Chapter 5: Installation

This chapter describes how to install and test the hardware for a PTP 650 link. It contains the following topics:

- Safety on page 5-2 contains important safety guidelines that must be observed by personnel installing or operating PTP 650 equipment.
- Installing the ODU and top LPU on page 5-5 describes how to mount and ground an integrated or connectorized ODU, how to mount and ground the top LPU, and how to mount and connect an external antenna for the connectorized ODU.
- Installing the copper Cat5e Ethernet interface on page 5-13 describes how to install the copper Cat5e power over Ethernet interface from the ODU (PSU port) to the PSU.
- Installing the PSU on page 5-21 describes how to install a power supply unit for the PTP 650, either the AC Power Injector or the AC+DC Enhanced Power Injector.
- Installing an SFP Ethernet interface on page 5-23 describes how to install an optical or copper Cat5e Ethernet interface from the ODU (SFP port) to a connected device.
- Installing an Aux Ethernet interface on page 5-32 describes how to install a copper Cat5e Ethernet interface from the ODU (Aux port) to a connected device.
- Supplemental installation information on page 5-33 contains detailed installation procedures that are not included in the above topics, such as how to strip cables, create grounding points and weatherproof connectors.

Note

These instructions assume that LPUs are being installed from the PTP 650 LPU and grounding kit (Cambium part number C000065L007). If the installation does not require LPUs, adapt these instructions as appropriate.

If LPUs are being installed, only use the five black-capped EMC cable glands supplied in the LPU and grounding kit. The silver-capped cable glands supplied in the ODU kits must only be used in PTP 650 installations which do not require LPUs.

Safety

Warning

To prevent loss of life or physical injury, observe the following safety guidelines. In no event shall Cambium Networks be liable for any injury or damage caused during the installation of the Cambium PTP 650. Ensure that only qualified personnel install a PTP 650 link.

Power lines

Exercise extreme care when working near power lines.

Working at heights

Exercise extreme care when working at heights.

PSU

Always use one of the Cambium PTP 650 Series power supply units (PSU) to power the ODU. Failure to use a Cambium supplied PSU could result in equipment damage and will invalidate the safety certification and may cause a safety hazard.

Grounding and protective earth

The Outdoor Unit (ODU) must be properly grounded to protect against lightning. It is the user's responsibility to install the equipment in accordance with national regulations. In the USA follow the requirements of the National Electrical code NFPA 70-2005 and 780-2004 *Installation of Lightning Protection Systems*. In Canada, follow Section 54 of the *Canadian Electrical Code*. These codes describe correct installation procedures for grounding the outdoor unit, mast, lead-in wire and discharge unit, size of grounding conductors and connection requirements for grounding electrodes. Other regulations may apply in different countries and therefore it is recommended that installation of the outdoor unit be contracted to a professional installer.

DC supply

To power the ODU from a DC supply, use the AC+DC Enhanced Power Injector (PSU) (Cambium part number C000065L002). Ensure that the DC power supply meets the requirements specified in PSU DC power supply on page 3-12.

Powering down before servicing

Before servicing PTP 650 equipment, always switch off the power supply and unplug it from the PSU.

Do not disconnect the RJ45 drop cable connectors from the ODU while the PSU is connected to the power supply. Always remove the AC or DC input power from the PSU.

Primary disconnect device

The main power supply is the primary disconnect device. The AC+DC Enhanced power injector is fused on the DC input. Some installations will also require an additional circuit breaker or isolation switch to be fitted in the DC supply.

External cables

Safety may be compromised if outdoor rated cables are not used for connections that will be exposed to the outdoor environment. For outdoor copper Cat5e Ethernet interfaces, always use Cat5e cable that is gel-filled and shielded with copper-plated steel. Alternative types of drop cable are not supported by Cambium Networks.

Drop cable tester

The PSU output voltage may be hazardous in some conditions, for example in wet weather. Do NOT connect the drop cable tester to the PSU, either directly or via LPUs.

RF exposure near the antenna

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

Minimum separation distances

Ensure that personnel are not exposed to unsafe levels of RF energy. The units start to radiate RF energy as soon as they are powered up. Never work in front of the antenna when the ODU is powered. Install the ODUs so as to provide and maintain the minimum separation distances from all persons. For minimum separation distances, see Calculated distances and power compliance margins on page 4-25.

Grounding and lightning protection requirements

Ensure that the installation meets the requirements defined in Grounding and lightning protection on page 3-8.

Grounding cable installation methods

To provide effective protection against lightning induced surges, observe these requirements:

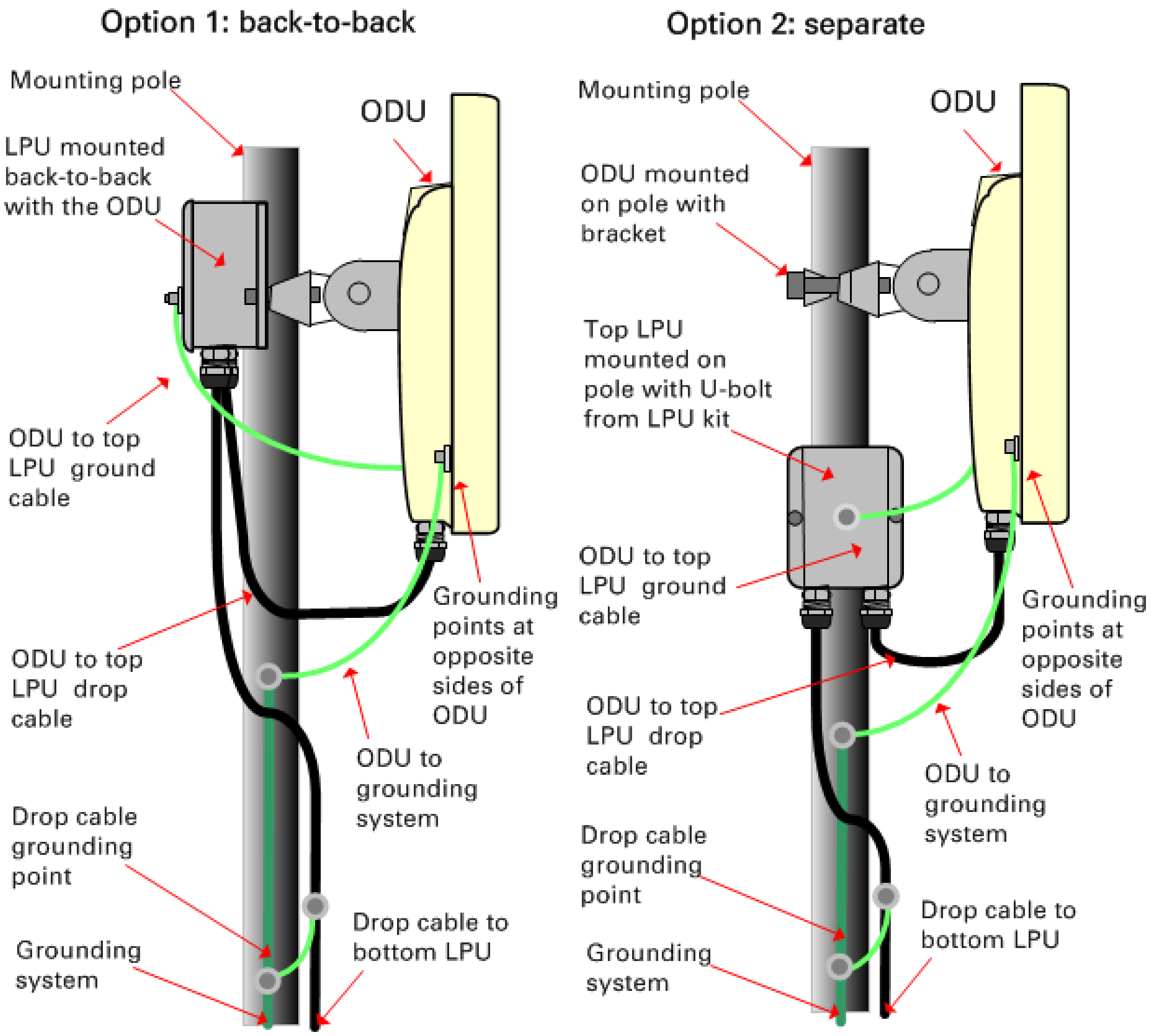
- Grounding conductor runs are as short, straight and smooth as possible, with bends and curves kept to a minimum.
- Grounding cables must not be installed with drip loops.
- All bends must have a minimum radius of 203 mm (8 in) and a minimum angle of 90°. A diagonal run is preferable to a bend, even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

Siting ODUs and antennas

ODUs and external antennas are not designed to survive direct lightning strikes. For this reason they must be installed in Zone B as defined in Lightning protection zones on page 3-8. Mounting in Zone A may put equipment, structures and life at risk.

Installing the ODU and top LPU

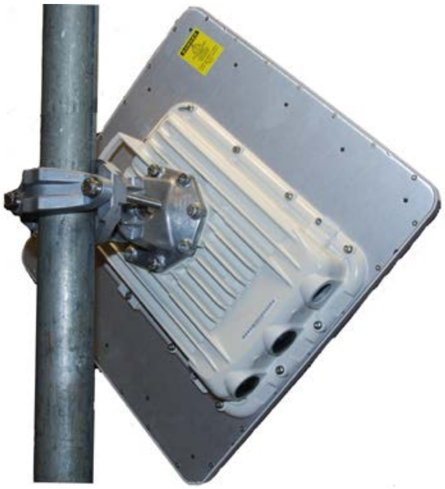
Decide how to mount the ODU and top LPU


Option 1: back-to-back
Mounting pole
ODU
LPU mounted back-to-back with the ODU
ODU to top LPU ground cable
ODU to top LPU drop cable
Grounding points at opposite sides of ODU
ODU to grounding system
Drop cable grounding point
Grounding system
Drop cable to bottom LPU
Option 2: separate
Mounting pole
ODU
ODU mounted on pole with bracket
Top LPU mounted on pole with U-bolt from LPU kit
ODU to top LPU ground cable
ODU to top LPU drop cable
Grounding points at opposite sides of ODU
ODU to grounding system
Drop cable grounding point
Grounding system
Drop cable to bottom LPU

Note

For improved radio performance, mount the integrated ODU at 45 degrees to the vertical.

The mounting pole may be vertical or horizontal.



Prepare ODU for mounting

1 Use the correct mounting bracket for the pole diameter and ODU type:

- If pole diameter is between 50 and 75 mm (2 and 3 inches):

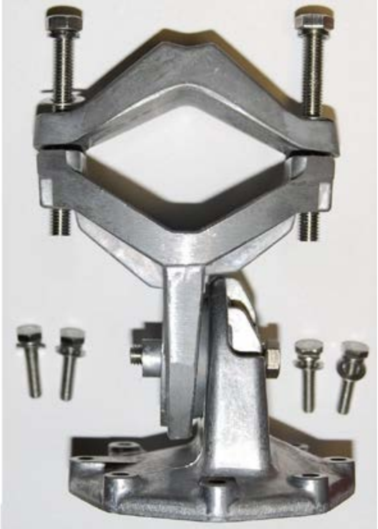
  (a) For an integrated ODU, use the integrated mounting bracket, Cambium part number N000065L031.

  (b) For a connectorized ODU, use the connectorized mounting bracket supplied with the ODU (alternatively, use the integrated ODU bracket).

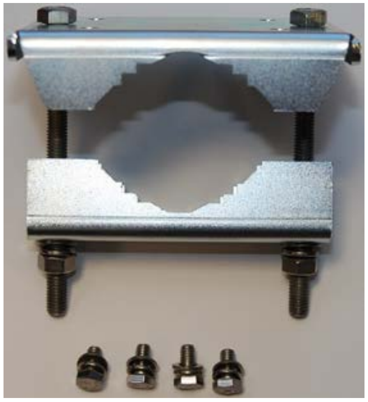
- If pole diameter is **either** 90 mm (3.5 inches) **or** 115 mm (4.5 inches):

  (c) For both integrated and connectorized ODUs, use the extended mounting bracket, Cambium part number N000065L030.

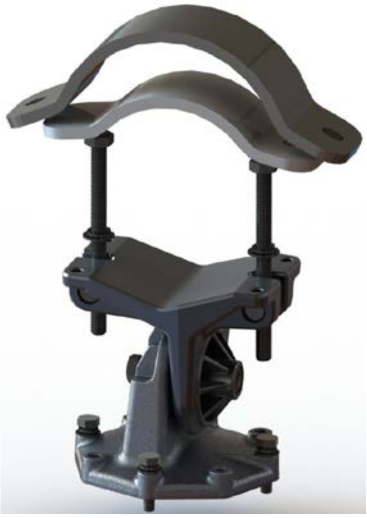
(a) Integrated bracket:



(b) Connectorized bracket:

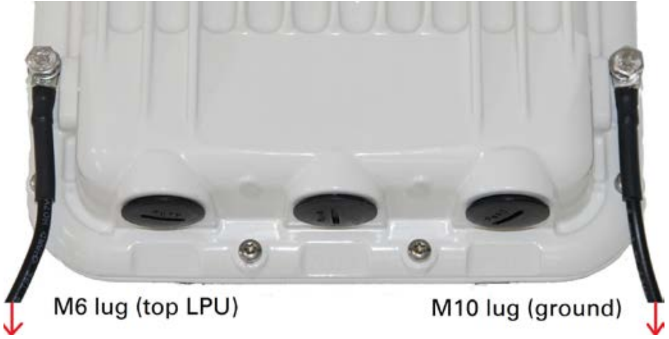


(c) Extended bracket:

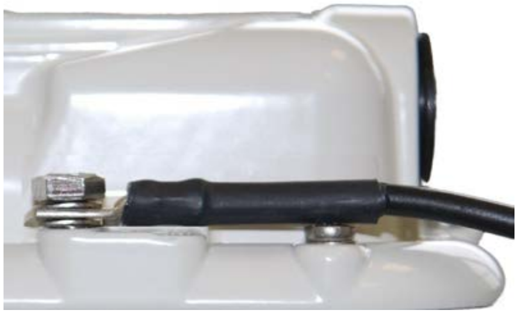


2 (a) Fasten one ground cable to each ODU grounding point using the M6 (small) lugs: one is for the top LPU (M6 lug at other end) and the other is for the tower or building (M10 lug at other end). It does not matter which cable goes on which ODU grounding point. (b) Tighten both ODU grounding bolts to a torque of 5 Nm (3.9 lb ft).

(a) ODU ground cables:



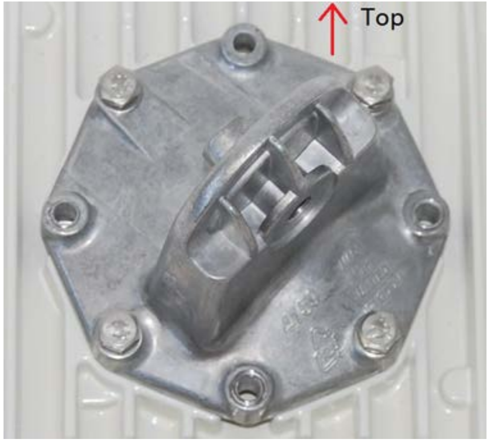
(b) ODU ground cable tightened:



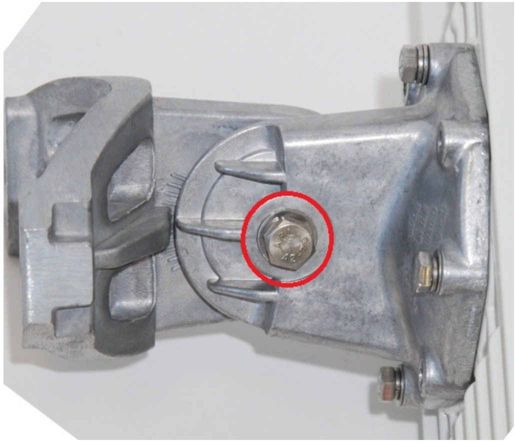
Integrated ODU

1 (a) Fix the mounting plate to the back of the ODU at an angle of 45 degrees to the vertical using the bolts and washers provided. Tighten the four bolts to a torque setting of 5 Nm (4 lb ft). (b) Fix the bracket body to the mounting plate using the M8 bolt.

(a) Fix the mounting plate:



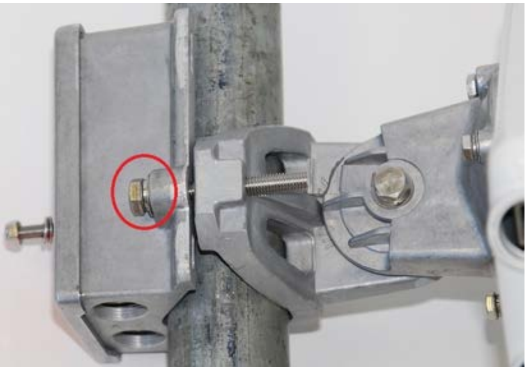
(b) Fix the bracket body:



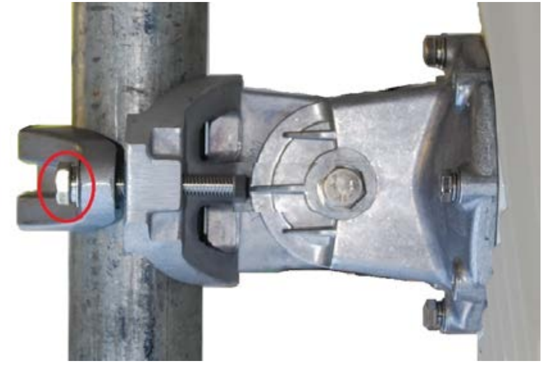
2 Hoist the ODU up to its position on the mounting pole.

3 (a) For back-to-back LPU mounting, fix the ODU to the pole using the LPU.
(b) For separate LPU mounting, fix the ODU to the pole using the bracket strap.

(a) Back-to-back LPU:

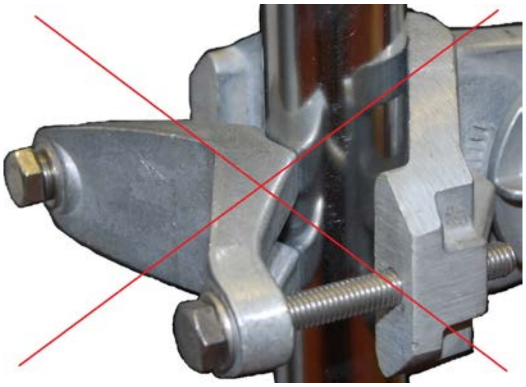


(b) Separate LPU:

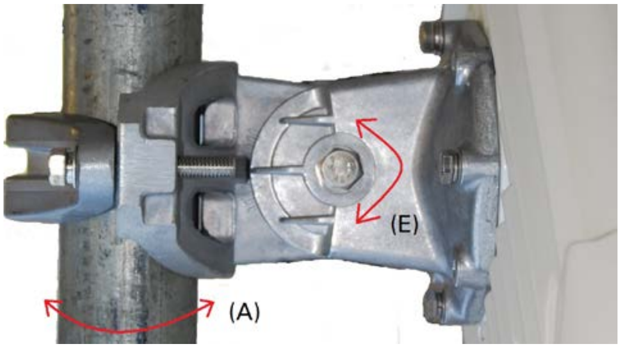


Caution

Do not reverse the ODU bracket strap, as this arrangement may lead to failure of the assembly:



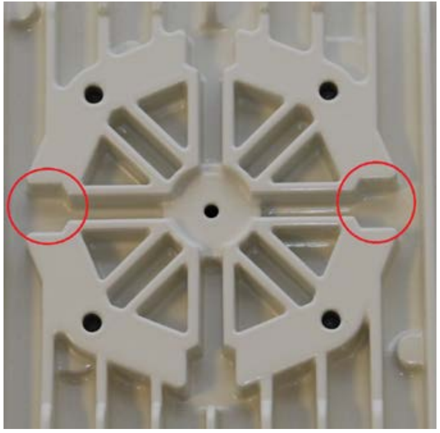
4 Adjust the elevation (E) and azimuth (A) of the unit to achieve initial alignment. Tighten all three M8 ODU bracket bolts to a torque setting of 14 Nm (11 lb ft). Do not over-tighten the bolts, as this may lead to failure of the assembly:



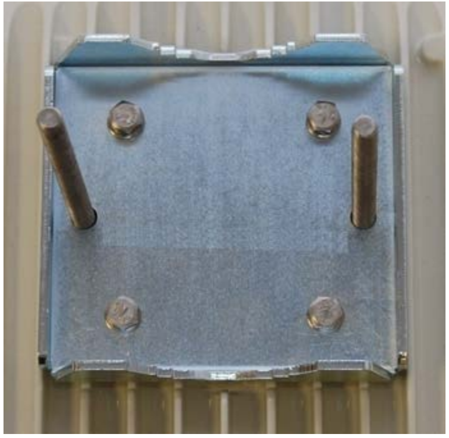
Connectorized ODU

1 (a) Line up the bolt heads with receptacles in the ODU. (b) Fix the mounting plate and bracket bolts to the back of the ODU using the bolts and washers. Tighten to a torque setting of 5 Nm (4 lb ft).

(a) Receptacles for bracket bolts:



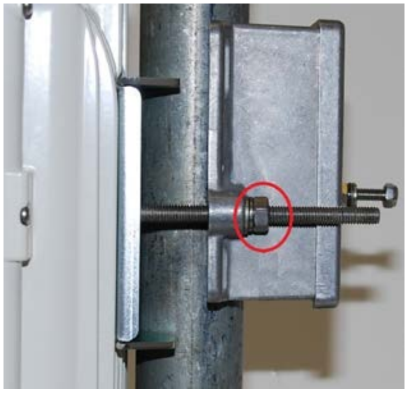
(b) Mounting plate fixed:



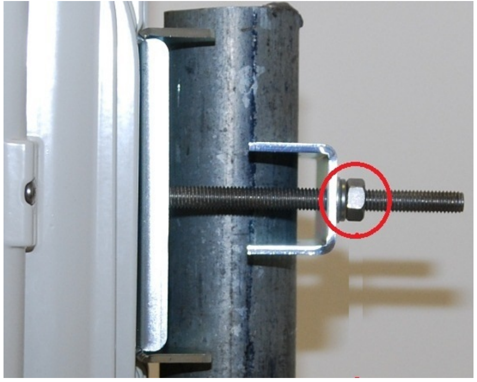
2 Hoist the ODU up to its position on the mounting pole.

3 (a) For back-to-back LPU mounting, fix the ODU to the pole using the LPU.
(b) For separate LPU mounting, fix the ODU to the pole using the bracket strap.

(c) Back-to-back LPU:



(d) Separate LPU:



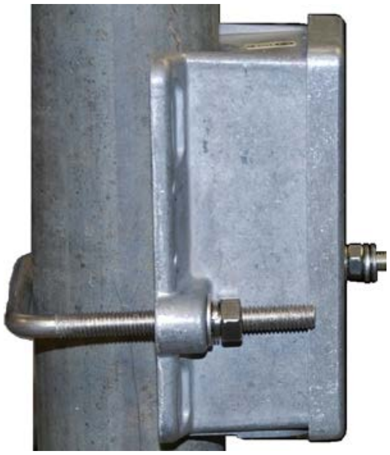
4 Tighten the mounting bolts to a torque setting of 7 Nm (5.5 lb ft). Do not over-tighten the bolts, as this may lead to failure of the assembly.

Ground the ODU and top LPU

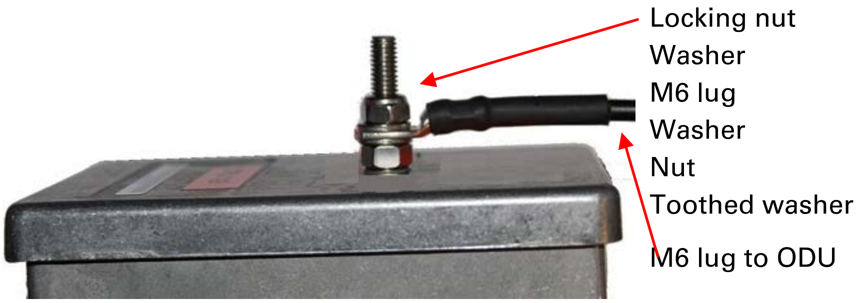
Caution

Do not attach grounding cables to the ODU mounting bracket bolts, as this arrangement will not provide full protection.

1 For separate LPU mounting, use the U-bolt bracket from the LPU kit to mount the top LPU on the pole below the ODU. Tighten to a torque setting of 7 Nm (5.5 lb ft):



2 Fasten the ODU grounding cable to the top LPU using the M6 (small) lug. Tighten both nuts to a torque of 5 Nm (3.9 lb ft):



3 Select a tower or building grounding point within 0.3 meters (1 ft) of the ODU bracket. Remove paint from the surface and apply anti-oxidant compound. Fasten the ODU grounding cable to this point using the M10 (large) lug.

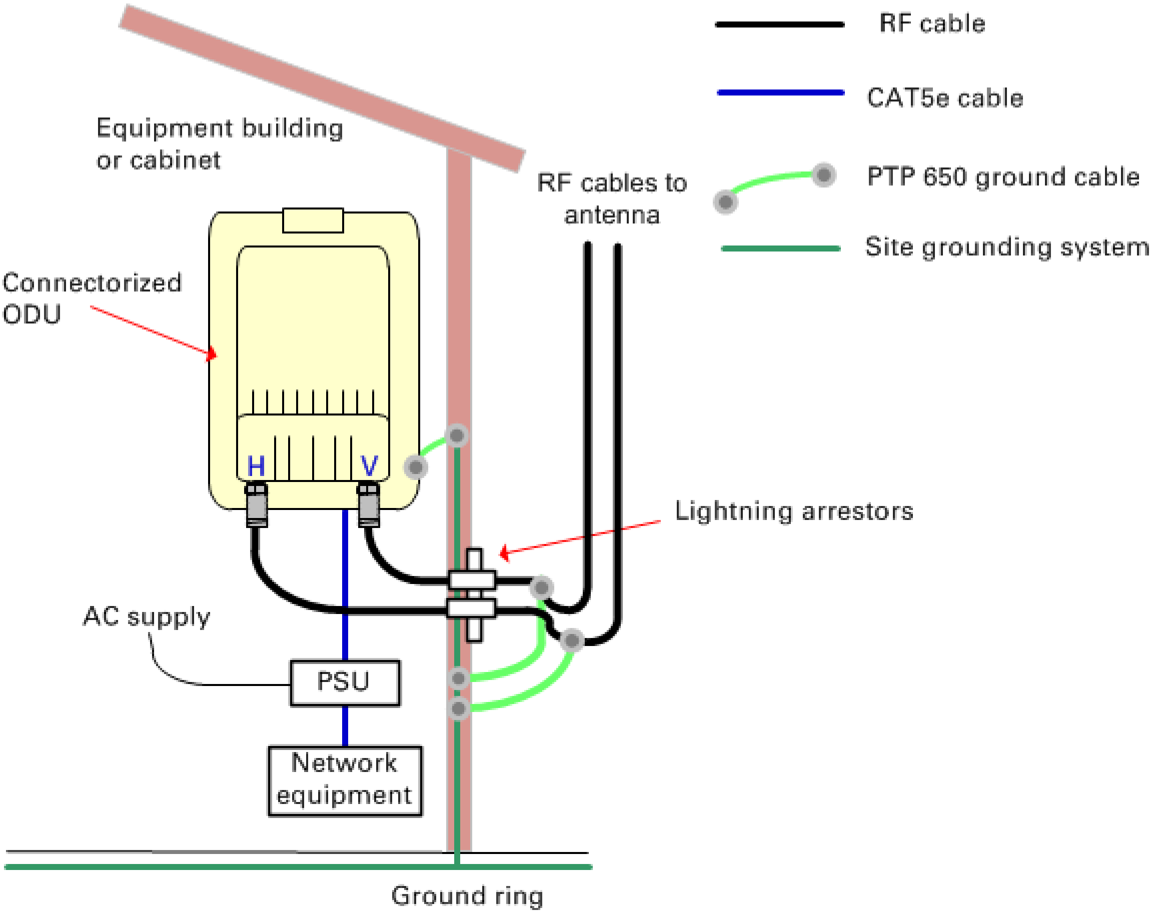
4 If local regulations mandate the independent grounding of all devices, add a third ground cable to connect the top LPU directly to the grounding system.

Install external antennas for a connectorized ODU

1 Mount the antenna(s) according to manufacturer's instructions. When using separate antennas to achieve spatial diversity, mount one with Horizontal polarization and the other with Vertical polarization.

2 Connect the ODU V and H interfaces to the antenna(s) with RF cable of type CNT-400 (Cambium part numbers 30010194001 and 30010195001) and N type connectors (Cambium part number 09010091001). Tighten the N type connectors to a torque setting of 1.7 Nm (1.3 lb ft).

3 If the ODU is mounted indoors, install lightning arrestors at the building entry point:

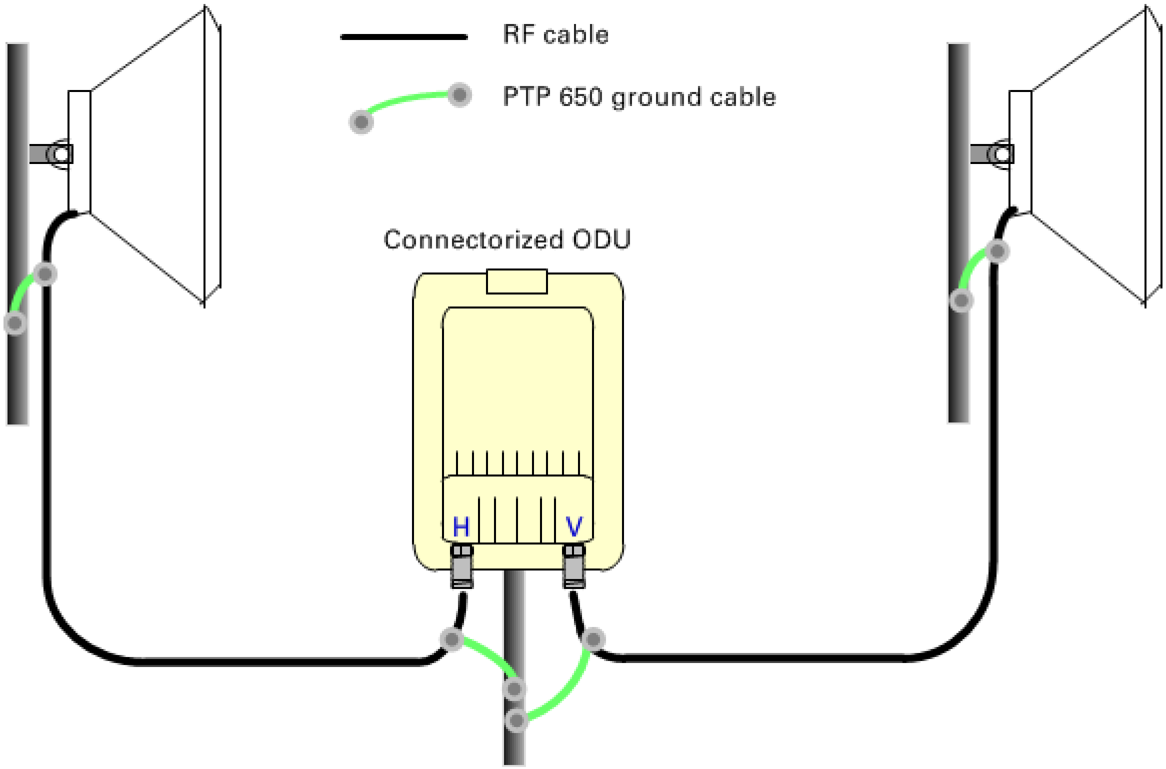


4 Form drip loops near the lower ends of the antenna cables. These ensure that water is not channeled towards the connectors.

5 If the ODU is mounted outdoors, weatherproof the N type connectors (when antenna alignment is complete) using PVC tape and self-amalgamating rubber tape.

6 Weatherproof the antenna connectors in the same way (unless the antenna manufacturer specifies a different method).

7 Ground the antenna cables to the supporting structure within 0.3 meters (1 foot) of the ODU and antennas using the Cambium grounding kit (part number 01010419001):



8 Fix the antenna cables to the supporting structure using site approved methods. Ensure that no undue strain is placed on the ODU or antenna connectors.

Caution

Ensure that the cables do not flap in the wind, as flapping cables are prone to damage and induce unwanted vibrations in the supporting structure.

Installing the copper Cat5e Ethernet interface

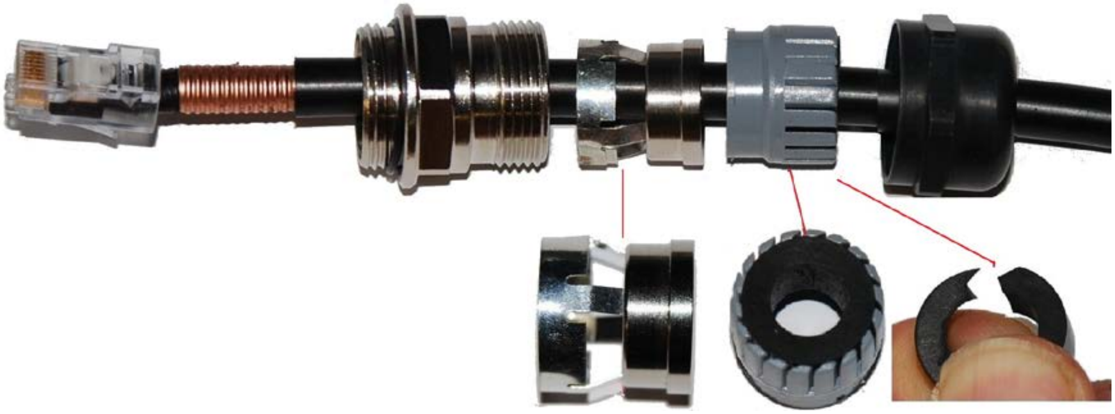
⚠	**Caution** To avoid damage to the installation, do not connect or disconnect the drop cable when power is applied to the PSU or network terminating equipment.
⚠	**Caution** Do not connect the SFP or Aux drop cables to the PSU, as this may damage equipment.
⚠	**Caution** Always use Cat5e cable that is gel-filled and shielded with copper-plated steel. Alternative types of Cat5e cable are not supported by Cambium Networks. Cambium Networks supply this cable (Cambium part numbers WB3175 and WB3176), RJ45 connectors (Cambium part number WB3177) and a crimp tool (Cambium part number WB3211). The LPU and grounding kit contains a 600 mm length of this cable.

Install the ODU to top LPU drop cable

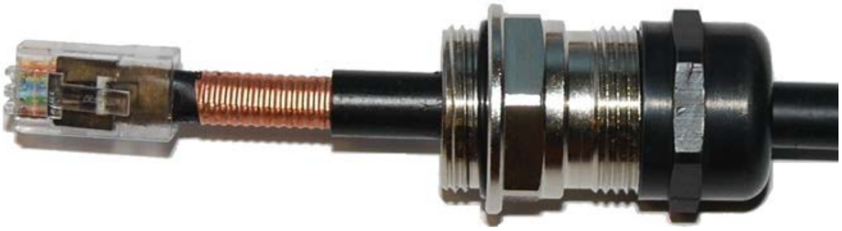
Fit glands to the ODU to top LPU drop cable

Fit EMC strain relief cable glands (with black caps) to both ends of the 600 mm length of pre-terminated cable. These parts are supplied in the LPU and grounding kit.

1 Disassemble the gland and thread each part onto the cable (the rubber bung is split). Assemble the spring clip and the rubber bung:



2 Fit the parts into the body and lightly screw on the gland nut (do not tighten it):

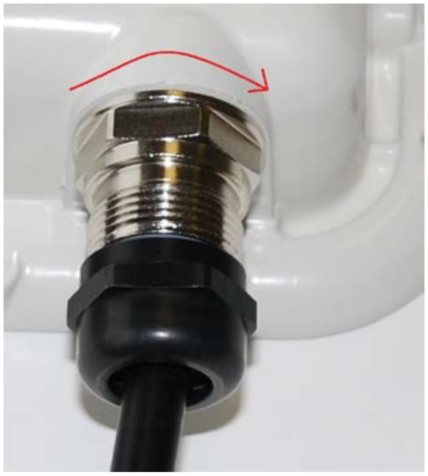


Connect the drop cable to the ODU (PSU port) and LPU

1 (a) Plug the RJ45 connector into the socket in the unit, ensuring that it snaps home.
(b) Fit the gland body to the RJ45 port and tighten it to a torque of 5.5 Nm (4.3 lb ft):

(a)

(b)

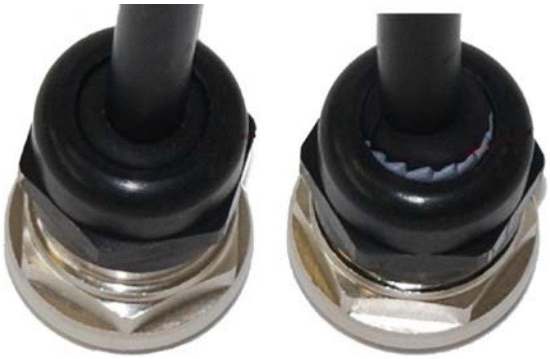


2 (a) Fit the gland nut and tighten until the rubber seal closes on the cable. (b) Do not over-tighten the gland nut, as there is a risk of damage to its internal components:

(a)

(b)

Correct Incorrect

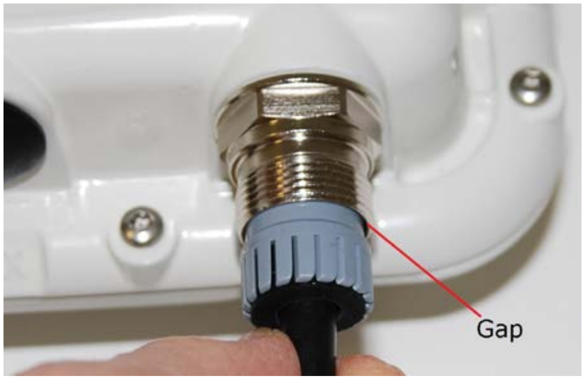


Disconnect the drop cable from the LPU or ODU

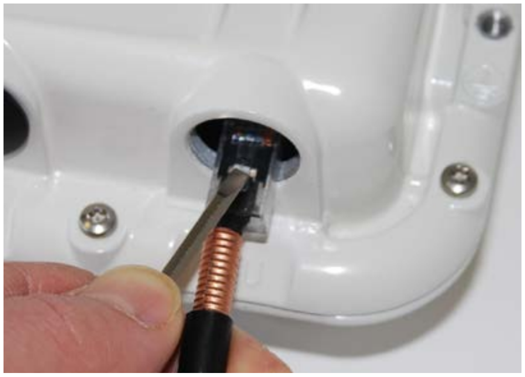
Use this procedure if it is necessary to remove an EMC strain relief cable gland and RJ45 connector from the ODU (as illustrated) or LPU.

1 (a) Remove the gland nut. Wiggle the drop cable to release the tension of the gland body. When the tension in the gland body is released, a gap opens at the point show. Unscrew the gland body.
(b) Use a small screwdriver to press the RJ45 locking tab, then remove the RJ45 connector.

(a)



(b)



Install the main drop cable

Warning

The metal screen of the drop cable is very sharp and may cause personal injury.

- ALWAYS wear cut-resistant gloves (check the label to ensure they are cut resistant).
- ALWAYS wear protective eyewear.
- ALWAYS use a rotary blade tool to strip the cable (DO NOT use a bladed knife).

Warning

Failure to obey the following precautions may result in injury or death:

- Use the proper hoisting grip for the cable being installed. If the wrong hoisting grip is used, slippage or insufficient gripping strength will result.
- Do not reuse hoisting grips. Used grips may have lost elasticity, stretched, or become weakened. Reusing a grip can cause the cable to slip, break, or fall.
- The minimum requirement is one hoisting grip for each 60 m (200 ft) of cable.

Cut to length and fit hoisting grips

1. Cut the main drop cable to length from the top LPU to the bottom LPU.
2. Slide one or more hoisting grips onto the top end of the drop cable.
3. Secure the hoisting grip to the cable using a special tool, as recommended by the manufacturer.

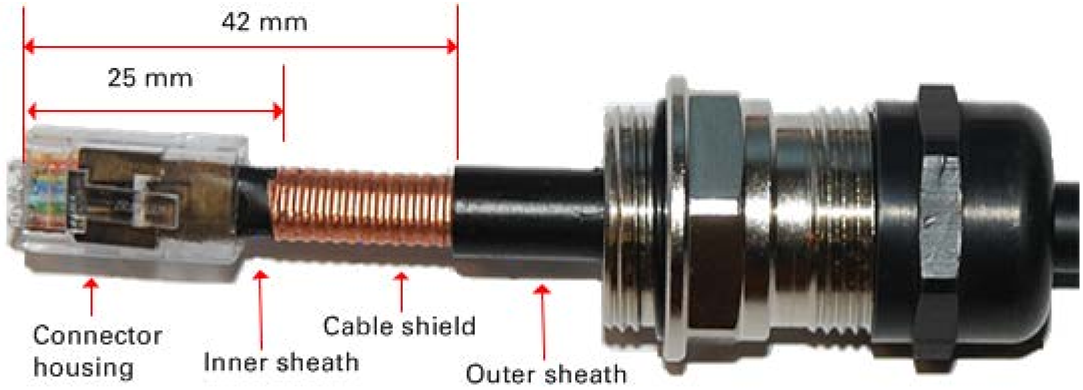
Terminate with RJ45 connectors and glands

Caution

Check that the crimp tool matches the RJ45 connector, otherwise the cable or connector may be damaged.

1. Thread the cable gland (with black cap) onto the main drop cable.
2. Strip the cable outer sheath and fit the RJ45 connector load bar.

3 Fit the RJ45 connector housing as shown. To ensure there is effective strain relief, locate the cable inner sheath under the connector housing tang. Do not tighten the gland nut:



Hoist and fix the main drop cable

Warning

Failure to obey the following precautions may result in injury or death:

- Use the hoisting grip to hoist one cable only. Attempting to hoist more than one cable may cause the hoisting grip to break or the cables to fall.
- Do not use the hoisting grip for lowering cable unless the clamp is securely in place.
- Maintain tension on the hoisting grip during hoisting. Loss of tension can cause dangerous movement of the cable and result in injury or death to personnel.
- Do not release tension on the grip until after the grip handle has been fastened to the supporting structure.
- Do not apply any strain to the RJ45 connectors.

Caution

Do not lay the drop cable alongside a lightning air terminal.

1 Hoist the top end of the main drop cable up to the top LPU, following the hoist manufacturer's instructions. When the cable is in position, fasten the grip handle to the supporting structure and remove the hoist line.

2 Connect the main drop cable to the top LPU by following the procedure Connect the drop cable to the ODU (PSU port) and LPU on page 5-14.

3 Run the main drop cable to the site of the bottom LPU.

4 Attach the main drop cable to the supporting structure using site approved methods.

Ground the main drop cable

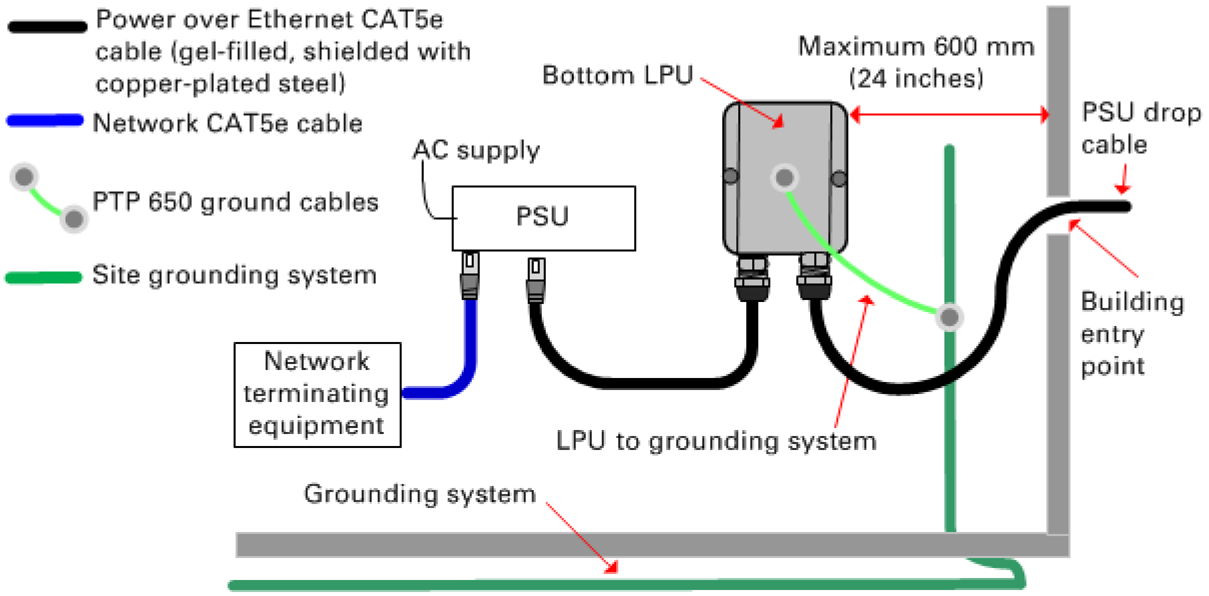
At all required grounding points, connect the screen of the main drop cable to the metal of the supporting structure using the cable grounding kit (Cambium part number 01010419001).

Install the bottom LPU to PSU drop cable

Install the bottom LPU

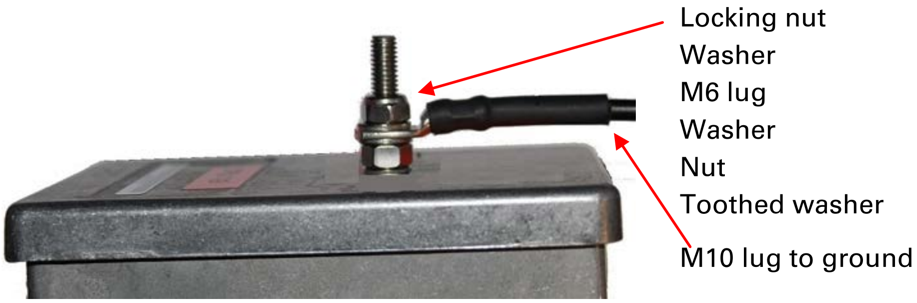
Install the bottom LPU, ground it, and connect it to the main drop cable.

1 Select a mounting point for the bottom LPU within 600 mm (24 in) of the building entry point. Mount the LPU vertically with cable glands facing downwards.



2 Connect the main drop cable to the bottom LPU by following the procedure Connect the drop cable to the ODU (PSU port) and LPU on page 5-14.

3 Fasten one ground cable to the bottom LPU using the M6 (small) lug. Tighten both nuts to a torque of 5 Nm (3.9 lb ft):



4 Select a building grounding point near the LPU bracket. Remove paint from the surface and apply anti-oxidant compound. Fasten the LPU ground cable using the M10 (large) lug.

Install the LPU to PSU drop cable

Use this procedure to terminate the bottom LPU to PSU drop cable with RJ45 connectors at both ends, and with a cable gland at the LPU end.

Warning

The metal screen of the drop cable is very sharp and may cause personal injury. ALWAYS wear cut-resistant gloves (check the label to ensure they are cut resistant). ALWAYS wear protective eyewear. ALWAYS use a rotary blade tool to strip the cable, not a bladed knife.

Caution

Check that the crimp tool matches the RJ45 connector, otherwise the cable or connector may be damaged.

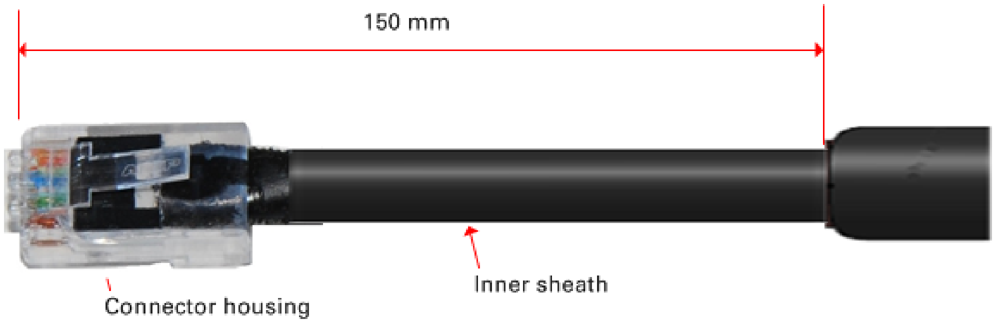
1 Cut the drop cable to the length required from bottom LPU to PSU.

2 **At the LPU end only**:

- Fit one cable gland and one RJ45 connector by following the procedure Terminate with RJ45 connectors and glands on page 5-16.

- Connect this cable and gland to the bottom LPU by following the procedure Connect the drop cable to the ODU (PSU port) and LPU on page 5-14.

4 **At the PSU end only**: Do not fit a cable gland. Strip the cable outer sheath and fit the RJ45 connector load bar. Fit the RJ45 connector housing. To ensure there is effective strain relief, locate the cable inner sheath under the connector housing tang:



Test resistance in the drop cable

Connect the bottom end of the copper Cat5e drop cable to a PTP drop cable tester and test that the resistances between pins are within the correct limits, as specified in the table below. If any of the tests fail, examine the drop cable for wiring faults. Order the PTP drop cable tester from the support website (http://www.cambiumnetworks.com/support).

Measure the resistance between…	Enter measured resistance	To pass test, resistance must be…	Circle "Pass" or "Fail"	Additional tests and notes
Pins 1 and 2	Ohms	<20 Ohms (60 Ohms) (*1)	Pass Fail	Resistances must be within 10% of each other (*2). Circle "Pass" or "Fail": Pass Fail
Pins 3 and 6	Ohms	<20 Ohms (60 Ohms) (*1)	Pass Fail	
Pins 4 and 5	Ohms	<20 Ohms (60 Ohms) (*1)	Pass Fail	
Pins 7 and 8	Ohms	<20 Ohms (60 Ohms) (*1)	Pass Fail	
Pin 1 and screen (ODU ground)	K Ohms	>100K Ohms	Pass Fail	These limits apply regardless of cable length.
Pin 8 and screen (ODU ground)	K Ohms	>100K Ohms	Pass Fail	

(*1) A resistance of 20 Ohms is the maximum allowed when the cable is carrying Ethernet.
A resistance of 60 Ohms is the maximum allowed when the cable is carrying only power to the ODU (when Ethernet is carried by one of the other ODU interfaces).

(*2) Ensure that these resistances are within 10% of each other by multiplying the lowest resistance by 1.1 – if any of the other resistances are greater than this, the test has failed.

Installing the PSU

Install one of the following types of PSU (as specified in the installation plan):

- PTP 650 AC Power Injector (Cambium part number N000065L001).
- PTP 650 AC+DC Enhanced Power Injector (Cambium part number C000065L002).

⚠ **Caution**

As the PSU is not waterproof, locate it away from sources of moisture, either in the equipment building or in a ventilated moisture-proof enclosure. Do not locate the PSU in a position where it may exceed its temperature rating.

⚠ **Caution**

Do not plug any device other than a PTP 650 ODU into the ODU port of the PSU. Other devices may be damaged due to the non-standard techniques employed to inject DC power into the Ethernet connection between the PSU and the ODU.

Do not plug any device other than a Cambium PTP 650 PSU into the PSU port of the ODU. Plugging any other device into the PSU port of the ODU may damage the ODU and device.

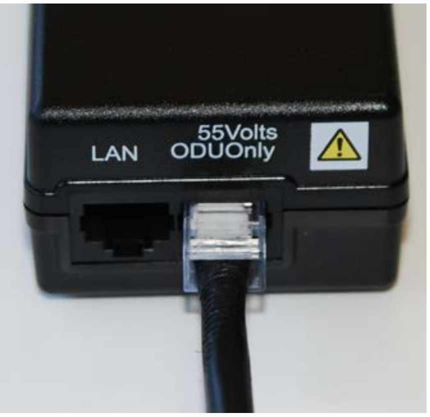
Installing the AC Power Injector

Follow this procedure to install the AC Power Injector (Cambium part number N000065L001):

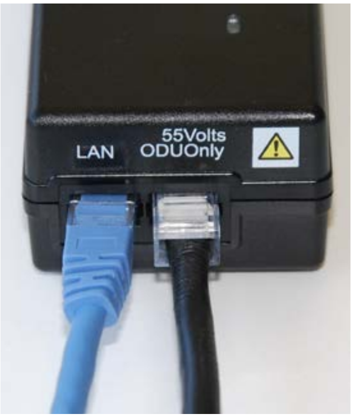
1. Form a drip loop on the PSU end of the LPU to PSU drop cable. The drip loop ensures that any moisture that runs down the cable cannot enter the PSU.

2. (a) Place the AC Power Injector on a horizontal surface. Plug the LPU to PSU drop cable into the PSU port labeled ODU. (b) When the system is ready for network connection, connect the network Cat5e cable to the LAN port of the PSU:

(a)



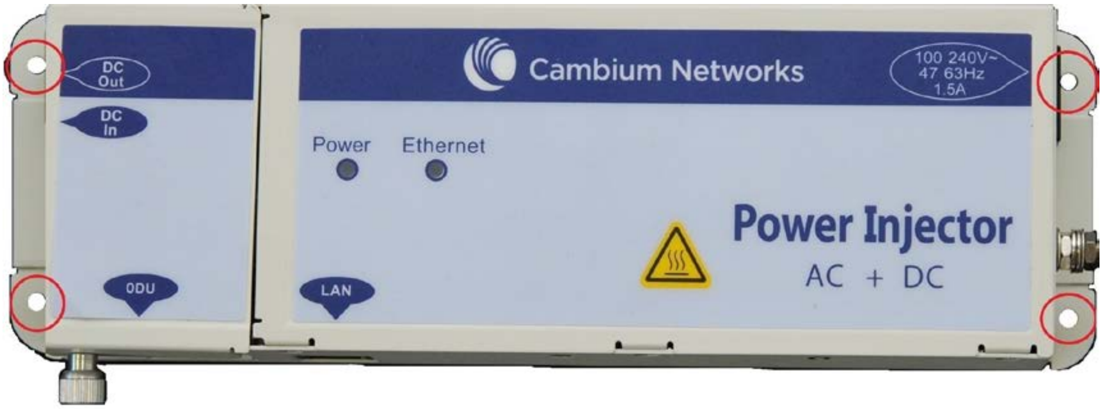
(b)



Installing the AC+DC Enhanced Power Injector

Follow this procedure to install the AC+DC Enhanced Power Injector (Cambium part number C000065L002):

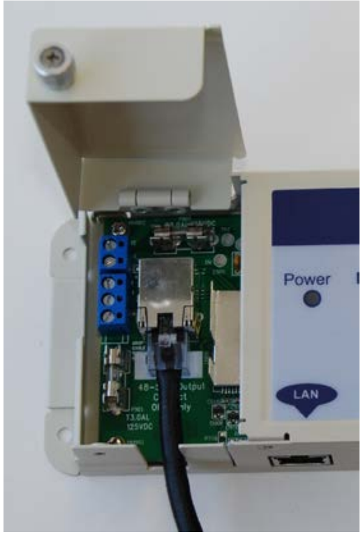
1 Mount the AC+DC power injector by screwing it to a vertical or horizontal surface using the four screw holes (circled):



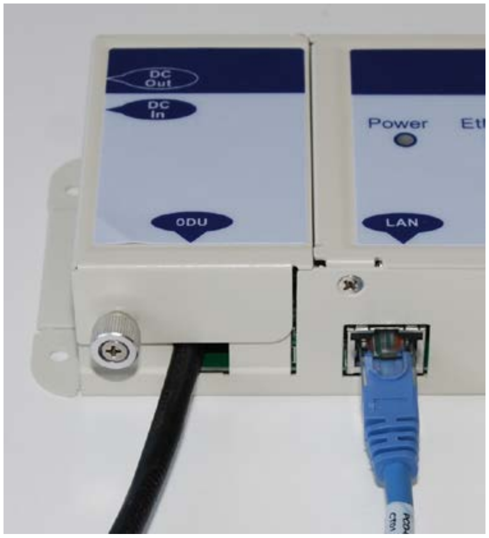
2 Form a drip loop on the PSU end of the LPU to PSU drop cable. The drip loop ensures that any moisture that runs down the cable into the cabinet or enclosure cannot enter the PSU.

3 (a) Undo the retaining screw, hinge back the cover and plug the drop cable into the port. (b) Close the cover and secure with the screw. (c) When the system is ready for network connection, connect the network Cat5e cable to the LAN port of the PSU:

(a)



(b) and (c)



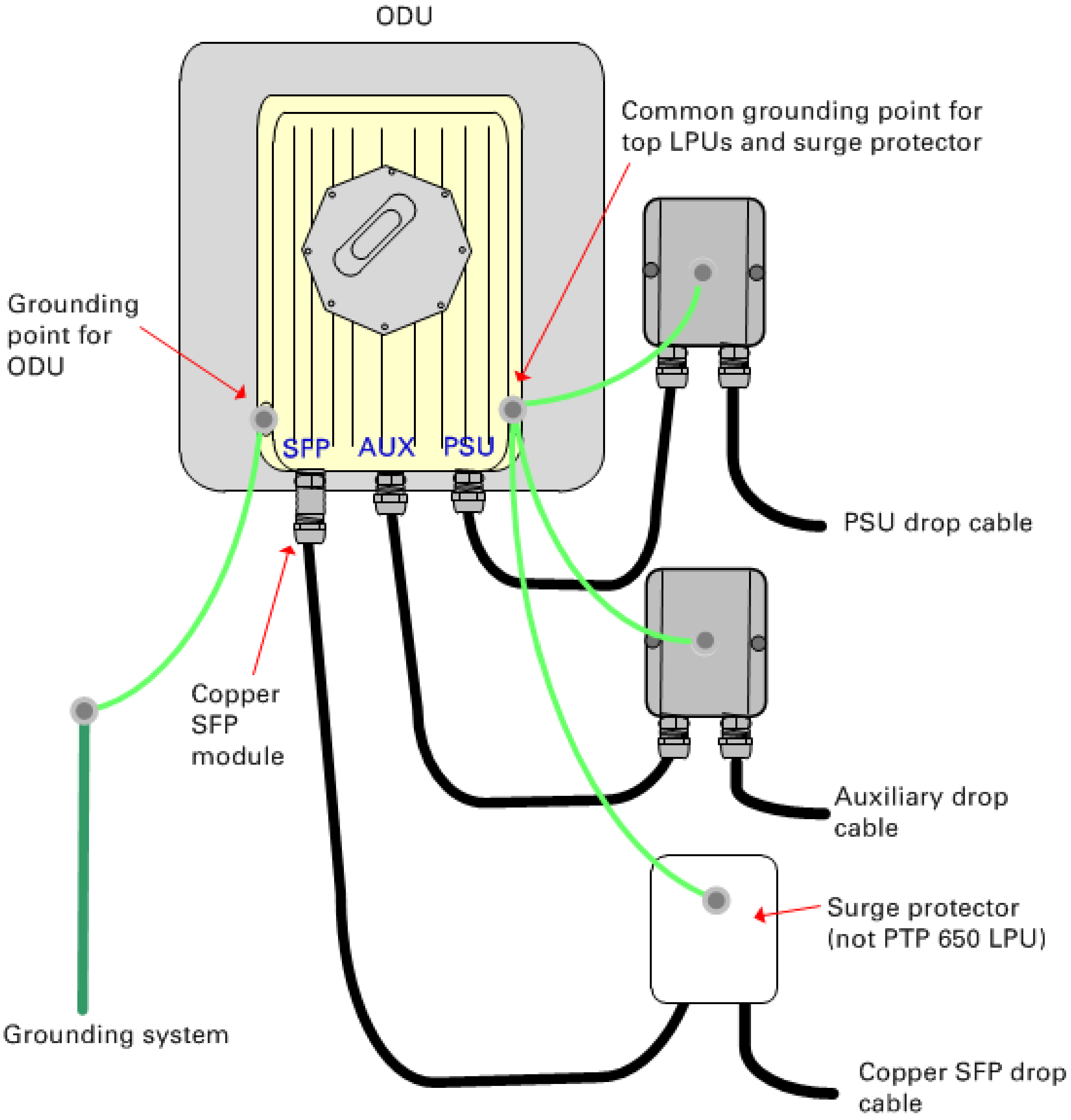
Installing an SFP Ethernet interface

In more advanced configurations, there may be an optical or copper Cat5e Ethernet interface connected to the SFP port of the ODU. Refer to Typical deployment on page 3-2 for diagrams of these configurations.

Adapt the installation procedures in this chapter as appropriate for SFP interfaces, noting the following differences from a PSU interface:

- Install an optical or copper SFP module in the ODU (SFP port) and connect the SFP optical or copper cable into this module using the long cable gland from the SFP module kit. This is described in the following procedures:
  - Fitting the long cable gland on page 5-25
  - Inserting the SFP module on page 5-26
  - Connecting the cable on page 5-29
  - Fitting the gland on page 5-30
  - Removing the cable and SFP module on page 5-31
- Optical cables do not require LPUs or ground cables.
- At the remote end of an SFP drop cable, use an appropriate termination for the connected device.
- If the connected device is outdoors, not in the equipment building or cabinet, adapt the grounding instructions as appropriate.
- PTP 650 LPUs are not suitable for installation on SFP copper Cat5e interfaces. For SFP drop cables, obtain suitable surge protectors from a specialist supplier.
- Ground the top LPUs and surge protector to the same point on the ODU (Figure 57).

