

Figure 151 LAN Configuration page (PTP topology, TDM support)

LAN Configuration

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

Attributes	Value	Units
IP Interface		
IP Version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> Dual IPv4 and IPv6	
IPv4 Address	10 . 10 . 10 . 12	
Subnet Mask	255 . 255 . 0 . 0	
Gateway IP Address	169 . 254 . 0 . 0	
Use VLAN For Management Interfaces	No VLAN Tagging	▼
DSCP Management Priority	00 - DF	▼
Data Service	<input checked="" type="radio"/> Main PSU Port	
Second Data Service	<input type="radio"/> None <input checked="" type="radio"/> Aux Port <input type="radio"/> SFP Port	
Management Service	<input type="radio"/> None <input checked="" type="radio"/> In-Band Main PSU Port <input type="radio"/> In-Band Aux Port	
Local Management Service	<input checked="" type="checkbox"/> Out-of-Band SFP Port	
Ethernet Loopback Mode	<input checked="" type="radio"/> Disabled <input type="radio"/> Aux to Main PSU <input type="radio"/> Aux to SFP	
Data Port Wireless Down Alert	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	
Second Data Port Wireless Down Alert	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	
Main PSU Port		
Main PSU Port Auto Negotiation	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Main PSU Port Auto Neg Advertisement	<input checked="" type="checkbox"/> 1000 Mbps Full Duplex <input checked="" type="checkbox"/> 100 Mbps Full Duplex	
Main PSU Port Auto Mdix	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
NIDU Lan Port		
NIDU Lan Port Auto Negotiation	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
NIDU Lan Port Auto Neg Advertisement	<input checked="" type="checkbox"/> 1000 Mbps Full Duplex <input checked="" type="checkbox"/> 100 Mbps Full Duplex	
NIDU Lan Port Auto Mdix	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Aux Port		
Aux Port Auto Negotiation	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Aux Port Auto Neg Advertisement	<input checked="" type="checkbox"/> 1000 Mbps Full Duplex <input checked="" type="checkbox"/> 100 Mbps Full Duplex	
Aux Port Auto Mdix	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Aux Port Power Over Ethernet Output	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	
Bridging		
Local Packet Filtering	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Data Port Pause Frames	<input type="radio"/> Tunnel <input checked="" type="radio"/> Discard	
Second Data Port Pause Frames	<input type="radio"/> Tunnel <input checked="" type="radio"/> Discard	
Synchronous Ethernet		
Sync E Tracking	Internal TDM Use Only	
IEEE 1588		
Transparent Clock	Disabled	
<input type="button" value="Submit Updated System Configuration"/> <input type="button" value="Reset Form"/>		

Figure 152 LAN Configuration page (PTP topology, SFP support)

