-SYNC unit.

This task consists of the following procedures:


- Preparing for PTP-SYNC installation on page 5-29
- Mounting the PTP-SYNC unit on page 5-30
- Connecting up the PTP-SYNC unit on page 5-31
- Powering up the PTP-SYNC installation on page 5-33


**⚠ CAUTION**

The PTP-SYNC unit should not be installed in a domestic (home) environment as it is a Class A product. In a domestic environment, it may cause radio frequency (RF) interference in other appliances.

**⚠ CAUTION**

The PTP-SYNC unit must be installed indoors in a non-condensing environment, otherwise it will be prone to water damage.

**⚠ CAUTION**

To protect the PTP-SYNC from damage, disconnect the power supply from the PIDU Plus before connecting up the PTP-SYNC.

## Preparing for PTP-SYNC installation

Check that the correct components are available, as described in Installation inventories on page 4-2.

# Mounting the PTP-SYNC unit

Install the PTP-SYNC unit in the equipment building, either in a rack or on a wall.

## Rack mounting

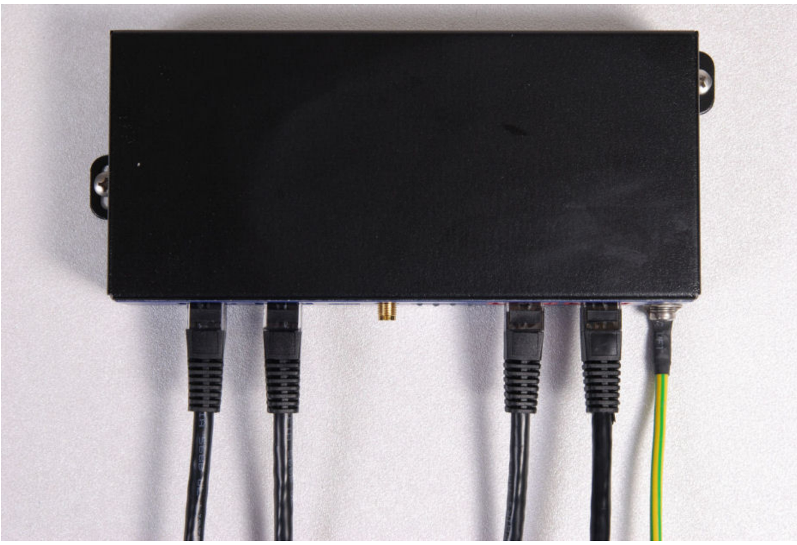
If the PTP-SYNC is to be in a rack, fix it to the rack mount using the M3 screws from the rack mount installation kit (Figure 5-11).

**Figure 5-11** Rack mount securing screws for PTP-SYNC


## Wall mounting

If the PTP-SYNC is to be on a wall, mount it vertically with interfaces and cabling facing downwards (Figure 5-12).

**Figure 5-12** PTP-SYNC mounted on a wall



## Connecting up the PTP-SYNC unit

To connect the PTP-SYNC to the PIDU Plus, ODU, GPS receiver (if fitted), and LPU (if fitted), proceed as follows:

**Procedure 5-9** Connect up PTP-SYNC

| | |
|---|---|
| **1** | Disconnect the power supply from the PIDU Plus.   |
| **2** | If using GPS, connect the cable from the GPS unit to the GPS/SYNC IN port.   |

**3** To link clustered PTP-SYNC units, connect the SYNC OUT port of the first PTP-SYNC to the GPS/SYNC IN port of the second PTP-SYNC in the chain. Repeat for subsequent PTP-SYNC units in the chain.

**4** Connect the cable from the PIDU Plus to the PIDU IN port.


**5** Connect the cable from the ODU to the ODU OUT port.

| | |
|---|---|
| **6** | Use a grounding cable to connect the ground stud of the PTP-SYNC to the master ground bar of the building.<br><br> |

## Powering up the PTP-SYNC installation

To power up the installation, proceed as follows:

**Procedure 5-10** Powering up PTP-SYNC

| | |
|---|---|
| **1** | Ensure that all cables are connected to the correct interfaces of the PTP-SYNC unit and the GPS receiver (if used). Ensure that the installation is correctly grounded.<br>⚠ CAUTION<br>Failure to do so may result in damage to the equipment. |
| **2** | Connect the power supply to the PIDU Plus. |
| **3** | Within 90 seconds, the PTP-SYNC ’STATUS’ LED should blink once every second to show that satellite lock has been achieved. |
| **4** | If the system does not operate correctly, refer to Testing PTP-SYNC on page 8-17. |

# Installing a GPS receiver for PTP-SYNC

If the chosen TDD synchronization method for PTP 500 requires a GPS timing reference source (see TDD synchronization configurations supported on page 2-25), then perform this task to install a GPS receiver.

This task consists of the following procedures:

- Preparing for GPS receiver installation on page 5-34
- Mounting the GPS receiver on page 5-34
- Connecting the drop cable to the GPS receiver on page 5-35
- Grounding the GPS receiver drop cable on page 5-39
- Mounting the LPU and connecting the GPS receiver on page 5-40

**⚠ CAUTION**

Prior to power-up of equipment, ensure that all cables are connected to the correct interfaces of the PTP-SYNC unit and the GPS receiver module. Failure to do so may result in damage to the equipment.

## Preparing for GPS receiver installation

Check that the correct components are available, as described in Installation inventories on page 4-2.

## Mounting the GPS receiver

Mount the GPS receiver (following manufacturer's instructions) upon either an external wall or a metal tower or mast. For more information on these options, refer to Mounting options for the PTP-SYNC GPS receiver on page 2-29.

## Connecting the drop cable to the GPS receiver

If the chosen GPS receiver is Trimble Acutime™ Gold, then follow this procedure.

The drop cable connecting the Trimble GPS receiver to the LPU must be of the supported cable type. The drop cable must have a Trimble 12-pin connector at the GPS end (supplied in the Trimble kit), and an RJ45 connector and standard gland at the LPU end.

⚠ **CAUTION**

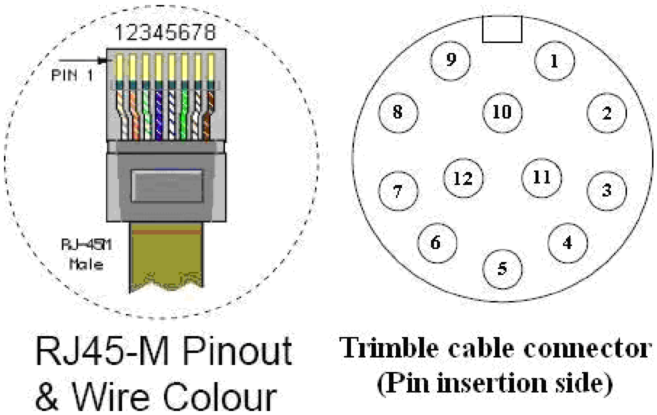
The drop cable has solid copper conductors. There is a limited number of times each conductor can be bent before it fatigues and fails.

Table 5-1 shows how the Trimble connector pins (at the GPS end of the drop cable) map to the RJ45 connector pins (at the LPU end). Figure 5-13 shows the positions of the pins in each type of connector.

**Table 5-1** Trimble connector to RJ45 pin mappings

| Trimble 12-pin conn | Function | RJ45 wire color | | PTP-SYNC (J10) RJ45 pin |
|---|---|---|---|---|
| | | Conventional | Supported drop cable | |
| 1 | DC Pwr (12V) | Orange/White | Light Orange | 1 |
| 2 | RxB- | Brown/White | Light Brown | 7 |
| 3 | RxB+ | Brown | Brown | 8 |
| 4 | TxB- | Blue | Blue | 4 |
| 5 | TxB+ | Blue/White | Light Blue | 5 |
| 6 | RxA- | N.C | N.C | --- |
| 7 | RxA+ | N.C | N.C | --- |
| 8 | TxA- | N.C | N.C | --- |
| 9 | DC Ground | Orange | Orange | 2 |
| 10 | TxA+ | N.C | N.C | --- |
| 11 | Tx1PPS+ | Green/White | Light Green | 3 |
| 12 | Tx1PPS- | Green | Green | 6 |

**Figure 5-13** RJ45 and Trimble connector pins




To connect the drop cable to the Trimble GPS receiver, proceed as follows:

**Procedure 5-11** Connect drop cable to Trimble GPS receiver

| | |
|---|---|
| **1** | Prepare the drop cable end as follows:<br>Bare back the cable outer and copper screen to 50mm.<br>Bare back the cable inner to 17mm.<br>Un-twist the cable pairs.<br>Strip the individual conductors to 5mm.<br> |
| **2** | Fit the adaptor outer, associated boot, and boot insert.<br> |

**3** Connect the socket contacts using either of the following techniques:

**Crimp**

Crimp the socket contacts onto each of the conductors using the correct crimp tool and positioner, setting the wire size selector to ‘3’ for 24AWG wire.


**Solder**

When soldering the socket contacts onto each of the conductors, ensure that there is no solder or flux residue on the outside of the contact. Care should also be taken that the individual conductor insulation does not peel back with the soldering heat, allowing possible shorts when assembled into the connector shell.

**4** Fit four contacts into the unused locations, to provide strength and sealing.

Pin insert side:

Connector mating side:

**5** Insert the eight contacts into the connector body in accordance with Table 5-1. It is easiest to insert the pins from the inside out, in the order 12, 11, 9, 5, 4, 3, 2, 1. Push the contacts in so that the shoulder on the contact fits into the hole in the connector shell. When all contacts have been fitted, push them in further to engage with the locking mechanism in the connector shell. This can be done by applying pressure to the contact with a small diameter stiff object, such as tweezers.

If a contact is pushed in to the point where the locking mechanism engages before all of the contacts have been inserted it will limit the amount of room available to fit the remaining contacts, requiring harder bends to be applied.

**6** Fit the adaptor to the connector shell. The plastic ring fits inside the rubber boot and ensures a tight fit when the adaptor body is clipped onto the connector shell. Be aware that the adaptor body is a hard push fit onto the connector shell.

**7** Fit the strain relief clip.

**8** Connect the adapter to the GPS, then wrap a layer of self-amalgamating tape, starting 25mm below the bared back outer of the cable and finishing at the GPS housing.

| | |
|---|---|
| **9** | Wrap a layer of PVC tape, starting just below the start of the self-amalgamating tape and finishing at the GPS housing, overlapping at half width.<br>Repeat with a further four layers of PVC tape alternating the start and finish ends.<br> |

## Grounding the GPS receiver drop cable

For installations where the GPS receiver module is fitted to a metal tower or mast, ground bond the GPS receiver drop cable to the tower or mast. To identify the required grounding points, refer to Mounting the GPS receiver module on a metal tower or mast on page 2-31.

To ground the cable, follow the procedure described in Making a drop cable ground point on page 5-9.

## Mounting the LPU and connecting the GPS receiver

To mount the LPU and connect it to the drop cable from the GPS receiver, proceed as follows:

**Procedure 5-12** Mount LPU and connect to GPS receiver

| | |
|---|---|
| **1** | Check the contents of the LPU box. |
| **2** | Mount the LPU (following manufacturer's instructions) at the point where the drop cable from the GPS receiver enters the building (Figure 2-12 or Figure 2-13). Mount the LPU vertically with cable glands facing downwards. Ground the LPU. |
| **3** | Prepare the LPU end of the GPS receiver drop cable as described in Assembling an RJ45 connector and gland on page 5-4. |
| **4** | Connect the cable gland of the GPS receiver drop cable to the LPU as described in Connecting an RJ45 and gland to a unit on page 5-6. |
| **5** | Lay the drop cable from the LPU into the building up to the PTP-SYNC mounting point. |

# Installing an E1 or T1 interface

Perform this task to install an optional E1 or T1 interface.

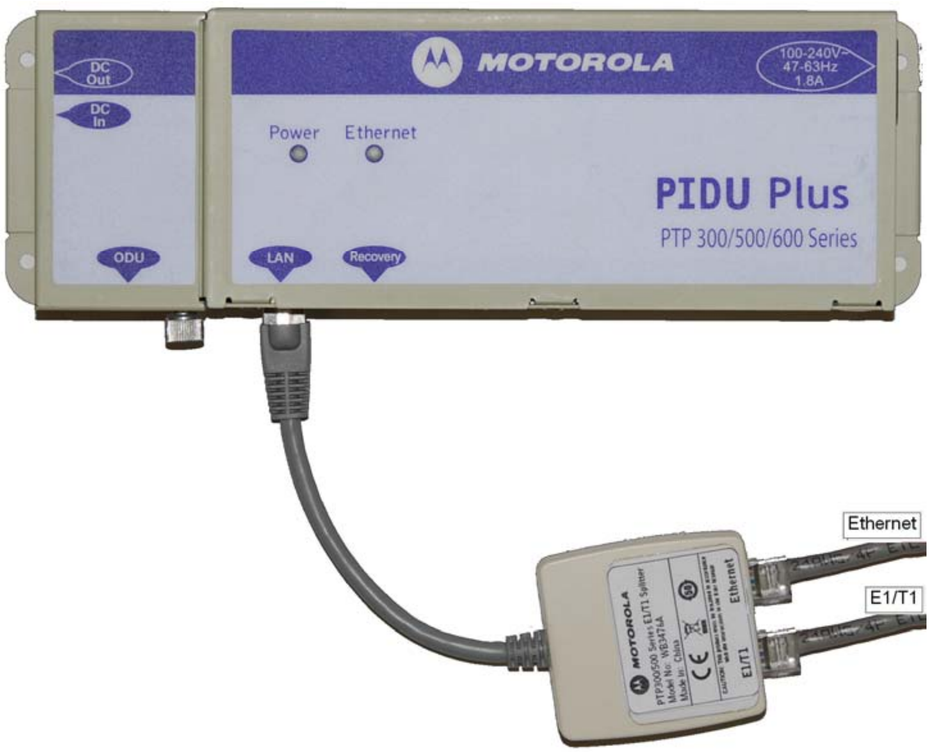
This task consists of the following procedures:

- Connecting the E1/T1 cable to the PIDU Plus on page 5-41
- Testing the E1/T1 installation on page 5-42

## Connecting the E1/T1 cable to the PIDU Plus

The E1/T1 cable and the Ethernet cable share the LAN port of the PIDU Plus. They are connected via the PTP 300/500 Series E1/T1 Splitter (Figure 5-14).

**Figure 5-14** E1/T1 splitter



The E1/T1 splitter output pin connections are specified in Table 5-2.

**Table 5-2** E1/T1 splitter output pin connections

| Port | Pin Number | Connection |
|---|---|---|
| Ethernet | 1 | Rx1 |
| | 2 | Rx2 |
| | 3 | Tx1 |
| | 4 | |
| | 5 | |
| | 6 | Tx2 |
| | 7 | |
| | 8 | |
| E1/T1 | 1 | Rx Ring |
| | 2 | Rx Tip |
| | 3 | |
| | 4 | Tx Ring |
| | 5 | Tx Tip |
| | 6 | |
| | 7 | |
| | 8 | |

# Testing the E1/T1 installation

Test the telecoms links by performing loopback connection tests as described in Testing a telecoms link on page 8-19.

# Chapter 6 Configuration and alignment

This chapter describes all configuration and alignment tasks that are performed when a PTP 300 or PTP 500 link is deployed.

The following tasks are usually performed during staging before site installation:



**CAUTION**

USA only: if the system designer has provided a list of channels to be barred for TDWR radar avoidance, the affected channels must be barred during staging, before the units are allowed to radiate on site, otherwise FCC rules will be infringed.

The following tasks are always performed after installation is complete at both sites:



The following tasks may be performed during staging or after installation:

# Task 1: Connecting to the unit

This task consists of the following procedures:


- Configuring the management PC on page 6-2
- Connecting to the PC and powering up on page 6-4
- Logging into the web interface on page 6-4


## Configuring the management PC

To configure the local management PC to communicate with the PTP 300 or PTP 500, proceed as follows:

**Procedure 6-1** Configure the IP interface on the PC

| | |
|---|---|
| **1** | Select **Properties** for the Ethernet port. |
| **2** | Select the Internet Protocol (TCP/IP) item as shown in Figure 6-1. |
| **3** | Click on **Properties**. |
| **4** | Enter an IP address that is valid for the 169.254.X.X network, avoiding:<br>169.254.0.0 and 169.254.1.1 and 169.254.1.2<br>A good example is 169.254.1.3 as shown in Figure 6-2. |
| **5** | Enter a subnet mask of 255.255.0.0.<br>Leave the default gateway blank. |

**Figure 6-1** IP configuration on the PC

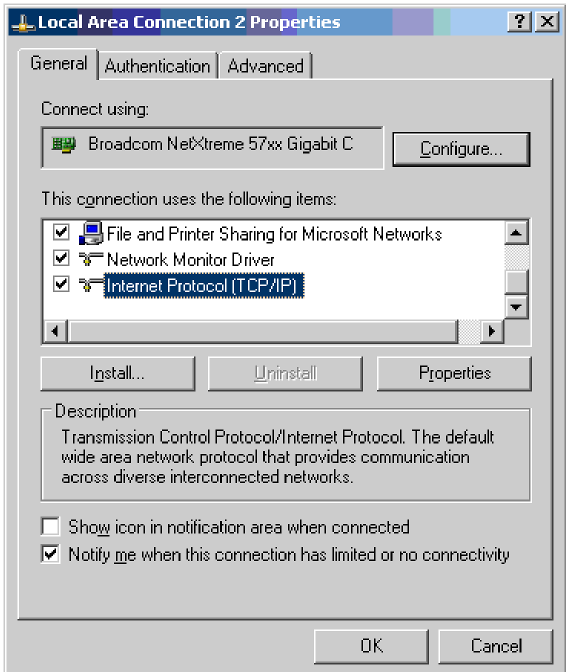
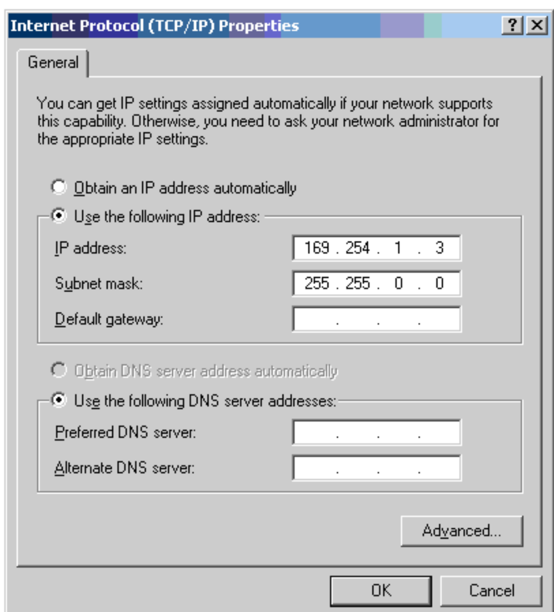



**Figure 6-2** Internet Protocol (TCP/IP) Properties page



## Connecting to the PC and powering up

To connect the ODU to the PC and power up the unit, proceed as follows:

**Procedure 6-2** Power up and log into the unit

| | |
|---|---|
| **1** | Check that the ODU and PIDU Plus are correctly connected. |
| **2** | Connect the PC Ethernet port to the LAN port of the PIDU Plus using a standard (not crossed) Ethernet cable. |
| **3** | Apply mains or battery power to the PIDU Plus. The green Power LED should illuminate continuously. |
| **4** | After about 45 seconds, check that the orange Ethernet LED starts with 10 slow flashes. |
| **5** | Check that the Ethernet LED then illuminates continuously. |

**NOTE**

If the Power and Ethernet LEDs do not illuminate correctly, refer to Testing link end hardware on page 8-2.

## Logging into the web interface

**NOTE**

If a PTP 300 or PTP 500 link has been purchased, one unit will be factory configured as a Master unit with an IP address of 169.254.1.2. The other unit will be factory configured as a Slave unit with an IP address of 169.254.1.1.

If a single PTP 300 or PTP 500 unit has been purchased, it will be factory configured as a Slave unit with an IP address of 169.254.1.1.

To log into the web interface as a system administrator, proceed as follows:

**Procedure 6-3** Log into the unit

| | |
|---|---|
| **1** | Start the web browser from the management PC. |
| **2** | Type the IP address of the unit into the address bar. The factory default IP address will be either 169.254.1.1 or 169.254.1.2. Press ENTER. The web interface menu and System Summary page are displayed (Figure 6-3). |
| **3** | Select menu option **System Administration**. The login page is displayed (Figure 6-4). |
| **4** | Leave the Password blank and select **Login**. |
| **5** | Check that the PIDU Plus Ethernet LED blinks randomly as traffic passes through. If it does not illuminate correctly, refer to Testing link end hardware on page 8-2. |

**Figure 6-3** Menu and System Summary page

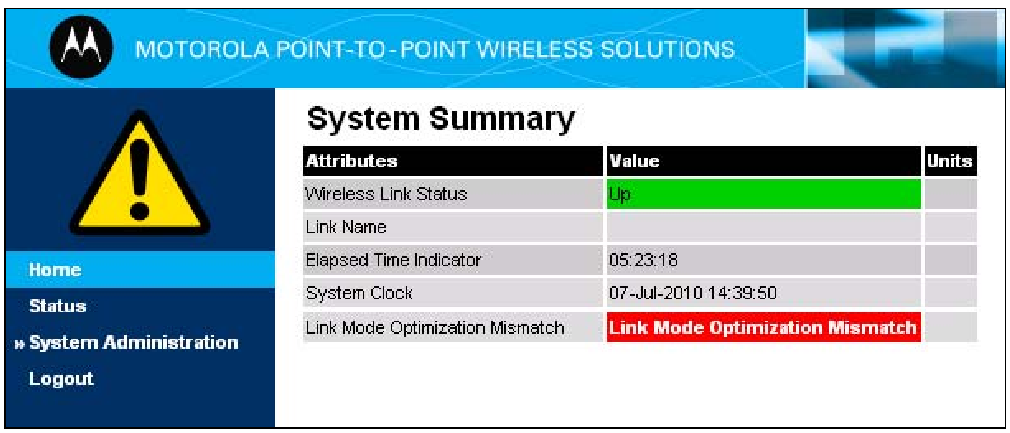
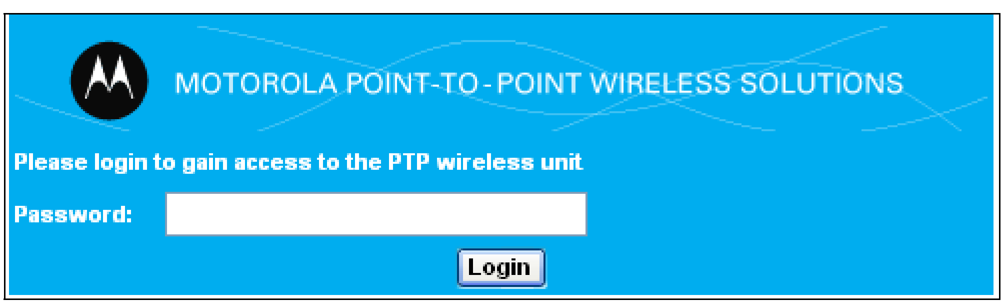



**Figure 6-4** Login page



# Task 2: Configuring IP and Ethernet interfaces

This task consists of the following procedures:

- Configuring IP and Ethernet attributes on page 6-6
- Reconnecting to the management PC on page 6-11

## Configuring IP and Ethernet attributes

To update the IP and Ethernet configuration of the ODU to meet network requirements, proceed as follows:

**Procedure 6-4** Update IP and Ethernet configuration for network

| | |
|---|---|
| **1** | Select menu option **System, Configuration, LAN Configuration**. The LAN configuration page is displayed (Figure 6-5 or Figure 6-6 or Figure 6-7). |
| **2** | Update IP Address, Subnet Mask and Gateway IP Address to meet network requirements (as specified by the network administrator). |
| **3** | Review the other attributes and update them, if required (Table 6-1). |
| **4** | Select **Submit Updated System Configuration**. The reboot verification page is displayed (Figure 6-8 or Figure 6-9). |
| **5** | Select **Reboot Wireless Unit** and then **OK** to confirm the reboot. |

**Figure 6-5** LAN Configuration page

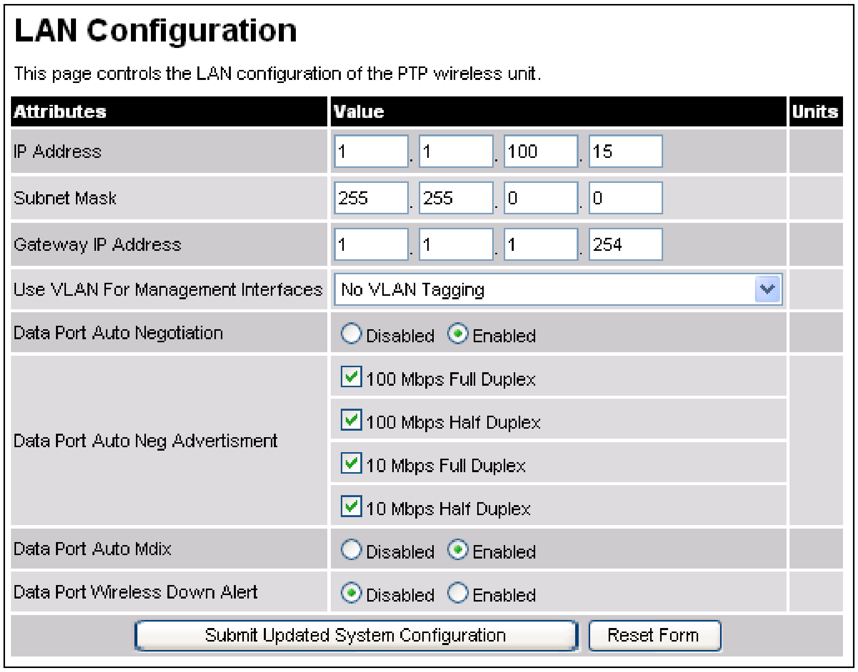



**Figure 6-6** LAN Configuration page with VLAN enabled

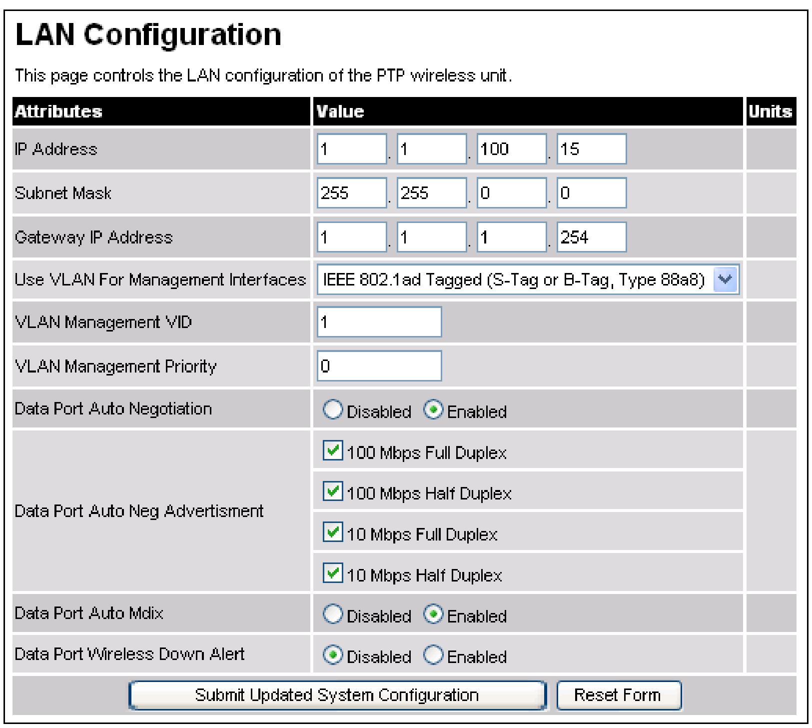


**Figure 6-7** LAN Configuration page with auto-negotiation disabled

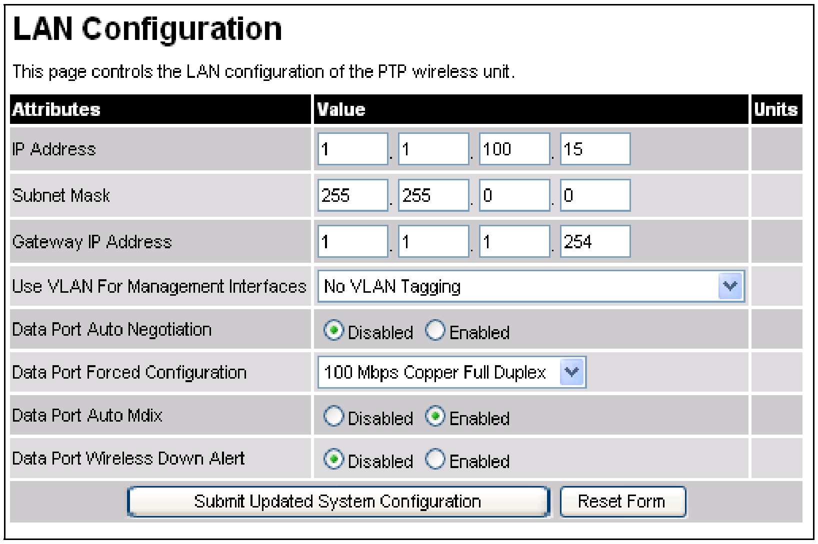



**Table 6-1** LAN Configuration attributes

| Attribute | Meaning |
|---|---|
| IP Address | Internet protocol (IP) address. This address is used by the family of Internet protocols to uniquely identify this unit on a network. |
| Subnet Mask | Defines the address range of the connected IP network. |
| Gateway IP Address | The IP address of a computer on the current network that acts as a gateway. A gateway acts as an entrance and exit to packets from and to other networks. |
| Use VLAN For Management Interfaces | This controls whether or not the management interfaces (WWW/SNMP/SMTP/SNTP) use VLAN tags.<br>**CAUTION**<br>Ensure that the configured VLAN is accessible, otherwise it will not be possible to access the unit following the next reboot.<br>The management function is only compatible with single VLAN tagged packets. Any management packet with two or more packets will be ignored. |

| Attribute | Meaning |
|---|---|
| VLAN Management VID | Only displayed when ‘Use VLAN for Management Interfaces’ is enabled (Figure 6-6).<br>Enter the VLAN VID (range 0 to 4094) that will be included in Ethernet frames generated by the management interfaces. |
| VLAN Management Priority | Only displayed when ‘Use VLAN for Management Interfaces’ is enabled (Figure 6-6).<br>Enter the VLAN priority (range 0 to 7) that will be included in Ethernet frames generated by the management interfaces. |
| Data Port Auto Negotiation | ‘Enabled’ means that configuration is automatically negotiated. This is the default setting.<br>‘Disabled’ means that configuration is forced.<br>Use the same setting for both ends of the link.<br>When Data Port Auto Negotiation is Disabled, the format of the LAN configuration page changes (Figure 6-7).<br>The configuration should only be forced if problems are experienced with auto-negotiation.<br>**NOTE**<br>Instead of forcing configuration, the IEEE802.3 specification recommends enabling Auto Negotiation with only the specific ability or abilities advertised. |
| Data Port Forced Configuration | Only displayed when Data Port Auto Negotiation is disabled (Figure 6-7).<br>This forces the speed and duplex setting of the Ethernet interface. Over the air throughput will be capped to the rate of the Ethernet interface at the receiving end of the link.<br>Use the same setting for both ends of the link.<br>**CAUTION**<br>The same configuration must be forced on connected network equipment, otherwise a duplex mismatch will occur and data throughput will be greatly reduced. |

| Attribute | Meaning |
|---|---|
| Data Port Auto Neg Advertisement | Only displayed when Data Port Auto Negotiation is enabled. Select the data rate that the auto-negotiation mechanism will advertise as available. Use the same setting for both ends of the link.<br><br>Only select a data rate that is within the capability of connected network equipment, otherwise loss of service may occur. |
| Data Port Auto Mdix | This enables/disables the Auto Medium Dependent Interface (MDI)/Medium Dependent Interface Crossover (MDIX) capability. Default is 'Enabled'. |
| Data Port Wireless Down Alert | When enabled, this causes the Ethernet link to be dropped briefly when the wireless link drops. This signals to the connected network equipment that this link is no longer available. Connected Ethernet switches can be configured to forward Ethernet frames on an alternative path identified using the Spanning Tree Protocol (STP). |

**Figure 6-8** Configuration Reboot page

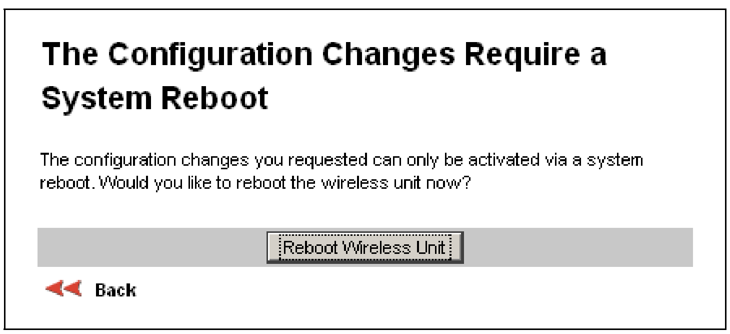
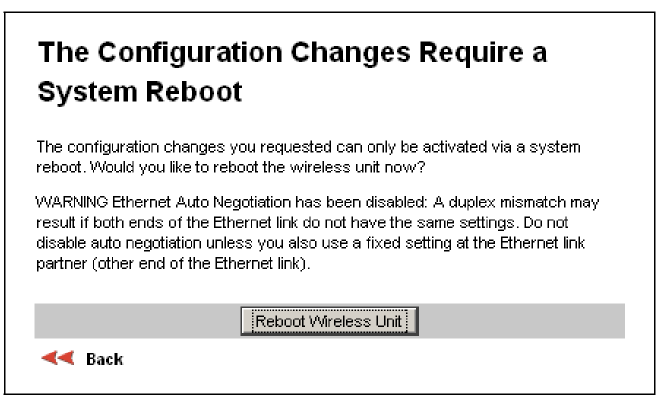



**Figure 6-9** Configuration Reboot page - Ethernet auto negotiation disabled



## Reconnecting to the management PC

If the IP Address, Subnet Mask and Gateway IP Address of the unit have been updated to meet network requirements, then reconfigure the local management PC to use an IP address that is valid for the network. Refer to Configuring the management PC on page 6-2.

When the unit has rebooted, log in using the new IP address. Refer to Logging into the web interface on page 6-4.

# Task 3: Configuring quality of service

## Configuring QoS

To assign priority encoded Ethernet frames to eight traffic classes, proceed as follows:

**Procedure 6-5** Configure QoS

| | |
|---|---|
| **1** | Select menu option **System, Configuration, QoS Configuration**. The QoS Configuration page is displayed (Figure 6-10). |
| **2** | Update the Priority Queue Mapping as required. The higher the queue number the greater its priority. The default rules are shown in Table 6-2. |
| **3** | To use IEEE 802.1Q classification rules, select **Set Default 802.1Q Priority Mappings**. The 802.1Q rules are shown in Table 6-2. |
| **4** | Select **Submit Updated Values**. |

**Figure 6-10** QoS Configuration page

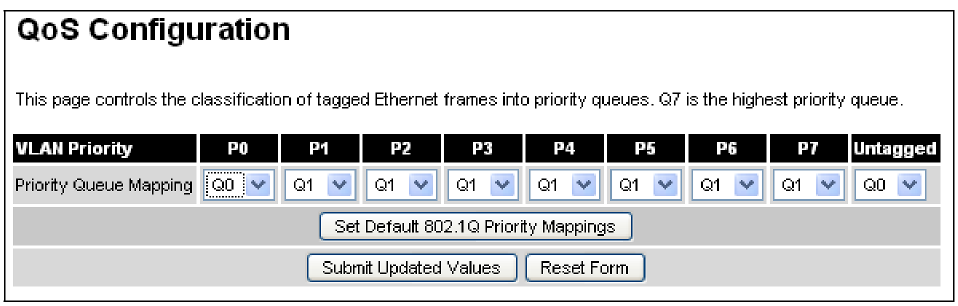


**Table 6-2** QoS default settings

| VLAN Priority | QoS default traffic class | IEEE802.1Q traffic class |
|---|---|---|
| P0 | Q0 | Q1 |
| P1 | Q1 | Q0 |
| P2 | Q1 | Q2 |
| P3 | Q1 | Q3 |
| P4 | Q1 | Q4 |
| P5 | Q1 | Q5 |
| P6 | Q1 | Q6 |
| P7 | Q1 | Q7 |
| Untagged | Q0 | Q1 |

# Task 4: Installing license keys

This task consists of the following procedures:

- Checking licensed capabilities on page 6-14
- Generating a new license key on page 6-16
- Entering a new license key on page 6-16

Some PTP 300 and PTP 500 products are supplied with two license keys: one installed at the factory and one alternative key.