Figure 57 ODU with copper Cat5e connections to all three Ethernet ports

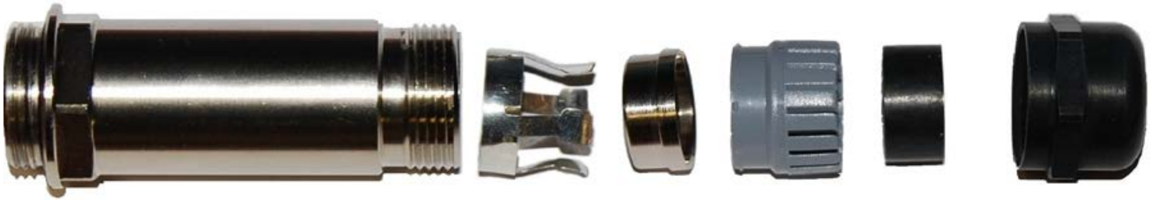


Fitting the long cable gland

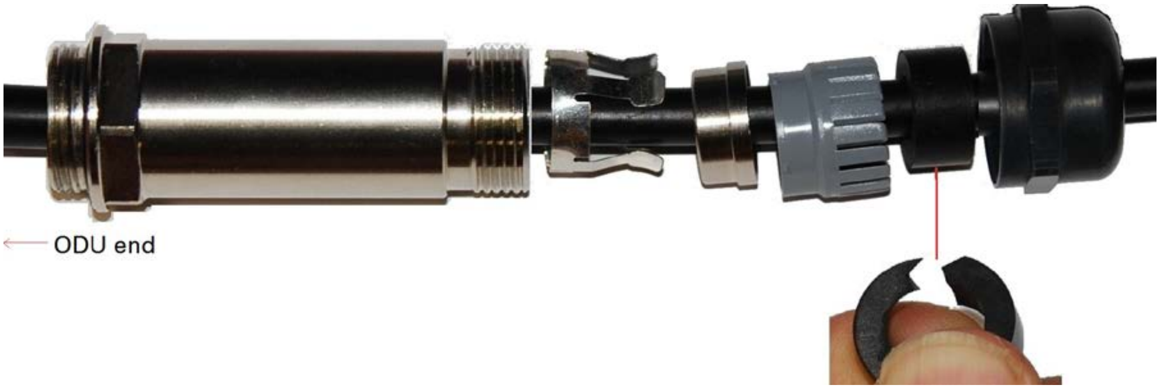
Optical SFP interface: Disassemble the long cable gland and thread its components over the LC connector at the ODU end as shown below.

Copper Cat5e SFP interface: Disassemble the long cable gland and thread its components over the RJ45 connector at the ODU end as shown below.

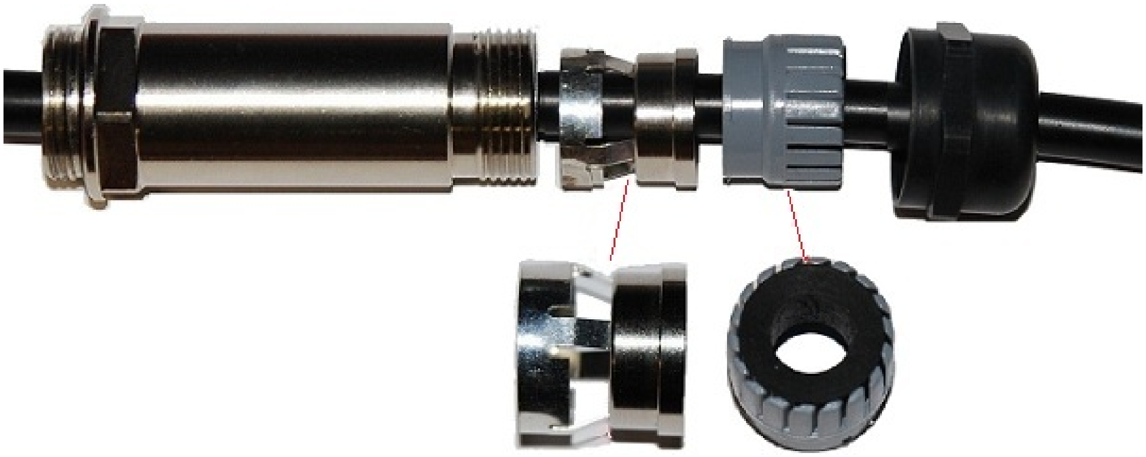
1 Disassemble the gland:



2 Thread each part onto the cable (the rubber bung is split):

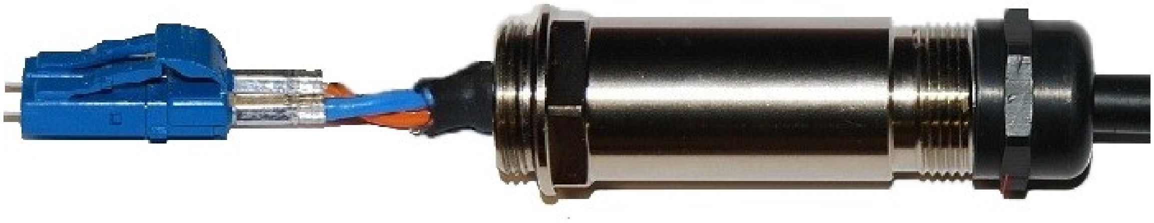


3 Assemble the spring clip and the rubber bung (the clips go inside the ring):

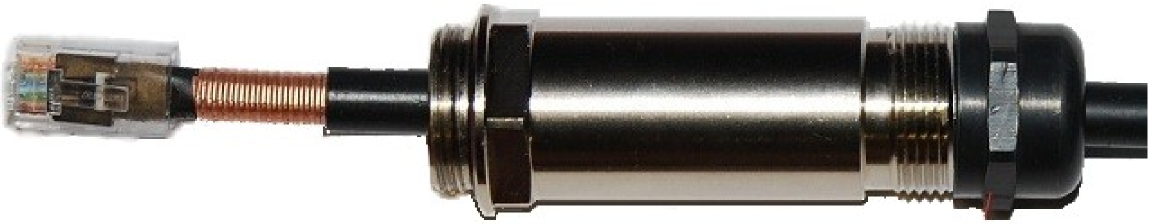


4 Fit the parts into the body and lightly screw on the gland nut (do not tighten it):

Optical



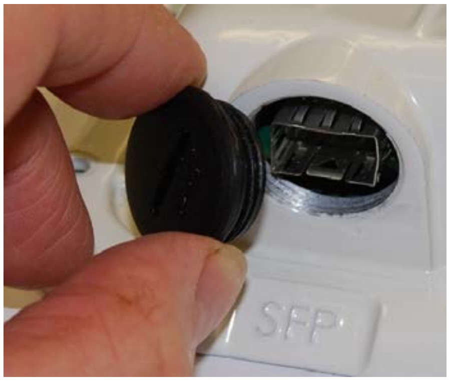
Copper



Inserting the SFP module

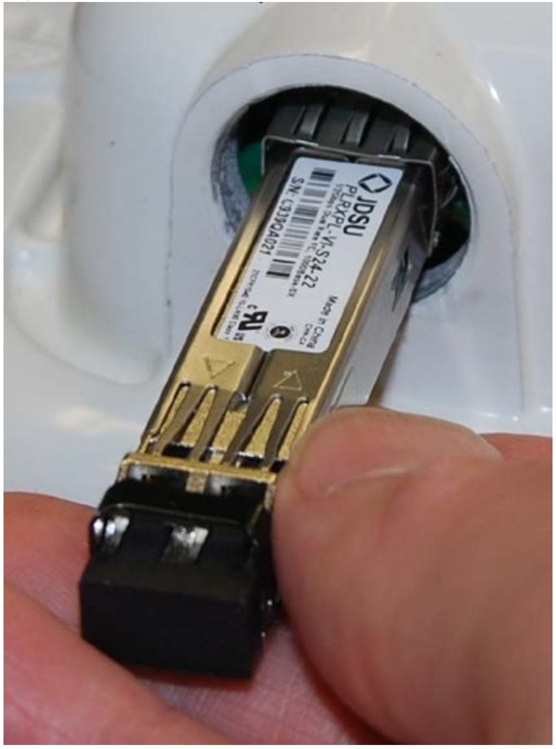
To insert the SFP module into the ODU, proceed as follows:

1 Remove the blanking plug from the SFP port of the ODU:

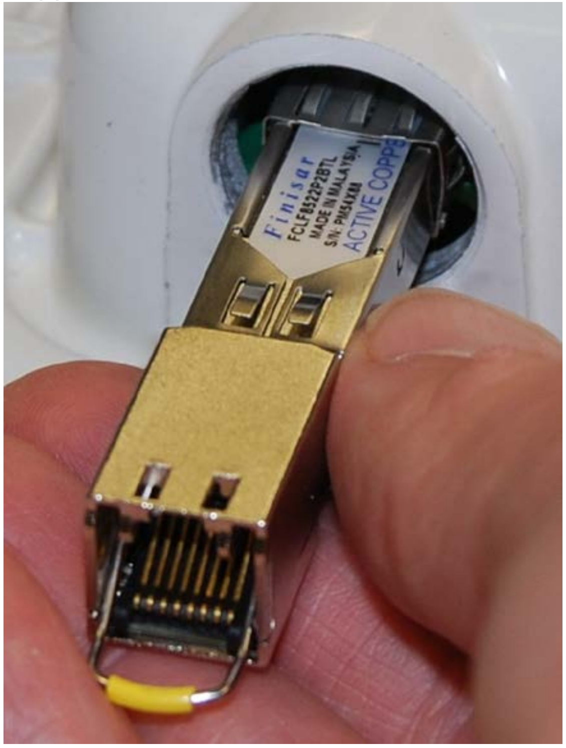


2 Insert the SFP module into the SFP receptacle with the label up:

Optical

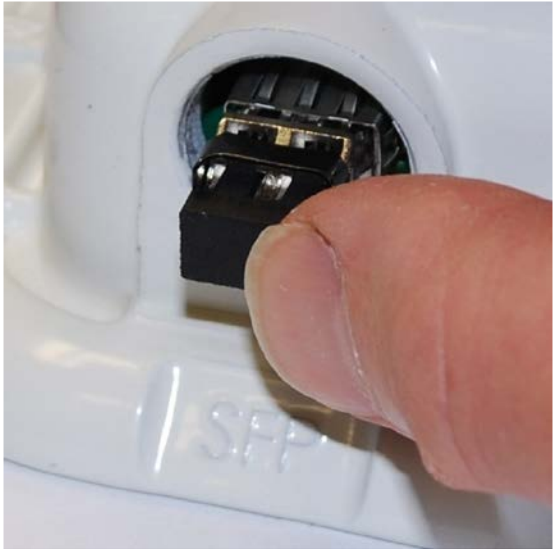


Copper

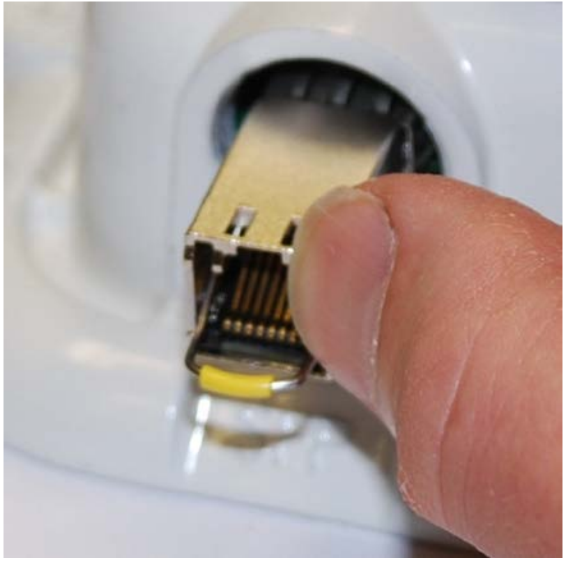


3 Push the module home until it clicks into place:

Optical

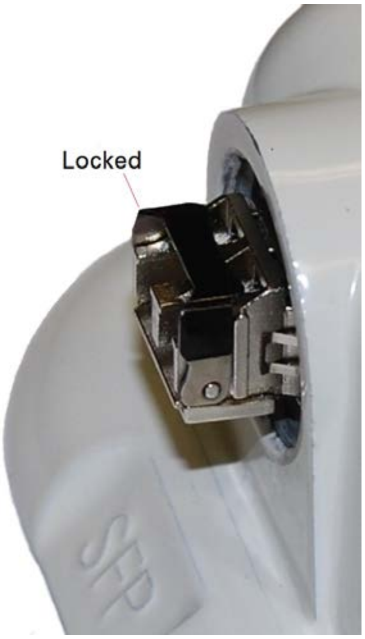


Copper

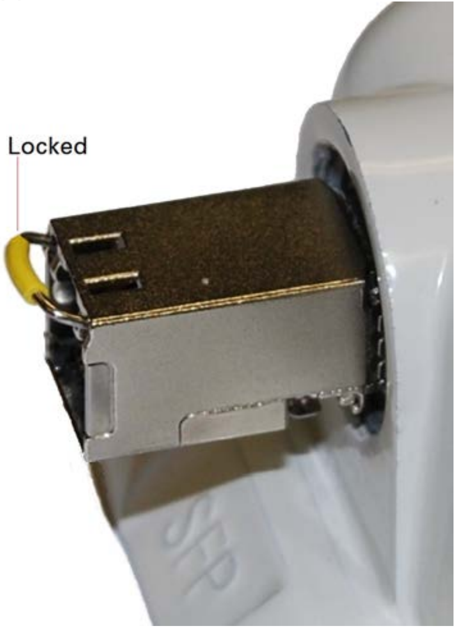


4 Rotate the latch to the locked position:

Optical



Copper



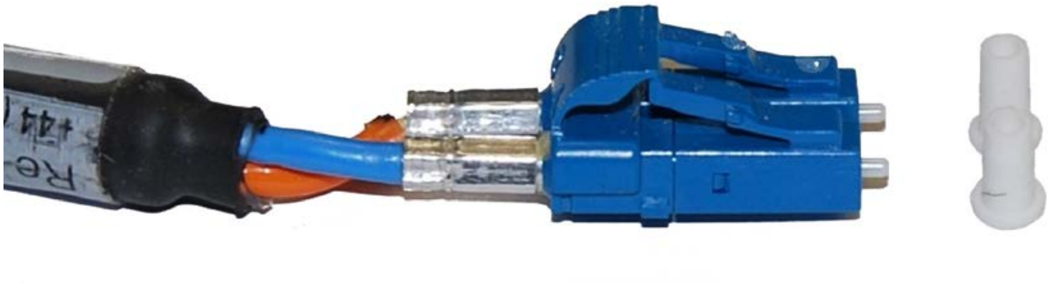
Connecting the cable

Caution

The fiber optic cable assembly is very delicate. To avoid damage, handle it with extreme care. Ensure that the fiber optic cable does not twist during assembly, especially when fitting and tightening the weatherproofing gland.

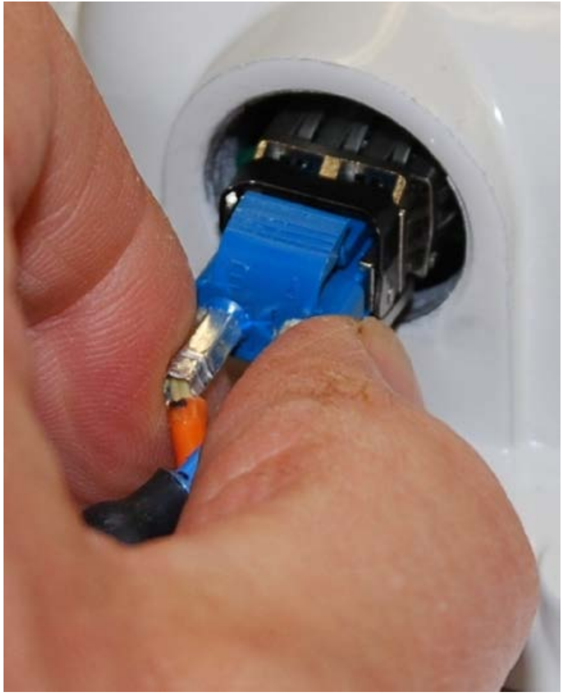
Do not insert the power over Ethernet drop cable from the PSU into the SFP module, as this will damage the module.

1 Remove the LC connector dust caps from the ODU end (optical cable only):

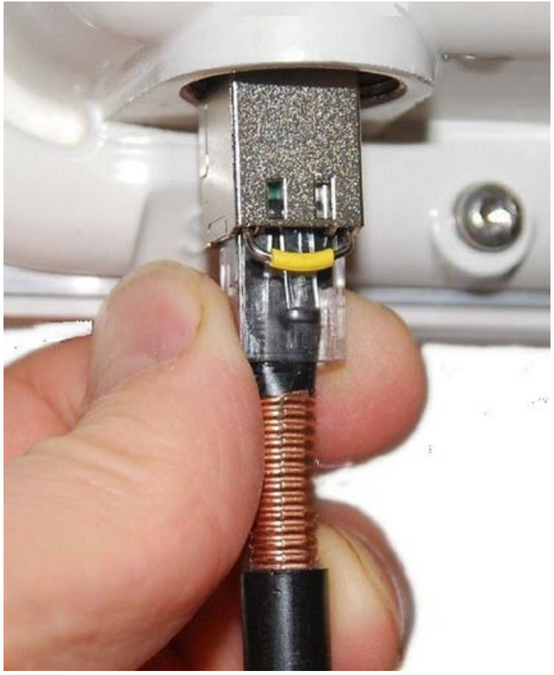


2 Plug the connector into the SFP module, ensuring that it snaps home:

Optical

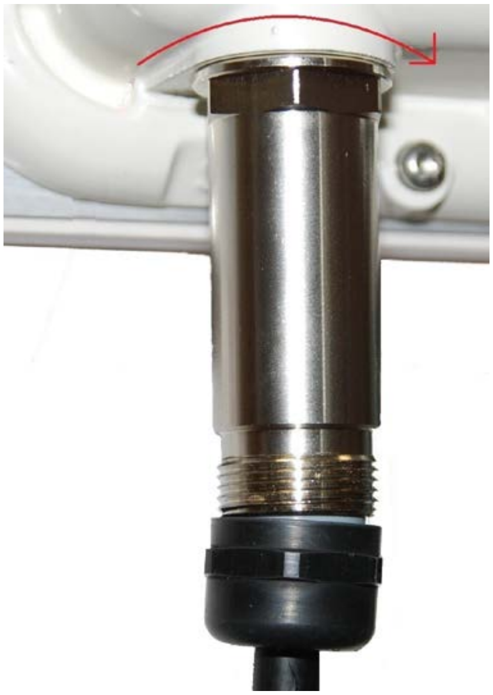


Copper

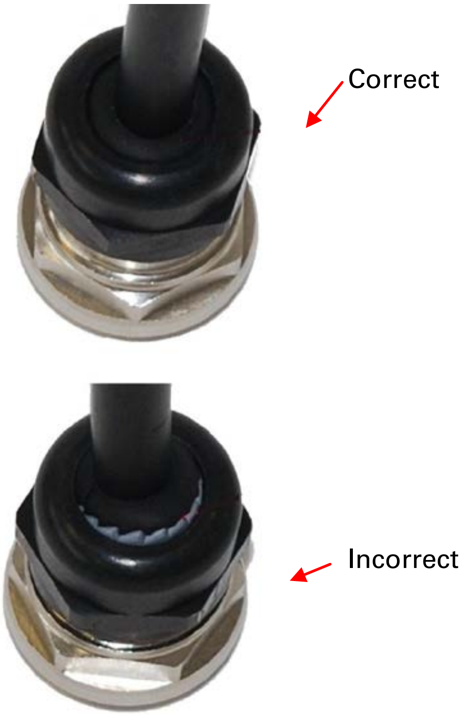


Fitting the gland

1 Fit the gland body to the SFP port and tighten it to a torque of 5.5 Nm (4.3 lb ft)



2 Fit the gland nut and tighten until the rubber seal closes on the cable. Do not over-tighten the gland nut, as there is a risk of damage to its internal components:

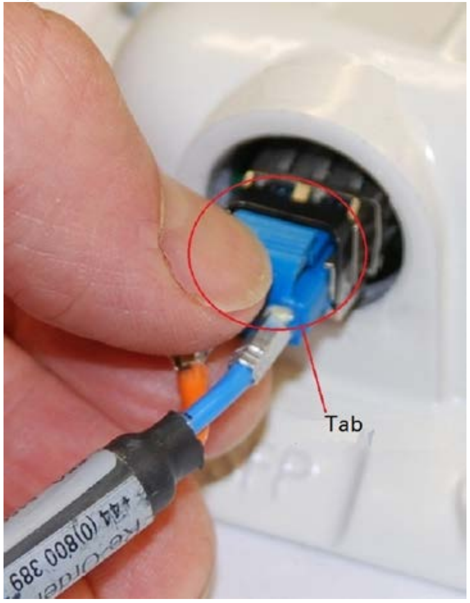


Removing the cable and SFP module

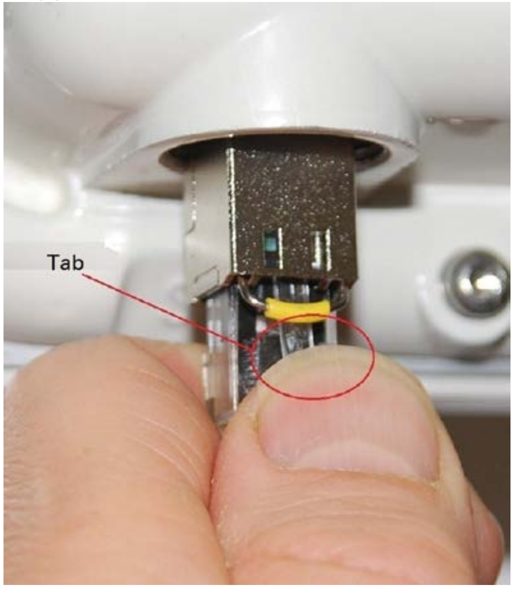
Do not attempt to remove the module without disconnecting the cable, otherwise the locking mechanism in the ODU will be damaged.

1 Remove the cable connector by pressing its release tab before pulling it out:

Optical

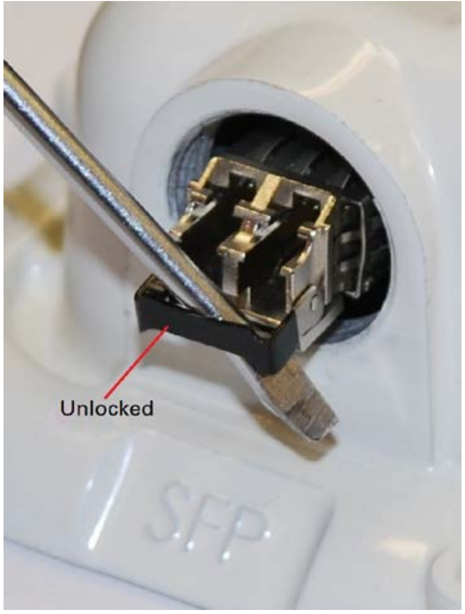


Copper

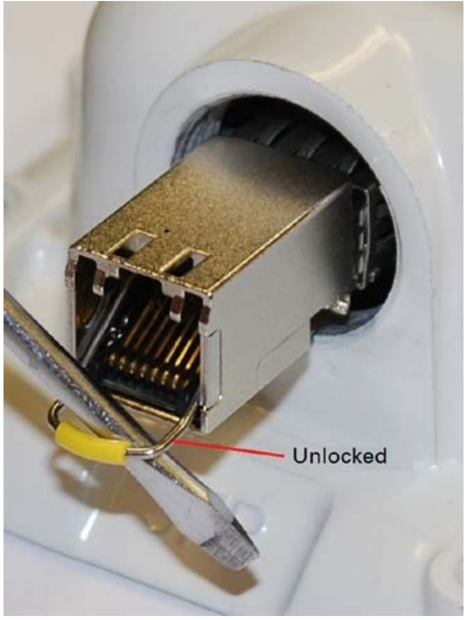


2 Rotate the latch to the unlocked position. Extract the module by using a screwdriver:

Optical



Copper



Installing an Aux Ethernet interface

In more advanced configurations, there may be a copper Cat5e Ethernet interface connected to the Aux port of the ODU. Refer to Typical deployment on page 3-2 for a diagram of this configuration.

Adapt the installation procedures in this chapter as appropriate for the Aux interface, noting the following differences:

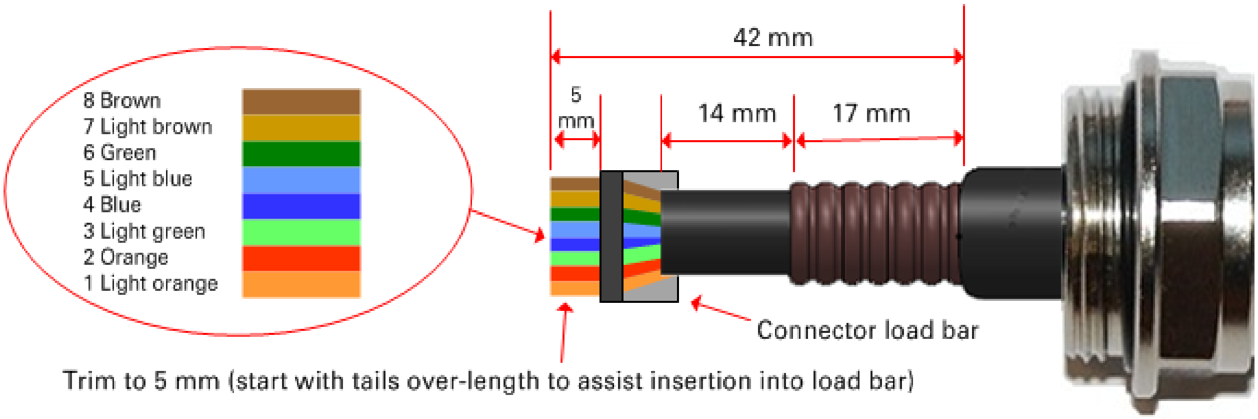
- At the remote end of the Aux drop cable, use an appropriate termination for the connected device (for example, a video camera or wireless access point).
- If the connected device is outdoors, not in the equipment building or cabinet, adapt the grounding instructions as appropriate.
- Ground the top LPUs and surge protector to the same point on the ODU (Figure 57).

Supplemental installation information

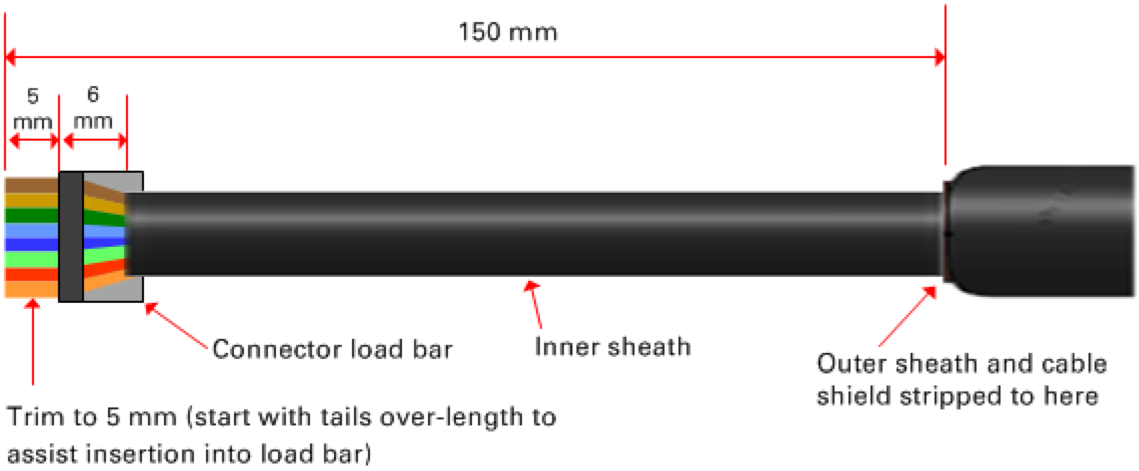
This section contains detailed installation procedures that are not included in the above topics, such as how to strip cables, create grounding points and weatherproof connectors.

Stripping drop cable

When preparing drop cable for connection to the PTP 650 ODU or LPU, use the following measurements:



When preparing drop cable for connection to the PTP 650 PSU (without a cable gland), use the following measurements:

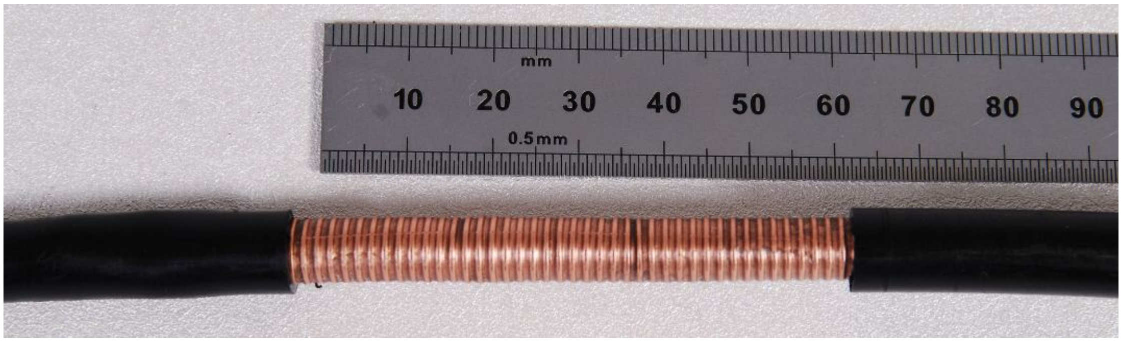

150 mm
5 mm
6 mm
Connector load bar
Inner sheath
Outer sheath and cable shield stripped to here
Trim to 5 mm (start with tails over-length to assist insertion into load bar)

Creating a drop cable grounding point

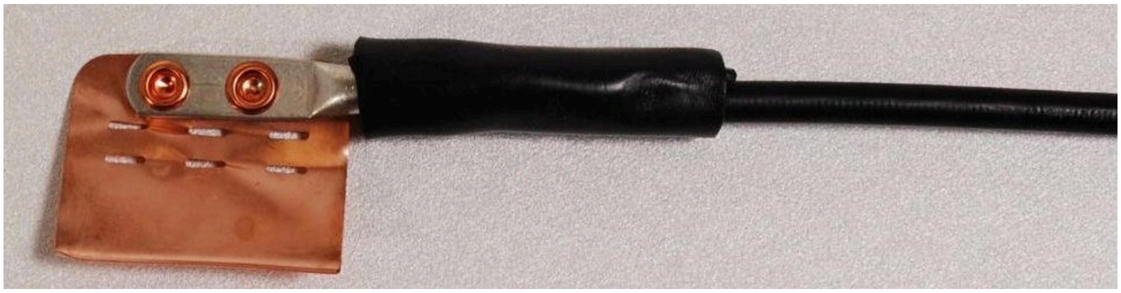
Use this procedure to connect the screen of the main drop cable to the metal of the supporting structure using the cable grounding kit (Cambium part number 01010419001).

To identify suitable grounding points, refer to Drop cable grounding points on page 3-13.

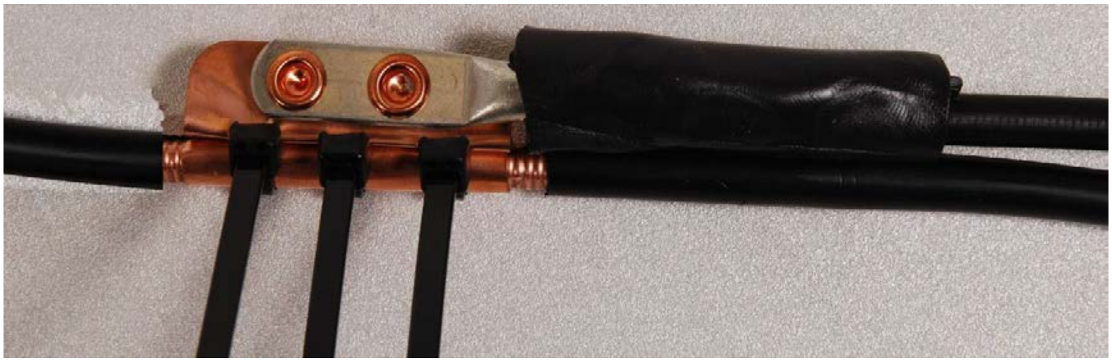
1. Remove 60 mm (2.5 inches) of the drop cable outer sheath.



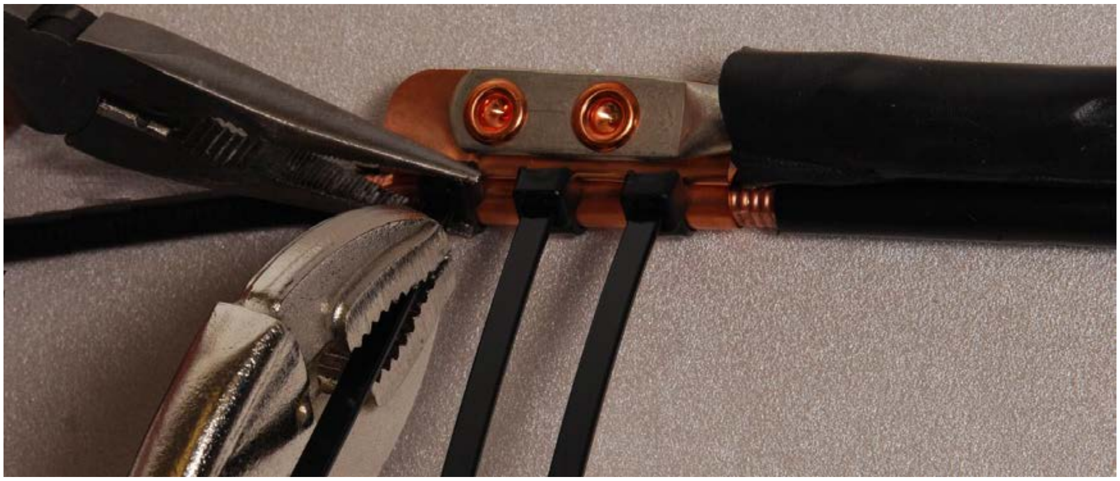
2. Cut 38mm (1.5 inches) of rubber tape (self-amalgamating) and fit to the ground cable lug. Wrap the tape completely around the lug and cable.



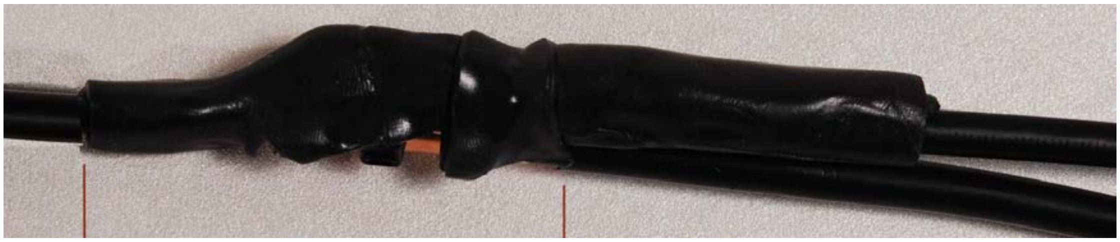
3. Fold the ground wire strap around the drop cable screen and fit cable ties.



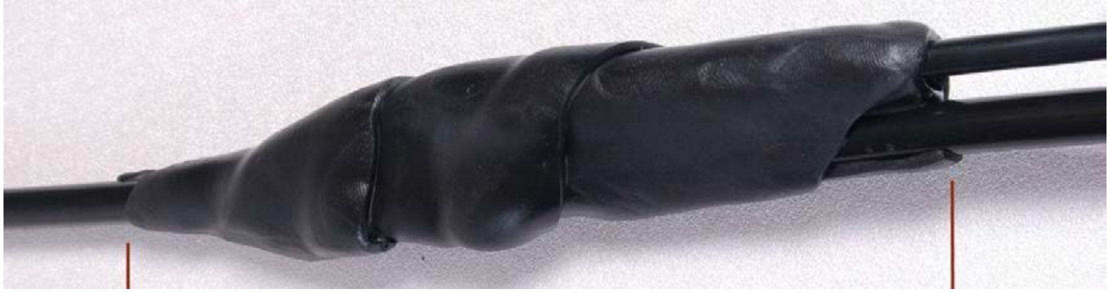
4 Tighten the cable ties with pliers. Cut the surplus from the cable ties.



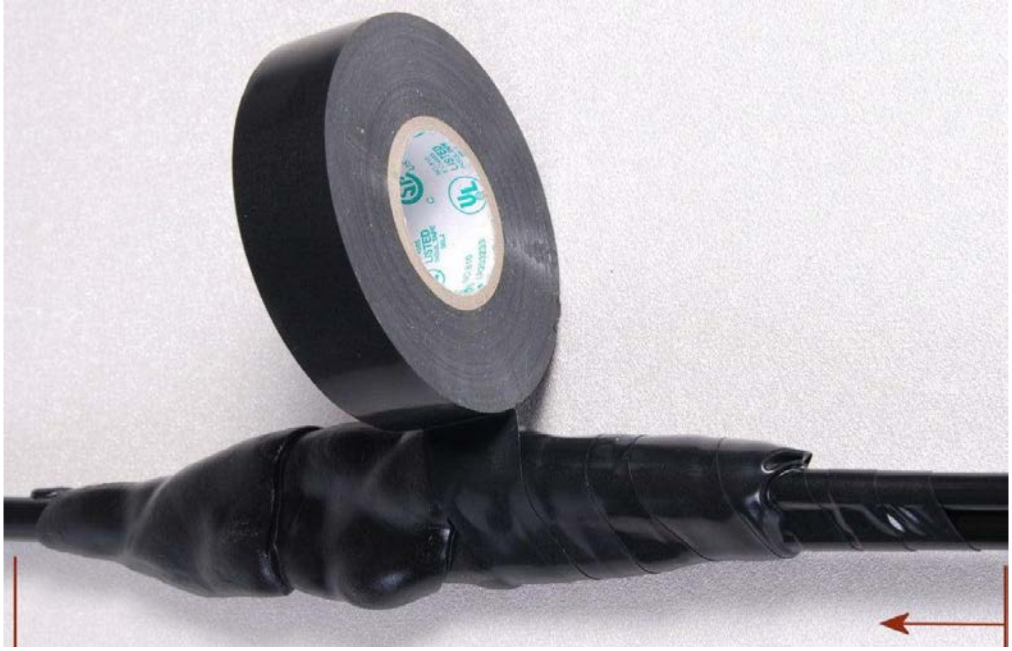
5 Cut a 38mm (1.5 inches) section of self-amalgamating tape and wrap it completely around the joint between the drop and ground cables.



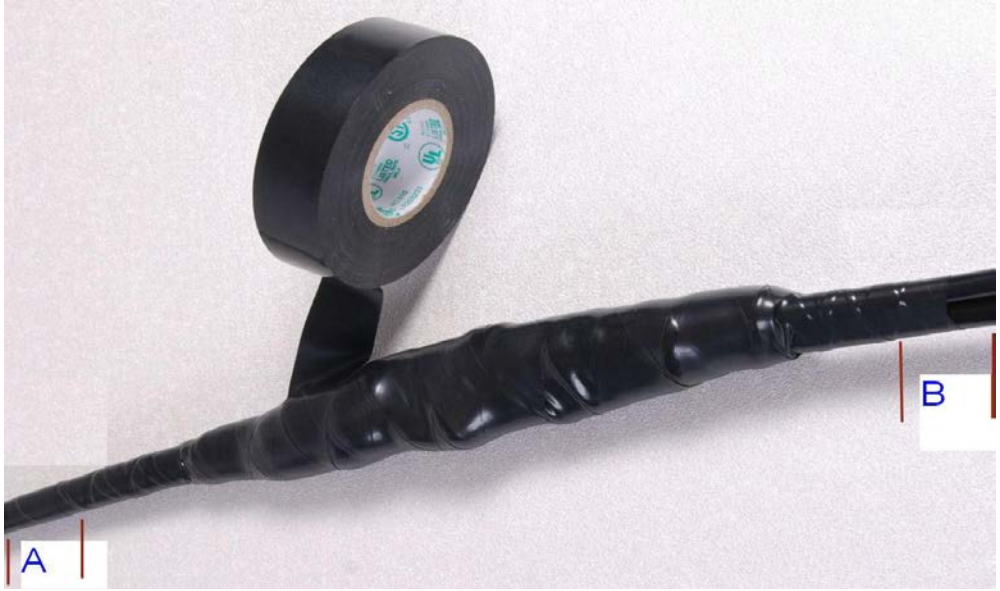
6 Use the remainder of the self-amalgamating tape to wrap the complete assembly. Press the tape edges together so that there are no gaps.



7 Wrap a layer of PVC tape from bottom to top, starting from 25 mm (1 inch) below and finishing 25 mm (1 inch) above the edge of the self-amalgamating tape, over lapping at half width.



8 Repeat with a further four layers of PVC tape, always overlapping at half width. Wrap the layers in alternate directions (top to bottom, then bottom to top). The edges of each layer should be 25mm (1 inch) above (A) and 25 mm (1 inch) below (B) the previous layer.



9 Prepare the metal grounding point of the supporting structure to provide a good electrical contact with the grounding cable clamp. Remove paint, grease or dirt, if present. Apply anti-oxidant compound liberally between the two metals.

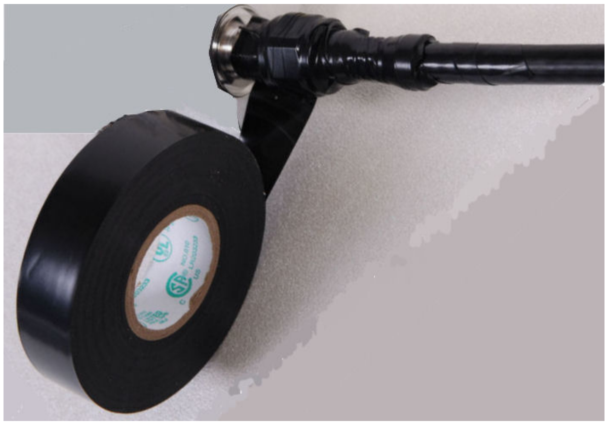
10 Clamp the bottom lug of the grounding cable to the supporting structure using site approved methods. Use a two-hole lug secured with fasteners in both holes. This provides better protection than a single-hole lug.

Weatherproofing an N type connector

Use this procedure to weatherproof the N type connectors fitted to the connectorized ODU and external antenna (if recommended by the antenna manufacturer).

1 Ensure the connection is tight. A torque wrench should be used if available:

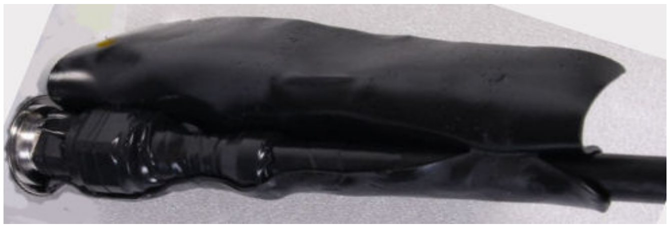
2 Wrap the connection with a layer of 19 mm (0.75 inch) PVC tape, starting 25 mm (1 inch) below the connector body. Overlap the tape to half-width and extend the wrapping to the body of the LPU. Avoid making creases or wrinkles:



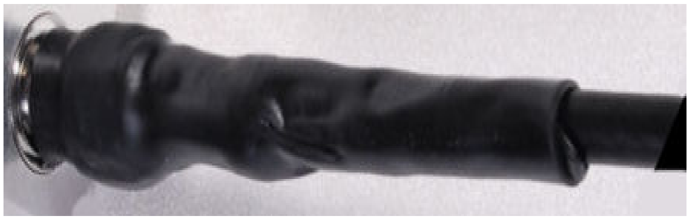
3 Smooth the tape edges:

4 Cut a 125mm (5 inches) length of rubber tape (self-amalgamating):

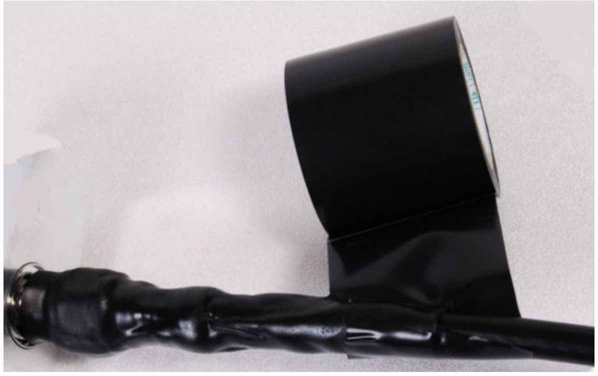
5 Expand the width of the tape by stretching it so that it will wrap completely around the connector and cable:



6 Press the tape edges together so that there are no gaps. The tape should extend 25 mm (1 inch) beyond the PVC tape:



7 Wrap a layer of 50 mm (2 inch) PVC tape from bottom to top, starting from 25 mm (1 inch) below the edge of the self-amalgamating tape, overlapping at half width.

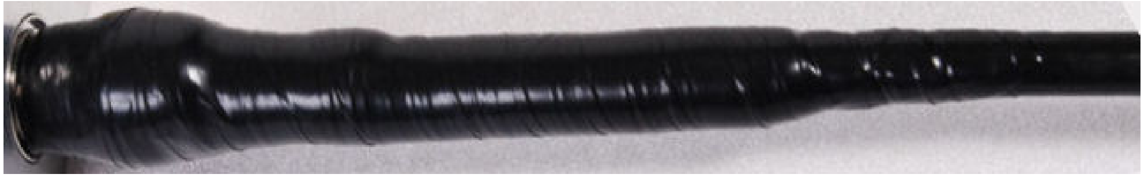


8 Repeat with a further four layers of 19 mm (0.75 inch) PVC tape, always overlapping at half width. Wrap the layers in alternate directions:

- Second layer: top to bottom.
- Third layer: bottom to top.
- Fourth layer: top to bottom.
- Fifth layer: bottom to top.

The bottom edge of each layer should be 25 mm (1 inch) below the previous layer.

9 Check the completed weatherproof connection:

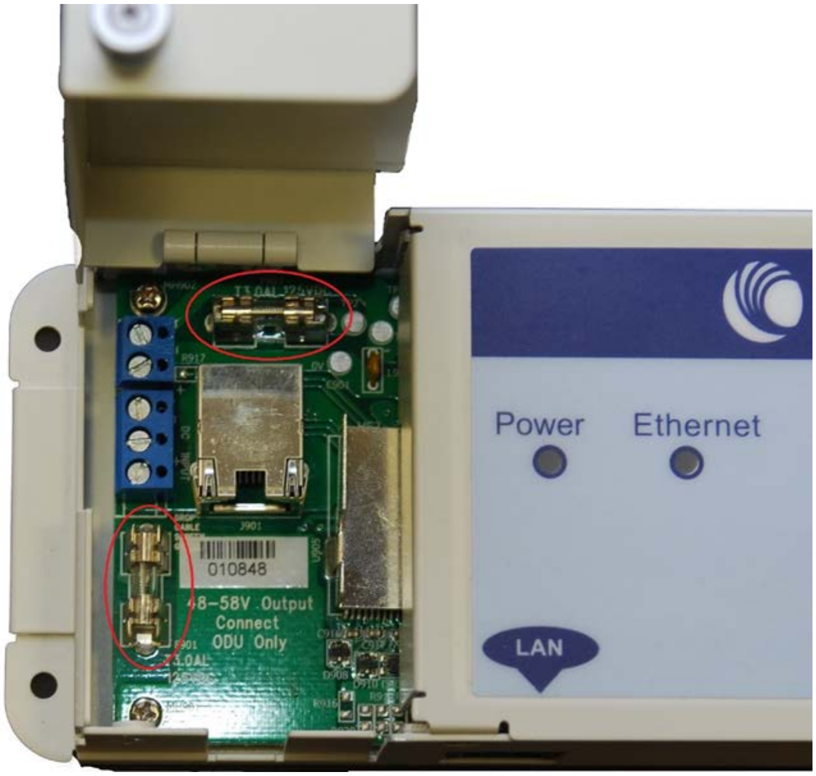


Replacing PSU fuses

The AC+ DC Enhanced Power Injector contains two replaceable fuses. These fuses protect the positive and negative grounded DC input voltages. If an incorrect power supply (that is, not in the range 37V to 60V DC) is connected to the DC input terminals, one or both fuses may blow.

Both fuses are 3 Amp slow-blow, for example Littlefuse part number 0229003.

To replace these fuses, undo the retaining screw and hinge back the cover as indicated:



Note

No other fuses are replaceable in the AC+DC Enhanced Power Injector.

Note

The AC Power Injector does not contain replaceable fuses.

Chapter 6: Configuration and alignment

This chapter describes how to use the web interface to configure the PTP 650 link. It also describes how to align antennas. This chapter contains the following topics:

Preparing for configuration and alignment

This section describes the checks to be performed before proceeding with unit configuration and antenna alignment.

Safety precautions

All national and local safety standards must be followed while configuring the units and aligning the antennas.

Warning

Ensure that personnel are not exposed to unsafe levels of RF energy. The units start to radiate RF energy as soon as they are powered up. Respect the safety standards defined in Compliance with safety standards on page 4-23, in particular the minimum separation distances.

Observe the following guidelines:

- Never work in front of the antenna when the ODU is powered.
- Always power down the PSU before connecting or disconnecting the drop cable from the PSU, ODU or LPU.

Regulatory compliance

All applicable radio regulations must be followed while configuring the units and aligning the antennas. For more information, refer to Compliance with radio regulations on page 4-27.

Caution

If the system designer has provided a list of channels to be barred for TDWR radar avoidance, the affected channels must be barred before the units are allowed to radiate on site, otherwise the regulations will be infringed. To bar these channels, follow the procedure Barring channels on page 7-31.

Selecting configuration options

Use the installation report to determine which configuration options are required. Refer to PTP LINKPlanner on page 3-21.

Generating a License Key

ODUs are shipped with a default License Key factory installed. The default license key enables a limited set of capabilities as follows:

- Operation in selected regulatory bands (these are restricted by the ODU regional variant):
  - FCC/IC variants: 5.8 GHz USA (regulatory band 1).
  - RoW variants: 5.4 GHz unrestricted (regulatory band 8) and 5.8 GHz unrestricted (regulatory band 35).
  - EU variants: 5.4 GHz ETSI (regulatory band 26)
- “Lite” throughput capability (up to 125 Mbps).

A license key is required to upgrade the ODU to the following capabilities:

- To allow the ODU to operate in other regulatory bands (these are restricted by the ODU regional variant). This capability is free of charge.
- To enable the SFP port. An Access Key for this capability is provided in the SFP module kits (SFP module kits on page 2-27).
- To allow “Med” (up to 250 Mbps) or “Full” (up to 450 Mbps) throughput capability. Purchase an access key from Cambium Networks (Table 68). Cambium will email one Access Key for each upgrade purchased.
- To allow 128-bit or 256-bit AES encryption. Purchase an access key from Cambium Networks (Table 68). Cambium will email one Access Key for each upgrade purchased.

Table 68 Capability upgrades

Cambium description (*1)	Cambium part number
PTP 650 128-bit AES Encryption – per ODU (*2)	C000065K018
PTP 650 256-bit AES Encryption – per ODU (*2)	C000065K019
PTP 650 Lite (Up to 125Mbps) to Mid (Up to 250Mbps) Link Capacity upgrade license per ODU	C000065K021
PTP 650 Lite (Up to 125Mbps) to Full (Up to 450Mbps) Link Capacity upgrade license per ODU	C000065K022
PTP 650 Mid (Up to 250Mbps) to Full (Up to 450Mbps) Link Capacity upgrade license per ODU	C000065K023

(*1) If the Cambium description contains the words “per ODU”, then order two upgrades per link.

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

To obtain the License Key, proceed as follows:

- Obtain the MAC Address of the unit (it is on the System Status page).
- Go to the Cambium Support web page (see Contacting Cambium Networks on page 1) and navigate to the **Cambium Networks License Key Generator**.
- Complete the required fields, including MAC Address and Country. For SFP capability, AES encryption and data throughput upgrades only, enter the Access Key.
- Submit the web form. Cambium will send the License Key by email.

Connecting to the unit

This section describes how to connect the unit to a management PC and power it up.

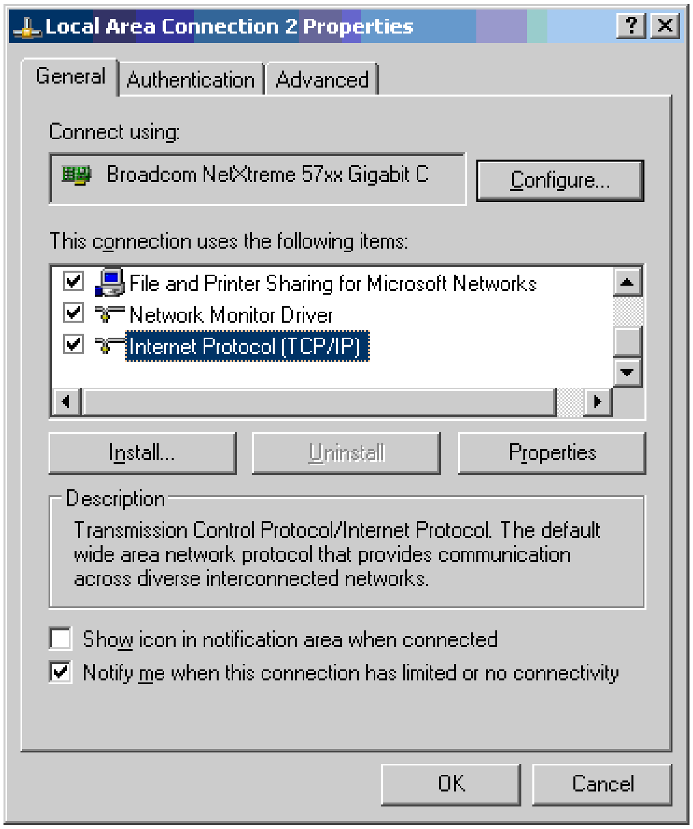
Configuring the management PC

Use this procedure to configure the local management PC to communicate with the PTP 650.

Procedure:

1 Select **Properties** for the Ethernet port. In Windows 7 this is found in **Control Panel > Network and Internet > Network Connections > Local Area Connection**.

2 Select **Internet Protocol (TCP/IP)**:



Connect using:

Broadcom NetXtreme 57xx Gigabit C

This connection uses the following items:

☑ File and Printer Sharing for Microsoft Networks
☑ Network Monitor Driver
☑ Internet Protocol (TCP/IP)

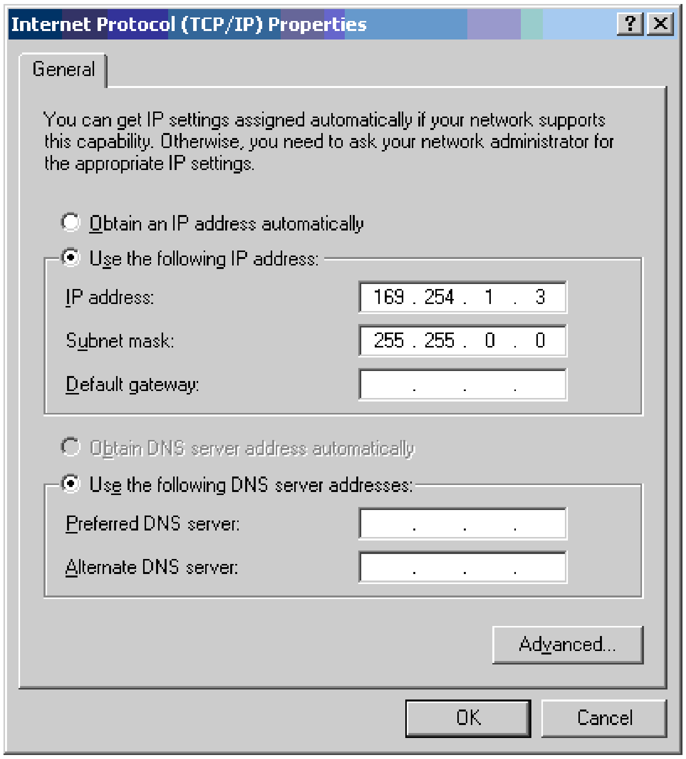
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected
☑ Notify me when this connection has limited or no connectivity

3 Click **Properties**.

4 Enter an IP address that is valid for the 169.254.X.X network, avoiding 169.254.0.0 and 169.254.1.1. A good example is 169.254.1.3:



Internet Protocol (TCP/IP) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 169 . 254 . 1 . 3

Subnet mask: 255 . 255 . 0 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

5 Enter a subnet mask of 255.255.0.0. Leave the default gateway blank.

Connecting to the PC and powering up

Use this procedure to connect a management PC and power up the PTP 650.

Procedure:

1 Check that the ODU and PSU are correctly connected.

2 Connect the PC Ethernet port to the LAN port of the PSU using a standard (not crossed) Ethernet cable.

3 Apply mains or battery power to the PSU. The green Power LED should illuminate continuously.

4 After about 45 seconds, check that the orange Ethernet LED starts with 10 slow flashes.

5 Check that the Ethernet LED then illuminates continuously. If the Power and Ethernet LEDs do not illuminate correctly, refer to Testing link end hardware on page 8-2.

Using the web interface

This section describes how to log into the PTP 650 web interface and use its menus.

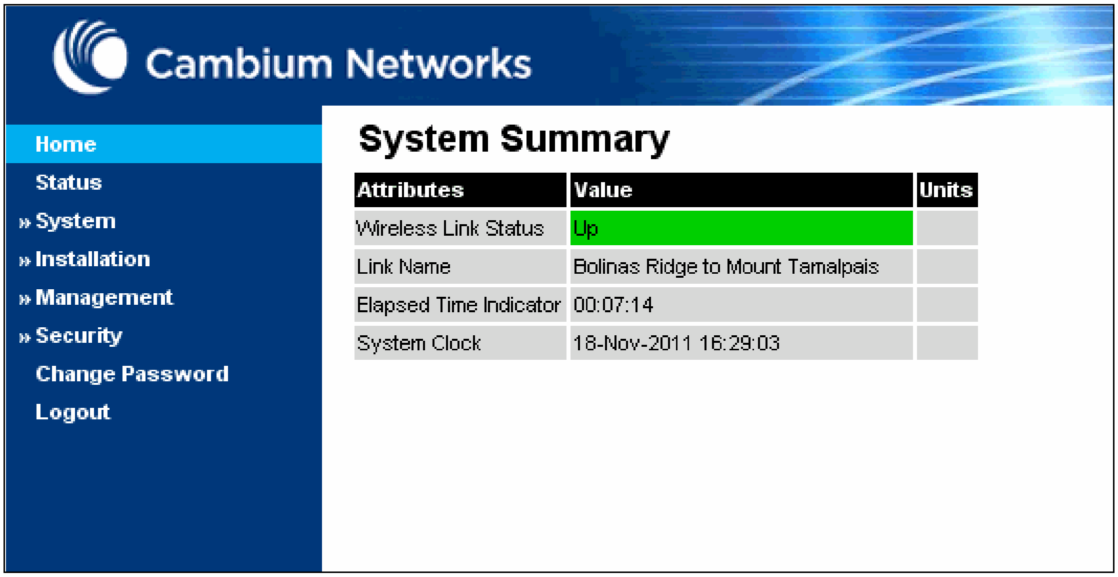
Logging into the web interface

Use this procedure to log into the web interface as a system administrator.

Procedure:

1 Start the web browser from the management PC.

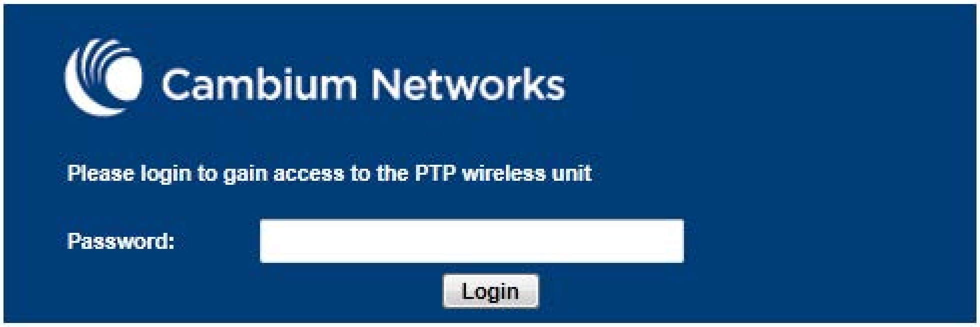
2 Type the IP address of the unit into the address bar. The factory default IP address is **169.254.1.1**. Press ENTER. The web interface menu and System Summary page are displayed:



System Summary

Attributes	Value	Units
Wireless Link Status	Up	
Link Name	Bolinas Ridge to Mount Tamalpais	
Elapsed Time Indicator	00:07:14	
System Clock	18-Nov-2011 16:29:03	

3 On the menu, click **System**. The login page is displayed with Password only (the default) or with Username and Password (if identity-based user accounts have been enabled):



Please login to gain access to the PTP wireless unit

Password:

4 Enter Username (if requested) and Password (the default is blank) and click **Login**.

Using the menu options

Use the menu navigation bar in the left panel to navigate to each web page. Some of the menu options are only displayed for specific system configurations. Use Table 69 to locate information about using each web page.

Table 69 Menu options and web pages

Main menu	Menu option	Web page information
Home		System Summary page on page 7-2
Status		System Status page on page 7-3
System		
	Configuration	System Configuration page on page 6-21
	LAN Configuration	LAN Configuration page on page 6-24
	QoS Configuration	QoS Configuration page on page 6-30
	SFP Configuration	SFP Configuration page on page 6-33
	Save and Restore	Save & Restore Configuration page on page 6-34
	Spectrum Management	Spectrum Management page on page 7-20 Barring channels on page 7-31
	Statistics	System Statistics page on page 7-32 Comparing actual to predicted performance on page 6-94
	Wireless Port Counters	Wireless Port Counters page on page 7-37 Test Ethernet packet errors reported by ODU on page 8-7
	Main Port Counters	Main Port Counters page on page 7-38
	Aux Port Counters	Aux Port Counters page on page 7-40
	SFP Port Counters	SFP Port Counters page on page 7-41
	Diagnostics Plotter	Diagnostics Plotter page on page 7-42
	CSV Download	Generate Downloadable Diagnostics page on page 7-43
	Software Upgrade	Software Upgrade page on page 6-37
	Reboot	Reboot Wireless Unit page on page 7-9

Main menu	Menu option	Web page information
Installation		Installation menu on page 6-10
	Graphical Install	Graphical Install page on page 6-92
Management		
	Web	Web-Based Management page on page 6-39
	Local User Accounts	Local User Accounts page on page 6-42
	RADIUS Configuration	RADIUS Configuration page on page 6-47
	Login Information	Login Information page on page 7-9
	Web Properties	Webpage Properties page on page 6-49
	SNMP	SNMP pages (for SNMPv3) on page 6-61 SNMP pages (for SNMPv1/2c) on page 6-71
	Email	Email Configuration page on page 6-52
	Diagnostic Alarms	Diagnostic Alarms page on page 6-54
	Time	Time Configuration page on page 6-55
	Syslog	Syslog page on page 7-16
	Syslog Configuration	Syslog Configuration page on page 6-59
Security		Security menu on page 6-75
	Zeroize CSPs	Zeroize CSPs page on page 6-86
Change Password		Change Password page on page 7-10
Logout		Logging out on page 7-11

Installation menu

This section describes how to use the Installation Wizard to complete the essential system configuration tasks that must be performed on a new link.