LAN Configuration

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

Attributes	Value	Units	
IP Interface			
IP Version	IPv4		
IPv4 Address	10 . 10 . 10 . 15		
Subnet Mask	255 . 255 . 255 . 0		
Gateway IP Address	10 . 10 . 10 . 9		
Use VLAN For Management Interfaces	No VLAN Tagging		
DSCP Management Priority	00 - DF		
Data Service	<input checked="" type="radio"/> Main PSU Port	<input type="radio"/> Aux Port	<input type="radio"/> SFP Port
Second Data Service	<input type="radio"/> None	<input checked="" type="radio"/> Aux Port	<input type="radio"/> SFP Port
Management Service	<input type="radio"/> None	<input type="radio"/> In-Band Main PSU Port	<input checked="" type="radio"/> In-Band Aux Port
Local Management Service	<input checked="" type="checkbox"/> Out-of-Band SFP Port		
Ethernet Loopback Mode	<input checked="" type="radio"/> Disabled	<input type="radio"/> Aux to Main PSU	<input type="radio"/> Aux to SFP
Data Port Wireless Down Alert	<input type="radio"/> Disabled	<input checked="" type="radio"/> Enabled	
Second Data Port Wireless Down Alert	<input checked="" type="radio"/> Disabled	<input type="radio"/> Enabled	
Main PSU Port			
Main PSU Port Auto Negotiation	<input type="radio"/> Disabled	<input checked="" type="radio"/> Enabled	
Main PSU Port Auto Neg Advertisement	<input checked="" type="checkbox"/> 1000 Mbps Full Duplex		
	<input checked="" type="checkbox"/> 100 Mbps Full Duplex		
Main PSU Port Auto Mdix	<input type="radio"/> Disabled	<input checked="" type="radio"/> Enabled	
Aux Port			
Aux Port Auto Negotiation	<input type="radio"/> Disabled	<input checked="" type="radio"/> Enabled	
Aux Port Auto Neg Advertisement	<input checked="" type="checkbox"/> 1000 Mbps Full Duplex		
	<input checked="" type="checkbox"/> 100 Mbps Full Duplex		
Aux Port Auto Mdix	<input type="radio"/> Disabled	<input checked="" type="radio"/> Enabled	
Aux Port Power Over Ethernet Output	<input checked="" type="radio"/> Disabled	<input type="radio"/> Enabled	
SFP Port			
SFP Port Auto Negotiation	<input type="radio"/> Disabled	<input checked="" type="radio"/> Enabled	
SFP Port Auto Neg Advertisement	<input checked="" type="checkbox"/> 1000 Mbps Full Duplex		
	<input checked="" type="checkbox"/> 100 Mbps Full Duplex		
SFP Port Auto Mdix	<input type="radio"/> Disabled	<input checked="" type="radio"/> Enabled	
Bridging			
Local Packet Filtering	<input type="radio"/> Disabled	<input checked="" type="radio"/> Enabled	
Data Port Pause Frames	<input type="radio"/> Tunnel	<input checked="" type="radio"/> Discard	
Second Data Port Pause Frames	<input type="radio"/> Tunnel	<input checked="" type="radio"/> Discard	
Synchronous Ethernet			
Sync E Tracking	<input checked="" type="radio"/> Disabled	<input type="radio"/> Enabled	
IEEE 1588			
Transparent Clock	<input checked="" type="radio"/> Disabled	<input type="radio"/> Enabled	
<input type="button" value="Submit Updated System Configuration"/> <input type="button" value="Reset Form"/>			

Figure 153 LAN Configuration page (Sync E and IEEE 1588 support)

SFP Port	
SFP Port Auto Negotiation	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Bridging	
Local Packet Filtering	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Data Port Pause Frames	<input type="radio"/> Tunnel <input checked="" type="radio"/> Discard
Synchronous Ethernet	
Sync E Tracking	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Sync E Equipment Clock	<input checked="" type="radio"/> EEC-Option 1 <input type="radio"/> EEC-Option 2
Sync E Slave Port	<input checked="" type="radio"/> Main PSU Port <input type="radio"/> SFP Port
Main PSU Port QL Rx Overwrite	Disabled
Main PSU Port SSM Tx	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Aux Port SSM Tx	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
SFP Port SSM Tx	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
IEEE 1588	
Transparent Clock	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
Transparent Clock VLAN	<input checked="" type="radio"/> All <input type="radio"/> S-Tagged <input type="radio"/> C-Tagged
Transparent Clock Port	<input checked="" type="radio"/> Main PSU
<input type="button" value="Submit Updated System Configuration"/> <input type="button" value="Reset Form"/>	

Figure 154 LAN Configuration page (HCMP topology)

LAN Configuration		
This page controls the LAN configuration of this unit.		
Attributes	Value	Units
IP Interface		
IP Version	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 <input type="radio"/> Dual IPv4 and IPv6	
IPv4 Address	10 . 10 . 10 . 13	
Subnet Mask	255 . 255 . 0 . 0	
Gateway IP Address	10 . 10 . 10 . 100	
Use VLAN For Management Interfaces	No VLAN Tagging	
DSCP Management Priority	00 - DF	
Data Service	Main PSU Port + Aux Port + SFP Port	
Management Service	In-Band	
Local Management Service	None	
Main PSU Port		
Main PSU Port Auto Negotiation	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Main PSU Port Auto Neg Advertisement	<input checked="" type="checkbox"/> 1000 Mbps Full Duplex <input checked="" type="checkbox"/> 100 Mbps Full Duplex	
Main PSU Port Auto Mdix	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Aux Port		
Aux Port Auto Negotiation	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Aux Port Auto Neg Advertisement	<input checked="" type="checkbox"/> 1000 Mbps Full Duplex <input checked="" type="checkbox"/> 100 Mbps Full Duplex	
Aux Port Auto Mdix	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Aux Port Power Over Ethernet Output	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	
SFP Port		
SFP Port Auto Negotiation	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Bridging		
Local Packet Filtering	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Data Port Pause Frames	<input type="radio"/> Tunnel <input checked="" type="radio"/> Discard	
<input type="button" value="Submit Updated System Configuration"/> <input type="button" value="Reset Form"/>		