## Checking licensed capabilities

To check that the capabilities of the installed license key meet the operator's requirements, proceed as follows:

**Procedure 6-6** Check capability summary

| | |
|---|---|
| **1** | Select menu option **System, License Key.** The Software License Key page is displayed (Figure 6-11). |
| **2** | Check the attributes in the Capability summary section (Table 6-3), in particular:<br>Region Code must be correct.<br>If encryption is required, ensure that the Encryption Algorithm setting is correct. |
| **3** | If the region code in the installed license key is incorrect, install the alternative license key as described in Entering a new license key on page 6-16 and check its capabilities. |
| **4** | If the available license keys do not have the required capabilities, then determine the new requirements and refer to Generating a new license key on page 6-16. |

**Figure 6-11** Software License Key page

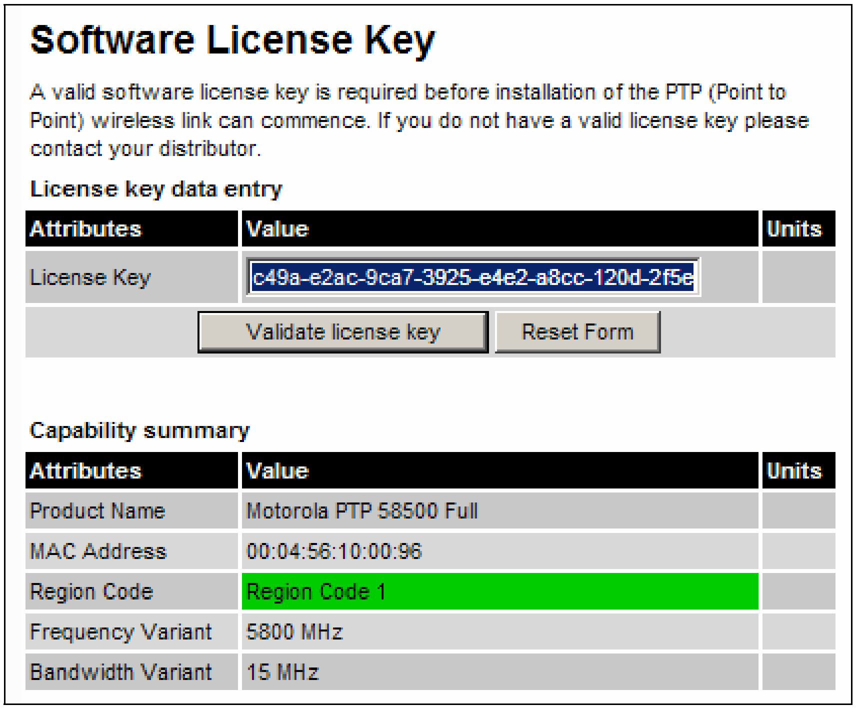



**Table 6-3** Capability summary attributes

| Attribute | Meaning |
|---|---|
| Product Name | The name of the product variant. |
| MAC Address | The MAC address of the ODU. |
| Region Code | The region code prohibits the wireless unit from operating outside the regulated limits. An invalid region code indicates a corrupted license key. |
| Encryption Algorithm | The encryption algorithms available for use at the wireless interface of the ODU. Encryption algorithm and keys must be the same at BOTH ends of the link for it to function correctly. This attribute is only displayed if the current license key permits encryption. |
| Frequency Variant | Frequency variant of the wireless unit. |
| Bandwidth Variant | Bandwidth variant of the wireless unit. |

## Generating a new license key

To generate a new license key to activate new licensed capabilities (for example region code or Encryption Algorithm), proceed as follows:

**Procedure 6-7** Use an access key to generate a license key

| | |
|---|---|
| **1** | Purchase the required new capabilities from the Motorola authorized Point-To-Point dealer who supplied the link.<br>The dealer will supply one or more access keys. |
| **2** | Go to the PTP web support page at http://www.motorola.com/ptp/support and select **Key Generator**. The PTP License Key Generator form should be displayed. |
| **3** | Enter the required details, including the access keys supplied by the dealer. |
| **4** | Submit the web form.<br>The PTP License Key Generator will respond with the new license key. |

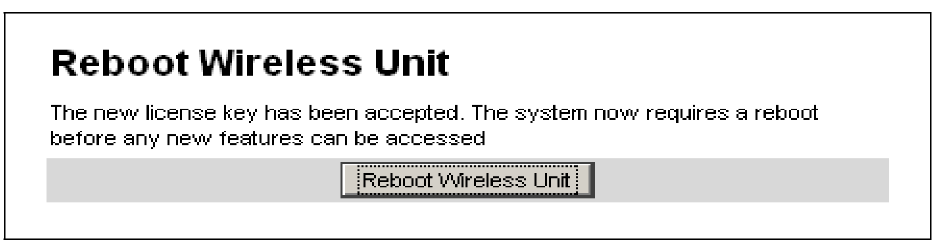
## Entering a new license key

To upgrade the unit to a new license key, proceed as follows:

**Procedure 6-8** Upgrade unit to a new license key

| | |
|---|---|
| **1** | Select menu option **System, License Key**. The Software License Key page is displayed (Figure 6-11). |
| **2** | Enter the new License Key. |
| **3** | Select **Validate license key**. If the license key is valid, the Reboot Wireless Unit dialog is displayed (Figure 6-12). |
| **4** | Select **Reboot Wireless Unit** and select **OK** to confirm. |
| **5** | On completion, the unit restarts with the new license key. |

**Figure 6-12** Reboot Wireless Unit dialog



# Task 5: Upgrading software version

This task consists of the following procedures:

- Checking the installed software version on page 6-17
- Saving the system configuration on page 6-18
- Upgrading to a new software version on page 6-19

**CAUTION**

Ensure that the correct units are upgraded, as units cannot easily be downgraded afterwards.

If the link is operational, ensure that the remote end of the link is upgraded first using the wireless connection, and then the local end can be upgraded. Otherwise, the remote end may not be accessible.

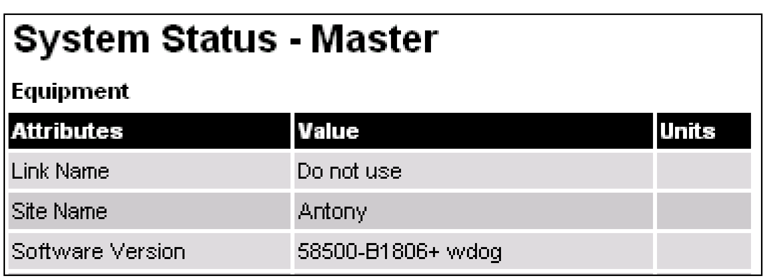
## Checking the installed software version

To check the installed software version, proceed as follows:

**Procedure 6-9** Check software version

| | |
|---|---|
| **1** | Select menu option **Status**. The System Status page is displayed. Software Version is near the top (Figure 6-13). |
| **2** | Go to http://www.motorola.com/ptp/support and find Point-to-Point software updates. Check that the latest software version (for example 500-04-01) is the same as the installed Software Version. |
| **3** | If the software needs to be upgraded to the latest version, perform Saving the system configuration on page 6-18 and Upgrading to a new software version on page 6-19. |

**Figure 6-13** Software Version in System Status page



System Status - Master

Equipment

| Attributes | Value | Units |
|---|---|---|
| Link Name | Do not use | |
| Site Name | Antony | |
| Software Version | 58500-B1806+ wdog | |

# Saving the system configuration

To save the current configuration before upgrading to a new software version, proceed as follows:

**Procedure 6-10** Save configuration file

| | |
|---|---|
| **1** | Select menu option **System, Configuration**, **Save And Restore**. The Save & Restore Configuration page is displayed (Figure 6-14). |
| **2** | Select **Save Configuration File**. |
| **3** | Save the configuration file to a PC hard drive. |

The configuration file format is:

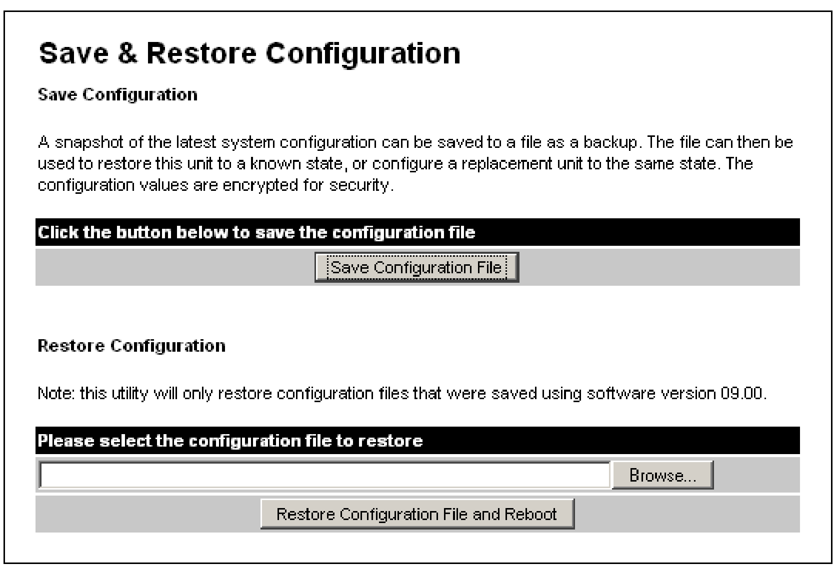
MAC-mm-mm-mm_IP-iii-iii-iii-iii.cfg

| **Where:** | **Is:** |
|---|---|
| mm-mm-mm | MAC address of unit |
| iii-iii-iii-iii | IP address of unit. |

**NOTE**

Internet Explorer inspects the content of any downloadable file and decides whether to treat the file as ASCII or binary. As a result of this feature, Internet Explorer always treats the configuration file as ASCII and attempts to display it instead of downloading it. Firefox makes no such assumption.

**Figure 6-14** Save & Restore Configuration page



# Upgrading to a new software version

Before performing a software upgrade, save the configuration as described in Saving the system configuration on page 6-18.

To upgrade to a new software version, proceed as follows:

**Procedure 6-11** Upgrade software version

| | |
|---|---|
| **1** | Go to http://www.motorola.com/ptp/support and find Point-to-Point software updates. Download and save the required software image (for example `PTP500-04-01.DLD2`). |
| **2** | Select menu option **System, Software Upgrade**. The Software Upgrade page is displayed (Figure 6-15). |
| **3** | Select **Browse**. Navigate to the folder containing the downloaded software image and select **Open**. |
| **4** | Select **Upload Software Image**. The Software Upgrade Confirmation page is displayed (Figure 6-16). |
| **5** | Select **Program Software Image into Non-Volatile Memory**. The Progress Tracker page is displayed (Figure 6-17).<br>CAUTION<br>The upgrade process should not be interrupted, as this can result in a corrupt main software image, which will result in the recovery image being booted at the next reset cycle. |
| **6** | On completion, the Software Upgrade Complete page is displayed (Figure 6-18).<br>Select **Reboot Wireless Unit** and select **OK** to confirm. The unit begins the reboot process. |
| **7** | The reboot process will take up to 120 seconds. During this time it will not be possible to communicate with the unit. After the reboot, check that the required software image is loaded and running. |

NOTE

If communication with the unit is not restored after 120 seconds , this could indicate a problem with the memory update process. If this happens, enter Recovery Mode as described in Using recovery mode on page 7-53.

**Figure 6-15** Software Upgrade page

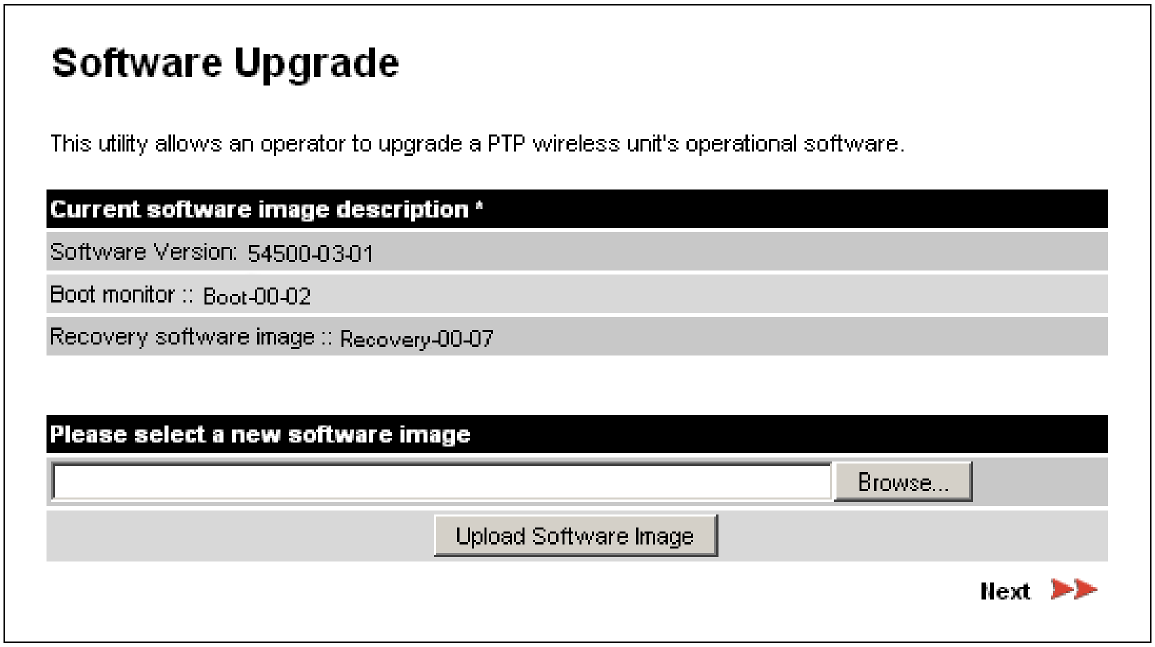



**Figure 6-16** Software Upgrade Confirmation page

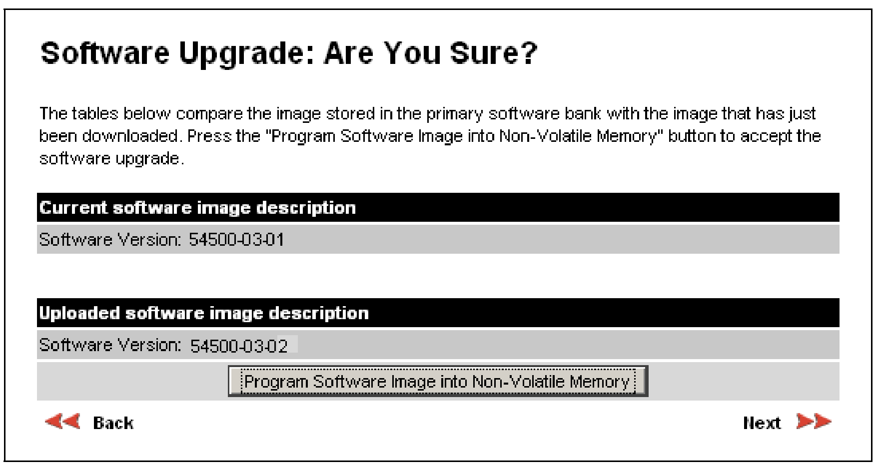


**Figure 6-17** Upgrade Progress Tracker page

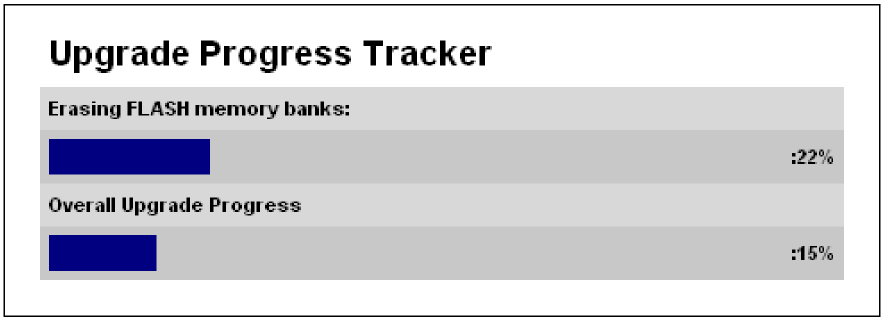
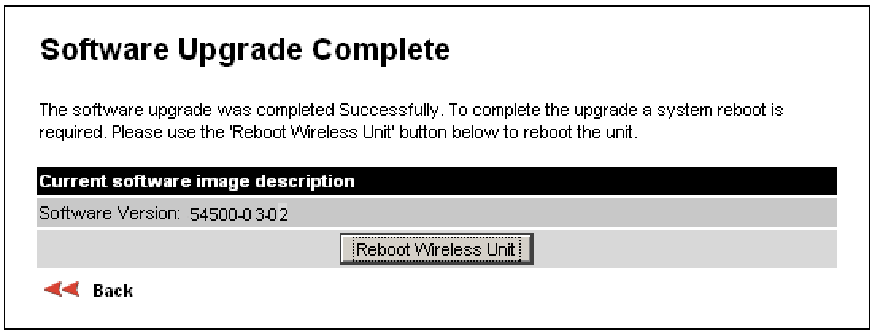



**Figure 6-18** Software Upgrade Complete page



# Task 6: Configuring security

## Configuring AES encryption

This procedure is only performed when the link requires AES encryption.

**CAUTION**

Before connecting the unit to the network, ensure that access to the web-based management interface is controlled in accordance with the network operator's security policy.

AES link encryption is only available to users who have purchased an appropriate license key. Refer to Task 4: Installing license keys on page 6-14.

To configure AES link encryption (before the link is operational), proceed as follows:

**Procedure 6-12** Configure AES link encryption on an unlinked unit

| | |
|---|---|
| 1 | Select menu option **System, Configuration**. The System Configuration page is displayed (Figure 6-19). |
| 2 | Select the Encryption Algorithm, either 'AES 128-bit' or 'AES 256-bit'. The same algorithm must be used at both ends of the link. |
| 3 | Enter and confirm the encryption key. The key consists of 32 or 64 case insensitive hexadecimal characters. The same key must be used at both ends of the link. |
| 4 | Select **Submit Updated System Configuration**. The reboot confirmation dialog is displayed (Figure 6-20). |
| 6 | Select **Reboot Wireless Unit**. |

**NOTE**

To enable AES encryption over an established link: open two browsers, log into the web interfaces at each end of the link, perform the above procedure at each unit, then reboot both ends of the link. The software is designed to allow five seconds so that a user can command both ends of the link to reboot before the wireless link drops.

⚠ **CAUTION**

Configuring link encryption over an established link will necessitate a service outage. Therefore, the configuration process should be scheduled during a period of low link utilization.

**Figure 6-19** System Configuration page

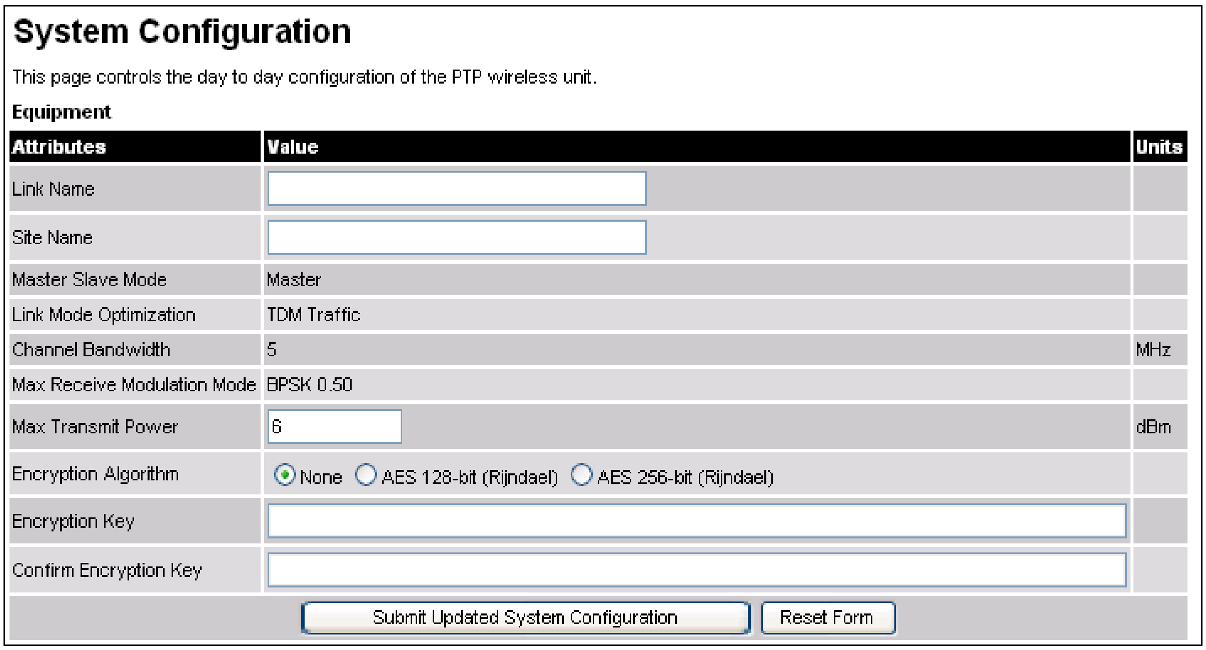
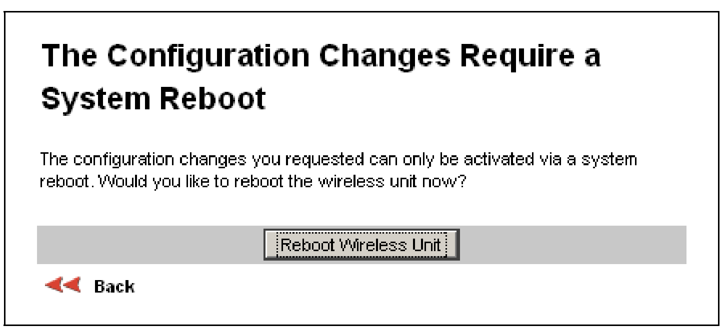



**Figure 6-20** Configuration Reboot dialog



# Task 7: Setting passwords

This task consists of the following procedures:

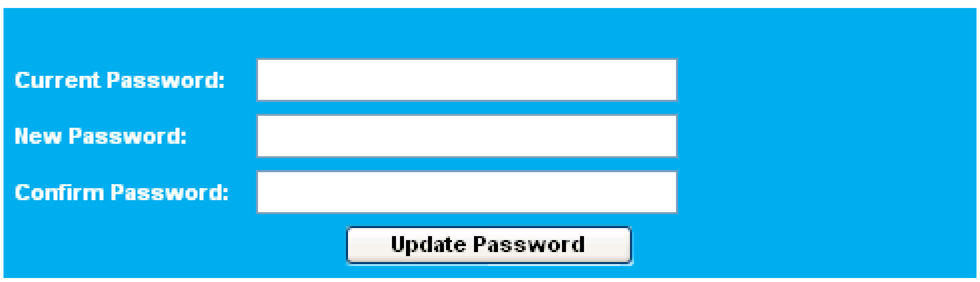
- Changing password on page 6-24
- Protecting access to the summary and status pages on page 6-25

## Changing password

This method is used for any user to change his/her own password.

Select menu option **Change Password**. The Change Password page is displayed (Figure 6-21). Enter and confirm the new password (the factory default is blank).

**Figure 6-21** Change Password page (System Administration example)



## Protecting access to the summary and status pages

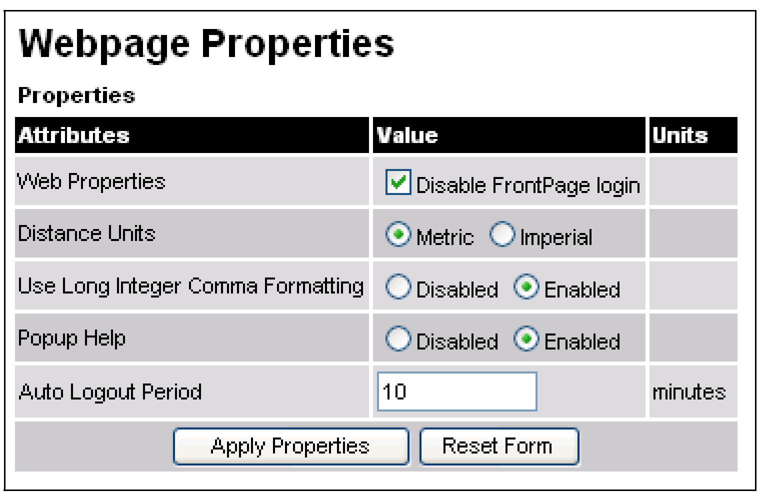
By default, the Home and Status menu items are not protected by password. If a higher level of system security is required, password protection can be extended to these pages.

To apply password access to the System Summary and System Status pages, proceed as follows:

**Procedure 6-13** Enable front page login

| | |
|---|---|
| **1** | Select menu option **Management, Web, Web Properties**. The Webpage Properties page is displayed (Figure 6-22). |
| **2** | In the Web Properties attribute, uncheck the 'Disable FrontPage login' box. |
| **3** | Select **Apply Properties**. |
| **4** | If the System Administration Password has not yet been set, see Changing password on page 6-24. |

**Figure 6-22** Webpage Properties page



# Task 8: Configuring wireless and telecoms interfaces

The wireless and telecoms interfaces are configured using the installation wizard. The installation wizard may also be used to re-configure the Ethernet interface if required.

This task consists of the following procedures:



## Starting installation wizard

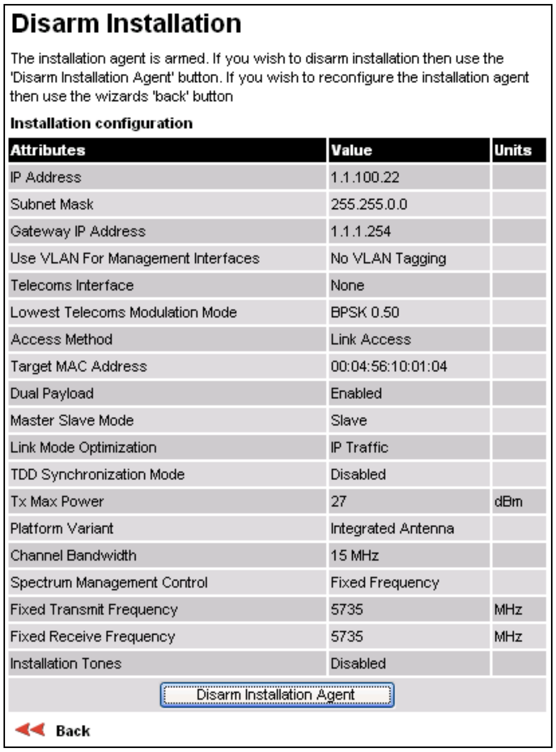
To check that the wireless configuration meets network requirements, select menu option **Installation**. The response depends upon the state of the unit:

- If the unit is armed for alignment (factory default configuration), the Disarm Installation page is displayed (Figure 6-23).
- If the unit is not armed, the Current Installation Summary page (Figure 6-24) is displayed.

Review the configuration:

- If it already meets requirements, skip this task and go to Task 10: Aligning antennas on page 6-44.
- If it does not meet requirements, execute the installation wizard by one of the following methods:
  - From the Disarm Installation page (Figure 6-23), select **Back**.
  - From the Current Installation Summary page (Figure 6-24), select **Continue to Installlation Wizard**.

**Figure 6-23** Disarm Installation page (when unit is armed)



## Disarm Installation

The installation agent is armed. If you wish to disarm installation then use the 'Disarm Installation Agent' button. If you wish to reconfigure the installation agent then use the wizards 'back' button

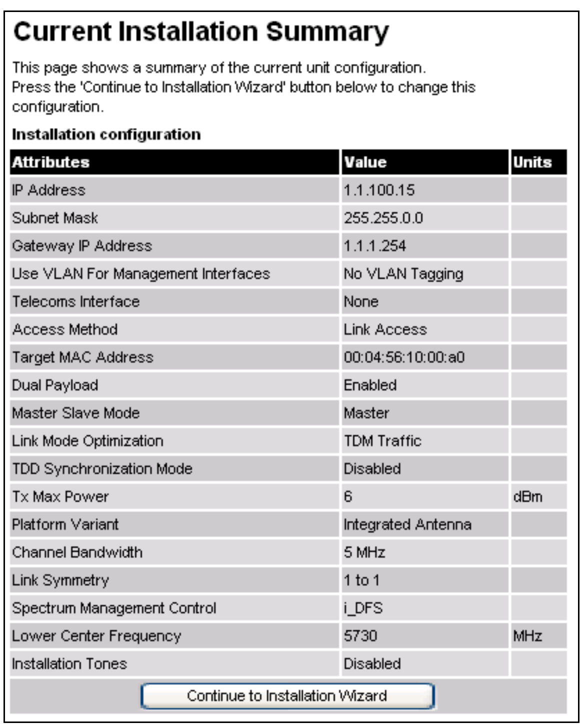
**Installation configuration**

| Attributes | Value | Units |
|---|---|---|
| IP Address | 1.1.100.22 | |
| Subnet Mask | 255.255.0.0 | |
| Gateway IP Address | 1.1.1.254 | |
| Use VLAN For Management Interfaces | No VLAN Tagging | |
| Telecoms Interface | None | |
| Lowest Telecoms Modulation Mode | BPSK 0.50 | |
| Access Method | Link Access | |
| Target MAC Address | 00:04:56:10:01:04 | |
| Dual Payload | Enabled | |
| Master Slave Mode | Slave | |
| Link Mode Optimization | IP Traffic | |
| TDD Synchronization Mode | Disabled | |
| Tx Max Power | 27 | dBm |
| Platform Variant | Integrated Antenna | |
| Channel Bandwidth | 15 MHz | |
| Spectrum Management Control | Fixed Frequency | |
| Fixed Transmit Frequency | 5735 | MHz |
| Fixed Receive Frequency | 5735 | MHz |
| Installation Tones | Disabled | |

Disarm Installation Agent

Back

**Figure 6-24** Current Installation Summary page (when unit is disarmed)



## Current Installation Summary

This page shows a summary of the current unit configuration.
Press the 'Continue to Installation Wizard' button below to change this configuration.

**Installation configuration**

| Attributes | Value | Units |
|---|---|---|
| IP Address | 1.1.100.15 | |
| Subnet Mask | 255.255.0.0 | |
| Gateway IP Address | 1.1.1.254 | |
| Use VLAN For Management Interfaces | No VLAN Tagging | |
| Telecoms Interface | None | |
| Access Method | Link Access | |
| Target MAC Address | 00:04:56:10:00:a0 | |
| Dual Payload | Enabled | |
| Master Slave Mode | Master | |
| Link Mode Optimization | TDM Traffic | |
| TDD Synchronization Mode | Disabled | |
| Tx Max Power | 6 | dBm |
| Platform Variant | Integrated Antenna | |
| Channel Bandwidth | 5 MHz | |
| Link Symmetry | 1 to 1 | |
| Spectrum Management Control | i_DFS | |
| Lower Center Frequency | 5730 | MHz |
| Installation Tones | Disabled | |

Continue to Installation Wizard

## Step 1: Interface configuration

Step 1 of the Installation wizard is for updating the interface configuration (Figure 6-25 or Figure 6-26). The attributes are described in Table 6-4. Update the attributes as required and select **Next**.

**NOTE**

If a copper loopback is used to test the E1 or T1 link (if enabled), ensure that the test set is configured manually. If the test set is allowed to configure automatically, neither it nor the ODU send a signal until they receive one, so the test appears to fail.

**Figure 6-25** Step 1: Interface Configuration page

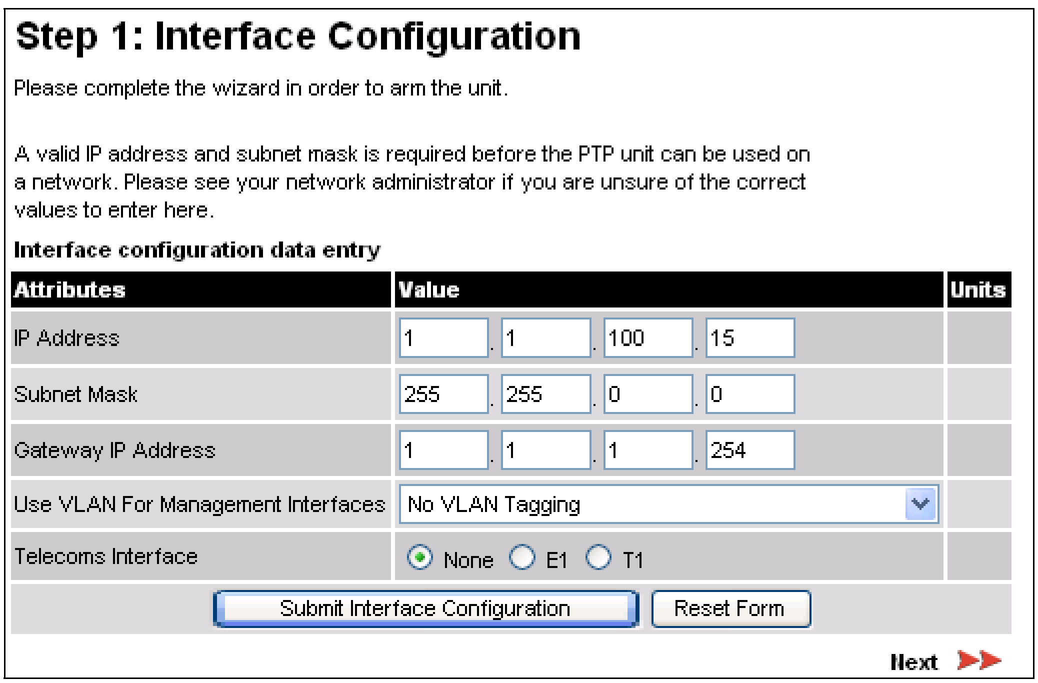


**Figure 6-26** Step 1: Interface Configuration page with T1 enabled

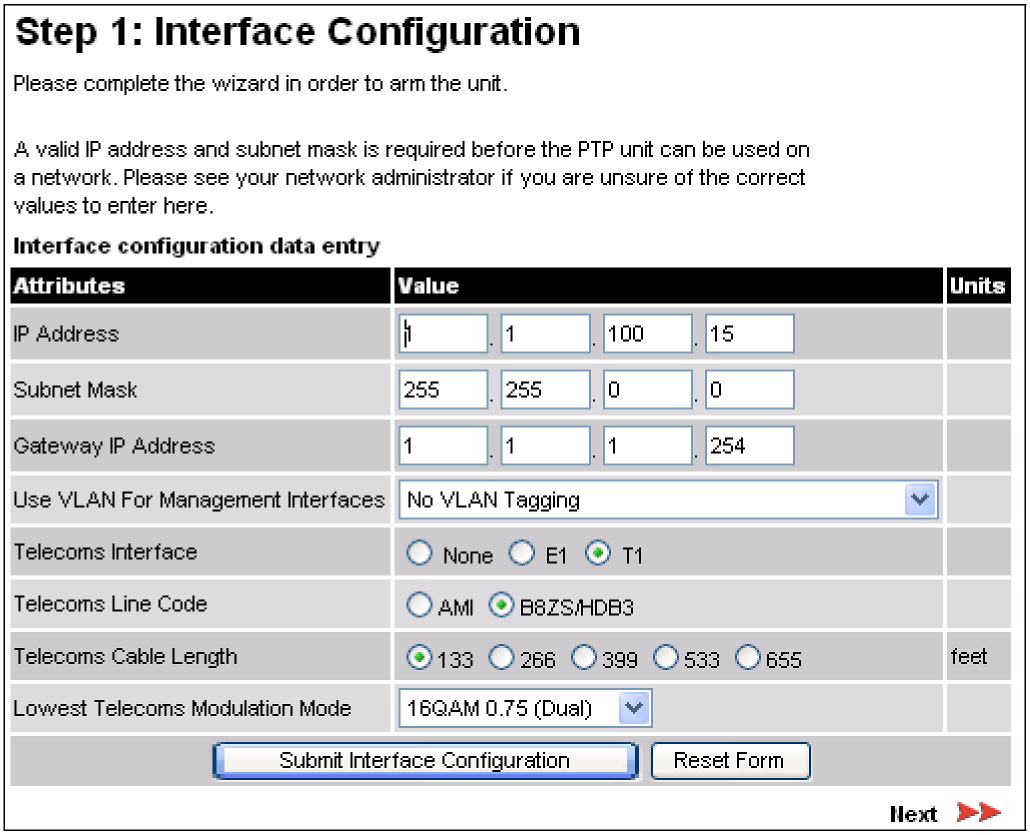



**Table 6-4** Step 1: Interface Configuration standard attributes

| Attribute | Meaning |
|---|---|
| IP Address | Updated in Configuring IP and Ethernet attributes on page 6-6. |
| Subnet Mask | Updated in Configuring IP and Ethernet attributes on page 6-6. |
| Gateway IP Address | Updated in Configuring IP and Ethernet attributes on page 6-6. |
| Use VLAN For Management Interfaces | Updated in Configuring IP and Ethernet attributes on page 6-6. |
| VLAN Management VID | Only displayed when Use VLAN for Management Interfaces is enabled. Updated in Configuring IP and Ethernet attributes on page 6-6. |

| Attribute | Meaning |
|---|---|
| VLAN Management Priority | Only displayed when Use VLAN for Management Interfaces is enabled. Updated in Configuring IP and Ethernet attributes on page 6-6. |
| VLAN Management VID Validation | Only displayed when Use VLAN for Management Interfaces is enabled. Updated in Configuring IP and Ethernet attributes on page 6-6. |
| Telecoms Interface | This allows the activation of the telecoms interface. The selection options are None, E1 or T1. |
| Telecoms Line Code | Only displayed when 'E1' or 'T1' are selected (Figure 6-26). Must match the setting of the device connected. |
| Telecoms Cable Length | Only displayed when 'T1' is selected (Figure 6-26). The length of the cable connecting the ODU to the channel A transceiver. |
| Lowest Telecoms Modulation Mode | The lowest modulation mode at which telecoms data can be sent. If the link cannot sustain telecoms data in this mode then the effective lowest modulation mode may differ.<br>In conjunction with the PTP LINKPlanner tool, this setting may be used to optimize the latency for links which operate in consistently high modulation modes. High data rate links are able to support lower latencies.<br>The effective lowest modulation mode is displayed on the Telecoms page. |

## Step 2: Wireless configuration

Step 2 of the Installation wizard is for updating the wireless configuration (Figure 6-27 or Figure 6-28). The attributes are described in Table 6-5. Update the attributes as required and select **Next**.