Caution

If the system designer has provided a list of channels to be barred for TDWR radar avoidance, the affected channels must be barred before the units are allowed to radiate on site, otherwise the regulations will be infringed. To bar these channels, follow the procedure Barring channels on page 7-31.

Starting the Installation Wizard

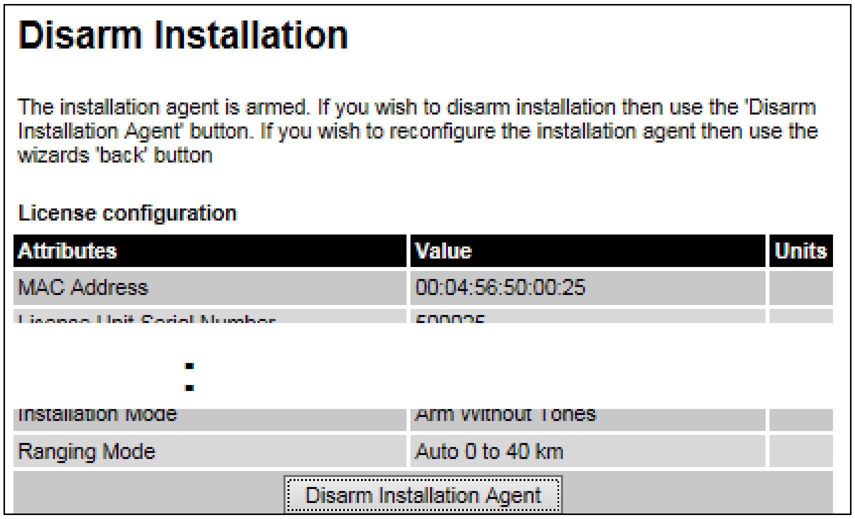
To start the Installation Wizard: on the menu, click **Installation**. The response depends upon the state of the unit:

- If the unit is newly installed, the Software License Key page is displayed. Continue at Software License Key page on page 6-12.
- If the unit is armed for alignment, the Disarm Installation page is displayed. Continue at Disarm Installation page on page 6-11.
- If the unit is not armed, the Current Installation Summary page is displayed. Continue at Current Installation Summary page on page 6-11.

Disarm Installation page

Menu option: **Installation** (Figure 58). This page is displayed only when unit is armed.

Figure 58 Disarm Installation page (top and bottom of page shown)



Disarm Installation

The installation agent is armed. If you wish to disarm installation then use the 'Disarm Installation Agent' button. If you wish to reconfigure the installation agent then use the wizards 'back' button

License configuration

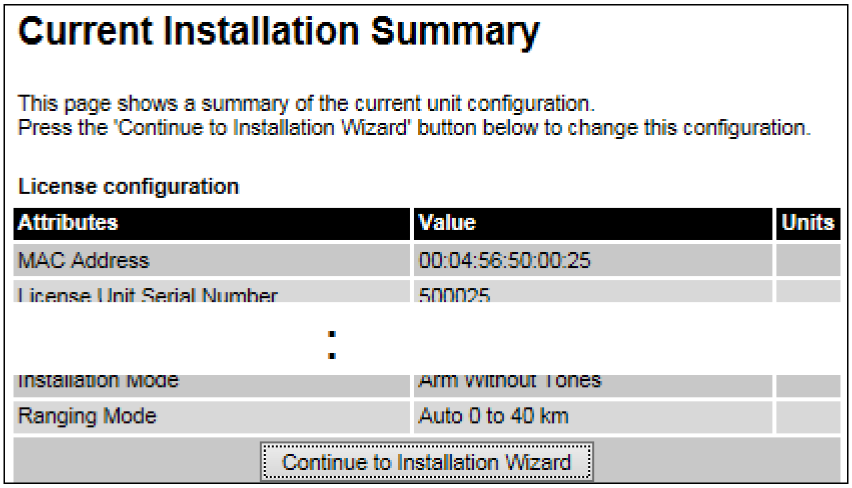
Attributes	Value	Units
MAC Address	00:04:56:50:00:25	
License Unit Serial Number	500025	
:		
Installation Mode	Arm Without Tones	
Ranging Mode	Auto 0 to 40 km	

To disarm the unit, click **Disarm Installation Agent.**

Current Installation Summary page

Menu option: **Installation** (Figure 59). This page is displayed only when unit is not armed.

Figure 59 Current Installation Summary page (top and bottom of page shown)



Current Installation Summary

This page shows a summary of the current unit configuration.
Press the 'Continue to Installation Wizard' button below to change this configuration.

License configuration

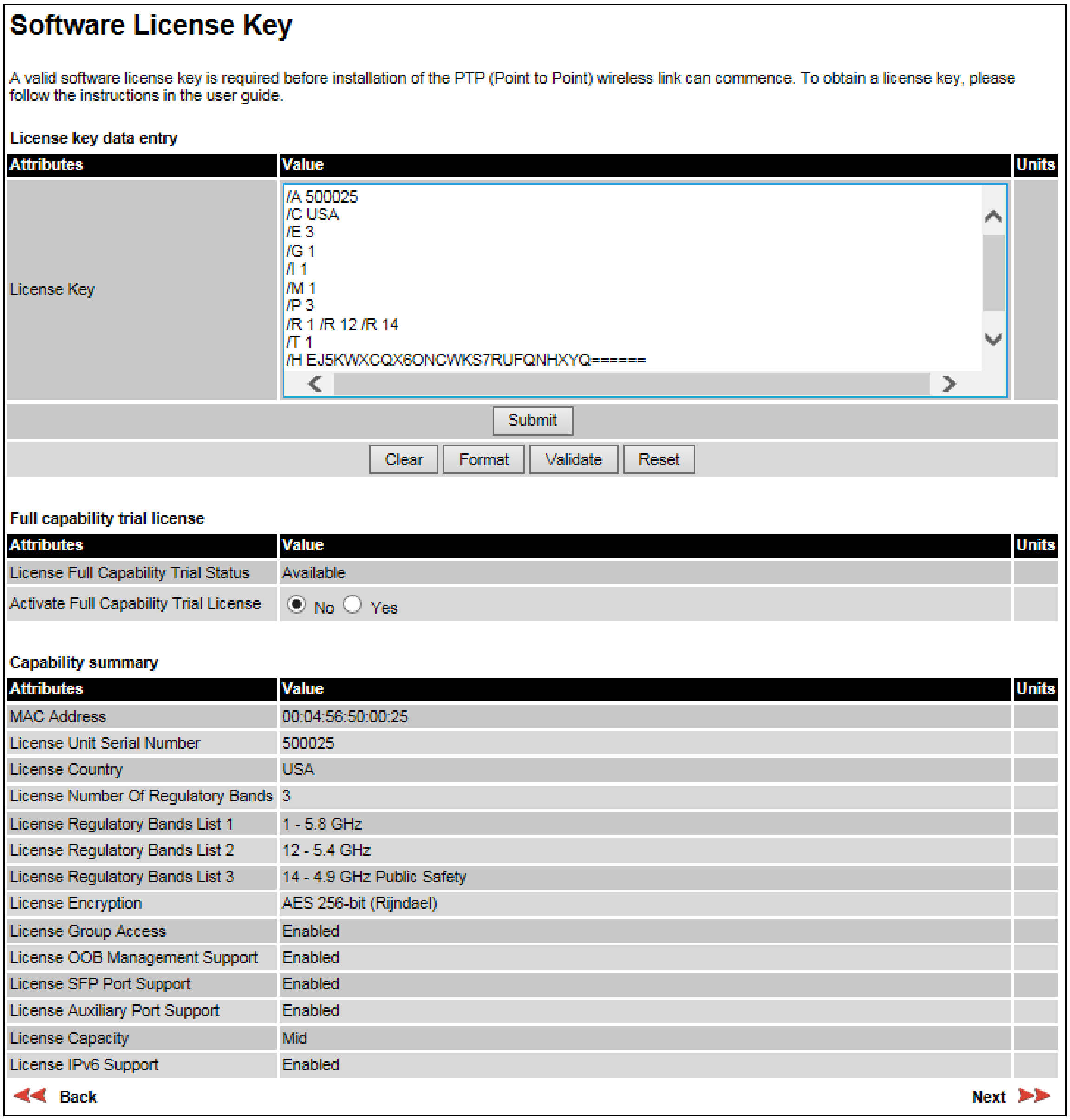
Attributes	Value	Units
MAC Address	00:04:56:50:00:25	
License Unit Serial Number	500025	
:		
Installation Mode	Arm Without Tones	
Ranging Mode	Auto 0 to 40 km	

Click **Continue to Installation Wizard.**

Software License Key page

Menu option: **Installation** (Figure 60). Use this page to configure the unit with a new License Key and to review the capabilities of an installed License Key. The Capability Summary section is not displayed until a License Key is submitted and accepted. Ensure that Licenses Keys are available (Generating a License Key on page 6-3).

Figure 60 Software License Key page (showing a Mid license)



Software License Key

A valid software license key is required before installation of the PTP (Point to Point) wireless link can commence. To obtain a license key, please follow the instructions in the user guide.

License key data entry

Attributes	Value	Units
License Key	/A 500025 /C USA /E 3 /G 1 /I 1 /M 1 /P 3 /R 1 /R 12 /R 14 /T 1 /H EJ5KWXCQX6ONCWKS7RUFQNHXYQ======	

Full capability trial license

Attributes	Value	Units
License Full Capability Trial Status	Available	
Activate Full Capability Trial License	● No ○ Yes	

Capability summary

Attributes	Value	Units
MAC Address	00:04:56:50:00:25	
License Unit Serial Number	500025	
License Country	USA	
License Number Of Regulatory Bands	3	
License Regulatory Bands List 1	1 - 5.8 GHz	
License Regulatory Bands List 2	12 - 5.4 GHz	
License Regulatory Bands List 3	14 - 4.9 GHz Public Safety	
License Encryption	AES 256-bit (Rijndael)	
License Group Access	Enabled	
License OOB Management Support	Enabled	
License SFP Port Support	Enabled	
License Auxiliary Port Support	Enabled	
License Capacity	Mid	
License IPv6 Support	Enabled	

Note

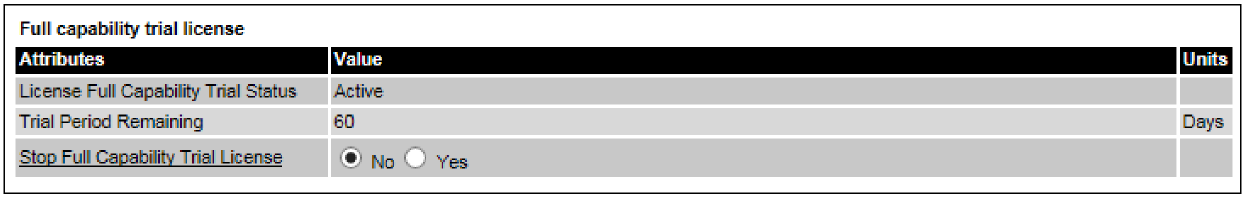
Full capability is available only when both ODUs have the trial active or are already licensed to operate with that capacity.

When the trial has started, the Software License Key page displays the Trial Period Remaining attribute (Figure 61). This shows the number of days remaining before the full capacity trial period expires.

Procedure:

- To clear the existing License Key (if present), click **Clear**.
- To format the new License Key: copy it from the Cambium notification email, paste it into the License Key box and click **Format**. The page is redisplayed with the License Key formatted.
- For Lite and Mid licenses only, select one of the following options:
  - If License Full Capability Trial Status is **Available** (Figure 60): to start the full capability trial period, set Activate Full Capability Trial License to **Yes**.
  - If License Full Capability Trial Status is **Active** (Figure 61): to suspend the full capability trial period, set Stop Full Capability Trial License to **Yes**.
  - If License Full Capability Trial Status is **Inactive** (Figure 62): to resume the full capability trial period, set Start Full Capability Trial License to **Yes**.
- To enter the new License Key, click **Submit**. The page is redisplayed with the Capability Summary.
- To continue with the Installation Wizard, click **Next**.

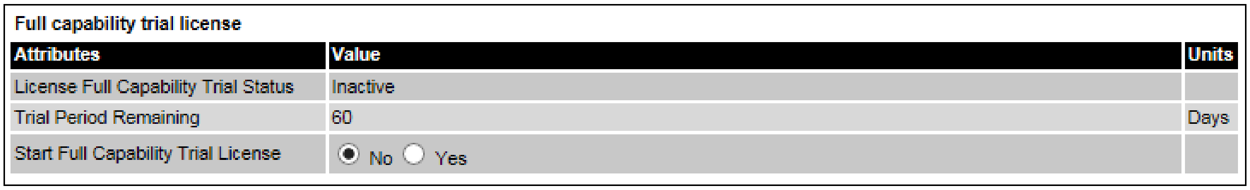
Figure 61 Software License Key page (extract) with full capability trial active



Full capability trial license

Attributes	Value	Units
License Full Capability Trial Status	Active	
Trial Period Remaining	60	Days
Stop Full Capability Trial License	● No ○ Yes	

Figure 62 Software License Key page (extract) with full capability trial inactive



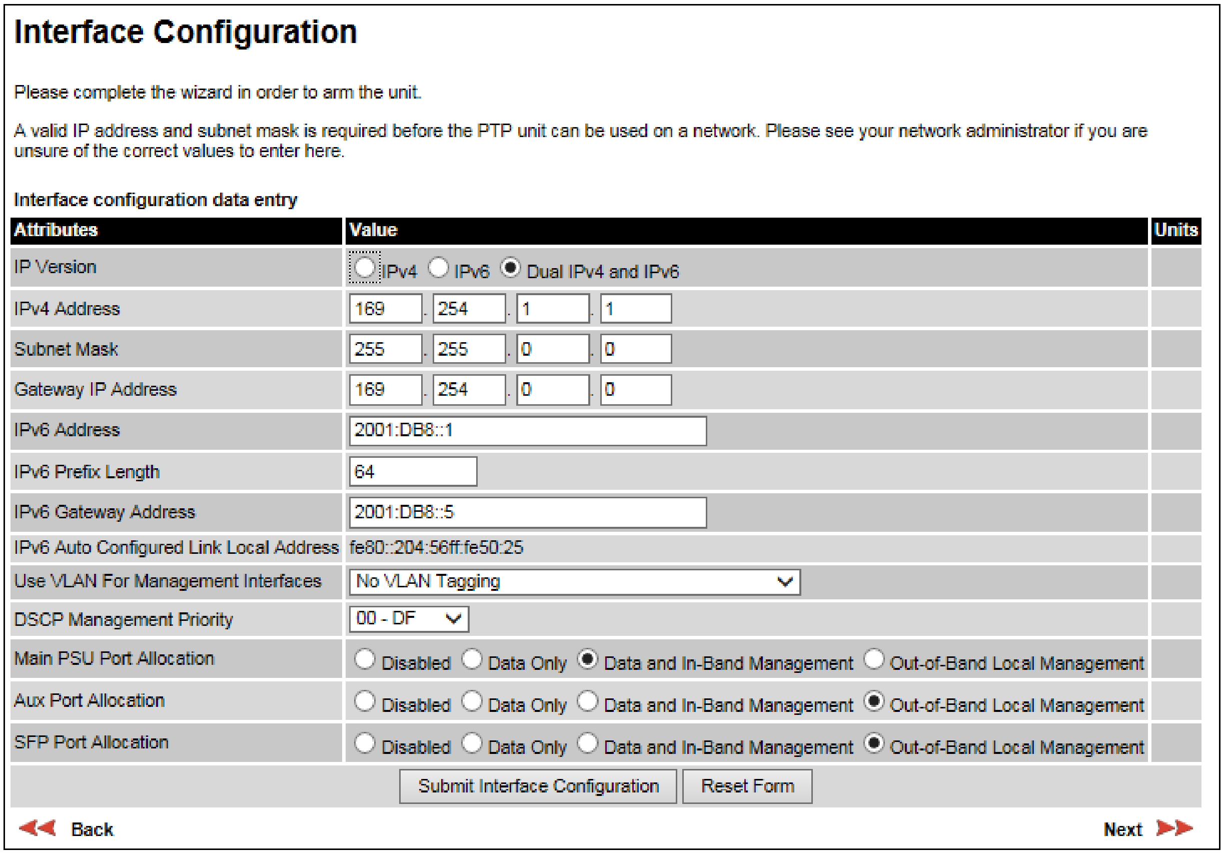
Full capability trial license

Attributes	Value	Units
License Full Capability Trial Status	Inactive	
Trial Period Remaining	60	Days
Start Full Capability Trial License	● No ○ Yes	

Interface Configuration page

Menu option: **Installation** (Figure 63). Use this page to update the IP interface attributes.

Figure 63 Interface Configuration page (showing Dual IPv4 and IPv6)



Interface Configuration

Please complete the wizard in order to arm the unit.

A valid IP address and subnet mask is required before the PTP unit can be used on a network. Please see your network administrator if you are unsure of the correct values to enter here.

Interface configuration data entry

Attributes	Value	Units
IP Version	○ IPv4 ○ IPv6 ● Dual IPv4 and IPv6	
IPv4 Address	169 . 254 . 1 . 1	
Subnet Mask	255 . 255 . 0 . 0	
Gateway IP Address	169 . 254 . 0 . 0	
IPv6 Address	2001:DB8::1	
IPv6 Prefix Length	64	
IPv6 Gateway Address	2001:DB8::5	
IPv6 Auto Configured Link Local Address	fe80::204:56ff:fe50:25	
Use VLAN For Management Interfaces	No VLAN Tagging	
DSCP Management Priority	00 - DF	
Main PSU Port Allocation	○ Disabled ○ Data Only ● Data and In-Band Management ○ Out-of-Band Local Management	
Aux Port Allocation	○ Disabled ○ Data Only ○ Data and In-Band Management ● Out-of-Band Local Management	
SFP Port Allocation	○ Disabled ○ Data Only ○ Data and In-Band Management ● Out-of-Band Local Management	

Review and update the attributes: they are repeated in the LAN Configuration page (Table 72).

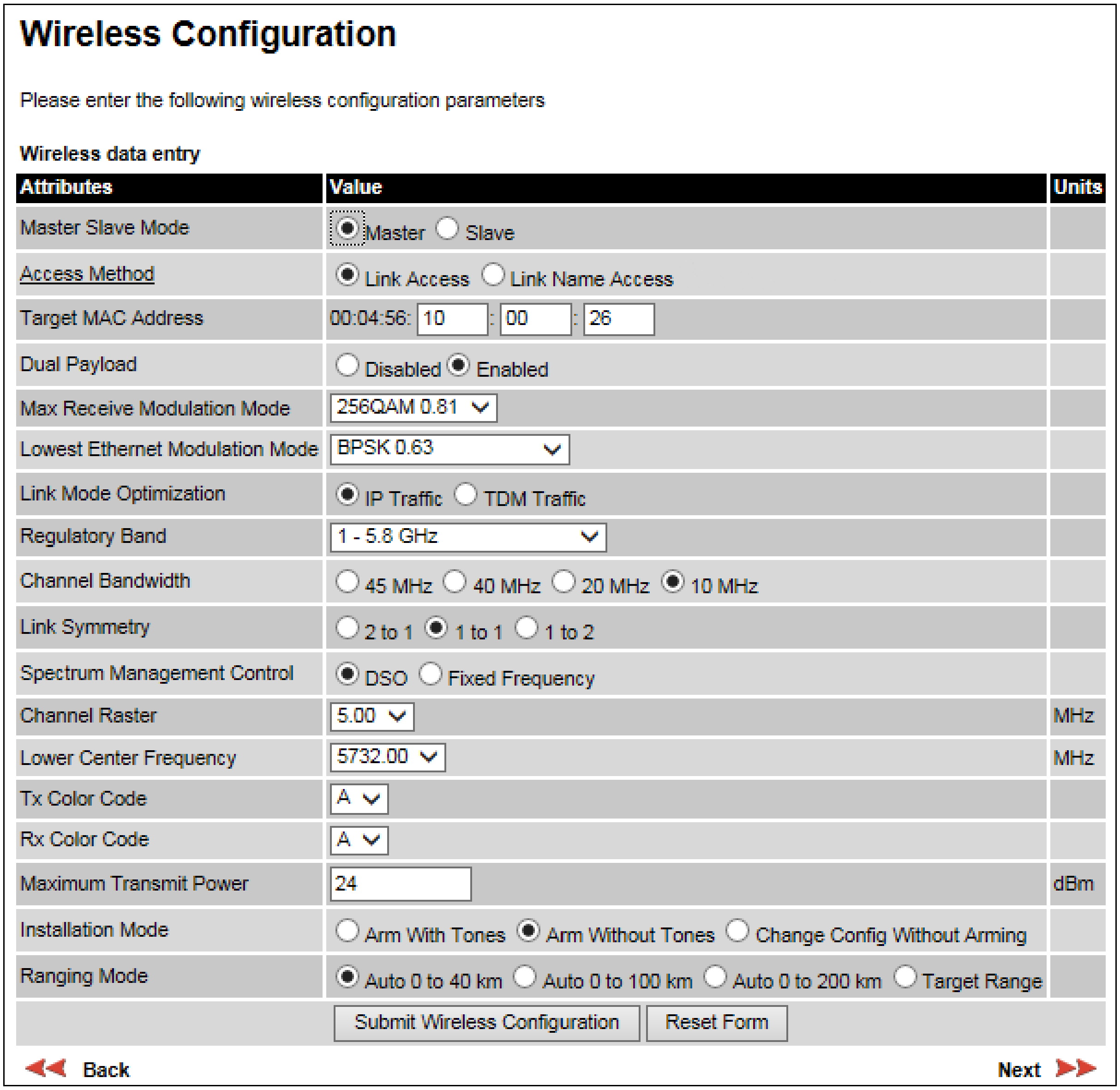
To continue with the Installation Wizard, click **Next** or **Submit Interface Configuration**.

Wireless Configuration page

Menu option: **Installation** (Figure 64).

This page is part of the Installation Wizard. Use it to update the wireless attributes.

Figure 64 Wireless Configuration page



Wireless Configuration

Please enter the following wireless configuration parameters

Wireless data entry

Attributes	Value	Units
Master Slave Mode	● Master ○ Slave	
Access Method	● Link Access ○ Link Name Access	
Target MAC Address	00:04:56: 10 : 00 : 26	
Dual Payload	○ Disabled ● Enabled	
Max Receive Modulation Mode	256QAM 0.81	
Lowest Ethernet Modulation Mode	BPSK 0.63	
Link Mode Optimization	● IP Traffic ○ TDM Traffic	
Regulatory Band	1 - 5.8 GHz	
Channel Bandwidth	○ 45 MHz ○ 40 MHz ○ 20 MHz ● 10 MHz	
Link Symmetry	○ 2 to 1 ● 1 to 1 ○ 1 to 2	
Spectrum Management Control	● DSO ○ Fixed Frequency	
Channel Raster	5.00	MHz
Lower Center Frequency	5732.00	MHz
Tx Color Code	A	
Rx Color Code	A	
Maximum Transmit Power	24	dBm
Installation Mode	○ Arm With Tones ● Arm Without Tones ○ Change Config Without Arming	
Ranging Mode	● Auto 0 to 40 km ○ Auto 0 to 100 km ○ Auto 0 to 200 km ○ Target Range	

Procedure:

- Update the attributes (Table 70).
- To save any changes and continue with the Installation Wizard, click **Next** or click **Submit Wireless Configuration**.

Caution

The lower center frequency attribute must be configured to the same value for both the Master and Slave, otherwise the wireless link will fail to establish. The only way to recover from this situation is to modify the Lower Center Frequency attributes so that they are identical on both the master and slave units.

Note

When configuring a linked pair of units, use the Master Slave Mode to ensure that one unit is **Master** and the other is **Slave**.

Table 70 Wireless Configuration attributes

Attribute	Meaning
Master Slave Mode	**Master:** The unit controls the point-to-point link and its maintenance. On startup, the Master transmits until a link with the Slave is made. **Slave:** The unit listens for its peer and only transmits when the peer has been identified.
Access Method	ODUs must be configured in pairs before a link can be established. Access Method determines how paired ODUs will recognize each other. **Link Access:** Each ODU must be configured with Target MAC Address equal to the MAC Address of the other unit. **Link Name Access:** Both ODUs must be configured with the same Link Name.
Target MAC Address	Only displayed when Access Method is set to **Link Access**. This is the MAC Address of the peer unit that will be at the other end of the wireless link. This is used by the system to ensure the unit establishes a wireless link to the correct peer. The MAC Address can be found embedded within the serial number of the unit. The last six characters of the serial number are the last three bytes of the unit's MAC address.
Link Name	Only displayed when Access Method is set to **Link Name Access**. Link Name may consist of letters (A-Z and a-z), numbers (0-9), spaces, and the following special characters: (),-.,:<=>[]_{} Link Name must be same at both ends and different to site name.
Dual Payload	**Disabled:** The link maximizes robustness against fading and interference. **Enabled:** The link attempts to reach maximum throughput at the expense of robustness against fading and interference.

Attribute	Meaning
Max Receive Modulation Mode	The maximum mode the unit will use as its adaptive modulation. By default the Max Receive Modulation Mode is the highest mode available. For minimum error rates, set the maximum modulation mode to the minimum necessary to carry the required traffic.
Lowest Ethernet Modulation Mode	The lowest modulation mode that must be achieved before the link is allowed to bridge Ethernet frames.
Link Mode Optimization	**IP Traffic:** The link is optimized for IP traffic to provide the maximum possible link capacity. **TDM Traffic:** The link is optimized for TDM traffic to provide the lowest possible latency.
Regulatory Band	The regulatory band selected from the list in the license key.
Channel Bandwidth	Bandwidth of the transmit and receive radio channels.
Link Symmetry	Only displayed when Master Slave Mode is set to **Master**. **Adaptive**: Allows link symmetry to vary dynamically in response to offered traffic load. This is not supported in the following cases: • Where radar avoidance is mandated in the region. • Link Mode Optimization is set to **TDM Traffic**. **"2 to 1"**, "**1 to 1"** or "**1 to 2"**: There is a fixed division between transmit and receive time in the TDD frame of the master ODU. The first number in the ratio represents the time allowed for the transmit direction and the second number represents the time allowed for the receive direction. The appropriate matching Link Symmetry is set at the slave ODU automatically. For example, if Link Symmetry is set to "**2 to 1"** at the master ODU, then the slave ODU will be set automatically as "**1 to 2"**. In this example, the master-slave direction has double the capacity of the slave-master direction.
Spectrum Management Control	In regions that do not mandate DFS (radar detection), the options are: **DSO** **Fixed Frequency** In regions that mandate DFS (radar detection), the options are: **DFS** **DFS with DSO** This attribute is disabled if the regulatory requirement is fixed frequency only.

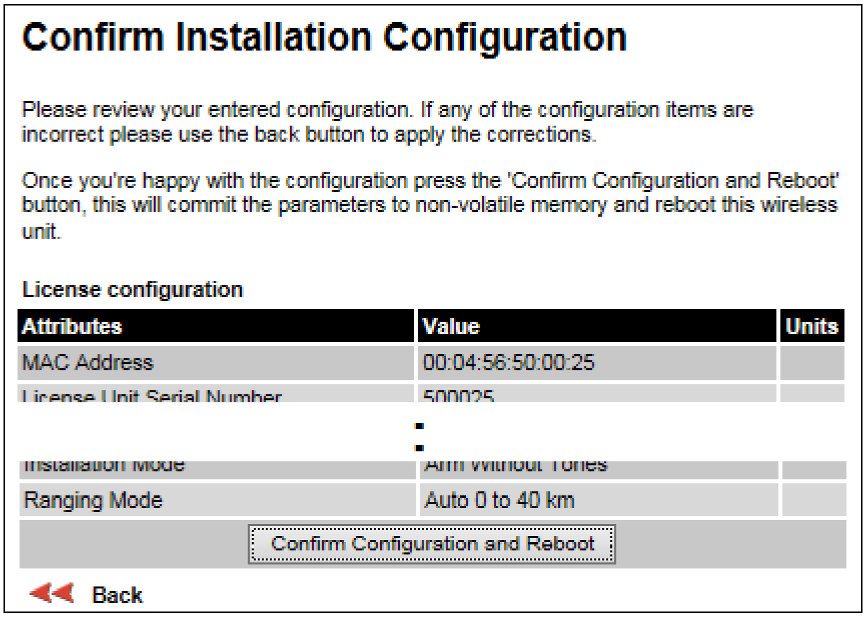
Attribute	Meaning
Lower Center Frequency	The center frequency (MHz) of the lowest channel that may be used by this link. Not displayed when Spectrum Management Control is set to **Fixed Frequency**. Use this attribute to slide the available channels up and down the band.
Default Raster	This is only displayed when Spectrum Management Control is set to **Fixed Frequency**. Limits frequency selection to the unit's default raster setting.
Fixed Tx Frequency, Fixed Rx Frequency	This is only displayed when Spectrum Management Control is set to **Fixed Frequency**. The settings must be compatible at each end of the link. Once configured, the spectrum management software will not attempt to move the wireless link to a channel with lower co-channel or adjacent channel interference. Therefore this mode of operation is only recommended for deployments where the installer has a good understanding of the prevailing interference environment.
Tx Color Code, Rx Color Code	Tx Color Code and Rx Color Code may be used to minimize interference in a dense network of synchronized PTP 650 units where some of the units are operating on the same frequency. When this type of network is designed, the Color Code values are normally specified in the link planning report. In all other cases, Cambium Networks recommend that Tx Color Code and Rx Color Code are left at the default value of **A**. The value of Tx Color Code MUST always match the value of Rx Color Code at the other end of the link.
Antenna Gain	Only displayed when the ODU is connectorized. Gain of the remote antenna.
Cable Loss	Only displayed when the ODU is connectorized. Loss in the ODU-antenna RF cable. If there is a significant difference in length of the RF cables for the two antenna ports, then the average value should be entered.
Maximum Transmit Power	The maximum power (dBm) at which the unit will transmit, configurable in steps of 1 dB. Its maximum value is controlled by the selected combination of Regulatory Band, Bandwidth and (for connectorized units) Antenna Gain and Cable Loss. To prepare for antenna alignment, set this attribute to the alignment value specified in the installation report (PTP LINKPlanner). To prepare for link operation, set this attribute to the operational value specified in the installation report (PTP LINKPlanner). This may be higher than the alignment value.

Attribute	Meaning
Installation Mode	**Arm With Tones**: Audio tones will be emitted during antenna alignment (the recommended option). **Arm Without Tones**: Audio tones will not be emitted during antenna alignment. **Change Config Without Arming**: Configuration changes will be made without arming the ODU for alignment.
Ranging Mode	This can only be modified if Installation Mode is **Arm With Tones** or **Arm Without Tones**. **Auto..**: During alignment, the wireless units use algorithms to calculate link range. To implement automatic ranging, select a value that corresponds to the estimated maximum range of the link: **Auto 0 to 40 km** (0 to 25 miles). **Auto 0 to 100km** (0 to 62 miles). **Auto 0 to 200km** (0 to 125 miles). **Target Range**: During alignment, the wireless units use the approximate link distance (entered in Target Range) to calculate link range. The main advantage of Target Range mode is that it reduces the time taken by the units to range. If preferred, range functions can be configured to operate in miles, as described in Webpage Properties page on page 6-49.
Target Range	Only available when Ranging Mode is set to **Target Range**. The approximate distance between the two wireless units to within ± 1 km. Enter the same value at both ends of the link.

Confirm Installation Configuration page

Menu option: **Installation** (Figure 65). Use this page to review and confirm the updated wireless configuration of the unit.

Figure 65 Confirm Installation Configuration page (top and bottom of page shown)



Confirm Installation Configuration

Please review your entered configuration. If any of the configuration items are incorrect please use the back button to apply the corrections.

Once you're happy with the configuration press the 'Confirm Configuration and Reboot' button, this will commit the parameters to non-volatile memory and reboot this wireless unit.

License configuration

Attributes	Value	Units
MAC Address	00:04:56:50:00:25	
License Unit Serial Number	500025	
:		
Installation Mode	Arm Without Tones	
Ranging Mode	Auto 0 to 40 km	

Procedure:

- To undo or correct any updates, click **Back.**
- To confirm the updates and arm the installation, click **Confirm Configuration and Reboot** and click **OK** to reboot the unit.
- If IP Address, Subnet Mask or Gateway IP Address have been changed: reconfigure the local management PC to use an IP address that is valid for the network. Refer to Configuring the management PC on page 6-5.
- If IP Address has been changed, use the new IP address to log into the unit.

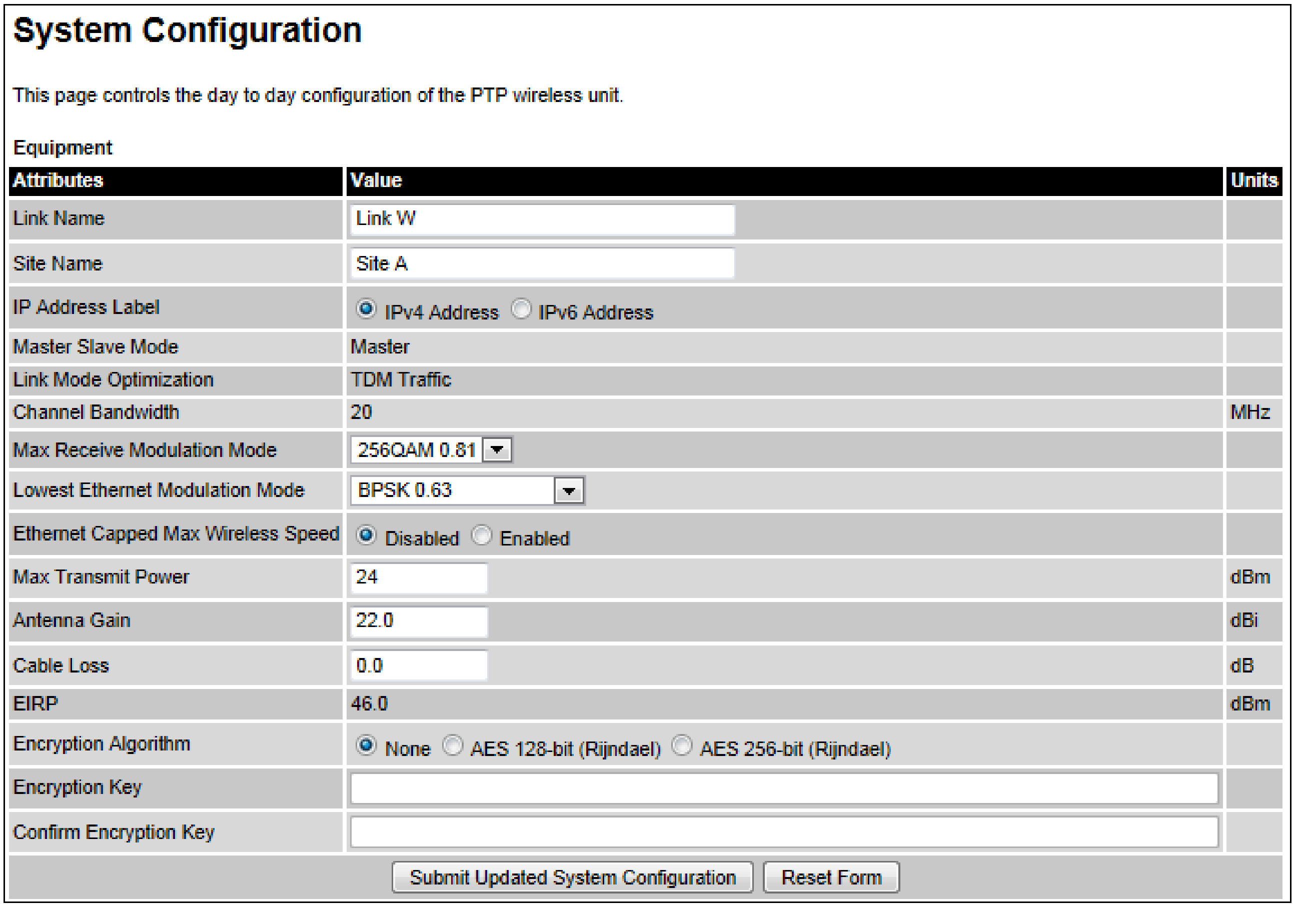
System menu

This section describes how to configure the IP and Ethernet interfaces of the PTP 650 unit.

System Configuration page

Menu option: **System > Configuration** (Figure 66). Use this page to enable AES encryption and to review and update key wireless attributes of the unit.

Figure 66 System Configuration page



System Configuration

This page controls the day to day configuration of the PTP wireless unit.

Equipment

Attributes	Value	Units
Link Name	Link W	
Site Name	Site A	
IP Address Label	● IPv4 Address ○ IPv6 Address	
Master Slave Mode	Master	
Link Mode Optimization	TDM Traffic	
Channel Bandwidth	20	MHz
Max Receive Modulation Mode	256QAM 0.81 ▾	
Lowest Ethernet Modulation Mode	BPSK 0.63 ▾	
Ethernet Capped Max Wireless Speed	● Disabled ○ Enabled	
Max Transmit Power	24	dBm
Antenna Gain	22.0	dBi
Cable Loss	0.0	dB
EIRP	46.0	dBm
Encryption Algorithm	● None ○ AES 128-bit (Rijndael) ○ AES 256-bit (Rijndael)	
Encryption Key		
Confirm Encryption Key		

Caution

Configuring link encryption over an operational link will necessitate a service outage. Therefore, the configuration process should be scheduled during a period of low link utilization.

Procedure:

- If AES encryption is required but the System Configuration page does not contain the Encryption Algorithm or Encryption Key attributes, then order the necessary AES capability upgrade, generate a license key and enter it on the Software License Key page (Software License Key page on page 6-12).
- Update the attributes (Table 71).
- To save changes, click **Submit Updated System Configuration**.
- If a reboot request is displayed, click **Reboot Wireless Unit** and **OK** to confirm.

Table 71 System Configuration attributes

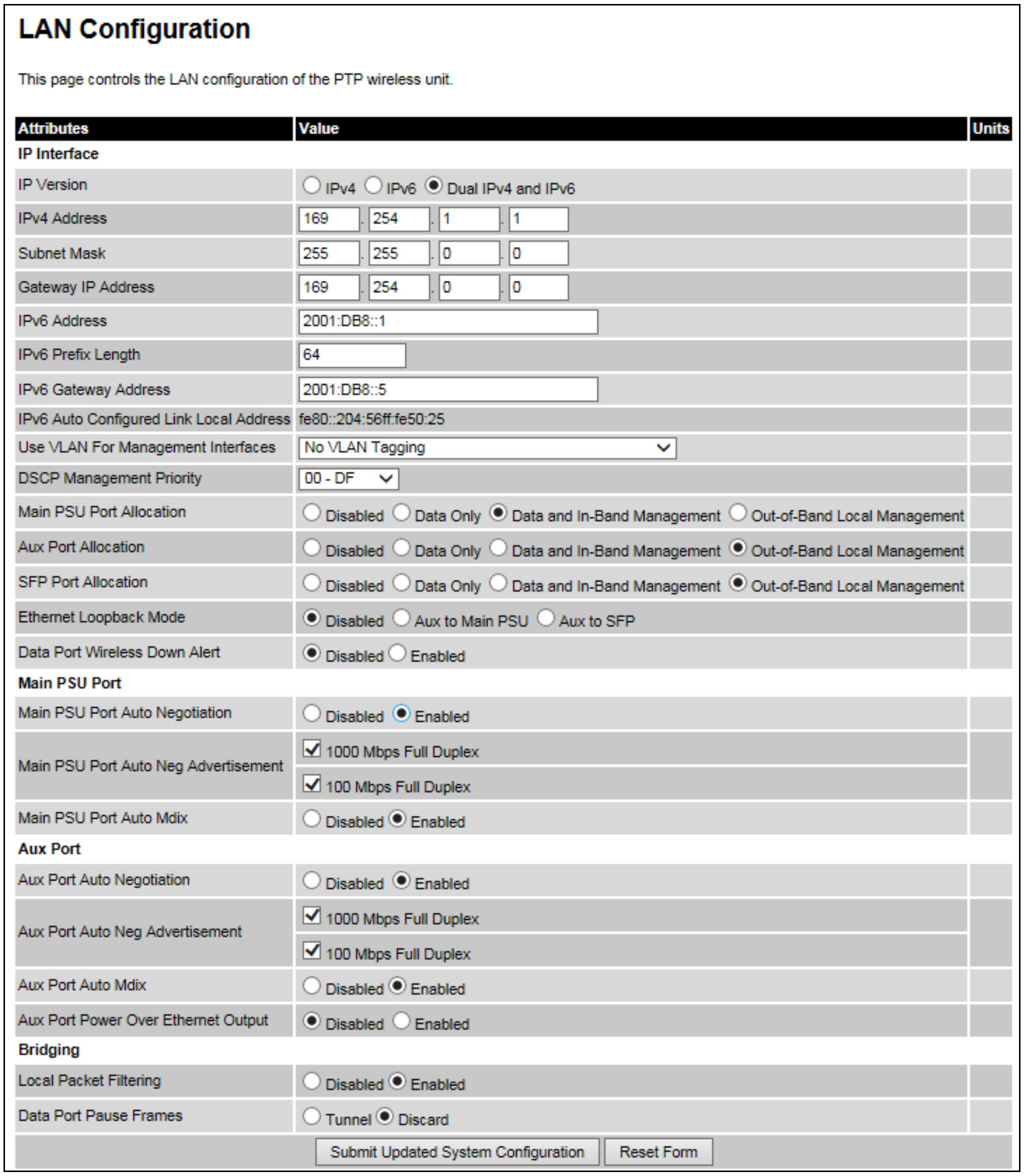
Attribute	Meaning
Link Name	Link Name may consist of letters (A-Z and a-z), numbers (0-9), spaces, and the following special characters: (),-.,:<=>[]_{}. Link Name must be same at both ends and different to site name.
Site Name	User defined name for the site, with additional notes (if required).
IP Address Label	Read only. The IP Address version used to identify the unit in SMTP messages, fault logs and other system outputs. **IPv4** or **IPv6**: The unit is identified using its IPv4 or IPv6 Address. These options are only available when IP Version is set to **Dual IPv4 and IPv6** in the in the LAN Configuration page (Table 72).
Master Slave Mode	**Master:** The unit is a Master, that is, it controls the point-to-point link and its maintenance. On startup, the Master transmits until a link with the Slave is made. **Slave:** The unit is a Slave, that is, it listens for its peer and only transmits when the peer has been identified. Read only.
Link Mode Optimization	**IP Traffic:** The link is optimized for IP traffic to provide the maximum possible link capacity. **TDM Traffic:** The link is optimized for TDM traffic to provide the lowest possible latency. Read only.
Channel Bandwidth	Bandwidth of the transmit and receive radio channels. Read only.
Max Receive Modulation Mode	The maximum mode the unit will use as its adaptive modulation. By default the Max Receive Modulation Mode is the highest mode available. For minimum error rates, set the maximum modulation mode to the minimum necessary to carry the required traffic.

Attribute	Meaning
Lowest Ethernet Modulation Mode	The lowest modulation mode that must be achieved before the link is allowed to bridge Ethernet frames.
Ethernet Capped Max Wireless Speed	**Disabled**: Wireless speed is not limited by the connected Ethernet link. **Enabled:** Wireless speed is limited to a mode that the connected Ethernet link can sustain. If either ODU is connected to an Ethernet link operating at less than 1000 Mbps, set this attribute to **Enabled**.
Max Transmit Power	The maximum power (dBm) at which the unit will transmit, configurable in steps of 1 dB. Its maximum value is controlled by the combination of the selected Regulatory Band, Bandwidth and (for connectorized units) Antenna Gain and Cable Loss. To prepare for antenna alignment, set this attribute to the alignment value specified in the installation report (PTP LINKPlanner). To prepare for link operation, set this attribute to the operational value specified in the installation report (PTP LINKPlanner). This may be higher than the alignment value.
Antenna Gain	Only displayed when the ODU is connectorized. Gain of the remote antenna.
Cable Loss	Only displayed when the ODU is connectorized. Loss in the ODU-antenna RF cable. If there is a significant difference in length of the RF cables for the two antenna ports, then the average value should be entered.
EIRP	Only displayed when the ODU is connectorized. Effective Isotropic Radiated Power (EIRP) describes the strength of the radio signal leaving the wireless unit. Use it to verify that the link configuration (Max Transmit Power, Antenna Gain and Cable Loss) does not exceed any applicable regulatory limit. Read only.
Encryption Algorithm	Only displayed when AES encryption is enabled by license key. Values are: **None**, **AES 128-bit** or **AES 256-bit**. Use the same setting at both link ends.
Encryption Key	Only displayed when AES encryption is enabled by license key. The key consists of 32 or 64 case-insensitive hexadecimal characters. Use the same key at both link ends.
Confirm Encryption Key	Only displayed when AES encryption is enabled by license key. Retype the Encryption Key.

LAN Configuration page

Menu option: **System > Configuration > LAN Configuration** (Figure 67). Use this page to control how users connect to the PTP 650 web interface, either from a locally connected computer or from a management network.

Figure 67 LAN Configuration page (showing Dual IPv4 and IPv6)



LAN Configuration

This page controls the LAN configuration of the PTP wireless unit.

Attributes	Value	Units
IP Interface		
IP Version	○ IPv4 ○ IPv6 ● Dual IPv4 and IPv6	
IPv4 Address	169 . 254 . 1 . 1	
Subnet Mask	255 . 255 . 0 . 0	
Gateway IP Address	169 . 254 . 0 . 0	
IPv6 Address	2001:DB8::1	
IPv6 Prefix Length	64	
IPv6 Gateway Address	2001:DB8::5	
IPv6 Auto Configured Link Local Address	fe80::204:56ff:fe50:25	
Use VLAN For Management Interfaces	No VLAN Tagging	
DSCP Management Priority	00 - DF	
Main PSU Port Allocation	○ Disabled ○ Data Only ● Data and In-Band Management ○ Out-of-Band Local Management	
Aux Port Allocation	○ Disabled ○ Data Only ○ Data and In-Band Management ● Out-of-Band Local Management	
SFP Port Allocation	○ Disabled ○ Data Only ○ Data and In-Band Management ● Out-of-Band Local Management	
Ethernet Loopback Mode	● Disabled ○ Aux to Main PSU ○ Aux to SFP	
Data Port Wireless Down Alert	● Disabled ○ Enabled	
Main PSU Port		
Main PSU Port Auto Negotiation	○ Disabled ● Enabled	
Main PSU Port Auto Neg Advertisement	☑ 1000 Mbps Full Duplex ☑ 100 Mbps Full Duplex	
Main PSU Port Auto Mdix	○ Disabled ● Enabled	
Aux Port		
Aux Port Auto Negotiation	○ Disabled ● Enabled	
Aux Port Auto Neg Advertisement	☑ 1000 Mbps Full Duplex ☑ 100 Mbps Full Duplex	
Aux Port Auto Mdix	○ Disabled ● Enabled	
Aux Port Power Over Ethernet Output	● Disabled ○ Enabled	
Bridging		
Local Packet Filtering	○ Disabled ● Enabled	
Data Port Pause Frames	○ Tunnel ● Discard	

Caution

Before configuring a VLAN for management interfaces, ensure that the VLAN is accessible, otherwise the unit will be inaccessible after the next reboot.

Caution

Before configuring in-band management, ensure that the Master and Slave units are configured with different IP addresses, otherwise the management agent will not be able to distinguish the two units.

Caution

Auto-negotiation and forced Ethernet configuration:

- To operate an Ethernet link at a fixed speed, set Auto Negotiation to **Enabled** and limit Auto Neg Advertisement to the desired speed. If constrained auto-negotiation fails, set Auto Negotiation to **Disabled** (forced Ethernet configuration), but only as a last resort.
- Both ends of an Ethernet link must be configured identically, because forced and auto-negotiation are not compatible: a mixed configuration will cause a duplex mismatch, resulting in greatly reduced data capacity.
- The Auto Neg Advertisement or Forced Configuration data rates must be within the capability of the Ethernet link partner, otherwise loss of service will occur.

Procedure:

1. Review and update the attributes: IP Interface (Table 72); Main PSU or Aux Port (Table 73); Bridging (Table 74).
2. To save changes, click **Submit Updated System Configuration**. Some updates will cause the system to reboot.
3. If Main PSU Port Allocation has been changed to **Disabled** or **Data Only**, connect the management PC to whichever port (Aux or SFP) has been set to **Data and In-Band Management** or **Out-of-Band Local Management**.
4. If IP Address, Subnet Mask or Gateway IP Address have been changed, reconfigure the local management PC to use an IP address that is valid for the network. Refer to Configuring the management PC on page 6-5.
5. If IP Address has been changed, use the new IP address to log into the unit.

Table 72 IP interface attributes

Attribute	Meaning
IP Version	The internet protocols to be supported by this ODU: **IPv4:** IPv4 protocols only. IPv4 attributes are displayed. **IPv6:** IPv6 protocols only. IPv6 attributes are displayed. **Dual IPv4 and IPv6:** Both IPv4 and IPv6 protocols. IPv4 and IPv6 attributes are displayed.
IPv4 Address	The IPv4 internet protocol address. This address is used by the family of Internet protocols to uniquely identify this unit on a network.
Subnet Mask	The address range of the connected IPv4 network.
Gateway IP Address	The IPv4 address of a computer on the current network that acts as an IPv4 gateway. A gateway acts as an entrance and exit to frames from and to other networks.
IPv6 Address	The IPv6 internet protocol address. This address is used by the family of Internet protocols to uniquely identify this unit on a network.
IPv6 Prefix Length	Length of the IPv6 subnet prefix (default 64 bits).
IPv6 Gateway Address	The IPv6 address of a computer on the current network that acts as an IPv6 gateway. A gateway acts as an entrance and exit to frames from and to other networks. It is usual to use the link-local address of the gateway.
IPv6 Auto Configured Link Local Address	The link-local address of the IPv6 gateway (displayed only, not updateable).
Use VLAN For Management Interfaces	VLAN tagging options for the management interfaces: **No VLAN Tagging** **IEEE 802.1Q Tagged (C-Tag, Type 8100)** **IEEE 802.1ad Tagged (S-Tag or B-Tag, Type 88a8)** Ensure that the configured VLAN is accessible, otherwise it will not be possible to access the unit following the next reboot. The PTP 650 management function is only compatible with single VLAN tagged frames. Any management frame with two or more tags will be ignored.

Attribute	Meaning
VLAN Management VID	Only displayed when Use VLAN for Management Interfaces is not set to **No VLAN Tagging**. The VLAN VID (range 0 to 4094) that will be included in Ethernet frames generated by the management interfaces.
VLAN Management Priority	Only displayed when Use VLAN for Management Interfaces is not set to **No VLAN Tagging**. The VLAN priority (range 0 to 7) that will be included in Ethernet frames generated by the management interfaces.
DSCP Management Priority	Differentiated Services Code Point (DSCP) value to be inserted in the IP header of all IP datagrams transmitted by the management interface.
Main PSU Port Allocation Aux Port Allocation SFP Port Allocation	**Disabled**: The port is not used. **Data Only**: The port handles customer data only. **Data and In-Band Management**: The port handles both customer data and network management data. It can be used to access the web interface of the local unit, and if the wireless link is established, the remote unit. Ensure that the local and remote units have different IP addresses. **Out-of-band Local Management**: The port handles local management data only. It can be used to access the web interface of the local unit. Only one port can be allocated to customer data. At least one port must be allocated to management data.
Ethernet Loopback Mode	Sets a temporary loopback between the selected ports. The loopback is disabled on a reboot. This mode is provided to allow access to a device connected to the local ODU Aux port via either the main PSU or SFP port. Loopback does not work with jumbo frames: the maximum frame size is 1536 bytes in loopback.
Data Port Wireless Down Alert	**Disabled:** The data Ethernet link will not be dropped when the wireless link drops. **Enabled:** The data Ethernet link will be dropped briefly when the wireless link drops. This signals to the connected network equipment that this link is no longer available. Connected Ethernet switches can be configured to forward Ethernet frames on an alternative path identified using the Spanning Tree Protocol (STP).

Table 73 Main PSU Port and Aux Port attributes

Attribute	Meaning
Auto Negotiation	**Disabled:** Configuration of the Ethernet interface is forced. **Enabled:** Configuration of the Ethernet interface is automatically negotiated (default). This is the preferred setting. See the caution at the start of this section about auto-negotiation versus forced Ethernet configuration. Use the same setting for the Ethernet link partner.
Auto Neg Advertisement	Only displayed when Auto Negotiation is set to **Enabled**. The data rate that the auto-negotiation mechanism will advertise as available on the Ethernet interface (1000 Mbps or 100 Mbps Full Duplex). Select a data rate that is within the capability of the Ethernet link partner. Use the same setting for the Ethernet link partner.
Forced Configuration	Only displayed when Auto Negotiation is set to **Disabled**. This forces the speed and duplex setting of the Ethernet interface. Over-the-air throughput will be capped to the rate of the Ethernet interface at the receiving end of the link. Select a data rate that is within the capability of the Ethernet link partner. Use the same setting for the Ethernet link partner.
Auto Mdix	**Disabled:** The Auto Medium Dependent Interface (MDI)/Medium Dependent Interface Crossover (MDIX) capability is disabled. **Enabled:** The Auto Medium Dependent Interface (MDI)/Medium Dependent Interface Crossover (MDIX) capability is enabled.
Power Over Ethernet Output	Aux port only. **Disabled:** The ODU does not supply power to the auxiliary device. **Enabled:** The ODU supplies power to the auxiliary device.

Table 74 Bridging attributes

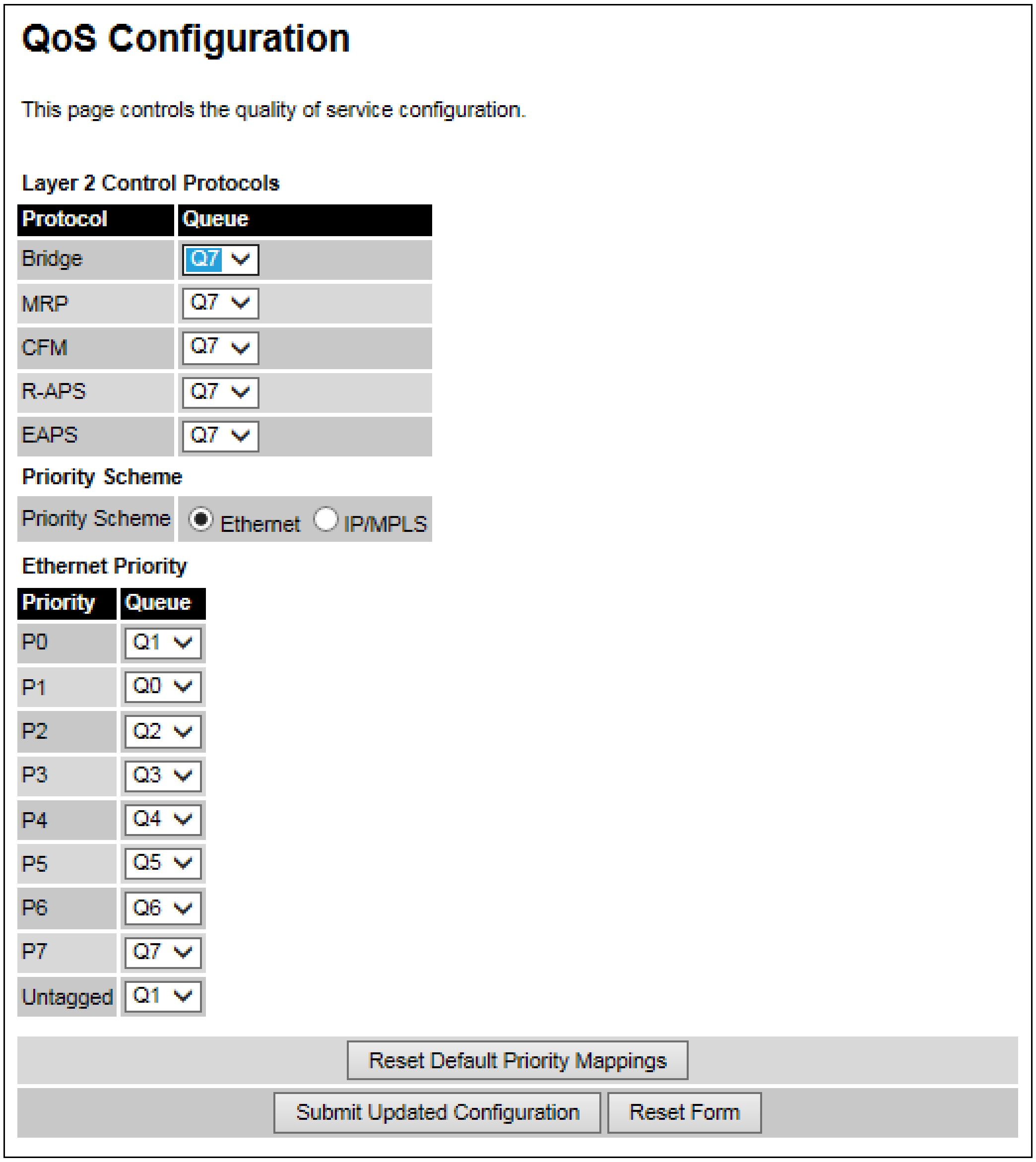
Attribute	Meaning
Local Packet Filtering	**Enabled:** The management agent learns the location of end stations from the source addresses in received management frames. The agent filters transmitted management frames to ensure that the frame is transmitted at the Ethernet (data or management) port, or over the wireless link as appropriate. If the end station address is unknown, then management traffic is transmitted at the Ethernet port and over the wireless link. In out-of-band local management mode, management frames are not transmitted over the wireless link, and so address learning is not active.
Data Port Pause Frames	Controls whether the bridge tunnels or discards Layer 2 pause frames arriving at the data port. Such frames are identified by the destination MAC Address being equal to 01-80-C2-00-00-01.

QoS Configuration page

Menu option: **System > Configuration > QoS Configuration** (Figure 68 or Figure 69).

Use this page to control the quality of service configuration. Classification may be based on fields in the Ethernet header (Layer 2) or in the network header (Layer 3). The unit recognizes two network layer protocols: IP and MPLS.

Figure 68 QoS Configuration page (Ethernet)



QoS Configuration

This page controls the quality of service configuration.

Layer 2 Control Protocols

Protocol	Queue
Bridge	Q7
MRP	Q7
CFM	Q7
R-APS	Q7
EAPS	Q7

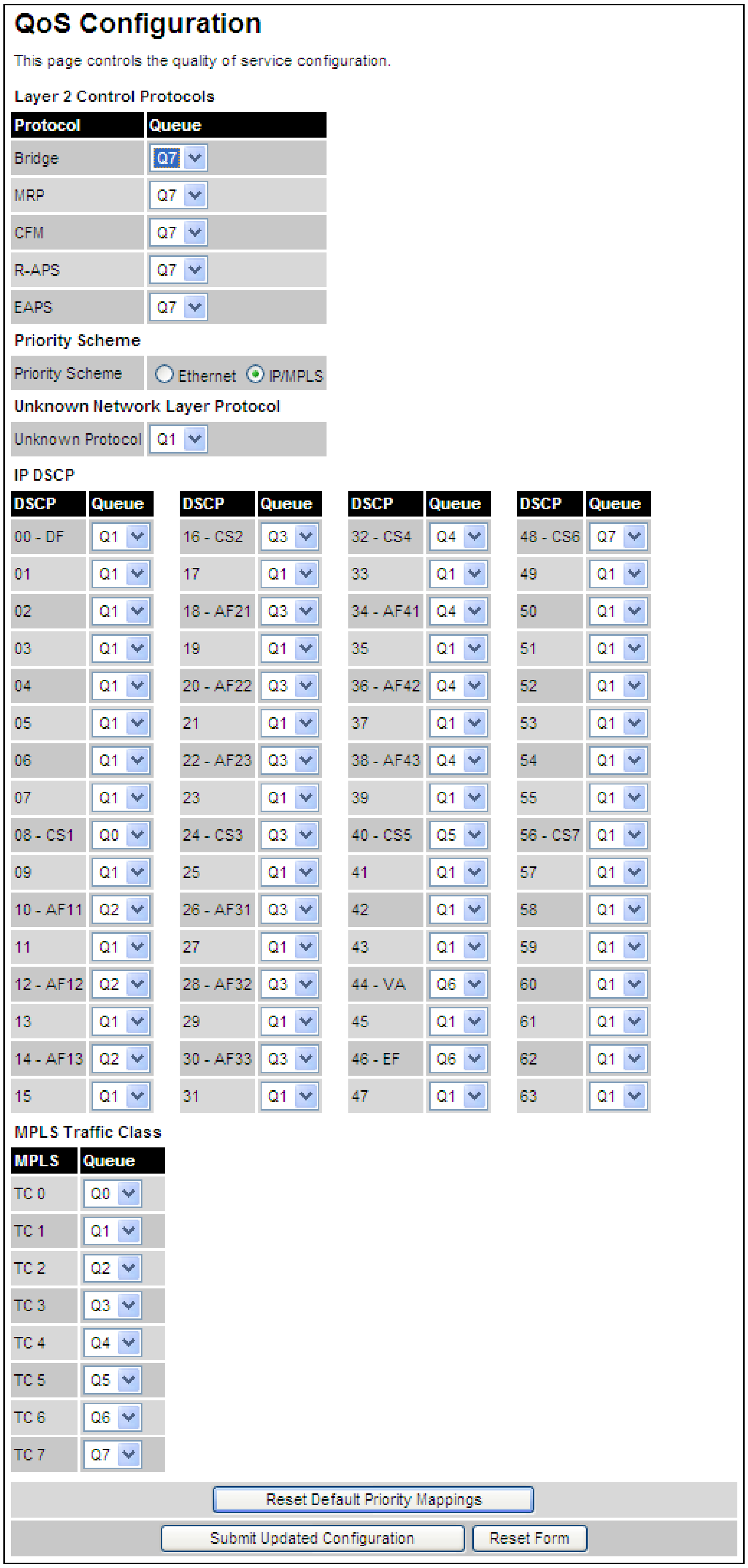
Priority Scheme

Priority Scheme	● Ethernet ○ IP/MPLS

Ethernet Priority

Priority	Queue
P0	Q1
P1	Q0
P2	Q2
P3	Q3
P4	Q4
P5	Q5
P6	Q6
P7	Q7
Untagged	Q1

Figure 69 QoS Configuration page (IP/MPLS)



QoS Configuration

This page controls the quality of service configuration.