Procedure:

- 1 Review and update the attributes: IP Interface ([Table 160](#)); Main PSU or Aux Port ([Table 161](#)); Bridging ([Table 163](#)).
- 2 To save changes, click **Submit Updated System Configuration**. The system may reboot.
- 3 If Main PSU Port is selected for **Data Service** only (and not for **Management Service**), connect management PC to the port (Aux or SFP) that was selected for Management or Local Management Service
- 4 If IP Address, Subnet Mask or Gateway IP Address have been changed, reconfigure the local management PC to use an IP address that is valid for the network. Refer to [Configuring the management PC](#) on page 6-4.
- 5 If IP Address has been changed, use the new IP address to log into the unit.

Table 160 IP interface attributes

Attribute	Meaning
IP Version	Defined in Table 153 .
IPv4 Address	Defined in Table 153 .
Subnet Mask	Defined in Table 153 .
Gateway IP Address	Defined in Table 153 .
IPv6 Address	Defined in Table 153 .
IPv6 Prefix Length	Defined in Table 153 .
IPv6 Gateway Address	Defined in Table 153 .
IPv6 Auto Configured	Defined in Table 153 .
Link Local Address	
Use VLAN For Management Interfaces	Defined in Table 153 .
VLAN Management VID	Defined in Table 153 .
VLAN Management Priority	Defined in Table 153 .
DSCP Management Priority	Defined in Table 153 .
Data Service	Defined in Table 153 . For more help, see Ethernet port allocation for PTP topology on page 3-37 and Ethernet port allocation for HCMP topology on page 3-46.
Second Data Service	Defined in Table 153 . For more help, see Ethernet port allocation for PTP topology on page 3-37.
Management Service	Defined in Table 153 . For more help, see Ethernet port allocation for PTP topology on page 3-37 and Ethernet port allocation for HCMP topology on page 3-46.

Attribute	Meaning
Local Management Service	Defined in Table 153 For more help, see Ethernet port allocation for PTP topology on page 3-37 .
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	<p>Disabled: The data Ethernet link will not be dropped when the wireless link drops.</p> <p>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). When TDM is enabled, the link is dropped briefly at the NIDU LAN port, and not at the ODU.</p>
Second Data Port Wireless Down Alert	<p>Disabled: The Second Data Ethernet link will not be dropped when the wireless link drops.</p> <p>Enabled: The Second 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). When TDM is enabled, the link is dropped briefly at the NIDU LAN port, and not at the ODU.</p>
Management Port Wireless Down Alert	<p>Only displayed when an Out-of-Band Port is selected for Management Service.</p> <p>Disabled: The management Ethernet link will not be dropped when the wireless link drops.</p> <p>Enabled: The management Ethernet link will be dropped briefly when the wireless link drops. This signals to the connected network equipment that this link is no longer available. Connected Ethernet switches can be configured to forward Ethernet frames on an alternative path identified using the Spanning Tree Protocol (STP).</p>
Management Network Access Enabled	<p>Only displayed when one of the Port selection attributes (Main PSU, Aux or SFP) is set to Out-of-Band Management Service and Second Data Service is disabled or set to None.</p> <p>Yes: The local out-of-band management interface can be used to access the remote management network.</p> <p>No: The local out-of-band management interface cannot be used to access the remote management network.</p>

Table 161 Main PSU Port, NIDU LAN Port and Aux Port attributes

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

Table 162 SFP Port (connected with copper module) attributes

Attribute	Meaning
SFP Port Auto Negotiation	Disabled: Configuration of the Ethernet interface is forced. This is to be used as a last resort only if auto-negotiation fails. Enabled: Configuration of the Ethernet interface is automatically negotiated (default). This is the preferred setting.
SFP Port Auto Neg Advertisement	Only displayed when SFP Port Auto Negotiation is set to Enabled and SFP port is connected with copper module. The data rate that the auto-negotiation mechanism will advertise as available on the Ethernet interface (1000 Mbps or 100 Mbps Full Duplex). Select a data rate that is within the capability of the Ethernet link partner. Use the same setting for the Ethernet link partner.