**Figure 6-27** Step 2: Wireless Configuration page

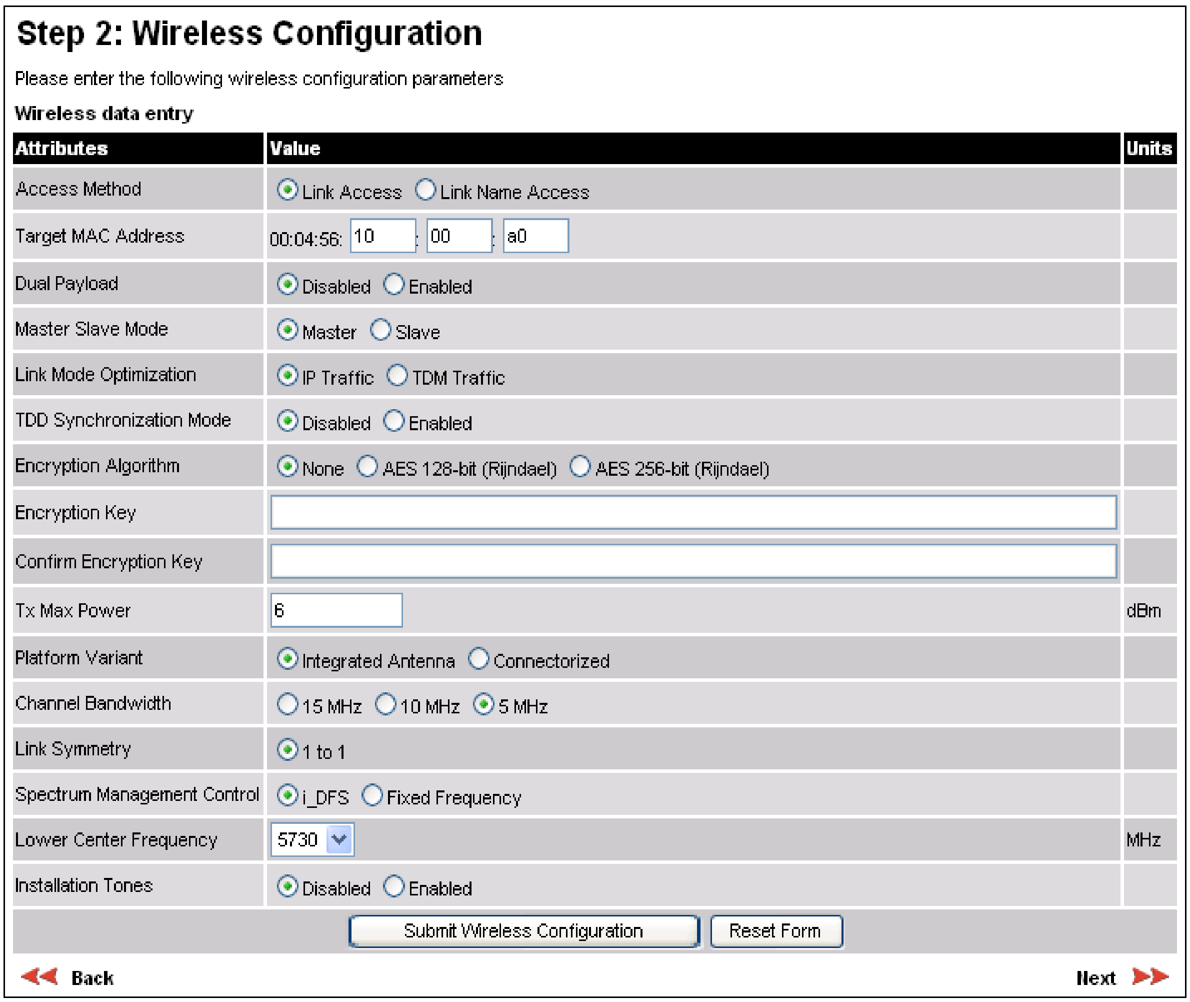
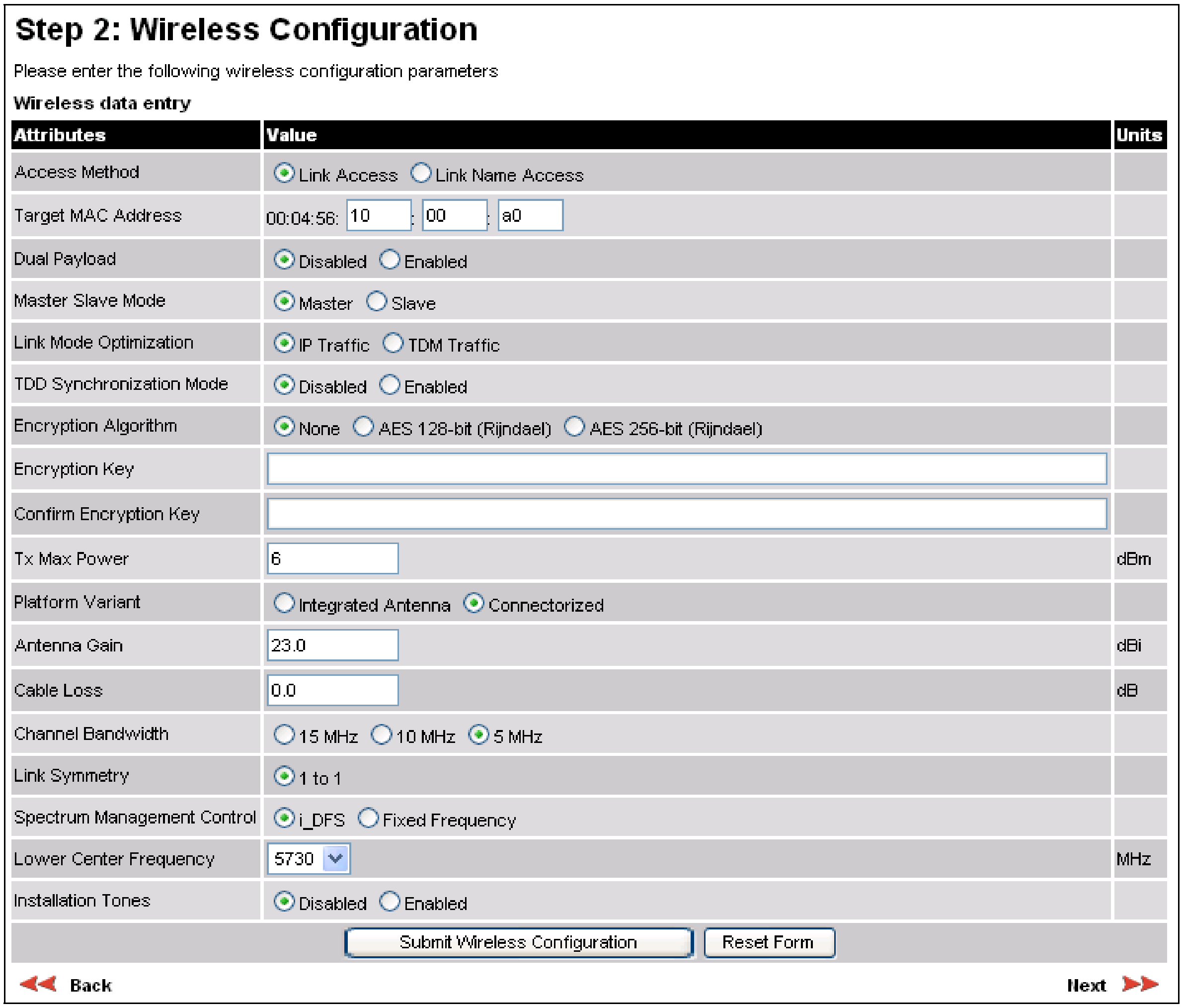


**Figure 6-28** Step 2: Wireless Configuration page for connectorized ODUs



## Step 2: Wireless Configuration

Please enter the following wireless configuration parameters

**Wireless data entry**

| Attributes | Value | Units |
|---|---|---|
| Access Method | (•) Link Access ( ) Link Name Access | |
| Target MAC Address | 00:04:56: 10 : 00 : a0 | |
| Dual Payload | (•) Disabled ( ) Enabled | |
| Master Slave Mode | (•) Master ( ) Slave | |
| Link Mode Optimization | (•) IP Traffic ( ) TDM Traffic | |
| TDD Synchronization Mode | (•) Disabled ( ) Enabled | |
| Encryption Algorithm | (•) None ( ) AES 128-bit (Rijndael) ( ) AES 256-bit (Rijndael) | |
| Encryption Key | | |
| Confirm Encryption Key | | |
| Tx Max Power | 6 | dBm |
| Platform Variant | ( ) Integrated Antenna (•) Connectorized | |
| Antenna Gain | 23.0 | dBi |
| Cable Loss | 0.0 | dB |
| Channel Bandwidth | ( ) 15 MHz ( ) 10 MHz (•) 5 MHz | |
| Link Symmetry | (•) 1 to 1 | |
| Spectrum Management Control | (•) i_DFS ( ) Fixed Frequency | |
| Lower Center Frequency | 5730 | MHz |
| Installation Tones | (•) Disabled ( ) Enabled | |

Submit Wireless Configuration | Reset Form

Back | Next

The contents of the Wireless Configuration page vary depending upon the options selected as follows:

- If Spectrum Management Control is set to 'Fixed Frequency', the Lower Center Frequency field is replaced by Fixed Tx Frequency and Fixed Rx Frequency.
- If Platform Variant is set to 'Connectorized', Antenna Gain and Cable Loss are also displayed.

**Table 6-5** Step 2: Wireless Configuration attributes

| Attribute | Meaning |
|---|---|
| Access Method | This attribute controls how the unit identifies and connects to the correct peer unit. There are two methods:<br>'Link Access' means that each unit must be configured with a Target MAC Address equal to the actual MAC address of its peer.<br>'Link Name Access' means that both units must be configured with the same Link Name. |
| Link Name | Only displayed when Access Method is set to 'Link Name Access'. A link can only be established between units that have identical Link Names.<br>Link Name may consist of letters (A-Z and a-z), numbers (0-9), spaces, and the following special characters:<br>(),-.,:<=>[]_{} |
| Target MAC Address | This is only displayed when Access Method is set to 'Link Access'. This is the MAC Address of the peer unit that will be at the other end of the wireless link. This is used by the system to ensure the unit establishes a wireless link to the correct peer. The MAC Address can be found embedded within the serial number of the unit. The last six characters of the serial number are the last three bytes of the unit's MAC address.<br>**NOTE**<br>A PTP 300 or PTP 500 Series system is shipped as a pair of units with pre-loaded correct MAC addresses. Target MAC addresses will only need to be entered if an existing unit has to be replaced in the field or the units configuration has been erased. |

| Attribute | Meaning |
|---|---|
| Dual Payload | This controls whether the link takes advantage of the channel condition to increase the link throughput. If set to 'Disable', the robustness of the link is improved. The default value is 'Enabled'.<br><br>This control is automatically set to 'Enabled' if either E1 or T1 is enabled and Lowest Telecoms Modulation Mode is set to a Dual Payload modulation. |
| Master Slave Mode | At this point it is necessary to decide which end will designate a Master. The Master unit is the controlling unit with respect to the point-to-point link and its maintenance. The master transmits until the link is made, while the Slave listens for its peer and only transmits when the peer has been identified. |
| Link Mode Optimization | Optimizes the link behavior according to the type of traffic that will be bridged. There are two modes to choose from: IP and TDM. For more information, see Link mode optimization on page 1-21. |
| TDD Synchronization Mode | PTP 500 only. Enables the TDD synchronization feature. See TDD synchronization on page 1-30 for basic description and Step 3: TDD synchronization (optional) on page 6-39 for installation and configuration details. |
| Encryption Algorithm | This is only displayed when encryption is enabled by license key. The same algorithm must be used at both ends of the link. Updated in Task 6: Configuring security on page 6-22. |
| Encryption Key | This is only displayed when encryption is enabled by license key. The same key must be used at both ends of the link. When identity based user accounts are enabled, only the Security Officer can change the encryption key. Updated in Task 6: Configuring security on page 6-22. |
| Confirm Encryption Key | This is only displayed when encryption is enabled by license key. Must contain the same value as Encryption Key. |
| Tx Max Power | This is the maximum transmit power (dBm) at which the unit will transmit.<br><br>Set this to the value (dBm) for antenna alignment as recommended in the installation report. |

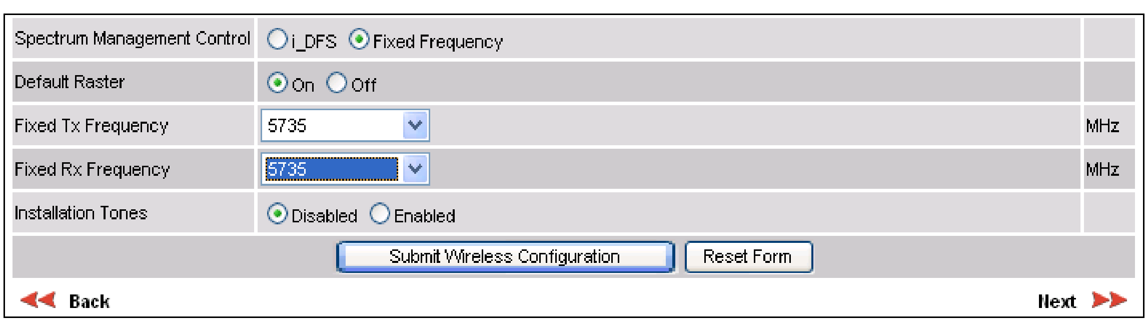
| Attribute | Meaning |
|---|---|
| Platform Variant | Chooses between an integrated unit or a connectorized unit that requires an external antenna. |
| Antenna Gain | Gain of the antenna that is connected to the unit, see Antenna specifications on page 4-19. |
| Cable Loss | Loss in the cable between the ODU and the antenna.<br>**NOTE**<br>If there is a significant difference in length of the antenna cables for the two antenna ports, then the average value should be entered. |
| Channel Bandwidth | Users can choose a variable channel bandwidth for the available spectrum. The selection depends upon the frequency variant and region. For more information, see Table 1-1. |
| Line Of Sight Mode | PTP 300 Master only. This attribute controls the Line Of Sight Mode. It is hidden unless the line of sight capability is enabled by license key. Values of 'Enabled' or 'Disabled' (the default) can be selected. Line Of Site mode may be used only when the path is completely unobstructed and the link range is less than 10 km (6 miles). If the control is 'Enabled', it allows the link to operate at higher data throughput rates. |

| Attribute | Meaning |
|---|---|
| Link Symmetry | (Master only) Values of "Adaptive", "3 to 1", "1 to 1" and "1 to 3" can be selected. The adaptive setting allows link symmetry to vary dynamically in response to offered traffic load. The remaining values select three options for fixed division between transmit and receive time in the TDD frame of the master ODU. The first number in the ratio represents the time allowed for the transmit direction and the second number represents the time allowed for the receive direction.<br><br>The appropriate matching Link Symmetry is set at the slave ODU automatically. For example, if Link Symmetry is configured as ‘3 to 1’ at the master ODU, then the slave ODU will be set automatically as ‘1 to 3’. In this example, the master-slave direction has triple the capacity of the slave-master direction.<br><br>Link Symmetry is subject to the following restrictions:<br><br>‘Adaptive’ is not supported in regions where radar avoidance is in use.<br><br>‘Adaptive’ is not supported when link optimization is set to ‘TDM’.<br><br>‘Adaptive’ is not supported in 5 MHz channel bandwidth.<br><br>‘3 to 1’ and ‘1 to 3’ are not supported in 5 MHz channel bandwidth.<br><br>‘3 to 1’ and ‘1 to 3’ are not supported when E1/T1 services are enabled. |
| Spectrum Management Control | Is used to configure the Spectrum Management features, see Managing spectrum on page 7-20 for more details. In regions that do not mandate DFS (Radar Detection), the Spectrum Management Control options are ‘i-DFS’ and ‘Fixed Frequency’. In regions that mandate DFS (Radar Detection), the Spectrum Management Control options are ‘DFS’ and ‘DFS with i-DFS’. |

| Attribute | Meaning |
|---|---|
| Lower Center Frequency | Not displayed when Spectrum Management Control is set to 'Fixed Frequency'. The software allows a user to optionally adjust the channel center frequencies. Changing the Lower Center Frequency attribute causes all channel center frequencies to be offset. It effectively slides the channelization up or down.<br>⚠ CAUTION<br>The lower center frequency attribute must be configured to the same value for both the master and slave. Failure to do so will cause the wireless link to fail reestablishment. The only way to recover from this situation is to modify the Lower Center Frequency attribute so that they are identical on both the master and slave unit. |
| Default Raster | This is only displayed when Spectrum Management Control is set to 'Fixed Frequency'. If this is set to 'On', the list of options presented in the fixed Tx frequency box is limited by the default raster. |

| Attribute | Meaning |
|---|---|
| Fixed Tx Frequency, Fixed Rx Frequency | This is only displayed when Spectrum Management Control is set to 'Fixed Frequency'. The software allows a user to optionally fix the Transmit and the Receive frequencies for a wireless link. The settings must be compatible at each end of the link. Once configured, the spectrum management software will not attempt to move the wireless link to a channel with lower co-channel or adjacent channel interference. Therefore this mode of operation is only recommended for deployments where the installer has a good understanding of the prevailing interference environment.<br><br>Figure 6-29 shows an example fixed frequency configuration for a 15 MHz channel bandwidth. In this example, the Fixed Transmit Frequency is set to 5735 MHz and the Fixed Receive Frequency is set to 5735 MHz. Care must be taken when configuring the Fixed Transmit and Receive Frequencies to ensure that both frequencies are on the same channel raster as the Lower Center Frequency. For example, if the channel raster is 5 MHz, both the Fixed Transmit and Receive Frequencies must be a multiple of 5 MHz from the Lower Center Frequency (5740 = 5735 + 5 MHz) and (5745 = 5735 + 5 MHz x 2).<br><br>**NOTE**<br><br>A raster limits the selection of the Rx frequency based upon the setting of the Tx frequency. |
| Installation Tones | 'Disabled' means that audio tones will not be emitted during antenna alignment.<br><br>'Enabled' means that audio tones will be emitted during antenna alignment (the recommended option). |

**Figure 6-29** Step 2: Wireless Configuration page (extract) for fixed frequency



# Step 3: TDD synchronization (optional)

To enable TDD Synchronization in a PTP 500 link, set the TDD Synchronization Mode attribute to 'Enabled' in the Step 2: Wireless Configuration page (Figure 6-27) and select **Next**. Step 3: TDD Synchronization page is displayed (Figure 6-30). The attributes are described in Table 6-6. Update the attributes as required and select **Next**.

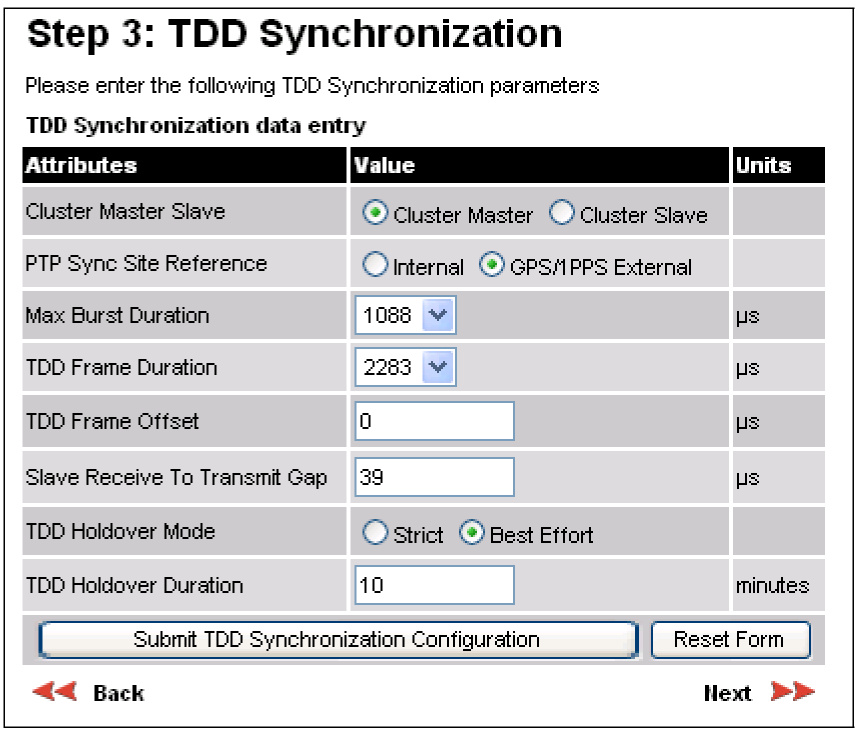
**NOTE**

TDD synchronization is not supported in the PTP 300 Series.

For more information on the available options, refer to Configuration options for TDD synchronization on page 2-25.

When TDD Synchronization is enabled, Link Symmetry is forced to '1:1' operation only.

**Figure 6-30** Step 3: TDD Synchronization page




**NOTE**

The data required to populate this screen is available in PTP LINKPlanner.

**Table 6-6** Step 3: TDD Synchronization attributes

| Attribute | Meaning |
|---|---|
| Cluster Master Slave | 'Cluster Master' is the first ODU in the synchronization chain.<br><br>'Cluster Slave' is the second or subsequent ODU in the chain. |
| PTP-SYNC Site Reference | 'Internal' means standalone operation with no external timing reference.<br><br>'GPS/1PPS External' means that an external GPS receiver will provide a 1 pps timing reference. |
| Max Burst Duration | The maximum duration of the burst opportunity. Select a value in the range 1088 to 2176 microseconds. |
| TDD Frame Duration | Select a value in the range 2283 to 4367 microseconds. |
| TDD Frame Offset | The delay of the start of the TDD frame from the epoch of the external timing reference. This permits the design of synchronized networks in which the phase of the TDD frame is independent of the master/slave function. Enter a value in the range from zero to one microsecond less than the TDD Frame Duration. |
| Slave Receive To Transmit Gap | The duration of the gap between receive and transmit at the slave ODU. |
| TDD Holdover Mode | (Master only). 'Strict' means that the unit will not transmit when synchronization is lost. 'Best Effort' means that the unit will synchronize when there is a reference signal, but otherwise will operate in unsynchronized mode. |
| TDD Holdover Duration | (Master only). Default value 10 minutes, maximum 60 minutes. Specifies duration of holdover period following loss of the external timing reference for TDD synchronization. |

## Step 3 or 4: Confirm installation configuration

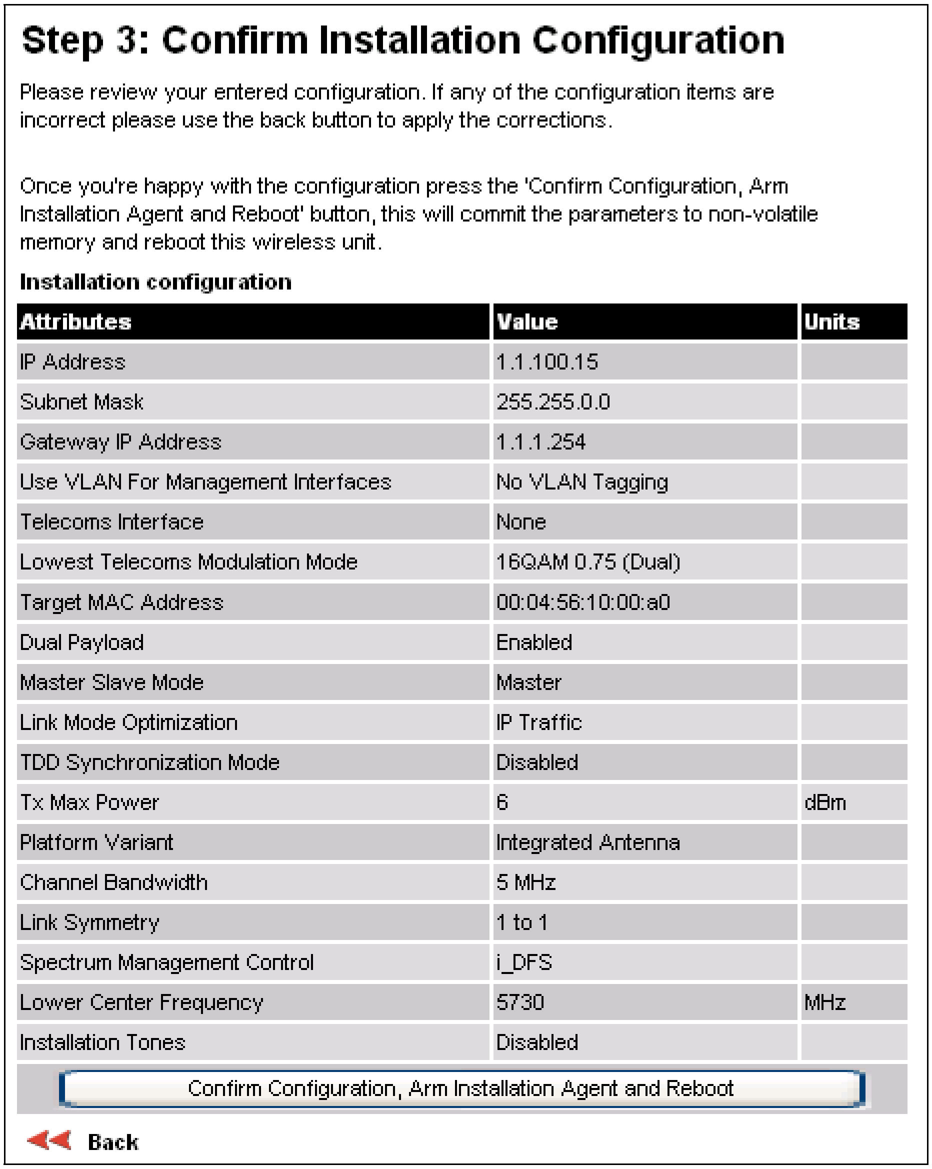
Step 3 of the Installation wizard is provided for reviewing and confirming the wireless configuration parameters (Figure 6-31) (this becomes Step 4 if TDD Synchronization is enabled). The page contents vary depending upon the product variant and configuration options selected.

If any of the Installation wizard attributes have been updated, select **Confirm Configuration, Arm Installation and Reboot**. The confirmation popup is displayed (Figure 6-32). Select **OK** to reboot.

**NOTE**

If any of the interface attributes have been updated in Step 1 of the Installation wizard, the local management PC will not be able to communicate after the changes are confirmed and the reboot occurs. If it is necessary to make further configuration changes using the local management PC, modify the network configuration of the PC Ethernet port to match the new IP and VLAN configuration of the unit.

**Figure 6-31** Step 3: Confirm Installation Configuration page



# Step 3: Confirm Installation Configuration

Please review your entered configuration. If any of the configuration items are incorrect please use the back button to apply the corrections.

Once you're happy with the configuration press the 'Confirm Configuration, Arm Installation Agent and Reboot' button, this will commit the parameters to non-volatile memory and reboot this wireless unit.

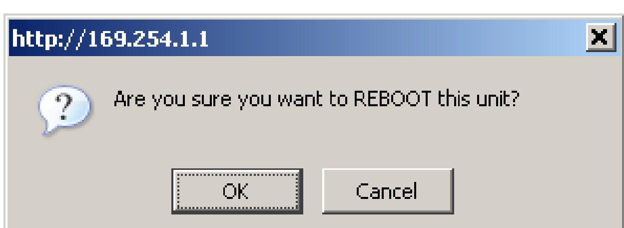
**Installation configuration**

| Attributes | Value | Units |
|---|---|---|
| IP Address | 1.1.100.15 | |
| Subnet Mask | 255.255.0.0 | |
| Gateway IP Address | 1.1.1.254 | |
| Use VLAN For Management Interfaces | No VLAN Tagging | |
| Telecoms Interface | None | |
| Lowest Telecoms Modulation Mode | 16QAM 0.75 (Dual) | |
| Target MAC Address | 00:04:56:10:00:a0 | |
| Dual Payload | Enabled | |
| Master Slave Mode | Master | |
| Link Mode Optimization | IP Traffic | |
| TDD Synchronization Mode | Disabled | |
| Tx Max Power | 6 | dBm |
| Platform Variant | Integrated Antenna | |
| Channel Bandwidth | 5 MHz | |
| Link Symmetry | 1 to 1 | |
| Spectrum Management Control | i_DFS | |
| Lower Center Frequency | 5730 | MHz |
| Installation Tones | Disabled | |

Confirm Configuration, Arm Installation Agent and Reboot

Back

**Figure 6-32** Reboot confirmation pop up



# Task 9: Barring channels

## Barring channels to avoid TDWR radars (USA)

For units operating within the FCC, certain channels may need to be barred from operation, as planned in Avoidance of weather radars (USA only) on page 2-5.

If this requirement exists, the system designer will have provided a list of channel center frequencies to be barred. The affected channels must be barred during staging, before the units are allowed to radiate on site.

To bar channels, proceed as follows:

**Procedure 6-14** Bar weather radar channels (USA)

| | |
|---|---|
| **1** | Log into the master unit. |
| **2** | Select menu option **System, Spectrum Management**. The Spectrum Management page is displayed (Figure 7-8). |
| **3** | Click on the appropriate channel center frequencies on the Local or Peer channel spectrum plots. When the confirmation dialog is displayed, select **OK**. |

# Task 10: Aligning antennas

Before performing this task, check that hardware installation is complete (apart from the network connections) at both the Master and Slave sites.

This task consists of the following procedures:


- Starting up the units on page 6-44
- Checking that the units are armed on page 6-45
- Aligning antennas on page 6-45
- Aligning separate antennas for spatial diversity on page 6-47
- Monitoring received signal level on page 6-47.
- Disarming the units on page 6-52


## Starting up the units

To connect one of the units to a management PC and start up both units, proceed as follows:

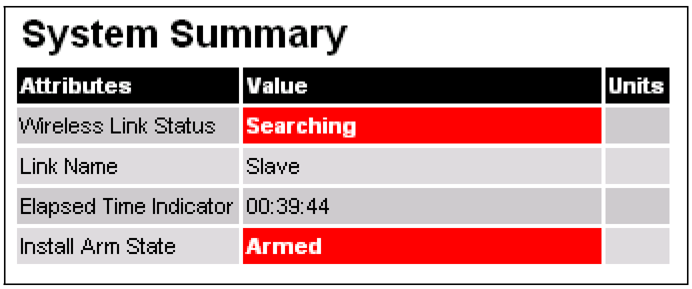
**Procedure 6-15** Starting the units after site hardware installation

| | |
|---|---|
| **1** | Select the unit from which this process is to be controlled; either Master or Slave. This is the 'local' unit. |
| **2** | Check that the management PC is connected to the local unit, powered up and logged on. |
| **3** | Start the local unit. |
| **4** | Start the remote unit. |
| **5** | Log into the local unit as described in Logging into the web interface on page 6-4. |

## Checking that the units are armed

Select menu option **Home**. The System Summary page is displayed. Check that the Install Arm State is set to 'Armed' (Figure 6-33); this confirms that the units are ready for alignment.

**Figure 6-33** System Summary page (when unit is armed)




If the units are not armed, execute the installation wizard as described in Task 8: Configuring wireless and telecoms interfaces on page 6-26.

## Aligning antennas

Use this procedure to align linked antennas (master and slave), whether integrated or connectorized.

Prior to alignment, ensure that the following parameters are available:

- Location of both sites (latitude and longitude).
- Bearing to the other end of the link for both sites.
- Prediction of receive signal level for both ends of the link.
- Prediction of link loss.

PTP LINKPlanner provides all of these parameters in the form of an installation report.

If a connectorized ODU is installed at either site with two separate antennas for spatial diversity, refer to Aligning separate antennas for spatial diversity on page 6-47 before starting alignment.

**NOTE**

To achieve best results, make small incremental changes to elevation and azimuth.

**⚠ CAUTION**

The action of tightening the mounting bolts can alter antenna alignment. This can be helpful when fine-tuning alignment, but it can also lead to misalignment. To prevent misalignment, continue to monitor receive signal level during final tightening of the bolts.

To align the antennas, proceed as follows:

**Procedure 6-16** Align antennas

| | |
|---|---|
| **1** | At each end of the link, adjust the antenna to point at the other end of the link. This should be done with the aid of a compass. |
| **2** | Without moving the master antenna, adjust the elevation and azimuth of the slave antenna to achieve the highest receive signal level (using one of the three recommended methods in Monitoring received signal level on page 6-47). |
| **3** | Without moving the Slave antenna, adjust the elevation and azimuth of the Master antenna to achieve the highest receive signal level (using one of the three recommended methods). |
| **4** | Repeat steps 2 and 3 as necessary to fine-tune the alignment to find the center of the beam. |
| **5** | When the antennas have been aligned on the center of the beam, verify that the receive level is within the predicted range (from the installation report). If this is not the case, go back to step 2.<br><br>The current value of receive level can be verified by using the DVM method (see Method #2: digital voltmeter (DVM) on page 6-50) the graphical installation method (see Method #3: graphical install on page 6-51) or by selecting menu option **Status** and monitoring the Receive Power attribute on the System Status page. |
| **6** | If after repeated attempts to align, the receive level still does not lie within the predicted range, this may be because the  data provided to the prediction tool (such as PTP LINKPlanner) is inaccurate. For example estimates of path obstructions, antenna heights or site locations may be inaccurate. Check this data and update the prediction as necessary. |
| **7** | Once the antennas have been aligned correctly, tighten the integrated ODU (or connectorized antenna) mountings. To ensure that the action of tightening does not alter antenna alignment, continue to monitor received signal level. |

## Aligning separate antennas for spatial diversity

If a connectorized ODU is installed at either site with two separate antennas for spatial diversity, proceed as follows:

**Procedure 6-17** Aligning spatial diversity antennas

| | |
|---|---|
| **1** | Connect the horizontal polarization antenna to the ODU, disconnect the vertical polarization antenna, then perform Aligning antennas on page 6-45. |
| **2** | Connect the vertical polarization antenna to the ODU, disconnect the horizontal polarization antenna, then perform Aligning antennas on page 6-45. |
| **3** | Re-connect the horizontal polarization antennas. The received signal level should increase. |
| **4** | Weatherproof the antenna connections at the ‘H’ and ‘V’ interfaces of the ODUs, as described in Mounting and connecting antennas on page 5-17. |

## Monitoring received signal level

The goal of antenna alignment is to find the center of the main beam. This is done by adjusting the antennas while monitoring the receive signal level. Choose one of three methods for monitoring receive signal level:

- Method #1: ODU installation tones on page 6-48
- Method #2: digital voltmeter (DVM) on page 6-50
- Method #3: graphical install on page 6-51

## Method #1: ODU installation tones

This is the first of three methods that may be used to monitor receive signal level during antenna alignment.

The ODU emits audible tones during installation to assist with alignment. The pitch of the alignment tone is proportional to the received power of the wireless signals. Adjust the alignment of the unit in both azimuth and elevation until the highest pitch tone is achieved.

**NOTE**

When using ODU installation tones to align connectorized antennas, it may not be possible to hear the tones. To overcome this problem, either use an assistant, or use a stethoscope to give a longer reach.

The tones and their meanings are described in Table 6-7. In each of the states detailed in the table, align the unit to give the highest pitch tone.

**Table 6-7** ODU installation tones

| State Name | Tone Description | State Description | Pitch Indication |
|---|---|---|---|
| Free Channel Search | Regular beep | Executing band scan | N/A |
| Scanning | Slow broken tone | Not demodulating the wanted signal | Rx Power |
| Synchronized | Fast broken tone | Demodulating the wanted signal | Rx Power |
| Registered | Solid tone | Both Master and Slave units exchanging Radio layer MAC management messages | Rx Power |
| Alarm | Fast broken dual tone | A fatal error has occurred. | |

The term ‘wanted signal’ refers to that of the peer unit being installed.

**CAUTION**

If, when in the Synchronized or Registered state, the tone varies wildly, there may be interference or a fast fading link. Installing in this situation may not give a reliable link. Investigate the cause of the problem.

During alignment, the installation tones should exhibit the following behavior:

- **Band scan:** When first started up and from time to time, the Master unit will carry out a band scan to determine which channels are not in use. During this time, between 10 and 15 seconds, the Master unit will not transmit and as a consequence of this neither will the Slave unit. During this time the installation tone on the master unit will drop back to the band scan state, and the Slave unit will drop back to the Scanning state with the pitch of the tone set to the background noise level. Alignment of the unit should cease during this time.
- **Radar detection:** If the unit is operating where mandatory radar avoidance algorithms are implemented, the ranging behavior may be affected. The Master has to monitor the initially chosen channel for 60 seconds to make sure it is clear of radar signals before transmitting. If a radar is detected during any of the installation phases, a further compulsory 60 seconds channel scan will take place as the master unit attempts to locate a new channel that is free of radar interference.
- **Ranging:** The PTP 300 and PTP 500 Series do not require the user to enter the link range. The Master unit typically takes less than 60 seconds to determine the length of the link being installed. The Master unit will remain in the Scanning state until the range of the link has been established. The Master unit will only move to the Synchronized state when the range of the link has been established.

  The Slave unit does not have a ranging process. The slave unit will change to the Synchronized state as soon as the wanted signal is demodulated.
- **Retrying same channel:** If, at the end of the ranging period, the Registered state is not achieved due to interference or other reasons, the Master unit will retry twice more on the same channel before moving to another available channel. Should this occur it might take a number of minutes to establish a link in the Registered state.

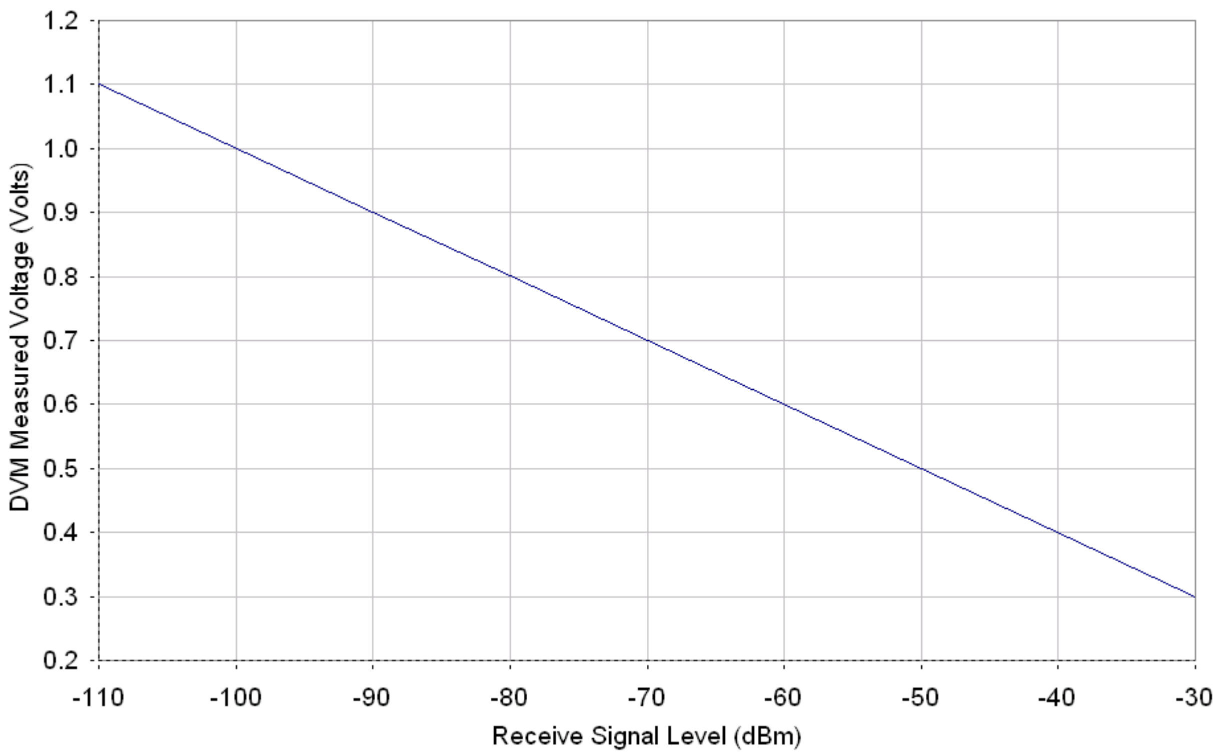
## Method #2: digital voltmeter (DVM)

This is the second of three methods that may be used to monitor receive signal level during antenna alignment.

The BNC connector at the ODU provides an analogue voltage which is proportional to the receive signal strength. To use, remove the protective cap from the BNC connector and connect a DVM.

Figure 6-34 shows the relationship between measured values and the receive signal strength.