Layer 2 Control Protocols

Protocol	Queue
Bridge	Q7
MRP	Q7
CFM	Q7
R-APS	Q7
EAPS	Q7

Priority Scheme

Priority Scheme	○ Ethernet ● IP/MPLS

Unknown Network Layer Protocol

Unknown Protocol	Q1

IP DSCP

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
00 - DF	Q1	16 - CS2	Q3	32 - CS4	Q4	48 - CS6	Q7
01	Q1	17	Q1	33	Q1	49	Q1
02	Q1	18 - AF21	Q3	34 - AF41	Q4	50	Q1
03	Q1	19	Q1	35	Q1	51	Q1
04	Q1	20 - AF22	Q3	36 - AF42	Q4	52	Q1
05	Q1	21	Q1	37	Q1	53	Q1
06	Q1	22 - AF23	Q3	38 - AF43	Q4	54	Q1
07	Q1	23	Q1	39	Q1	55	Q1
08 - CS1	Q0	24 - CS3	Q3	40 - CS5	Q5	56 - CS7	Q1
09	Q1	25	Q1	41	Q1	57	Q1
10 - AF11	Q2	26 - AF31	Q3	42	Q1	58	Q1
11	Q1	27	Q1	43	Q1	59	Q1
12 - AF12	Q2	28 - AF32	Q3	44 - VA	Q6	60	Q1
13	Q1	29	Q1	45	Q1	61	Q1
14 - AF13	Q2	30 - AF33	Q3	46 - EF	Q6	62	Q1
15	Q1	31	Q1	47	Q1	63	Q1

MPLS Traffic Class

MPLS	Queue
TC 0	Q0
TC 1	Q1
TC 2	Q2
TC 3	Q3
TC 4	Q4
TC 5	Q5
TC 6	Q6
TC 7	Q7

Procedures:

- Review and update the attributes: Layer 2 and Priority Scheme (Table 75).
- To use IEEE 802.1Q classification rules, click **Reset Default Priority Mappings**.
- To save changes, click: **Submit Updated Configuration**.

Note

Priority mapping must be configured the same at both Master and Slave units on the wireless link.

Table 75 QoS Configuration attributes

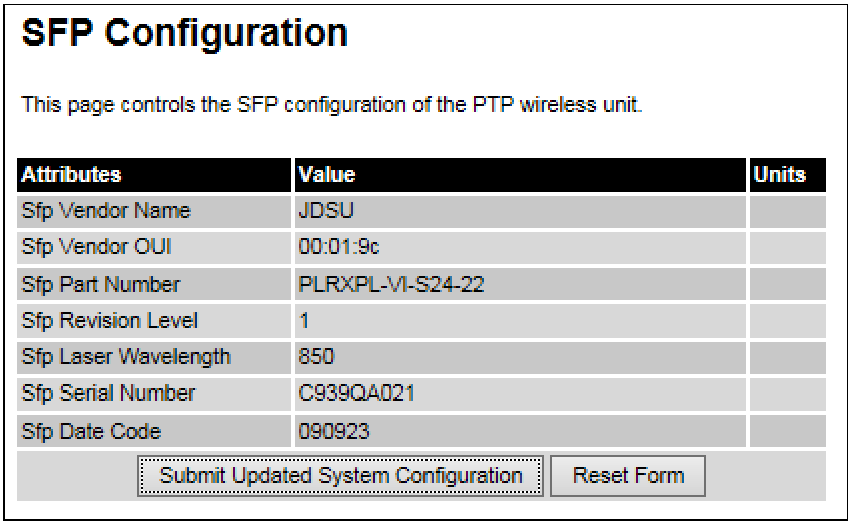
Attribute	Meaning
Bridge	The classification of each layer 2 control protocol (L2CP) to an egress queue at the wireless port.
MRP	
CFM	
R-APS	
EAPS	
Priority Scheme	**Ethernet**: Classification is based on fields in the Ethernet header (Layer 2). **IP/MPLS**: Classification is based on fields in the network header (Layer 3). IP includes IPv4 and IPv6.
Unknown Protocol	Only displayed when Priority Scheme is **IP/MPLS**. The classification of unknown network protocols (that is, not IP or MPLS) to an egress queue at the wireless port.

SFP Configuration page

Menu option: **System > Configuration > SFP Configuration**.

This page is only available when the ODU detects an optical (Figure 70) or copper (Figure 71) SFP module in the SFP port. Use it to configure the way in which the unit connects to the network via the SFP interface.

Figure 70 SFP Configuration page (optical SFP module)

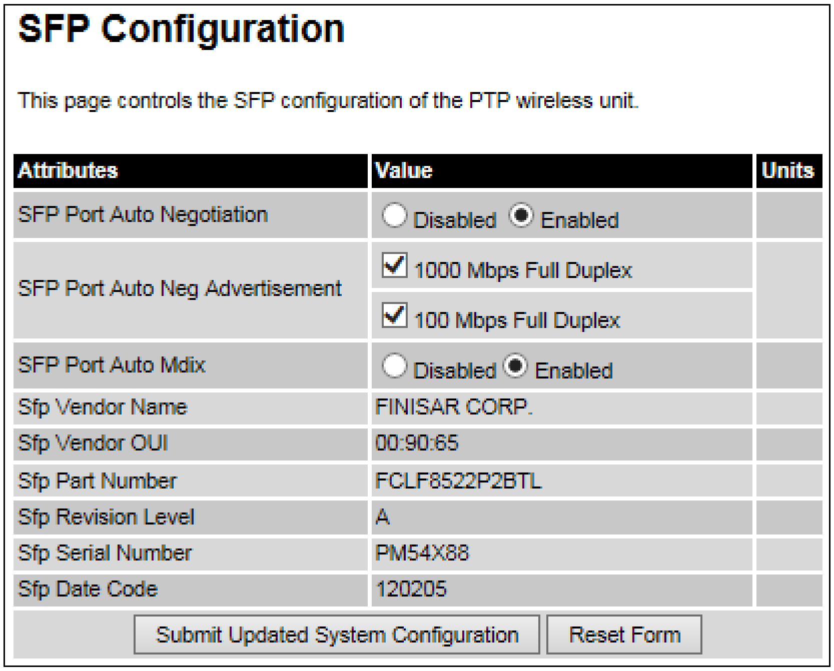


SFP Configuration

This page controls the SFP configuration of the PTP wireless unit.

Attributes	Value	Units
Sfp Vendor Name	JDSU	
Sfp Vendor OUI	00:01:9c	
Sfp Part Number	PLRXPL-VI-S24-22	
Sfp Revision Level	1	
Sfp Laser Wavelength	850	
Sfp Serial Number	C939QA021	
Sfp Date Code	090923	

Figure 71 SFP Configuration page (copper SFP module)



SFP Configuration

This page controls the SFP configuration of the PTP wireless unit.

Attributes	Value	Units
SFP Port Auto Negotiation	○ Disabled ● Enabled	
SFP Port Auto Neg Advertisement	☑ 1000 Mbps Full Duplex ☑ 100 Mbps Full Duplex	
SFP Port Auto Mdix	○ Disabled ● Enabled	
Sfp Vendor Name	FINISAR CORP.	
Sfp Vendor OUI	00:90:65	
Sfp Part Number	FCLF8522P2BTL	
Sfp Revision Level	A	
Sfp Serial Number	PM54X88	
Sfp Date Code	120205	

Procedure (only applies when copper SFP module is installed)**:**

- Update the attributes (Table 76).
- To save changes, click **Submit Updated System Configuration**.

Table 76 SFP Configuration (copper SFP module) attributes

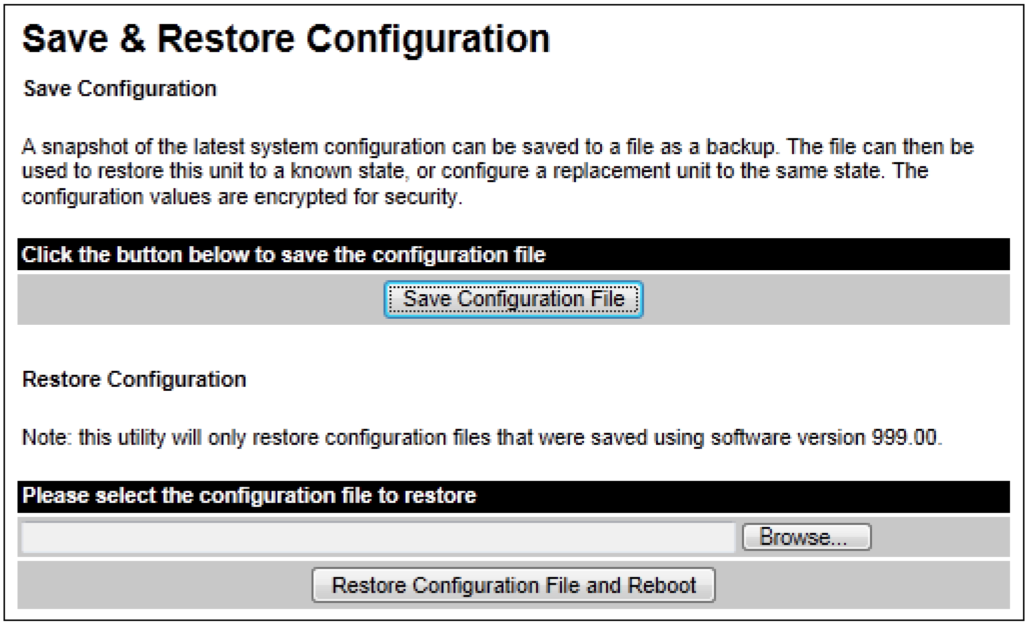
Attribute	Meaning
SFP Port Auto Negotiation	**Disabled:** Configuration of the Ethernet interface is forced. This is to be used as a last resort only if auto-negotiation fails. **Enabled:** Configuration of the Ethernet interface is automatically negotiated (default). This is the preferred setting.
SFP Port Auto Neg Advertisement	Only displayed when SFP Port Auto Negotiation is set to **Enabled**. The data rate that the auto-negotiation mechanism will advertise as available on the Ethernet interface (1000 Mbps or 100 Mbps Full Duplex). Select a data rate that is within the capability of the Ethernet link partner. Use the same setting for the Ethernet link partner.
Forced Configuration	Only displayed when SFP Port Auto Negotiation is set to **Disabled**. This forces the speed and duplex setting of the Ethernet interface. Over-the-air throughput will be capped to the rate of the Ethernet interface at the receiving end of the link. Select a data rate that is within the capability of the Ethernet link partner. Use the same setting for the Ethernet link partner.
Auto Mdix	**Disabled:** The Auto Medium Dependent Interface (MDI)/Medium Dependent Interface Crossover (MDIX) capability is disabled. **Enabled:** The Auto Medium Dependent Interface (MDI)/Medium Dependent Interface Crossover (MDIX) capability is enabled.

Save & Restore Configuration page

Menu option: **System > Configuration > Save And Restore** (Figure 72).

Use the Save & Restore Configuration page to take a snapshot of the latest system configuration as a backup. The file can then be used to restore this unit to a known state, or to configure a replacement unit to the same state. The configuration values are encrypted for security.

Figure 72 Save & Restore Configuration page


Save & Restore Configuration

Save Configuration

A snapshot of the latest system configuration can be saved to a file as a backup. The file can then be used to restore this unit to a known state, or configure a replacement unit to the same state. The configuration values are encrypted for security.

Click the button below to save the configuration file

Restore Configuration

Note: this utility will only restore configuration files that were saved using software version 999.00.

Please select the configuration file to restore

Save the system configuration in the following situations:

- After a new unit has been fully configured as described in this chapter.
- After any change has been made to the configuration.
- Before upgrading the unit to a new software version.
- After upgrading the unit to a new software version.

Note

The restore is only guaranteed to work if the installed software version has not been changed since the configuration file was saved. This is why the configuration should always be saved immediately after upgrading the software version.

Note

The license key is restored automatically if the configuration file is saved and then loaded on the same unit. However, the license key is not restored if the configuration file is loaded on a different unit. Before restoring configuration to a different PTP 650 unit, ensure that a valid license key is installed (with optional capabilities enabled where appropriate).

Most of the configuration can be restored from the backup. However, certain attributes that were part of the configuration are not saved or restored automatically. Use the web interface to reconfigure the following attributes:

- Usernames, passwords and roles for the web-based interface.
- Key of Keys
- HTTPS Entropy
- HTTPS Private Key
- HTTPS Public Key Certificate
- HTTP Access Enabled
- HTTPS Access Enabled
- Telnet Access Enabled
- HTTP Port Number
- HTTPS Port Number
- Telnet Port Number
- Encryption Algorithm
- Encryption Key
- SNMP Control Of HTTP And Telnet
- SNMP Control of Passwords

Procedures:

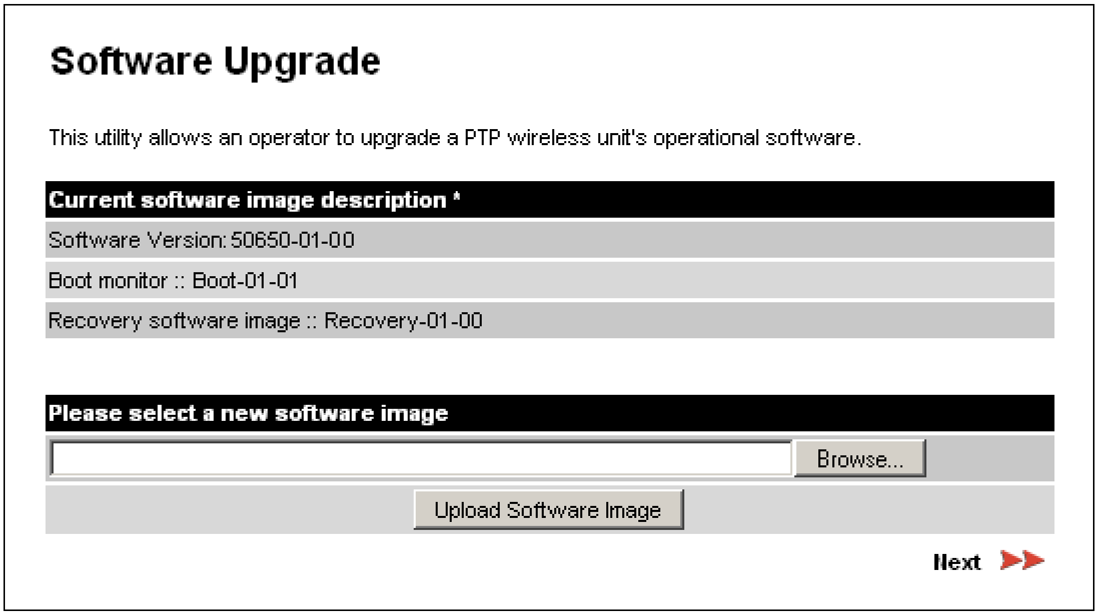
- To save the configuration:
  - Click Save Configuration File.
  - Save the file using the format **MAC-mm-mm-mm_IP-iii-iii-iii-iii.cfg**, where **mm-mm-mm** is MAC address of unit and **iii-iii-iii-iii** is Internet address of unit (IPv4 or IPv6, depending on IP address label).
- To restore the configuration:
  - Click **Browse** and navigate to the PC folder containing the saved configuration file (.cfg).
  - Click **Restore Configuration File and Reboot**.
  - Click **OK** to confirm the restore. The configuration file is uploaded and used to reconfigure the new unit to the same state as the old unit. On completion, the unit reboots.

Software Upgrade page

Menu option: **System > Software Upgrade** (Figure 73).

Use this page to upgrade the unit to a new version of PTP 650 operational software.

Figure 73 Software Upgrade page



Software Upgrade

This utility allows an operator to upgrade a PTP wireless unit's operational software.

Current software image description *

Software Version: 50650-01-00

Boot monitor :: Boot-01-01

Recovery software image :: Recovery-01-00

Please select a new software image

Caution

Ensure that the correct units are upgraded, as units cannot easily be downgraded afterwards.

Caution

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

Caution

If the link is operational, upgrade the remote end of the link first, then upgrade the local end. Otherwise, the remote end may not be accessible.

Preparation:

- Go to the Cambium Support web page (see Contacting Cambium Networks on page 1) and navigate to **Point-to-Point Software and Documentation**, **PTP 650 Series**.
- If the support web page contains a later Software Version than that installed on the PTP 650 unit, perform the procedure below.

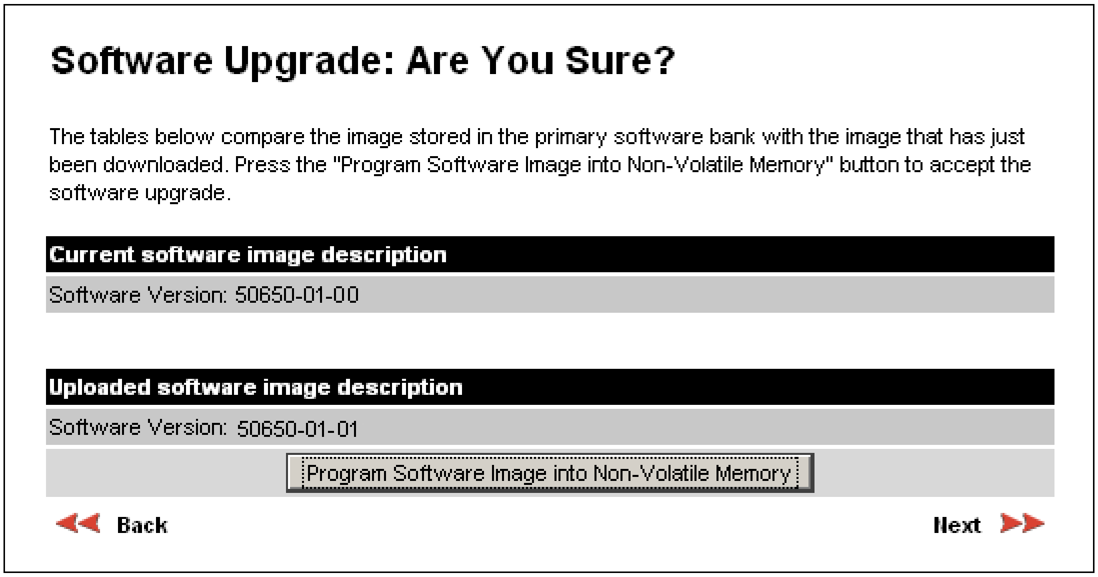
Procedure:

1 Save the system configuration; see Save & Restore Configuration page on page 6-34.

2 On the Cambium Support web page, select the latest PTP 650 software image (dld2 file) and save it to the local management PC.

3 On the Software Upgrade page, click **Browse**. Navigate to the folder containing the downloaded software image and click **Open**.

4 Click **Upload Software Image**. The Software Upgrade Confirmation page is displayed:



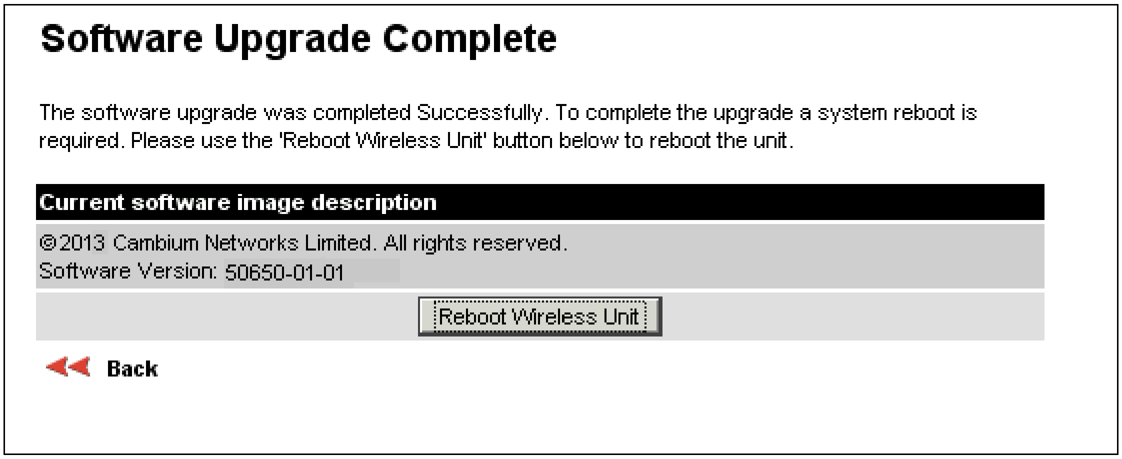
Software Upgrade: Are You Sure?

The tables below compare the image stored in the primary software bank with the image that has just been downloaded. Press the "Program Software Image into Non-Volatile Memory" button to accept the software upgrade.

Current software image description
Software Version: 50650-01-00

Uploaded software image description
Software Version: 50650-01-01

5 Click **Program Software Image into Non-Volatile Memory**. The Progress Tracker page is displayed. On completion, the Software Upgrade Complete page is displayed:



Software Upgrade Complete

The software upgrade was completed Successfully. To complete the upgrade a system reboot is required. Please use the 'Reboot Wireless Unit' button below to reboot the unit.

Current software image description
©2013 Cambium Networks Limited. All rights reserved. Software Version: 50650-01-01

6 Click **Reboot Wireless Unit**, then click **OK** to confirm. The unit reboots with the new software installed.

7 Save the post-upgrade system configuration; see Save & Restore Configuration page on page 6-34.

Management menu

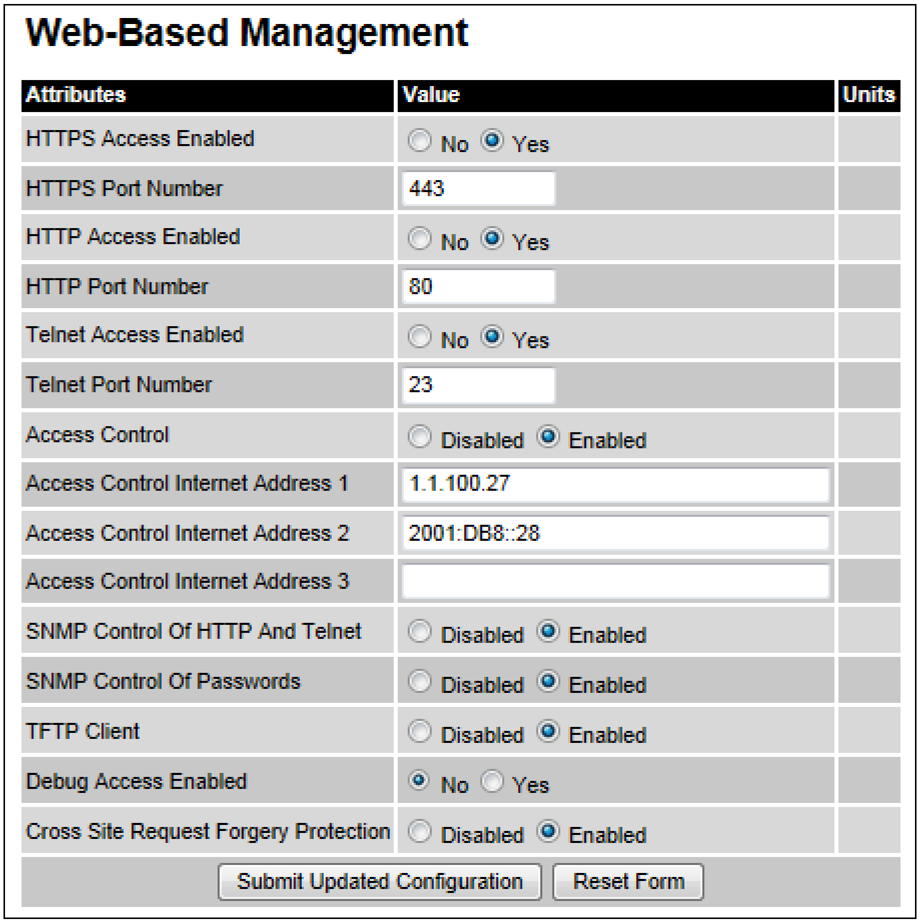
This section describes how to configure web-based management of the PTP 650 unit.

Web-Based Management page

Menu option: **Management > Web** (Figure 74).

Use this page to configure web-based management of the unit.

Figure 74 Web-Based Management page



Web-Based Management

Attributes	Value	Units
HTTPS Access Enabled	○ No ● Yes	
HTTPS Port Number	443	
HTTP Access Enabled	○ No ● Yes	
HTTP Port Number	80	
Telnet Access Enabled	○ No ● Yes	
Telnet Port Number	23	
Access Control	○ Disabled ● Enabled	
Access Control Internet Address 1	1.1.100.27	
Access Control Internet Address 2	2001:DB8::28	
Access Control Internet Address 3		
SNMP Control Of HTTP And Telnet	○ Disabled ● Enabled	
SNMP Control Of Passwords	○ Disabled ● Enabled	
TFTP Client	○ Disabled ● Enabled	
Debug Access Enabled	● No ○ Yes	
Cross Site Request Forgery Protection	○ Disabled ● Enabled	

Caution

If the HTTP, HTTPS, Telnet and SNMP interfaces are all disabled, then it will be necessary to use the Recovery image to reset IP & Ethernet Configuration back to defaults to re-enable the interfaces.

Note

The HTTP and Telnet interfaces should be disabled if the HTTPS interface is configured. (Preparing for HTTPS/TLS page 6-75).

Procedure:

- Review and update the attributes (Table 77).
- To save changes, click **Submit Updated Configuration**.

Table 77 Web-Based Management attributes

Attribute	Meaning
HTTPS Access Enabled	Only displayed when HTTPS is configured. **No:** The unit will not respond to any requests on the HTTPS port. **Yes:** The unit will respond to requests on the HTTPS port.
HTTPS Port Number	Only displayed when HTTPS is configured. The port number for HTTPS access. A value of zero means the wireless unit uses the default port.
HTTP Access Enabled	**No:** The unit will not respond to any requests on the HTTP port. **Yes:** The unit will respond to requests on the HTTP port. Remote management via HTTPS is not affected by this setting.
HTTP Port Number	The port number for HTTP access. A value of zero means the wireless unit uses the default port.
Telnet Access Enabled	**No:** The unit will not respond to any requests on the Telnet port. **Yes:** The unit will respond to requests on the Telnet port.
Telnet Port Number	The port number for Telnet access. A value of zero means the wireless unit uses the default port.
Access Control	Enables or disables access control to web-based management by Internet Address.
Access Control Internet Address 1/2/3	A list of up to three IPv4 or IPv6 Addresses permitted to perform web-based management. Only displayed when Access Control is set to **Enabled**.

Attribute	Meaning
SNMP Control of HTTP And Telnet	**Disabled:** Neither HTTP nor Telnet can be controlled remotely via SNMP. **Enabled:** Both HTTP and Telnet can be controlled remotely via SNMP.
SNMP Control of Passwords	**Enabled:** Passwords for identity-based user accounts in the web-based interface can be updated via SNMP. This option can be used together with SNMPv3 to provide a secure means to update passwords from a central network manager. **Disabled**: Passwords for identity-based user accounts can be updated only via the web-based interface (default).
TFTP Client	**Disabled:** The unit will not respond to any TFTP software download requests. **Enabled:** Software can be downloaded via TFTP, as described in Upgrading software using TFTP on page 6-96.
Debug Access Enabled	**Yes:** Cambium Technical Support is allowed to access the system to investigate faults.
Cross Site Request Forgery Protection	**Enabled:** The system is protected against cross-site request forgery attacks at the web-based interface.

Local User Accounts page

Menu option: **Management > Web > Local User Accounts**.

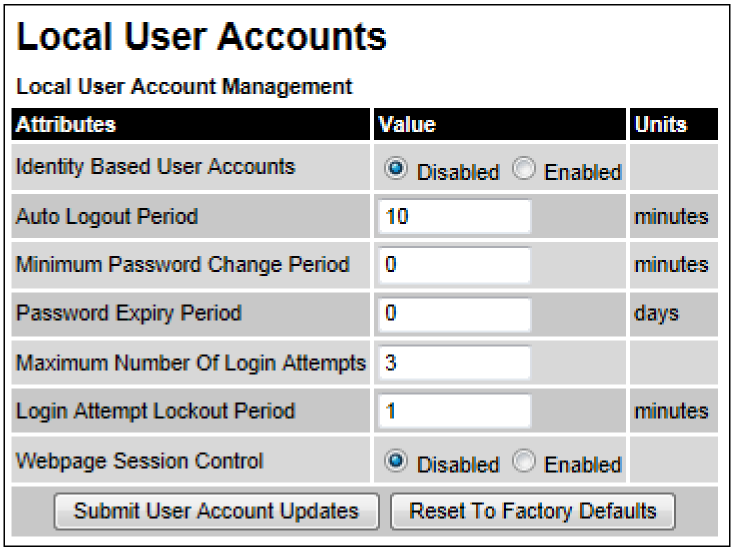
The contents of this page depend upon the setting of Identity Based User Accounts: **Disabled** (Figure 75) or **Enabled** (Figure 76).

Use this page to ensure that user access to the web-based management interface is controlled in accordance with the network operator’s security policy. The Identity Based User Accounts option allows multiple users (from one to ten) to access the unit with one of three levels of access: Security Officer, System Administrator and Read Only. If Identity Based User Accounts are **Enabled**, this procedure may only be performed by a Security Officer.

Note

Local User Account Names, Roles and Passwords are critical security parameters that can be rest from the Zeroize CSPs page (Zeroize CSPs page on page 6-86**).**

Figure 75 Local User Accounts page (Identity Based User Accounts disabled)

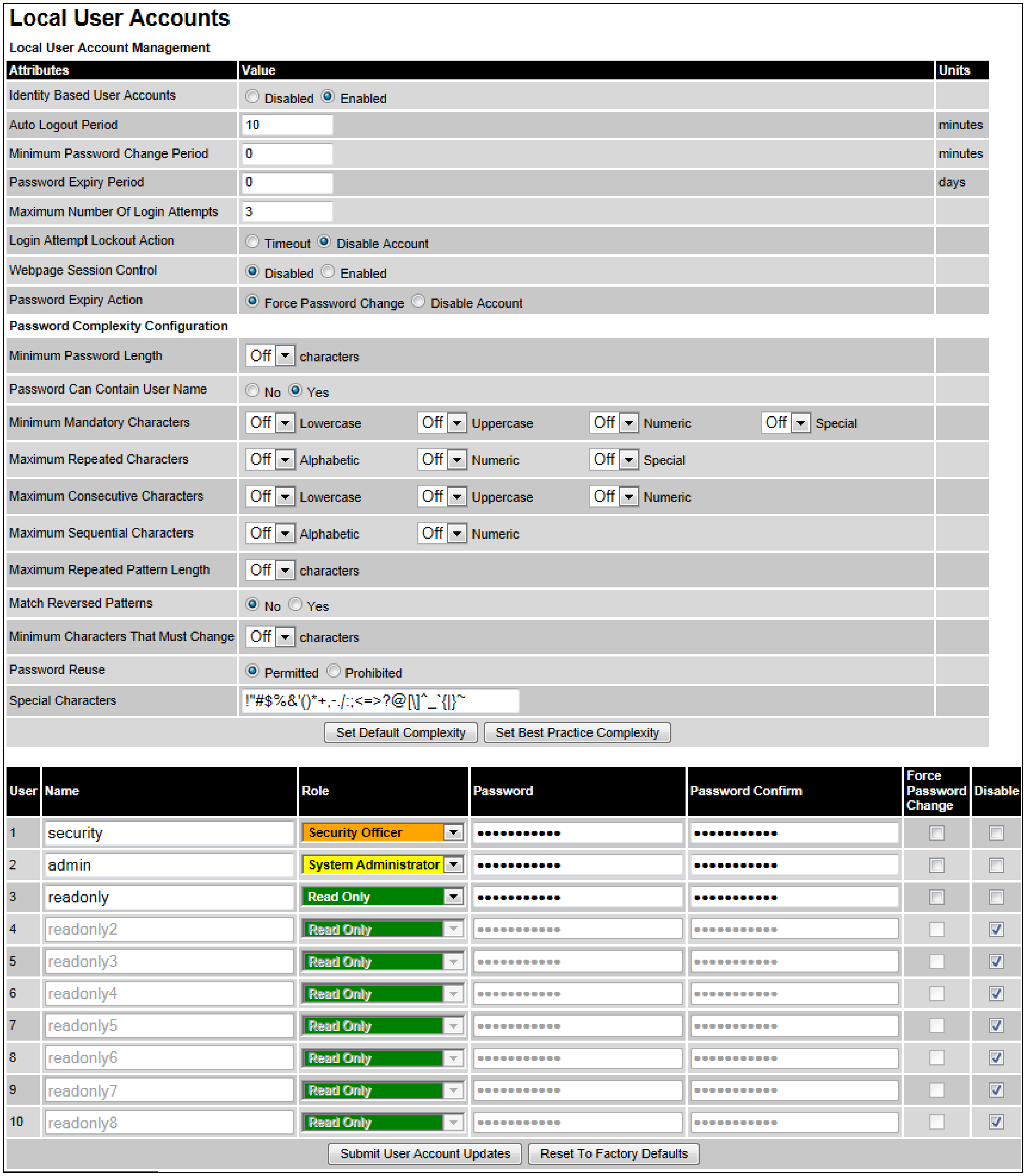


Local User Accounts

Local User Account Management

Attributes	Value	Units
Identity Based User Accounts	● Disabled ○ Enabled	
Auto Logout Period	10	minutes
Minimum Password Change Period	0	minutes
Password Expiry Period	0	days
Maximum Number Of Login Attempts	3	
Login Attempt Lockout Period	1	minutes
Webpage Session Control	● Disabled ○ Enabled	

Figure 76 Local User Accounts page (Identity Based User Accounts enabled)



Local User Accounts

Local User Account Management

Attributes	Value	Units
Identity Based User Accounts	○ Disabled ● Enabled	
Auto Logout Period	10	minutes
Minimum Password Change Period	0	minutes
Password Expiry Period	0	days
Maximum Number Of Login Attempts	3	
Login Attempt Lockout Action	○ Timeout ● Disable Account	
Webpage Session Control	● Disabled ○ Enabled	
Password Expiry Action	● Force Password Change ○ Disable Account	
Password Complexity Configuration		
Minimum Password Length	Off characters	
Password Can Contain User Name	○ No ● Yes	
Minimum Mandatory Characters	Off Lowercase Off Uppercase Off Numeric Off Special	
Maximum Repeated Characters	Off Alphabetic Off Numeric Off Special	
Maximum Consecutive Characters	Off Lowercase Off Uppercase Off Numeric	
Maximum Sequential Characters	Off Alphabetic Off Numeric	
Maximum Repeated Pattern Length	Off characters	
Match Reversed Patterns	● No ○ Yes	
Minimum Characters That Must Change	Off characters	
Password Reuse	● Permitted ○ Prohibited	
Special Characters	!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~	

User	Name	Role	Password	Password Confirm	Force Password Change	Disable
1	security	Security Officer	●●●●●●●●●●●	●●●●●●●●●●●	□	□
2	admin	System Administrator	●●●●●●●●●●●	●●●●●●●●●●●	□	□
3	readonly	Read Only	●●●●●●●●●●●	●●●●●●●●●●●	□	□
4	readonly2	Read Only	●●●●●●●●●●●	●●●●●●●●●●●	□	☑
5	readonly3	Read Only	●●●●●●●●●●●	●●●●●●●●●●●	□	☑
6	readonly4	Read Only	●●●●●●●●●●●	●●●●●●●●●●●	□	☑
7	readonly5	Read Only	●●●●●●●●●●●	●●●●●●●●●●●	□	☑
8	readonly6	Read Only	●●●●●●●●●●●	●●●●●●●●●●●	□	☑
9	readonly7	Read Only	●●●●●●●●●●●	●●●●●●●●●●●	□	☑
10	readonly8	Read Only	●●●●●●●●●●●	●●●●●●●●●●●	□	☑

Procedure:

- Choose whether to set Identity Based User Accounts to **Disabled** or **Enabled**.
- Review and update the Local User Account Management attributes (Table 78).
- If Identity Based User Accounts is set to **Enabled:**
    - Review and update the Password Complexity Configuration attributes (Table 79). To reset all attributes to the best practice values, click **Set Best Practice Complexity**. To return to default values, click **Set Default Complexity.**
    - Review and update up to 10 identity-based user accounts (Table 80).
- If any attributes have been updated, click **Submit User Account Updates**.

Table 78 Local User Account Management attributes

Attribute	Meaning
Identity Based User Accounts	**Disabled**: Access to the web interface is controlled by a single system administration password. **Enabled**: Up to 10 users may access the unit.
Auto Logout Period	The time without user activity that elapses before a user is automatically logged out (minutes). A value of zero disables this feature.
Minimum Password Change Period	The minimum time that elapses before a user is allowed to change a password (minutes). A value of zero disables this feature.
Password Expiry Period	The time that elapses before a password expires (days). A value of zero disables this feature.
Maximum Number of Login Attempts	The maximum number of login attempts (with incorrect password) that are allowed before a user is locked out. Also, the maximum number of password change attempts before a user is locked out.
Login Attempt Lockout Action	Only displayed when Identity Based User Accounts is **Enabled.** **Timeout**: When a user is locked out, the user is allowed to log in again after a specified period. **Disabled**: When a user is locked out, the user is disabled.
Login Attempt Lockout Period	Only displayed when Identity Based User Accounts is **Disabled.** The time that elapses before a locked out user is allowed to log in again (minutes). Only displayed when Login Attempt Lockout Action is set to **Timeout**.
Webpage Session Control	When this is enabled, any attempt to open a new tab or browser instance will force the user to re-enter password.

Attribute	Meaning
Password Expiry Action	Only displayed when Identity Based User Accounts is **Enabled**. The action to be taken by the PTP 650 when a password expires.

Table 79 Password Complexity Configuration attributes

Attribute	Meaning	Best practice
Minimum Password Length	The minimum number of characters required in passwords.	10
Password Can Contain User Name	**No**: Passwords must not contain the user name. **Yes**: Passwords may contain the user name.	No
Minimum Mandatory Characters	The minimum number of lowercase, uppercase, numeric and special characters required in passwords. For example, if all values are set to **2**, then **FredBloggs** will be rejected, but **FredBloggs(25)** will be accepted.	2
Maximum Repeated Characters	The maximum number of consecutive repeated alphabetic, numeric and special characters permitted in passwords. For example, if all values are set to **2**, then **aaa**, **XXX**, **999** and **$$$** will be rejected, but **aa**, **XX**, **99** or **$$** will be accepted.	2
Maximum Consecutive Characters	The maximum number of consecutive lowercase, uppercase and numeric characters permitted in passwords. For example, if all values are set to **5**, then **ALFRED**, **neuman** and **834030** will be rejected.	5
Maximum Sequential Characters	The maximum number of alphabetic and numeric characters permitted in passwords. For example, if set to **3**, then **abcd**, **WXYZ** and **0123** will be rejected, but **abc**, **xyz** and **123** will be accepted.	3
Maximum Repeated Pattern Length	The maximum sequence of characters that can be repeated consecutively in passwords. For example, if set to **3**, then **BlahBlah** and **31st31st** will be rejected, but **TicTicTock** and **GeeGee** will be accepted. **Blah-Blah** will be accepted because the two sequences are not consecutive.	3

Attribute	Meaning	Best practice
Match Reversed Patterns	**No**: Reversed patterns are not checked. **Yes**: Reversed patterns are checked. For example, if Maximum Repeated Pattern Length is set to **3** and Match Reversed Patterns is set to **Yes**, then **AB1221BA** will be rejected.	Yes
Minimum Characters That Must Change	The minimum number of password characters that must change every time a password is updated.	4
Password Reuse	**Permitted**: A user may reuse a previous password. **Prohibited**: A user must not reuse a previous password.	Prohibited
Special Characters	User defined set of special characters used in password construction. The only characters permitted in a password are: (a-z), (A-Z), (0-9) and any of the special characters entered here.	!"%&'()*+,-./:;<=>?

Table 80 Identity-based user accounts attributes

Attribute	Meaning
Name	Enter a user name.
Role	Select a role from the list: **Security Officer, System Administrator** or **Read Only**.
Password	Enter a password for the user. Passwords must comply with the complexity rules (Table 79).
Password Confirm	Retype the password to confirm.
Force Password Change	Force this user to change their password when they next log on.
Disable	Tick the box to disable a user account.

Note

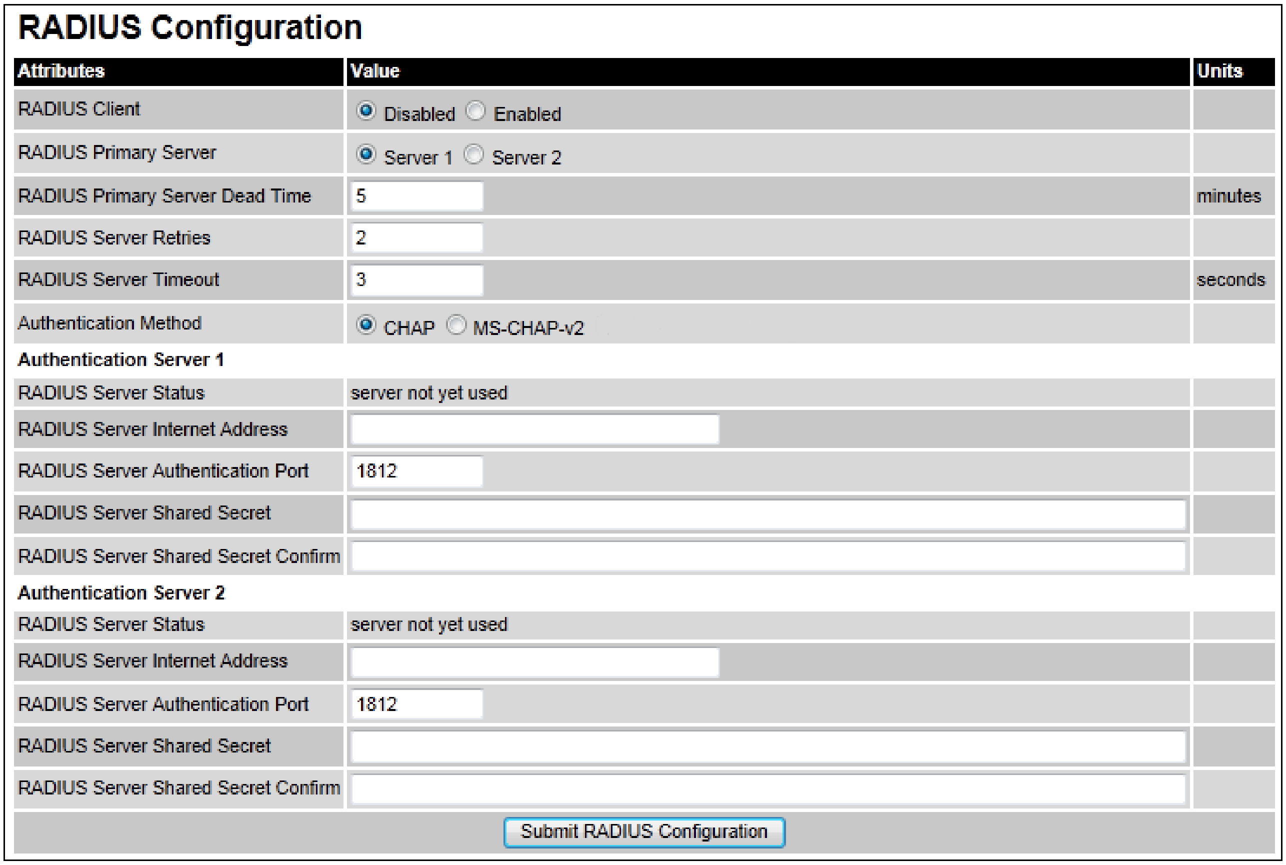
At least one user must be assigned the Security Officer role. If RADIUS is enabled, then this rule is relaxed, in which case the RADIUS server(s) SHOULD be configured with at least one user with **Security Officer** privileges.

RADIUS Configuration page

Menu option: **Management > Web > Radius Configuration** (Figure 77).

Use this page to configure RADIUS authentication. RADIUS authentication is only available when PTP 650 is configured for Identity-based User Accounts and when RADIUS servers are connected to the network.

Figure 77 RADIUS Configuration page



RADIUS Configuration

Attributes	Value	Units
RADIUS Client	● Disabled ○ Enabled	
RADIUS Primary Server	● Server 1 ○ Server 2	
RADIUS Primary Server Dead Time	5	minutes
RADIUS Server Retries	2	
RADIUS Server Timeout	3	seconds
Authentication Method	● CHAP ○ MS-CHAP-v2	
Authentication Server 1		
RADIUS Server Status	server not yet used	
RADIUS Server Internet Address		
RADIUS Server Authentication Port	1812	
RADIUS Server Shared Secret		
RADIUS Server Shared Secret Confirm		
Authentication Server 2		
RADIUS Server Status	server not yet used	
RADIUS Server Internet Address		
RADIUS Server Authentication Port	1812	
RADIUS Server Shared Secret		
RADIUS Server Shared Secret Confirm		

Note

Only users with **Security Officer** role are permitted to configure RADIUS authentication.

Note

When RADIUS is enabled, the Security Officer may disable all user accounts.

Note

At least one user with Security Officer privileges must exist and be enabled, in order to disable the RADIUS client.

Procedure:

- Update the attributes (Table 81).
- Click **Submit RADIUS Configuration**.

Table 81 RADIUS Authentication attributes

Attribute	Meaning
RADIUS Client Enabled	**Enabled:** PTP 650 users may be authenticated via the RADIUS servers. **Disabled**: RADIUS authentication is not used. This may only be selected if at least one user with Security Officer privileges exists.
RADIUS Primary Server	Specifies the primary server, determining the order in which the servers are tried.
RADIUS Primary Server Dead Time	Time (in minutes) to hold off trying to communicate with a previously unavailable RADIUS server. Setting the value to zero disables the timer.
RADIUS Server Retries	Number of times the PTP 650 will retry after a RADIUS server fails to respond to an initial request.
RADIUS Server Timeout	Time (in seconds) the PTP 650 will wait for a response from a RADIUS server.
Authentication Method	Method used by RADIUS to authenticate users.
Authentication Server 1 and 2:	
RADIUS Server Status	The status of the RADIUS server. This contains the time of the last test and an indication of success or failure. If the Authentication Server attributes are incorrect, the displayed status is "`server config not valid`".
RADIUS Server Internet Address	IPv4 or IPv6 address of the RADIUS server.
RADIUS Server Authentication Port	Network port used by RADIUS server for authentication services.
RADIUS Server Shared Secret	Shared secret used in RADIUS server communications. May contain alphabetic, numeric, special characters or spaces, but not extended unicode characters. The maximum length is 127 characters.

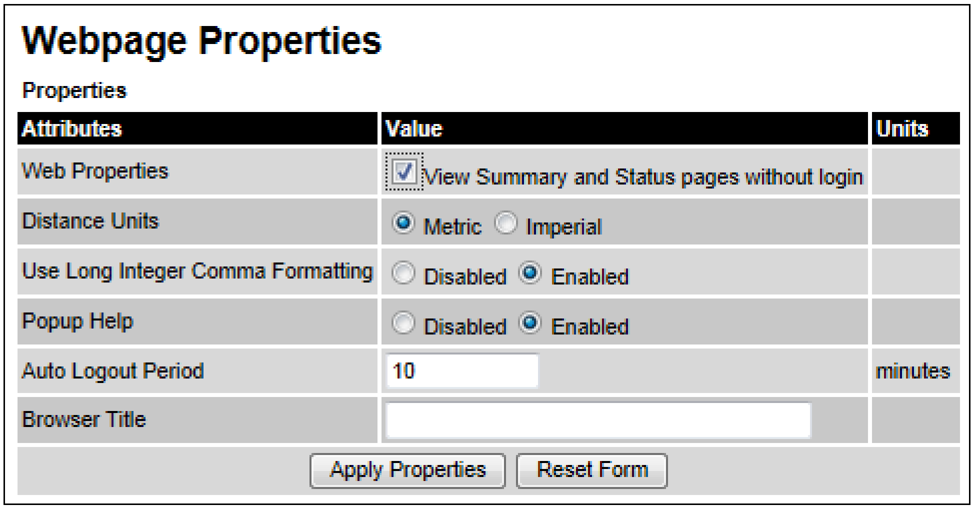
Attribute	Meaning
RADIUS Server Shared Secret Confirm	Shared secret confirmation.

Webpage Properties page

Menu option: **Management > Web > Web Properties** (Figure 78).

Use this page to control the display of the web interface.

Figure 78 Webpage Properties page



Webpage Properties

Properties

Attributes	Value	Units
Web Properties	☑ View Summary and Status pages without login	
Distance Units	● Metric ○ Imperial	
Use Long Integer Comma Formatting	○ Disabled ● Enabled	
Popup Help	○ Disabled ● Enabled	
Auto Logout Period	10	minutes
Browser Title		

Procedure:

- Update the attributes (Table 82).
- Click Apply Properties.

Table 82 Webpage Properties attributes

Attribute	Meaning
Web Properties	**View Summary and Status pages without login**: • If ticked (the default setting), users can view the Summary and Status web pages without entering a password. • If not ticked, users must enter a password before viewing the Summary and Status pages. This is only effective if the System Administration Password has been set, see Change Password page on page 7-10.
Distance Units	**Metric:** Distances are displayed in kilometers or meters. **Imperial:** Distances are displayed in miles or feet.
Use Long Integer Comma Formatting	**Disabled:** Long integers are displayed thus: 1234567. **Enabled:** Long integers are displayed thus: 1,234,567.
Popup Help	**Disabled:** Web page popup help is not displayed. **Enabled:** Web page popup help is displayed.
Send HTTPS Close Notify Alerts	Only displayed when HTTPS is configured. Controls whether or not the HTTPS server sends TLS Close Notify Alerts before it shuts down each socket. **Disabled**: TLS Close Notify Alerts are not sent before closing each socket. This is the default because these alerts can cause problems with some browsers (e.g. Internet Explorer) **Enabled**: TLS Close Notify Alerts are sent before closing each socket.
Auto Logout Period	Only displayed if role-based user accounts are in use. Automatic logout period in minutes. If there is no user activity within this time, the user is required to log in again. Think this is only displayed when not using identity based user accounts.
Browser Title	By default, the PTP 650 web interface displays the following text in web browser tab titles: **`Cambium PTP 50650 - <current page> (IP=<ipAddress>)`** To change the default text, enter simple text and optional variables (prefixed with a $ character). The full list of variables is in Table 83.

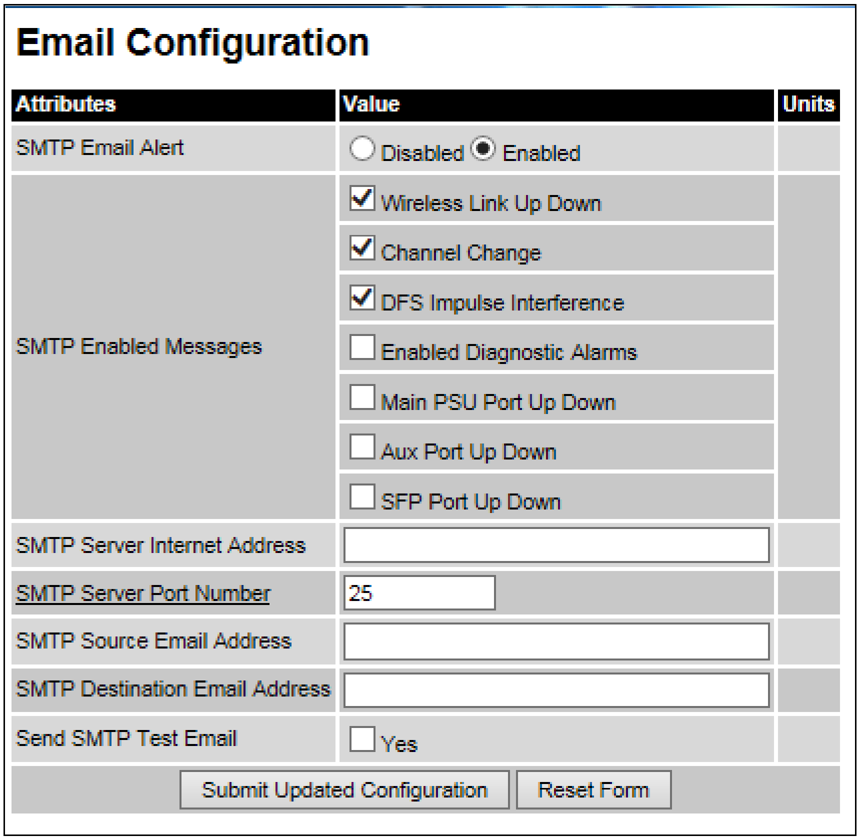
Table 83 Browser Title attribute variables

Variable	Meaning
$siteName	Site Name, as set in the System Configuration page (Table 71).
$linkName	Link Name, as set in the System Configuration page (Table 71).
$masterSlaveMode	Master Slave Mode, as set in the Step 2: Wireless Configuration page (Table 70).
$ipAddress	IP Address currently used to identify the ODU, either IPv4 or IPv6 Address, depending upon the setting of IP Address Label in the System Configuration page (Table 71): • **IPv4**: $ipAddress = $ipv4Address • **IPv6**: $ipAddress = $ipv6Address (if not blank) or $ipv6LinkLocalAddress
$ipv4Address	IPv4 Address of the ODU, as set in the LAN Configuration page (Table 72).
$ipv6Address	IPv6 Address of the ODU, as set in the LAN Configuration page (Table 72).
$ipv6LinkLocalAddress	IPv6 Auto Configured Link Local Address of the ODU. This cannot be updated, but it can be viewed in the LAN Configuration page (Table 72).
$sysName	Sys Name for this SNMP managed node, as set in the Step 2: SNMP MIB-II System Objects page (Table 89).
$productName	The product variant, for example **Cambium PTP50650**. Not updateable.
$pageName	Name of the page currently being browsed.

Email Configuration page

Menu option: **Management** > **Email** (Figure 79). Use this page to enable the PTP 650 to generate Simple Mail Transfer Protocol (SMTP) email messages to notify the system administrator when certain events occur.

Figure 79 Email Configuration page



Email Configuration

Attributes	Value	Units
SMTP Email Alert	○ Disabled ● Enabled	
SMTP Enabled Messages	☑ Wireless Link Up Down ☑ Channel Change ☑ DFS Impulse Interference ☐ Enabled Diagnostic Alarms ☐ Main PSU Port Up Down ☐ Aux Port Up Down ☐ SFP Port Up Down	
SMTP Server Internet Address		
SMTP Server Port Number	25	
SMTP Source Email Address		
SMTP Destination Email Address		
Send SMTP Test Email	☐ Yes	

Procedure:

- Update the attributes (Table 84).
- Click **Submit Updated Configuration**. The Configuration Change Reboot dialog is displayed.
- Click **Reboot Wireless Unit** and click **OK**. The reboot progress message is displayed. On completion, the unit restarts.

Table 84 Email Configuration attributes

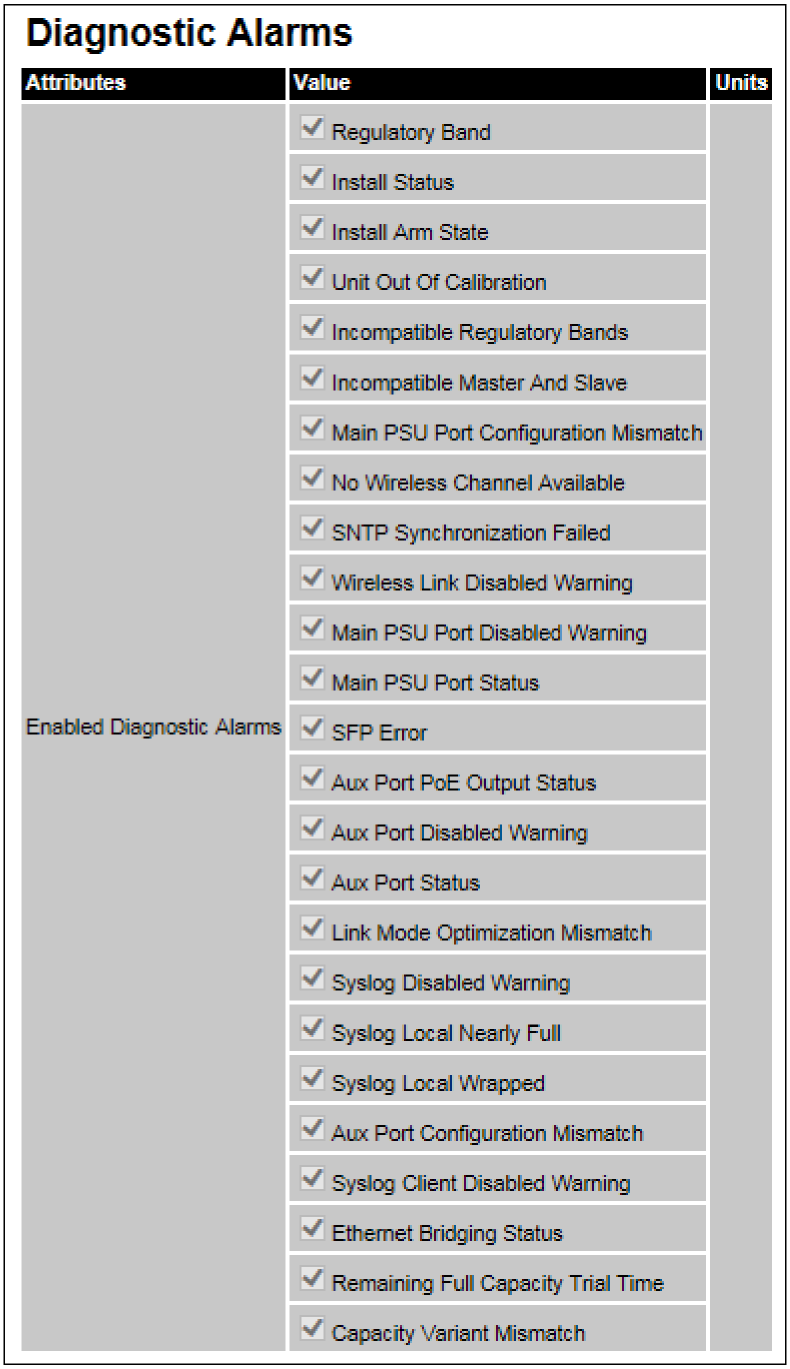
Attribute	Meaning
SMTP Email Alert	Controls the activation of the SMTP client.
SMTP Enabled Messages	The SMTP Enabled Messages attribute controls which email alerts the unit will send.
SMTP Server Internet Address	The IPv4 or IPv6 Address of the networked SMTP server.
SMTP Server Port Number	The SMTP Port Number is the port number used by the networked SMTP server. By convention the default value for the port number is 25.
SMTP Source Email Address	The email address used by the PTP 650 Series to log into the SMTP server. This must be a valid email address that will be accepted by your SMTP Server.
SMTP Destination Email Address	The email address to which the PTP 650 Series will send the alert messages.
Send SMTP Test Email	Generate and send an email in order to test the SMTP settings. The tick box will self-clear when **Submit** is clicked.

Diagnostic Alarms page

Menu option: **Management** > **Diagnostic Alarms** (Figure 80).

Use this page to select which diagnostic alarms will be notified to the system administrator.

Figure 80 Diagnostic Alarms page



Diagnostic Alarms

Attributes	Value	Units
Enabled Diagnostic Alarms	☑ Regulatory Band	
	☑ Install Status	
	☑ Install Arm State	
	☑ Unit Out Of Calibration	
	☑ Incompatible Regulatory Bands	
	☑ Incompatible Master And Slave	
	☑ Main PSU Port Configuration Mismatch	
	☑ No Wireless Channel Available	
	☑ SNTP Synchronization Failed	
	☑ Wireless Link Disabled Warning	
	☑ Main PSU Port Disabled Warning	
	☑ Main PSU Port Status	
	☑ SFP Error	
	☑ Aux Port PoE Output Status	
	☑ Aux Port Disabled Warning	
	☑ Aux Port Status	
	☑ Link Mode Optimization Mismatch	
	☑ Syslog Disabled Warning	
	☑ Syslog Local Nearly Full	
	☑ Syslog Local Wrapped	
	☑ Aux Port Configuration Mismatch	
	☑ Syslog Client Disabled Warning	
	☑ Ethernet Bridging Status	
	☑ Remaining Full Capacity Trial Time	
	☑ Capacity Variant Mismatch	

Procedure:

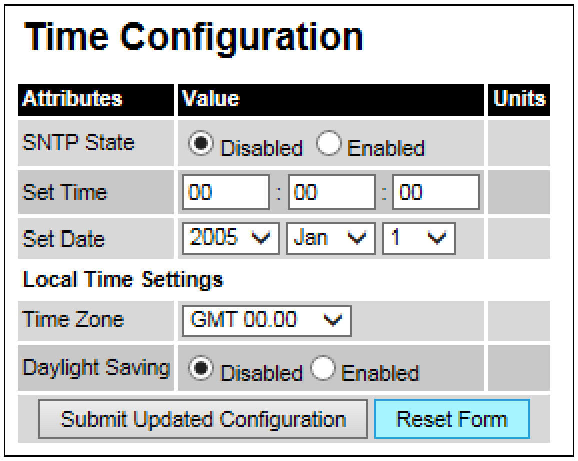
- Tick the required alarms. These alarms are described in Alarms on page 7-12.
- Click **Submit Updated Configuration**.

Time Configuration page

Menu option: **Management > Time** (Figure 81 and Figure 82)

Use this page to set the real-time clock of the PTP 650.