Attribute	Meaning
Forced Configuration	<p>Only displayed when SFP Port Auto Negotiation is set to Disabled and SFP port is connected with copper module.</p> <p>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.</p>
Auto Mdix	<p>Only displayed when SFP port is connected with copper module.</p> <p>Disabled: The Auto Medium Dependent Interface (MDI)/Medium Dependent Interface Crossover (MDIX) capability is disabled.</p> <p>Enabled: The Auto Medium Dependent Interface (MDI)/Medium Dependent Interface Crossover (MDIX) capability is enabled.</p>

Table 163 Bridging attributes

Attribute	Meaning
Local Packet Filtering	<p>Enabled: The management agent learns the location of end stations from the source addresses in received management frames. The agent filters transmitted management frames to ensure that the frame is transmitted at the Ethernet (data or management) port, or over the wireless link. If the end station address is unknown, then management traffic is transmitted at the Ethernet port and over the wireless link.</p> <p>In the Local Management Service, management frames are not transmitted over the wireless link, and so address learning is not active.</p>
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.
Second Data Port Pause Frames	<p>Tunnel: The Layer 2 pause frames arriving at the port selected for Second Data Service will be bridged across to the port selected for Second Data Service on remote device over the wireless link.</p> <p>Discard: The Layer 2 pause frames arriving at the port selected for Second Data Service will be dropped.</p>

Table 164 Synchronous Ethernet attributes

Attribute	Meaning
Sync E Tracking	<p>Disabled: The synchronous Ethernet feature is disabled. Synchronization Status Messages received at the Main PSU port will be discarded.</p> <p>Enabled: The synchronous Ethernet feature is enabled. Internal TDM Use Only: Sync E Tracking is enabled, but is being used internally as part of the TDM feature. Sync E is not available to relay synchronization between external network equipment.</p>
Sync E Equipment Clock	<p>EEC-Option 1: Select this option if the equipment is operating in a 2048 kbit/s synchronisation hierarchy (ITU-T G.813 Option 1)</p> <p>EEC-Option 2: Select this option if the equipment is operating in a 1544 kbit/s synchronisation hierarchy (Type IV clock from ITU-T G.812)</p>
Sync E Slave Port	<p>This control configures either the Main PSU Port or the SFP Port as a candidate for selection as a Sync E Slave port.</p> <p>Only ports that are allocated to one of the standard services (Data Service, Second Data Service, Management Service, Local Management Service) are offered as options here.</p>
Main PSU Port QL Rx Overwrite	<p>This control provides the facility to overwrite the Quality Level (QL) of received Synchronisation Status Messages (SSM). It may be useful in a test environment, or for interworking with equipment that does not generate SSMs.</p> <p>Disabled: The recommended setting, the QL of received SSMs is unmodified.</p> <p>“QL-PRC” or “QL-SSU A / QL-TNC” or “QL-SSU B” or “QL-EEC1 / QL-SEC” or “QL-DNU / QL-DUS”: The overwritten value of the QL. Where two QLs are given, the QL used is dependent upon the setting of “Sync E Equipment Clock” type.</p> <p>This control is hidden if Sync E Slave Port is set to SFP Port.</p>
SFP Port QL Rx Overwrite	<p>This control provides the facility to overwrite the Quality Level (QL) of Synchronisation Status Messages (SSM) received at the SFP port. It may be useful in a test environment, or for interworking with equipment that does not generate SSMs.</p> <p>Disabled: The recommended setting, the QL of received SSMs is unmodified.</p> <p>“QL-PRC” or “QL-SSU A / QL-TNC” or “QL-SSU B” or “QL-EEC1 / QL-SEC” or “QL-DNU / QL-DUS”: The overwritten value of the QL. Where two QLs are given, the QL used is dependent upon the setting of “Sync E Equipment Clock” type.</p> <p>This control is hidden if Sync E Slave Port is set to Main PSU Port.</p>

Attribute	Meaning
Main PSU Port SSM Tx	Disabled: SSMs are not transmitted from the Main PSU port. Disabling SSMs may be useful in a test environment. Enabled: SSMs are transmitted from the Main PSU port (normal operation)
Aux Port SSM Tx	Disabled: SSMs are not transmitted from the Aux Port. Disabling SSMs may be useful in a test environment. Enabled: SSMs are transmitted from the Aux Port (normal operation)
SFP Port SSM Tx	Disabled: SSMs are not transmitted from the SFP port. Disabling SSMs may be useful in a test environment. Enabled: SSMs are transmitted from the SFP port (normal operation)