**Figure 6-34** Using DVM for alignment

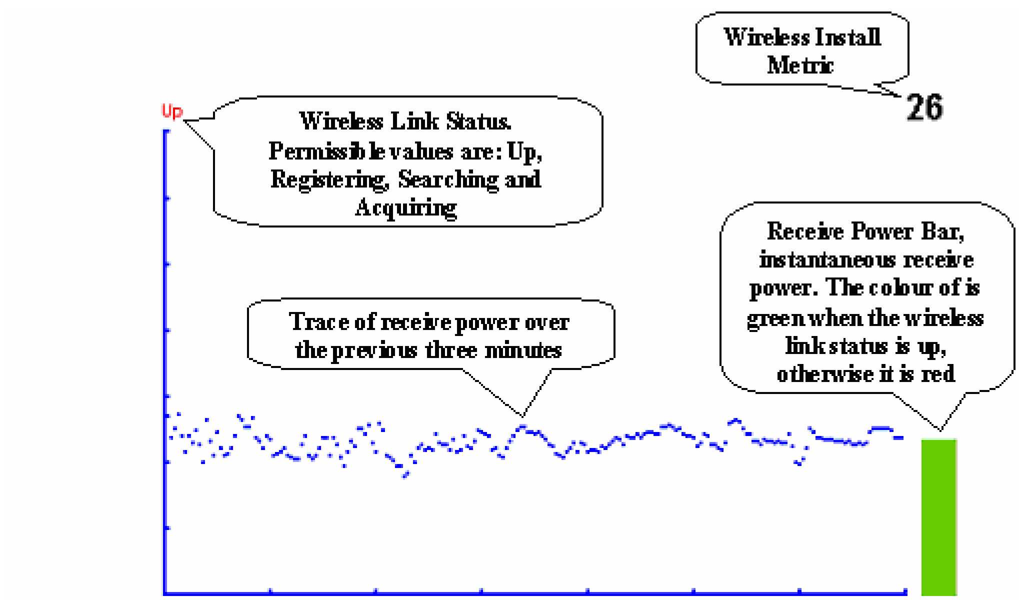


## Method #3: graphical install

This is the third of three methods that may be used to monitor receive signal level during antenna alignment.

Select menu option **Installation, Graphical Install**. The Graphical Install page is displayed (Figure 6-35).

**Figure 6-35** Graphical installation page




The screen displays the receive power over the last three minutes. This will allow the installer to slowly sweep the antenna during installation and monitor the variation in signal strength with angular position. The screen automatically refreshes every three seconds.

The screen also displays the current state of the wireless link in two ways. First, the actual state of the wireless link is written in the top left corner of the screen. The instantaneous receive power bar also encodes the state of the wireless link using green to signify that the wireless link is up and red for all other states.

The installation metric is simply the instantaneous receive power in dBm + 110.

**PDA version:** To access the PDA version of the graphical installation tool, use a hidden URL -
**http://<ip-address>/pda.cgi**. This link is only available to system administrators.

## Disarming the units

When antenna alignment is complete, both units in the link must be disarmed in order to:

- Turn off the audible alignment aid.
- Enable adaptive modulation.
- Fully enable spectrum management features (such as i-DFS, if configured).
- Clear unwanted installation information from the various systems statistics.
- Store the link range for fast link acquisition on link drop.
- Enable higher data rates.

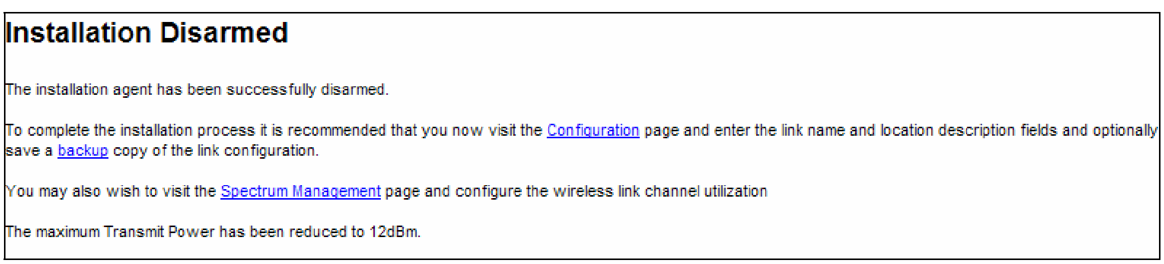
**NOTE**

The PTP 300 and PTP 500 incorporate automatic transmit power control to prevent overload of the receiver at the other end of the link. Only disarm after a period of two minutes has expired since the final antenna adjustment. This ensures that the transmit power has settled.

After 24 hours, the units will be disarmed automatically, provided that they are armed and that the link is up.

To disarm the units,select menu option **Installation**. The Disarm Installation page is displayed (Figure 6-23). Select **Disarm Installation Agent**. The confirmation pages is displayed (Figure 6-36).

**Figure 6-36** Optional post-disarm configuration




To proceed directly to Task 11: Updating system configuration on page 6-53, click the Configuration link on the above page.

# Task 11: Updating system configuration

## Reviewing system configuration attributes

When antenna alignment is complete and the units have been disarmed, the system configuration should be reviewed and updated as necessary.

To update the system configuration, select menu option **System, Configuration**. The System Configuration page is displayed (Figure 6-19). Update the attributes as required (Table 6-8), then select **Submit Updated System Configuration**.

**Table 6-8** System Configuration attributes

| Attribute | Meaning |
|---|---|
| Link Name | User defined identity for the link. Updated in Step 2: Wireless configuration on page 6-31. |
| Site Name | User defined name for the site, with additional notes (optional). |
| Master Slave Mode | Read only. Updated in Step 2: Wireless configuration on page 6-31. |
| Link Mode Optimization | Read only. Updated in Step 2: Wireless configuration on page 6-31. |
| Channel Bandwidth | Read only. Updated in Step 2: Wireless configuration on page 6-31. |
| Max Receive Modulation Mode | The maximum mode the unit will use as its adaptive modulation. By default the Max Receive Modulation Mode is the highest mode available.<br>For minimum error rates, set the maximum modulation mode to the minimum necessary to carry the required traffic. |
| Max Transmit Power | This is the maximum transmit power at which the unit will operate, configurable in steps of 1 dB. Its maximum setting is dependent on the region of operation and this is controlled by the license key.<br>It will normally show the value configured during the alignment task. For short links however, the unit may have automatically reduced this to 12 dBm in order to prevent receiver overload at the other end of the link. |

| Attribute | Meaning |
|---|---|
| Antenna Gain | Only displayed when Platform Variant is set to ‘Connectorized’ in Step 2 of the Installation wizard. Updated in Step 2: Wireless configuration on page 6-31. |
| Cable Loss | Only displayed when Platform Variant is set to ‘Connectorized’ in Step 2 of the Installation wizard. Updated in Step 2: Wireless configuration on page 6-31. |
| EIRP | Only displayed when Platform Variant is set to ‘Connectorized’ in Step 2 of the Installation wizard.<br>Effective Isotropic Radiated Power (EIRP) describes the strength of the radio signal leaving the wireless unit. Use it to verify that the link configuration (Max Transmit Power, Antenna Gain and Cable Loss) does not exceed any applicable regulatory limit. |
| Encryption Algorithm | Only displayed when AES encryption is enabled by licensed key. Updated in Task 6: Configuring security on page 6-22. |
| Encryption Key | Only displayed when AES encryption is enabled by license key. Updated in Task 6: Configuring security on page 6-22. |
| Confirm Encryption Key | Only displayed when AES encryption is enabled by license key. Updated in Task 6: Configuring security on page 6-22. |

# Task 12: Checking wireless performance

## Comparing actual to predicted performance

For at least one hour of operation after disarming, the link should be monitored to check that it is achieving predicted levels of performance.

To check performance, select menu option **System, Statistics**. The System Statistic page is displayed (Figure 7-16). Monitor the following attributes:

- Link Loss
- Transmit Data Rate
- Receive Data Rate

PTP LINKPlanner provides the prediction in the form of an installation report.

For more information, refer to Managing spectrum on page 7-20.

# Task 13: Connecting link to the network

This task consists of the following procedures:

- Connecting to the network on page 6-56
- Setting the real-time clock on page 6-57

## Connecting to the network

To connect to the network, proceed as follows:

**Procedure 6-18** Connect to network – in-band management

| | |
|---|---|
| **1** | Disconnect the local PC from the PIDU Plus at the Master and Slave sites. |
| **2** | At each site, connect the PIDU Plus LAN ports to a router port, switch port or other network equipment in the data network using the CAT5e cable that was prepared for this purpose in Preparing the PIDU Plus to LAN cable on page 5-28. |
| **3** | Check that the Master and Slave units are reachable from the network management system by opening the web interface to the management agents, or by requesting ICMP echo response packets using the Ping application. The network management system will normally be geographically remote from the sites, so it may be necessary to request that this action is completed by co-workers at the management center. Alternatively, it may be possible to use remote login to the management system. |
| **4** | Check the data network for correct operation across the wireless link. This may be by requesting ICMP echo response packets between hosts in the connected network segments, or by some more structured use of network testing tools. |

# Setting the real-time clock

Perform this task to set the real-time clock.

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):

- In the absence of an SNTP server connection, the clock can be set to run manually. The clock is battery backed and will continue to operate for several days after the ODU is switched off.
- If an SNTP server connection is available, the clock can be set to synchronize with the server time at regular intervals.

## Setting the real-time clock manually

To set the clock to keep time without connecting to a networked time server, proceed as follows:

**Procedure 6-19** Set the real-time clock manually

| | |
|---|---|
| **1** | Select menu option **Management, Time.** The Time Configuration page is displayed (Figure 6-37). |
| **2** | Set the SNTP State attribute to **Disabled**. The manual clock attributes are displayed. |
| **3** | Review and update the manual clock attributes (Table 6-9). |
| **4** | Select **Submit Updated Configuration**. |

**Figure 6-37** Time Configuration page (SNTP disabled)

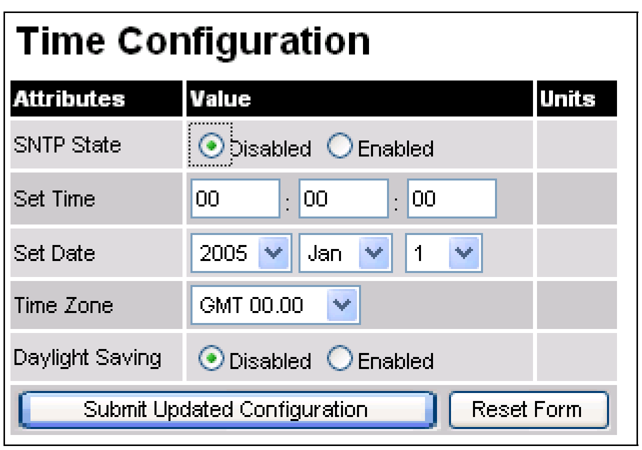


**Table 6-9** Manual clock attributes

| Attribute | Meaning |
|---|---|
| SNTP State | 'Disabled' means that the unit will keep time without connecting to a networked time server. |
| Set Time | Set hours, minutes and seconds. |
| Set Date | Set year, month and day. |
| Time Zone | Set the time zone offset from Greenwich Mean Time (GMT). |
| Daylight Saving | 'Disabled' means that daylight saving adjustments will not be applied to the time. 'Enabled' means that daylight saving adjustments will be applied, according to local rules. |

## Setting the real-time clock to synchronize using SNTP

To set the clock to synchronize with a networked time server, proceed as follows:

**Procedure 6-20** Set the real-time clock using SNTP

| | |
|---|---|
| **1** | Select menu option **Management, Time.** The Time Configuration page is displayed. |
| **2** | Set the SNTP State attribute to **Enabled**. The SNTP clock attributes are displayed (Figure 6-38). |
| **3** | Review and update the SNTP clock attributes (Table 6-10). |
| **4** | Select **Submit Updated Configuration**. |

**Figure 6-38** Time Configuration page (SNTP enabled)

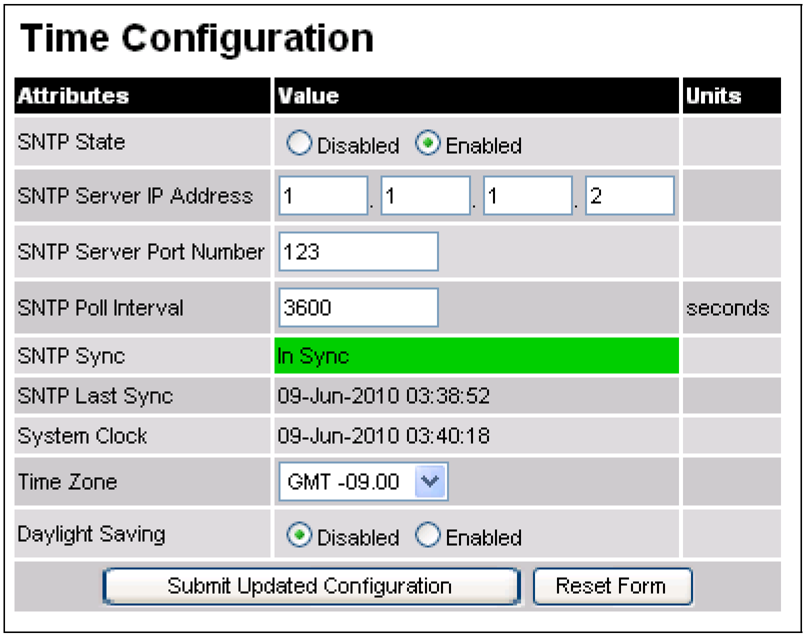



**Table 6-10** SNTP clock attributes

| Attribute | Meaning |
|---|---|
| SNTP State | 'Enabled' means that the CMU will obtain accurate date and time updates from a networked time server. |
| SNTP Server IP Address | Enter the IP address of the networked SNTP server. |
| SNTP Server Port Number | Enter the port number of the networked SNTP server. By convention the default value for the port number is 123. |
| SNTP Poll Interval | Enter the period at which the SNTP client polls the server for time correction updates (default 1 hour). If an SNTP poll fails, the client will automatically perform three retries before waiting for the user defined poll period. |
| SNTP Sync | This shows the current status of SNTP synchronization. If 'No Sync' is displayed, then review the SNTP Server IP Address and Port Number. A change of state may generate an SNMP trap or SMTP email alert. |
| SNTP Last Sync | This shows the date and time of the last SNTP synchronization. |

| Attribute | Meaning |
|---|---|
| System Clock | This displays the local time, allowing for the Time Zone and Daylight Saving settings. |
| Time Zone | Set the time zone offset from Greenwich Mean Time (GMT). |
| Daylight Saving | 'Disabled' means that daylight saving adjustments will not be applied to the time.<br>'Enabled' means that daylight saving adjustments will be applied to the time, according to local rules. |

# Task 14: Setting up SNMP agent

If SNMP is enabled, when an event occurs, the SNMP agent on the unit sends a trap to whatever SNMP trap receivers have been configured.

Depending upon which SNMP version is required, choose one of the following procedures::

- Configuring generation of SNMPv3 notifications on page 6-61
- Configuring generation of SNMPv1/2c notifications on page 6-70

## Configuring generation of SNMPv3 notifications

Perform this task to enable the system to generate Simple Network Management Protocol version 3 (SNMPv3) traps.

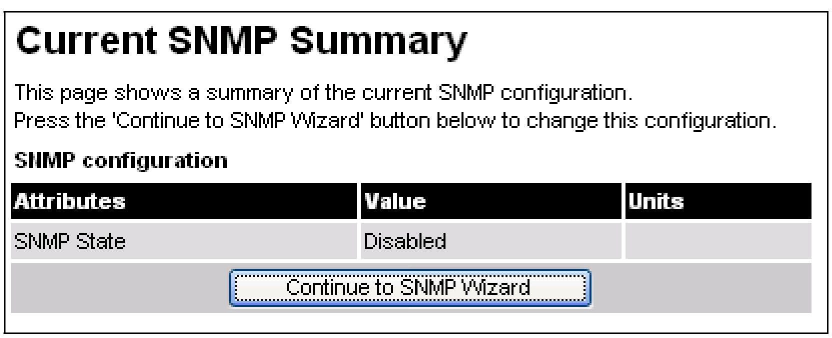
### Starting SNMP wizard

To start the SNMP wizard, proceed as follows:

**Procedure 6-21** Start SNMP wizard

| | |
|---|---|
| **1** | Select menu option **Management, SNMP**. The Current SNMP Summary page is displayed (Figure 6-39). |
| **2** | Review the summary. |
| **3** | If any updates are required, select **Continue to SNMP Wizard**. |

**Figure 6-39** Current SNMP Summary page (when SNMP is disabled)



## Step 1: SNMP configuration (for SNMPv3)

To configure SNMPv3 notifications, proceed as follows:

**Procedure 6-22** Configure SNMP notifications (for SNMPv3)

| | |
|---|---|
| **1** | When the Step 1: SNMP Configuration page is displayed, set SNMP State to 'Enabled' and set SNMP Version to 'v3'. The page is redisplayed with SNMPv3 attributes (Figure 6-40). |
| **2** | Update the attributes (Table 6-11). |
| **3** | Select **Next**. |
| **4** | The next step depends upon which SNMP Security Mode is selected:<br>If it is 'Web-based', go to Step 2: SNMP user policy configuration (for SNMPv3) on page 6-63.<br>If it is 'MIB-based', go to Confirming SNMP configuration (for SNMPv3) on page 6-68. |

**Figure 6-40** Step 1: SNMP Configuration page (for SNMPv3)

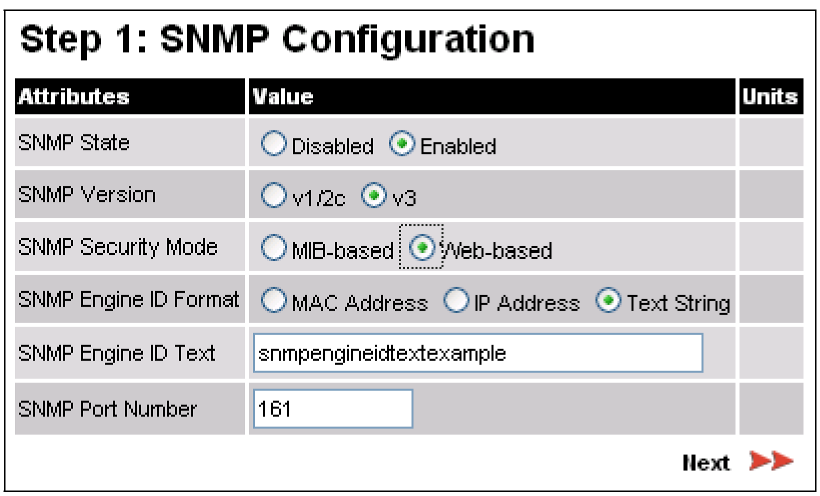


**Table 6-11** Step 1: SNMP Configuration attributes (for SNMPv3)

| Attribute | Meaning |
|---|---|
| SNMP Security Mode | 'MIB-based' means that SNMPv3 security parameters are managed via SNMP MIBs.<br><br>'Web-based' means that the SNMPv3 security parameters are not available over SNMP, but instead are configured using the SNMP Accounts page, as described in Step 2: SNMP user policy configuration (for SNMPv3) on page 6-63. |
| SNMP Engine ID Format | Specifies whether the Engine ID is generated from the MAC Address, IP Address or Text String. |
| SNMP Engine ID Text | Only enabled when SNMP Engine ID Format is set to 'Text String'. Text used to generate the SNMP Engine ID. |
| SNMP Port Number | Enter the port that the SNMP agent is listening to for commands from a management system. |

## Step 2: SNMP user policy configuration (for SNMPv3)

If the chosen SNMP Security Mode is 'Web-based', then SNMP user accounts must be configured to access the unit. SNMP users may have one of two security profiles: 'System administrator' or 'Read only'.

To configure SNMP accounts, proceed as follows:

**Procedure 6-23** Configure SNMP user policy (for SNMPv3)

| | |
|---|---|
| **1** | The Step 2: SNMP User Policy Configuration page is displayed (Figure 6-41). |
| **2** | Update the web-based security profile attributes (Table 6-12). These will determine which authentication and privacy protocols are required for SNMP users with roles 'System administrator' and 'Read only'. |
| **3** | Select **Next**. |

**Figure 6-41** Step 2: SNMP User Policy Configuration page (for SNMPv3)

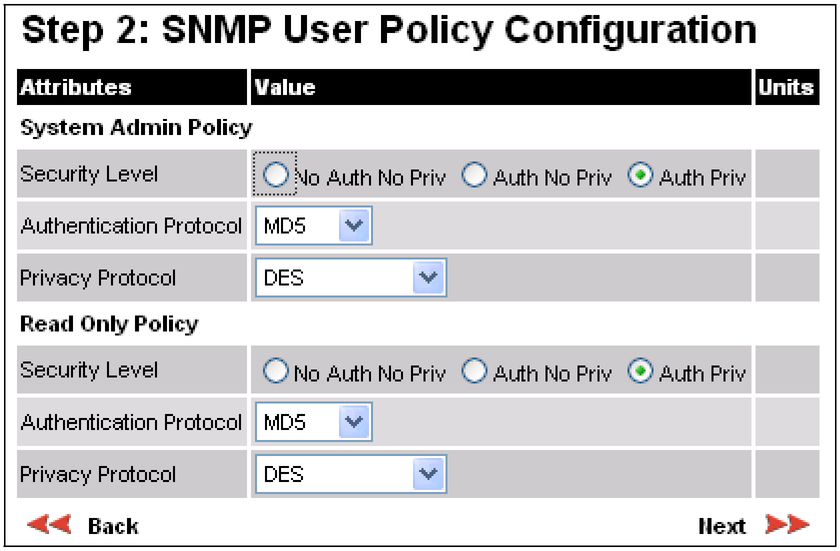



**Table 6-12** Step 2: SNMP User Policy Configuration attributes (for SNMPv3)

| Attribute | Meaning |
|---|---|
| Security Level | Defines the security level and associated protocols that are required to allow SNMP users to access the system.<br>'No Auth No Priv' means that users are not required to use authentication or privacy protocols.<br>'Auth No Priv' means that users are required to use only authentication protocols.<br>'Auth Priv' means that users are required to use both authentication and privacy protocols. |
| Authentication Protocol | The authentication protocol to be used to access the system via SNMP. This is disabled when Security Level is set to 'No Auth No Priv'.<br>'MD5' means Message Digest Algorithm.<br>'SHA' means NIST FIPS 180-1, Secure Hash Algorithm SHA-1. |

| Attribute | Meaning |
|---|---|
| Privacy Protocol | The privacy protocol to be used to access the system via SNMP. This is disabled when Security Level is set to 'No Auth No Priv' or 'Auth No Priv'.<br>'DES' means Data Encryption Standard (DES) symmetric encryption protocol.<br>'AES' means Advanced Encryption Standard (AES) cipher algorithm.<br>NOTE<br>A user configured to use AES privacy protocol will not be able to transmit and receive encrypted messages unless the license key enables the AES capability. |

## Step 3: SNMP user accounts configuration (for SNMPv3)

To configure SNMP user accounts, proceed as follows:

**Procedure 6-24** Configure SNMP user accounts (for SNMPv3)

| | |
|---|---|
| **1** | The Step 3: SNMP User Accounts Configuration page is displayed (Figure 6-42). |
| **2** | Update the individual user attributes (Table 6-13) for up to 10 SNMP users. |
| **3** | Select **Next**. |

**Figure 6-42** Step 3: SNMP User Accounts Configuration page (for SNMPv3)

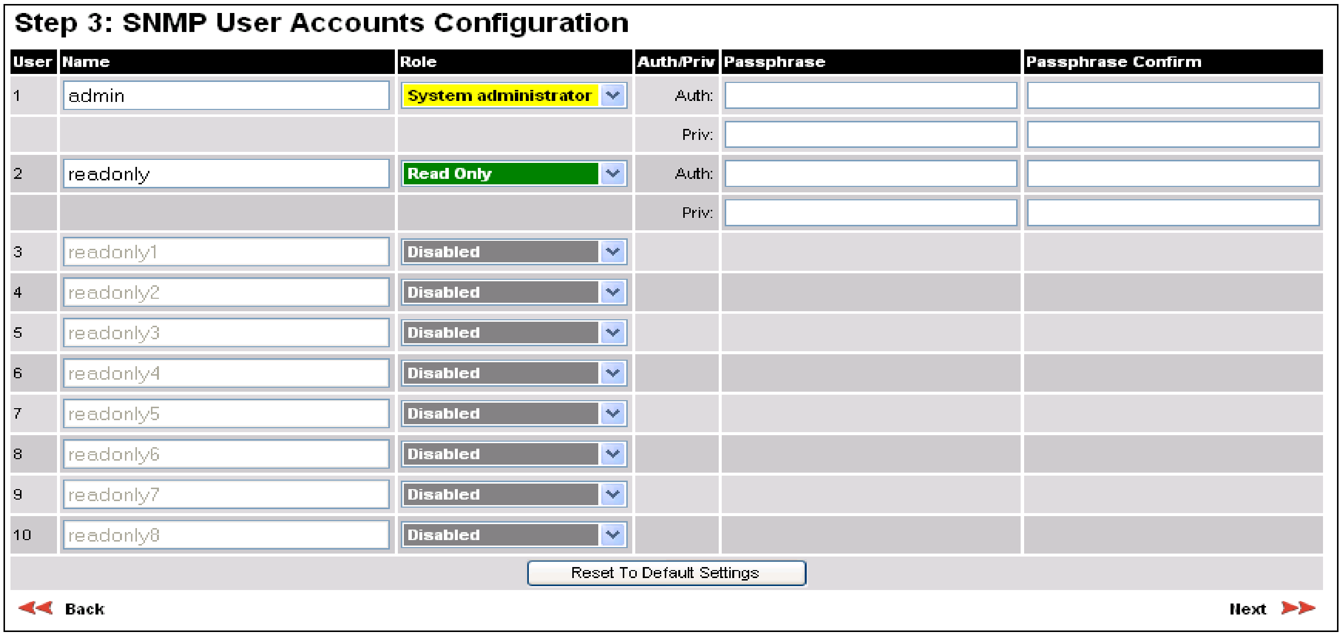



**Table 6-13** Step 3: SNMP User Accounts Configuration attributes (for SNMPv3)

| Attribute | Meaning |
|---|---|
| Name | Name to be used by the SNMP user to access the system. |
| Role | Selects which of the two web-based security profiles are applied to this user: 'System administrator' or 'Read only'.<br><br>Select 'Disabled' to disable the SNMP account. |
| Auth/Priv | Indicates whether the Passphrase applies to authentication or privacy protocols. |
| Passphrase | The phrase to be entered by this SNMP user to access the system using an authentication or privacy protocol. Length must be between 8 and 32 characters. May contain spaces.<br><br>The 'Auth:' Passphrase is hidden when Security Level for this user's Role is set to 'No Auth No Priv'.<br><br>The 'Priv:' Passphrase is hidden when Security Level for this user's Role is set to 'No Auth No Priv' or 'Auth No Priv'. |
| Passphrase Confirm | Passphrase must be reentered to confirm it has not been mis-keyed. |

## Step 4: SNMP trap configuration (for SNMPv3)

To configure SNMP traps, proceed as follows:

**Procedure 6-25** Configure SNMP traps (for SNMPv3)

| | |
|---|---|
| **1** | The Step 4: SNMP Trap Configuration page is displayed (Figure 6-43). |
| **2** | Update the attributes (Table 6-14). |
| **3** | Select **Next**. |

**Figure 6-43** Step 4: SNMP Trap Configuration page (for SNMPv3)

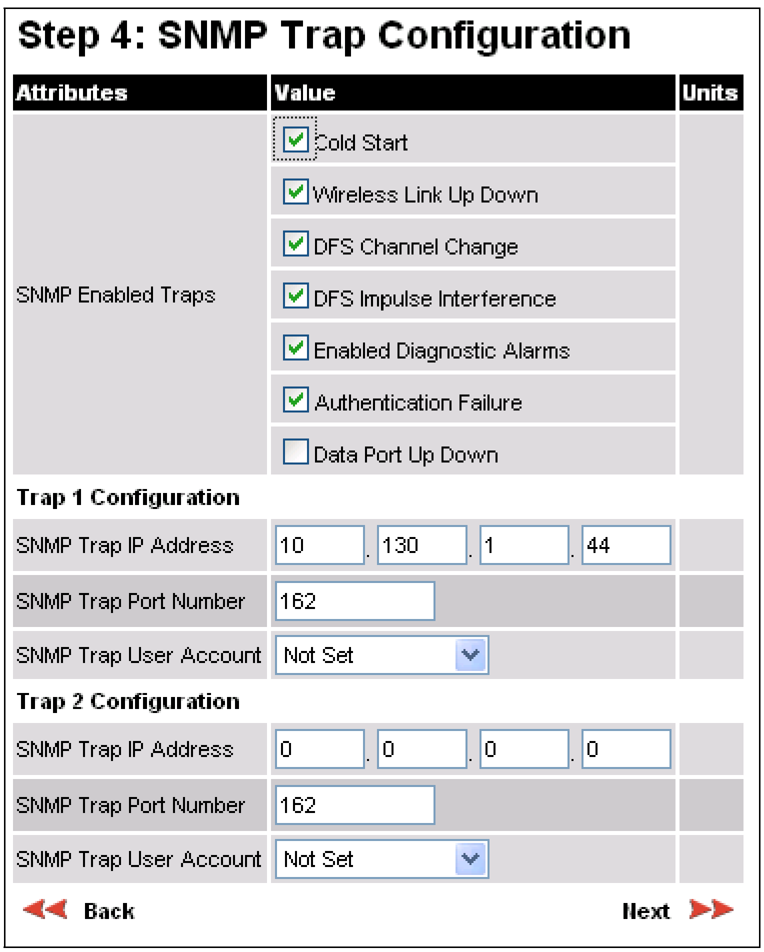


**Table 6-14** Step 4: SNMP Trap Configuration attributes (for SNMPv3)

| Attribute | Meaning |
|---|---|
| SNMP Enabled Traps | Select the events that will generate SNMP traps. |
| SNMP Trap IP Address 1 | The IP address of the first SNMP server (trap receiver). This will normally be the network management system, but it may be a separate trap receiver.<br>Enter zeros to disable logging on the first SNMP server. |
| SNMP Trap Port Number 1 | The server 1 port at which SNMP traps are received. |
| SNMP Trap User Account 1 | The user name (and associated protocols) to use when sending SNMP traps to server 1. |
| SNMP Trap IP Address 2 | The IP address of the second SNMP server (trap receiver). This will normally be the network management system, but it may be a separate trap receiver.<br>Enter zeros to disable logging on the second SNMP server. |
| SNMP Trap Port Number 2 | The server 2 port at which SNMP traps are received. |
| SNMP Trap User Account 2 | The user name (and associated protocols) to use when sending SNMP traps to server 2. |

## Confirming SNMP configuration (for SNMPv3)

When the Confirm SNMP Configuration page (Figure 6-44) is displayed, review the settings and select either **Back** or **Confirm SNMP Configuration and Reboot**. When the settings are confirmed, the unit reboots.

**Figure 6-44** Confirm SNMP Configuration page (for SNMPv3)

## Confirm SNMP Configuration

| Attributes | Value | Units |
|---|---|---|
| SNMP State | Enabled | |
| SNMP Version | v3 | |
| SNMP Security Mode | Web-based | |
| SNMP Engine ID Format | Text String | |
| SNMP Engine ID Text | | |
| SNMP Port Number | 161 | |
| **System Admin Policy** | | |
| Security Level | Auth Priv | |
| Authentication Protocol | MD5 | |
| Privacy Protocol | DES | |
| **Read Only Policy** | | |
| Security Level | Auth No Priv | |
| Authentication Protocol | MD5 | |
| **User 1** | | |
| Name | admin | |
| Role | System administrator | |
| **User 2** | | |
| Name | readonly | |
| Role | Read Only | |
| **Trap Configuration** | | |
| SNMP Enabled Traps | ☑ Cold Start<br>☑ Wireless Link Up Down<br>☑ DFS Channel Change<br>☑ DFS Impulse Interference<br>☑ Enabled Diagnostic Alarms<br>☑ Authentication Failure<br>☐ Data Port Up Down | |
| **Trap 1 Configuration** | | |
| SNMP Trap IP Address | 10.130.1.44 | |
| SNMP Trap Port Number | 162 | |
| SNMP Trap User Account | Not Set | |
| **Trap 2 Configuration** | | |
| SNMP Trap IP Address | 0.0.0.0 | |
| SNMP Trap Port Number | 162 | |
| SNMP Trap User Account | Not Set | |

Confirm SNMP Configuration and Reboot

Back

# Configuring generation of SNMPv1/2c notifications

Perform this task to enable the system to generate Simple Network Management Protocol version 1 or 2c (SNMPv1 or SNMPv2c) traps.

## Start SNMP wizard

To start the SNMP wizard, proceed as follows:

**Procedure 6-26** Start SNMP wizard

| | |
|---|---|
| **1** | Select menu option **Management, SNMP**. The Current SNMP Summary page is displayed (Figure 6-39). |
| **2** | Review the summary. |
| **3** | If any updates are required, select **Continue to SNMP Wizard**. |

## Step 1: SNMP Configuration (for SNMPv1/2c)

To configure SNMPv1 or SNMPv2c notifications, proceed as follows:

**Procedure 6-27** Configure SNMP notifications (for SNMPv1/2c)

| | |
|---|---|
| **1** | When the Step 1: SNMP Configuration page is displayed, set SNMP State to 'Enabled' and set SNMP Version to 'v1/2c'. The page is redisplayed with SNMPv1/2c attributes (Figure 6-45). |
| **2** | Update the attributes (Table 6-15). |
| **3** | Select **Next**. |

**Figure 6-45** Step 1: SNMP Configuration page (for SNMPv1/2c)

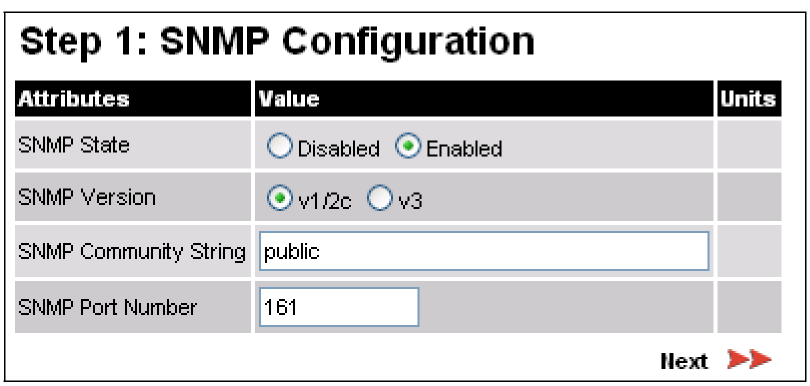


**Table 6-15** Step 1: SNMP Configuration attributes (for SNMPv1/2c)

| Attribute | Meaning |
|---|---|
| SNMP Community String | The SNMP community string acts like a password between the network management system and the distributed SNMP clients (PTP 300 or PTP 500 ODUs). Only if the community string is configured correctly on all SNMP entities can the flow of management information take place. By convention the default value is set to 'public'. |
| SNMP Port Number | Enter the port that the SNMP agent is listening to for commands from a management system. |

## Step 2: SNMP Trap Configuration (for SNMPv1/2c)

To configure SNMP traps, proceed as follows:

**Procedure 6-28** Configure SNMP traps (for SNMPv1/2c)

| | |
|---|---|
| 1 | The Step 2: SNMP Trap Configuration page is displayed (Figure 6-46). |
| 2 | Update the attributes (Table 6-16). |
| 3 | Select **Next**. |

**Figure 6-46** Step 2: SNMP Trap Configuration page (for SNMPv1/2c)

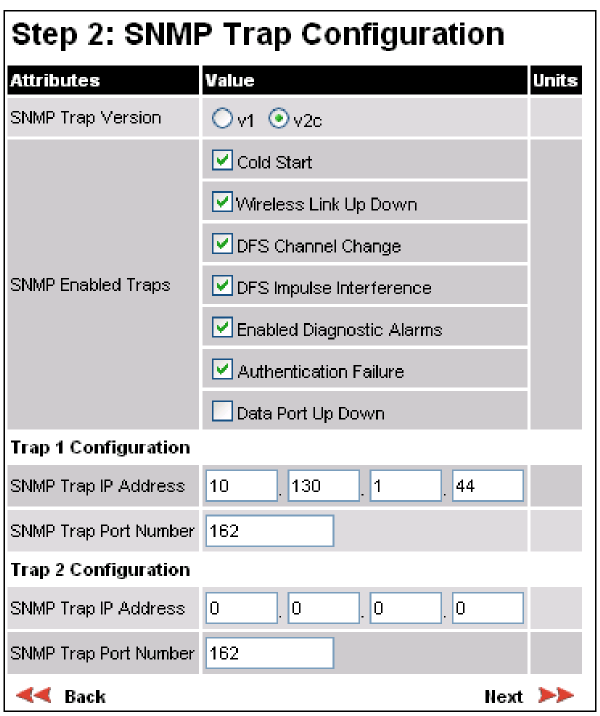


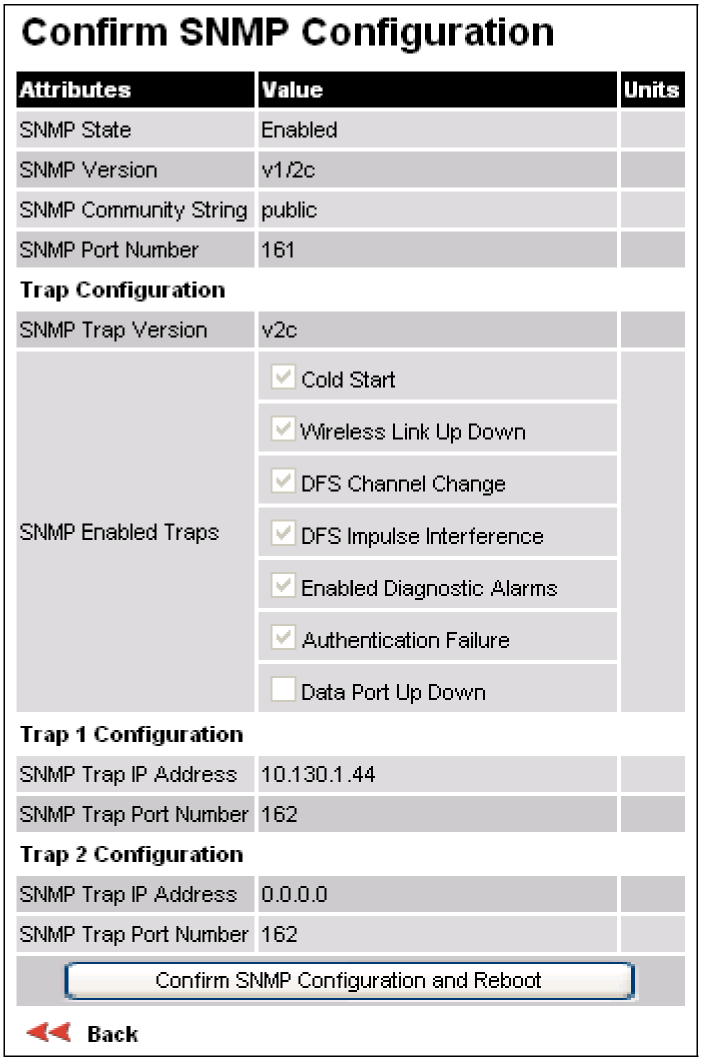
**Table 6-16** Step 2: SNMP Trap Configuration attributes (for SNMPv1/2c)

| Attribute | Meaning |
| --- | --- |
| SNMP Trap Version | Select the SNMP protocol version to use for SNMP traps: 'v1' or 'v2c'. |
| SNMP Enabled Traps | Select the events that will generate SNMP traps. |
| SNMP Trap IP Address 1 | The IP address of the first SNMP server (trap receiver). This will normally be the network management system, but it may be a separate trap receiver.<br><br>Enter zeros to disable logging on the first SNMP server. |
| SNMP Trap Port Number 1 | The server 1 port at which SNMP traps are received. |
| SNMP Trap IP Address 2 | The IP address of the second SNMP server (trap receiver). This will normally be the network management system, but it may be a separate trap receiver.<br><br>Enter zeros to disable logging on the second SNMP server. |
| SNMP Trap Port Number 2 | The server 2 port at which SNMP traps are received. |

## Confirm SNMP Configuration (for SNMPv1/2c)

When the Confirm SNMP Configuration page (Figure 6-47) is displayed, review the settings and select either **Back** or **Confirm SNMP Configuration and Reboot**. When the settings are confirmed, the unit reboots.