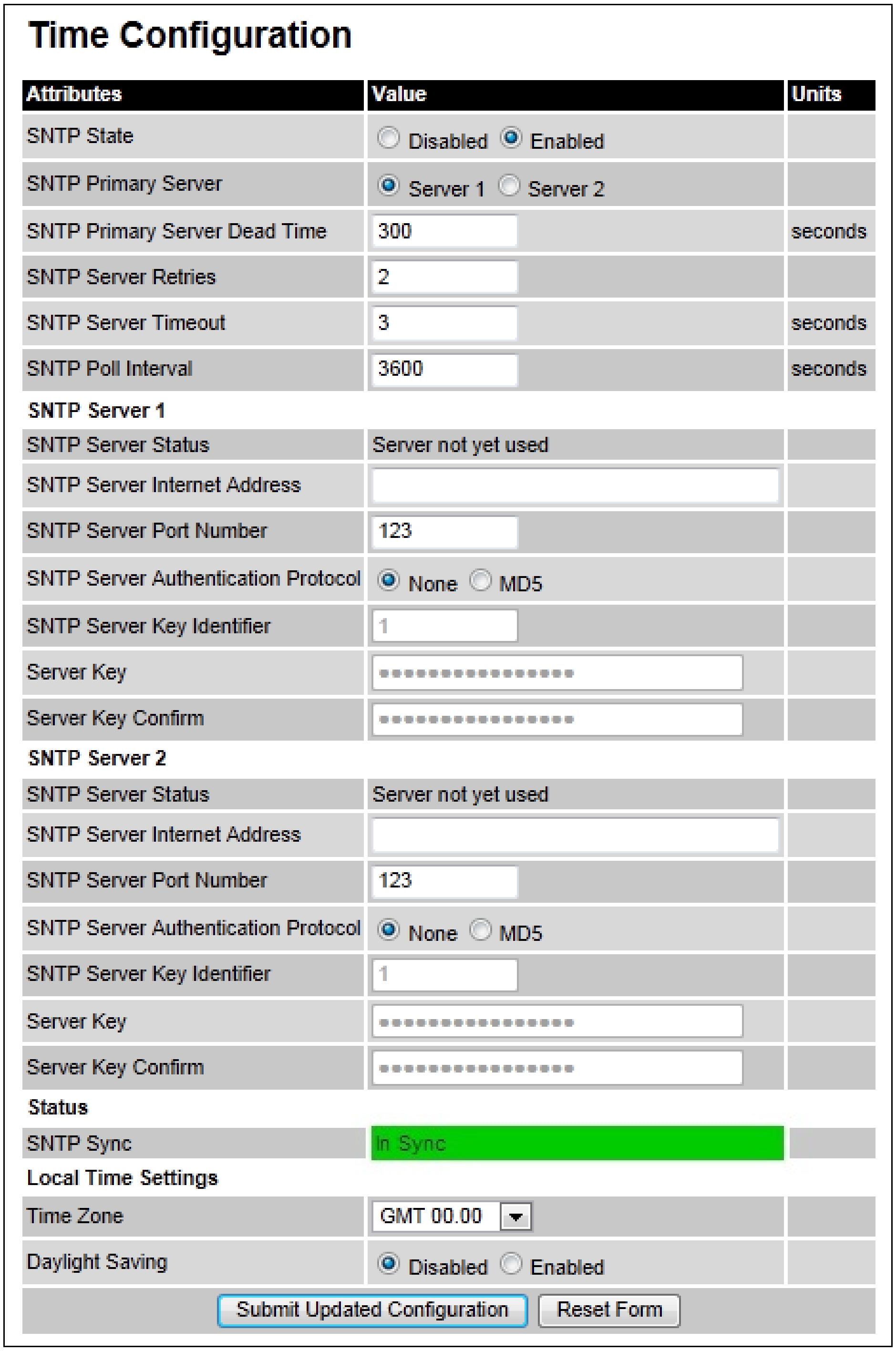
Figure 81 Time Configuration page (SNTP disabled)



Time Configuration

Attributes	Value	Units
SNTP State	● Disabled ○ Enabled	
Set Time	00 : 00 : 00	
Set Date	2005 Jan 1	
Local Time Settings		
Time Zone	GMT 00.00	
Daylight Saving	● Disabled ○ Enabled	

Figure 82 Time Configuration page (SNTP enabled)



Time Configuration

Attributes	Value	Units
SNTP State	○ Disabled ● Enabled	
SNTP Primary Server	● Server 1 ○ Server 2	
SNTP Primary Server Dead Time	300	seconds
SNTP Server Retries	2	
SNTP Server Timeout	3	seconds
SNTP Poll Interval	3600	seconds
SNTP Server 1		
SNTP Server Status	Server not yet used	
SNTP Server Internet Address		
SNTP Server Port Number	123	
SNTP Server Authentication Protocol	● None ○ MD5	
SNTP Server Key Identifier	1	
Server Key	••••••••••••••••	
Server Key Confirm	••••••••••••••••	
SNTP Server 2		
SNTP Server Status	Server not yet used	
SNTP Server Internet Address		
SNTP Server Port Number	123	
SNTP Server Authentication Protocol	● None ○ MD5	
SNTP Server Key Identifier	1	
Server Key	••••••••••••••••	
Server Key Confirm	••••••••••••••••	
Status		
SNTP Sync	In Sync	
Local Time Settings		
Time Zone	GMT 00.00	
Daylight Saving	● Disabled ○ Enabled	

Setting the real-time clock manually

Use this procedure to keep time without connecting to a networked time server.

Note

If SNTP is disabled, it will be necessary to reset the time manually after each system reboot.

Procedure:

- Set SNTP State to **Disabled**.
- Review and update the manual clock attributes (Table 85).
- Click **Submit Updated Configuration**.

Table 85 Manual clock attributes

Attribute	Meaning
SNTP State	**Disabled:** the PTP 650 will keep time without connecting to a networked time server.
Set Time	Set hours, minutes and seconds.
Set Date	Set year, month and day.
Time Zone	Set the time zone offset from Greenwich Mean Time (GMT). To set the clock to UTC time, set Time Zone to **GMT 00.00**.
Daylight Saving	**Disabled:** There is no offset for daylight saving time. **Enabled:** System clock is moved forward one hour to adjust for daylight saving time. To set the clock to UTC time, set Daylight Saving to **Disabled**.

Setting the real-time clock to synchronize using SNTP

Use this procedure to synchronize the unit with a networked time server:

Procedure:

- Set the SNTP State attribute to **Enabled**.
- Review and update the SNTP clock attributes (Table 86).
- Click **Submit Updated Configuration**.

Table 86 SNTP clock attributes

Attribute	Meaning
SNTP State	**Enabled:** the ODU will obtain accurate date and time updates from a networked time server.
SNTP Primary Server	Specifies the primary SNTP server, determining the order in which the servers are tried.
SNTP Primary Server Dead Time	Time (in seconds) to wait before retrying communications with an unresponsive primary SNTP server. Setting the value to zero disables the timer.
SNTP Server Retries	Number of times the PTP will retry after an SNTP server fails to respond.
SNTP Server Timeout	Time (in seconds) the PTP will wait for a response from an SNTP server.
SNTP Poll Interval	The SNTP server polling interval.
SNTP Server 1 and 2:	
SNTP Server Status	Status message reflecting the state of communications with the SNTP server.
SNTP Server Internet Address	The IPv4 or IPv6 Address of the networked SNTP server.
SNTP Server Port Number	The port number of the networked SNTP server. By convention the default value for the port number is 123.
SNTP Server Authentication Protocol	Authentication protocol to be used with this SNTP server (**None** or **MD5**).
SNTP Server Key Identifier	SNTP key identifier. A key of zeros is reserved for testing.
Server Key	Key used to authenticate SNTP communications.
Server Key Confirm	Must match the Server Key.
Status:	
SNTP Sync	This shows the current status of SNTP synchronization. If **No Sync** is displayed, then review the SNTP Server Internet Address and Port Number. A change of state may generate an SNMP trap or SMTP email alert.
SNTP Last Sync	This shows the date and time of the last SNTP synchronization.

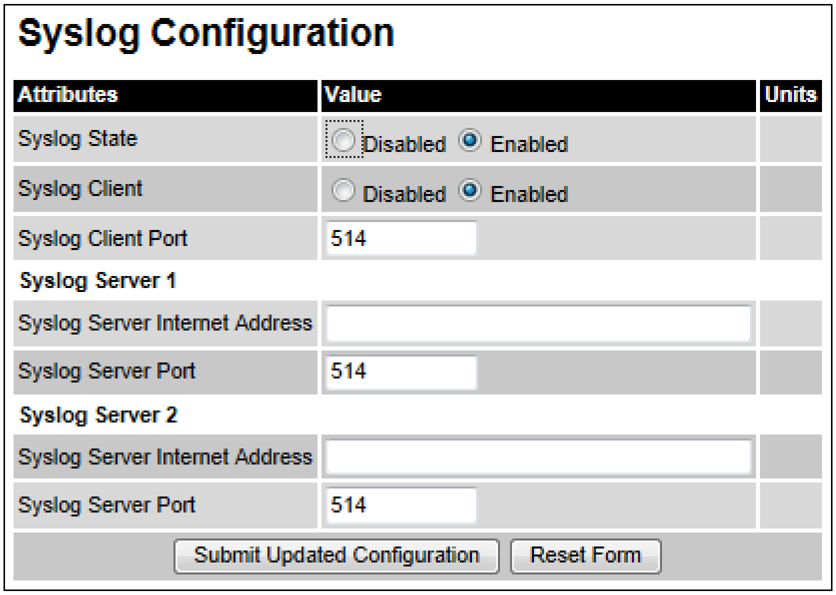
Attribute	Meaning
System Clock	This displays the local time, allowing for the Time Zone and Daylight Saving settings.
Local Time Settings:	
Time Zone	Set the time zone offset from Greenwich Mean Time (GMT). To set the clock to UTC time, set Time Zone to **GMT 00.00**.
Daylight Saving	**Disabled:** Daylight saving adjustments will not be applied to the time. **Enabled:** Daylight saving adjustments will be applied to the time, according to local rules. To set the clock to UTC time, set Daylight Saving to **Disabled**.

Syslog Configuration page

Menu option: **Management** > **Syslog** > **Syslog configuration** (Figure 83).

Use this page to configure system logging. Only users with **Security Officer** role are permitted to configure the syslog client.

Figure 83 Syslog Configuration page



Syslog Configuration

Attributes	Value	Units
Syslog State	○ Disabled ● Enabled	
Syslog Client	○ Disabled ● Enabled	
Syslog Client Port	514	
Syslog Server 1		
Syslog Server Internet Address		
Syslog Server Port	514	
Syslog Server 2		
Syslog Server Internet Address		
Syslog Server Port	514	

Note

To record Coordinated Universal Time (UTC time) in syslog messages, use the Time Configuration page to set Time Zone to **GMT 00.00** and Daylight Saving to **Disabled** (Time Configuration page on page 6-55).

Procedure:

- Update the attributes (Table 87).
- Click **Submit Updated Configuration**.

Table 87 Syslog Configuration attributes

Attribute	Meaning
Syslog State	When system logging is enabled, log entries are added to the internal log and (optionally) transmitted as UDP messages to one or two syslog servers.
Syslog Client	**Enabled:** Event messages are logged. **Disabled:** Event messages are not logged.
Syslog Client Port	The client port from which syslog messages are sent.
Syslog Server 1 and 2:	
Syslog Server Internet Address	The IPv4 or IPv6 Address of the syslog server. Delete the IP address to disable logging on the syslog server.
Syslog Server Port	The server port at which syslog messages are received.

SNMP pages (for SNMPv3)

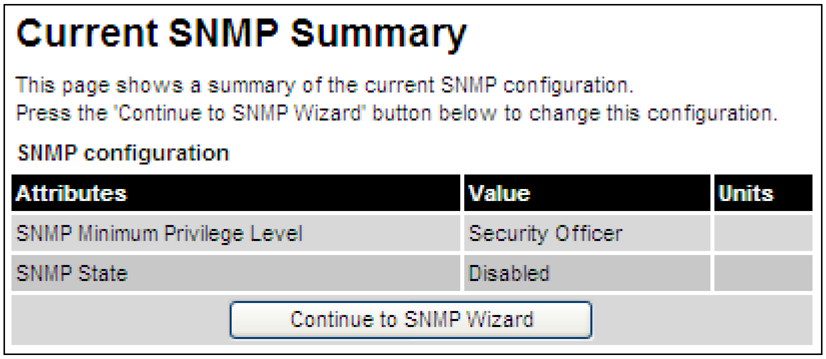
This section describes how to configure Simple Network Management Protocol version 3 (SNMPv3) traps using the SNMP Wizard.

Current SNMP Summary (for SNMPv3)

Menu option: **Management > SNMP** (Figure 84).

Use this page to review the current SNMP configuration and start the SNMP Wizard.

Figure 84 Current SNMP Summary page (when SNMP is disabled)



Current SNMP Summary

This page shows a summary of the current SNMP configuration.
Press the 'Continue to SNMP Wizard' button below to change this configuration.

SNMP configuration

Attributes	Value	Units
SNMP Minimum Privilege Level	Security Officer	
SNMP State	Disabled	

Procedure:

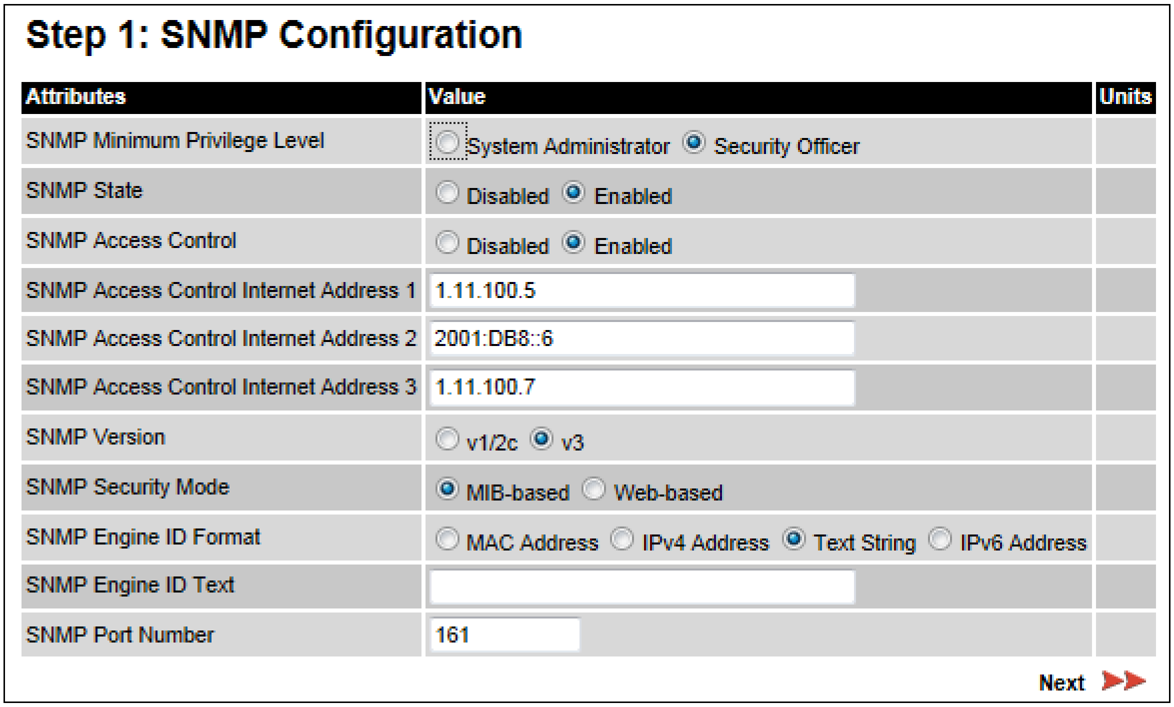
- Review the summary.
- If any updates are required, click **Continue to SNMP Wizard**.

Step 1: SNMP Configuration (for SNMPv3)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 85).

Use this page to enable SNMP, select SNMPv3 and configure access to the SNMP server.

Figure 85 Step 1: SNMP Configuration page (for SNMPv3)



Step 1: SNMP Configuration

Attributes	Value	Units
SNMP Minimum Privilege Level	○ System Administrator ● Security Officer	
SNMP State	○ Disabled ● Enabled	
SNMP Access Control	○ Disabled ● Enabled	
SNMP Access Control Internet Address 1	1.11.100.5	
SNMP Access Control Internet Address 2	2001:DB8::6	
SNMP Access Control Internet Address 3	1.11.100.7	
SNMP Version	○ v1/2c ● v3	
SNMP Security Mode	● MIB-based ○ Web-based	
SNMP Engine ID Format	○ MAC Address ○ IPv4 Address ● Text String ○ IPv6 Address	
SNMP Engine ID Text		
SNMP Port Number	161	

Procedure:

- Set SNMP State to **Enabled**.
- Set SNMP Version to **v3**. The page is redisplayed with SNMPv3 attributes.
- Update the attributes (Table 88).
- Click **Next**.

Table 88 Step 1: SNMP Configuration attributes (for SNMPv3)

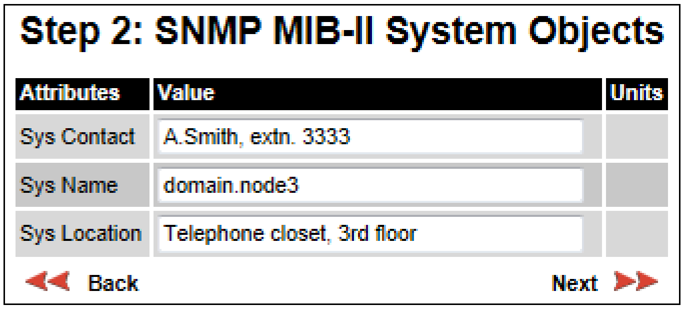
Attribute	Meaning
SNMP Minimum Privilege Level	Minimum security level which is permitted to administer SNMP security settings. Only displayed when Identity Based User Accounts are **Enabled** on the User Accounts page (Table 78).
SNMP State	Enables or disables SNMP.
SNMP Access Control	Enables or disables access control to SNMP management by IP address.
SNMP Access Control Internet Address 1/2/3	A list of up to three IPv4 or IPv6 Addresses permitted to perform SNMP management. Only displayed when SNMP Access Control is set to **Enabled**.
SNMP Version	SNMP protocol version: **v1/2c** or **v3**.
SNMP Security Mode	**MIB-based**: SNMPv3 security parameters are managed via SNMP MIBs. **Web-based**: SNMPv3 security parameters are not available over SNMP, but instead are configured using the SNMP Accounts page, as described in Step 3: SNMP User Policy Configuration (for SNMPv3) on page 6-65.
SNMP Engine ID Format	Specifies whether the Engine ID is generated from the **MAC Address**, **IP4 Address**, **Text String** or **IPv6 Address**.
SNMP Engine ID Text	Only enabled when SNMP Engine ID Format is set to **Text String**. Text used to generate the SNMP Engine ID.
SNMP Port Number	The port that the SNMP agent is listening to for commands from a management system.

Step 2: SNMP MIB-II System Objects (for SNMPv3)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 86).

Use this page to enter details of the SNMP managed node.

Figure 86 Step 2: SNMP MIB-II System Objects page (for SNMPv3)



Step 2: SNMP MIB-II System Objects

Attributes	Value	Units
Sys Contact	A.Smith, extn. 3333	
Sys Name	domain.node3	
Sys Location	Telephone closet, 3rd floor	

Procedure:

- Update the attributes (Table 89).
- Click **Next.**
- The next step depends upon which SNMP Security Mode was selected in the Step 1: SNMP Configuration page:
  - If **Web-based**, go to Step 3: SNMP User Policy Configuration (for SNMPv3) on page 6-65.
  - If **MIB-based**, go to Confirm SNMP Configuration (for SNMPv3) on page 6-70.

Table 89 Step 2: SNMP MIB-II System Objects attributes (for SNMPv3)

Attribute	Meaning
Sys Contact	The name of the contact person for this managed node, together with information on how to contact this person.
Sys Name	An administratively-assigned name for this managed node. By convention, this is the fully qualified domain name of the node.
Sys Location	The physical location of this node, for example **Telephone closet, 3rd floor**.

Step 3: SNMP User Policy Configuration (for SNMPv3)

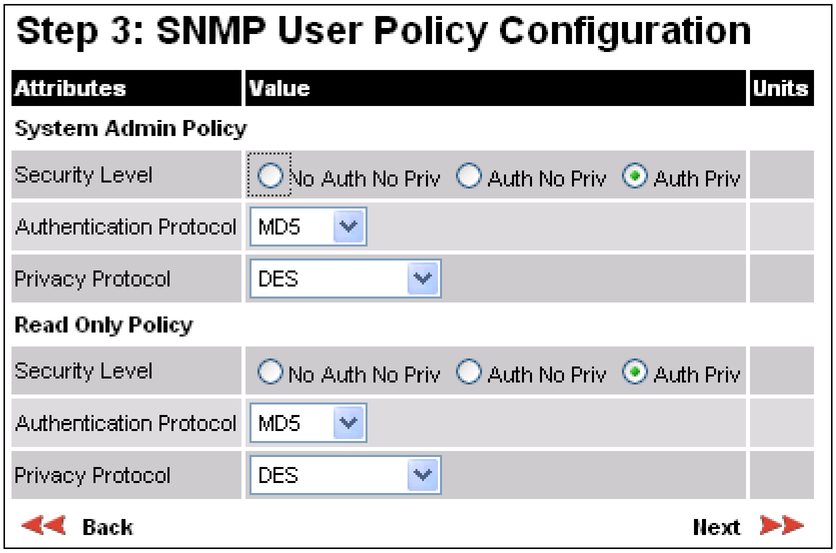
Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 87).

This page is only displayed when SNMP Security Mode is set to **Web-based** in the Step 1: SNMP Configuration page. Use this page to configure which authentication and privacy protocols are required for SNMP users with roles **System administrator** and **Read only**.

Procedure:

- Update the attributes (Table 90).
- Click **Next**.

Figure 87 Step 3: SNMP User Policy Configuration page (for SNMPv3)



Step 3: SNMP User Policy Configuration

Attributes	Value	Units
System Admin Policy		
Security Level	○ No Auth No Priv ○ Auth No Priv ● Auth Priv	
Authentication Protocol	MD5	
Privacy Protocol	DES	
Read Only Policy		
Security Level	○ No Auth No Priv ○ Auth No Priv ● Auth Priv	
Authentication Protocol	MD5	
Privacy Protocol	DES	

Table 90 Step 3: SNMP User Policy Configuration attributes (for SNMPv3)

Attribute	Meaning
Security Level	Defines the security level and associated protocols that are required to allow SNMP users to access the PTP 650. **No Auth No Priv**: Users are not required to use authentication or privacy protocols. **Auth No Priv**: Users are required to use only authentication protocols. **Auth Priv**: Users are required to use both authentication and privacy protocols.

Attribute	Meaning
Authentication Protocol	The authentication protocol to be used to access the PTP 650 via SNMP. This is disabled when Security Level is set to **Auth No Priv**. **MD5**: Message Digest Algorithm is used. **SHA**: NIST FIPS 180-1, Secure Hash Algorithm SHA-1 is used.
Privacy Protocol	The privacy protocol to be used to access the PTP 650 via SNMP. This is disabled when Security Level is set to **No Auth No Priv** or **Auth No Priv**. **DES**: Data Encryption Standard (DES) symmetric encryption protocol. **AES**: Advanced Encryption Standard (AES) cipher algorithm.

Note

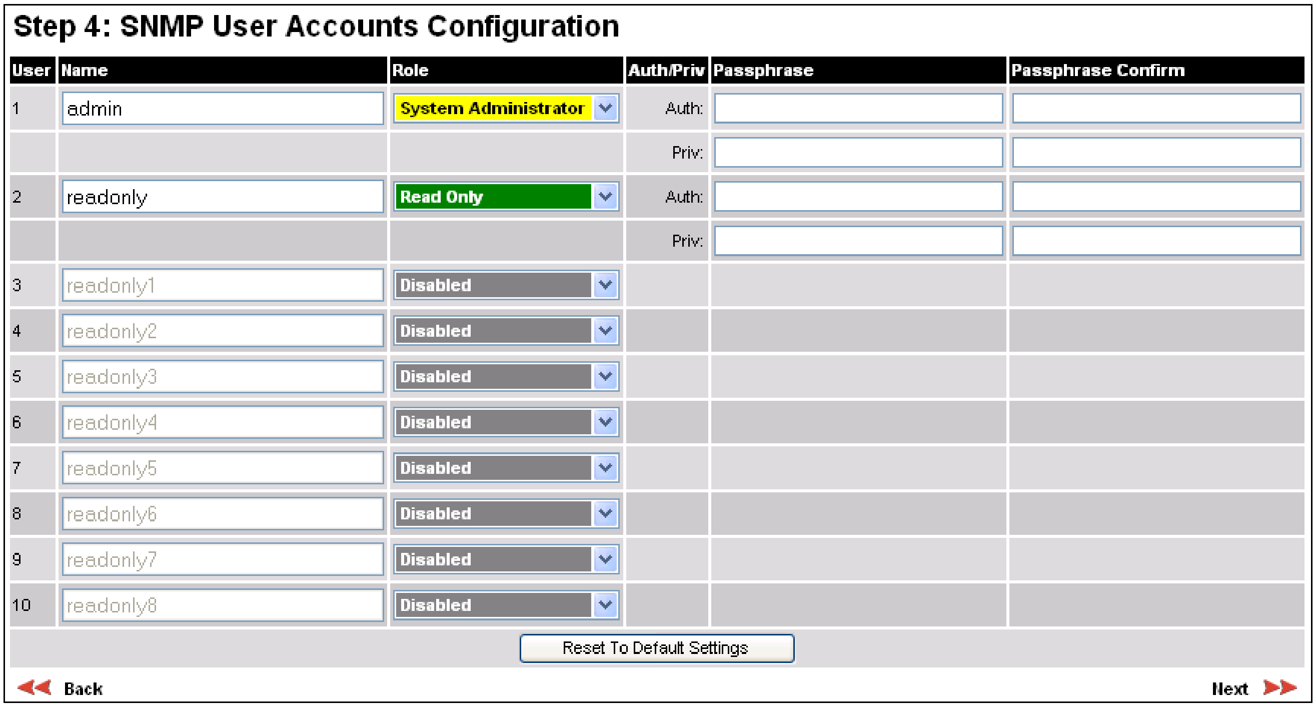
A user configured to use AES privacy protocol will not be able to transmit and receive encrypted messages unless the license key enables the AES capability.

Step 4: SNMP User Accounts Configuration (for SNMPv3)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 88).

This page is only displayed when SNMP Security Mode is set to **Web-based** in the Step 1: SNMP Configuration page. Use this page to update the SNMP user accounts.

Figure 88 Step 4: SNMP User Accounts Configuration page (for SNMPv3)



Step 4: SNMP User Accounts Configuration

User	Name	Role	Auth/Priv	Passphrase	Passphrase Confirm
1	admin	System Administrator	Auth:		
			Priv:		
2	readonly	Read Only	Auth:		
			Priv:		
3	readonly1	Disabled			
4	readonly2	Disabled			
5	readonly3	Disabled			
6	readonly4	Disabled			
7	readonly5	Disabled			
8	readonly6	Disabled			
9	readonly7	Disabled			
10	readonly8	Disabled			

Procedure:

- Update the individual user attributes (Table 91) for up to 10 SNMP users.
- Click **Next**.

Table 91 Step 4: SNMP User Accounts Configuration attributes (for SNMPv3)

Attribute	Meaning
Name	Name to be used by the SNMP user to access the system.
Role	Selects which of the two web-based security profiles are applied to this user: **System administrator** or **Read only**. Select **Disabled** to disable the SNMP account.
Auth/Priv	Indicates whether the Passphrase applies to authentication or privacy protocols.

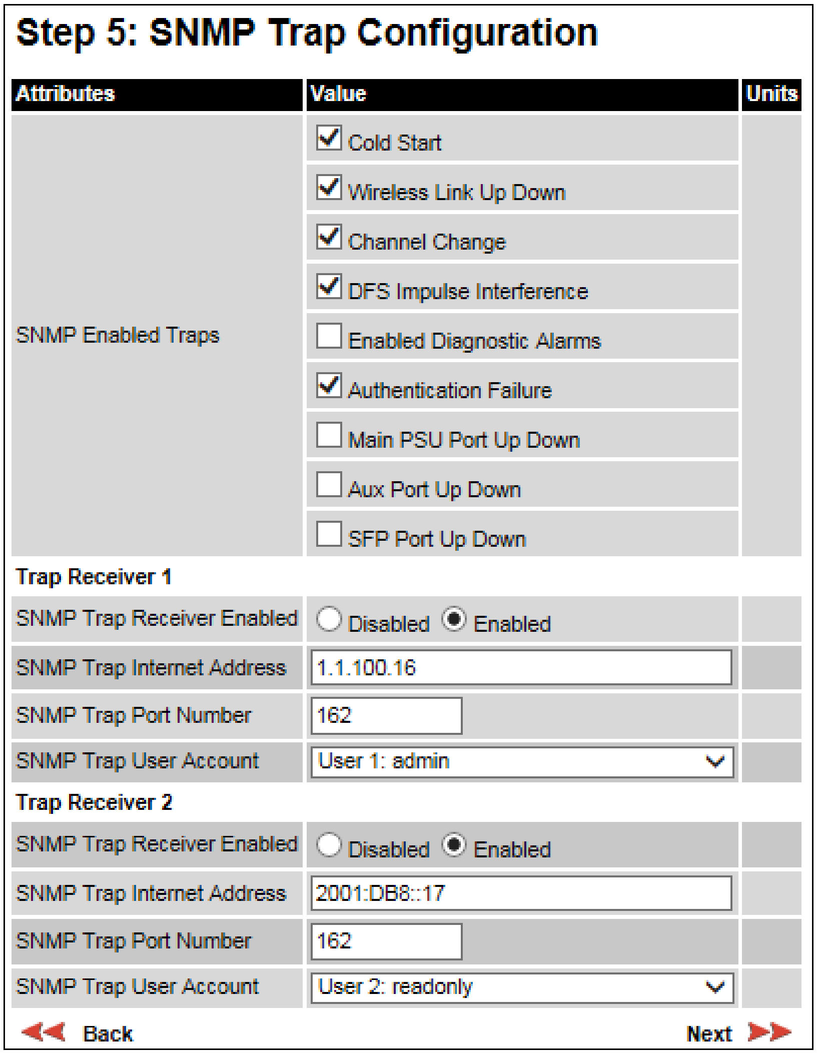
Attribute	Meaning
Passphrase	The phrase to be entered by this SNMP user to access the system using an authentication or privacy protocol. Length must be between 8 and 32 characters. May contain spaces. The Auth Passphrase is hidden when Security Level for this user's Role is set to **No Auth No Priv**. The Priv Passphrase is hidden when Security Level for this user's Role is set to **No Auth No Priv** or **Auth No Priv**.
Passphrase Confirm	Passphrase must be reentered to confirm it has been correctly typed.

Step 5: SNMP Trap Configuration (for SNMPv3)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 89).

This page is only displayed when SNMP Security Mode is set to **Web-based** in the Step 1: SNMP Configuration page. Use this page to configure the events that will generate SNMP traps and to set up trap receivers.

Figure 89 Step 5: SNMP Trap Configuration page (for SNMPv3)



Step 5: SNMP Trap Configuration

Attributes	Value	Units
SNMP Enabled Traps	☑ Cold Start ☑ Wireless Link Up Down ☑ Channel Change ☑ DFS Impulse Interference ☐ Enabled Diagnostic Alarms ☑ Authentication Failure ☐ Main PSU Port Up Down ☐ Aux Port Up Down ☐ SFP Port Up Down	
Trap Receiver 1		
SNMP Trap Receiver Enabled	○ Disabled ● Enabled	
SNMP Trap Internet Address	1.1.100.16	
SNMP Trap Port Number	162	
SNMP Trap User Account	User 1: admin	
Trap Receiver 2		
SNMP Trap Receiver Enabled	○ Disabled ● Enabled	
SNMP Trap Internet Address	2001:DB8::17	
SNMP Trap Port Number	162	
SNMP Trap User Account	User 2: readonly	

Procedure:

- Update the attributes (Table 92).
- Click **Next**.

Table 92 Step 5: SNMP Trap Configuration attributes (for SNMPv3)

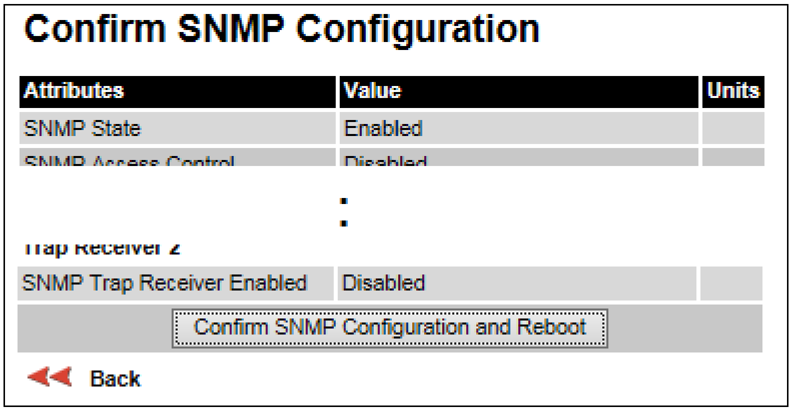
Attribute	Meaning
SNMP Enabled Traps	Select the events that will generate SNMP traps.
SNMP Trap Receiver 1 and SNMP Trap Receiver 2:	
SNMP Trap Receiver Enabled	**Disabled**: SNMP traps are not sent to the corresponding SNMP Trap Receiver (1 or 2). **Enabled**: SNMP traps are sent to the corresponding SNMP Trap Receiver (1 or 2).
SNMP Trap Internet Address	The IPv4 or IPv6 Address of the SNMP server (trap receiver). This is normally the network management system, but it may be a separate trap receiver.
SNMP Trap Port Number	The server port at which SNMP traps are received.
SNMP Trap User Account	The user name (and associated protocols) to use when sending SNMP traps to the server.

Confirm SNMP Configuration (for SNMPv3)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 90).

Use this page to review and confirm the updated SNMPv3 configuration of the unit.

Figure 90 Confirm SNMP Configuration page (for SNMPv3) (top and bottom of page shown)



Confirm SNMP Configuration

Attributes	Value	Units
SNMP State	Enabled	
SNMP Access Control	Disabled	

:

Trap Receiver 2

SNMP Trap Receiver Enabled	Disabled	

Procedure:

- To ensure that the changes take effect, click **Confirm SNMP Configuration and Reboot**. The unit reboots and the changes take effect.

SNMP pages (for SNMPv1/2c)

This section describes how to configure Simple Network Management Protocol version 1 or 2c (SNMPv1 or SNMPv2c) traps using the SNMP Wizard.

Current SNMP Summary (for SNMPv1/2c)

Menu option: **Management > SNMP** (Figure 84).

Use this page to review the current SNMP configuration and start the SNMP Wizard.

Procedure:

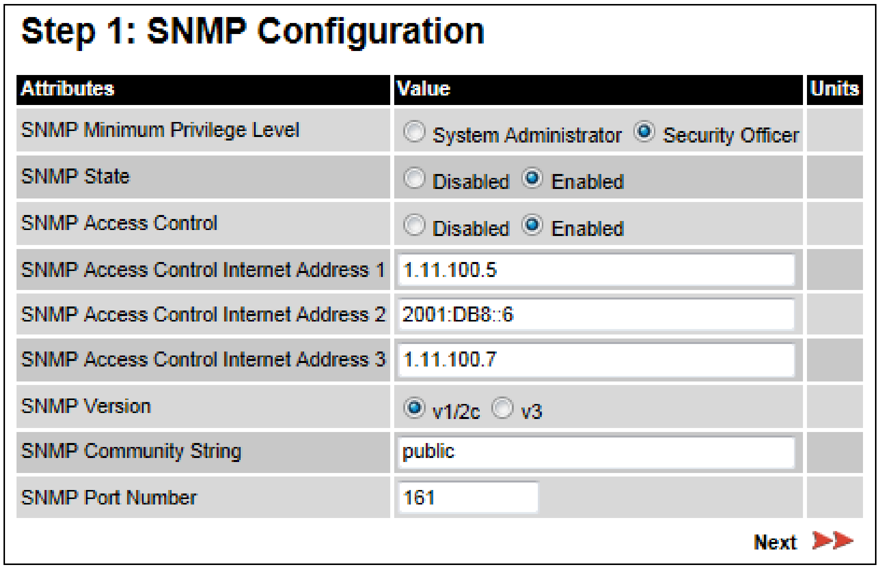
- Review the summary.
- If any updates are required, click **Continue to SNMP Wizard**.

Step 1: SNMP Configuration (for SNMPv1/2c)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 91).

Use this page to enable SNMP, select SNMPv1/2c and configure access to the SNMP server.

Figure 91 Step 1: SNMP Configuration page (for SNMPv1/2c)



Step 1: SNMP Configuration

Attributes	Value	Units
SNMP Minimum Privilege Level	○ System Administrator ● Security Officer	
SNMP State	○ Disabled ● Enabled	
SNMP Access Control	○ Disabled ● Enabled	
SNMP Access Control Internet Address 1	1.11.100.5	
SNMP Access Control Internet Address 2	2001:DB8::6	
SNMP Access Control Internet Address 3	1.11.100.7	
SNMP Version	● v1/2c ○ v3	
SNMP Community String	public	
SNMP Port Number	161	

Procedure:

- Set SNMP State to **Enabled**.
- Set SNMP Version to **v1/2c**. The page is redisplayed with SNMPv1/2c attributes.
- Update the attributes (Table 93).
- Click **Next**.

Table 93 Step 1: SNMP Configuration attributes (for SNMPv1/2c)

Attribute	Meaning
SNMP Minimum Privilege Level	Minimum security level which is permitted to administer SNMP security settings. Only displayed when Identity Based User Accounts are **Enabled** on the User Accounts page (Table 78).
SNMP State	Enables or disables SNMP.
SNMP Access Control	Enables or disables access control to SNMP management by IP address.
SNMP Access Control Internet Address 1/2/3	A list of up to three IPv4 or IPv6 Addresses permitted to perform SNMP management. Only displayed when SNMP Access Control is set to **Enabled**.
SNMP Version	SNMP protocol version: **v1/2c** or **v3**.
SNMP Community String	The SNMP community string acts like a password between the network management system and the distributed SNMP clients (PTP 650 ODUs). Only if the community string is configured correctly on all SNMP entities can the flow of management information take place. By convention the default value is set to **public**.
SNMP Port Number	Enter the port that the SNMP agent is listening to for commands from a management system.

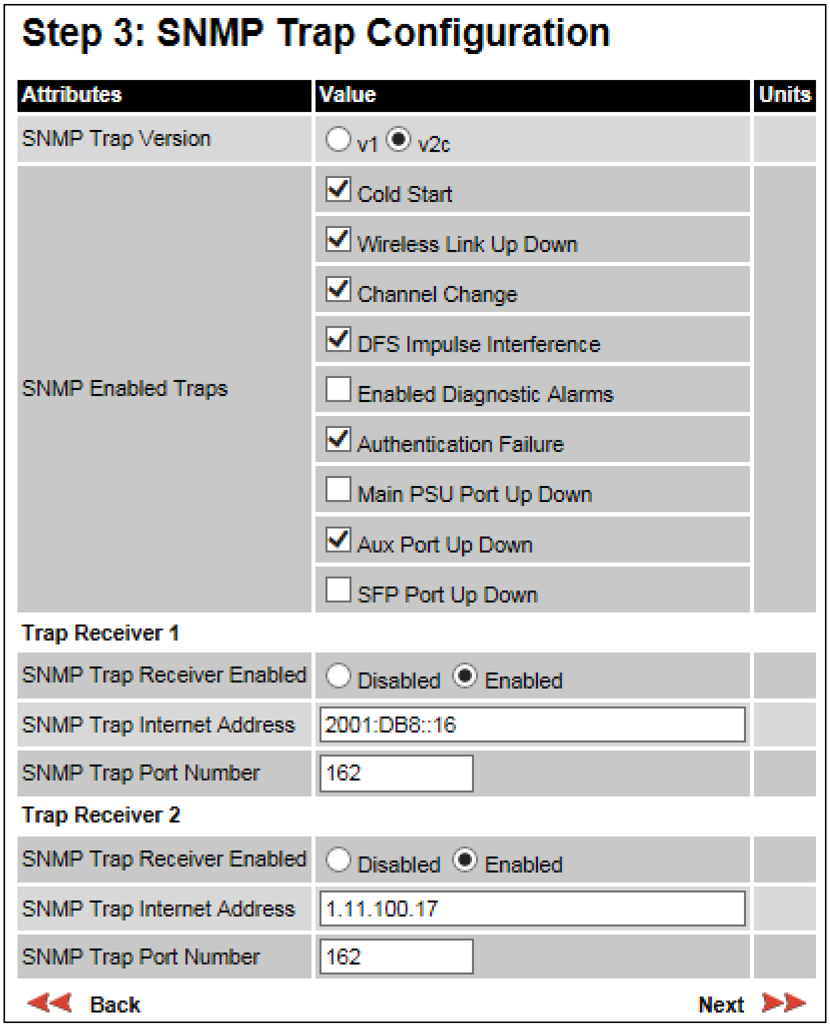
Step 2: SNMP MIB-II System Objects (for SNMPv1/2c)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 86). Use this page to enter details of the SNMP managed node. Update the attributes (Table 89) and click **Next**.

Step 3: SNMP Trap Configuration (for SNMPv1/2c)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 92).

Figure 92 Step 3: SNMP Trap Configuration page (for SNMPv1/2c)



Step 3: SNMP Trap Configuration

Attributes	Value	Units
SNMP Trap Version	○ v1 ● v2c	
SNMP Enabled Traps	☑ Cold Start	
	☑ Wireless Link Up Down	
	☑ Channel Change	
	☑ DFS Impulse Interference	
	□ Enabled Diagnostic Alarms	
	☑ Authentication Failure	
	□ Main PSU Port Up Down	
	☑ Aux Port Up Down	
	□ SFP Port Up Down	
Trap Receiver 1		
SNMP Trap Receiver Enabled	○ Disabled ● Enabled	
SNMP Trap Internet Address	2001:DB8::16	
SNMP Trap Port Number	162	
Trap Receiver 2		
SNMP Trap Receiver Enabled	○ Disabled ● Enabled	
SNMP Trap Internet Address	1.11.100.17	
SNMP Trap Port Number	162	

Procedure:

- Update the attributes (Table 94).
- Click **Next**.

Table 94 Step 3: SNMP Trap Configuration attributes (for SNMPv1/2c)

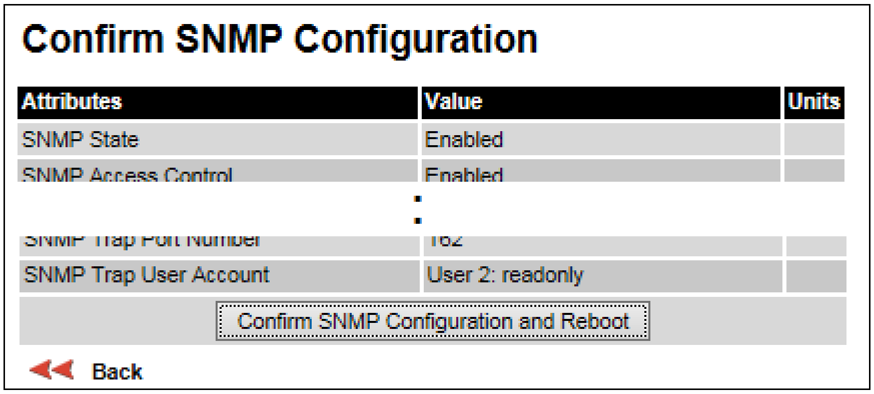
Attribute	Meaning
SNMP Trap Version	Select the SNMP protocol version to use for SNMP traps: **v1** or **v2c**.
SNMP Enabled Traps	Select the events that will generate SNMP traps.
SNMP Trap Receiver Enabled	**Disabled**: SNMP traps are not sent to the corresponding SNMP Trap Receiver (1 or 2). **Enabled**: SNMP traps are sent to the corresponding SNMP Trap Receiver (1 or 2).
SNMP Trap Internet Address	The IPv4 or IPv6 Address of the SNMP server (trap receiver). This is normally the network management system, but it may be a separate trap receiver.
SNMP Trap Port Number	The server port at which SNMP traps are received.

Confirm SNMP Configuration (for SNMPv1/2c)

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 93).

Use this page to review and confirm the updated SNMPv1/2c configuration of the unit.

Figure 93 Confirm SNMP Configuration page (for SNMPv1/2c) (top and bottom of page shown)



Confirm SNMP Configuration

Attributes	Value	Units
SNMP State	Enabled	
SNMP Access Control	Enabled	
:		
SNMP Trap Port Number	162	
SNMP Trap User Account	User 2: readonly	

Procedure:

- To ensure that the changes take effect, click **Confirm SNMP Configuration and Reboot**. The unit reboots and the changes take effect.

Security menu

This section describes how to configure HTTPS/TLS security using the Security Wizard.

Caution

Ensure that the operator's security requirements are configured before connecting the PTP 650 to the network. Otherwise, security may be compromised.

Preparing for HTTPS/TLS

Before running the Security Configuration Wizard, obtain the necessary cryptographic material and ensure that the unit has AES capability. For more information, refer to Planning for HTTPS/TLS operation on page 3-33.

Procedure:

1 Ensure that the following cryptographic material has been generated:

- Key Of Keys
- TLS Private Key and Public Certificates (for the correct IP address)
- User Defined Security Banner
- Random Number Entropy Input

2 Order the necessary AES capability upgrade, generate a license key and enter it on the Software License Key page (Software License Key page on page 6-12).

3 Identify the Port numbers for HTTPS, HTTP and Telnet.

4 Ensure that the web browsers used are enabled for HTTPS/TLS operation.

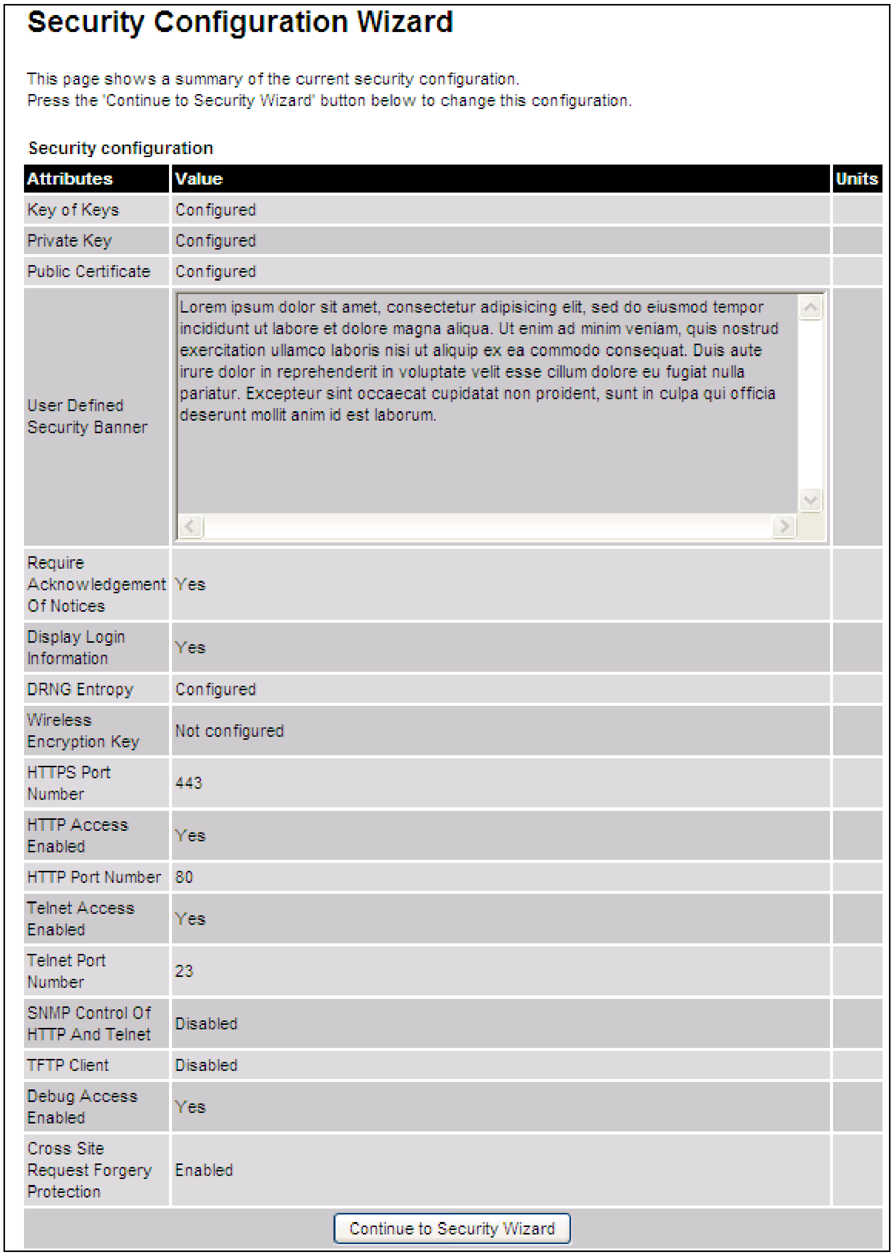
5 On the Local User Accounts page (Local User Accounts page on page 6-42), check that:

- Either: Identity Based User Accounts are set to **Disabled**,
- Or: Identity Based User Accounts are set to **Enabled** and the current user's role is **Security Officer**.

Security Configuration Wizard page

Menu option: **Security**. Displayed only when AES encryption is enabled by license key (Figure 94). Use this page to review the current security configuration of the unit.

Figure 94 Security Configuration Wizard page



Security Configuration Wizard

This page shows a summary of the current security configuration.
Press the 'Continue to Security Wizard' button below to change this configuration.

Security configuration

Attributes	Value	Units
Key of Keys	Configured	
Private Key	Configured	
Public Certificate	Configured	
User Defined Security Banner	Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.	
Require Acknowledgement Of Notices	Yes	
Display Login Information	Yes	
DRNG Entropy	Configured	
Wireless Encryption Key	Not configured	
HTTPS Port Number	443	
HTTP Access Enabled	Yes	
HTTP Port Number	80	
Telnet Access Enabled	Yes	
Telnet Port Number	23	
SNMP Control Of HTTP And Telnet	Disabled	
TFTP Client	Disabled	
Debug Access Enabled	Yes	
Cross Site Request Forgery Protection	Enabled	

Procedure:

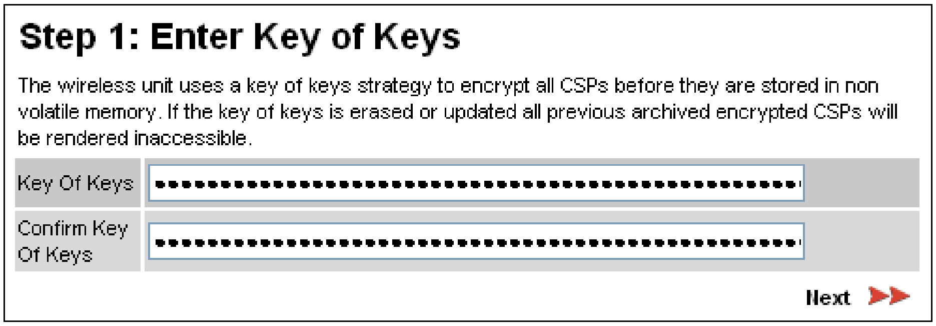
- To continue with the Security Wizard, click **Continue to Security Wizard**.

Step 1: Enter Key of Keys

Menu option: **Security**. Part of the Security Wizard (Figure 95).

Use this page to enter a Key of Keys to encrypt all critical security parameters (CSPs) before they are stored in non-volatile memory.

Figure 95 Step 1: Enter Key of Keys page



Step 1: Enter Key of Keys

The wireless unit uses a key of keys strategy to encrypt all CSPs before they are stored in non volatile memory. If the key of keys is erased or updated all previous archived encrypted CSPs will be rendered inaccessible.

Key Of Keys

Confirm Key Of Keys

Caution

Erasing or changing the key of keys erases all CSPs.

Procedure:

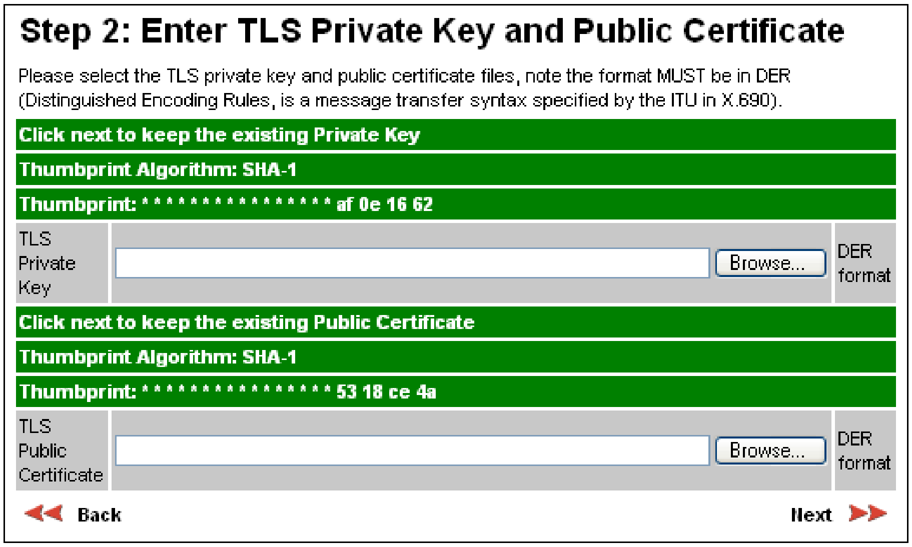
- Enter and confirm the generated Key of Keys.
- Click **Next**.

Step 2: Enter TLS Private Key and Public Certificate

Menu option: **Security**. Part of the Security Wizard (Figure 96).

Use this page to select and upload the TLS Private Key and Public Certificate files.

Figure 96 Step 2: Enter TLS Private Key and Public Certificate page



Step 2: Enter TLS Private Key and Public Certificate

Please select the TLS private key and public certificate files, note the format MUST be in DER (Distinguished Encoding Rules, is a message transfer syntax specified by the ITU in X.690).

Click next to keep the existing Private Key

Thumbprint Algorithm: SHA-1

Thumbprint: * * * * * * * * * * * * * * * * af 0e 16 62

TLS Private Key	Browse...	DER format

Click next to keep the existing Public Certificate

Thumbprint Algorithm: SHA-1

Thumbprint: * * * * * * * * * * * * * * * * 53 18 ce 4a

TLS Public Certificate	Browse...	DER format

Caution

If the certificates expire, the unit will be unreachable. If this occurs, put the unit into recovery mode and erase all configuration settings. For more information, refer to Recovery mode on page 7-44.

Procedure:

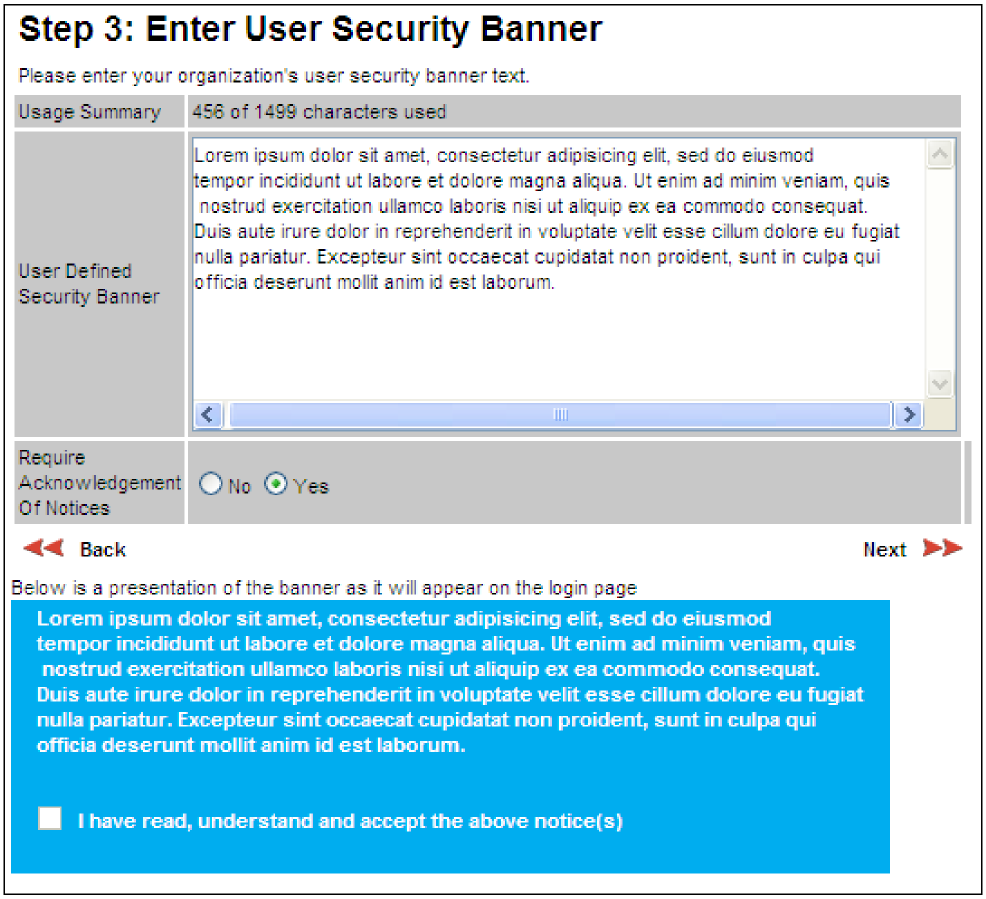
- If a valid TLS private key exists, then an SHA-1 thumbprint of the key is displayed. If this key is correct, then take no action. Otherwise, click **Browse** and select the generated private key file (.der).
- If a valid TLS public certificate exists, then an SHA-1 thumbprint of the certificate is displayed. If this certificate is correct, then take no action. Otherwise, click **Browse** and select the generated certificate file (.der).
- Click **Next.**

Step 3: Enter User Security Banner

Menu option: **Security**. Part of the Security Wizard (Figure 97).

Use this page to enter a banner that will be displayed every time a user attempts to login to the wireless unit.

Figure 97 Step 3: Enter User Security Banner page



Step 3: Enter User Security Banner

Please enter your organization's user security banner text.

Usage Summary	456 of 1499 characters used
User Defined Security Banner	Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.
Require Acknowledgement Of Notices	○ No ● Yes

Below is a presentation of the banner as it will appear on the login page

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

☐ I have read, understand and accept the above notice(s)

Procedure:

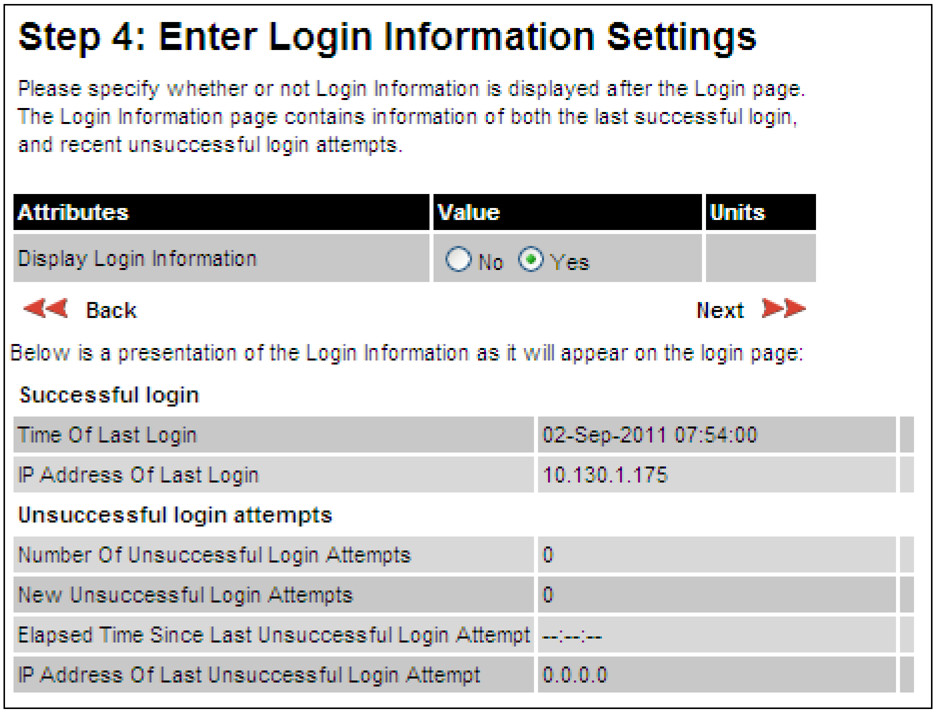
- Update the User Defined Security Banner (optional).
- Set the Acknowledgement to **No** or **Yes**.
- Click **Next**.

Step 4: Enter Login Information Settings

Menu option: **Security**. Part of the Security Wizard (Figure 98).

Use this page to choose whether or not to display information about previous login attempts when the user logs into the web interface.

Figure 98 Step 4: Enter Login Information Settings page



Step 4: Enter Login Information Settings

Please specify whether or not Login Information is displayed after the Login page. The Login Information page contains information of both the last successful login, and recent unsuccessful login attempts.