**Figure 6-47** Confirm SNMP Configuration page (for SNMPv1/2c)



Confirm SNMP Configuration

| Attributes | Value | Units |
|---|---|---|
| SNMP State | Enabled | |
| SNMP Version | v1/2c | |
| SNMP Community String | public | |
| SNMP Port Number | 161 | |
| **Trap Configuration** | | |
| SNMP Trap Version | v2c | |
| SNMP Enabled Traps | ☑ Cold Start<br>☑ Wireless Link Up Down<br>☑ DFS Channel Change<br>☑ DFS Impulse Interference<br>☑ Enabled Diagnostic Alarms<br>☑ Authentication Failure<br>☐ Data Port Up Down | |
| **Trap 1 Configuration** | | |
| SNMP Trap IP Address | 10.130.1.44 | |
| SNMP Trap Port Number | 162 | |
| **Trap 2 Configuration** | | |
| SNMP Trap IP Address | 0.0.0.0 | |
| SNMP Trap Port Number | 162 | |

Confirm SNMP Configuration and Reboot

Back

# Task 15: Configuring alarms and messages

This task consists of the following procedures:

- Configuring generation of diagnostics alarms on page 6-74
- Configuring generation of email messages on page 6-75

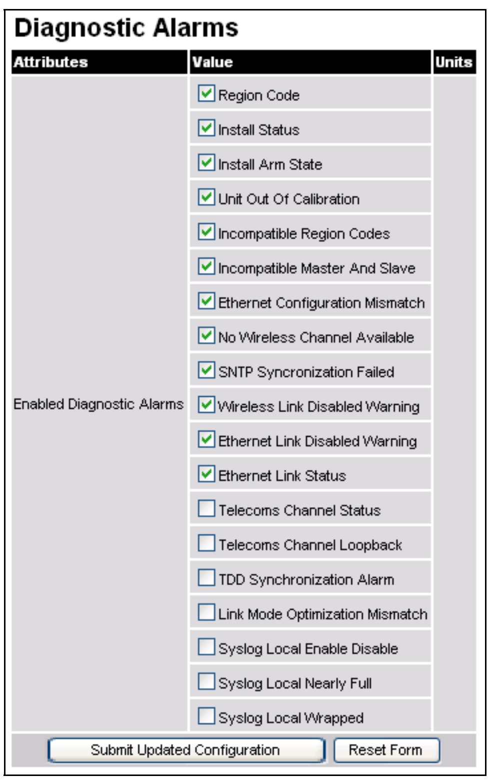
## Configuring generation of diagnostics alarms

To select which diagnostic alarms will be notified to the system administrator:

**Procedure 6-29** Configure diagnostic alarms

| | |
|---|---|
| **1** | Select menu option **Management, Diagnostic Alarms**. The Diagnostic Alarms page is displayed (Figure 6-48). |
| **2** | Tick the boxes against the required alarms. These alarms are described in Alarm display on page 7-7. |
| **3** | Select **Submit Updated Configuration**. |

**Figure 6-48** Diagnostic Alarms page



# Configuring generation of email messages

To enable the system to generate Simple Mail Transfer Protocol (SMTP) email messages to notify the system administrator when certain events occur, proceed as follows:

**Procedure 6-30** Configure SMTP messages

| | |
|---|---|
| **1** | Select menu option **Management, Email**. The Email Configuration page is displayed (Figure 6-49). |
| **2** | Update the Email Configuration attributes (Table 6-17). |
| **3** | Select **Submit Updated Configuration**. The Configuration Change Reboot dialog is displayed. |
| **4** | Select **Reboot Wireless Unit**. The Reboot Confirmation dialog is displayed. |
| **5** | Select **OK**. The reboot progress message is displayed. On completion, the unit restarts. |

**Figure 6-49** Email Configuration page

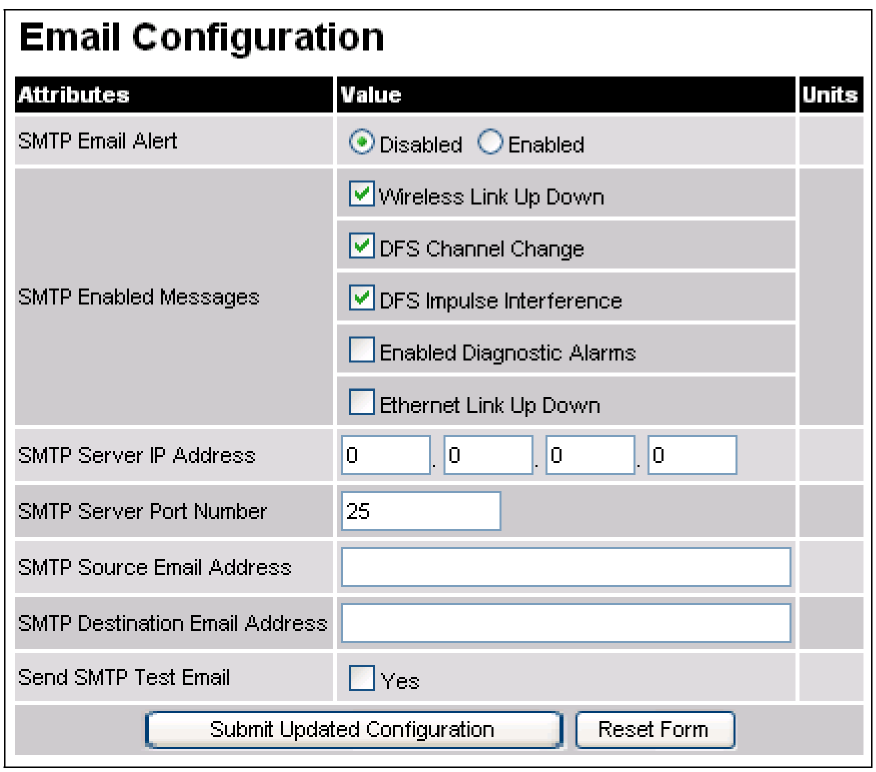


**Table 6-17** Email Configuration attributes

| Attribute | Meaning |
|---|---|
| SMTP Email Alert | Controls the activation of the SMTP client. |
| SMTP Enabled Messages | The SMTP Enabled Messages attribute controls which email alerts the unit will send. |
| SMTP Server IP Address | The IP address of the networked SMTP server. |
| SMTP Server Port Number | The SMTP Port Number is the port number used by the networked SMTP server. By convention the default value for the port number is 25. |
| SMTP Source Email Address | The email address used by the unit to log into the SMTP server. This must be a valid email address that will be accepted by your SMTP Server. |
| SMTP Destination Email Address | The email address to which the unit will send the alert messages. |
| Send SMTP Test Email | Generate and send an email in order to test the SMTP settings. The tick box will self-clear when **Submit** is selected. |

# Task 16: Configuring remote access

## Configuring web-based management attributes

**CAUTION**

If the HTTP, Telnet and SNMP interfaces are all disabled, then it will be necessary to use the Recovery image to reset IP & Ethernet Configuration back to factory defaults to re-enable the interfaces.

To configure HTTP, Telnet and TFTP access, proceed as follows:

**Procedure 6-31** Configure HTTP, Telnet and TFTP access

| | |
|---|---|
| **1** | Select menu option **Management, Web**. The Web-Based Management page is displayed (Figure 6-50). |
| **2** | Update the attributes as required (Table 6-18). |
| **3** | Select **Submit Updated Configuration**. |

**Figure 6-50** Web-Based Management page

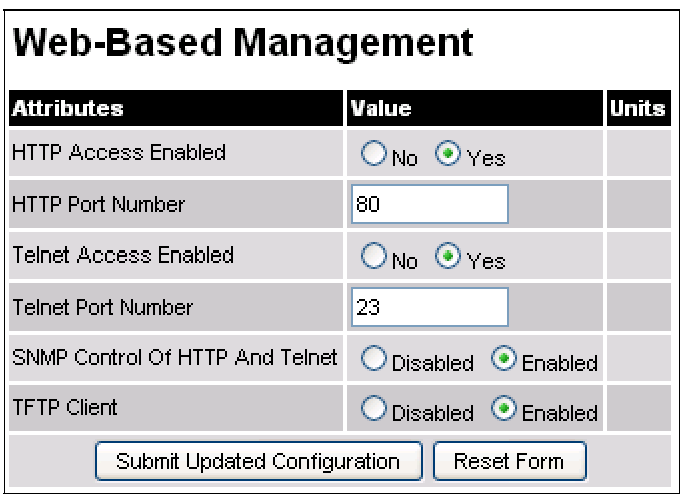


**Table 6-18** Web-Based Management attributes

| Attribute | Meaning |
|---|---|
| HTTP Access Enabled | 'No' means that the unit will not respond to any requests on the HTTP port.<br><br>'Yes' means that the unit will respond to requests on the HTTP port. |
| HTTP Port Number | The port number for HTTP access. A value of zero means the wireless unit uses the default port. |
| Telnet Access Enabled | 'No' means that the unit will not respond to any requests on the Telnet port.<br><br>'Yes' means that the unit will respond to requests on the Telnet port. |
| Telnet Port Number | The port number for Telnet access. A value of zero means the wireless unit uses the default port. |
| SNMP Control of HTTP And Telnet | 'Disabled' means that neither HTTP nor Telnet can be controlled remotely via SNMP.<br><br>'Enabled' means that both HTTP and Telnet can be controlled remotely via SNMP. |
| TFTP Client | 'Disabled' means that the unit will not respond to any TFTP software download requests.<br><br>'Enabled' means that software can be downloaded via TFTP, as described in Upgrading software via remote access on page 7-35. |

# Chapter 7 Operation

This chapter provides instructions for operators of the PTP 300 or PTP 500 web user interface.

The following topics are described in this chapter:

# Web-based management

This section describes the layout and the main menu options of the PTP 300 or PTP 500 web-based management interface. The following topics are covered:

- Accessing the web interface on page 7-2
- Menu navigation bar on page 7-3
- Using the menu options on page 7-4
- Viewing the system summary on page 7-6
- Viewing the system status on page 7-11

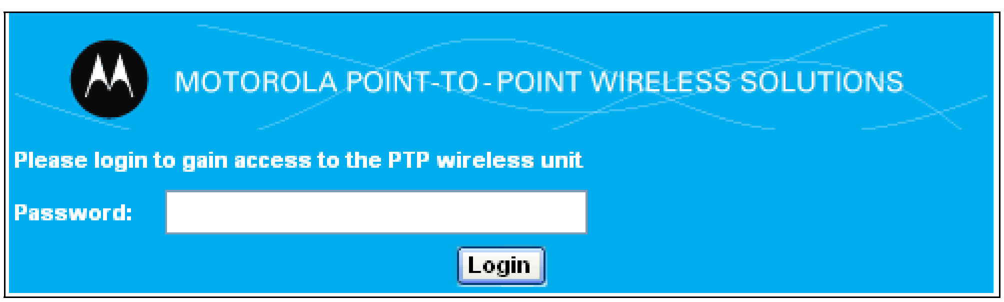
For a general description of the purpose of the web interface, see Web server on page 1-40.

## Accessing the web interface

The web interface is best viewed using a screen resolution of at least 1024 x 768 pixels. The web pages have been tested with Internet Explorer 7, Internet Explorer 8, Firefox 3 and Firefox 3.5. Other browsers have not been tested.

To access the web interface, type the IP address of the unit into the browser address bar and press ENTER. If the login page is not displayed, select menu option **System Administration**. When the login page is displayed (Figure 7-1), enter Password (if set) and select **Login**.

**Figure 7-1** Login page



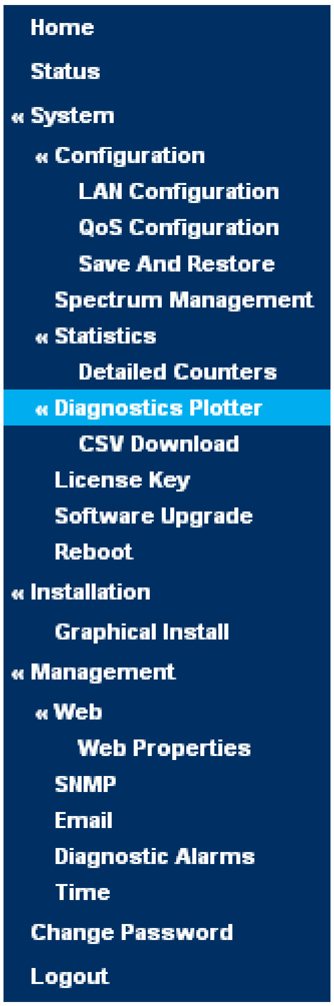

**CAUTION**

To maintain security, always log out at the end of a session by selecting menu option **Logout**.

# Menu navigation bar

All web pages contain the menu navigation bar on the left hand side (Figure 7-2). The menu is used to navigate to other web pages. The currently selected option is always highlighted with a light blue background.

**Figure 7-2** Menu navigation bar



## Using the menu options

Table 7-1 lists the procedures that may be performed from each menu option. Many of these procedures are part of the initial configuration and alignment process described in Chapter 6 Configuration and alignment.

**Table 7-1** Procedures performed from each menu option

| Menu option | Procedures |
|---|---|
| Home | Viewing the system summary on page 7-6<br>Checking that the units are armed on page 6-45 |
| Status | Viewing the system status on page 7-11<br>Checking the installed software version on page 6-17 |
| System | |
| Configuration | Reviewing system configuration attributes on page 6-53<br>Configuring AES encryption on page 6-22 |
| LAN Configuration | Configuring IP and Ethernet attributes on page 6-6 |
| QoS Configuration | Configuring QoS on page 6-12 |
| Telecoms | Performing a telecoms loopback test on page 8-19 |
| Save and Restore | Saving the system configuration on page 6-18<br>Restoring the configuration file on page 7-60 |
| Spectrum Management | Configuring spectrum usage at the master on page 7-20<br>Viewing spectrum usage at the slave on page 7-23<br>Barring channels to avoid TDWR radars (USA) on page 6-43 |
| Statistics | Checking system statistics on page 7-38<br>Resetting system histograms and counters on page 7-45<br>Comparing actual to predicted performance on page 6-55 |
| Detailed Counters | Checking detailed counters on page 7-45<br>Test Ethernet packet errors reported by ODU on page 8-9 |
| Diagnostics Plotter | Using the diagnostics plotter on page 7-48 |

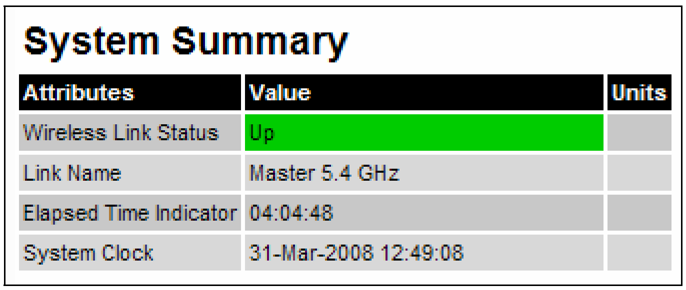
| Menu option | Procedures |
|---|---|
| CSV Download | Downloading diagnostic data on page 7-50 |
| License Key | Checking licensed capabilities on page 6-14<br>Entering a new license key on page 6-16 |
| Software Upgrade | Upgrading to a new software version on page 6-19 |
| Reboot | Rebooting or reviewing reboot reasons on page 7-52 |
| Installation | Starting installation wizard on page 6-26<br>Disarming the units on page 6-52 |
| Graphical Install | Method #3: graphical install on page 6-51 |
| Management | |
| Web | Configuring web-based management attributes on page 6-77 |
| Web Properties | Protecting access to the summary and status pages on page 6-25<br>Checking system statistics on page 7-38 |
| SNMP | Configuring generation of SNMPv3 notifications on page 6-61<br>Configuring generation of SNMPv1/2c notifications on page 6-70 |
| Email | Configuring generation of email messages on page 6-75 |
| Diagnostic Alarms | Configuring generation of diagnostics alarms on page 6-74 |
| Time | Setting the real-time clock on page 6-57 |
| Change Password | Changing password on page 6-24 |
| Logout | |

## Viewing the system summary

To display the System Summary page, select menu option **Home**.

The System Summary page (Figure 7-3) contains a high level summary of the status of the wireless link and associated equipment.

**Figure 7-3** System Summary page



System Summary

| Attributes | Value | Units |
|---|---|---|
| Wireless Link Status | Up | |
| Link Name | Master 5.4 GHz | |
| Elapsed Time Indicator | 04:04:48 | |
| System Clock | 31-Mar-2008 12:49:08 | |

The attributes of the System Summary page are described in Table 7-2.

**Table 7-2** System Summary attributes

| Attribute | Meaning |
|---|---|
| Wireless Link Status | Current status of the wireless link.<br><br>A green background with status text ‘Up’ means that the point-to-point link is established.<br><br>A red background with suitable status text (for example ‘Searching’) indicates that the link is not established. |
| Link Name | The name of the PTP link, as set in the System Configuration page. |
| Elapsed Time Indicator | The time (hh:mm:ss) that has elapsed since the last system reboot.<br><br>The system can reboot for several reasons, for example, commanded reboot from the system reboot webpage, or a power cycle of the equipment. |
| System Clock | The system clock presented as local time, allowing for zone and daylight saving. |
| Status attributes | Status attributes may be displayed in the System Summary page to indicate abnormal states. |

## Alarm display

Whenever system alarms are outstanding, a yellow warning triangle is displayed on the navigation bar. The warning triangle is visible from all web pages. Click the warning triangle to return to the System Summary page and view the alarms.

The example in Figure 7-4 shows the warning triangle in the navigation bar and the Install Arm State alarm displayed in the System Summary page.

The alarms are defined in Table 7-3.

**Figure 7-4** Alarm warning triangle

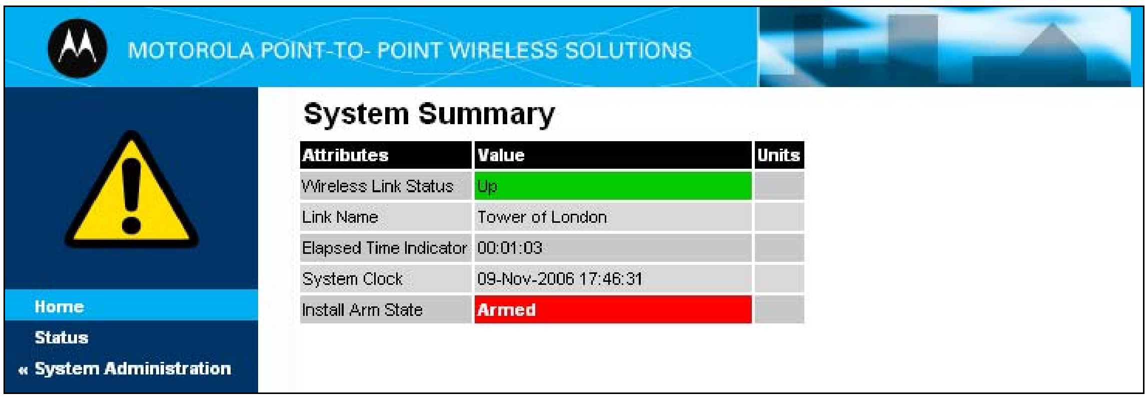



**Table 7-3** System alarms

| Alarm | Meaning |
|---|---|
| Region Code | The region code prohibits the wireless unit from operating outside the regulated limits. An invalid region code indicates a corrupted license key. Note that a change of state may generate an SNMP trap and/or SMTP email alert. |
| Install Status | A non-OK value indicates that signaling was received with the wrong MAC address. Note that it is very unusual to detect this, because units with wrongly configured Target MAC Address will normally fail to establish a wireless link. However, rare circumstances may establish a partial wireless link and detect this situation. NB: A non-OK value on start-up, or a change of value during operation, may generate an SNMP trap and/or SMTP email alert. |

| Alarm | Meaning |
|---|---|
| Install Arm State | This alarm warns when a wireless unit is in installation mode. After installation the wireless unit should be disarmed. This will increase the wireless link's data-carrying capacity and stop the installation tone generator. The wireless link is disarmed from the 'Installation' process, see Disarming the units on page 6-52. A change of state may generate an SNMP trap and/or SMTP email alert. |
| Unit Out Of Calibration | The unit is out of calibration and must be returned to the factory using the RMA process for re-calibration. |
| Incompatible Region Codes | The PTP 300 and PTP 500 Series use region codes to comply with local regulatory requirements governing the transmission of wireless signals in the frequency bands in which it operates. Region codes can only be changed by obtaining a new PTP 300 or PTP 500 Series license key. If this alarm is encountered, the appropriate license keys from the country of operation should be obtained from your distributor. Applying license keys containing the same region codes to both ends of the link will remove the alarm. A change of state may generate an SNMP trap and/or SMTP email alert. |
| Incompatible Master and Slave | A non-zero value indicates that the master and slave ends of the wireless link are different hardware products, or have different software versions. Note that it is very unusual to detect this because incompatible units will normally fail to establish a wireless link. However, some combinations may establish a partial wireless link and detect this situation. Note that a non-zero value may generate an SNMP trap and/or SMTP email alert. |
| Ethernet Configuration Mismatch | The detection of Ethernet fragments (runt packets) when the link is in full duplex is an indication of an auto-negotiation or forced configuration mismatch. Note that a change of state may generate an SNMP trap and/or SMTP email alert. |
| No Wireless Channel Available | Spectrum Management was unable to locate a suitable wireless channel to operate on. Note that a change of state may generate an SNMP trap and/or SMTP email alert. |

| Alarm | Meaning |
|---|---|
| SNTP Synchronization failed | This warning indicates that SNTP has been enabled but that the unit is unable to synchronize with the specified SNTP server. Section Setting the real-time clock on page 6-57 explains how to configure SNTP. Note that a change of state may generate an SNMP trap and/or SMTP email alert. |
| Wireless Link Disabled Warning | This warning is displayed if the Wireless link has been administratively disabled via the SNMP Interface. The Wireless Interface MIB-II ifAdminStatus attribute has been set to DOWN. To enable the Ethernet interface, set the ifAdminStatus attribute to UP. Note that a change of state may generate an SNMP trap and/or SMTP email alert. |
| Ethernet Link Disabled Warning | This warning is displayed if the Ethernet link has been administratively disabled via the SNMP Interface. The Ethernet Interface MIB-II ifAdminStatus attribute has been set to DOWN. To enable the Ethernet interface, set the ifAdminStatus attribute to UP. Note that a change of state may generate an SNMP trap and/or SMTP email alert. |
| Ethernet Link Status | Current status of the Ethernet link. If there are any problems with the Ethernet interface, this alarm will be asserted. This alarm will most likely be seen if the unit has no Ethernet cable plugged into its Ethernet socket. Note that a change of state may generate an SNMP trap and/or SMTP email alert. |
| Telecoms Interface Loopback | The loopback status of the telecoms channel. This is intended for installation testing and should be set to 'None' for normal operation. The wire connections to a unit can be tested by applying a 'Copper' loopback to the local unit. The wireless connection to the remote unit can be tested by applying a 'Wireless' loopback to the remote unit with no loopback on the local unit.<br><br>A change of state may generate an SNMP trap and/or SMTP email alert. The loopback can be disabled from the telecoms configuration sub menu (see Performing a telecoms loopback test on page 8-19). |
| TDD Synchronization Alarm | PTP 500 only. Indicates the current status of the TDD Synchronization (OK, Timing System Failure, Not Synchronized). Note that a change of state may generate an SNMP trap and/or SMTP email alert. |

| Alarm | Meaning |
|---|---|
| Link Mode Optimization Mismatch | The Master and Slave ODUs are configured to use different link mode optimization methods (one is set to IP and the other TDM). |
| Light Of Sight Mode Inactive | PTP 300 only. This warning is displayed if Line Of Sight Mode is set to "LOS" but the link range exceeds 10 km (6.2 miles). The link drops back to "NLOS" modes and data rates. |
| Telecoms Channel Status | Indicates an alarm condition on a telecoms channel (Table 7-4). In remote timing mode the ODU will transmit an Alarm Indication Signal (AIS), consisting of all-ones, from the associated telecoms interface. A change of state may generate an SNMP trap and/or SMTP email alert. |

**Table 7-4** Telecoms channel alarm conditions

| Alarm Condition | Meaning |
|---|---|
| No Signal (Local) | There is no telecoms signal present at the connection to the ODU at the local end. |
| No Signal (Remote) | There is an absence of telecoms data across the wireless link. |
| No Signal (Local and Remote) | The above two alarm conditions occur concurrently. |
| Remote Timing | There is insufficient wireless capacity available to carry telecoms data. Under these conditions telecoms timing information is still sent to keep the telecoms clocks synchronized. |
| No Signal (Local) and Remote Timing | Indicates both no local signal and remote timing. |

# Viewing the system status

To display the System Status page, select menu option **Status**.

The System Status page (Figure 7-5) gives the user a detailed view of the operation of the system from both the wireless and network perspectives.

**Figure 7-5** System Status page

## System Status - Master

**Equipment**

| Attributes | Value | Units |
|---|---|---|
| Link Name | | |
| Site Name | | |
| Software Version | G4-DEV-B771+ wdog | |
| Hardware Version | D00-R02.00-I | |
| Region Code | Region Code 1 | |
| Elapsed Time Indicator | 01:00:41 | |
| **Ethernet / Internet** | | |
| Ethernet Link Status | Copper Link Up | |
| Ethernet Speed And Duplex | 100 Mbps Full Duplex | |
| MAC Address | 00:04:56:10:00:96 | |
| Remote MAC Address | 00:04:56:10:00:a0 | |
| Remote IP Address | 1.1.100.16 | |
| **Telecoms** | | |
| Status | Disabled | |
| **TDD Synchronization** | | |
| TDD Synchronization Inactive | TDD Sync Disabled | |

**Wireless**

| Attributes | Value | Units |
|---|---|---|
| Wireless Link Status | Up | |
| Maximum Transmit Power | 6 | dBm |
| Remote Maximum Transmit Power | 6 | dBm |
| Transmit Power | 6.0, 6.0, 6.0, 6.0 | dBm |
| Receive Power | -55.8, -56.0, -56.1, -56.1 | dBm |
| Vector Error | -18.8, -26.4, -29.0, -29.0 | dB |
| Link Loss | 108.1, 108.0, 107.8, 108.1 | dB |
| Transmit Data Rate | 16.57, 16.54, 1.96, 16.57 | Mbps |
| Receive Data Rate | 16.57, 12.60, 0.63, 16.57 | Mbps |
| Link Capacity | 33.13 | Mbps |
| Transmit Modulation Mode | 64QAM 0.83 (Dual) (5 MHz) | |
| Receive Modulation Mode | 64QAM 0.83 (Dual) (5 MHz) | |
| Link Symmetry | 1 to 1 | |
| Receive Modulation Mode Detail | Running At Maximum Receive Mode | |
| Range | 5.1 | km |
| | | |

The page is subdivided into five categories:

- **Equipment**: This contains the unit's inventory and identification information.
- **Wireless**: This presents the key wireless metrics, which are displayed as a series of measurements.
- **Ethernet/Internet**: This describes the unit's network identity and connectivity.
- **Telecoms**: This describes the unit's E1/T1 telecoms interface parameters.
- **TDD Synchronization**: This shows the status of TDD synchronization (PTP 500 only).

The status page can be configured to refresh itself at an operator defined rate (if the user is logged in as system administrator). The refresh period defaults to 3600 seconds and can easily be changed to refresh at any period between 2 seconds and 3600 seconds. Pressing the **Update Page Refresh Period** button causes a new page refresh period to be adopted by the system. The page refresh mechanism uses an HTML Meta refresh command. Therefore the refresh is always initiated by the local browser and not by the ODU at this interval.

The two ODUs are arranged in a master and slave relationship. The roles of the units in this relationship are displayed in the page title. The master unit will always have the title '- Master', and the slave will always have '- Slave' appended to the 'Systems Status' page title.

The status page attributes are defined in Table 7-5..

**Table 7-5** System Status attributes

| Attribute | Meaning |
|---|---|
| Link Name | The link name is allocated by the system administrator and is used to identify the equipment on the network. The link name attribute is limited to a maximum size of 63 ASCII characters. |
| Site Name | The site name is allocated by the system administrator and can be used as a generic scratch pad to describe the location of the equipment or any other equipment related notes. The site name attribute is limited to a maximum size of 63 ASCII characters. |
| Software Version | The attribute describes the version of software installed on the equipment. The format of the attributes is *FFSSS*-XX-*YY* where *FF* is the frequency variant (2.5, 4.5, 5.4, 5.8 or 5.9 GHz), *SSS* is the System Release, *XX* is the major release version and *YY* is the minor release version. |
| Hardware Version | The hardware version attribute contains all the combined hardware version information. The attribute is formatted as D*XX*-R*YY*-*Z* where D*XX* contain the version of the digital card, R*YY* contains the version of the RF (radio frequency) card and *Z* describes the antenna type which can be I (integrated) or C (connectorized). |

| Attribute | Meaning |
|---|---|
| Region Code | The region code is used by the system to constrain the wireless to operate within regulatory regime of the particular country. The region code is encoded in the product license key. If the operator wishes to change region code, a new license key must be obtained from Motorola or the local point-to-point distributor or system integrator. |
| Elapsed Time Indicator | The elapsed time indicator attribute presents the total time in years, days, hours, minutes and seconds since the last system restart. The system can restart for several reasons, for example commanded reboot from the system reboot web page, or a power cycle of the equipment. |
| Ethernet Link Status | This indicates the current status of the Ethernet link. A state of 'Up' with a green background indicates that an Ethernet link is established. A state of 'Down' with a red background indicates that the Ethernet link is not established. |
| Ethernet Speed and Duplex | The negotiated speed and duplex setting of the Ethernet interface. The speed setting is specified in Mbps.<br><br>Full Duplex data transmission means that data can be transmitted in both directions on a signal carrier at the same time. For example, on a local area network with a technology that has full duplex transmission; one workstation can be sending data on the line while another workstation is receiving data.<br><br>Half Duplex data transmission means that data can be transmitted in both directions on a signal carrier, but not at the same time. For example, on a local area network using a technology that has half duplex transmission, one workstation can send data on the line and then immediately receive data on the line from the same direction in which data was just transmitted. |
| Remote IP Address | Hyperlink to the other side of the Link. The IP address of the peer link is displayed if the Link is UP, otherwise 'unavailable' is displayed. |

| Attribute | Meaning |
|---|---|
| Telecoms Status | Indicate the current status of the telecoms channel. Channels which are disabled during installation are marked as such. Correctly operating channels display "Up" on a green background, but alarm conditions (described in Alarm display on page 7-7) have a red background.<br><br>The Telecoms Latency value, displayed in microseconds, is determined when the wireless link starts and will remain the same for a given wireless configuration. Section Telecoms circuits on page 1-38 describes methods for reducing telecoms latency on links which support high data rate modulation modes.<br><br>Under normal circumstances the unit will freely transition between modulation modes to suit the wireless conditions. The "Single Payload Lock" indicates that the ODU will prevent transitions from Single Payload modes to the higher Dual Payload modes in order to avoid loss of telecoms data. This field appears where such a transition would pass through modes which cannot carry telecoms data. This may be because, in order to control latency, the lowest modulation mode has been set to a higher Single Payload mode.<br><br>In the absence of the Single Payload Lock the wireless will transition to the faster Dual Payload modes as soon as the conditions are appropriate. With the lock enabled, the wireless will dwell in slower Single Payload modes whenever there are operational telecoms links (operational links are shown as "Up" in the telecoms channel field described above). When the lock is actively preventing transitions, the value displayed changes from "Enabled" to "Applied". |
| TDD Synchronization | PTP 500 only. Displays the TDD Synchronization status for the link. For more information, refer to TDD synchronization status on page 7-18. |
| Refresh Page Period | The Status page refreshes automatically according to the setting entered here (in seconds). This attribute is only displayed when the user is logged on as System Administrator. |

| Attribute | Meaning |
|---|---|
| Wireless Link Status | As the attribute name suggests it displays the current status of the wireless link. A state of 'Up' on a green background indicates that a point-to-point link is established. A state of 'Down' on a red background indicates that the wireless link is not established. |
| Maximum Transmit Power | The maximum transmit power that the local wireless unit is permitted to use to sustain a link. |
| Remote Maximum Transmit Power | The maximum transmit power that the remote wireless unit is permitted to use to sustain a link. |
| Transmit Power | Transmit power histogram is expressed in dBm and presented as: max, mean, min, and latest. The max, min and latest are true instantaneous measurements; the mean is the mean of a set of one second means. See Histogram data on page 7-19. |
| Receive Power | Receive power histogram is expressed in dBm and presented as: max, mean, min, and latest. The max, min and latest are true instantaneous measurements; the mean is the mean of a set of one second means. See Histogram data on page 7-19. |
| Vector Error | The vector error measurement compares the received signal's In phase / Quadrature (IQ) modulation characteristics to an ideal signal to determine the composite error vector magnitude. The results are stored in an histogram and expressed in dB and presented as: max, mean, min and latest. The max, min and latest are true instantaneous measurements; the mean is the mean of a set of one second means. The expected range for Vector Error would be approximately -1.5 dB (NLOS link operating at sensitivity limit on BPSK 0.50) to –28 dB (short LOS link running 64QAM 0.83). See Histogram data on page 7-19. |

| Attribute | Meaning |
|---|---|
| Link Loss | The link loss is the total attenuation of the wireless signal between the two point-to-point units. See Histogram data on page 7-19. The link loss calculation presented below:<br>$P_{ll} = P_{T_x} - P_{R_x} + g_{T_x} + g_{R_x}$<br>Where:<br>$P_{ll}$ = Link Loss (dB)<br>$P_{T_x}$ = Transmit power of the remote wireless unit (dBm)<br>$P_{R_x}$ = Received signal power at the local unit (dBm)<br>$g_{T_x}, g_{R_x}$ = Antenna gain at the remote and local units respectively (dBi). The antenna gain of the ODU (23.5 dBi) is used unless one or both of the units is a Connectorized version.<br>For connectorized ODUs, the link loss calculation is modified to allow for the increased antenna gains at each end of the link. |
| Transmit Data Rate | The data rate in the transmit direction, expressed in Mbps and presented as: max, mean, min, and latest in an histogram format. The max, min and latest are true instantaneous measurements; the mean is the mean of a set of one second means. Expected data rates can be found in Data rate calculations on page 4-77. |
| Receive Data Rate | The data rate in the receive direction, expressed in Mbps and presented as: max, mean, min, and latest in an histogram format. The max, min and latest are true instantaneous measurements; the mean is the mean of a set of one second means. Expected data rates can be found in Data rate calculations on page 4-77. |
| Link Capacity | The maximum aggregate data rate capacity available for user traffic, assuming the units have been connected using Gigabit Ethernet. The link capacity is variable and depends on the prevailing wireless conditions as well as the distance (range) between the two wireless units. |

| Attribute | Meaning |
|---|---|
| Transmit Modulation Mode | The modulation mode currently being used on the transmit channel. A list of all the modulation modes can be found in Data rate calculations on page 4-77, where data rate calculations plots are given for each available modulation mode. |
| Receive Modulation Mode | The modulation mode currently being used on the receive channel. A list of all the modulation modes can be found in Data rate calculations on page 4-77, where data rate calculations plots are given for each available modulation mode. |
| Link Symmetry | A ratio that expresses the division between transmit and receive time in the TDD frame. The first number in the ratio represents the time allowed for the transmit direction and the second number represents the time allowed for the receive direction.<br>**NOTE**<br>Link Symmetry is configured at the master ODU only. The appropriate matching Link Symmetry is set at the slave ODU automatically. For example, if Link Symmetry is configured as '2 to 1' at the master ODU, then the slave ODU will be set automatically as '1 to 2'. In this example, the master-slave direction has double the capacity of the slave-master direction. |
| Line Of Sight Mode | PTP 300 only. The current setting of the Line Of Sight Mode control, either 'Enabled' or 'Disabled'. This is hidden unless the line of sight capability is enabled by license key. |

| Attribute | Meaning |
|---|---|
| Receive Modulation Mode Detail | This supplies the user with information regarding the receive modulation mode in use. Possible values are:<br>'Running at maximum receive mode'<br>'Running at user-configured Max Modulation Mode'<br>'Restricted due to byte errors on the wireless link or local Ethernet Tx Fifo Drops'<br>'Restricted because a DFS channel change is in progress'<br>'Restricted due to telecoms acquisition mode'<br>'Restricted due to the low Ethernet link speed'<br>'Limited by the wireless conditions' |
| Range | The range between the two ODUs. This is displayed in km by default, but can be changed to miles by updating the 'Distance Units' attribute to imperial, as described in Protecting access to the summary and status pages on page 6-25. |

## TDD synchronization status (PTP 500 only)

The Status Page displays the TDD Synchronization status for the link.