Attributes	Value	Units
Display Login Information	○ No ● Yes	

Below is a presentation of the Login Information as it will appear on the login page:

Successful login

Time Of Last Login	02-Sep-2011 07:54:00
IP Address Of Last Login	10.130.1.175

Unsuccessful login attempts

Number Of Unsuccessful Login Attempts	0
New Unsuccessful Login Attempts	0
Elapsed Time Since Last Unsuccessful Login Attempt	--:--:--
IP Address Of Last Unsuccessful Login Attempt	0.0.0.0

Procedure:

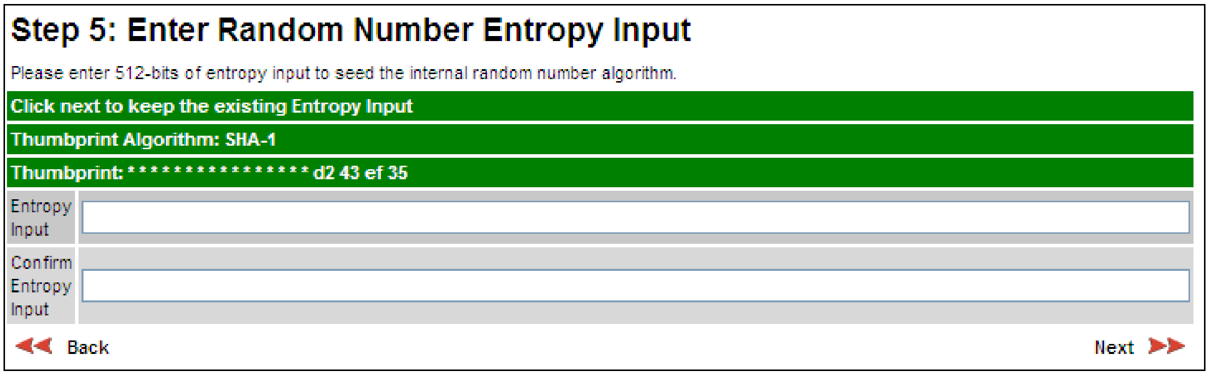
- Set Display Login Information to **No** or **Yes**.
- Click **Next**.

Step 5: Enter Random Number Entropy Input

Menu option: **Security**. Part of the Security Wizard (Figure 99).

Use this page to enter entropy input to seed the internal random number algorithm.

Figure 99 Step 5: Random Number Entropy Input page



Step 5: Enter Random Number Entropy Input

Please enter 512-bits of entropy input to seed the internal random number algorithm.

Click next to keep the existing Entropy Input

Thumbprint Algorithm: SHA-1

Thumbprint: *************** d2 43 ef 35

Entropy Input

Confirm Entropy Input

Procedure:

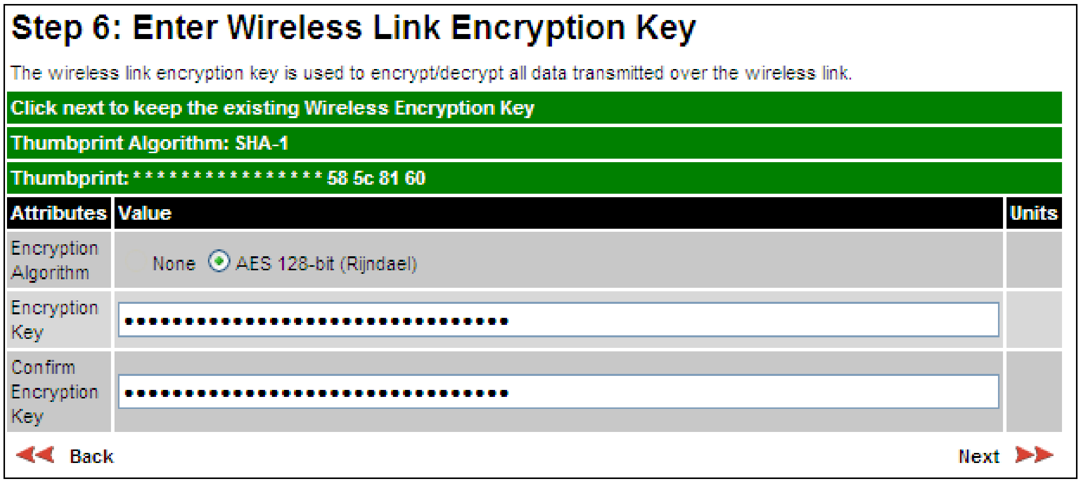
- If valid entropy input exists, then an SHA-1 thumbprint of the input is displayed. If this input is correct, then take no action. Otherwise, enter the generated input in the Entropy Input and Confirm Entropy Input fields.
- Click **Next**.

Step 6: Enter Wireless Link Encryption Key

Menu option: **Security**. Part of the Security Wizard (Figure 100).

Use this page to enable AES encryption and enter the encryption key. The wireless link encryption key is used to encrypt all traffic over the PTP 650 wireless link.

Figure 100 Step 6: Enter Wireless Link Encryption Key page



Step 6: Enter Wireless Link Encryption Key

The wireless link encryption key is used to encrypt/decrypt all data transmitted over the wireless link.

Click next to keep the existing Wireless Encryption Key

Thumbprint Algorithm: SHA-1

Thumbprint: * * * * * * * * * * * * * * * * 58 5c 81 60

Attributes	Value	Units
Encryption Algorithm	None ◉ AES 128-bit (Rijndael)	
Encryption Key	••••••••••••••••••••••••••••••••	
Confirm Encryption Key	••••••••••••••••••••••••••••••••	

Procedure:

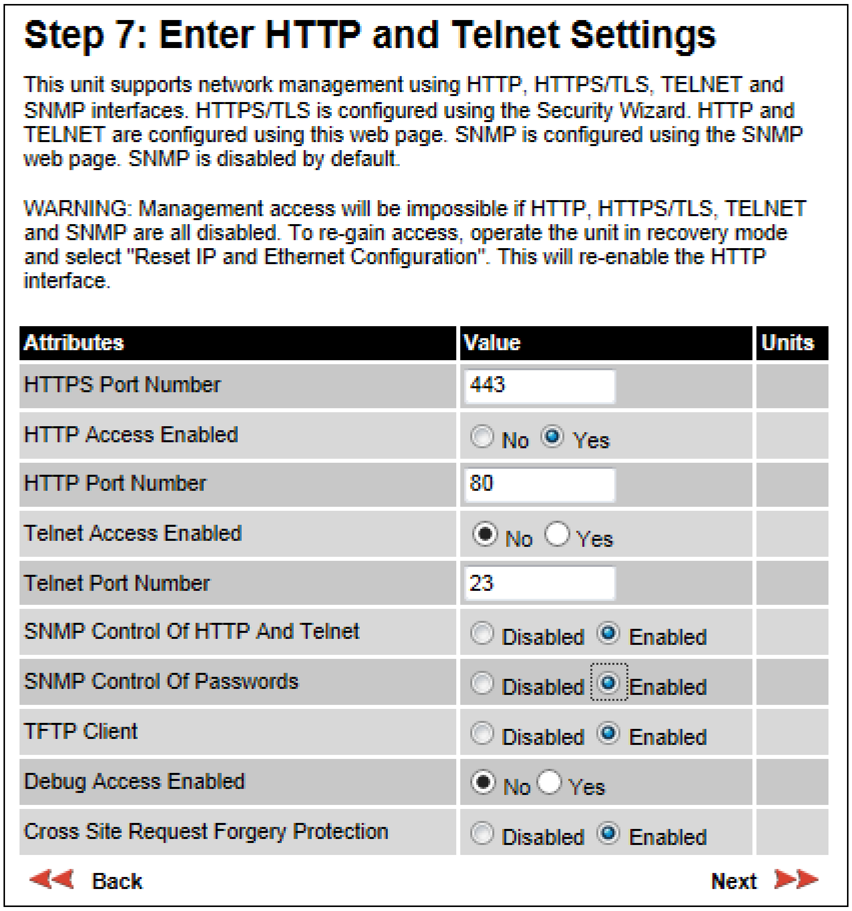
- Select the applicable value in the Encryption Algorithm field. If a valid encryption key exists, then an SHA-1 thumbprint of the key is displayed. If this key is correct, then take no action. Otherwise, enter the generated key in the Wireless Link Encryption Key and Confirm Wireless Link Encryption Key fields.
- Click **Next**.

Step 7: Enter HTTP and Telnet Settings

Menu option: **Security**. Part of the Security Wizard (Figure 101).

Use this page to configure network management of the PTP 650 using one or more of the following methods: HTTPS, HTTP, Telnet or SNMP.

Figure 101 Step 7: Enter HTTP and Telnet Settings page



Step 7: Enter HTTP and Telnet Settings

This unit supports network management using HTTP, HTTPS/TLS, TELNET and SNMP interfaces. HTTPS/TLS is configured using the Security Wizard. HTTP and TELNET are configured using this web page. SNMP is configured using the SNMP web page. SNMP is disabled by default.

WARNING: Management access will be impossible if HTTP, HTTPS/TLS, TELNET and SNMP are all disabled. To re-gain access, operate the unit in recovery mode and select "Reset IP and Ethernet Configuration". This will re-enable the HTTP interface.

Attributes	Value	Units
HTTPS Port Number	443	
HTTP Access Enabled	○ No ● Yes	
HTTP Port Number	80	
Telnet Access Enabled	● No ○ Yes	
Telnet Port Number	23	
SNMP Control Of HTTP And Telnet	○ Disabled ● Enabled	
SNMP Control Of Passwords	○ Disabled ● Enabled	
TFTP Client	○ Disabled ● Enabled	
Debug Access Enabled	● No ○ Yes	
Cross Site Request Forgery Protection	○ Disabled ● Enabled	

Caution

If HTTPS, HTTP, Telnet and SNMP are all disabled, management access will be impossible until the unit is placed in recovery mode.

Note

If HTTP, Telnet and SNMP are all disabled, the secure web server becomes the only management tool for the ODU web interface. To reenter the web interface after Step 7 of the Security Wizard, use the URL **https://aa.bb.cc.dd** (where aa.bb.cc.dd is the IP address of the unit). Enclose the IPv6 address in the URL in square brackets.

Procedure:

- Review and update the HTTP and Telnet attributes (Table 95) and click **Next**.

Table 95 HTTP and Telnet attributes

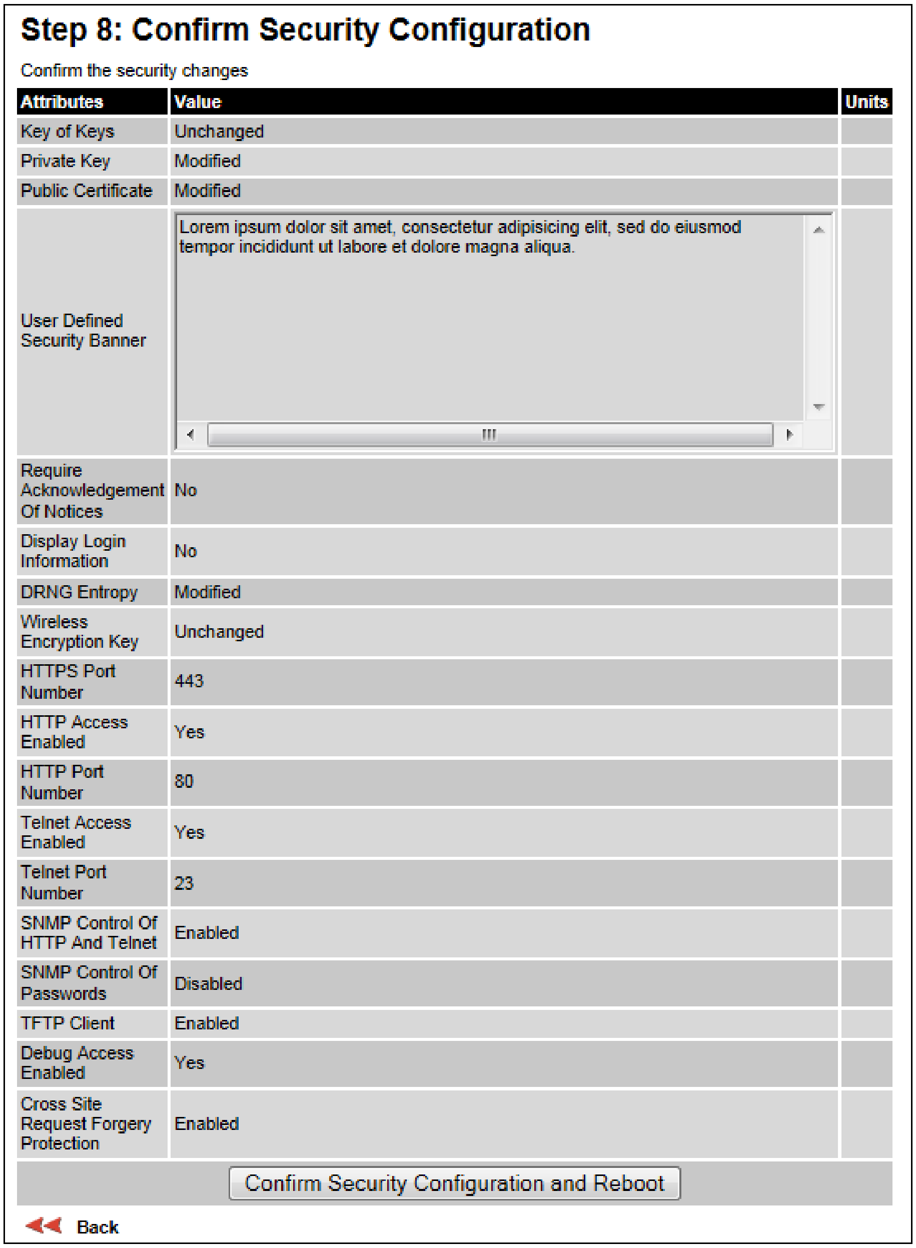
Attribute	Meaning
HTTPS Port Number	The port number for HTTPS access. Zero means use the default port.
HTTP Access Enabled	**No**: The unit will not respond to any requests on the HTTP port. **Yes**: The unit will respond to requests on the HTTP port. Remote management via HTTPS is not affected by this setting.
HTTP Port Number	The port number for HTTP access. Zero means use the default port.
Telnet Access Enabled	**No**: The unit will not respond to any requests on the Telnet port. **Yes**: The unit will respond to requests on the Telnet port.
Telnet Port Number	The port number for Telnet access. Zero means use the default port.
SNMP Control of HTTP And Telnet	**Disabled**: Neither HTTP nor Telnet can be controlled remotely via SNMP. **Enabled**: Both HTTP and Telnet can be controlled remotely via SNMP.
SNMP Control of Passwords	**Enabled:** Passwords for identity-based user accounts in the web-based interface can be updated via SNMP. Use this with SNMPv3 to provide secure password updating from a central network manager. **Disabled**: Passwords for identity-based user accounts can be updated only via the web-based interface (default).
TFTP Client	**Enabled**: The unit will respond to TFTP software download requests.
Debug Access Enabled	**Yes**: Cambium Technical Support is allowed to access the system to investigate faults.
Cross Site Request Forgery Protection	**Enabled**: The system is protected against cross-site request forgery attacks at the web-based interface.

Step 8: Commit Security Configuration

Menu option: **Security**. Part of the Security Wizard (Figure 102).

Use this page to review and confirm the updated security configuration of the unit.

Figure 102 Step 8: Commit Security Configuration page



Step 8: Confirm Security Configuration

Confirm the security changes

Attributes	Value	Units
Key of Keys	Unchanged	
Private Key	Modified	
Public Certificate	Modified	
User Defined Security Banner	Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.	
Require Acknowledgement Of Notices	No	
Display Login Information	No	
DRNG Entropy	Modified	
Wireless Encryption Key	Unchanged	
HTTPS Port Number	443	
HTTP Access Enabled	Yes	
HTTP Port Number	80	
Telnet Access Enabled	Yes	
Telnet Port Number	23	
SNMP Control Of HTTP And Telnet	Enabled	
SNMP Control Of Passwords	Disabled	
TFTP Client	Enabled	
Debug Access Enabled	Yes	
Cross Site Request Forgery Protection	Enabled	

Procedure:

- Review all changes that have been made in the Security Wizard.
- To ensure that the changes take effect, click **Commit Security Configuration and Reboot**. The unit reboots and the changes take effect.

Note

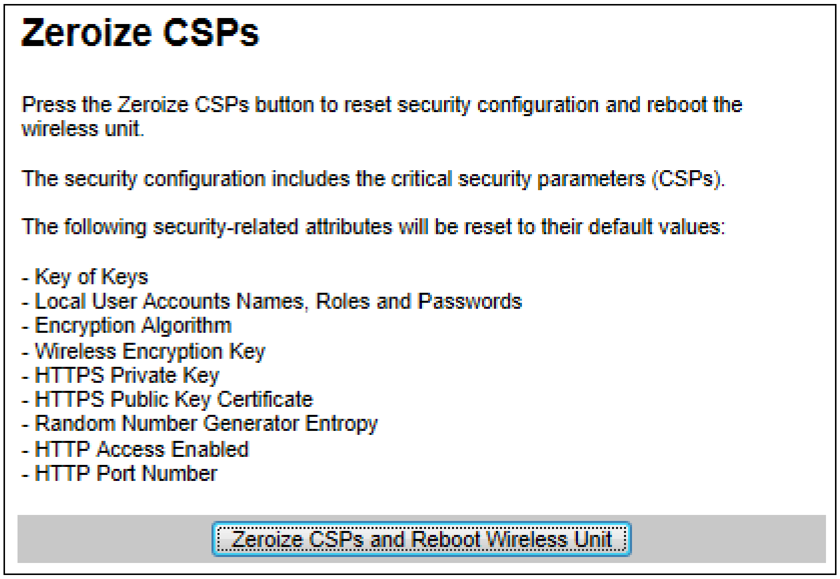
If the Key of keys is entered or modified in the Security Wizard, user accounts are reset when **Commit Security Configuration and Reboot** is clicked. It is then necessary to reconfigure them.

Zeroize CSPs page

Menu option: **Security** > **Zeroize CSPs** (Figure 103).

Use this page if it is necessary to zeroize Critical security parameters (CSPs).

Figure 103 Zeroize CSPs page



Zeroize CSPs

Press the Zeroize CSPs button to reset security configuration and reboot the wireless unit.

The security configuration includes the critical security parameters (CSPs).

The following security-related attributes will be reset to their default values:

- Key of Keys
- Local User Accounts Names, Roles and Passwords
- Encryption Algorithm
- Wireless Encryption Key
- HTTPS Private Key
- HTTPS Public Key Certificate
- Random Number Generator Entropy
- HTTP Access Enabled
- HTTP Port Number

Procedure:

- Click **Zeroize CSPs and Reboot Wireless Unit**.
- Confirm the reboot.

Aligning antennas

This section describes how to align the antennas in a PTP 650 link, use the web interface to assist with alignment, and check wireless performance after alignment.

Before performing this task, check that hardware installation is complete (apart from the network connections) at both the Master and Slave sites.

Starting up the units

Use this procedure to connect one of the units to a management PC and start up both units.

Procedure:

1 Select the unit from which this process is to be controlled; either Master or Slave. This is the “local” unit.

2 Check that the management PC is connected to the local unit, powered up and logged on as described in Connecting to the unit on page 6-5.

4 Power up the remote unit.

5 Log into the local unit as described in Logging into the web interface on page 6-7.

Checking that the units are armed

Use this procedure to confirm that the units are in the armed state, ready for alignment.

In the armed state, the modulation mode is fixed at BPSK 0.63 Single, the TDD frame duration is extended to allow the link to acquire at unknown range, and the transmit power is automatically adjusted for optimum operation.

Procedure:

- Select menu option **Home**. The System Summary page is displayed.
- Check that the Install Arm State is set to **Armed**.
- If the units are not armed, execute the installation wizard as described in Installation menu on page 6-10.

Aligning antennas

Use this procedure to align linked antennas (master and slave), whether integrated or connectorized. The goal of antenna alignment is to find the center of the main beam. This is done by adjusting the antennas while monitoring the receive signal level.

Preparation:

Ensure that the following parameters are available:

- Location of both sites (latitude and longitude).
- Bearing to the other end of the link for both sites.
- Prediction of receive signal level for both ends of the link.
- Prediction of link loss.

PTP LINKPlanner provides all of these parameters in the form of an installation report.

If a connectorized ODU is installed at either site with two separate antennas for spatial diversity, refer to Aligning separate antennas for spatial diversity on page 6-89 before starting alignment.

Note

For improved radio performance, mount the integrated ODU at 45 degrees to the vertical, as shown in Installing the ODU and top LPU on page 5-5.

To achieve best results, make small incremental changes to elevation and azimuth.

Caution

The action of tightening the mounting bolts can alter antenna alignment. This can be helpful when fine-tuning alignment, but it can also lead to misalignment. To prevent misalignment, continue to monitor receive signal level during final tightening of the bolts.

Procedure:

1 At each end of the link, adjust the antenna to point at the other end of the link. This should be done with the aid of a compass.

2 Without moving the master antenna, adjust the elevation and azimuth of the slave antenna to achieve the highest receive signal level using one of the following methods:

   - ODU installation tones on page 6-90
   - Graphical Install page on page 6-92

3 Without moving the Slave antenna, adjust the elevation and azimuth of the Master antenna to achieve the highest receive signal level (using one of the above methods).

4 Repeat steps 2 and 3 as necessary to fine-tune the alignment to find the center of the beam.

5 When the antennas have been aligned on the center of the beam, verify that the receive level is within the predicted range (from the installation report). If this is not the case, go back to step 2.

The current value of receive level can be verified by using the graphical installation method (see Graphical Install page on page 6-92) or by selecting menu option **Status** and monitoring the Receive Power attribute on the System Status page.

6 If after repeated attempts to align, the receive level still does not lie within the predicted range, this may be because the data provided to the prediction tool (such as PTP LINKPlanner) is inaccurate. For example estimates of path obstructions, antenna heights or site locations may be inaccurate. Check this data and update the prediction as necessary.

7 Once the antennas have been aligned correctly, tighten the integrated ODU (or connectorized antenna) mountings. To ensure that the action of tightening does not alter antenna alignment, continue to monitor received signal level.

Aligning separate antennas for spatial diversity

Use this procedure if a connectorized ODU is installed at either site with two separate antennas for spatial diversity.

Procedure:

1 Connect the horizontal polarization antenna to the ODU, disconnect the vertical polarization antenna, then perform Aligning antennas on page 6-88.

2 Connect the vertical polarization antenna to the ODU, disconnect the horizontal polarization antenna, then perform Aligning antennas on page 6-88.

3 Re-connect the horizontal polarization antennas. The received signal level should increase.

4 Weatherproof the antenna connections at the “H” and “V” interfaces of the ODUs, as described in Weatherproofing an N type connector on page 5-37.

ODU installation tones

This is the first of two methods that may be used to monitor receive signal level during antenna alignment.

The ODU emits audible tones during installation to assist with alignment. The pitch of the alignment tone is proportional to the received power of the wireless signals. Adjust the alignment of the unit in both azimuth and elevation until the highest pitch tone is achieved.

Note

When using ODU installation tones to align connectorized antennas, it may not be possible to hear the tones. To overcome this problem, either use an assistant, or use a stethoscope to give a longer reach.

The tones and their meanings are described in Table 96. In each of the states detailed in the table, align the unit to give the highest pitch tone. The term "wanted signal" refers to that of the peer unit being installed.

Table 96 ODU installation tones

State Name	Tone Description	State Description	Pitch Indication
Free Channel Search	Regular beep	Executing band scan	N/A
Scanning	Slow broken tone	Not demodulating the wanted signal	Rx Power
Synchronized	Fast broken tone	Demodulating the wanted signal	Rx Power
Registered	Solid tone	Both Master and Slave units exchanging Radio layer MAC management messages	Rx Power

Caution

If, when in the Synchronized or Registered state, the tone varies wildly, there may be interference or a fast fading link. Installing in this situation may not give a reliable link. Investigate the cause of the problem.

During alignment, the installation tones should exhibit the following behavior:

- **Band scan:** When first started up and from time to time, the Master unit will carry out a band scan to determine which channels are not in use. During this time, between 10 and 15 seconds, the Master unit will not transmit and as a consequence of this neither will the Slave unit. During this time the installation tone on the master unit will drop back to the band scan state, and the Slave unit will drop back to the Scanning state with the pitch of the tone set to the background noise level. Alignment of the unit should cease during this time.
- **Radar detection:** If the unit is operating where mandatory radar avoidance algorithms are implemented, the ranging behavior may be affected. The Master has to monitor the initially chosen channel for 60 seconds to make sure it is clear of radar signals before transmitting. If a radar signal is detected during any of the installation phases, a further compulsory 60 seconds channel scan will take place as the master unit attempts to locate a new channel that is free of radar interference.
- **Ranging:** The PTP 650 Series does not require the user to enter the link range. The Master unit typically takes less than 60 seconds to determine the length of the link being installed. The Master unit will remain in the Scanning state until the range of the link has been established. The Master unit will only move to the Synchronized state when the range of the link has been established.

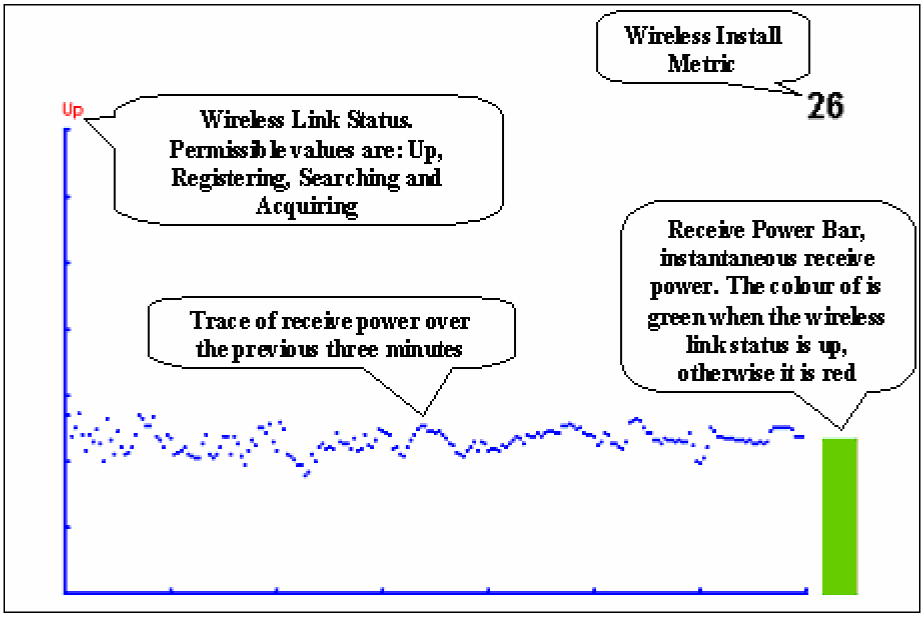
  The Slave unit does not have a ranging process. The slave unit will change to the Synchronized state as soon as the wanted signal is demodulated.
- **Retrying same channel:** If, at the end of the ranging period, the Registered state is not achieved due to interference or other reasons, the Master unit will retry twice more on the same channel before moving to another available channel. Should this occur it may take a number of minutes to establish a link in the Registered state.

Graphical Install page

Menu option: **Installation > Graphical Install** (Figure 104).

This is the second of two methods that may be used to monitor receive signal level during antenna alignment.

Figure 104 Graphical Install page


Wireless Install Metric
26
Up
Wireless Link Status. Permissible values are: Up, Registering, Searching and Acquiring
Trace of receive power over the previous three minutes
Receive Power Bar, instantaneous receive power. The colour of is green when the wireless link status is up, otherwise it is red

Procedure:

- Check that Wireless Link Status (top left) is “Up”, “Registering”, “Searching” or “Acquiring”.
- While slowly sweeping the antenna, monitor the trace of receive power over the last three minutes.
- Monitor the Receiver Power Bar (bottom right). Green signifies that the wireless link is up and red signifies all other states.
- Monitor the Wireless Install Metric (top right). This is the instantaneous receive power in dBm + 110.

Note

To access the PDA version of the graphical installation tool, use this URL - **http://<ip-address>/pda.cgi**. This link is only available to system administrators.

Disarming the units

When antenna alignment is complete, use this procedure to disarm both units in the link in order to:

- Turn off the audible alignment aid.
- Enable adaptive modulation.
- Fully enable spectrum management features (such as DSO, if configured).
- Clear unwanted installation information from the various systems statistics.
- Store the link range for fast link acquisition on link drop.
- Enable higher data rates.

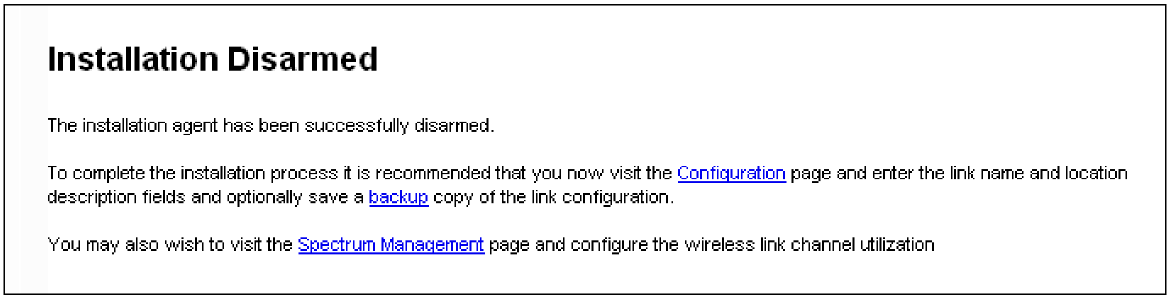
Note

After 24 hours, the units will be disarmed automatically, provided that they are armed and that the link is up.

Procedure:

- Select menu option **Installation.** The Disarm Installation page is displayed (Figure 58).
- Click **Disarm Installation Agent**. The confirmation page is displayed (Figure 105).

Figure 105 Optional post-disarm configuration



Installation Disarmed

The installation agent has been successfully disarmed.

To complete the installation process it is recommended that you now visit the Configuration page and enter the link name and location description fields and optionally save a backup copy of the link configuration.

You may also wish to visit the Spectrum Management page and configure the wireless link channel utilization

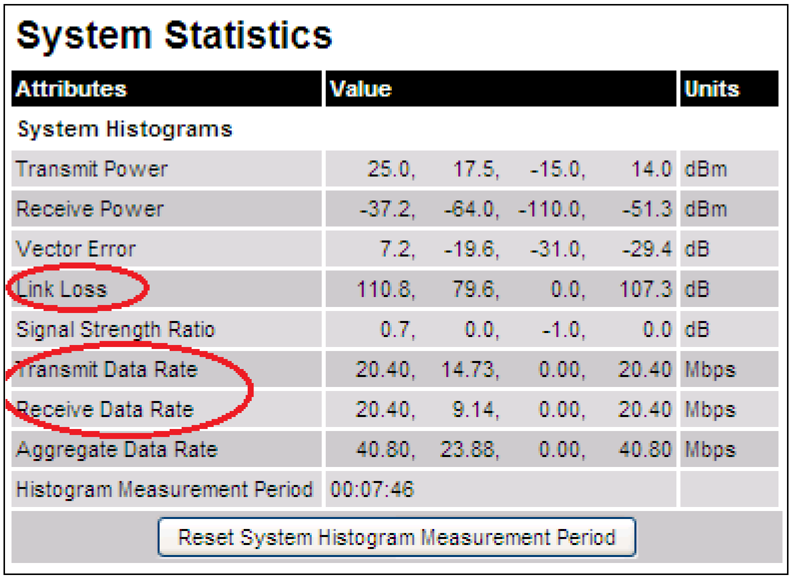
Comparing actual to predicted performance

For at least one hour of operation after disarming, use this procedure to monitor the link to check that it is achieving predicted levels of performance. PTP LINKPlanner provides the prediction in the form of an installation report.

Procedure:

- Select menu option **System > Statistics**. The System Statistic page is displayed (Figure 106).
- Monitor the following attributes:
  - Link Loss
  - Transmit Data Rate
  - Receive Data Rate

Figure 106 Statistics to be monitored after alignment



System Statistics

Attributes	Value				Units
System Histograms					
Transmit Power	25.0,	17.5,	-15.0,	14.0	dBm
Receive Power	-37.2,	-64.0,	-110.0,	-51.3	dBm
Vector Error	7.2,	-19.6,	-31.0,	-29.4	dB
Link Loss	110.8,	79.6,	0.0,	107.3	dB
Signal Strength Ratio	0.7,	0.0,	-1.0,	0.0	dB
Transmit Data Rate	20.40,	14.73,	0.00,	20.40	Mbps
Receive Data Rate	20.40,	9.14,	0.00,	20.40	Mbps
Aggregate Data Rate	40.80,	23.88,	0.00,	40.80	Mbps
Histogram Measurement Period	00:07:46				

For more information on the System Statistics page, refer to System Statistics page on page 7-32.

Other configuration tasks

This section describes other configuration tasks.

Connecting to the network

Use this procedure to complete and test network connections.

Procedure:

1 If a management PC is connected directly to the PTP 650, disconnect it.

2 Confirm that all ODU Ethernet interface cables (PSU, SFP and Aux) are connected to the correct network terminating equipment or devices.

If Main PSU Port Allocation is set to **Disabled** in the LAN Configuration page), it is not necessary to connect the PSU LAN port to network terminating equipment.

3 Test that the unit is reachable from the network management system by opening the web interface to the management agent, or by requesting ICMP echo response packets using the Ping application. For in-band management, test that both units are reachable from one PC.

If the network management system is remote from the sites, either ask co-workers at the management center to perform this test, or use remote login to the management system.

4 Test the data network for correct operation across the wireless link. This may be by requesting ICMP echo response packets between hosts in the connected network segments, or by some more structured use of network testing tools.

5 Monitor the Ethernet ports and wireless link to confirm that they are running normally. For instructions, see System Summary page on page 7-2 and System Status page on page 7-3.

Upgrading software using TFTP

Use this procedure to upgrade software remotely using Trivial FTP (TFTP) triggered by SNMP.

Procedure:

1. Check that the TFTP client is enabled. Refer to Web-Based Management page on page 6-39.
2. Set tFTP attributes as described in Table 97.
3. Monitor tFTP attributes as described in Table 98.
4. Reboot the ODU as described in Rebooting the unit on page 7-51.

Table 97 Setting tFTP attributes

Attribute	Meaning
tFTPServerInternetAddress	The IPv4 or IPv6 address of the TFTP server from which the TFTP software upgrade file Name will be retrieved. For example, to set the TFTP server IP address for the unit at 10.10.10.10 to the IPv4 address 10.10.10.1, enter this command: **`snmpset_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.7.9.19.0 a 10.10.10.1`**
tFTPServerPortNumber	This setting is optional. The port number of the TFTP server from which the TFTP software upgrade file name will be retrieved (default=69).
tFTPSoftwareUpgrade FileName	The filename of the software upgrade to be loaded from the TFTP server. For example, to set the TFTP software upgrade filename on 10.10.10.10 to "B1095.dld", enter this command: **`snmpset_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.7.9.7.0 s B1095.dld`**
tFTPStartSoftware Upgrade	Write “1” to this attribute to start the TFTP software upgrade process. The attribute will be reset to 0 when the upgrade process has finished. For example, enter this command: **`snmpset_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.7.9.8.0 i 1`**

Table 98 Monitoring tFTP attributes

Attribute	Meaning

tFTPSoftwareUpgradeStatus	This is the current status of the TFTP software upgrade process. Values:
	idle(0)
	uploadinprogress(1)
	uploadsuccessfulprogrammingFLASH(2)
	upgradesuccessfulreboottorunthenewsoftwareimage(3)
	upgradefailed(4).
	For example, enter this command:
	`snmpget_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.7.9.9.0`

tFTPSoftwareUpgradeStatusText	This describes the status of the TFTP software upgrade process, including any error details. For example, enter this command: `snmpget_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.7.9.10.0`
tFTPSoftwareUpgradeStatusAdditionalText	This is used if tFTPSoftwareUpgradeStatusText is full and there are more than 255 characters to report. It contains additional text describing the status of the TFTP software upgrade process, including any error details. For example, enter this command: `snmpget_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.7.9.11.0`

Chapter 7: Operation

This chapter provides instructions for operators of the PTP 650 wireless Ethernet bridge.

The following topics are described in this chapter:

System summary and status

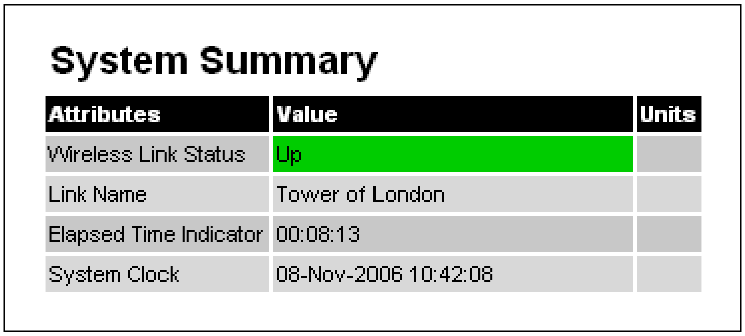
This section describes how to use the summary and status pages to monitor the status of the Ethernet ports and wireless link.

System Summary page

Menu option: **Home** (Figure 107).

This page contains a high level summary of the status of the wireless link and associated equipment.

Figure 107 System Summary page



System Summary

Attributes	Value	Units
Wireless Link Status	Up	
Link Name	Tower of London	
Elapsed Time Indicator	00:08:13	
System Clock	08-Nov-2006 10:42:08	

Procedure:

- Review the attributes (Table 99).
- Check that the Wireless Link Status is "Up" on both units. If it is not "Up", review any uncleared system alarms: these are displayed below the System Clock attribute. Whenever system alarms are outstanding, a yellow warning triangle is displayed on the navigation bar. For more information, refer to Alarms on page 7-12.

Table 99 System Summary attributes

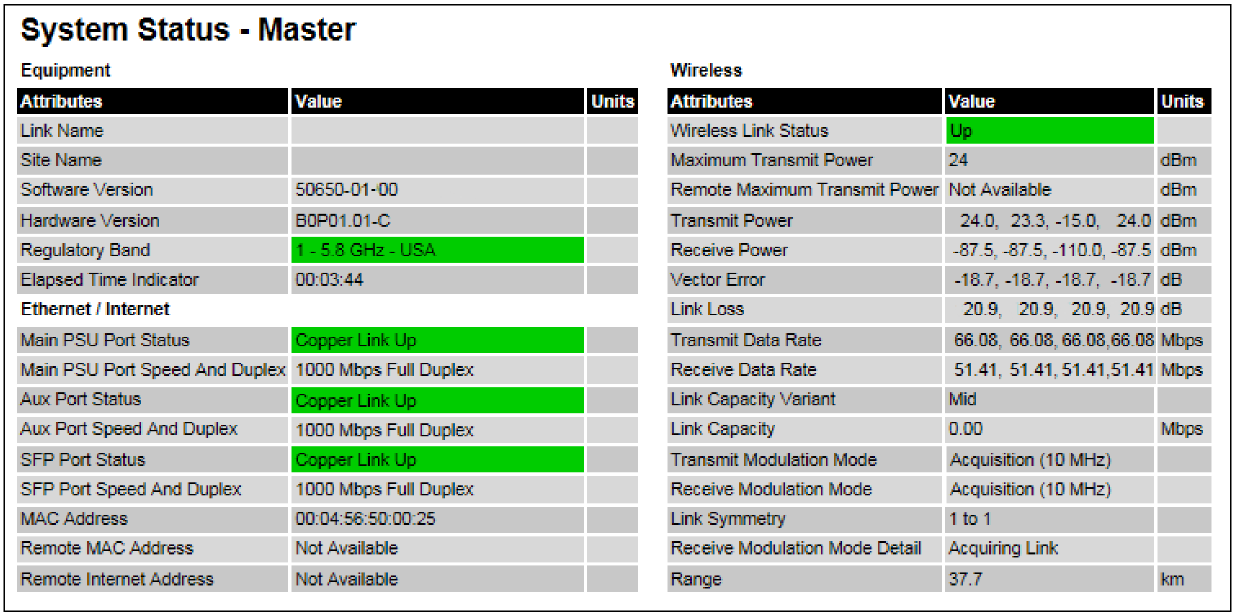
Attribute	Meaning
Wireless Link Status	Current status of the wireless link. A green background with status text "Up" means that the point-to-point link is established. A red background with suitable status text (for example "`Searching`") indicates that the link is not established.

Attribute	Meaning
Link Name	The name of the PTP link, as set in the System Configuration page.
Elapsed Time Indicator	The time (hh:mm:ss) that has elapsed since the last system reboot. The system can reboot for several reasons, for example, commanded reboot from the system reboot webpage, or a power cycle of the equipment.
System Clock	The system clock presented as local time, allowing for zone and daylight saving (if set).

System Status page

Menu option: **Status** (Figure 108). This page provides a detailed view of the operation of the PTP 650 link from both the wireless and network perspectives.

Figure 108 System Status page



System Status - Master

Equipment

Attributes	Value	Units
Link Name		
Site Name		
Software Version	50650-01-00	
Hardware Version	B0P01.01-C	
Regulatory Band	1 - 5.8 GHz - USA	
Elapsed Time Indicator	00:03:44	
Ethernet / Internet		
Main PSU Port Status	Copper Link Up	
Main PSU Port Speed And Duplex	1000 Mbps Full Duplex	
Aux Port Status	Copper Link Up	
Aux Port Speed And Duplex	1000 Mbps Full Duplex	
SFP Port Status	Copper Link Up	
SFP Port Speed And Duplex	1000 Mbps Full Duplex	
MAC Address	00:04:56:50:00:25	
Remote MAC Address	Not Available	
Remote Internet Address	Not Available	

Wireless

Attributes	Value	Units
Wireless Link Status	Up	
Maximum Transmit Power	24	dBm
Remote Maximum Transmit Power	Not Available	dBm
Transmit Power	24.0, 23.3, -15.0, 24.0	dBm
Receive Power	-87.5, -87.5, -110.0, -87.5	dBm
Vector Error	-18.7, -18.7, -18.7, -18.7	dB
Link Loss	20.9, 20.9, 20.9, 20.9	dB
Transmit Data Rate	66.08, 66.08, 66.08,66.08	Mbps
Receive Data Rate	51.41, 51.41, 51.41,51.41	Mbps
Link Capacity Variant	Mid	
Link Capacity	0.00	Mbps
Transmit Modulation Mode	Acquisition (10 MHz)	
Receive Modulation Mode	Acquisition (10 MHz)	
Link Symmetry	1 to 1	
Receive Modulation Mode Detail	Acquiring Link	
Range	37.7	km

The two PTP 650 Series units are arranged in a master and slave relationship. The roles of the units in this relationship are displayed in the page title. The master unit will always have the title "`- Master`", and the slave will always have "`- Slave`" appended to the "`Systems Status`" page title.

Note

Link Symmetry is configured at the master ODU only. The appropriate matching Link Symmetry is set at the slave ODU automatically. For example, if Link Symmetry is configured as **2 to 1** at the master ODU, then the slave ODU will be set automatically as **1 to 2**. In this example, the master-slave direction has double the capacity of the slave-master direction.

Procedures:

- Review the attributes (Table 100).
- Confirm that the Ethernet Link Status attributes are green and set to **Copper Link Up** or **Fiber Link Up**.

Table 100 System Status attributes

Attribute	Meaning
Link Name	The link name is allocated by the system administrator and is used to identify the equipment on the network. The link name attribute is limited to a maximum size of 63 ASCII characters.
Site Name	The site name is allocated by the system administrator and can be used as a generic scratch pad to describe the location of the equipment or any other equipment related notes. The site name attribute is limited to a maximum size of 63 ASCII characters.
Software Version	The version of PTP 650 software installed on the equipment.
Hardware Version	The PTP 650 hardware version. Formatted as "vvvv" where vvvv is the version of the printed circuit card
Regulatory Band	This is used by the system to constrain the wireless to operate within regulatory regime of a particular band and country. The license key provides the capability to operate in one or more regulatory bands. The Installation Wizard is used to choose one of those bands.
Elapsed Time Indicator	The elapsed time indicator attribute presents the total time in years, days, hours, minutes and seconds since the last system restart. The system can restart for several reasons, for example commanded reboot from the system reboot web page, or a power cycle of the equipment.
Main PSU Port Status	This indicates the current status of the Ethernet link to the PSU port. A state of "`Copper Link Up`" with a green background indicates that an Ethernet link is established. A state of "`Down`" with a red background indicates that the Ethernet link is not established.
Main PSU Port Speed and Duplex	The negotiated speed and duplex setting of the Ethernet link to the PSU port. The speed setting is specified in Mbps.

Attribute	Meaning
Aux Port Status	This indicates the current status of the Ethernet link to the Aux port. A state of "Copper Link Up" with a green background indicates that an Ethernet link is established. A state of "Down" with a red background indicates that the Ethernet link is not established.
Aux Port Speed and Duplex	The negotiated speed and duplex setting of the Ethernet link to the Aux port. The speed setting is specified in Mbps.
SFP Port Status	This indicates the current status of the Ethernet link to the SFP port. A state of "Copper Link Up" or "Fiber Link Up" with a green background indicates that an Ethernet link is established. A state of "Down" with a red background indicates that the Ethernet link is not established.
SFP Port Speed and Duplex	The negotiated speed and duplex setting of the Ethernet link to the PSU port. The speed setting is specified in Mbps.
MAC Address	The MAC Address of this unit.
Remote MAC Address	The MAC Address of the peer unit. If the link is down, this is set to "Not available".
Remote Internet Address	The Internet Address of the peer unit. To open the web interface of the peer unit, click on the hyperlink. If the link is down, this is set to "Not available". Depending on the settings of IP Version (Table 72) and IP Address Label (Table 71), this may be either an IPv4 or an IPv6 address.
Wireless Link Status	As the attribute name suggests it displays the current status of the wireless link. A state of "Up" on a green background indicates that a point-to-point link is established. A state of "Down" on a red background indicates that the wireless link is not established.
Maximum Transmit Power	The maximum transmit power that the local wireless unit is permitted to use to sustain a link.
Remote Maximum Transmit Power	The maximum transmit power that the remote wireless unit is permitted to use to sustain a link.
Transmit Power	The maximum, mean, minimum and latest measurements of Transmit Power (dBm). See System histograms on page 7-32.
Receive Power	The maximum, mean, minimum and latest measurements of Receive Power (dBm). See System histograms on page 7-32.

Attribute	Meaning
Vector Error	The maximum, mean, minimum and latest measurements of Vector Error (dB). See System histograms on page 7-32. Vector Error compares the received signals In phase / Quadrature (IQ) modulation characteristics to an ideal signal to determine the composite error vector magnitude. The expected range for Vector Error is approximately -2 dB (NLOS link operating at sensitivity limit on BPSK 0.67) to -33 dB (short LOS link running 256 QAM 0.83).
Link Loss	The maximum, mean, minimum and latest measurements of Link Loss (dB). See System histograms on page 7-32. The link loss is the total attenuation of the wireless signal between the two point-to-point units. The link loss calculation is presented below: $P_{ll} = P_{T_x} - P_{R_x} + g_{T_x} + g_{R_x}$ Where: P_{ll} = Link Loss (dB) P_{T_x} = Transmit power of the remote wireless unit (dBm) P_{R_x} = Received signal power at the local unit (dBm) g_{T_x}, g_{R_x} = Antenna gain at the remote and local units respectively (dBi). The antenna gain of the PTP 650 Series (23.5 dBi) is used unless one or both of the units is a Connectorized version. For connectorized ODUs, the link loss calculation is modified to allow for the increased antenna gains at each end of the link.
Transmit Data Rate	The maximum, mean, minimum and latest measurements of Transmit Data Rate (Mbps). See System histograms on page 7-32.
Receive Data Rate	The maximum, mean, minimum and latest measurements of Receive Data Rate (Mbps). See System histograms on page 7-32.
Link Capacity Variant	Indicates whether the installed license key is Lite, Mid or Full. When a link is established, this attribute shows the lower of the license keys at each end. For example, if this end is Full and the other end is Lite, it shows "Lite". To see the installed key, go to the Installation Wizard.

Attribute	Meaning
Link Capacity	The maximum aggregate data rate capacity available for user traffic, assuming the units have been connected using Gigabit Ethernet. The link capacity is variable and depends on the prevailing wireless conditions as well as the distance (range) between the two wireless units.
Transmit Modulation Mode	The modulation mode currently being used on the transmit channel.
Receive Modulation Mode	The modulation mode currently being used on the receive channel.
Link Symmetry	A ratio that expresses the division between transmit and receive time in the TDD frame. The first number in the ratio represents the time allowed for the transmit direction and the second number represents the time allowed for the receive direction.
Receive Modulation Mode Detail	The receive modulation mode in use. For a list of values and their meanings, see Table 101.
Range	The range between the PTP 650 Series ODUs. This is displayed in kilometers by default, but can be changed to miles by updating the Distance Units attribute to imperial, as described in Webpage Properties page on page 6-49.

Table 101 Receive Modulation Mode Detail values and meanings

Value	Meaning
Running At Maximum Receive Mode	The link is operating at maximum modulation mode in this channel and maximum throughput has been obtained.
Running At User-Configured Max Modulation Mode	The maximum modulation mode has been capped by the user and the link is operating at this cap.
Restricted Because Installation Is Armed	The Installation Wizard has been run and the unit is armed, forcing the link to operate in the lowest modulation mode. To remove this restriction, re-run the Installation Wizard to disarm the unit.
Restricted Because Of Byte Errors On The Wireless Link	The receiver has detected data errors on the radio and reduced the modulation mode accordingly. The radio may achieve a higher modulation mode as shown by the vector error, but there is some other error source, probably RF interference.
Restricted Because Channel Change Is In Progress	This is a transient event where the modulation mode is temporarily reduced during a channel change.

Value	Meaning
Limited By The Wireless Conditions	The radio is running at the maximum achievable modulation mode given the current wireless conditions shown by the vector error. The radio is capable of reaching a higher modulation mode if wireless conditions (vector error) improve.

Rebooting and logging out

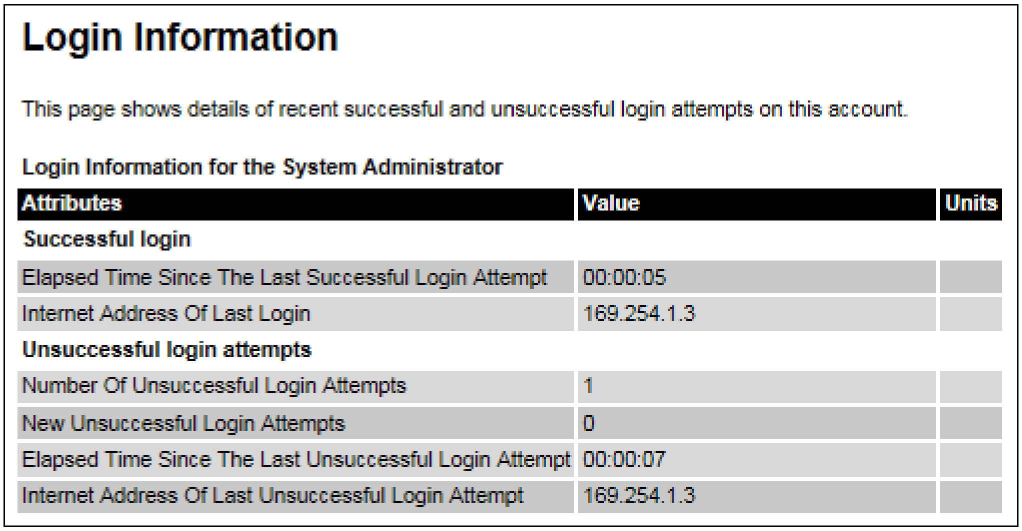
This section describes how to reboot the unit and log out of the web interface.

Login Information page

Menu option: **Management > Web > Login Information** (Figure 109).

Use this page to show recent successful and unsuccessful login attempts on this account.

Figure 109 Login Information page



Login Information

This page shows details of recent successful and unsuccessful login attempts on this account.

Login Information for the System Administrator

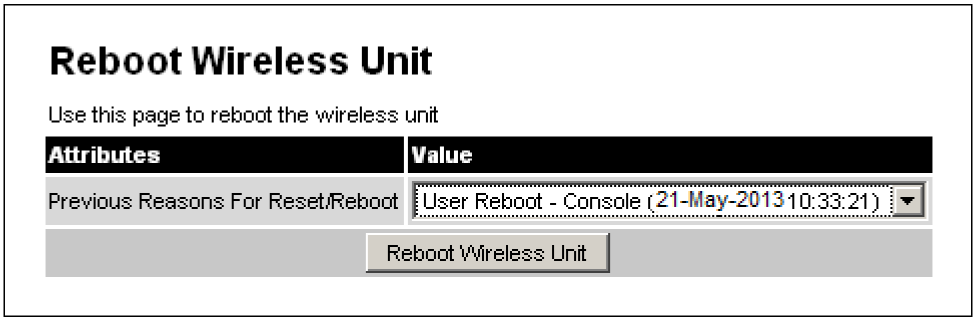
Attributes	Value	Units
Successful login		
Elapsed Time Since The Last Successful Login Attempt	00:00:05	
Internet Address Of Last Login	169.254.1.3	
Unsuccessful login attempts		
Number Of Unsuccessful Login Attempts	1	
New Unsuccessful Login Attempts	0	
Elapsed Time Since The Last Unsuccessful Login Attempt	00:00:07	
Internet Address Of Last Unsuccessful Login Attempt	169.254.1.3	

Reboot Wireless Unit page

Menu option: **System > Reboot** (Figure 110).

Use this page to reboot the ODU or view a list of previous reboot reasons.

Figure 110 Reboot Wireless Unit page



Reboot Wireless Unit

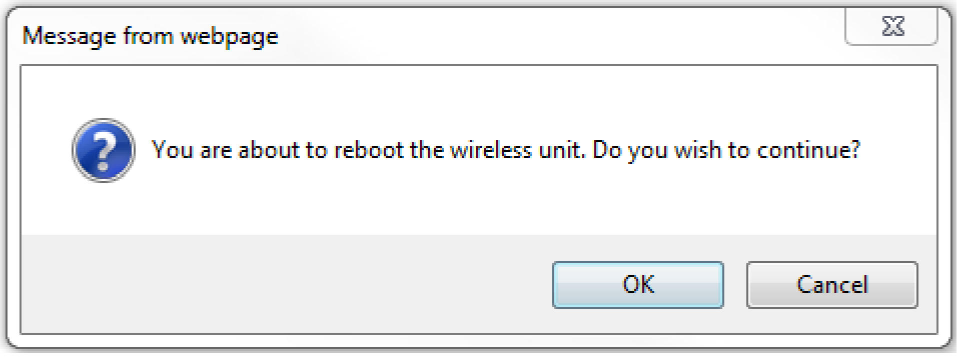
Use this page to reboot the wireless unit

Attributes	Value
Previous Reasons For Reset/Reboot	User Reboot - Console (21-May-2013 10:33:21)

Procedure:

- Use the drop-down list to view the Previous Reasons For Reset/Reboot.
- If a reboot is required:
  - o Click **Reboot Wireless Unit**. The Reboot Confirmation dialog is displayed (Figure 111).
  - o Click **OK**. The reboot progress message is displayed. On completion, the unit restarts.

Figure 111 Reboot confirmation pop up



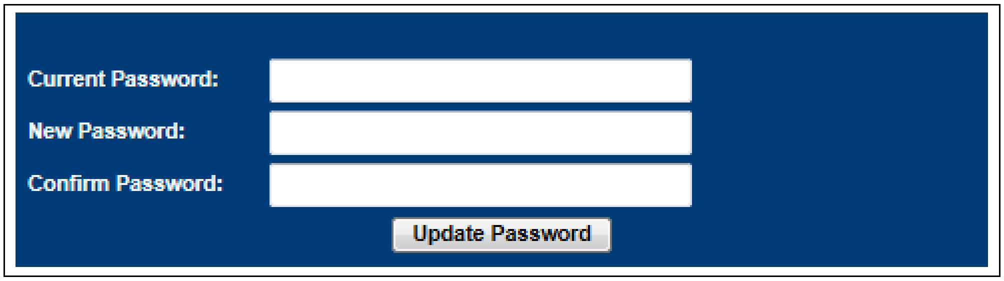
Message from webpage

You are about to reboot the wireless unit. Do you wish to continue?

Change Password page

Menu option: **Change Password** (Figure 112). Use this page to change a personal password.

Figure 112 Change Password page (System Administration example)



Current Password:

New Password:

Confirm Password:

Note

A security officer can change the passwords of other users using the User Accounts page, as described in Local User Accounts page on page 6-42.

Procedure:

- Enter and confirm the new password (the default is blank). The new password must comply with the complexity rules (Table 79).

Logging out

To maintain security, always log out at the end of a session: on the menu, click **Logout**.

The unit will log out automatically if there is no user activity for a set time, but this depends upon Auto Logout Period in the Webpage Properties page (Figure 78).

Alarms, alerts and messages

This section describes how to use alarms, alerts and syslog messages to monitor the status of a PTP 650 link.

Alarms

Whenever system alarms are outstanding, a yellow warning triangle is displayed on the navigation bar. The warning triangle is visible from all web pages.

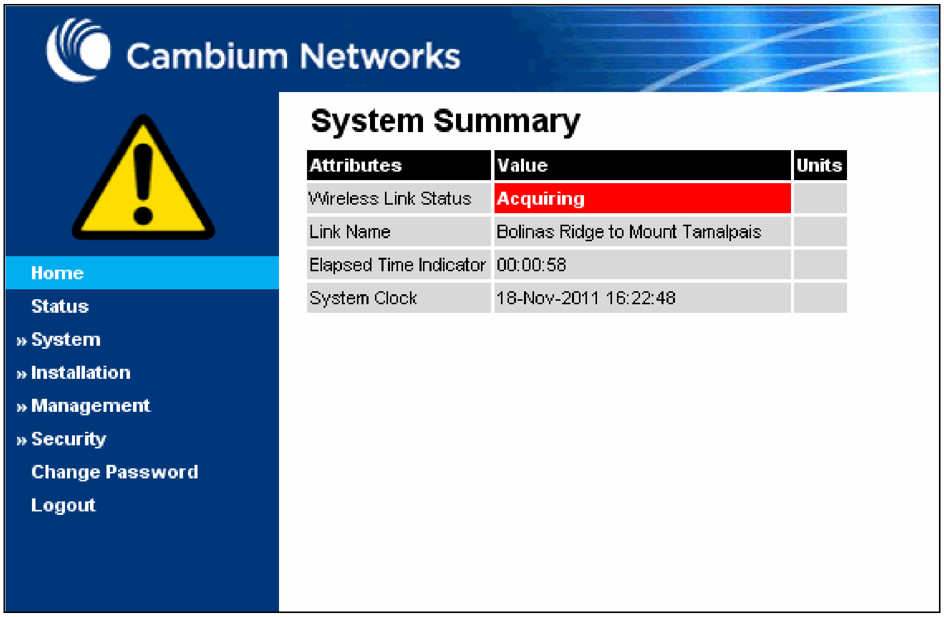
Procedure:

- Click the warning triangle (or menu option **Home**) to return to the System Summary page and view the alarms. If the warning triangle disappears when it is clicked, it indicates that the outstanding alarms have been cleared.

The example in Figure 113 shows the warning triangle in the navigation bar and an alarm displayed in the System Summary page. The alarms are defined in Table 102.

A change of state in most alarms generates an SNMP trap or an SMTP email alert.

Figure 113 Alarm warning triangle



System Summary

Attributes	Value	Units
Wireless Link Status	Acquiring	
Link Name	Bolinas Ridge to Mount Tamalpais	
Elapsed Time Indicator	00:00:58	
System Clock	18-Nov-2011 16:22:48	

Table 102 System alarms

Alarm	Meaning
Regulatory Band	The installed license key contains an invalid Regulatory Band. The wireless unit is prohibited from operating outside the regulated limits.
Install Status	Signaling was received with the wrong MAC address. It is very unusual to detect this, because units with wrongly configured Target MAC Address will normally fail to establish a wireless link. However, rare circumstances may establish a partial wireless link and detect this situation.
Install Arm State	A wireless unit is in installation mode. After installation, the wireless unit should be disarmed. This will increase the data-carrying capacity and stop the installation tone generator. The wireless link is disarmed from the "Installation" process, see Disarming the units on page 6-93.
Unit Out Of Calibration	The unit is out of calibration and must be returned to the factory using the RMA process for re-calibration.
Incompatible Regulatory Bands	The two linked units have different Regulatory Bands. To clear this alarm, obtain and install license keys for the correct country and select the same Regulatory Band at each end of the link.
Incompatible Master and Slave	The master and slave ends of the wireless link are different hardware products, or have different software versions. It is very unusual to detect this because incompatible units will normally fail to establish a wireless link. However, some combinations may establish a partial wireless link and detect this situation.
Main PSU Port Configuration Mismatch	Ethernet fragments (runt packets) have been detected when the PSU port is in full duplex. This indicates an auto-negotiation or forced configuration mismatch.
No Wireless Channel Available	Spectrum Management was unable to locate a suitable wireless channel to operate on.
SNTP Synchronization failed	SNTP has been enabled but the unit is unable to synchronize with the specified SNTP server.

Alarm	Meaning
Wireless Link Disabled Warning	The wireless link has been administratively disabled via the SNMP Interface. The wireless interface MIB-II ifAdminStatus attribute has been set to **DOWN**. To enable the Ethernet interface, set the ifAdminStatus attribute to **UP**.
Main PSU Port Disabled Warning	The PSU port link has been administratively disabled via the SNMP Interface.
Main PSU Port Status	The PSU port link is down. The most likely cause is that the unit has no Ethernet cable plugged into its Aux port.
SFP Error	A non-OK value indicates that the SFP link is down. There are two possible causes: • Either: the fiber link has been installed but disabled (because the license key does not include SFP support), • Or: the SFP link could not be established even though an SFP carrier was detected (due perhaps to a cabling fault or the link is disabled at the link partner).
SFP Port Configuration Mismatch	Ethernet fragments (runt packets) have been detected when the SFP port is in full duplex. This indicates an auto-negotiation or forced configuration mismatch.
SFP Port Disabled Warning	The SFP port link has been administratively disabled via the SNMP Interface.
SFP Port Status	The SFP port link is down. The most likely cause is that the unit has no Ethernet cable plugged into its SFP port.
Aux Port PoE Output Status	The Aux port link is down. The most likely cause is that the unit has no Ethernet cable plugged into its Aux port.
Aux Port Disabled Warning	The Aux port link has been administratively disabled via the SNMP Interface.
Aux Port Status	The Aux port link is down. The most likely cause is that the unit has no Ethernet cable plugged into its Aux port.
Link Mode Optimization Mismatch	The Master and Slave ODUs are configured to use different link mode optimization methods (one is set to IP and the other TDM).
Syslog Enabled/ Disabled Warning	The local log of event messages has been enabled or disabled.
Syslog Local Nearly Full	The local log of event messages is nearly full.