If TDD Synchronization is not enabled, the Attribute is set to 'TDD Synchronization Inactive' and the Value is set to 'TDD Sync Disabled'.

If TDD Synchronization is enabled and the installation is rebooted, the Attribute is set to 'TDD Synchronization Status' and the Value is set to one of the following:

- 'Locked' (Figure 7-6)
- 'Holdover'
- 'Holdover (Not Connected)'
- 'Acquiring Lock'
- 'No Timing Reference'
- 'Timing System Not Connected' (Figure 7-7)
- 'Initializing'

**Figure 7-6** Status page - TDD enabled and synchronized

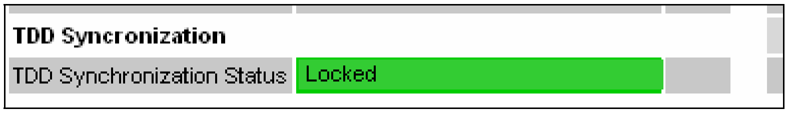
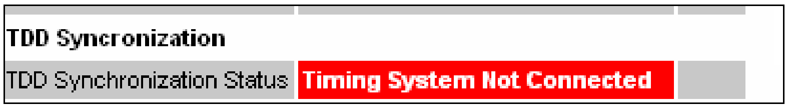



**Figure 7-7** Status page - TDD enabled and not synchronized




## Histogram data

The histogram is calculated over a one hour period. If the equipment has been running for less than one hour, then the histogram is calculated over the current elapsed time. The data used to compute the histogram statistics can be downloaded in an ASCII comma separated value (CSV) format via the diagnostics CSV Download page, see Downloading diagnostic data on page 7-50.

# Managing spectrum

This section describes how to configure the spectrum management feature of the PTP 300 or PTP 500 and how to interpret spectrum management graphical plots.

This section contains the following procedures:


- Configuring spectrum usage at the master on page 7-20
- Viewing spectrum usage at the slave on page 7-23
- Interpreting the spectrum management plots on page 7-25
- Viewing the active channel history on page 7-33
- Viewing historic spectrum management metrics on page 7-34


## Configuring spectrum usage at the master

All spectrum management configuration changes are applied at the master ODU only. These changes are then sent from the master to the slave, so that both master and slave keep identical copies of spectrum management configuration. It is therefore possible to swap master and slave roles on an active link without modifying Spectrum Management configuration.

**NOTE**

Before attempting to improve the performance of the spectrum management algorithm by changing the default configuration, consulting the Motorola Point-to-Point distributor or one of the system field support engineers.

The default channelization can be modified by varying the lower center frequency attribute in the installation wizard, as described in Step 2: Wireless configuration on page 6-31.

To configure spectrum usage at the master, proceed as follows:

**Procedure 7-1** Configure spectrum usage at the master

| | |
|---|---|
| **1** | Log into the master ODU for the link. |
| **2** | Select menu option **System, Spectrum Management**. The Spectrum Management page is displayed (Figure 7-8). |
| **3** | Review and update the configuration attributes (Table 7-6). |
| **4** | Select **Submit configuration changes**. |

**NOTE**

Figure 7-8 illustrates 15 MHz operation; other channel bandwidths are similar. The width of the vertical green bar represents the channel width.

**Figure 7-8** Spectrum Management as seen from the Master

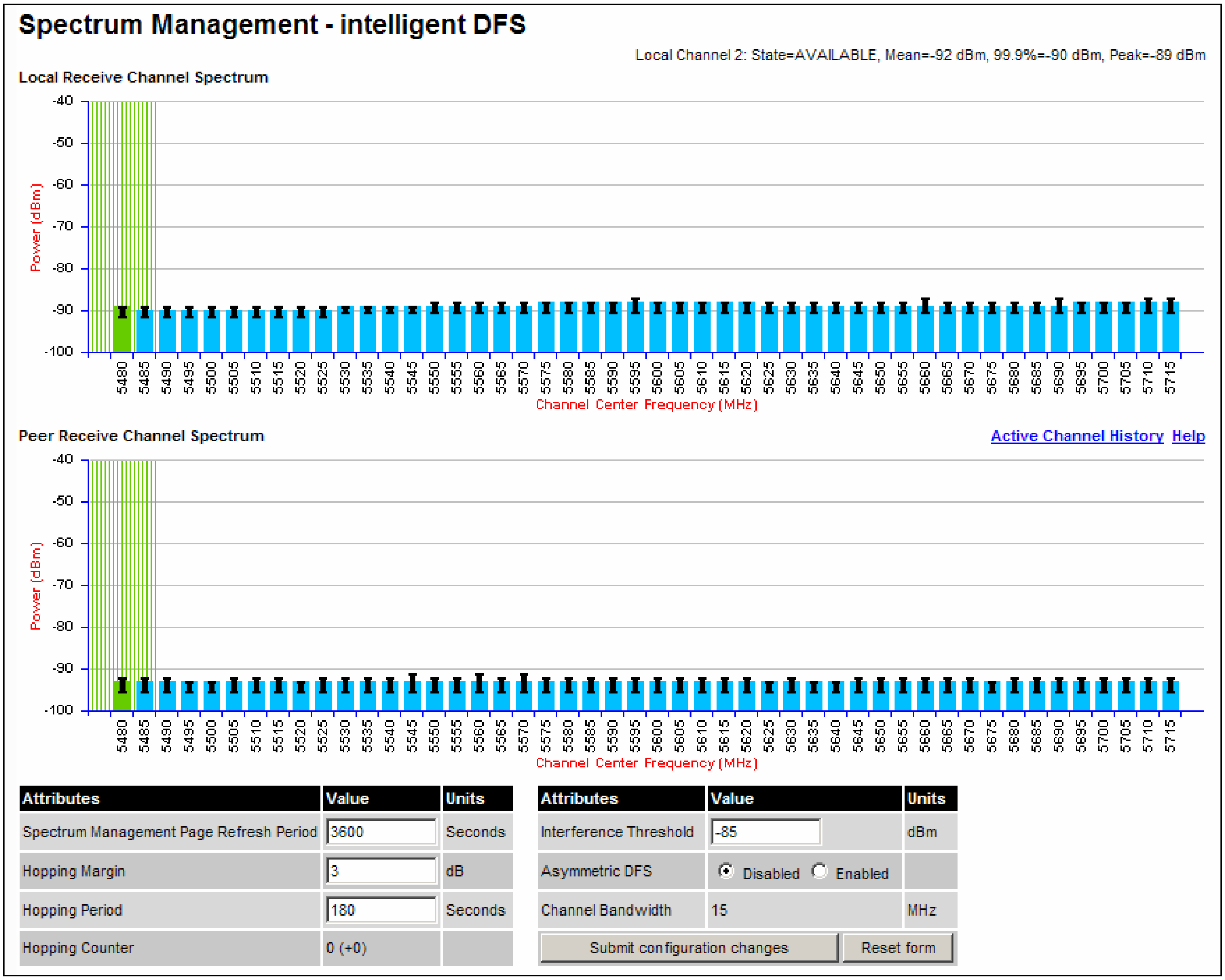


**Table 7-6** Spectrum Management attributes

| Attribute | Meaning |
|---|---|
| Page Refresh Period | The page refreshes automatically according to the setting entered here (in seconds). |
| Hopping Margin | Spectrum Management uses this margin when making a channel hop decision. If the interference level of the target channel is lower than that of the active channel by at least the Hopping Margin, the link will hop to the target channel. The default setting is 3 dB in non-radar regions, or 10 dB in radar regions. |
| Asymmetric DFS | Only displayed in non-radar regions when i-DFS is enabled. The default configuration of symmetric operation constrains the link to operate symmetrically, using the same transmit and receive channels. When in symmetric mode the slave unit will always follow the master. If the master moves to a new channel the slave will hop to the same channel. When the Point-to-Point link is configured as an asymmetric link both the master and slave are free to select the best channel from their own set of local interference metrics. |
| Spectrum Management Control | Only displayed in radar regions. The options are ‘DFS’ and ‘DFS with i-DFS’. |
| Hopping Period | The Spectrum Management algorithm evaluates the metrics every ‘Hopping Period’ seconds (180 seconds by default) looking for a channel with lower levels of interference. If a better channel is located, Spectrum Management performs an automated channel hop. If SNMP or SMTP alerts are enabled an SNMP TRAP or an email alert is sent warning the system administrator of the channel change. |
| Hopping Counter | This is used to record the number of channel hops. The number in the (+) brackets indicates the number of channel changes since the last screen refresh. |

| Attribute | Meaning |
|---|---|
| Interference Threshold | Spectrum Management uses the interference threshold to perform instantaneous channel hops. If the measured interference on a channel exceeds the specified threshold, then i-DFS will instruct the wireless to immediately move to a better channel. If a better channel cannot be found, the system will continue to use the current active channel. (Default –85 dBm). |
| Channel Bandwidth (not configurable) | This shows the value of the variable channel bandwidth selected. |

### Barring a channel

Channels can only be barred or unbarred from the master Spectrum Management web page. Refer to Task 9: Barring channels on page 6-43.

The channel bar will take effect immediately and is not related to the measurement quantization period.

## Viewing spectrum usage at the slave

To view spectrum usage at the slave, proceed as follows:

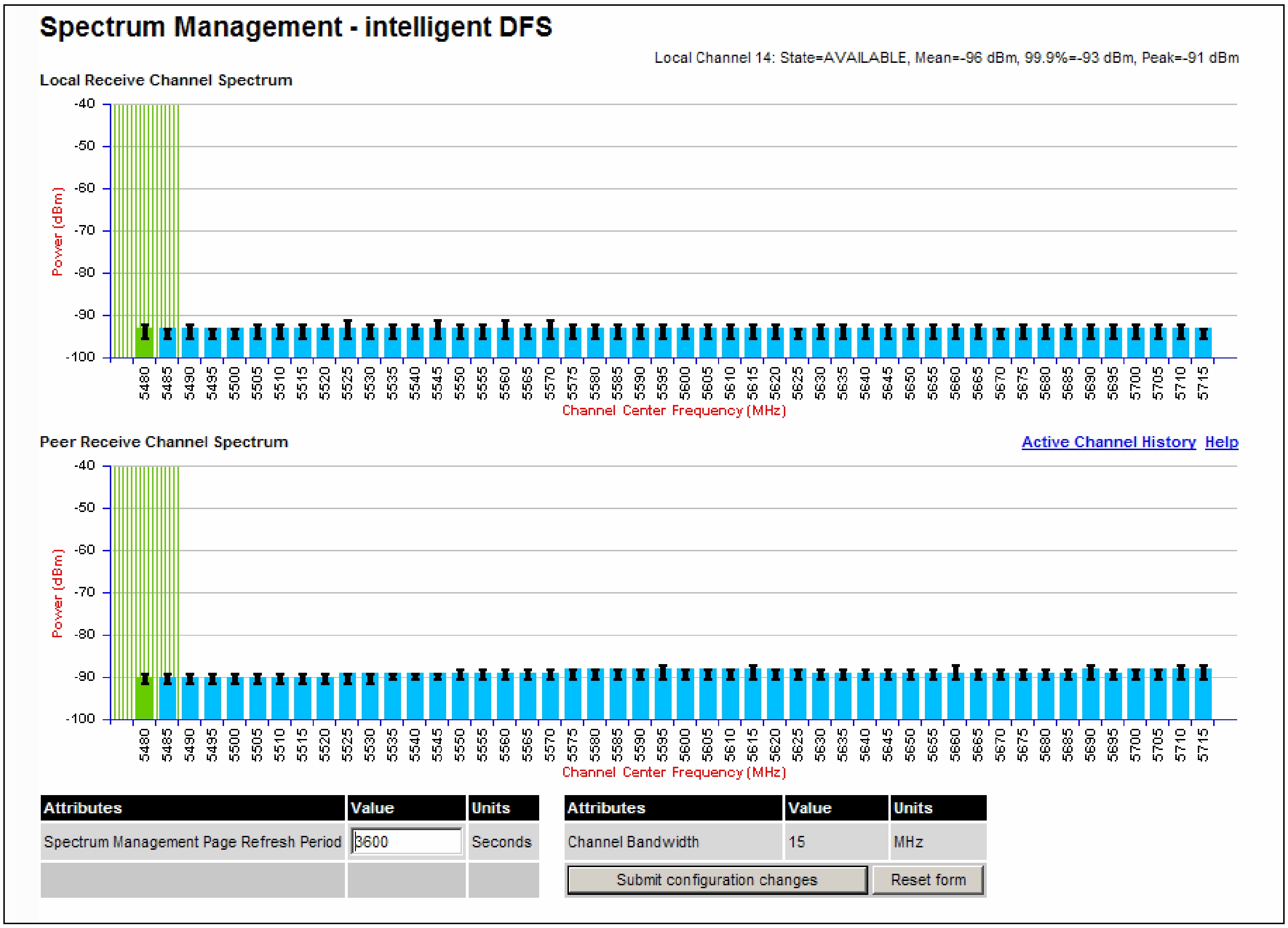
**Procedure 7-2** View spectrum usage at the slave

| | |
|---|---|
| **1** | Log into the slave ODU for the link. |
| **2** | Select menu option **System, Spectrum Management**. The Spectrum Management page is displayed (Figure 7-9). |
| **3** | If necessary, update the Page Refresh Period and select **Submit configuration changes**. |

**NOTE**

Figure 7-9 illustrates 15 MHz operation; other channel bandwidths are similar. The width of the vertical green bar represents the channel width.

**Figure 7-9** Spectrum Management as seen from the Slave



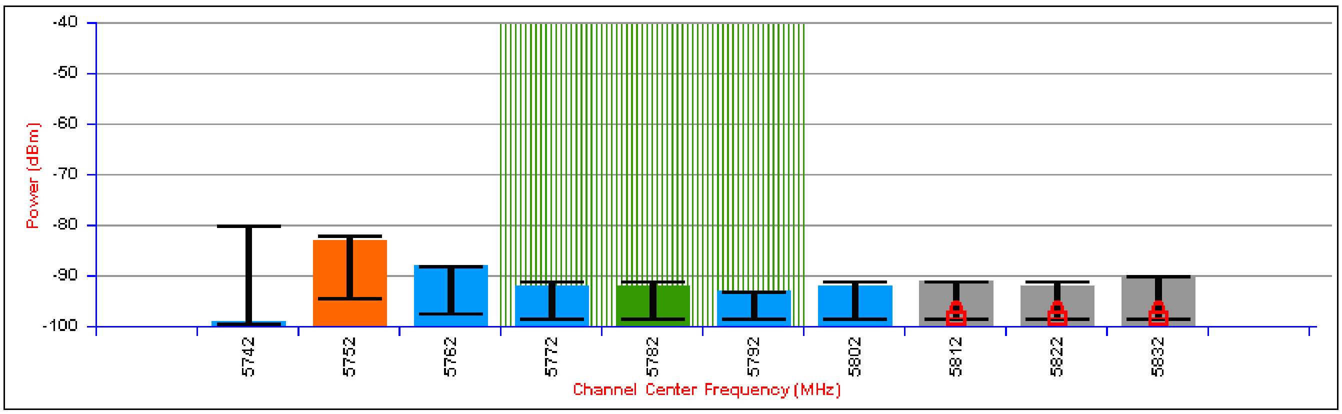
# Interpreting the spectrum management plots

The Spectrum Management pages at the master and slave (Figure 7-8 and Figure 7-9) display two graphical plots:

- Local Receive Channel Spectrum
- Peer Receive Channel Spectrum

A more detailed example of one of these plots is shown in Figure 7-10.

**Figure 7-10** Example spectrum management plot




NOTE

For more information, select the **Help** hyperlink from the Spectrum Management page.

## X axis and Y axis

The X-axis shows a stylized view of the selectable wireless channels. Adjacent channels on the display have a 10 MHz overlap. Channels are displayed separately for clarity. The axis is labeled using the channel center frequencies in MHz.

The Y-axis shows the interference power levels from –100 to –40 dBm.

## Channel states

The active channel (channel 5 in Figure 7-10) is always marked using hatched green and white lines. The width of the hatching is directly proportional the channel bandwidth spectral occupancy of the channel.

The individual channel metrics are displayed using a colored bar and an ‘I’ bar. The colored bar represents the channel state (Table 7-7).

**Table 7-7** Channel states represented in the spectrum management plot

| State | Meaning |
|---|---|
| Active | The channel is currently in use, hosting the Point-to-Point wireless link. |
| Interference | The channel has interference above the interference threshold . |
| Available | The channel has an interference level below the interference threshold and is considered by the Spectrum Management algorithm suitable for hosting the Point-to-Point link. |
| Barred | The system administrator has barred this channel from use. For improved visibility, an additional red ‘lock’ symbol is used to indicate that a channel is barred. |

## Key metrics

The 'I' bar and top of the colored bar represent three key metrics (Table 7-8). The vertical part of the 'I' bar represents the statistical spread between the peak and the mean of the statistical distribution.

**Table 7-8** Key metrics represented in the spectrum management plot

| Metric | Description | How represented |
|---|---|---|
| Peak of Means | The largest mean interference measurement encountered during the quantization period. The peak of means is useful for detecting slightly longer duration spikes in the interference environment. | Upper horizontal bar. |
| Mean of Means | The arithmetic mean of the measured means during a quantization period. The mean of means is a coarse measure of signal interference and gives an indication of the average interference level measured during the quantization period. The metric is not very good at predicting intermittent interference and is included to show the spread between the Mean of Means, the 99.9% Percentile and the Peak of Means. | Lower horizontal bar. |
| 99.9% Percentile of the Means | The value of mean interference measurement which 99.9% of all mean measurements fall below, during the quantization period. The 99.9% percentile metric is useful for detecting short duration repetitive interference that by its very nature has a minimal effect of the mean of means. | Top of the colored bar. |

**NOTE**

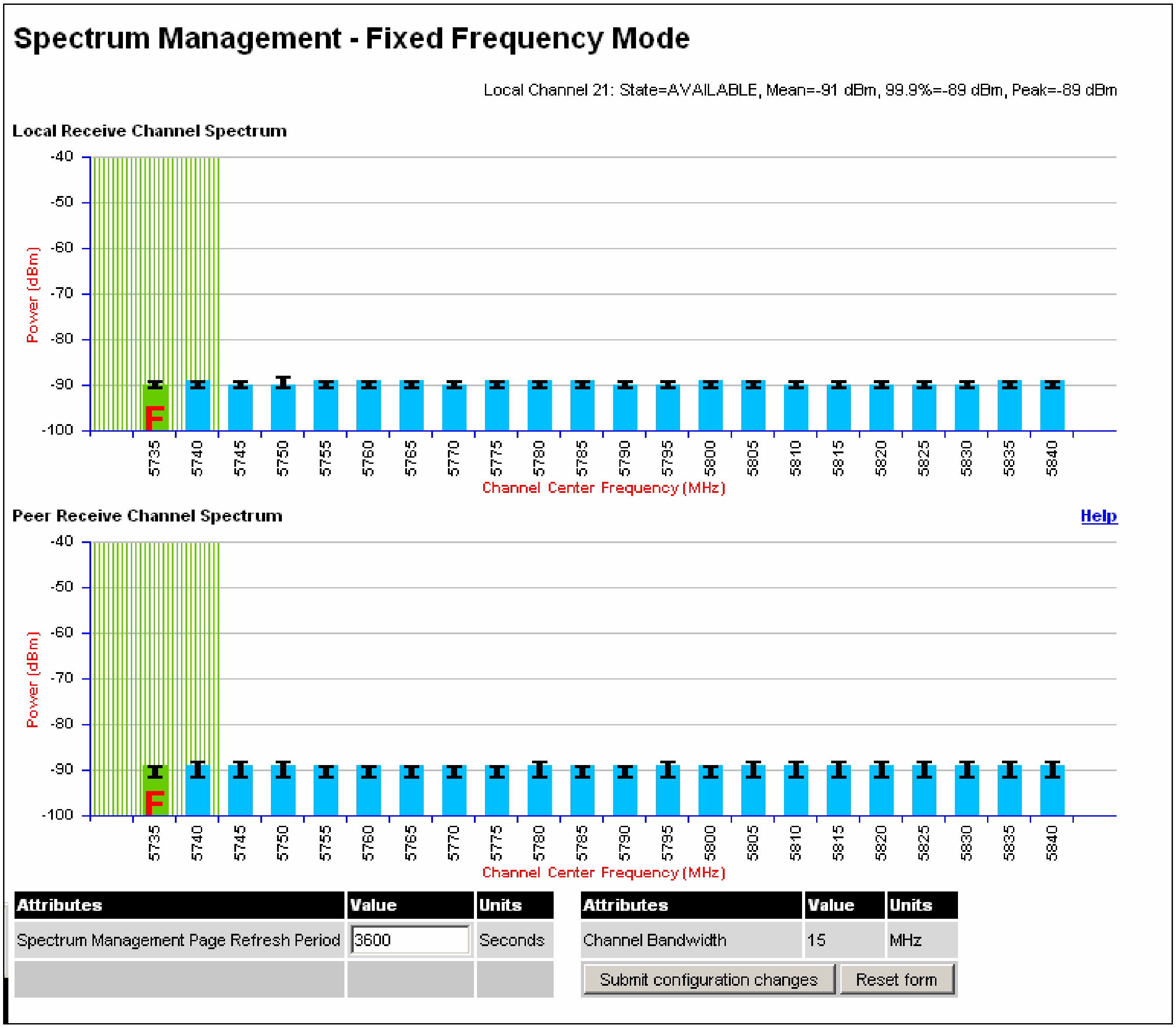
The arithmetic mean is the true power mean and not the mean of the values expressed in dBm.

Spectrum Management uses the 99.9% Percentile as the prime interference measurement. All subsequent references to interference level refer to this percentile measurement.

## Spectrum management in fixed frequency mode

When the link is operating in fixed frequency mode, the Spectrum Management page uses two visual cues (Figure 7-11). The main page title has the 'Fixed Frequency Mode' suffix and the selected channels are identified by a red capital 'F'.

**Figure 7-11** Spectrum Management Fixed Frequency Mode page




Channel barring is disabled in fixed frequency mode; it is not required as dynamic channel hopping is prohibited in this mode.

The only controls available to the master are the Page Refresh Period and Interference Threshold attributes. They will have no effect on the operation of the wireless link and will only effect the generation of the channel spectrum graphics.

The active channel history menu is removed in this mode of operation, as channel hopping is prohibited.

## Spectrum management in radar avoidance mode

When the link is operating in radar avoidance mode, the Spectrum Management page (Figure 7-12 and Figure 7-13) contains the following additional information:

- The main page title has the 'Radar Avoidance' suffix.
- The only controls available to the master are the Interference Threshold attribute. This has no effect on the operation of the wireless link and will only affect the generation of the channel spectrum graphics.
- Extra color coding of the interference histogram is provided (Table 7-9).

When operating with RTTT (Road transport and Traffic Telematics) Avoidance enabled or other regulatory restrictions on channel usage, the page contains the following additional information:

- All channels marked with a 'no entry' symbol with their associated statistics colored black are the prohibited channels. These channels are never used to host the wireless link, but CAC measurements are still taken so that adjacent channel biases can be calculated correctly and so the user can see if other equipment is in use.

**Figure 7-12** Spectrum Management page with radar avoidance - master

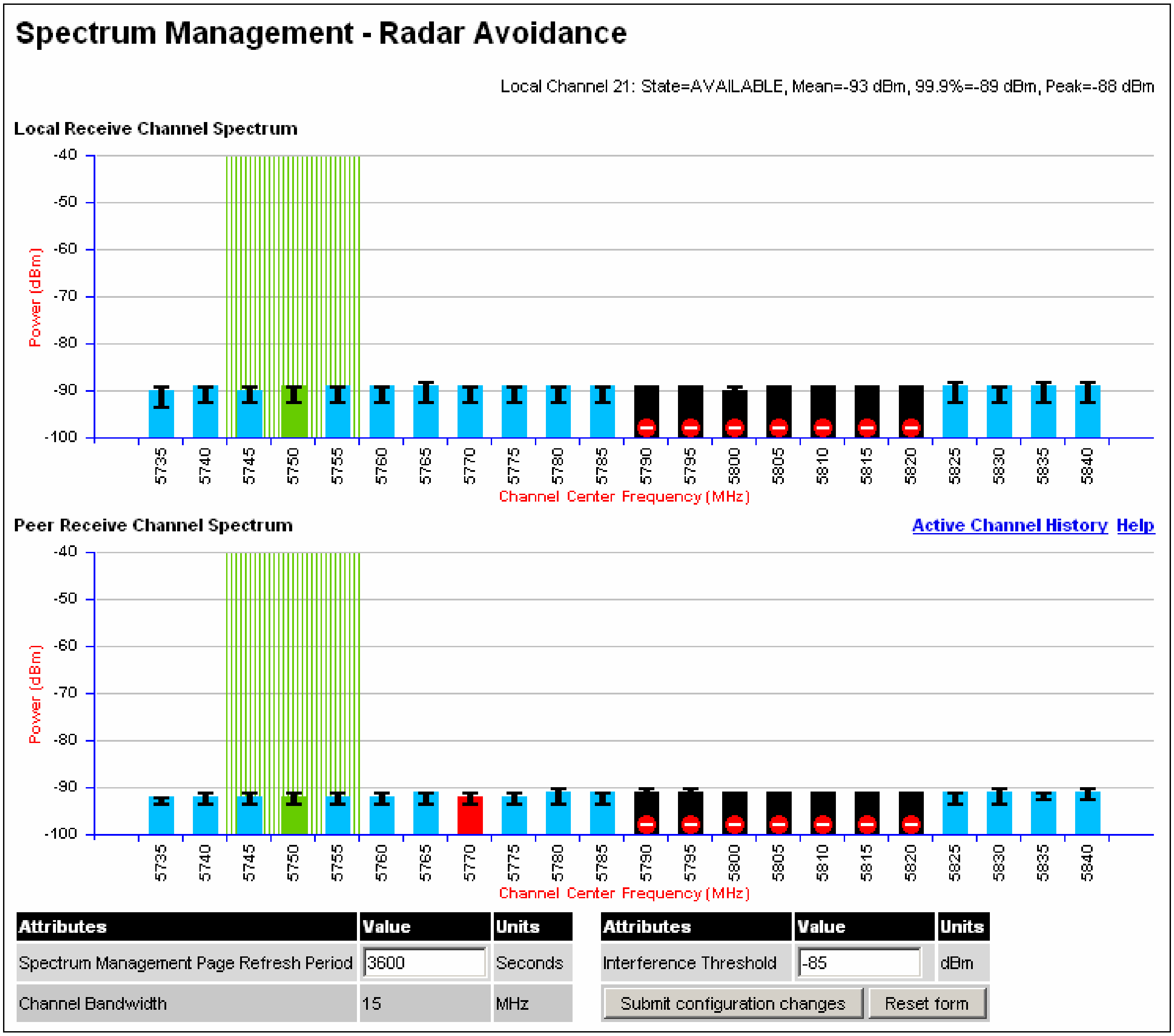


**Figure 7-13** Spectrum Management page with radar avoidance - slave

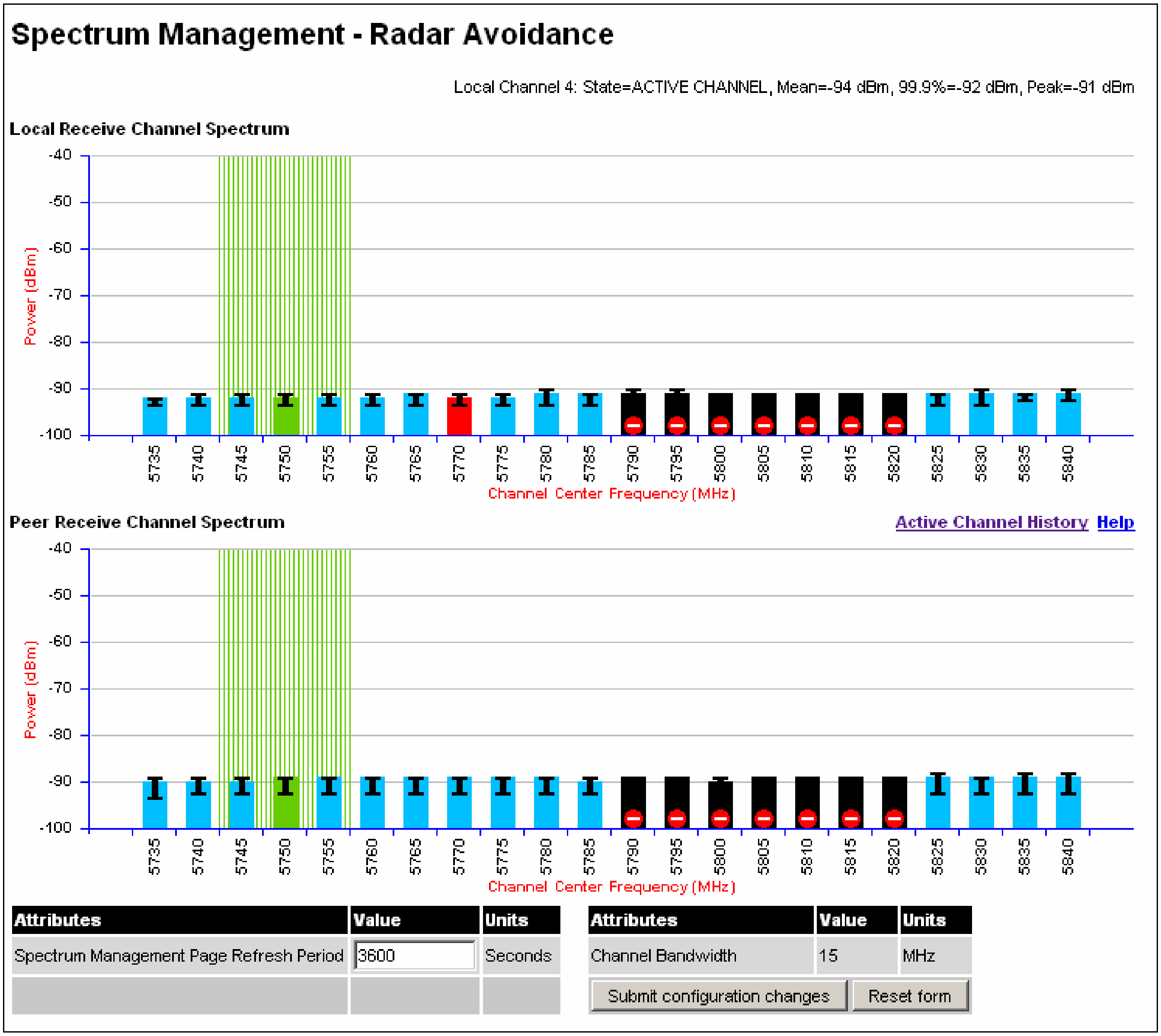


**Table 7-9** Channel states represented in the spectrum management plot (radar avoidance)

| State and color | Meaning |
|---|---|
| Active | This channel is currently in use hosting the Point-to-Point wireless link. |
| Interference | This channel has interference above the interference threshold |
| Available | This channel has an interference level below the interference threshold and is considered by the Spectrum Management algorithm suitable for hosting the Point-to-Point link |
| Barred | The system administrator has barred this channel from use. Because the low signal levels encountered when a unit is powered up in a laboratory environment prior to installation (which makes the grey of the channel bar difficult to see). An additional red 'lock' symbol is used to indicate that a channel is barred. |
| Unavailable | This channel needs to be monitored for one minute and found free of radar signal before it can be used for transmitting. |
| Radar Detected | Impulsive Radar Interference has been detected on this channel and the channel is unavailable for 30 minutes. At the end of the 30 minute period a Channel Availability Check is required to demonstrate no radar signals remain on this channel before it can be used for the radio link. |
| Region Bar | This channel has been barred from use by the local region regulator |

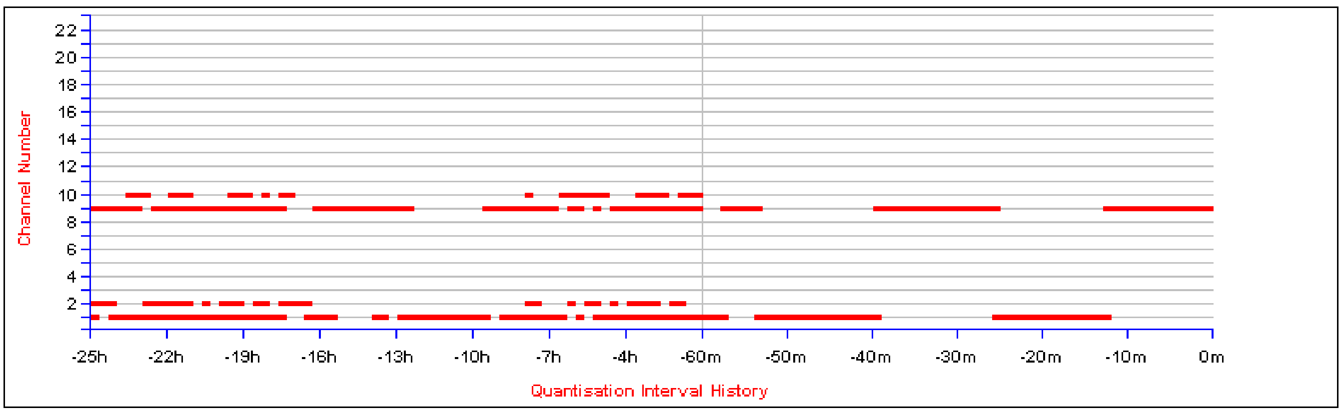
## Viewing the active channel history

The active channel history is a time series display of the channels used by the PTP 300 or PTP 500 Series over the last 25 hours.

To view the active channel history, select the **Active Channel History** hyperlink from the Spectrum Management page.

An example of the active channel history display is shown in Figure 7-14. Where there are parallel entries on the display this signifies that the wireless link occupied this channel during the measurement period. The measurement periods are one minute (from zero to sixty minutes) and twenty minutes from (60 minutes to twenty five hours).

**Figure 7-14** Active channel history screen



## Viewing historic spectrum management metrics

The results of previous measurement quantization periods can be viewed from both the master and slave Spectrum Management pages.

To view these results, hold down the shift key and click the appropriate channel on the Local Receive Channel Separation plot.

The time series plot is displayed (Figure 7-15). This plot displays the results of all previous measurement quantization periods, up to a maximum of 132 periods. The colored lines represent interference measurements (Table 7-10).

**Figure 7-15** Spectrum management time series plot

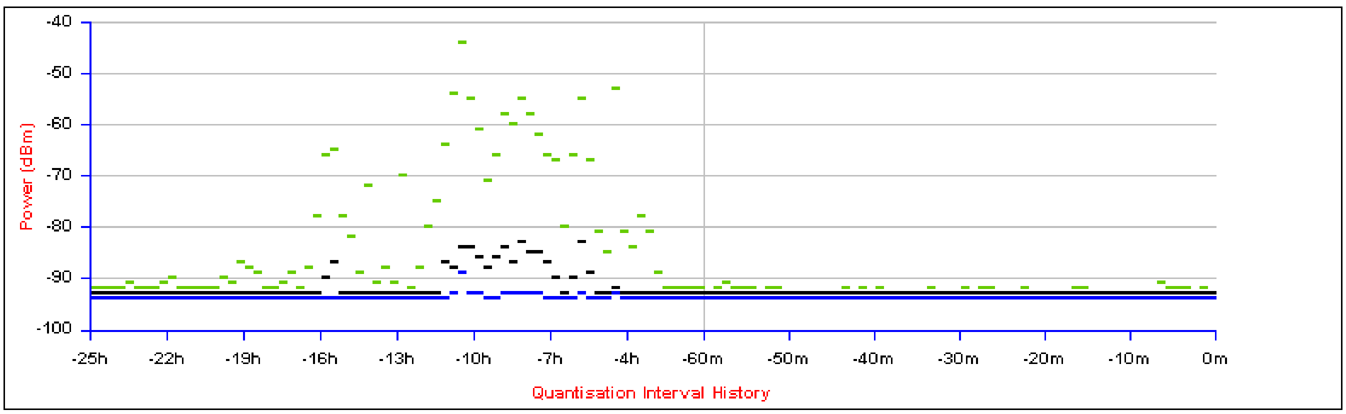



**Table 7-10** Interference represented in the time series plot

| Color | Meaning |
|---|---|
| GREEN | Peak of Means interference measurement |
| BLACK | 99.9% percentile of means interference measurement |
| BLUE | Mean of Means interference measurement |

# Upgrading software via remote access

## Upgrading software using TFTP

This section describes how to upgrade the PTP 300 or PTP 500 software remotely using Trivial FTP (TFTP) triggered by SNMP.

To perform a remote software upgrade, follow this procedure:

**Procedure 7-3** Remote software upgrade

| | |
|---|---|
| **1** | Check that the TFTP client is enabled. Refer to Configuring web-based management attributes on page 6-77. |
| **2** | Set tFTP attributes as described in Table 7-11. |
| **3** | Monitor tFTP attributes as described in Table 7-12. |
| **4** | When the upgrade is complete, reboot the ODU to run the newly loaded software image as described in Rebooting the unit on page 7-59. |

**Table 7-11** Setting tFTP attributes

| Attribute | Meaning |
|---|---|
| tFTPServerIPAddress | The IP address of the TFTP server from which the TFTP software upgrade file Name will be retrieved.<br>For example, to set the TFTP server IP address for unit 10.10.10.10 to 10.10.10.1, enter this command:<br>**snmpset_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.1.9.5.0 a 10.10.10.1** |
| tFTPServerPortNumber | This setting is optional. The port number of the TFTP server from which the TFTP software upgrade file name will be retrieved (default=69). |
| tFTPSoftwareUpgrade FileName | The filename of the software upgrade to be loaded from the TFTP server.<br>For example, to set the TFTP software upgrade filename on 10.10.10.10 to "B1095.dld", enter this command:<br>**snmpset_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.1.9.7.0 s B1095.dld** |
| tFTPStartSoftware Upgrade | Write '1' to this attribute to start the TFTP software upgrade process. The attribute will be reset to 0 when the upgrade process has finished.<br>For example, enter this command:<br>**snmpset_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.1.9.8.0 i 1** |

**Table 7-12** Monitoring tFTP attributes

| Attribute | Meaning |
|---|---|
| tFTPSoftwareUpgradeStatus | This is the current status of the TFTP software upgrade process. Values:<br>idle(0)<br>uploadinprogress(1)<br>uploadsuccessfulprogrammingFLASH(2)<br>upgradesuccessfulreboottorunthenewsoftwareimage(3)<br>upgradefailed(4).<br>For example, enter this command:<br>**snmpget_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.1.9.9.0** |
| tFTPSoftwareUpgradeStatusText | This describes the status of the TFTP software upgrade process, including any error details.<br>For example, enter this command:<br>**snmpget_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.1.9.10.0** |
| tFTPSoftwareUpgradeStatusAdditionalText | This is used if tFTPSoftwareUpgradeStatusText is full and there are more than 255 characters to report. It contains additional text describing the status of the TFTP software upgrade process, including any error details.<br>For example, enter this command:<br>**snmpget_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.1.9.11.0** |

# Managing performance

This section describes how to manage the performance of the PTP 300 or PTP 500 link.