Alarm	Meaning
Syslog Local Wrapped	The local log of event messages is full and is now being overwritten by new messages.
Aux Port Configuration Mismatch	Ethernet fragments (runt packets) have been detected when the Aux port is in full duplex. This indicates an auto-negotiation or forced configuration mismatch.
Syslog Client Enabled/Disabled Warning	The local syslog client has been enabled or disabled.
Ethernet Bridging Status	"`Disabled`" means that the link has stopped bridging Ethernet frames because the Lowest Ethernet Modulation Mode is not being achieved or because the wireless link is down.
Remaining Full Capacity Time Trial	Time remaining on the full capability trial period. Activated when seven days or less of the trial period remain.
Capacity Variant Mismatch	The link ends are different capability variants, for example, one is Full and the other is Med.

Email alerts

The management agent can be configured to generate alerts by electronic mail when certain events occur. The alerts are defined in Table 103.

Table 103 Email alerts

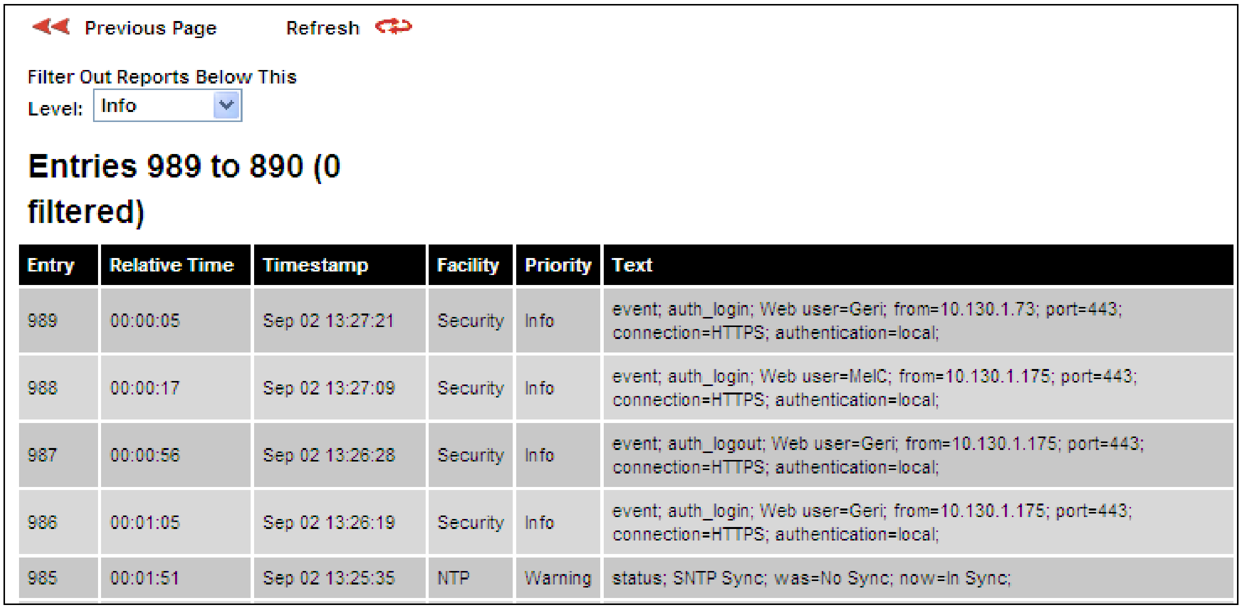
Alert	Meaning
Wireless Link Up Down	There has been a change in the status of the wireless link.
Channel Change	DFS has forced a change of channel.
DFS Impulse Interference	DFS has detected impulse interference.
Enabled Diagnostic Alarms	Diagnostic alarms have been enabled.
Main PSU Port Up Down	There has been a change in the status of the PSU data port.
Aux Port Up Down	There has been a change in the status of the Aux port.
SFP Port Up Down	There has been a change in the status of the SFP port.

Syslog page

Menu option: **Management > Syslog** (Figure 114).

Use this page to view the local log of event messages.

Figure 114 Syslog local log



Filter Out Reports Below This Level: Info

Entries 989 to 890 (0 filtered)

Entry	Relative Time	Timestamp	Facility	Priority	Text
989	00:00:05	Sep 02 13:27:21	Security	Info	event; auth_login; Web user=Geri; from=10.130.1.73; port=443; connection=HTTPS; authentication=local;
988	00:00:17	Sep 02 13:27:09	Security	Info	event; auth_login; Web user=MelC; from=10.130.1.175; port=443; connection=HTTPS; authentication=local;
987	00:00:56	Sep 02 13:26:28	Security	Info	event; auth_logout; Web user=Geri; from=10.130.1.175; port=443; connection=HTTPS; authentication=local;
986	00:01:05	Sep 02 13:26:19	Security	Info	event; auth_login; Web user=Geri; from=10.130.1.175; port=443; connection=HTTPS; authentication=local;
985	00:01:51	Sep 02 13:25:35	NTP	Warning	status; SNTP Sync; was=No Sync; now=In Sync;

Note

For more information about system logging, refer to:

- System logging (syslog) on page 1-32 describes the system logging feature.
- Syslog Configuration page on page 6-59 describes how to enable system logging.

Format of syslog server messages

PTP 650 generates syslog messages in this format:

```
SP = “ ” = %x20

CO = “:” = %x3A

SC = “;” = %x3B

LT = “<” = %x3C

GT = “>” = %x3E

syslog = pri header SP message

pri = LT “1”-“182” GT

header = timestamp SP hostname

timestamp = month SP days SP hours “:” minutes “:” seconds

month = “Jan”|“Feb”|“Mar”|“Apr”|“May”|“Jun”|
“Jul”|“Aug”|“Sep”|“Oct”|“Nov”|“Dec”

days = “ 1”-“31”

hours = “00”-“23”

minutes = seconds = “00”-“59”

hostname = “0.0.0.0”-“255.255.255.255”

message = “PTP650” CO SP (configuration | status | event)

configuration = “configuration” SC SP attribute-name SC SP (“Web
user”|“SNMP user”|“SNTP”) SC SP “was=” previous-value SC SP “now=”
new-value SC

status = “status” SC SP attribute-name SC SP “was=” previous-value SC
SP “now=” new-value SC

event = “event” SC SP identifier SC SP event-message-content SC
```

Configuration and status messages

Configuration and status messages contain all of the relevant attributes.

This is an example of a configuration message:

```
PTP650: configuration; IP Address; Web user; was=10.10.10.10;
now=169.254.1.1;
```

This is an example of a status message:

```
PTP650: status; Data Port Status; was=Down; now=Up;
```

Event messages

Event messages are listed in Table 104. Definition of abbreviations:

SC = ";"

SP = " "

This is an example of an event message:

```
PTP650: event; auth_login; web user=MarkT; from=169.254.1.1; port=80;
connection=HTTP; authentication=local;
```

Table 104 Event messages

Facility	Severity	Identifier	Message content
security(4)	warning(4)	auth_idle	"Web user=" user-name SC SP "from=" IP-address SC SP "port=" port-number SC SP "connection=" ("HTTP" | "HTTPS") SC SP "authentication=" ("local" | "RADIUS") SC
security(4)	info(6)	auth_login	
security(4)	warning(4)	auth_login_failed	
security(4)	warning(4)	auth_login_locked	
security(4)	info(6)	auth_logout	
kernel(0)	warning(4)	cold_start	"PTP wireless bridge has reinitialized, reason=" reset-reason SC
security(4)	warning(4)	License_update	"License Key updated" SC
syslog(5)	warning(4)	log_full	"Syslog local flash log is 90% full" SC
syslog(5)	warning(4)	log_wrap	"Syslog local flash log has wrapped" SC
security(4)	info(6)	radius_auth	"RADIUS user=" user-name SC SP "server " ("1" | "2") " at " IP-address SP "succeeded" SC
security(4)	warning(4)	radius_auth_fail	"RADIUS user=" user-name SC SP "server " ("1" | "2") " at " IP-address SP ("failed" | "succeeded" | "failed (no response)") SC
security(4)	alert(1)	resource_low	"Potential DoS attack on packet ingress " ("warning" | "cleared") SC
security(4)	warning(4)	sec_zeroize	"Critical Security Parameters (CSPs) zeroized" SC
local6(22)	warning(4)	snmpv3_asn1	"ASN.1 parse error" SC

Facility	Severity	Identifier	Message content
security(4)	warning(4)	snmpv3_auth	"Authentication failure" SC
local6(22)	warning(4)	snmpv3_decryption	"Decryption failure" SC
local6(22)	warning(4)	snmpv3_engine_id	"Unknown engine ID" SC
local6(22)	warning(4)	snmpv3_sec_level	"Unknown security level" SC
kernel(0)	warning(4)	sys_reboot	"System Reboot, reason=" reset-reason SC
security(4)	warning(4)	sys_software _upgrade	"Software upgraded from " software-version " to " software-version SC
local6(22)	warning(4)	telnet_idle	"Telnet user=" user-name SC SP "from=" IP-address SC SP "port=" port-number SC
local6(22)	info(6)	telnet_login	
local6(22)	warning(4)	telnet_login_failed	
local6(22)	info(6)	telnet_logout	
local6(22)	info(6)	tftp_complete	"TFTP software upgrade finished" SC
local6(22)	info(6)	tftp_failure	"TFTP software upgrade failed, reason=" reason SC
local6(22)	info(6)	tftp_start	"TFTP software upgrade started" SC
NTP(12)	info(6)	time_auth	"SNTP authentication succeeded at IP-address=" IP-address SC SP "port-number=" port SC
NTP(12)	warning(4)	time_auth_failed	"SNTP authentication failed at IP-address=" IP-address SC SP "port-number=" port SC
NTP(12)	warning(4)	time_conn_failed	"SNTP connection failed at IP-address=" IP-address SC SP "port-number=" port SC SP "reason=" reason SC

Spectrum management

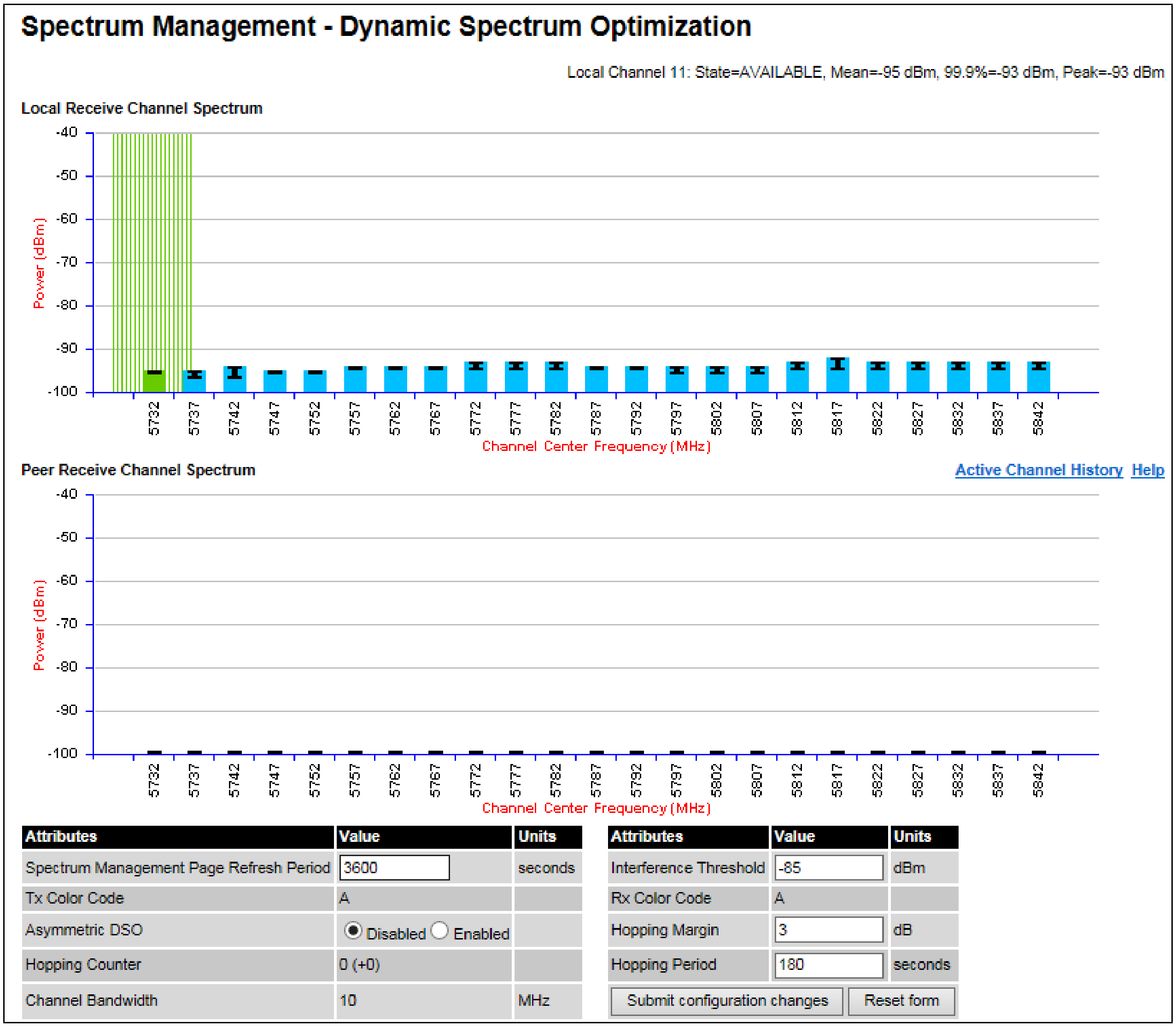
This section describes how to use the spectrum management pages to monitor the radio spectrum usage of the PTP 650 link.

Spectrum Management page

Menu option: **System > Spectrum Management** (Figure 115 and Figure 116).

Use this page to view and configure spectrum usage. The width of the vertical green bar represents the channel width (10 MHz illustrated).

Figure 115 Spectrum Management page (master unit)

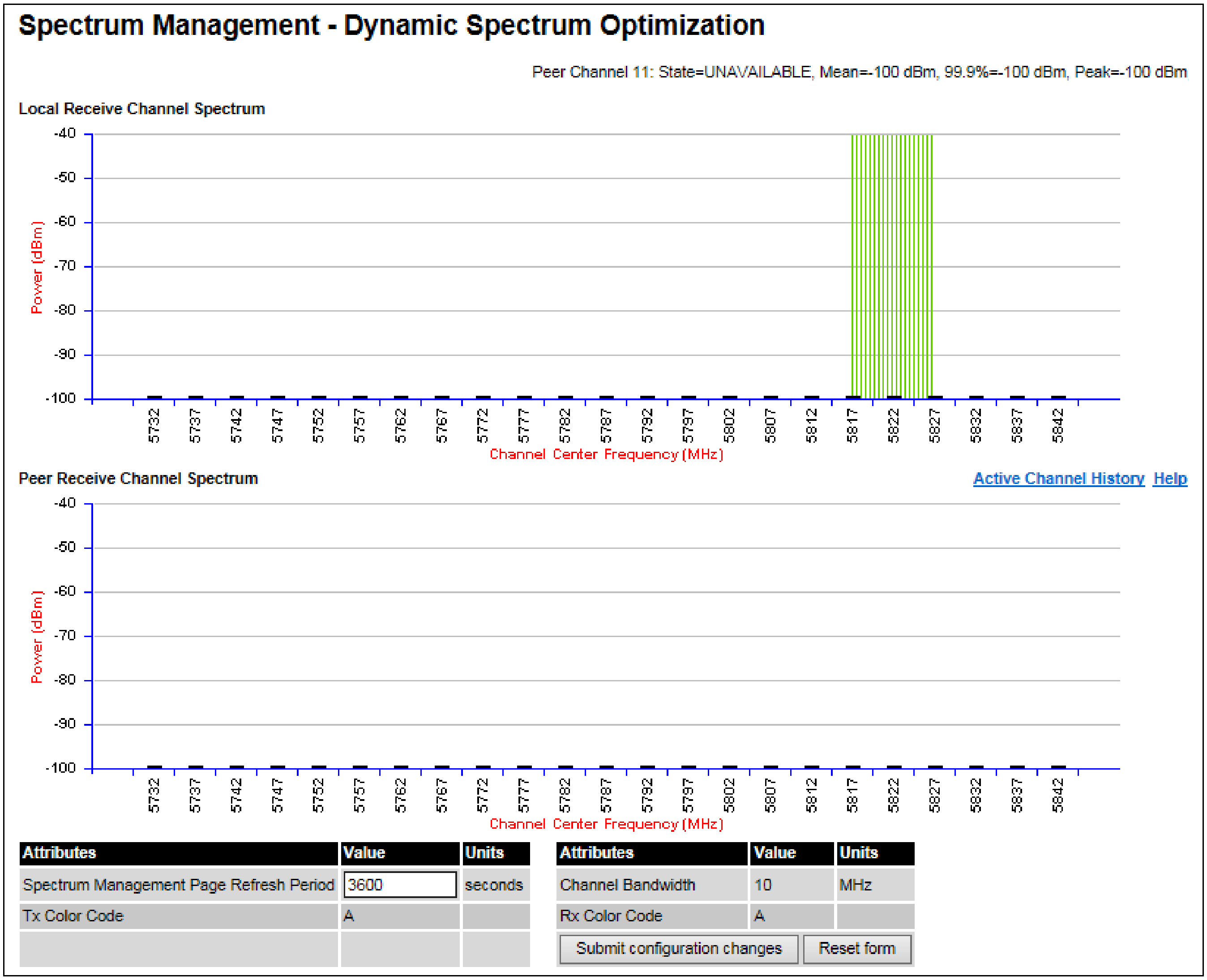


Spectrum Management - Dynamic Spectrum Optimization

Local Channel 11: State=AVAILABLE, Mean=-95 dBm, 99.9%=-93 dBm, Peak=-93 dBm

Attributes	Value	Units	Attributes	Value	Units
Spectrum Management Page Refresh Period	3600	seconds	Interference Threshold	-85	dBm
Tx Color Code	A		Rx Color Code	A	
Asymmetric DSO	● Disabled ○ Enabled		Hopping Margin	3	dB
Hopping Counter	0 (+0)		Hopping Period	180	seconds
Channel Bandwidth	10	MHz	Submit configuration changes	Reset form	

Figure 116 Spectrum Management page (slave unit)



Spectrum Management - Dynamic Spectrum Optimization

Peer Channel 11: State=UNAVAILABLE, Mean=-100 dBm, 99.9%=-100 dBm, Peak=-100 dBm

Attributes	Value	Units	Attributes	Value	Units
Spectrum Management Page Refresh Period	3600	seconds	Channel Bandwidth	10	MHz
Tx Color Code	A		Rx Color Code	A	
			Submit configuration changes	Reset form	

All spectrum management configuration changes are applied at the master ODU only. These changes are then sent from the master to the slave, so that both master and slave keep identical copies of spectrum management configuration. It is therefore possible to swap master and slave roles on an active PTP 650 link without modifying Spectrum Management configuration.

The default channelization can be modified by varying the lower center frequency attribute in the installation wizard, as described in Wireless Configuration page on page 6-15.

Note

Before attempting to improve the performance of the spectrum management algorithm by changing the default configuration, consult the Cambium Point-to-Point distributor or one of the system field support engineers.

Procedure:

- Review the configuration attributes (Table 105)
- Update the attributes as required. At the slave unit, only Page Refresh Period can be updated.
- To save changes, click Submit configuration changes.

Table 105 Spectrum Management attributes

Attribute	Meaning
Page Refresh Period	The page refreshes automatically according to the setting entered here (in seconds).
Hopping Margin	Spectrum Management uses this margin when making a channel hop decision. If the interference level of the target channel is lower than that of the active channel by at least the Hopping Margin, the link will hop to the target channel. The default setting is 3 dB in non-radar regions, or 10 dB in radar regions.
Asymmetric DSO	Only displayed in non-radar regions when DSO is enabled. The default configuration of symmetric operation constrains the link to operate symmetrically, using the same transmit and receive channels. When in symmetric mode the slave unit will always follow the master. If the master moves to a new channel the slave will hop to the same channel. When the Point-to-Point link is configured as an asymmetric link both the master and slave are free to select the best channel from their own set of local interference metrics.
Spectrum Management Control	Only displayed in radar regions. The options are **DFS** and **DFS with DSO**.
Hopping Period (not configurable)	The Spectrum Management algorithm evaluates the metrics every "Hopping Period" seconds (180 seconds by default) looking for a channel with lower levels of interference. If a better channel is located, Spectrum Management performs an automated channel hop. If SNMP or SMTP alerts are enabled an SNMP TRAP or an email alert is sent warning the system administrator of the channel change.
Hopping Counter	This is used to record the number of channel hops. The number in the (+) brackets indicates the number of channel changes since the last screen refresh.

Attribute	Meaning
Interference Threshold	Spectrum Management uses the interference threshold to perform instantaneous channel hops. If the measured interference on a channel exceeds the specified threshold, then DSO will instruct the wireless to immediately move to a better channel. If a better channel cannot be found the PTP 650 Series will continue to use the current active channel. (Default –85 dBm).
Channel Bandwidth (not configurable)	This shows the value of the variable channel bandwidth selected.

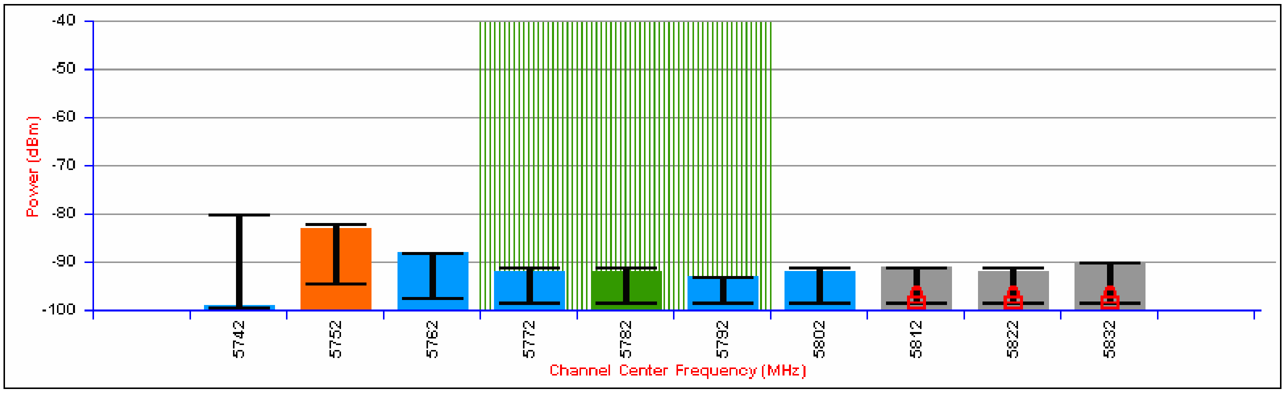
Interpreting the spectrum management plots

The Spectrum Management pages at the master and slave (Figure 115 and Figure 116) display two graphical plots:

- Local Receive Channel Spectrum
- Peer Receive Channel Spectrum

A more detailed example of one of these plots is shown in Figure 117.

Figure 117 Example spectrum management plot



Note

For more information, select the **Help** hyperlink from the Spectrum Management page.

X axis and Y axis

The X-axis shows a stylized view of the selectable wireless channels. Adjacent channels on the display have a 10 MHz overlap. Channels are displayed separately for clarity. The axis is labeled using the channel center frequencies in MHz.

The Y-axis shows the interference power levels from –100 to –40 dBm.

Channel states

The active channel (channel 5 in Figure 117) is always marked using hatched green and white lines. The width of the hatching is directly proportional the channel bandwidth spectral occupancy of the channel.

The individual channel metrics are displayed using a colored bar and an "I" bar. The colored bar represents the channel state (Table 106).

Table 106 Channel states represented in the spectrum management plot

Color	State	Meaning
Green	Active	The channel is currently in use, hosting the Point-to-Point wireless link.
Orange	Interference	The channel has interference above the interference threshold.
Blue	Available	The channel has an interference level below the interference threshold and is considered by the Spectrum Management algorithm suitable for hosting the Point-to-Point link.
Grey	Barred	The system administrator has barred this channel from use. For improved visibility, an additional red "lock" symbol is used to indicate that a channel is barred.

Key metrics

The “I” bar and top of the colored bar represent three key metrics (Table 107). The vertical part of the “I” bar represents the statistical spread between the peak and the mean of the statistical distribution.

Table 107 Key metrics represented in the spectrum management plot

Metric	Description	How represented
Peak of Means	The largest mean interference measurement encountered during the quantization period. The peak of means is useful for detecting slightly longer duration spikes in the interference environment.	Upper horizontal bar.
Mean of Means	The arithmetic mean of the measured means during a quantization period. The mean of means is a coarse measure of signal interference and gives an indication of the average interference level measured during the quantization period. The metric is not very good at predicting intermittent interference and is included to show the spread between the Mean of Means, the 99.9% Percentile and the Peak of Means.	Lower horizontal bar.
99.9% Percentile of the Means	The value of mean interference measurement which 99.9% of all mean measurements fall below, during the quantization period. The 99.9% percentile metric is useful for detecting short duration repetitive interference that by its very nature has a minimal effect of the mean of means.	Top of the colored bar.

Note

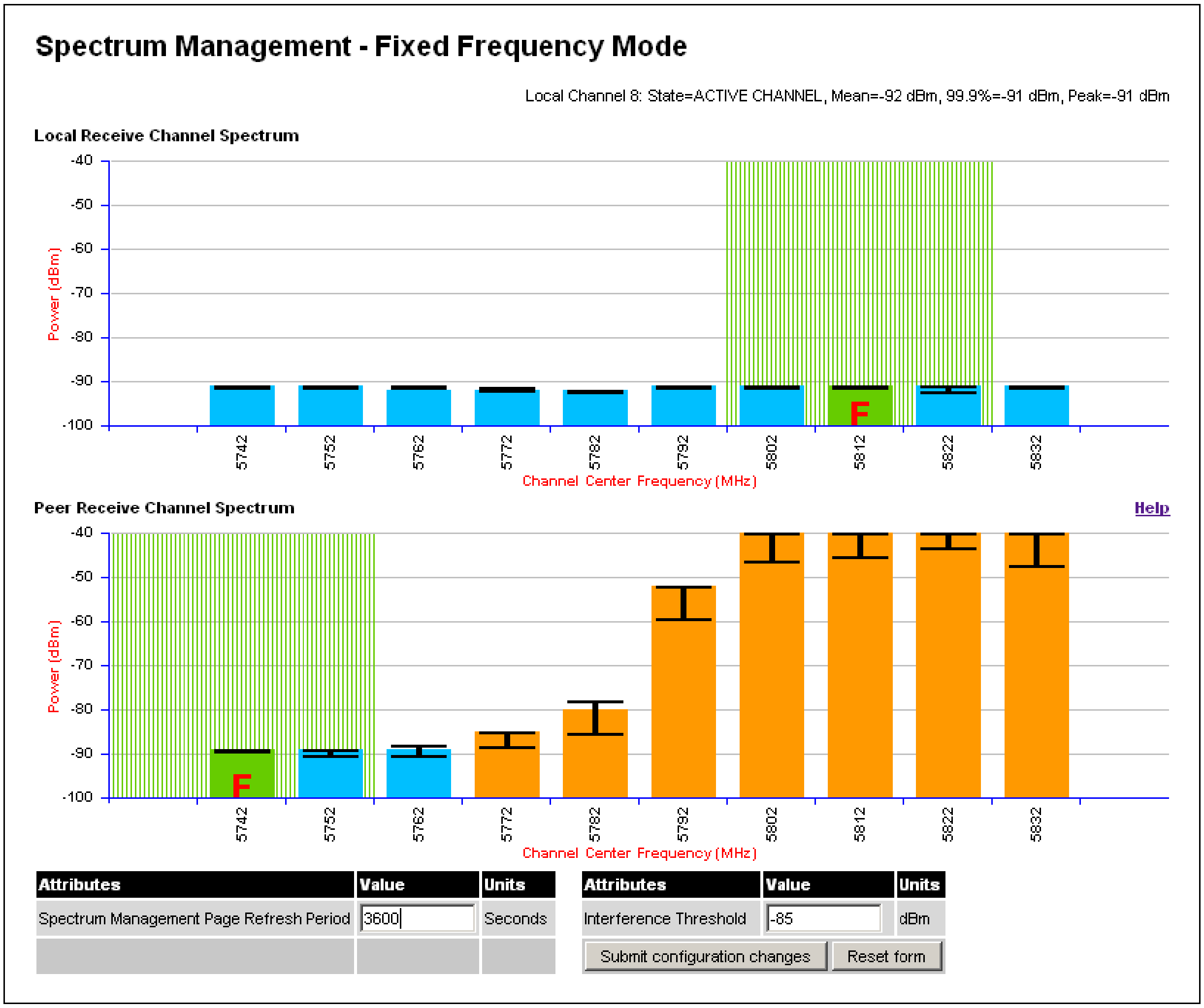
The arithmetic mean is the true power mean and not the mean of the values expressed in dBm.

Spectrum Management uses the 99.9% Percentile as the prime interference measurement. All subsequent references to interference level refer to this percentile measurement.

Spectrum management in fixed frequency mode

When the link is operating in fixed frequency mode, the Spectrum Management page uses two visual cues (Figure 118). The main page title has the "`Fixed Frequency Mode`" suffix and the selected channels are identified by a red capital "F".

Figure 118 Spectrum Management Fixed Frequency Mode page



Spectrum Management - Fixed Frequency Mode

Local Channel 8: State=ACTIVE CHANNEL, Mean=-92 dBm, 99.9%=-91 dBm, Peak=-91 dBm

Attributes	Value	Units
Spectrum Management Page Refresh Period	3600	Seconds

Attributes	Value	Units
Interference Threshold	-85	dBm

Channel barring is disabled in fixed frequency mode; it is not required as dynamic channel hopping is prohibited in this mode.

The only controls available to the master are the Page Refresh Period and Interference Threshold attributes. They will have no effect on the operation of the wireless link and will only effect the generation of the channel spectrum graphics.

The active channel history menu is removed in this mode of operation, as channel hopping is prohibited.

Spectrum management in radar avoidance mode

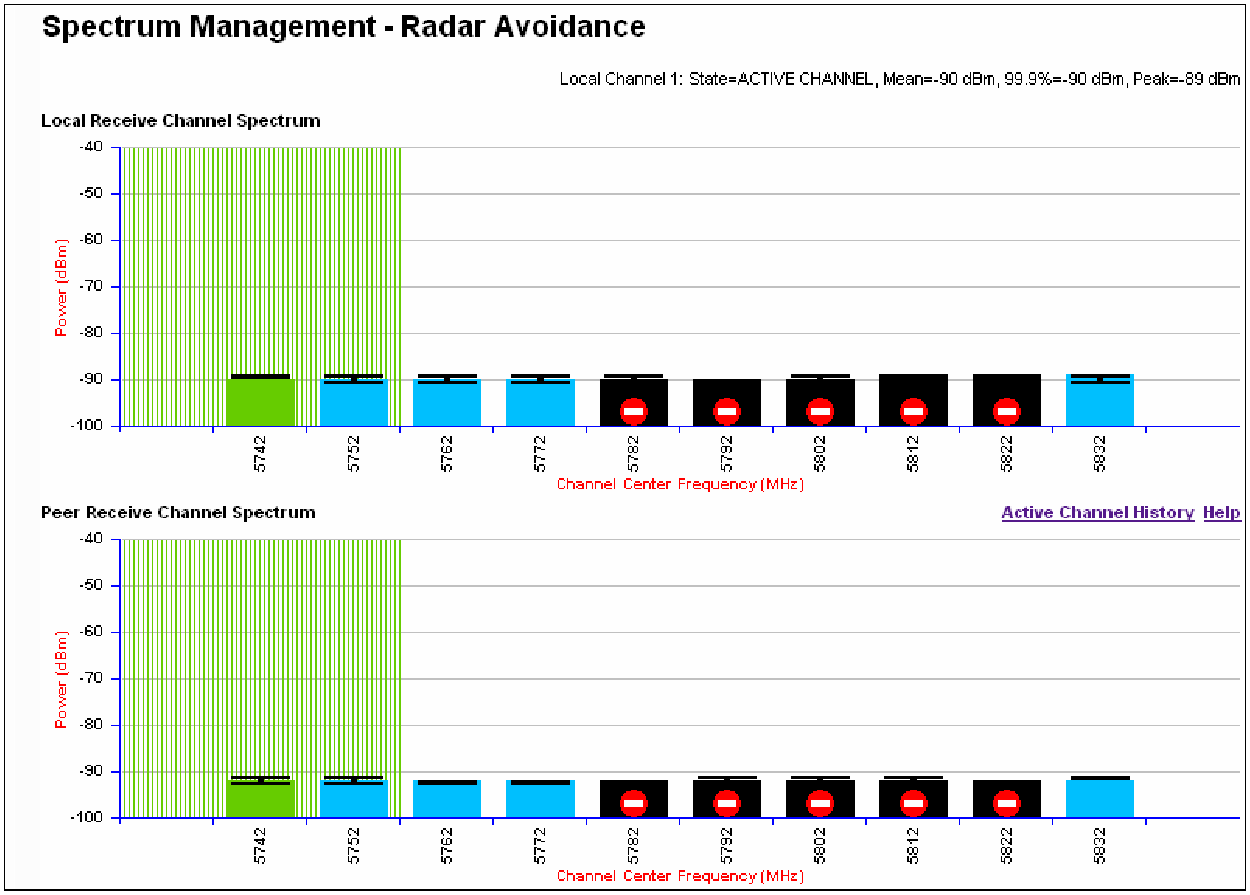
When the link is operating in radar avoidance mode, the Spectrum Management page (Figure 119 and Figure 120) contains the following additional information:

- The main page title has the "`Radar Avoidance`" suffix.
- The only controls available to the master are the Interference Threshold attribute. This has no effect on the operation of the wireless link and will only affect the generation of the channel spectrum graphics.
- Extra color coding of the interference histogram is provided (Table 108).

When operating with RTTT (Road transport and Traffic Telematics) Avoidance enabled or other regulatory restrictions on channel usage, the page contains the following additional information:

- All channels marked with a "no entry" symbol with their associated statistics colored black are the prohibited channels. These channels are never used to host the wireless link, but CAC measurements are still taken so that adjacent channel biases can be calculated correctly and so the user can see if other equipment is in use.

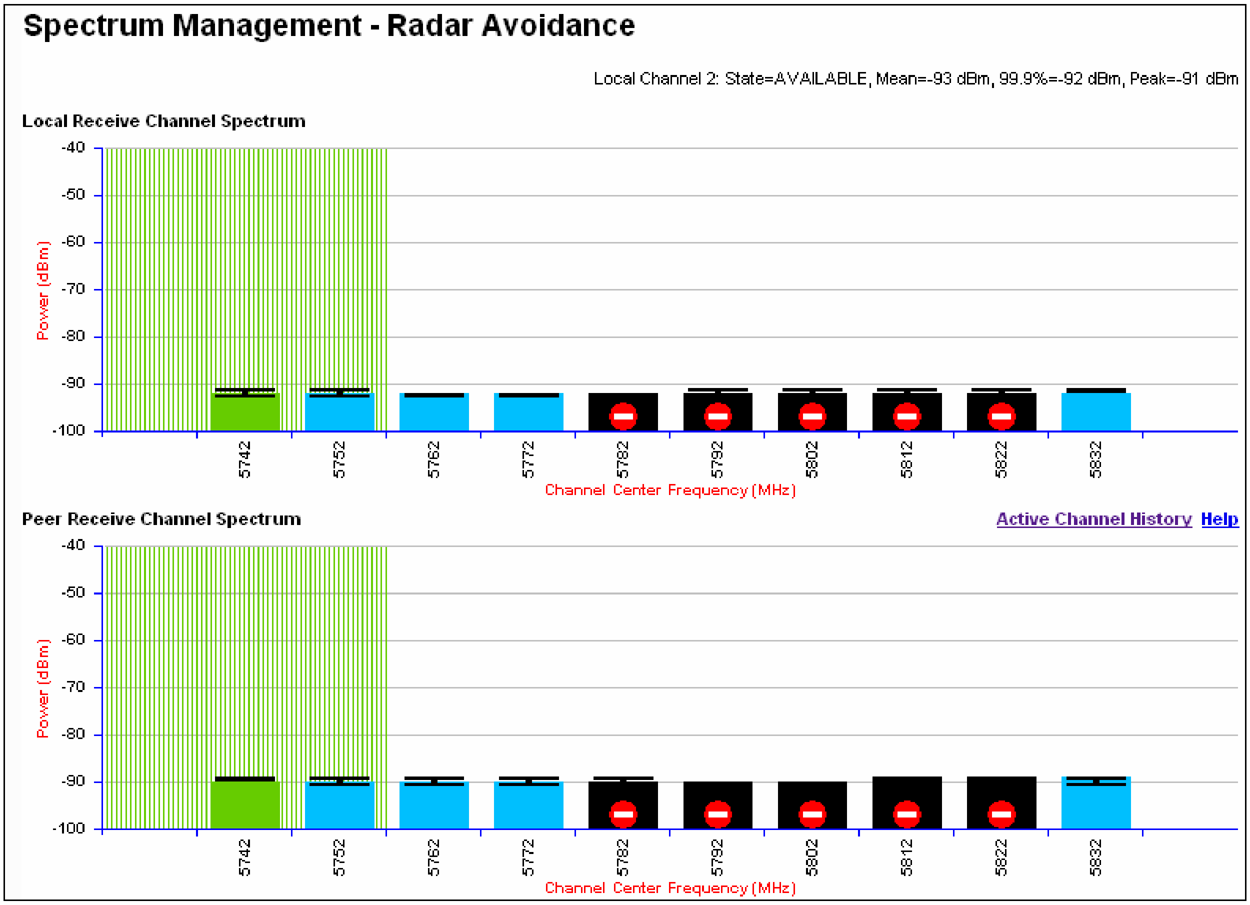
Figure 119 Spectrum Management page with radar avoidance - master



Spectrum Management - Radar Avoidance

Local Channel 1: State=ACTIVE CHANNEL, Mean=-90 dBm, 99.9%=-90 dBm, Peak=-89 dBm

Figure 120 Spectrum Management page with radar avoidance - slave



Spectrum Management - Radar Avoidance

Local Channel 2: State=AVAILABLE, Mean=-93 dBm, 99.9%=-92 dBm, Peak=-91 dBm

Table 108 Channel states in the spectrum management plot (radar avoidance)

Color	State and color	Meaning
Green	Active	This channel is currently in use hosting the Point-to-Point wireless link.
Orange	Interference	This channel has interference above the interference threshold
Blue	Available	This channel has an interference level below the interference threshold and is considered by the Spectrum Management algorithm suitable for hosting the Point-to-Point link
Dark grey	Barred	The system administrator has barred this channel from use. Because the low signal levels encountered when a unit is powered up in a laboratory environment prior to installation (which makes the grey of the channel bar difficult to see). An additional red “lock” symbol is used to indicate that a channel is barred.

Color	State and color	Meaning
Light grey	Unavailable	This channel needs to be monitored for one minute and found free of radar signal before it can be used for transmitting.
Red	Radar Detected	Impulsive Radar Interference has been detected on this channel and the channel is unavailable for 30 minutes. At the end of the 30 minute period a Channel Availability Check is required to demonstrate no radar signals remain on this channel before it can be used for the radio link.
Black	Region Bar	This channel has been barred from use by the local region regulator

Viewing the active channel history

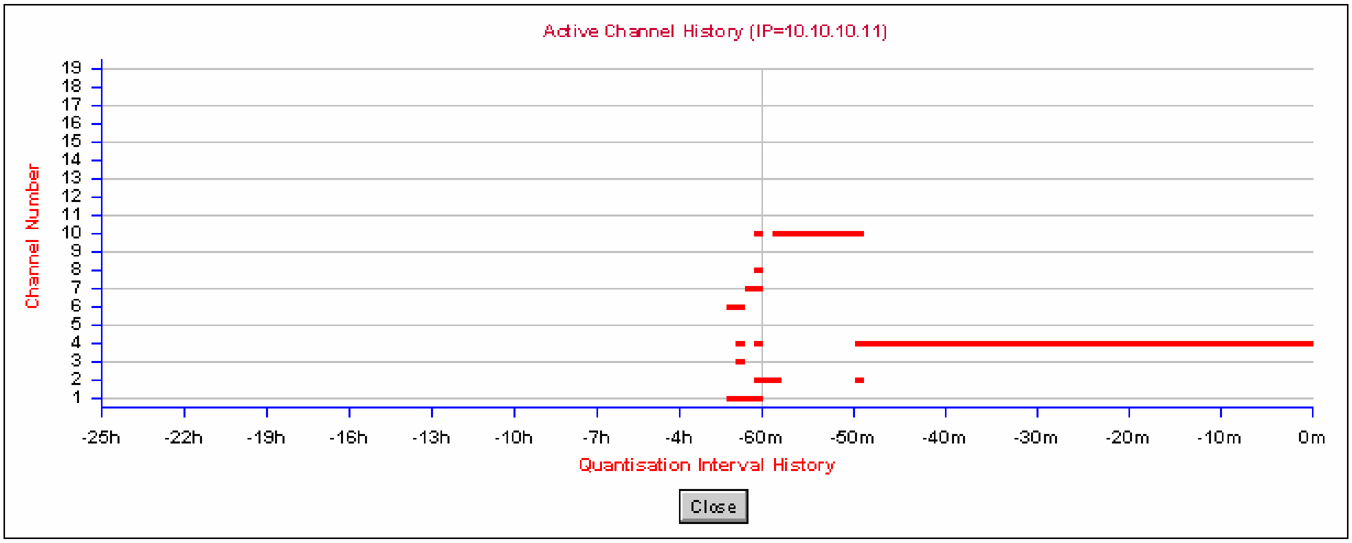
Use this procedure to view the active channel history. This is a time series display of the channels used by the PTP 650 Series over the last 25 hours.

Procedure:

- Select the **Active Channel History** hyperlink from the Spectrum Management page.

An example of the active channel history display is shown in Figure 121. Where there are parallel entries on the display this signifies that the wireless link occupied this channel during the measurement period. The measurement periods are one minute (from zero to sixty minutes) and twenty minutes from (60 minutes to twenty five hours).

Figure 121 Active channel history screen



Viewing historic spectrum management metrics

Use this procedure to view the results of previous measurement quantization periods from both the master and slave Spectrum Management pages.

Procedure:

- Hold down the shift key and click the appropriate channel on the Local Receive Channel Separation plot. The time series plot is displayed (Figure 122). This plot displays the results of all previous measurement quantization periods, up to a maximum of 132 periods. The colored lines represent interference measurements (Table 109).

Figure 122 Spectrum management time series plot

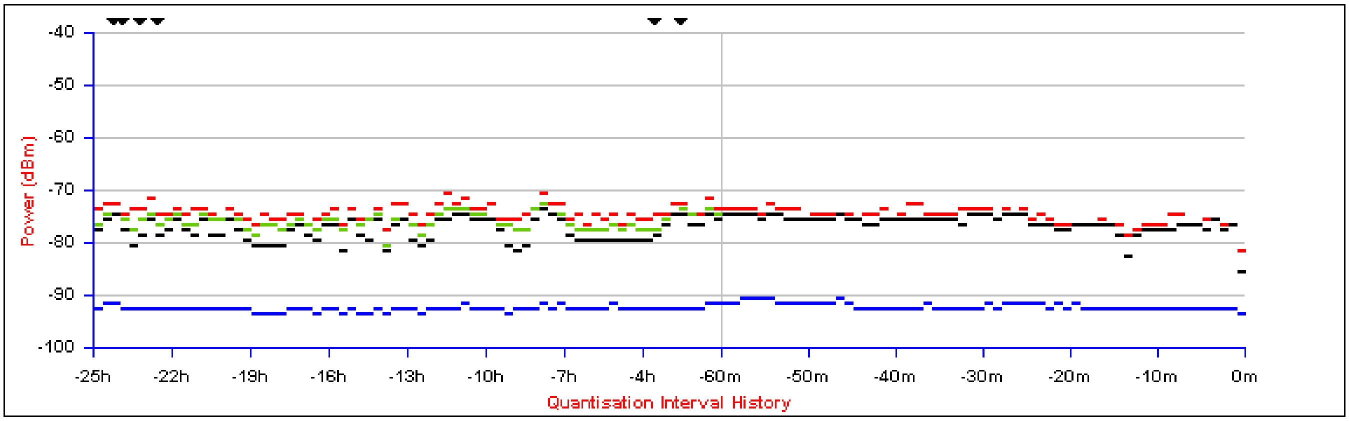


Table 109 Interference represented in the time series plot

Color	Meaning
GREEN	Peak of Means interference measurement
BLACK	99.9% percentile of means interference measurement
BLUE	Mean of Means interference measurement

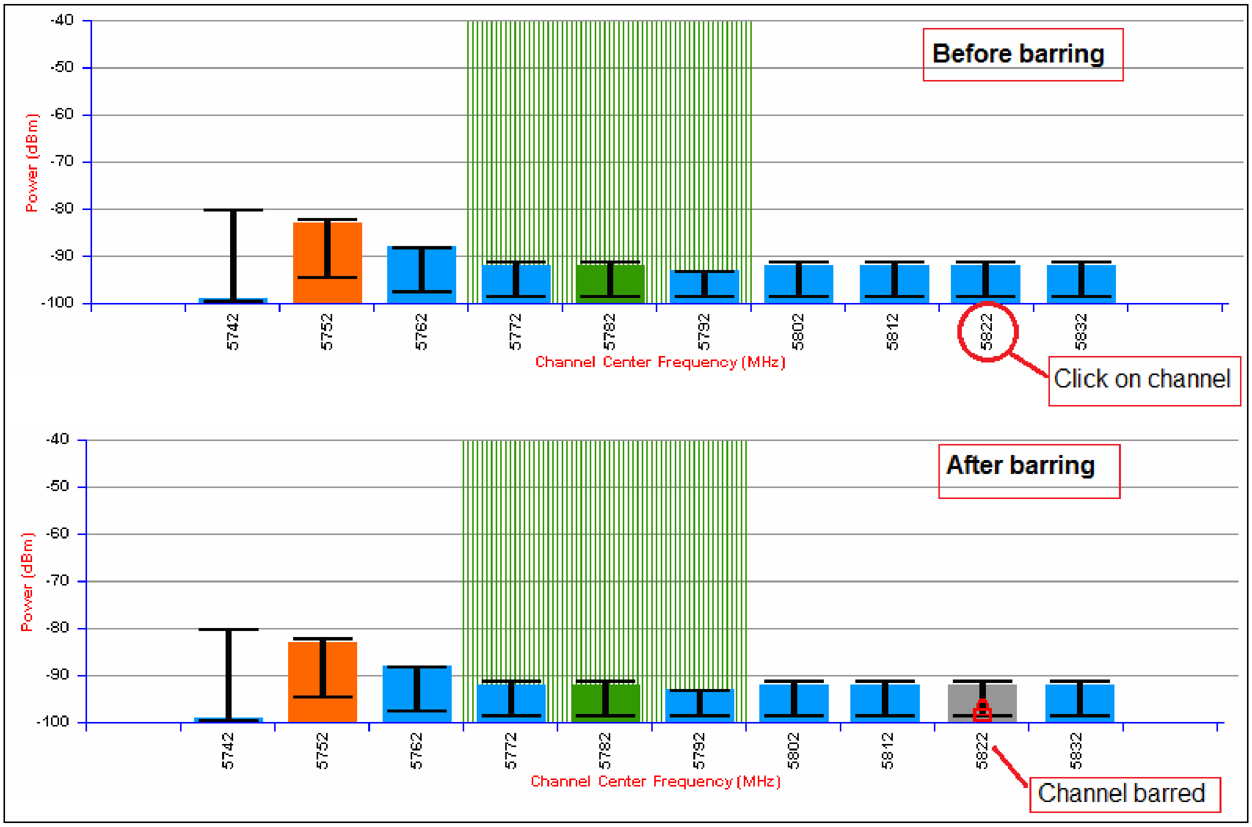
Barring channels

To comply with FCC rules, bar any channels that may interfere with TDWR radars. This must be done before the units are allowed to radiate on site. The system designer will have provided a list of any affected channels, based on the instructions in Avoidance of weather radars (USA only) on page 3-20.

Procedure:

- Log into the master unit.
- Select menu option **System > Spectrum Management**. The Spectrum Management page is displayed.
- Click on the appropriate channel center frequencies on the Local or Peer channel spectrum plots. The example in Figure 123 shows how to bar one channel (5822 MHz).
- When the confirmation dialog is displayed, click **OK**.

Figure 123 Barring a channel



System statistics

This section describes how to use the system statistics pages to manage the performance of the PTP 650 link, use the following web pages:

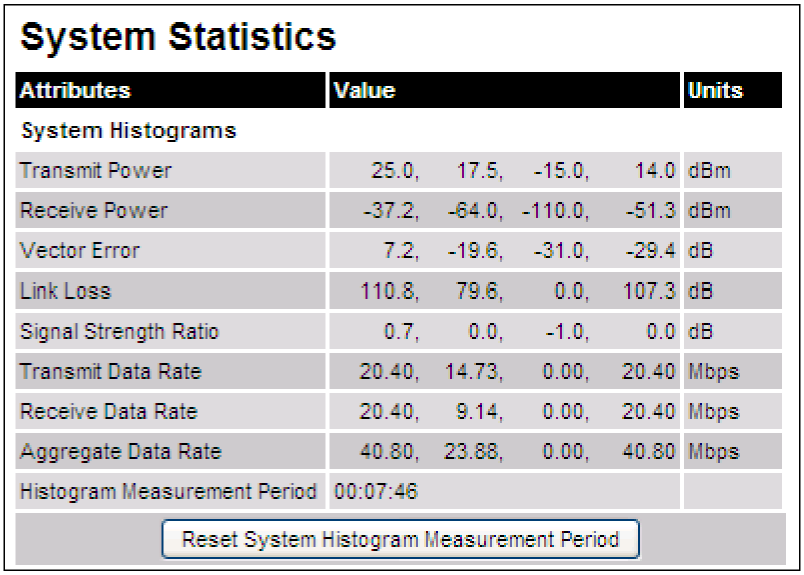
System Statistics page

Menu option: **System > Statistics**. Use this page to check system statistics.

System histograms

The System Histograms section of the System Statistics page (Figure 124) contains eight diagnostic attributes that are presented as arrays of four elements (Table 110).

Figure 124 System Histograms section of the System Statistics page



System Statistics

Attributes	Value	Units
System Histograms		
Transmit Power	25.0, 17.5, -15.0, 14.0	dBm
Receive Power	-37.2, -64.0, -110.0, -51.3	dBm
Vector Error	7.2, -19.6, -31.0, -29.4	dB
Link Loss	110.8, 79.6, 0.0, 107.3	dB
Signal Strength Ratio	0.7, 0.0, -1.0, 0.0	dB
Transmit Data Rate	20.40, 14.73, 0.00, 20.40	Mbps
Receive Data Rate	20.40, 9.14, 0.00, 20.40	Mbps
Aggregate Data Rate	40.80, 23.88, 0.00, 40.80	Mbps
Histogram Measurement Period	00:07:46	

The element arrays represent the following:

- Max: The maximum value measured over the last hour.
- Mean: The mean of a set of values recorded at one second intervals over the last hour.
- Min: The minimum value measured over the last hour.
- Latest: The latest value measured.

The values are calculated over the time that has elapsed since the link was established or since the measurement period was reset.

Note

Use the Diagnostics Plotter page on page 7-42 to plot these attributes against time. Use the Generate Downloadable Diagnostics page on page 7-43 to extract historical data for these attributes to a CSV file.

Procedure:

- To reset and restart measurement, click **Reset System Histograms and Measurement Period**.

Table 110 System Histogram attributes in the System Statistics page

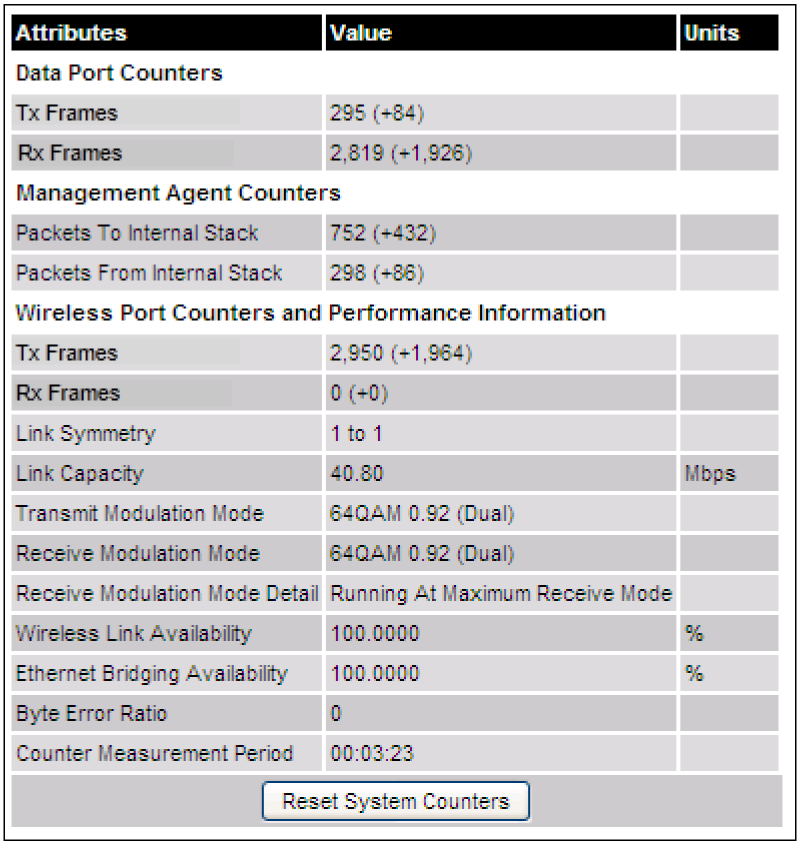
Attribute	Meaning
Transmit Power	The transmit power histogram, calculated over a one hour period.
Receive Power	The receive power histogram, calculated over a one hour period.
Vector Error	The vector error measurement compares (over a one hour period) the received signal IQ modulation characteristics to an ideal signal to determine the composite vector error magnitude.
Link Loss	Link loss calculated (over a one hour period) as follows: Peer_Tx_Power (dBm) – Local_Rx_Power (dBm) + 2 x Antenna_Pattern (dBi)
Signal Strength Ratio	The Signal Strength Ratio (calculated over a one hour period) is: Power received by the vertical antenna input (dB) ÷ Power received by the horizontal antenna input (dB) This ratio is presented as: max, mean, min, and latest. The max, min and latest are true instantaneous measurements; the mean is the mean of a set of one second means. Signal Strength Ratio is an aid to debugging a link. If it has a large positive or negative value then investigate the following potential problems: • An antenna coaxial lead may be disconnected. • When spatial diversity is employed, the antenna with the lower value may be pointing in the wrong direction. • When a dual polar antenna is deployed, the antenna may be directed using a side lobe rather than the main lobe. When there is a reflection from water on the link and spatial diversity is employed, then one expects large, slow swings in Signal Strength Ratio . This indicates the antenna system is doing exactly as intended.

Attribute	Meaning
Transmit, Receive and Aggregate Data Rates	The data rates in the transmit direction, the receive direction and in both directions, expressed in Mbps (max, mean, min, and latest). The max, min and latest are true instantaneous measurements. The mean is the mean of a set of one second means.
Histogram Measurement Period	The time over which the system histograms were collected.

System counters

The System Counters section of the System Statistics page (Figure 125) contains Data Port Counters (Table 111), Management Agent Counters (Table 112) and Wireless Port Counters and Performance Information (Table 113).

Figure 125 System Counters section of the System Statistics page



Attributes	Value	Units
Data Port Counters		
Tx Frames	295 (+84)	
Rx Frames	2,819 (+1,926)	
Management Agent Counters		
Packets To Internal Stack	752 (+432)	
Packets From Internal Stack	298 (+86)	
Wireless Port Counters and Performance Information		
Tx Frames	2,950 (+1,964)	
Rx Frames	0 (+0)	
Link Symmetry	1 to 1	
Link Capacity	40.80	Mbps
Transmit Modulation Mode	64QAM 0.92 (Dual)	
Receive Modulation Mode	64QAM 0.92 (Dual)	
Receive Modulation Mode Detail	Running At Maximum Receive Mode	
Wireless Link Availability	100.0000	%
Ethernet Bridging Availability	100.0000	%
Byte Error Ratio	0	
Counter Measurement Period	00:03:23	

Procedure:

- To reset all system counters to zero, click **Reset System Counters**.

The packet counter attributes each contain a number in parentheses; this shows the number of packets received since the last page refresh.

Table 111 Data Port Counters

Attribute	Meaning
Tx Frames	The total number of good frames the bridge has sent for transmission by the local Ethernet interface.
Rx Frames	The total number of good frames the bridge has received from transmission by the remote Ethernet interface.

Table 112 Management Agent Counters

Attribute	Meaning
Packets To Internal Stack	The total number of good packets the bridge has transmitted to the internal stack (for example, ARP, PING and HTTP requests).
Packets From Internal Stack	The total number of good packets the bridge has received from the internal stack (ARP responses, PING replies, HTTP responses).

Table 113 Wireless Port Counters and Performance Information

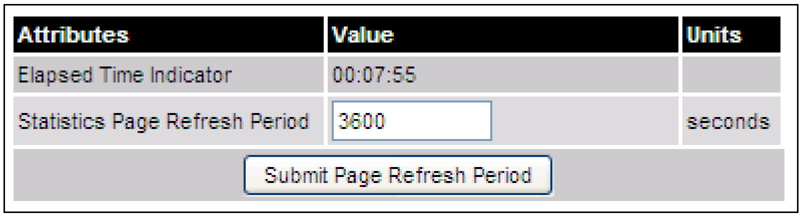
Attribute	Meaning
Tx Frames	Total number of good frames the bridge has sent for transmission by the wireless interface.
Rx Frames	Total number of good frames the bridge has received from the wireless interface.
Link Symmetry	Ratio between transmit and receive time in the TDD frame. The first number is the time allowed for the transmit direction and the second number is the time allowed for the receive direction.
Link Capacity	The maximum aggregate data capacity available for user traffic under the current radio link conditions, assuming the units have been connected using Gigabit Ethernet. The sum of the displayed Transmit and Receive data rates may be lower than this figure if the link is not fully loaded by the current traffic profile.
Transmit Modulation Mode	The modulation mode currently being used on the transmit channel. The number in brackets after the modulation mode and coding rate string is the effective data rate available to all MAC layer protocols.

Attribute	Meaning
Receive Modulation Mode	The modulation mode currently being used on the receive channel. The number in brackets after the modulation mode and coding rate string is the effective data rate available to all MAC layer protocols.
Receive Modulation Mode Detail	The receive modulation mode in use. For a list of values and their meanings, see Table 101.
Wireless Link Availability	Wireless link availability calculated since the last system counters reset.
Ethernet Bridging Availability	Link availability for bridging Ethernet traffic calculated since the last reset of the system counters. This is the percentage of time in which the Ethernet Bridging Status attribute has been set to "`Enabled`".
Byte Error Ratio	The ratio of detected Byte errors to the total number of bytes since the last system reboot. This measurement is made continually using null frames when there is no user data to transport.
Counter Measurement Period	The time over which the system counters were collected.

Other attributes

The bottom section of the System Statistics page (Figure 126) contains two attributes (Table 114).

Figure 126 Other attributes section of the System Statistics page



Attributes	Value	Units
Elapsed Time Indicator	00:07:55	
Statistics Page Refresh Period	3600	seconds

Procedure:

- After updating the Statistics Page Refresh Period field, click **Submit Page Refresh Period**.

Table 114 Other attributes in the System Statistics page

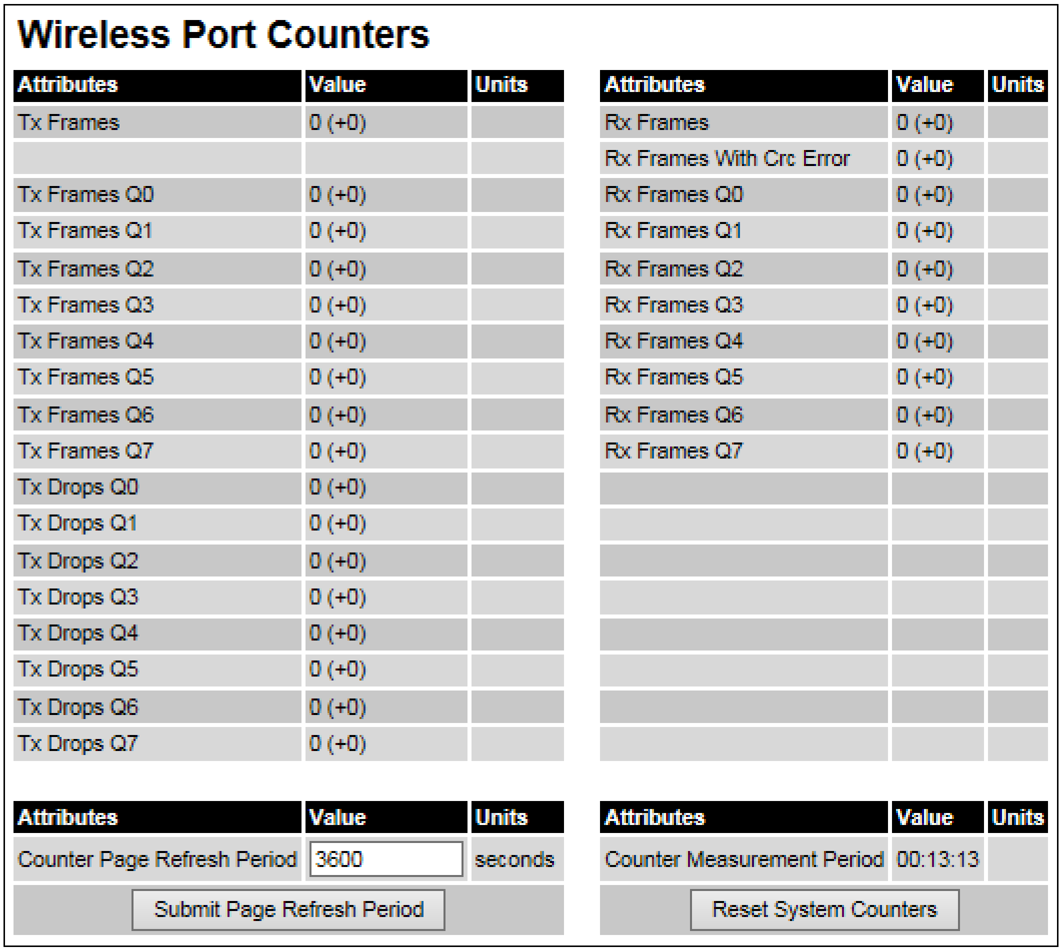
Attribute	Meaning
Elapsed Time Indicator	Elapsed time since the last system reboot.
Statistics Page Refresh Period	The statistics page refreshes automatically according to the setting entered here (in seconds).