This section contains the following procedures:



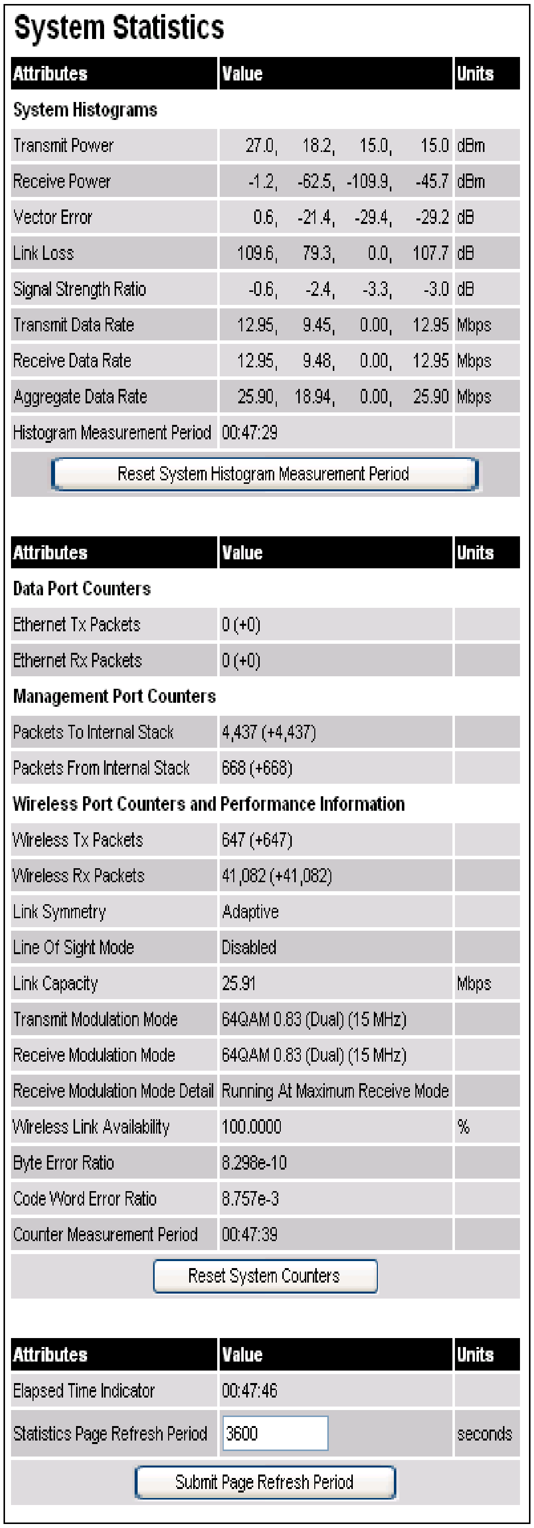
## Checking system statistics

To check system statistics, select menu option **System, Statistics**. The System Statistic page is displayed (Figure 7-16).

**NOTE**

To enable or disable the display of commas in long integers (for example 1,234,567), select menu option **Management, Web, Web Properties** and update the Use Long Integer Comma Formatting attribute.

**Figure 7-16** System Statistics page



## System Statistics

| Attributes | Value | Units |
|---|---|---|
| **System Histograms** | | |
| Transmit Power | 27.0, 18.2, 15.0, 15.0 | dBm |
| Receive Power | -1.2, -62.5, -109.9, -45.7 | dBm |
| Vector Error | 0.6, -21.4, -29.4, -29.2 | dB |
| Link Loss | 109.6, 79.3, 0.0, 107.7 | dB |
| Signal Strength Ratio | -0.6, -2.4, -3.3, -3.0 | dB |
| Transmit Data Rate | 12.95, 9.45, 0.00, 12.95 | Mbps |
| Receive Data Rate | 12.95, 9.48, 0.00, 12.95 | Mbps |
| Aggregate Data Rate | 25.90, 18.94, 0.00, 25.90 | Mbps |
| Histogram Measurement Period | 00:47:29 | |
| Reset System Histogram Measurement Period | | |

| Attributes | Value | Units |
|---|---|---|
| **Data Port Counters** | | |
| Ethernet Tx Packets | 0 (+0) | |
| Ethernet Rx Packets | 0 (+0) | |
| **Management Port Counters** | | |
| Packets To Internal Stack | 4,437 (+4,437) | |
| Packets From Internal Stack | 668 (+668) | |
| **Wireless Port Counters and Performance Information** | | |
| Wireless Tx Packets | 647 (+647) | |
| Wireless Rx Packets | 41,082 (+41,082) | |
| Link Symmetry | Adaptive | |
| Line Of Sight Mode | Disabled | |
| Link Capacity | 25.91 | Mbps |
| Transmit Modulation Mode | 64QAM 0.83 (Dual) (15 MHz) | |
| Receive Modulation Mode | 64QAM 0.83 (Dual) (15 MHz) | |
| Receive Modulation Mode Detail | Running At Maximum Receive Mode | |
| Wireless Link Availability | 100.0000 | % |
| Byte Error Ratio | 8.298e-10 | |
| Code Word Error Ratio | 8.757e-3 | |
| Counter Measurement Period | 00:47:39 | |
| Reset System Counters | | |

| Attributes | Value | Units |
|---|---|---|
| Elapsed Time Indicator | 00:47:46 | |
| Statistics Page Refresh Period | 3600 | seconds |
| Submit Page Refresh Period | | |

## System histograms

The System Histograms attributes (Table 7-13) are presented as an array of four elements. These elements represent the maximum, mean, minimum and latest values respectively. The maximum, mean and minimum are calculated over a running one hour period.

To reset all histograms and restart the measurement period, select **Reset System Histograms and Measurement Period**.

**Table 7-13** System Histograms attributes in the System Statistics page

| Attribute | Meaning |
|---|---|
| Transmit Power | The transmit power histogram, calculated over a one hour period. |
| Receive Power | The receive power histogram, calculated over a one hour period. |
| Vector Error | The vector error measurement compares the received signal IQ modulation characteristics to an ideal signal to determine the composite vector error magnitude. The histogram is calculated over a one hour period. |
| Link Loss | The link loss measurement is calculated as follows:<br>Peer_Tx_Power (dBm) – Local_Rx_Power (dBm) + 2 x Antenna_Pattern (dBi)<br>The histogram is calculated over a one hour period. |
| Signal Strength Ratio | The Signal Strength Ratio is:<br>Power received by the vertical antenna input (dB) ÷<br>Power received by the horizontal antenna input (dB)<br>This ratio is presented as: max, mean, min, and latest in an histogram format. The max, min and latest are true instantaneous measurements; the mean is the mean of a set of one second means. See Histogram data on page 7-19. |
| Transmit Data Rate | The data rate in the transmit direction, expressed in Mbps and presented as: max, mean, min, and latest in an histogram format. The max, min and latest are true instantaneous measurements; the mean is the mean of a set of one second means. Expected data rates can be found in Data rate calculations on page 4-77. |

| Attribute | Meaning |
|---|---|
| Receive Data Rate | The data rate in the receive direction, expressed in Mbps and presented as: max, mean, min, and latest in an histogram format. The max, min and latest are true instantaneous measurements; the mean is the mean of a set of one second means. Expected data rates can be found in Data rate calculations on page 4-77 |
| Aggregate Data Rate | The sum of the data rate in the directions expressed in Mbps and presented as: max, mean, min, and latest in an histogram format. The max, min and latest are true instantaneous measurements; the mean is the mean of a set of one second means. Expected data rates can be found in Data rate calculations on page 4-77. |
| Histogram Measurement Period | The time over which the system histograms were collected. |

Signal Strength Ratio is an aid to debugging a link. If it has a large positive or negative value then investigate the following potential problems:

- An antenna coaxial lead may be disconnected.
- When spatial diversity is employed, the antenna with the lower value may be pointing in the wrong direction.
- When a dual polar antenna is deployed, the antenna may be directed using a side lobe rather than the main lobe.

When there is a reflection from water on the link and spatial diversity is employed, then one expects large, slow swings in Signal Strength Ratio. This indicates the antenna system is doing exactly as intended.

## System counters

The System Statistics page contains the following system counters:

- Data port counters (Table 7-14)
- Management port counters (Table 7-15)
- Wireless port counters and performance information (Table 7-16)

The packet counter attributes each contain a number in parentheses; this shows the number of packets received since the last page refresh.

To reset all system counters to zero, select **Reset System Counters**.

**Table 7-14** Data Port Counter attributes in the System Statistics page

| Attribute | Meaning |
|---|---|
| Ethernet Tx Packets | This displays the total number of good packets the bridge has sent for transmission by the local Ethernet interface. |
| Ethernet Rx Packets | This displays the number of good and bad packets received from the local Ethernet interface. |

**Table 7-15** Management Port Counter attributes in the System Statistics page

| Attribute | Meaning |
|---|---|
| Packets To Internal Stack | This displays the total number of good packets the bridge has transmitted to the internal stack (for example, ARP requests, PING requests, HTTP requests). |
| Packets From Internal Stack | This displays the total number of good packets the bridge has received from the internal stack (for example ARP responses, PING replies, HTTP responses). |

**Table 7-16** Wireless Port Counter attributes in the System Statistics page

| Attribute | Meaning |
|---|---|
| Wireless Tx Packets | This displays the total number of good packets the bridge has sent for transmission by the wireless interface. |
| Wireless Rx Packets | This displays the total number of good packets the bridge has received from the wireless interface. |

| Attribute | Meaning |
|---|---|
| Link Symmetry | A ratio that expresses the division between transmit and receive time in the TDD frame. The first number in the ratio represents the time allowed for the transmit direction and the second number represents the time allowed for the receive direction. |
| Line Of Sight Mode | PTP 300 only. The current setting of the Line Of Sight Mode control, either ‘Enabled’ or ‘Disabled’. This is hidden unless the line of sight capability is enabled by license key. |
| Link Capacity | The maximum aggregate data capacity available for user traffic under the current radio link conditions, assuming the units have been connected using Gigabit Ethernet. The sum of the displayed Transmit and Receive data rates may be lower than this figure if the link isn't fully loaded by the current traffic profile. |
| Transmit Modulation Mode | The modulation mode currently being used on the transmit channel. The number in brackets after the modulation mode and coding rate string is the effective data rate available to all MAC layer protocols. List of all the modulation modes can be found in Data rate calculations on page 4-77, where data rate calculations plots are given for each available modulation mode. |
| Receive Modulation Mode | The modulation mode currently being used on the receive channel. The number in brackets after the modulation mode and coding rate string is the effective data rate available to all MAC layer protocols. List of all the modulation modes can be found in Data rate calculations on page 4-77, where data rate calculations plots are given for each available modulation mode. |

| Attribute | Meaning |
|---|---|
| Receive Modulation Mode Detail | This supplies the user with information regarding the receive modulation mode in use. Possible values are:<br>‘Running at maximum receive mode’<br>‘Running at user-configured Target Modulation Mode’<br>‘Restricted because Installation is armed’<br>‘Restricted because of byte errors on the wireless link’<br>‘Restricted because a DFS channel change is in progress’<br>‘Restricted due to the low Ethernet link speed’<br>‘Limited by the radio conditions’ |
| Wireless Link Availability | Expresses the link availability as a percentage of time since the first successful registration after a system restart, expressed as a percentage to four decimal places. |
| Byte Error Ratio | The ratio of detected Byte errors to the total number of bytes since the last system reboot. This is a true measure of link quality as this measurement is made continually using null frames when there is no user data to transport. |
| Code Word Error Ratio | The ratio of uncorrected code word errors to the total number of code words, calculated since the last reset of system counters. |
| Counter Measurement Period | The time over which the system counters were collected. |

### Other attributes

The System Statistics page contains two other attributes (Table 7-17).

After updating the Statistics Page Refresh Period field, select **Submit Page Refresh Period**.

**Table 7-17** Other attributes in the System Statistics page

| Attribute | Meaning |
|---|---|
| Elapsed Time Indicator | Elapsed time since the last system reboot. |
| Statistics Page Refresh Period | The statistics page refreshes automatically according to the setting entered here (in seconds). |

## Resetting system histograms and counters

To reset system histograms and counters, proceed as follows:

**Procedure 7-4** Reset system histograms and counters

| | |
|---|---|
| **1** | Select menu option **System, Statistics**. The System Statistics page is displayed (Figure 7-16). |
| **2** | To reset the System Histograms attributes, select **Reset System Histogram Measurement Period**. |
| **3** | To reset the Counters attributes, select **Reset System Counters**. |

## Checking detailed counters

The Detailed Counters page displays detailed statistics of the Ethernet Bridge and the underlying wireless performance. To check detailed counters, proceed as follows:

**Procedure 7-5** Check system statistics and counters

| | |
|---|---|
| **1** | Select menu option **System, Statistics, Detailed Counters**. The Detailed Counters page is displayed (Figure 7-17). |
| **2** | Review the detailed counters (Table 7-18). |

**Figure 7-17** Detailed Counters page

## Detailed Counters

**Ethernet**

| Attributes | Value | Units |
|---|---|---|
| Ethernet Rx Octets | 0 (+0) | |
| Ethernet Tx Octets | 0 (+0) | |
| Ethernet Rx Drops | 0 (+0) | |
| Ethernet Rx Packets | 0 (+0) | |
| Ethernet Rx Broadcasts | 0 (+0) | |
| Ethernet Rx Multicasts | 0 (+0) | |
| Ethernet Rx Crc And Align | 0 (+0) | |
| Ethernet Rx Undersize | 0 (+0) | |
| Ethernet Rx Oversize | 0 (+0) | |
| Ethernet Rx Fragments | 0 (+0) | |
| Ethernet Rx Jabbers | 0 (+0) | |
| Ethernet Tx Drops | 88,952 (+22,760) | |
| Ethernet Tx Packets | 0 (+0) | |
| Ethernet Tx Broadcasts | 0 (+0) | |
| Ethernet Tx Multicasts | 0 (+0) | |
| Ethernet Tx Collisions | 0 (+0) | |
| Ethernet Tx Fifo Drops | 0 (+0) | |
| Ethernet Rx Frames Q0 | 0 (+0) | |
| Ethernet Rx Frames Q1 | 0 (+0) | |
| Ethernet Rx Frames Q2 | 0 (+0) | |
| Ethernet Rx Frames Q3 | 0 (+0) | |
| Ethernet Rx Frames Q4 | 0 (+0) | |
| Ethernet Rx Frames Q5 | 0 (+0) | |
| Ethernet Rx Frames Q6 | 0 (+0) | |
| Ethernet Rx Frames Q7 | 0 (+0) | |
| Ethernet Tx Frames Q0 | 88,951 (+22,760) | |
| Ethernet Tx Frames Q1 | 0 (+0) | |
| Ethernet Tx Frames Q2 | 0 (+0) | |
| Ethernet Tx Frames Q3 | 0 (+0) | |
| Ethernet Tx Frames Q4 | 0 (+0) | |
| Ethernet Tx Frames Q5 | 0 (+0) | |
| Ethernet Tx Frames Q6 | 0 (+0) | |
| Ethernet Tx Frames Q7 | 0 (+0) | |
| Ethernet Rx Pause Frames | 0 (+0) | |
| Ethernet Tx Pause Frames | 0 (+0) | |
| **Internal Stack** | | |
| Packets To Internal Stack | 9,317 (+2,815) | |
| Packets From Internal Stack | 2,059 (+1,269) | |
| Packets Ignored By Internal Stack | 0 (+0) | |

**Wireless**

| Attributes | Value | Units |
|---|---|---|
| Wireless Rx Octets | 9,329,510 (+2,338,338) | |
| Wireless Tx Octets | 2,218,392 (+1,450,531) | |
| Wireless Rx Drops | 0 (+0) | |
| Wireless Rx Packets | 88,951 (+22,759) | |
| | | |
| | | |
| Wireless Rx Crc And Align | 0 (+0) | |
| Wireless Rx Undersize | 0 (+0) | |
| Wireless Rx Oversize | 0 (+0) | |
| | | |
| | | |
| Wireless Tx Drops | 1 (+0) | |
| Wireless Tx Packets | 2,027 (+1,260) | |
| | | |
| | | |
| | | |
| | | |
| Wireless Tx Frames Q0 | 2,027 (+1,260) | |
| Wireless Tx Frames Q1 | 0 (+0) | |
| Wireless Tx Frames Q2 | 0 (+0) | |
| Wireless Tx Frames Q3 | 0 (+0) | |
| Wireless Tx Frames Q4 | 0 (+0) | |
| Wireless Tx Frames Q5 | 0 (+0) | |
| Wireless Tx Frames Q6 | 0 (+0) | |
| Wireless Tx Frames Q7 | 0 (+0) | |
| Wireless Rx Frames Q0 | 88,951 (+22,759) | |
| Wireless Rx Frames Q1 | 0 (+0) | |
| Wireless Rx Frames Q2 | 0 (+0) | |
| Wireless Rx Frames Q3 | 0 (+0) | |
| Wireless Rx Frames Q4 | 0 (+0) | |
| Wireless Rx Frames Q5 | 0 (+0) | |
| Wireless Rx Frames Q6 | 0 (+0) | |
| Wireless Rx Frames Q7 | 0 (+0) | |

| Attributes | Value | Units |
|---|---|---|
| Detailed Counter Page Refresh Period | 3600 | seconds |
| Submit Page Refresh Period | | |

| Attributes | Value | Units |
|---|---|---|
| Counter Measurement Period | 01:29:04 | |
| Reset System Counters | | |

**Table 7-18** Detailed Counters attributes

| Attribute | Meaning |
|---|---|
| Tx & Rx Octets | Total number of octets (bytes) transmitted or received over the interface. |
| Rx Drops | Total number of frames dropped due to the lack of sufficient capacity in the receive buffer. |
| Rx Packets | Total number of packets received by the interface. This includes both good and bad packets. |
| Rx Broadcasts | Total number of good broadcast packets. |
| Rx Multicasts | Total number of good multicast packets. |
| Rx CRC and Align | Total number of packets with CRC or frame alignment errors. |
| Rx Undersize | Total number of packets received that are less than 64 bytes and have a valid CRC. |
| Rx Oversize | Total number of packets received that are greater than the maximum number of bytes with a valid CRC. |
| Rx Fragments | Total number of packets that are less than 64 bytes with an invalid CRC (these packet types are also known as runts). |
| Rx Jabbers | Total number of packets received that are greater than the maximum number of bytes with an invalid CRC. |
| Tx Drops | Total number of frames dropped due excessive collisions, late collision and frame ageing. |
| Tx Packets | Total number of packets received by the interface. This includes both good and bad packets. |
| Tx Broadcasts | Total number of good broadcast packets. |
| Tx Multicasts | Total number of good multicast packets. |
| Tx Collisions | Total number frames experiencing collisions. |
| Tx FIFO Drops | Total number frames dropped due to lack of capacity in the transmit buffer, for example when the unit is connected to the local Ethernet at a connection speed of less than 1 Gbps. |
| Rx & Tx Frames Q0…Q7 | Total number of received or transmitted frames for each Traffic Class (Q0 to Q7). |

| Attribute | Meaning |
|---|---|
| Rx & Tx Pause Frames | Total number of received or transmitted pause frames (Ethernet interface only). |
| Packets To Internal Stack | The total number of good packets the bridge has transmitted to the internal stack. |
| Packets From Internal Stack | The total number of good packets the bridge has received from the internal stack. |
| Packets Ignored By Internal Stack | The total number of bad packets the bridge has transmitted to the internal stack. |
| Detailed Counters Page Refresh Period | The statistics page refreshes automatically according to the setting entered here (in seconds). |
| Counter Measurement Period | The time over which the system counters were collected. |

## Using the diagnostics plotter

The diagnostics plotter can trace the following statistics (refer to Table 7-13 for definitions):

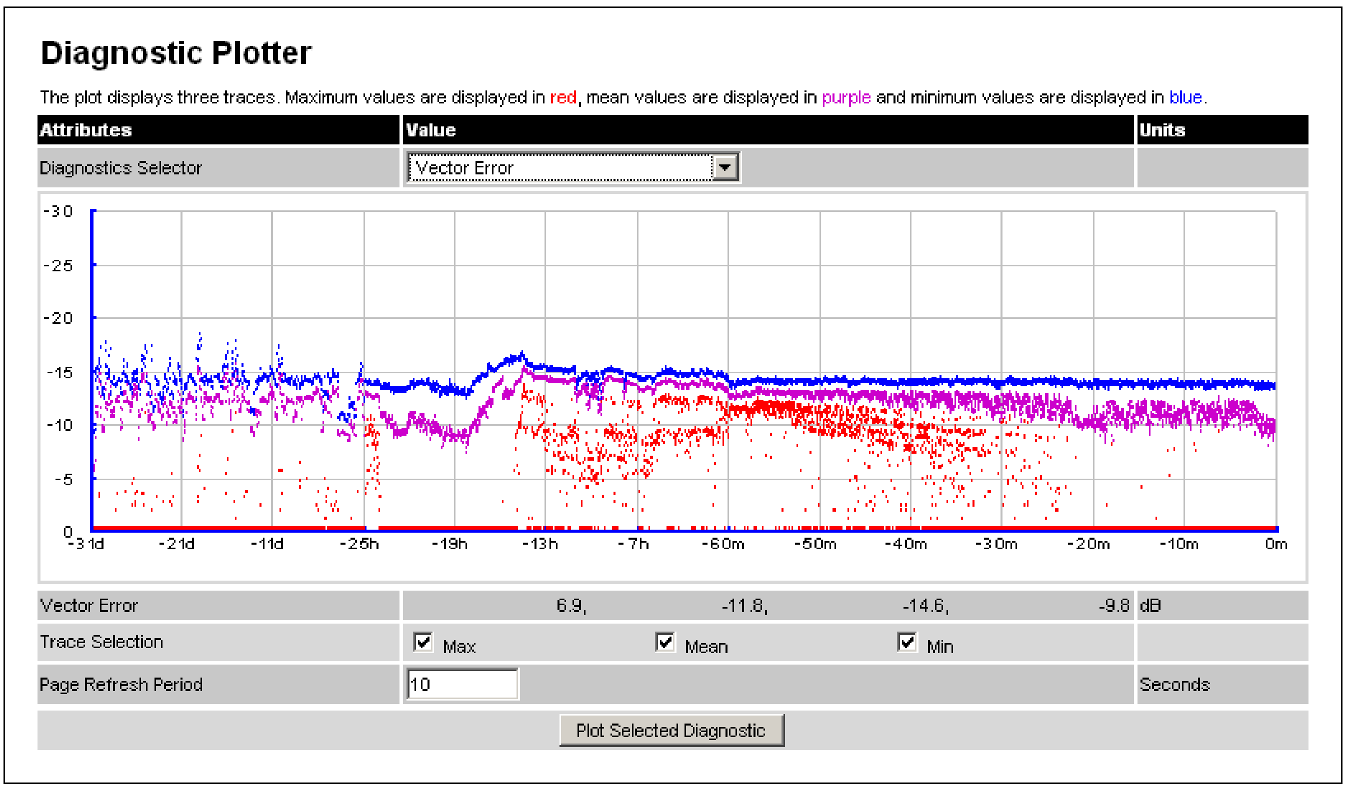
- Vector Error
- Rx Power
- Tx Power
- Signal Strength Ratio V/H
- Link Loss
- Rx Data Rate
- Tx Data Rate
- Aggregate Data Rate

To plot diagnostics, proceed as follows:

**Procedure 7-6** Plot diagnostics

| | |
|---|---|
| **1** | Select menu option **System, Diagnostics Plotter**. The Diagnostics Plotter page is displayed (Figure 7-18). |
| **2** | Use the Diagnostics Selector drop-down list to select a diagnostic type to plot. |
| **3** | Use the Trace Selection to select traces of the maximum, mean or minimum values of the diagnostic type. Maximum values are displayed in red, mean values are displayed in purple and minimum values are displayed in blue. |
| **4** | Select **Plot Selected Diagnostic**. The trace is displayed in the graph. |

**Figure 7-18** Diagnostic Plotter page



### Changing the diagnostics refresh period

The default refresh period is 3600 seconds (1 hour). If a much shorter refresh period is selected, for example 60 seconds, it is possible to monitor the performance of an operational PTP 800 link in real time.

To change the diagnostics refresh period, proceed as follows:

**Procedure 7-7** Change the diagnostics refresh period

| | |
|---|---|
| **1** | Select menu option **System, Diagnostics Plotter**. The Diagnostics Plotter page is displayed (Figure 7-18). |
| **2** | Enter the required refresh frequency in the Page Refresh Period attribute. |

## Downloading diagnostic data

The CSV file contains at most 5784 entries, recorded over a 32 day period:

- 3600 entries recorded in the last hour.
- 1440 entries recorded in the previous 24 hours.
- 744 entries recorded in the previous 31 days.

The following statistics can be downloaded (refer to Table 7-13 for definitions):

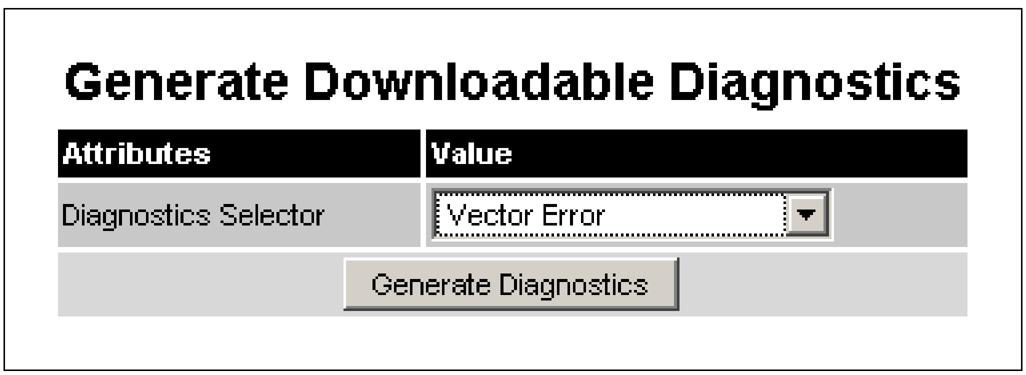
- Vector Error
- Rx Power
- Tx Power
- Signal Strength Ratio V/H
- Link Loss
- Rx Data Rate
- Tx Data Rate
- Aggregate Data Rate

To download diagnostics data, proceed as follows:

**Procedure 7-8** Download diagnostics

| | |
|---|---|
| **1** | Select menu option **System, Diagnostics Plotter, CSV Download**. The Generate Downloadable Diagnostics page is displayed (Figure 7-19). |
| **2** | Use the Diagnostics Selector drop-down list to select a diagnostic type to download. |
| **3** | Select **Generate Diagnostics**. The Generate Downloadable Diagnostics page is redisplayed with the name of the generated CSV file. |
| **4** | Click on the CSV file name and select Save File. Save the CSV file to the hard drive of the local computer. |
| **5** | Open the CSV file in MS Excel and use it to generate statistical reports and diagrams. |

**Figure 7-19** Generate Downloadable Diagnostics page



# Rebooting the unit

## Rebooting or reviewing reboot reasons

To reboot the ODU or view a list of previous reboot reasons, proceed as follows:

**Procedure 7-9** Reboot the ODU or view reboot reasons

| | |
|---|---|
| **1** | Select menu option **System, Reboot**. The Reboot Wireless Unit page is displayed (Figure 7-20). |
| **2** | Use the drop-down list to view the Previous Reasons For Reset/Reboot. |
| **3** | If a reboot is required, select **Reboot Wireless Unit**. The Reboot Confirmation dialog is displayed (Figure 7-21). |
| **4** | Select **OK**. The reboot progress message is displayed. On completion, the unit restarts. |

**Figure 7-20** Reboot Wireless Unit page

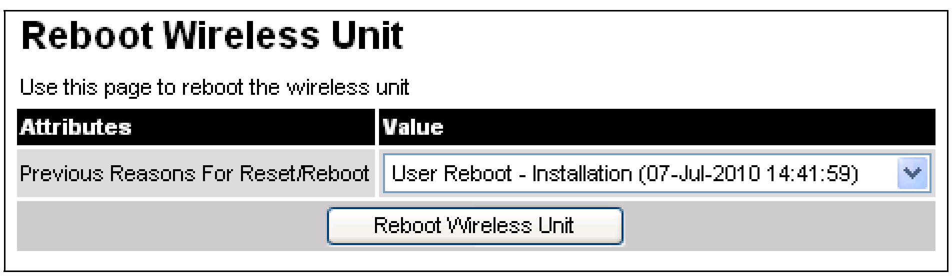
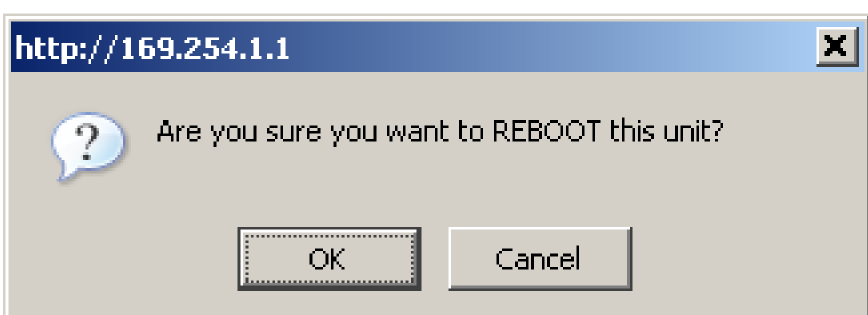



**Figure 7-21** Reboot confirmation pop up



# Using recovery mode

The Motorola PTP 300 and PTP 500 point-to-point wireless Ethernet bridges have a special mode of operation that allows the user to recover a unit from configuration errors or software image corruption. This section describes how to enter recovery mode and how to recover the unit.

The following topics are described in this section:

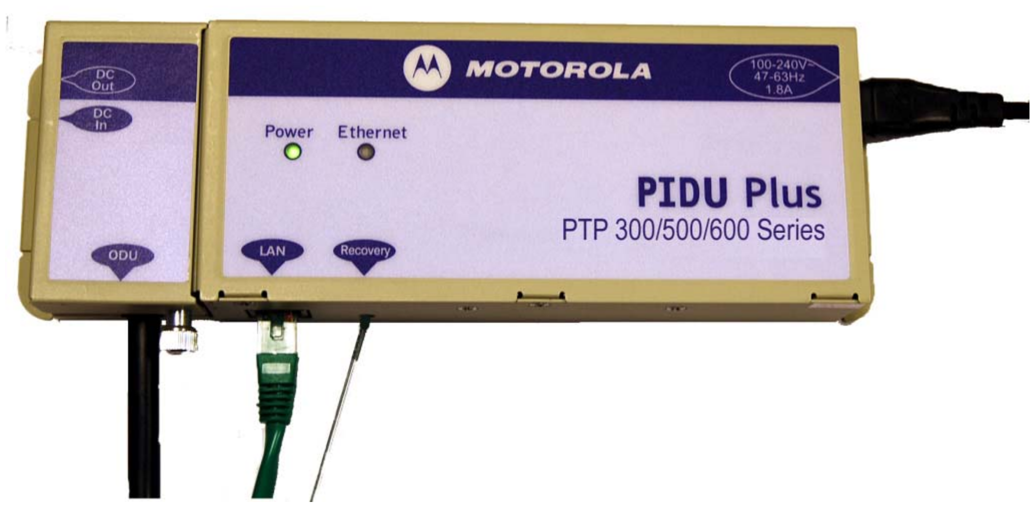


## Entering recovery mode

The unit may enter recovery mode automatically, in response to some failures.

To enter recovery mode manually, press the Recovery switch located on the underside of the PIDU Plus while applying mains power (Figure 7-22), hold the Recovery switch in for between 10 and 20 seconds, then release it. The Ethernet LED will double-flash 10 times at power up.

**Figure 7-22** PIDU Plus recovery switch location



## Selecting a recovery option

To select a recovery option when the unit is in recovery mode, proceed as follows:

**Procedure 7-10** Select a recovery option when in recovery mode

| | |
|---|---|
| **1** | Access the web interface by entering the default IP address 169.254.1.1. The Recovery Image Warning page is displayed (Figure 7-23). |
| **2** | Click on the warning page image. The Recovery Option Page is displayed (Figure 7-24). |
| **3** | Review the Software Version and Recovery Reason (Table 7-19). |
| **4** | Select a recovery option (Table 7-20). |

**Figure 7-23** Recovery Image Warning page


**Figure 7-24** Recovery Options page

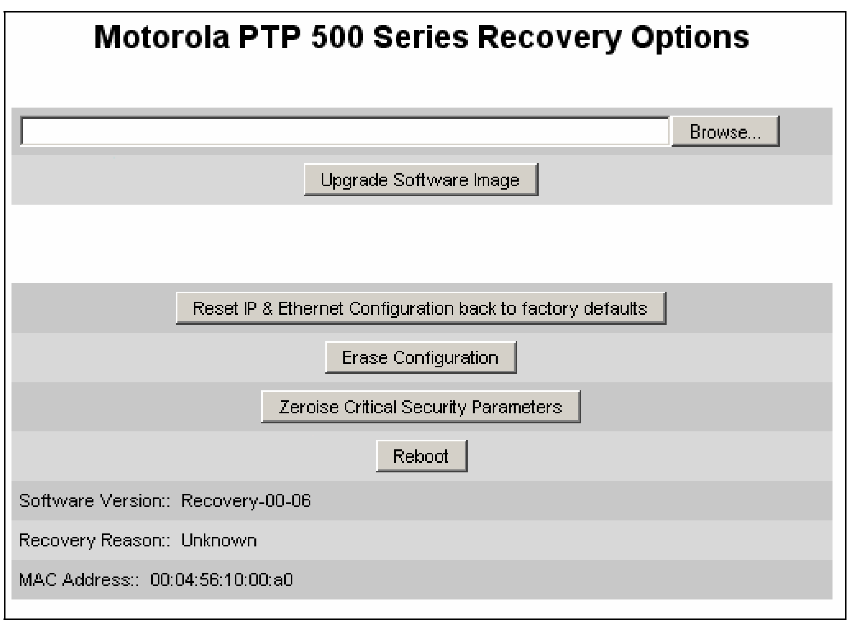


**Table 7-19** Recovery Options attributes

| Attribute | Meaning |
|---|---|
| Software Version | The software version of the recovery operating system permanently installed during manufacture. |
| Recovery Reason | The reason the unit is operating in Recovery mode, for example 'Recovery button active' or 'Invalid or corrupt image'. |
| MAC Address | The MAC address shown here is the MAC address of the unit programmed during manufacture. |

**Table 7-20** Recovery Options buttons

| Button | Purpose |
|---|---|
| Upgrade Software Image | Use this option to restore a working software version when software corruption is suspected, or when an incorrect software image has been loaded. Refer to Upgrading software image on page 7-56. |
| Reset IP & Ethernet Configuration back to factory defaults | Use this option to restore the IP and Ethernet attributes to their defaults. Refer to Resetting IP & Ethernet configuration on page 7-57. |
| Erase Configuration | Use this option to erase the entire configuration of the unit. This will also erase factory settings such as target MAC address, range setting and license key. Refer to Erasing configuration on page 7-58. |
| Reboot | Use this option to reboot the unit. Refer to Rebooting the unit on page 7-59. |

# Upgrading software image

To restore a working software image from the Recovery Options page (Figure 7-24), proceed as follows:

**Procedure 7-11** Upgrade software image when in recovery mode

| | |
|---|---|
| **1** | Select **Browse**. |
| **2** | Navigate to the required software image. This may be the most recent image if software corruption is suspected, or an older image if an incorrect image has just been loaded. Click on the image and select **OK**. |
| **3** | Select **Upgrade Software Image**. The Upgrade Progress Tracker page is displayed (Figure 7-25). |
| **4** | When the Software Upgrade Complete page is displayed (Figure 7-26), check that the correct image has been downloaded. |
| **5** | Select **Reboot Wireless Unit**. When the 'Are you sure?' pop up box is displayed, select **OK**. |
| **6** | The unit will now reboot. The unit should restart in normal operational mode and the link should recover. If the unit or link fails to recover, refer to Testing link end hardware on page 8-2. |

**Figure 7-25** Upgrade Progress Tracker page

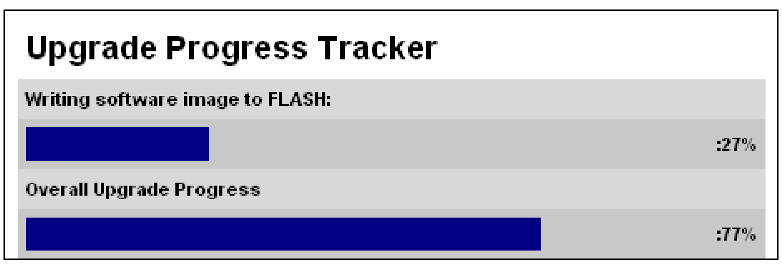
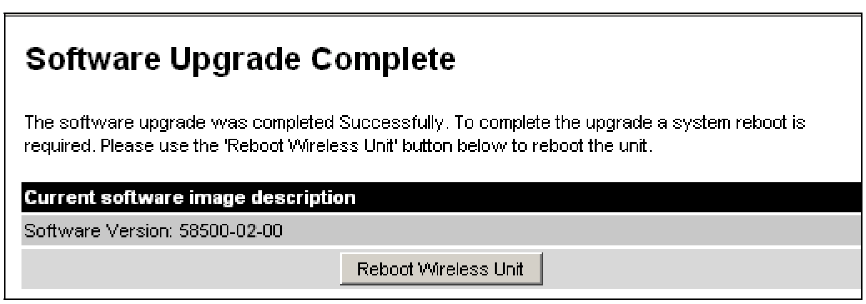



**Figure 7-26** Software Upgrade Complete page



# Resetting IP & Ethernet configuration

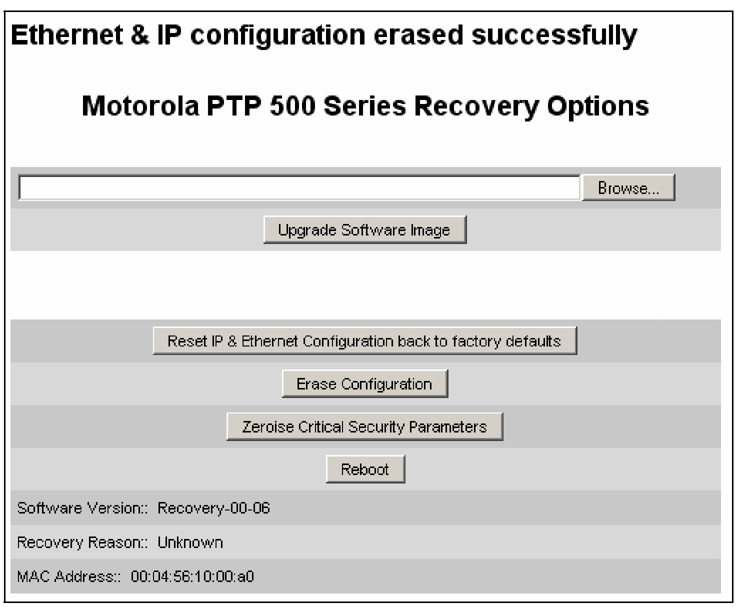
To reset IP and Ethernet configuration back to factory defaults from the Recovery Options page (Figure 7-24), proceed as follows:

**Procedure 7-12** Reset IP and Ethernet configuration when in recovery mode

| | |
|---|---|
| **1** | Select **Reset IP & Ethernet Configuration back to factory defaults**. The reset pop up box is displayed (Figure 7-27). Record the IP address, as it will be needed to log into the unit after recovery. |
| **2** | Select **OK**. The reset confirmation pageis displayed (Figure 7-28). |
| **3** | Select **Reboot**. When the 'Are you sure?' pop up box is displayed, select **OK**. |
| **4** | The unit will now reboot. The unit should now start up in normal mode but with the IP and Ethernet configuration reset to factory defaults. If the unit fails to recover, refer to Testing link end hardware on page 8-2. |

**Figure 7-27** Reset pop-up box


**Figure 7-28** Reset confirmation page



# Erasing configuration

To erase the entire configuration of the unit from the Recovery Options page (Figure 7-24), proceed as follows:

**Procedure 7-13** Reset IP and Ethernet configuration when in recovery mode

| | |
|---|---|
| **1** | Select **Erase Configuration**. The erase pop up box is displayed (Figure 7-29). |
| **2** | Select **OK**. The erase confirmation page is displayed (Figure 7-30). |
| **3** | Select **Reboot**. When the 'Are you sure?' pop up box is displayed, select **OK**. |
| **4** | The unit will now reboot. The unit should now start up in normal mode but with all configuration erased. If the unit fails to start up, refer to Testing link end hardware on page 8-2. |

**Figure 7-29** Erase pop-up box

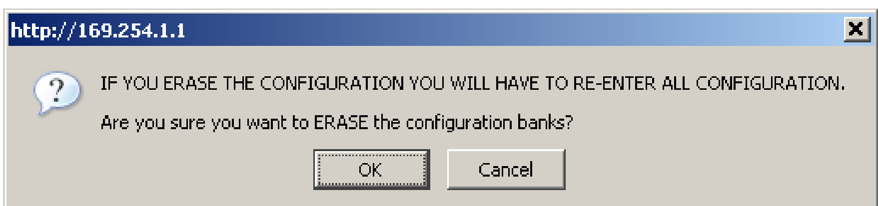
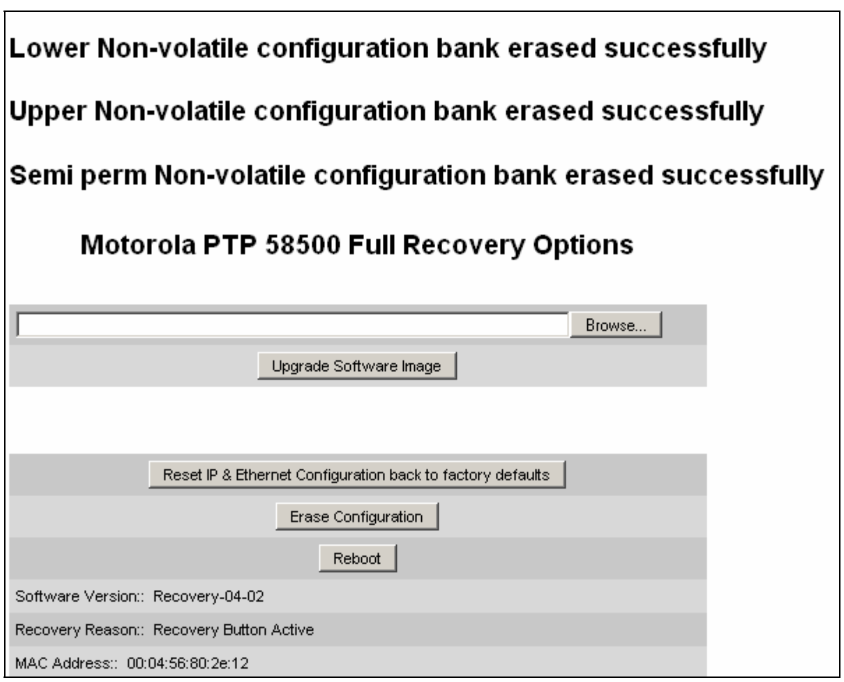



**Figure 7-30** Erase confirmation page



## Rebooting the unit

To reboot the unit from the Recovery Options page (Figure 7-24), select **Reboot**. When the 'Are you sure?' pop up box is displayed, select **OK**.