Wireless Port Counters page

Menu option: **System > Statistics > Wireless Port Counters** (Figure 127).

Use this page to check the Ethernet performance of the wireless bridge.

Figure 127 Wireless Port Counters page



Wireless Port Counters

Attributes	Value	Units	Attributes	Value	Units
Tx Frames	0 (+0)		Rx Frames	0 (+0)	
			Rx Frames With Crc Error	0 (+0)	
Tx Frames Q0	0 (+0)		Rx Frames Q0	0 (+0)	
Tx Frames Q1	0 (+0)		Rx Frames Q1	0 (+0)	
Tx Frames Q2	0 (+0)		Rx Frames Q2	0 (+0)	
Tx Frames Q3	0 (+0)		Rx Frames Q3	0 (+0)	
Tx Frames Q4	0 (+0)		Rx Frames Q4	0 (+0)	
Tx Frames Q5	0 (+0)		Rx Frames Q5	0 (+0)	
Tx Frames Q6	0 (+0)		Rx Frames Q6	0 (+0)	
Tx Frames Q7	0 (+0)		Rx Frames Q7	0 (+0)	
Tx Drops Q0	0 (+0)				
Tx Drops Q1	0 (+0)				
Tx Drops Q2	0 (+0)				
Tx Drops Q3	0 (+0)				
Tx Drops Q4	0 (+0)				
Tx Drops Q5	0 (+0)				
Tx Drops Q6	0 (+0)				
Tx Drops Q7	0 (+0)				

Attributes	Value	Units	Attributes	Value	Units
Counter Page Refresh Period	3600	seconds	Counter Measurement Period	00:13:13	

Procedure:

- Review the attributes (Table 115).
- To change the refresh period, update the Counter Page Refresh Period attribute and click **Submit Page Refresh Period**.
- To reset all counters to zero, click **Reset System Counters**.

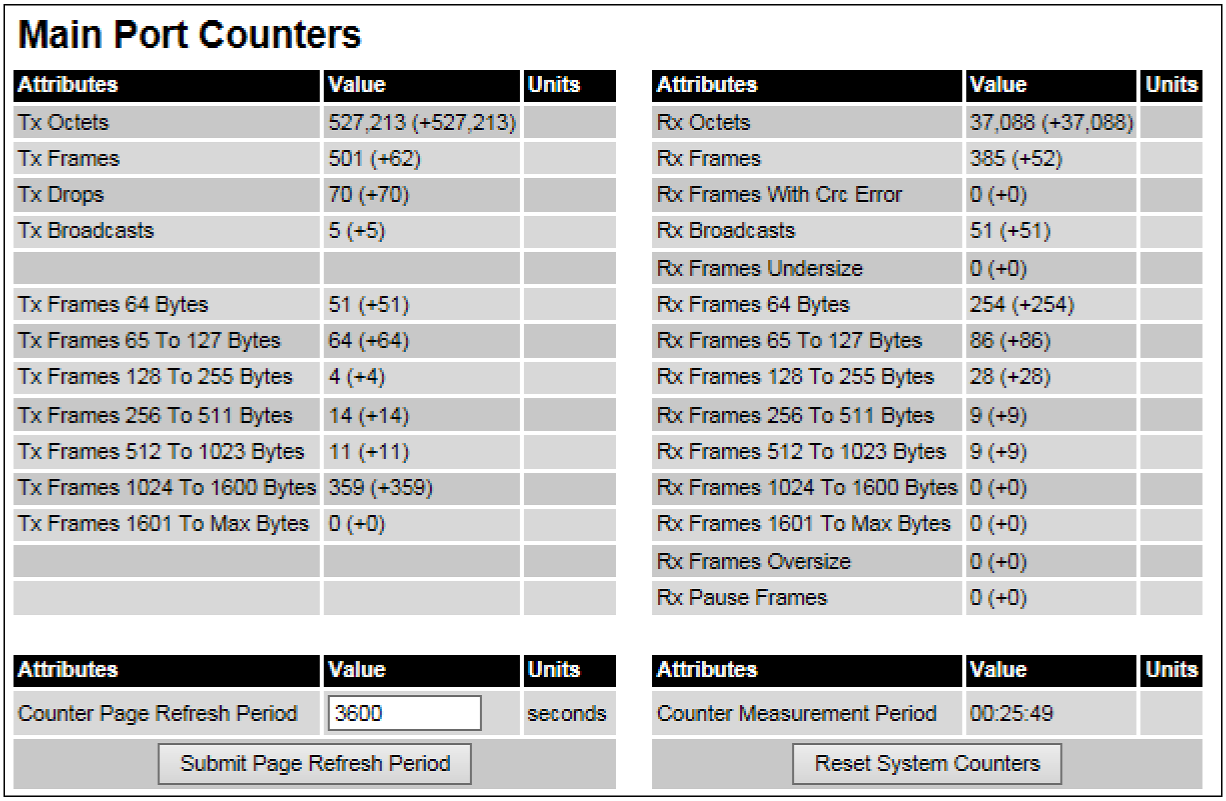
Table 115 Wireless Port Counters attributes

Attribute	Meaning
Tx/Rx Frames	Number of frames transmitted and received over the wireless bridge.
Rx Frames With Crc Error	Number of received frames with CRC errors.
Tx/Rx Frames Q0…Q7	Number of transmitted and received frames for each Traffic Class.
Tx Drops Q0…Q7	Number of transmitted frames dropped for each Traffic Class.
Rx Drops Q0…Q7	Total number of frames dropped due to the lack of sufficient capacity in the receive buffer, for each Traffic Class.

Main Port Counters page

Menu option: **System > Statistics > Main Port Counters** (Figure 128). Use this page to check the Ethernet performance of the PSU port. The displayed counters vary depending on which port is being used to bridge the traffic.

Figure 128 Main Port Counters page (when main port is bridging traffic)



Main Port Counters

Attributes	Value	Units	Attributes	Value	Units
Tx Octets	527,213 (+527,213)		Rx Octets	37,088 (+37,088)	
Tx Frames	501 (+62)		Rx Frames	385 (+52)	
Tx Drops	70 (+70)		Rx Frames With Crc Error	0 (+0)	
Tx Broadcasts	5 (+5)		Rx Broadcasts	51 (+51)	
			Rx Frames Undersize	0 (+0)	
Tx Frames 64 Bytes	51 (+51)		Rx Frames 64 Bytes	254 (+254)	
Tx Frames 65 To 127 Bytes	64 (+64)		Rx Frames 65 To 127 Bytes	86 (+86)	
Tx Frames 128 To 255 Bytes	4 (+4)		Rx Frames 128 To 255 Bytes	28 (+28)	
Tx Frames 256 To 511 Bytes	14 (+14)		Rx Frames 256 To 511 Bytes	9 (+9)	
Tx Frames 512 To 1023 Bytes	11 (+11)		Rx Frames 512 To 1023 Bytes	9 (+9)	
Tx Frames 1024 To 1600 Bytes	359 (+359)		Rx Frames 1024 To 1600 Bytes	0 (+0)	
Tx Frames 1601 To Max Bytes	0 (+0)		Rx Frames 1601 To Max Bytes	0 (+0)	
			Rx Frames Oversize	0 (+0)	
			Rx Pause Frames	0 (+0)	

Attributes	Value	Units	Attributes	Value	Units
Counter Page Refresh Period	3600	seconds	Counter Measurement Period	00:25:49	

Procedure:

- Review the attributes (Table 116).
- To change the refresh period, update the Counter Page Refresh Period attribute and click **Submit Page Refresh Period**.
- To reset all counters to zero, click **Reset System Counters**.

Table 116 Main Port Counters attributes

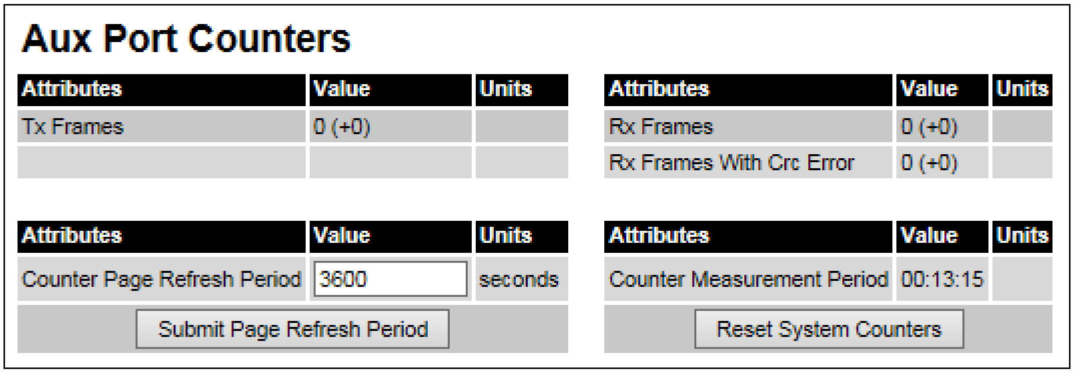
Attribute	Meaning
Tx/Rx Octets	Total number of octets (bytes) transmitted and received over the interface.
Tx/Rx Frames	Total number of frames transmitted and received over the interface. This includes both good and bad frames.
Tx Drops	Total number of transmit frames dropped.
Rx Frames With Crc Error	Total number of received frames with CRC errors.
Tx/Rx Broadcasts	Total number of good transmitted and received broadcast packets.
Rx Frames Undersize	Total number of frames received that are less than 64 bytes.
Tx/Rx Frames 64 Bytes	Total number 64 byte frames transmitted and received.
Tx/Rx Frames xxxx to yyyy Bytes	Total number of frames transmitted and received in the size range xxxx to yyyy bytes.
Tx/Rx Frames 1601 to Max bytes	Total number of frames transmitted and received in the size range 1601 to maximum bytes.
Rx Frames Oversize	Total number of frames received that are greater than the maximum number of bytes.
Rx Pause Frames	Total number of received pause frames.

Aux Port Counters page

Menu option: System > Statistics > **Aux Port Counters** (Figure 129).

Use this page to check the Ethernet performance of the Aux port.

Figure 129 Aux Port Counters page (when Aux port is out-of-band local)



Aux Port Counters

Attributes	Value	Units
Tx Frames	0 (+0)	

Attributes	Value	Units
Rx Frames	0 (+0)	
Rx Frames With Crc Error	0 (+0)	

Attributes	Value	Units
Counter Page Refresh Period	3600	seconds

Attributes	Value	Units
Counter Measurement Period	00:13:15	

Procedure:

- Review the attributes (Table 117).
- To change the refresh period, update the Counter Page Refresh Period attribute and click **Submit Page Refresh Period.**
- To reset all counters to zero, click **Reset System Counters**.

Table 117 Aux Port Counters attributes

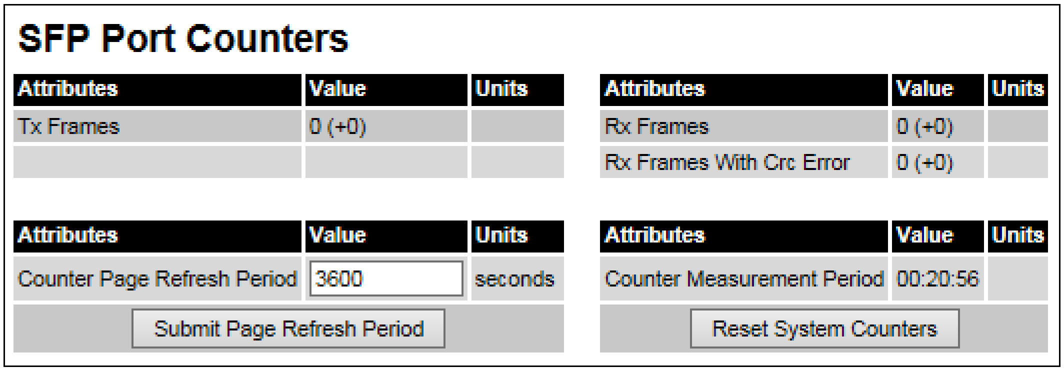
Attribute	Meaning
Tx/Rx Frames	Total number of frames transmitted and received over the interface. This includes both good and bad frames.
Rx Frames With Crc Error	Total number of received frames with CRC errors.

SFP Port Counters page

Menu option: System > Statistics > **SFP Port Counters** (Figure 130).

Use this page to check the Ethernet performance of the SFP port.

Figure 130 SFP Port Counters page (when SFP port is out-of-band local)



SFP Port Counters

Attributes	Value	Units
Tx Frames	0 (+0)	

Attributes	Value	Units
Rx Frames	0 (+0)	
Rx Frames With Crc Error	0 (+0)	

Attributes	Value	Units
Counter Page Refresh Period	3600	seconds

Attributes	Value	Units
Counter Measurement Period	00:20:56	

Procedure:

- Update the attributes (Table 118).
- To change the refresh period, update the Counter Page Refresh Period attribute and click **Submit Page Refresh Period**.
- To reset all counters to zero, click **Reset System Counters**.

Table 118 SFP Port Counters attributes

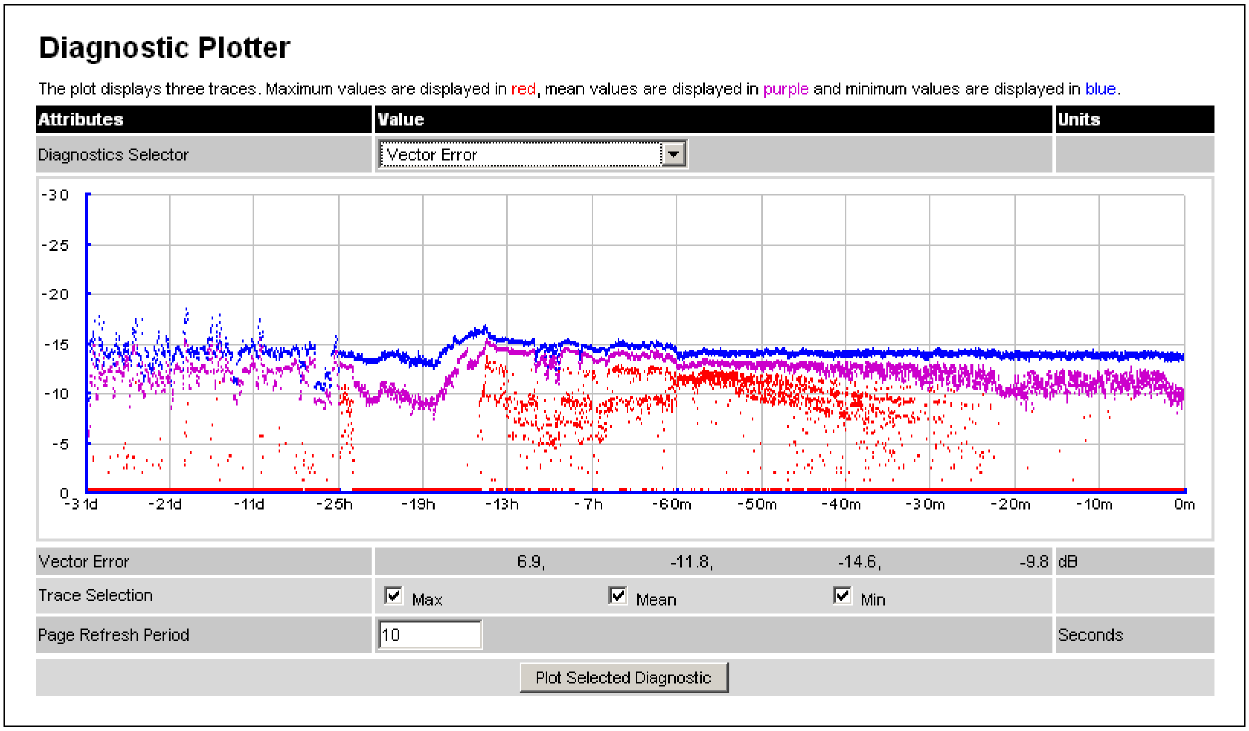
Attribute	Meaning
Tx/Rx Frames	Total number of frames transmitted and received over the interface. This includes both good and bad frames.
Rx Frames With Crc Error	Total number of received frames with CRC errors.

Diagnostics Plotter page

Menu option: **System** > **Diagnostics Plotter** (Figure 131).

Use this page to monitor the performance of an operational PTP 650 link over time.

Figure 131 Diagnostic Plotter page



Diagnostic Plotter

The plot displays three traces. Maximum values are displayed in red, mean values are displayed in purple and minimum values are displayed in blue.

Attributes	Value	Units
Diagnostics Selector	Vector Error ▾	

Vector Error	6.9, -11.8, -14.6, -9.8	dB
Trace Selection	☑ Max ☑ Mean ☑ Min	
Page Refresh Period	10	Seconds

Procedure:

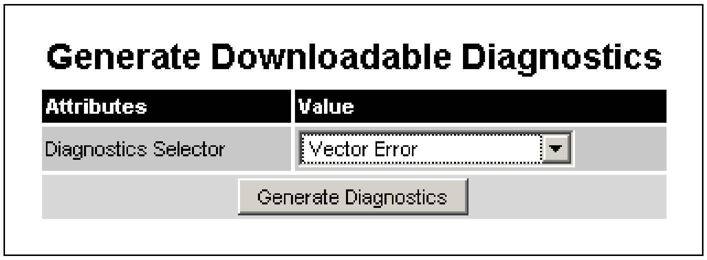
- Select a diagnostic from the Diagnostics Selector drop-down list. These are the same as the System Histogram attributes in the System Statistics page (Table 110).
- Tick the required Trace Selection boxes: Max, Mean and Min.
- Update the Page Refresh Period as required. The default period is 3600 seconds (1 hour). To monitor the performance of a link in real time, select a much shorter period, for example 60 seconds.
- Click **Plot Selected Diagnostic**. The selected diagnostic trace is displayed in the graph. Maximum values are displayed in red, mean values are displayed in purple and minimum values are displayed in blue.

Generate Downloadable Diagnostics page

Menu option: **System > Diagnostics Plotter > CSV Download** (Figure 132).

Use this page to download diagnostics data to a CSV file.

Figure 132 Generate Downloadable Diagnostics page



Generate Downloadable Diagnostics

Attributes	Value
Diagnostics Selector	Vector Error ▼

Procedure:

- Select a diagnostic from the Diagnostics Selector drop-down list.
- Click **Generate Diagnostics**. The Generate Downloadable Diagnostics page is redisplayed with the name of the generated CSV file.
- Click on the CSV file name and save the CSV file to the hard drive of the local computer.
- Open the CSV file in MS Excel and use it to generate reports and diagrams. The CSV file contains at most 5784 entries, recorded over a 32 day period:
  - o 3600 entries recorded in the last hour.
  - o 1440 entries recorded in the previous 24 hours.
  - o 744 entries recorded in the previous 31 days.

Recovery mode

This section describes how to recover a PTP 650 unit from configuration errors or software image corruption.

Entering recovery mode

Use this procedure to enter recovery mode manually.

Note

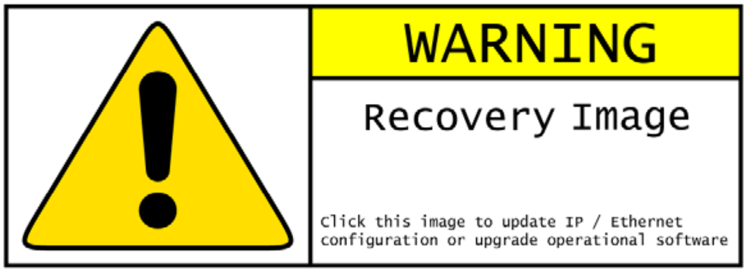
The unit may enter recovery mode automatically, in response to some failures.

Note

Once the unit has entered recovery, it will switch back to normal operation if no access has been made to the recovery web page within 30 seconds.

Procedure:

1. Apply power to PSU for at least 10 seconds.
2. Remove power for 5 seconds.
3. Re-apply power to the PSU.
4. When the unit is in recovery mode, access the web interface by entering the default IP address **169.254.1.1**. The Recovery Image Warning page is displayed:



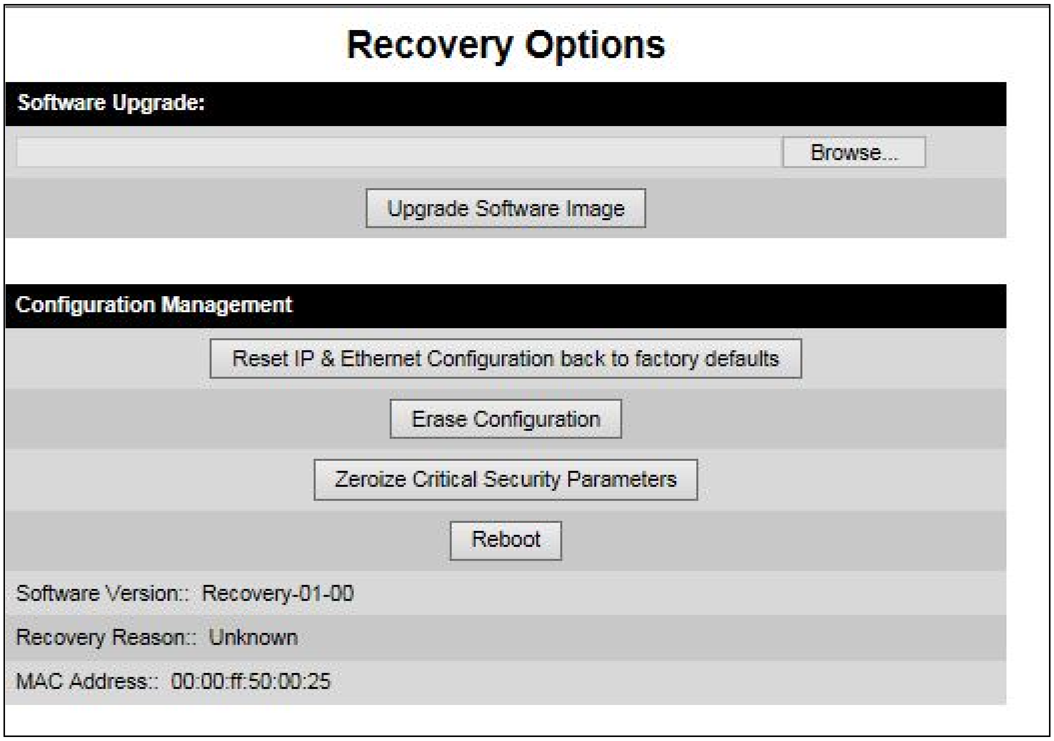
WARNING

Recovery Image

Click this image to update IP / Ethernet configuration or upgrade operational software

5. Click on the warning page image. The Recovery Option Page is displayed (Figure 133).`
6. Review the Software Version and Recovery Reason (Table 119).
7. Select a recovery option (Table 120).

Figure 133 Recovery Options page



Recovery Options

Software Version:: Recovery-01-00

Recovery Reason:: Unknown

MAC Address:: 00:00:ff:50:00:25

Table 119 Recovery Options attributes

Attribute	Meaning
Software Version	The software version of the recovery operating system permanently installed during manufacture.
Recovery Reason	The reason the unit is operating in Recovery mode, for example "Invalid or corrupt image". "Unknown" usually means there has been a power outage.
MAC Address	The MAC address of the unit programmed during manufacture.

Table 120 Recovery Options buttons

Button	Purpose
Upgrade Software Image	Use this option to restore a working software version when software corruption is suspected, or when an incorrect software image has been loaded. Refer to Upgrading software image on page 7-46.
Reset IP & Ethernet Configuration back to factory defaults	Use this option to restore the IP and Ethernet attributes to their defaults. Refer to Resetting IP & Ethernet configuration on page 7-47.
Erase Configuration	Use this option to erase the entire configuration of the unit. Refer to Erasing configuration on page 7-48.
Zeroize Critical Security Parameters	Use this option to reset encryption keys and the system administrator password. Refer to Zeroize Critical Security Parameters page on page 7-50.
Reboot	Use this option to reboot the unit. Refer to Rebooting the unit on page 7-51.

Upgrading software image

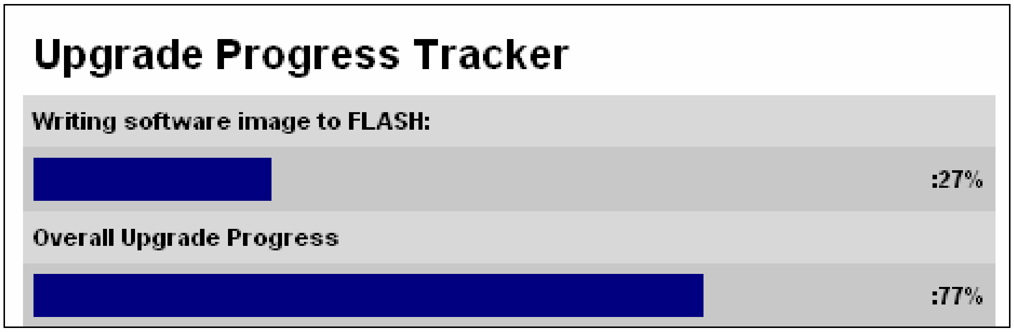
Use this option to restore a working software image from the Recovery Options page (Figure 133).

Procedure:

1 Click **Browse**.

2 Navigate to the required software image. This may be the most recent image if software corruption is suspected, or an older image if an incorrect image has just been loaded. Click on the image and click **Open**.

3 Click **Upgrade Software Image**. The Confirmation page is displayed. Click **Program Software Image into Non-Volatile Memory**. The Upgrade Progress Tracker page is displayed:



Upgrade Progress Tracker

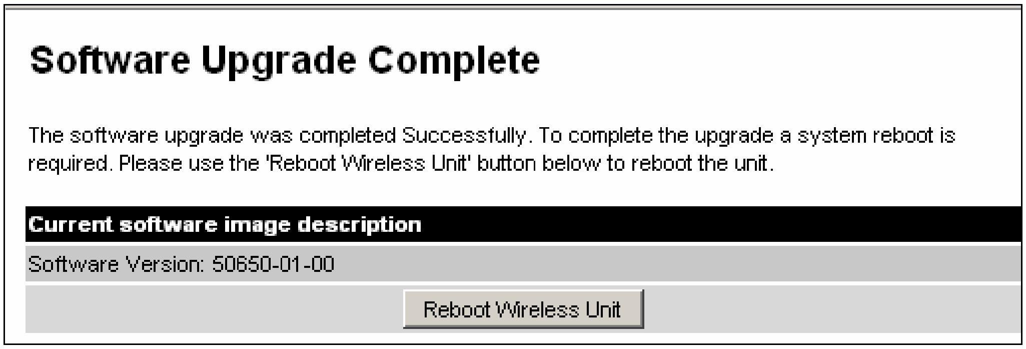
Writing software image to FLASH:

:27%

Overall Upgrade Progress

:77%

4 When the Software Upgrade Complete page is displayed, check that the correct image has been downloaded:



Software Upgrade Complete

The software upgrade was completed Successfully. To complete the upgrade a system reboot is required. Please use the 'Reboot Wireless Unit' button below to reboot the unit.

Current software image description

Software Version: 50650-01-00

5 Click **Reboot Wireless Unit.** When the “`Are you sure?`” message is displayed, click **OK**.

6 The unit will now reboot and restart in normal operational mode, and the link should recover. If the unit or link fails to recover, refer to Testing link end hardware on page 8-2.

Resetting IP & Ethernet configuration

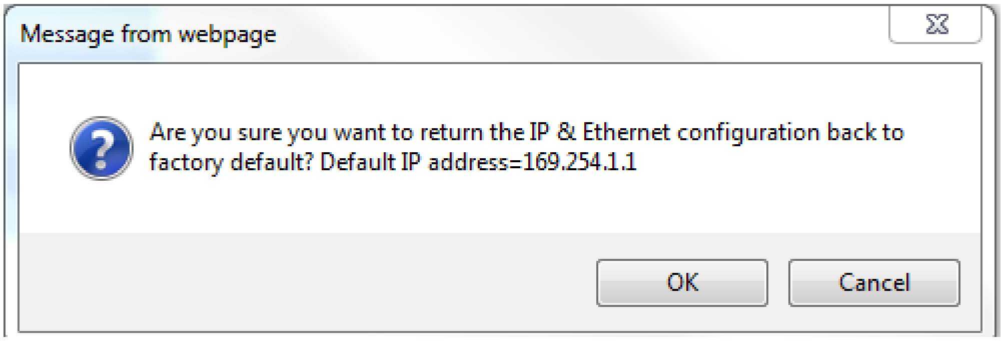
Use this option to reset IPv4, IPv6 and Ethernet configuration back to defaults from the Recovery Options page (Figure 133).

Note

This procedure resets the IP Version attribute to **IPv4**. It also resets the IPv6 configuration.

Procedure:

1 Click **Reset IP & Ethernet Configuration back to factory defaults.** The reset pop up box is displayed:

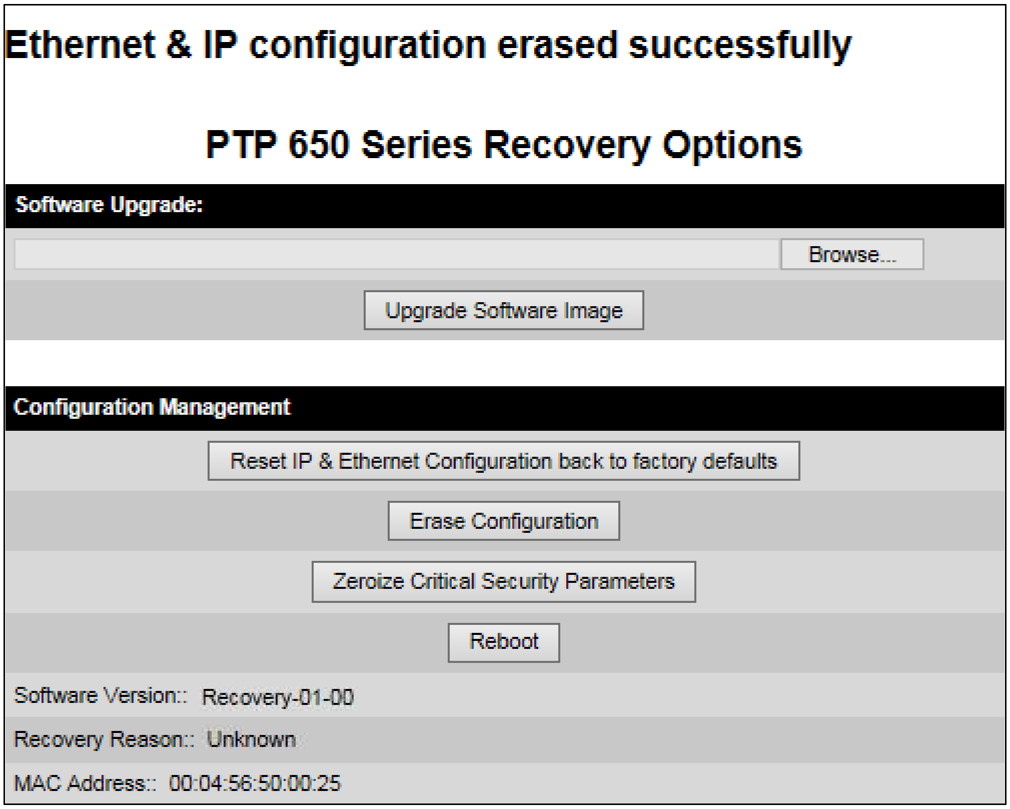


Message from webpage

Are you sure you want to return the IP & Ethernet configuration back to factory default? Default IP address=169.254.1.1

2 Record the IP address, as it will be needed to log into the unit after recovery.

3 Click **OK**. The reset confirmation page is displayed:



Ethernet & IP configuration erased successfully

PTP 650 Series Recovery Options

Software Version:: Recovery-01-00

Recovery Reason:: Unknown

MAC Address:: 00:04:56:50:00:25

4 Click **Reboot**. When the "`Are you sure you want to REBOOT this unit?`" message is displayed, click **OK**.

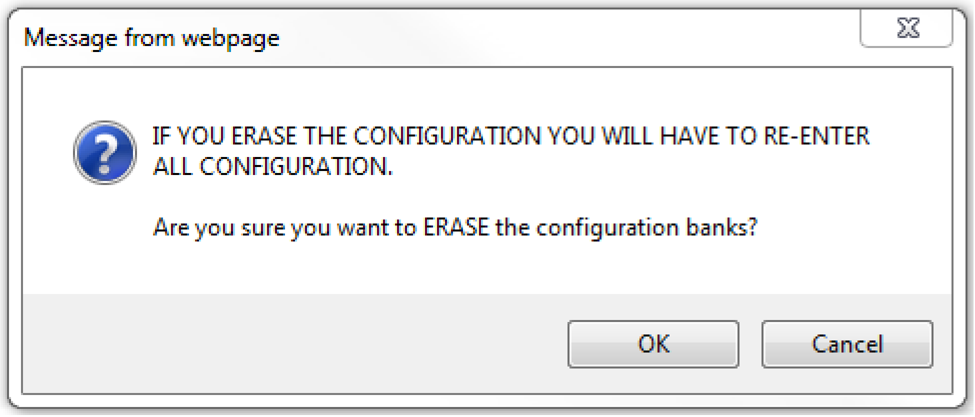
5 The unit will now reboot. The unit should now start up in normal mode but with the IP and Ethernet configuration reset to factory defaults. If the unit fails to recover, refer to Testing link end hardware on page 8-2.

Erasing configuration

Use this option to erase the entire configuration of the unit from the Recovery Options page (Figure 133).

Procedure:

1 Click **Erase Configuration**. The erase pop up box is displayed:

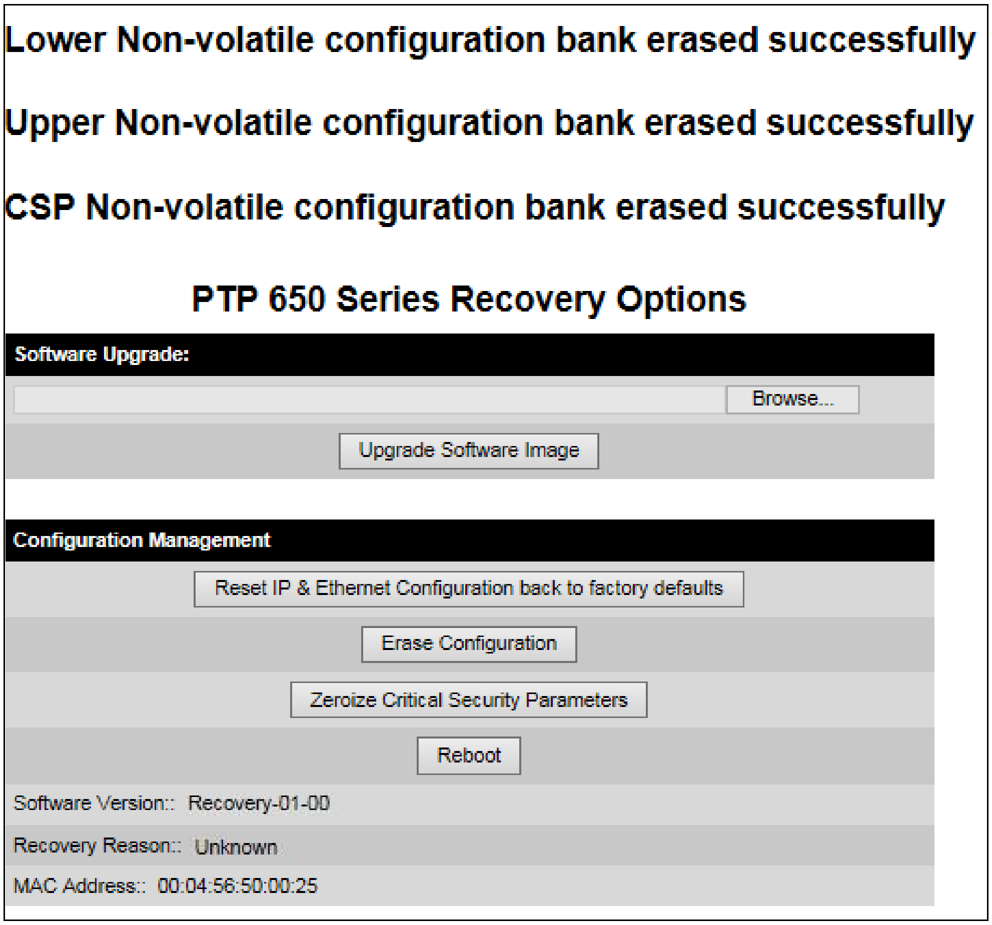


Message from webpage

IF YOU ERASE THE CONFIGURATION YOU WILL HAVE TO RE-ENTER ALL CONFIGURATION.

Are you sure you want to ERASE the configuration banks?

2 Click **OK**. The erase confirmation page is displayed:



Lower Non-volatile configuration bank erased successfully

Upper Non-volatile configuration bank erased successfully

CSP Non-volatile configuration bank erased successfully

PTP 650 Series Recovery Options

Software Upgrade:

Configuration Management

Software Version:: Recovery-01-00

Recovery Reason:: Unknown

MAC Address:: 00:04:56:50:00:25

Browse...
Upgrade Software Image
Reset IP & Ethernet Configuration back to factory defaults
Erase Configuration
Zeroize Critical Security Parameters
Reboot

3 Click **Reboot**. When the confirmation message is displayed, click **OK**.

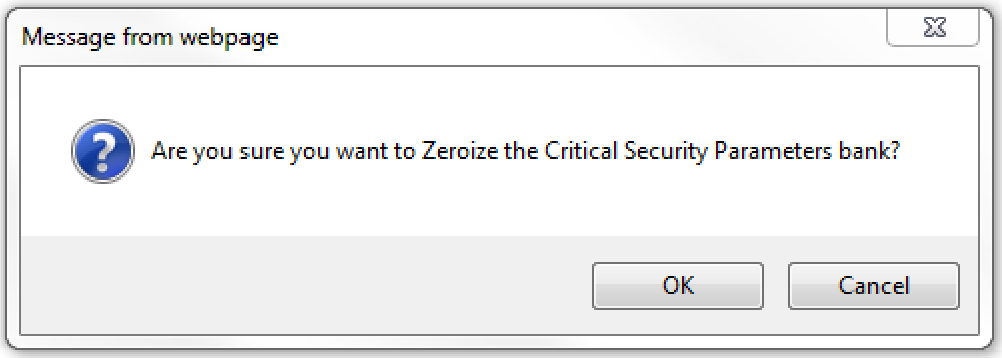
4 The unit reboots and starts up in normal mode but with all configuration erased. If the unit fails to start up, refer to Testing link end hardware on page 8-2.

Zeroize Critical Security Parameters page

Use this option to zeroize the critical security parameters (CSPs) of the unit from the Recovery Options page (Figure 133).

Procedure:

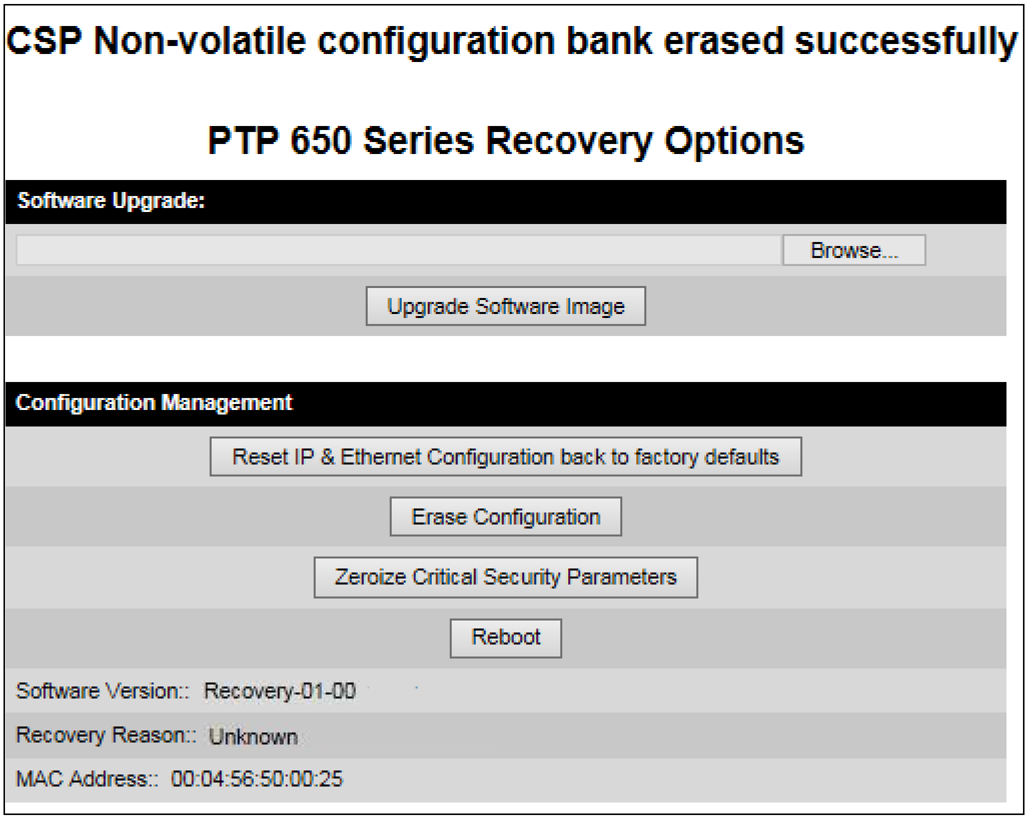
1 Click **Zeroize Critical Security Parameters.** The confirmation pop up box is displayed:



Message from webpage

Are you sure you want to Zeroize the Critical Security Parameters bank?

2 Click **OK.** The zeroize CSPs confirmation page is displayed:



CSP Non-volatile configuration bank erased successfully

PTP 650 Series Recovery Options

Software Upgrade:

Configuration Management

Software Version:: Recovery-01-00

Recovery Reason:: Unknown

MAC Address:: 00:04:56:50:00:25

Browse...
Upgrade Software Image
Reset IP & Ethernet Configuration back to factory defaults
Erase Configuration
Zeroize Critical Security Parameters
Reboot

3 Click **Reboot**. When the “`Are you sure you want to REBOOT this unit?`” message is displayed, click **OK**.

4 The unit will now reboot. The unit should now start up in normal mode but with the CSPs zeroized. If the unit fails to recover, refer to Testing link end hardware on page 8-2.

Rebooting the unit

Use this option to reboot the unit from the Recovery Options page (Figure 133).

Procedure:

- Click **Reboot**.
- When the “`Are you sure you want to REBOOT this unit?`” message is displayed, click **OK**. The unit will now reboot. The unit should now start up in normal operational mode. If the unit fails to start up, refer to Testing link end hardware on page 8-2.

Chapter 8: Troubleshooting

This chapter contains procedures for identifying and correcting faults in a PTP 650 link. These procedures can be performed either on a newly installed link, or on an operational link if communication is lost, or after a lightning strike.

The following topics are described in this chapter:

- Testing link end hardware on page 8-2 describes how to test the link end hardware, either when it fails on startup, or after a lightning strike.
- Testing the radio link on page 8-9 describes how to test the link when there is no radio communication, or when it is unreliable, or when the data throughput rate is too low.

Testing link end hardware

This section describes how to test the link end hardware when it fails on startup or during operation.

Before testing link end hardware, confirm that all outdoor drop cables, that is those that connect the ODU to equipment inside the building, are of the supported type, as defined in Outdoor copper Cat5e Ethernet cable on page 2-21.

AC Power Injector LED sequence

When the AC Power Injector is connected to the AC mains, the Power (green) LED should illuminate within 5 seconds of connection. If this does not happen, the AC injector is either not receiving power from the AC mains or there is a fault on the drop cable causing the power injector to sense an over current condition on the ODU output connector.

Action: Remove the ODU cable from the PSU and observe the effect on the power LED:

- If the power LED does not illuminate, confirm that the mains supply is working, for example check the plug and fuse (if fitted). If the power supply is working, report a suspected PSU fault to Cambium Networks.
- If the Power LED does illuminate, perform Test resistance in the drop cable on page 5-20.

AC+DC Enhanced power injector LED sequence

For the AC+DC Enhanced power injector, the expected power-up LED sequence is:

- The Power (green) LED illuminates steadily.
- After about 45 seconds, the Ethernet (yellow) LED blinks slowly 10 times.
- The Ethernet (yellow) LED illuminates steadily, then blinks randomly to show Ethernet activity.

If this sequence does not occur, take appropriate action depending on the LED states:

- Power LED is off on page 8-3
- Power LED is blinking on page 8-3
- Ethernet LED did not blink 10 times on page 8-3
- Ethernet LED blinks ten times then stays off on page 8-4
- Ethernet LED blinks irregularly on page 8-5 (for example a short blink followed by a long blink)
- Power LED is on, Ethernet LED blinks randomly on page 8-5

If a fault is suspected in the ODU-PSU drop cable, perform Test resistance in the drop cable on page 5-20.

Power LED is off

Meaning: Either the PSU is not receiving power from the AC/DC outlet, or there is a wiring fault in the ODU cable.

Action: Remove the ODU cable from the PSU and observe the effect on the Power LED:

- If the Power LED does not illuminate, confirm that the mains power supply is working, for example, check the plug and fuse (if fitted). If the power supply is working, report a suspected PSU fault to Cambium Networks.
- If the Power LED does illuminate, perform Test resistance in the drop cable on page 5-20.

Power LED is blinking

Meaning: The PSU is sensing there is an overload on the ODU port; this could be caused by a wiring error on the drop cable or a faulty ODU.

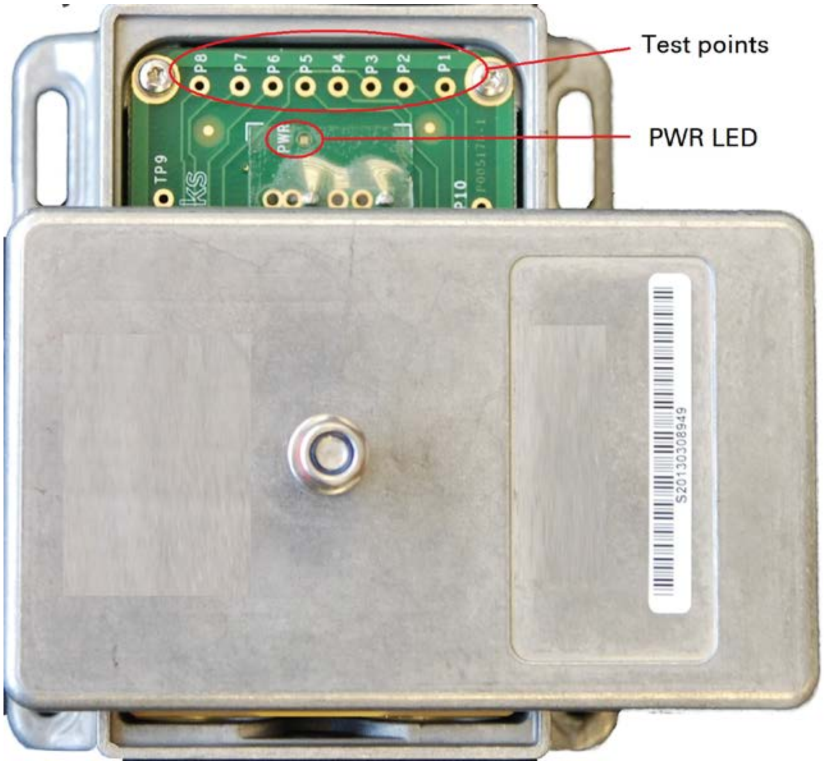
Action: Remove the ODU cable from the PSU. Check that pins 4&5 and 7&8 are not crossed with pins 1&2 and 3&6. Check that the resistance between pins 1&8 is greater than 100K ohms. If either check fails, replace or repair the ODU cable.

Ethernet LED did not blink 10 times

Meaning: The ODU flashes the LED on the AC+DC Enhanced Power Injector 10 times to show that the ODU is powered and booted correctly.

Action:

1. Remove the ODU cable from the PSU. Examine it for signs of damage. Check that the ODU cable resistances are correct, as specified in Test resistance in the drop cable on page 5-20. If the ODU cable is suspect, replace it.
2. Use the LPU (if installed) to check that power is available on the cable to the ODU. Access the connections by rotating the LPU lid as shown (slacken the lid nut but do not remove it):



4 Check that test point P1 on the LPU PCB corresponds to pin 1 on the RJ45. Repeat for points P2 to P8. This test is only valid if both the PSU and the ODU are disconnected.

5 Reconnect the ODU cable to the PSU.

6 Check that the PWR LED near the top right of the LPU PCB is illuminated to indicate power in the Ethernet cable.

7 If any test fails, replace or repair the cable that connects the PSU to the LPU or ODU.

Ethernet LED blinks ten times then stays off

Meaning: There is no Ethernet traffic between the PSU and ODU.

Action: The fault may be in the LAN or ODU cable:

- Confirm that Ethernet traffic is connected to the AC+DC injector LAN port, confirm the cable is not faulty, replace if necessary.
- If the LAN connection to the AC+DC power injector is working, check the drop cable is correctly wired using a suitable cable tester. Repeat the drop cable tests on page Test resistance in the drop cable on page 5-20.

Ethernet LED blinks irregularly

Meaning: If the Ethernet LED blinks irregularly, for example two rapid blinks followed by a longer gap, this indicates that the ODU has booted in recovery mode. The causes may be: installation wiring, or a corrupt ODU software load, or sufficient time has not been allowed between a repeat power up.

Action: Refer to Recovery mode on page 7-44.

Power LED is on, Ethernet LED blinks randomly

Meaning: Both LEDs are in their normal states, implying that the PSU is receiving power from the AC/DC outlet and there is normal Ethernet traffic between the PSU and ODU.

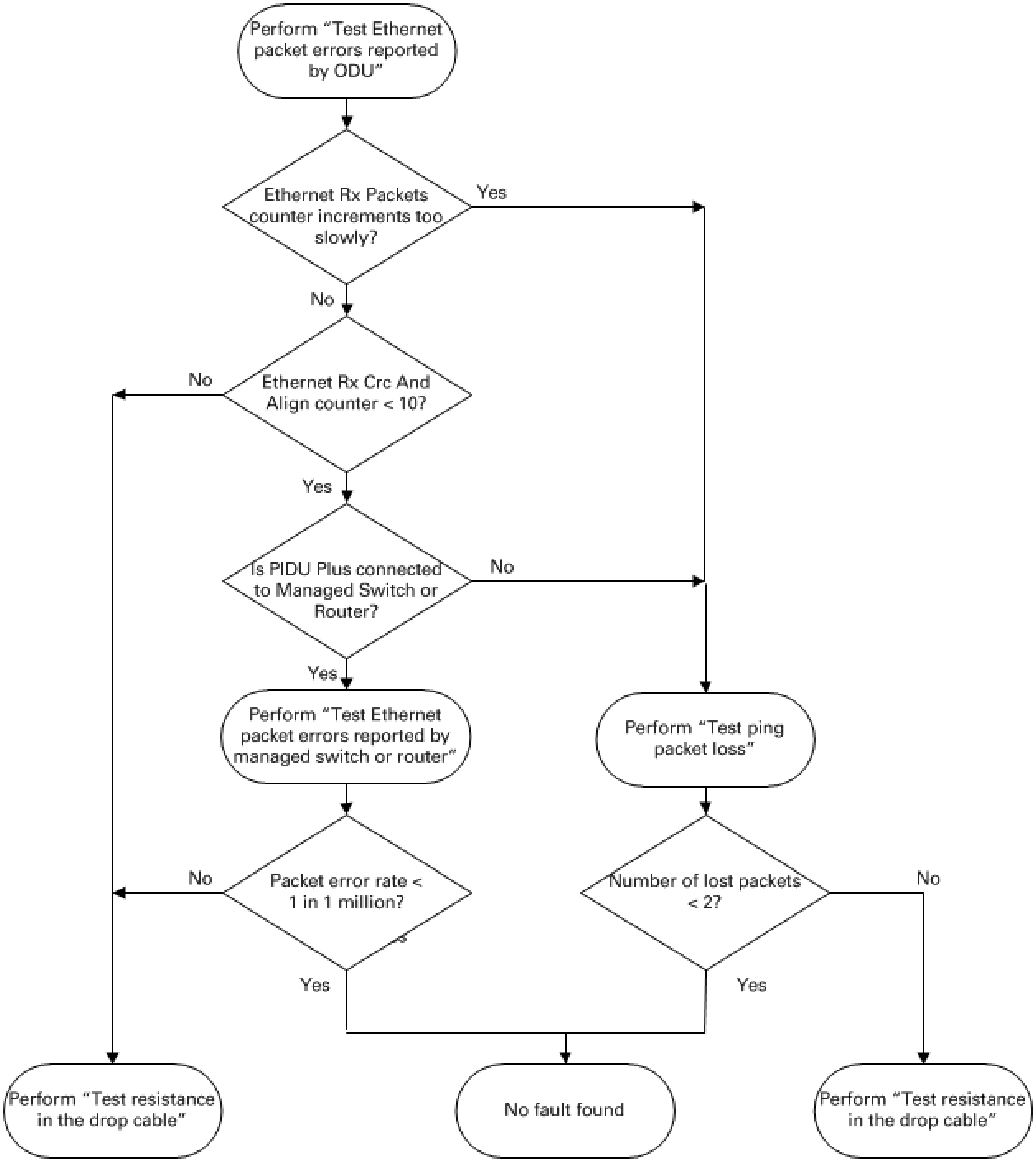
Action: If, in spite of this, a fault is suspected in the link end hardware:

- If the Ethernet connection to the network is only 100BASE-TX, when 1000BASE-T is expected: remove the ODU cable from the PSU, examine it, and check that the wiring to pins 4&5 and 7&8 is correct and not crossed.
- Perform Ethernet packet test on page 8-6.

Ethernet packet test

Follow the Ethernet packet test flowchart (Figure 134) and procedures below.

Figure 134 Ethernet packet test flowchart


Perform "Test Ethernet packet errors reported by ODU"
Ethernet Rx Packets counter increments too slowly?
Yes
No
Ethernet Rx Crc And Align counter < 10?
No
Yes
Is PIDU Plus connected to Managed Switch or Router?
No
Yes
Perform "Test Ethernet packet errors reported by managed switch or router"
Perform "Test ping packet loss"
Packet error rate < 1 in 1 million?
No
Yes
Number of lost packets < 2?
No
Yes
Perform "Test resistance in the drop cable"
No fault found
Perform "Test resistance in the drop cable"

Test Ethernet packet errors reported by ODU

Log into the unit and click **Administration**, **Statistics**, **Detailed Counters**. Click **Reset System Counters** at the bottom of the page and wait until the Ethernet Rx Packets counter has reached 1 million (the count will only update when the page is refreshed. If the counter does not increment or increments too slowly, because for example the PTP 650 is newly installed and there is no offered Ethernet traffic, then abandon this procedure and consider using the procedure Test ping packet loss on page 8-7.

Read the Ethernet Rx Crc And Align counter. The test has passed if this is less than 10.

Test Ethernet packet errors reported by managed switch or router

If the ODU is connected to a managed Ethernet switch or router, it may be possible to monitor the error rate of Ethernet packets. Please refer to the user guide of the managed network equipment. The test has passed if the rate of packet errors reported by the managed Ethernet switch or router is less than 10 in 1 million packets.

Test ping packet loss

Using a computer, it is possible to generate and monitor packets lost between the PSU and the ODU. This can be achieved by executing the Command Prompt application which is supplied as standard with Windows and MAC operating systems.

Caution

This procedure disrupt network traffic carried by the PTP 650 under test:

Procedure:

1. Ensure that the IP address of the computer is configured appropriately for connection to the PTP 650 under test, and does not clash with other devices connected to the network.
2. If the PSU is connected to an Ethernet switch or router then connect the computer to a spare port, if available.
3. If it is not possible to connect the computer to a spare port of an Ethernet switch or router, then the PSU will need to be disconnected from the network in order to execute this test:
   - Disconnect the PSU from the network.
   - Connect the computer directly to the LAN port of the PSU.
4. On the computer, open the Command Prompt application.

5 Send 1000 ping packets of length 1500 bytes. The process will take 1000 seconds, which is approximately 17 minutes.

If the computer is running a Windows operating system, this is achieved by typing (for an IPv6 address, use the **ping6** command):

```
ping –n 1000 –l 1500 <ipaddress>
```

where <ipaddress> is the IP address of the PTP 650 ODU under test.

If the computer is running a MAC operating system, this is achieved by typing:

```
ping –c 1000 –s 1492 <ipaddress>
```

where <ipaddress> is the IP address of the PTP 650 ODU under test.

6 Record how many Ping packets have been lost. This is reported by Command Prompt on completion of the test.

The test has passed if the number of lost packets is less than 2.

Testing the radio link

This section describes how to test the link when there is no radio communication, when it is unreliable, when the data throughput rate is too low, or when a unit is causing radio or TV interference. It may be necessary to test the units at both ends of the link.

No activity

If there is no wireless activity, proceed as follows:

1. Check for Alarm conditions on Home page.
2. Check that the software at each end of the link is the same version.
3. Check that the Target Mac address is correctly configured at each end of the link.
4. Check Range.
5. Check Tx Power.
6. Check License keys to ensure that both units are the same product variant.
7. Check Master/Slave status for each unit and ensure that one unit is Master and the other unit is slave.
8. Check that the link is not obstructed or the ODU misaligned.
9. Check the DFS page at each end of the link and establish that there is a quiet wireless channel to use.
10. If there are no faults found in the configuration and there is absolutely no wireless signal, retry the installation procedure.
11. If this does not work then report a suspected ODU fault to Cambium Networks.

Some activity

If there is some activity but the link is unreliable or does not achieve the data rates required, proceed as follows:

1. Check that the interference has not increased using the DSO measurements.
2. If a quieter channel is available check that it is not barred.
3. Check that the path loss is low enough for the communication rates required.
4. Check that the ODU has not become misaligned.

Radio and television interference

If a PTP 650 unit is interfering with radio or television reception (this can be determined by turning the equipment off and on), attempt the following corrective actions:

- Realign or relocate the antenna.
- Increase the separation between the affected equipment and antenna.
- Connect the ODU and PSU power supply into a power outlet on a circuit different from that to which the receiver is connected.
- Contact Cambium Point-to-Point for assistance.

Glossary

Term	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institution
ARP	Address Resolution Protocol
ATPC	Automatic Transmit Power Control
Aux	Auxiliary
BBDR	Broadband Disaster Relief
BPSK	Binary Phase Shift Keying
BW	Bandwidth
CFM	Connection Fault Management
CHAP	Challenge Handshake Authentication Protocol
CSP	Critical Security Parameter
DC	Direct Current
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Services Code Point
DSO	Dynamic Spectrum Optimization
EAPS	Ethernet Automatic Protection Switching
EIRP	Equivalent Isotropic Radiated Power
EMC	Electromagnetic Compatibility
EMD	Electro-Magnetic Discharge
EPL	Ethernet Private Line
ETSI	European Telecommunications Standards Institute
EU	European Union
FAQ	Frequently Asked Question

Term	Definition
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
GARP	Generic Attribute Registration Protocol
GE	Gigabit Ethernet
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
IB	In-Band
IC	Industry Canada
ICMP	Internet Control Message Protocol
ICNIRP	International Commission on Non-Ionizing Radiation Protection
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
IPSec	Internet Protocol Security
ISM	Industrial Scientific and Medical
ITPE	Initial Transmit Power Estimate
KDB	Knowledge Database
L2CP	Layer Two Control Protocols
LACP	Link Aggregation Control Protocol
LLDP	Link Layer Discovery Protocol
LAN	Local Area Network
LOS	Line-of-Sight (clear line-of-sight, and Fresnel zone is clear)
LPU	Lightning Protection Unit
MAC	Medium Access Control Layer
MDI (-X)	Medium Dependent Interface (-Crossover)
MEF	Metro Ethernet Forum
MIB	Management Information Base
MIMO	Multiple-Input Multiple-Output
MLD	Multicast Listener Discovery
MPLS	Multiprotocol Label Switching
MRP	Multiple Registration Protocol

Term	Definition
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NA	Neighbor Advertisement
NLOS	Non-Line-of-Sight
NMEA	National Marine Electronics Association
NS	Neighbor Solicitation
NTP	Network Time Protocol
NUD	Neighbor Un-reachability Detection
ODU	Outdoor Unit
OFDM	Orthogonal Frequency Division Multiplex
OOB	Out-of-Band
PC	IBM Compatible Personal Computer
PEAP	Protected Extensible Authentication Protocol
PIDU	Powered Indoor Unit
POE	Power over Ethernet
PSU	Power Supply Unit
PTP	Point-to-Point
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
R-APS	Ring Automatic Protection Switching
RADIUS	Remote Authentication Dial-In Service
RAM	Random Access Memory
RF	Radio Frequency
RFC	Request for Comments
RoW	Rest of World
RMA	Return Material Authorization
RSSI	Received Signal Strength Indication
RSTP	Rapid Spanning Tree Protocol
SELV	Safety Extra Low Voltage

Term	Definition
SFP	Small Form-factor Pluggable
SLAAC	Stateless Address Auto-configuration
SMTP	Simple Mail Transport Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
STP	Spanning Tree Protocol
Syslog	System Logging
TC	Traffic Class
TCP	Transmission Control Protocol
TDD	Time Division Duplexing
TDM	Time Division Multiplexing
TDWR	Terminal Doppler Weather Radar
TGB	Tower Ground Bus bar
TLS	Transport Layer Security
UNII	Unlicensed National Information Infrastructure
URL	Universal Resource Location
USM	User-based Security Model
UTC time	Coordinated Universal Time
UTP	Unshielded Twisted Pair
UV	Ultraviolet
VACM	View-based Access Control Model
VLAN	Virtual Local Area Network
WEEE	Waste Electrical and Electronic Equipment