The unit will now reboot. The unit should now start up in normal operational mode. If the unit fails to start up, refer to Testing link end hardware on page 8-2.

# Restoring the operational configuration

## Restoring the configuration file

Perform this procedure to restore the operational configuration of the unit.

Before starting this procedure, ensure that:

- The configuration file of the old (faulty) unit has been saved.
- The new (replacement) unit has been installed.
- The license key of the old unit has been entered in the new unit.

To restore the configuration file, proceed as follows:

**Procedure 7-14** Restore configuration file

| | |
|---|---|
| 1 | Select menu option **Configuration**, **Save And Restore**. The Save & Restore Configuration page is displayed (Figure 6-14). |
| 2 | Select **Browse** and navigate to the PC folder containing the saved configuration file (.cfg). |
| 3 | Select **Restore Configuration File and Reboot**. |
| 4 | Select **OK** to confirm the restore. The configuration file is uploaded and used to reconfigure the new unit to the same state as the old unit. On completion, the unit reboots. |

# Chapter 8 Troubleshooting

This section contains procedures for identifying and correcting faults in a PTP 300 or PTP 500 link. These procedures can be performed either on a newly installed link, or on an operational link if communication is lost.

Select appropriate test procedures from the following list:

# Testing link end hardware

Before testing link end hardware, confirm that all outdoor drop cables, that is those that connect the ODU or GPS receiver (if installed) to equipment inside the building, are of the supported type, as defined in Cable and connector specifications on page 4-17.

If the Power and Ethernet LEDs do not illuminate correctly during the start-up sequence, test the link end as described in the flowchart (Figure 8-1) and detailed test procedures that follow.

**Figure 8-1** Link end hardware test flowchart #1

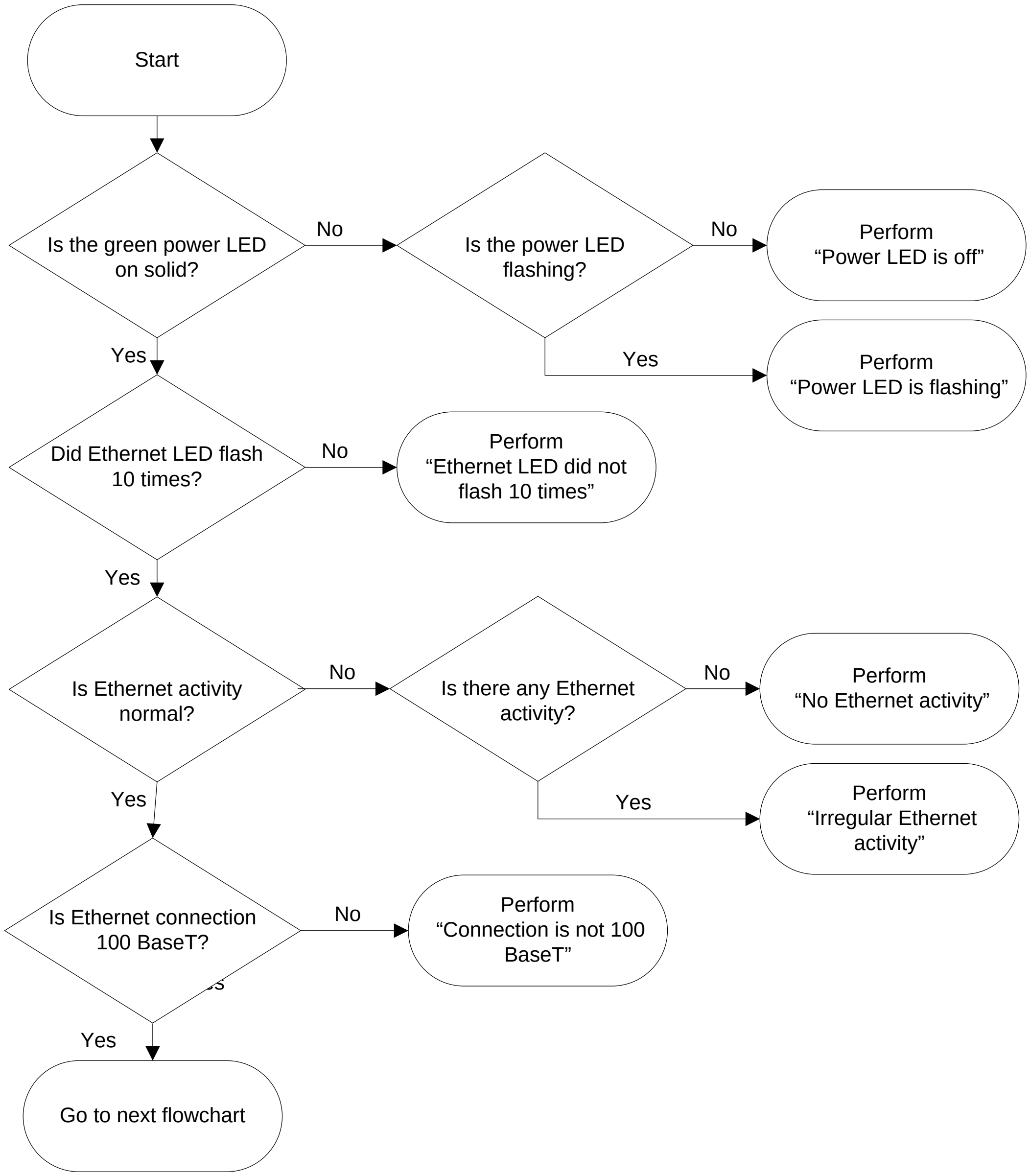
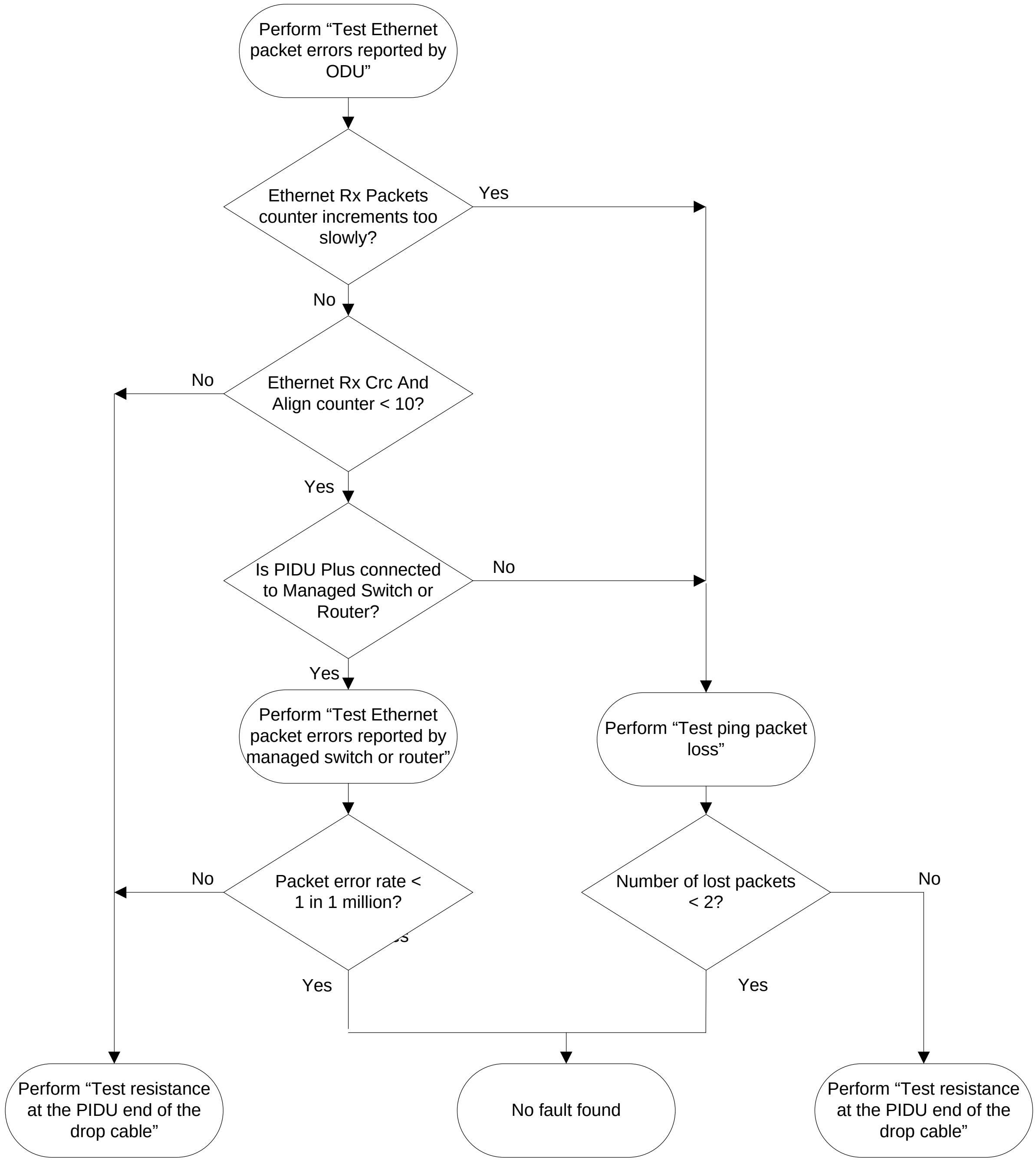


**Figure 8-2** Link end hardware test flowchart #2



## Power LED is off

If the Power LED is not on solid or flashing, proceed as follows:

**Procedure 8-1** Test the power supply

| | |
|---|---|
| **1** | Remove the power lead from the PIDU Plus. |
| **2** | Test that the power supply (mains or 56 V battery) is working. |
| **3** | If the power supply is not working, investigate the cause. |

If the power supply is working, proceed as follows:

**Procedure 8-2** Remove ODU cable from PIDU Plus

| | |
|---|---|
| **1** | Open the flap on the left hand side of the PIDU Plus. |
| **2** | Remove the ODU cable from the PIDU Plus. |
| **3** | Observe the effect on the Power LED; does it illuminate? |

If the Power LED does not illuminate when the ODU cable is removed, proceed as follows:

**Procedure 8-3** Power LED does not illuminate when ODU cable is removed

| | |
|---|---|
| **1** | Measure the voltage across the +55 V and 0 V pads inside the PIDU Plus flap.<br>If the voltage is incorrect, it indicates that the PIDU Plus is short-circuited. Report a suspected PIDU Plus fault to Motorola. |
| **2** | Measure the impedance across the Power connector.<br>If the impedance is incorrect, it indicates that the PIDU Plus is short-circuited. Report a suspected PIDU Plus fault to Motorola. |
| **3** | If both of the above tests produce correct readings, it is likely that the PIDU Plus Power LED is faulty. Report a suspected PIDU Plus fault to Motorola. |

If the Power LED does illuminate when the ODU cable is removed, proceed as follows:

**Procedure 8-4** Power LED does illuminate when ODU cable is removed

| | |
|---|---|
| **1** | Remove the jumper (J905) found inside the PIDU Plus flap. |
| **2** | Measure the current with an ammeter placed across the two jumper pins. It should be 10 mA with the ODU disconnected.<br>If the ammeter reading is incorrect, report a suspected PIDU Plus fault to Motorola. |

If all tests so far have succeeded, proceed as follows:

**Procedure 8-5** Other power tests

| | |
|---|---|
| **1** | Reconnect the ODU cable to the PIDU Plus. |
| **2** | Measure the current with an ammeter placed across the two jumper pins. It should be in the range 300 mA to 1 A with the ODU connected. |
| **3** | If the ammeter reading is too high, the ODU may be drawing too much power, or the ODU may be short-circuited. Report a suspected ODU fault to Motorola. |
| **4** | If the ammeter reading is too low, the PIDU Plus may be supplying too little power. Report a suspected PIDU Plus fault to Motorola. |

## Power LED is flashing

If the green Power LED is flashing, proceed as follows:

**Procedure 8-6** Power LED is flashing

| | |
|---|---|
| **1** | Remove and examine the cable that connects the PIDU Plus to the LPU or ODU. |
| **2** | Check that pins 4&5 and 7&8 are not crossed with pins 1&2 and 3&6. |
| **3** | Check that the resistance between pins 1&8 is greater than 100K ohms. |
| **4** | If either check fails, replace or repair the cable that connects the PIDU Plus to the LPU or ODU. |

## Ethernet LED did not flash 10 times

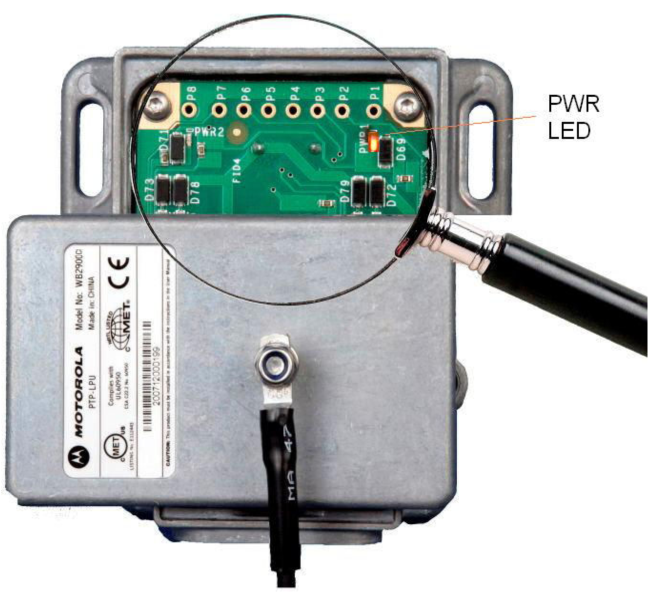
When the PIDU Plus is connected to the power supply and the green Power LED illuminates, there should be a 45 second delay, following which the yellow Ethernet LED should flash 10 times.

If the Ethernet LED did not flash 10 times, proceed as follows:

**Procedure 8-7** Ethernet LED did not flash 10 times

| | |
|---|---|
| **1** | Remove and examine the cable that connects the PIDU Plus to the LPU or ODU. |
| **2** | Check that the wiring to pins 4&5 and 7&8 is correct. For example, the wiring to pins 4 and 7 may be crossed. |
| **3** | Use the LPU (if installed) to check that power is available on the cable to the ODU. Access the connections by rotating the LPU lid as shown in Figure 8-3. Slacken the lid nut but do not remove it. |
| **4** | Test that test point P1 on the LPU PCB corresponds to pin 1 on the RJ45. Repeat for points P2 to P8. |
| **5** | Check that the PWR LED near the top right of the LPU PCB is illuminated to indicate power in the Ethernet cable (Figure 8-3). |
| **6** | If any test fails, replace or repair the cable that connects the PIDU Plus to the LPU or ODU. |

**Figure 8-3** PTP LPU test points and PWR LED



## No Ethernet activity

If the Ethernet LED did flash 10 times but then went off, proceed as follows:

**Procedure 8-8** Ethernet LED flashed 10 times then went out

| | |
|---|---|
| **1** | Check that the RJ45 connection from the LAN port of the PIDU Plus to the PC is working. |
| **2** | If the PC connection is working, remove and examine the cable that connects the PIDU Plus to the LPU or ODU. |
| **3** | Check that the wiring to pins 1&2 and 3&6 is correct. For example, the wiring to pins 1 and 3 may be crossed. |
| **4** | If this test fails, replace or repair the cable that connects the PIDU Plus to the LPU or ODU. |

## Irregular Ethernet activity

The yellow Ethernet LED should blink randomly as normal traffic passes through. If the Ethernet LED flashes irregularly, for example there is a short flash followed by a long flash, this indicates that the ODU has booted in recovery mode. The causes may be installation wiring or a corrupt ODU software load. For more information, see Using recovery mode on page 7-53.

## Connection is not 100 BaseT

If the Ethernet connection to the network is only 10 BaseT, when 100 BaseT is expected, proceed as follows:

**Procedure 8-9** Connection is not 100 BaseT

| | |
|---|---|
| **1** | Remove and examine the cable that connects the PIDU Plus to the LPU or ODU. |
| **2** | Check that the wiring to pins 4&5 and 7&8 is correct. For example, the wiring to pins 4 and 7 may be crossed. |
| **3** | If this test fails, replace or repair the cable that connects the PIDU Plus to the LPU or ODU. |

## Test Ethernet packet errors reported by ODU

To test for Ethernet packet errors, proceed as follows:

**Procedure 8-10** Test for Ethernet packet errors

| | |
|---|---|
| **1** | Log in to the ODU and select **Administration**, **Statistics**, **Detailed Counters**. |
| **2** | Select **Reset System Counters** at the bottom of the page and wait until the Ethernet Rx Packets counter has reached 1 million.<br>**NOTE**<br>The count will only update when the page is refreshed. |
| **3** | If the counter does not increment or increments too slowly, because for example the link is newly installed and there is no offered Ethernet traffic, then abandon this procedure and consider using the procedure Test ping packet loss on page 8-10. |
| **4** | Check the Ethernet Rx Crc And Align counter. The test has passed if this is less than 10. |

## Test Ethernet packet errors reported by managed switch or router

If the ODU is connected to a managed Ethernet switch or router, it may be possible to monitor the error rate of Ethernet packets. Please refer to the user guide of the managed network equipment.

The test has passed if the rate of packet errors reported by the managed Ethernet switch or router is less than 10 in 1 million packets.

## Test ping packet loss

Using a computer, it is possible to generate and monitor packets lost between the PIDU Plus and the ODU. This can be achieved by executing the Command Prompt application which is supplied as standard with Windows and MAC operating systems.

To test ping packet loss, proceed as follows:

**Procedure 8-11** Test ping packet loss

| | |
|---|---|
| **1** | Ensure that the IP address of the computer is configured appropriately for connection to the ODU under test. |
| **2** | Ensure that the IP address of the computer does not clash with other devices connected to the network. |
| **3** | If the PIDU Plus is connected to an Ethernet switch or router then connect the computer to a spare port, if available. |
| **4** | If it is not possible to connect the computer to a spare port of an Ethernet switch or router, then the PIDU Plus will need to be disconnected from the network in order to execute this test.<br>⚠ CAUTION<br>The following steps will disrupt network traffic carried by the ODU under test:<br>Disconnect the PIDU Plus from the network.<br>Connect the computer directly to the LAN port of the PIDU Plus. |
| **5** | On the computer, open the Command Prompt application. |

| | |
|---|---|
| **6** | Send 1000 ping packets of length 1500 bytes. The process will take 1000 seconds, which is approximately 17 minutes.<br>If the computer is running a Windows operating system, this is achieved by typing:<br>**`ping –n 1000 –l 1500 <ipaddress>`**<br>where <ipaddress> is the IP address of the ODU under test.<br>If the computer is running a MAC operating system, this is achieved by typing:<br>**`ping –c 1000 –s 1492 <ipaddress>`**<br>where <ipaddress> is the IP address of the ODU under test. |
| **7** | Record how many Ping packets have been lost. This is reported by Command Prompt on completion of the test.<br>The test has passed if the number of lost packets is less than 2. |

## Test resistance at the PIDU Plus end of the drop cable

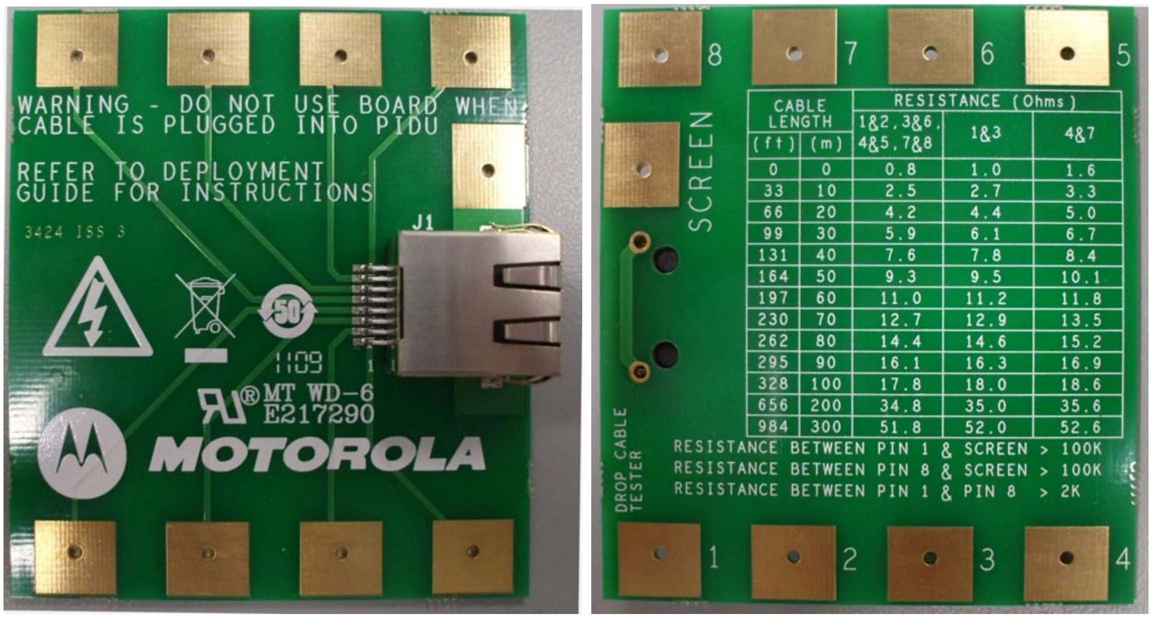
If the above procedures fail to diagnose the issue, there may be a fault in the wiring of the drop cable that connects the ODU (or LPU) to the PIDU Plus. Perform this task to test the resistances between the RJ45 pins.

Use the PTP drop cable tester (Figure 8-4) to make testing easier. This can be ordered from http://www.motorola.com/ptp/support by selecting **Order Cable Tester** and completing the order form.

**NOTE**

The values printed on the PTP drop cable tester are example values and should only be used for guidance.

**Figure 8-4** Drop cable tester (front and back views)




If PTP-SYNC is not installed, unplug the drop cable from the ODU port of the PIDU Plus. If PTP-SYNC is installed, unplug the drop cable from the ODU OUT port of the PTP-SYNC unit. Connect the drop cable tester to the end of the drop cable. Then, perform the tests described in Table 8-1. Record the results in the Result column, if this is helpful.

**Table 8-1** RJ45 cable resistance tests at the PIDU Plus end

| Step | Test | Result |
|---|---|---|
| 1 | Measure the resistance between pins 1 and 2. | Ohms |
| 2 | Measure the resistance between pins 3 and 6. | Ohms |
| 3 | Measure the resistance between pins 4 and 5. | Ohms |
| 4 | Measure the resistance between pins 7 and 8. | Ohms |
| 5 | Ensure that all the results of steps 1 to 4 are within 10% of each other as follows:<br>Take the minimum result and multiply by 1.1.<br>If any of the remaining steps 1 to 4 results are greater than this, the test has failed. | PASS or FAIL |

| Step | Test | Result |
|---|---|---|
| 6 | Measure the resistance between pins 1 and 3. Subtract 0.2 Ohms. | Ohms |
| 7 | Measure the resistance between pins 4 and 7. Subtract 0.8 Ohms. | Ohms |
| 8 | Compare the results of steps 1 to 4 and steps 6 to 7 to the maximum allowed, that is 20 Ohms.<br>If any of the steps 1 to 6 results are greater than the maximum allowed, the test has failed. | PASS or FAIL |
| 9 | Measure the resistance between pin 1 and the screen (ODU ground). If it is less than 100K ohms (regardless of cable length), the test has failed. | K Ohms<br>PASS or FAIL |
| 10 | Measure the resistance between pin 8 and the screen (ODU ground). If it is less than 100K ohms (regardless of cable length), the test has failed. | K Ohms<br>PASS or FAIL |
| 11 | Measure the resistance between pin 1 and pin 8. If it is less than 100K Ohms (regardless of cable length), the test has failed. | K Ohms<br>PASS or FAIL |

# Testing the radio link

If the radio link is not working, or it is unreliable, or the data throughput rate is too low, perform the tests specified in this section. It may be necessary to test the ODUs at both ends of the link.

## No activity

If there is no wireless activity, perform Procedure 8-12.

**Procedure 8-12** Testing an inactive radio link

| | |
|---|---|
| **1** | Check for Alarm conditions on Home page. |
| **2** | Check that the software at each end of the link is the same version. |
| **3** | Check that the Target Mac address is correctly configured at each end of the link. |
| **4** | Check Range. |
| **5** | Check Tx Power. |
| **6** | Check License keys to ensure that both units are the same product variant. |
| **7** | Check Master/Slave status for each unit and ensure that one unit is Master and the other unit is slave. |
| **8** | Check that the link is not obstructed or the ODU misaligned. |
| **9** | Check the DFS page at each end of the link and establish that there is a quiet wireless channel to use. |
| **10** | If there are no faults found in the configuration and there is absolutely no wireless signal, retry the installation procedure. |
| **11** | If this does not work then report a suspected ODU fault to Motorola. |

## Some activity

If there is some activity but the link is unreliable or does not achieve the data rates required, perform Procedure 8-13.

**Procedure 8-13** Testing a slow or unreliable radio link

| | |
|---|---|
| **1** | Check that the interference has not increased using the i-DFS measurements. |
| **2** | If a quieter channel is available check that it is not barred. |
| **3** | Check that the path loss is low enough for the communication rates required. |
| **4** | Check that the ODU has not become misaligned. |

# Testing after a lightning strike

If a link end installation is struck by lightning, perform Procedure 8-14.

**Procedure 8-14** Testing a link end after lightning strike

| | |
|---|---|
| **1** | Perform the tests specified in Testing link end hardware on page 8-2. |
| **2** | Ensure that the PIDU Plus is working and that the resistances are correct as specified in Test resistance at the PIDU Plus on page 8-11. |
| **3** | If the ODU is not working, power off the ODU and both LPUs and return them to Motorola. |
| **4** | If the ODU is working but there is suspicion of damage to the LPU, then refer to *LPU Operational Troubleshooting (phn-1362)*. |

# Testing PTP-SYNC

Refer to Table 1-6 for descriptions of the PTP-SYNC LEDs.

## LEDs do not illuminate

Ensure that there is a cable connection between the PIDU Plus 'ODU' interface and the 'PIDU IN' interface of the PTP-SYNC unit.

## The 'STATUS' LED does not blink

This probably indicates that a 1PPS synchronization pulse is not detected by the PTP-SYNC unit (no satellite lock).

Depending on system configuration, take one of the following actions:

- System using a GPS receiver module - Ensure that there is a cable connection between the PTP-SYNC 'GPS/SYNC IN' interface and the LPU, also that there is a cable connection between the LPU and the GPS receiver module. Check that the GPS receiver module has an uninterrupted view of the sky.
- System using an alternative 1PPS timing source - Ensure that there is a cable connection between the PTP-SYNC 'GPS/SYNC IN' or '1PPS IN' interface and the 1PPS timing source.
- On cluster slave units – Ensure that there is a cable connection between the slave GPS/SYNC IN interface and the SYNC OUT interface of the preceding unit in the chain.

## The 'ODU' LED does not illuminate within 90 seconds of power-up

This probably indicates that there is no communication between PTP-SYNC and ODU

Ensure that the PTP-SYNC 'ODU OUT' interface is connected to the ODU (and LPUs if installed) via the drop cable .

## The ‘GPS’ LED does not illuminate or blink on clustered PTP-SYNC units

This indicates a fault only when the timing source is a GPS receiver.

Table 8-2 describes the action to be taken depending upon the behavior of the ‘GPS’ LEDs at the master and slave(s).

**Table 8-2** Clustered PTP-SYNC units - ‘GPS’ LEDs Fault-finding

| Cluster timing source | ‘GPS’ LED on master | ‘GPS’ LED on slave(s) | Diagnosis |
|---|---|---|---|
| GPS receiver providing NMEA data | Blink | Blink | OK |
| | Off | Any | Fault in GPS unit or GPS cable |
| | Blink | Off | Fault in daisy chain cable |
| Alternative 1PPS source, no NMEA data | Off | Off | OK |
| | Off | On | Fault in alternative 1PPS source |
| One ODU is cluster timing master | Off | Off | OK |

# Testing a telecoms link

If an E1 or T1 link has been installed, it may be helpful to test the link by performing a loopback test.

This task consists of the following procedure:

- Performing a telecoms loopback test on page 8-19

## Performing a telecoms loopback test

The loopback test allows the telecoms data stream to be looped back at the copper or wireless interface. A typical T1 or E1 installation might include a 'Copper' loopback on the local unit followed by a 'Wireless' loopback on the remote unit.

NOTE

The Telecoms page is only available when the Telecoms Interface has been set to either T1 or E1, as described in Task 8: Configuring wireless and telecoms interfaces on page 6-26.

To perform a loopback test, proceed as follows:

**Procedure 8-15** Configure telecoms circuits for network

| | |
|---|---|
| **1** | Select menu option **System, Configuration, Telecoms**. The Telecoms page is displayed (Figure 8-5). |
| **2** | Select the Telecoms Loopback option: 'Copper' or 'Wireless' (Table 8-3). |
| **3** | Select **Submit Updated System Configuration**. |
| **4** | Perform loopback tests. |
| **5** | Reset Telecoms Loopback to 'None' for operational use.<br>Alarms on the Home Page indicate the presence of loopbacks on either channel. |

**Figure 8-5** Telecoms page

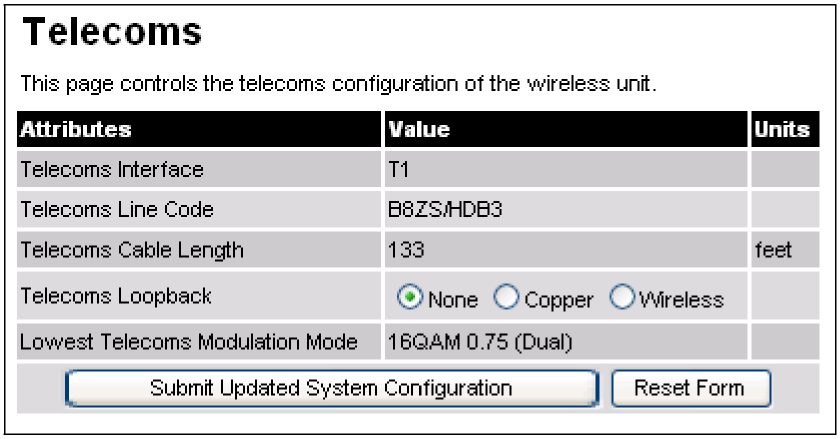



**Table 8-3** Telecoms Loopback values

| Value | Meaning |
|---|---|
| None | This is the required setting for an operational link. |
| Copper | Connects the received data on a given telecoms interface to the transmit interface.<br><br>May be used, in conjunction with a Bit Error Rate Tester, to confirm that the correct connections have been made to the ODU. This mode cannot be used for resistance tests, as it is only capable of looping back valid telecoms signals. |
| Wireless | Sends the telecoms data received from the wireless link back across the link on the same telecoms channel.<br><br>The link may be checked using, for example, a Bit Error Rate Tester to ensure that no errors are detected. |

# Glossary

| Term | Definition |
|---|---|
| ARP | Address Resolution Protocol |
| ATPC | Automatic Transmit Power Control |
| BPSK | Binary Phase Shift Keying |
| CSP | Critical Security Parameter |
| DC | Direct Current |
| DER | Distinguished Encoding Rules |
| DFS | Dynamic Frequency Selection |
| EIRP | Equivalent Isotropic Radiated Power |
| ETSI | European Telecommunications Standards Institute |
| FAQ | Frequently Asked Question |
| FIPS | Federal Information Processing Standard |
| GPS | Global Positioning System |
| HTTP | Hypertext Transfer Protocol |
| ID | Identity |
| IEEE | Institute of Electrical and Electronic Engineers |
| IP | Internet Protocol |
| ISM | Industrial Scientific and Medical |
| ITPE | Initial Transmit Power Estimate |
| LAN | Local Area Network |
| LOS | Line-of-Sight (clear line-of-sight, and Fresnel zone is clear) |
| LPU | Lightning Protection Unit |
| MAC | Medium Access Control Layer |

| Term | Definition |
|---|---|
| MDI | Medium Dependent Interface |
| MDIX | Medium Dependent Interface Crossover |
| MIB | Management Information Base |
| NLOS | Non-Line-of-Sight |
| NMEA | National Marine Electronics Association |
| ODU | Outdoor Unit |
| OFDM | Orthogonal Frequency Division Multiplex |
| PC | IBM Compatible Personal Computer |
| PIDU Plus | Powered Indoor Unit |
| PING | ICMP Echo Request |
| PTP | Point-to-Point |
| QAM | Quadrature Amplitude Modulation |
| RAM | Random Access Memory |
| RF | Radio Frequency |
| RSSI | Received Signal Strength Indication |
| SELV | Safety Extra Low Voltage |
| SMTP | Simple Mail Transport Protocol |
| SNMP | Simple Network Management Protocol |
| SNTP | Simple Network Time Protocol |
| STP | Shielded Twisted Pair |
| STP | Spanning Tree Protocol |
| TCP | Transmission Control Protocol |
| TDWR | Terminal Doppler Weather Radar |
| URL | Universal Resource Location |
| UTP | Unshielded Twisted Pair |
| UV | Ultraviolet |
| VLAN | Virtual Local Area Network |

# Index