Table 165 IEEE 1588 attributes

Attribute	Meaning
Transparent Clock	Disabled: The Transparent Clock function is disabled. IEEE 1588-2008 event frames will be forwarded, but residence time corrections will not be made. Enabled: The Transparent Clock function is enabled. Residence time corrections will be made to IEEE 1588-2008 event frames.
Transparent Clock Port	This specifies the transparent clock source port. It can be Main PSU or SFP Fiber. Only the ports allocated for Data / Second Data Path show up for selection.
Transparent Clock VLAN	All: The recommended setting. Residence time corrections will be made to all IEEE 1588-2008 event frames, regardless of any VLAN encapsulation. S-Tagged: Residence time corrections are only made to event frames tagged with a service tag equal to "Transparent Clock VID". C-Tagged: Residence time corrections are only made to event frames double tagged and with a customer tag equal to "Transparent Clock VID".
Transparent Clock VID	The VLAN Identifier (VID) used with "Transparent Clock VLAN" to restrict residence time corrections to IEEE 1588-2008 event frames in a specific VLAN.

QoS Configuration page

Menu option: **System > Configuration > QoS Configuration** (Figure 155 or Figure 156 or Figure 157). Use this page to control the quality of service configuration. Classification may be based on fields in the Ethernet header (Layer 2) or in the network header (Layer 3). The unit recognizes two network layer protocols: IP and MPLS.



Note

In PTP topology, eight QoS levels (Q0 to Q7) are supported, while in HCMP topology, only four QoS levels (Q0 to Q3) are supported for each wireless link.

Figure 155 QoS Configuration page (Ethernet)

QoS Configuration

This page controls the quality of service configuration.

Data Service

Layer 2 Control Protocols

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

Data 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 ▾

Second Data Service

Traffic Priority

Queue

Figure 156 QoS Configuration page (IP/MPLS)

QoS Configuration

This page controls the quality of service configuration.

Data Service

Layer 2 Control Protocols

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

Data Priority Scheme

Ethernet IP/MPLS

Unknown Network Layer Protocol

Unknown Protocol

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 ▾

Second Data Service

Traffic Priority

Queue

Figure 157 QoS Configuration page showing Out-of-Band Management

QoS Configuration

This page controls the quality of service configuration.

Data Service

Layer 2 Control Protocols

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

Data Priority Scheme

Data 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 ▾

Out-of-Band Management Service

Traffic Priority

Queue	Q7 ▾
-------	------

Procedures:

- Review and update the attributes ([Table 166](#), [Table 167](#) and [Table 168](#)).
- 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 166 QoS Configuration attributes – Data Service

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	
PPPoE Discovery	
Data Priority Scheme	Ethernet: Classification is based on fields in the Ethernet header (Layer 2). IP/MPLS: Classification is based on fields in the network header (Layer 3). IP includes IPv4 and IPv6.
Unknown Protocol	Only displayed when Priority Scheme is IP/MPLS . The classification of unknown network protocols (that is, not IP or MPLS) to an egress queue at the wireless port.
Ethernet Priority	Ethernet priority mapping to Queue

Table 167 QoS Configuration attributes – Second Data Service

Attribute	Meaning
Queue	Set a priority egress queue for Second Data Service traffic classification

Table 168 QoS Configuration attributes –Out-of-Band Management Service

Attribute	Meaning
Queue	Only displayed when one ODU port is allocated to Out-of-Band Management and Second Data Service port is not allocated (Configuring port allocations on page 6-23). The classification of out-of-band management traffic to an egress queue at the wireless port.

SFP Configuration page

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

This page is only available when the ODU detects an optical ([Figure 158](#)) or copper ([Figure 159](#)) 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 158 SFP Configuration page (optical SFP module)

SFP Configuration		
This page controls the SFP configuration of the PTP wireless unit.		
Attributes	Value	Units
SFP Port Auto Negotiation	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Sfp Vendor Name	JDSU	
Sfp Vendor OUI	00:01:9c	
Sfp Part Number	PLRXPL-VI-S24-22	
Sfp Revision Level	1	
Sfp Laser Wavelength	850	
Sfp Serial Number	CA51QA098	
Sfp Date Code	101214	

Figure 159 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	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
SFP Port Auto Neg Advertisement	<input checked="" type="checkbox"/> 1000 Mbps Full Duplex <input checked="" type="checkbox"/> 100 Mbps Full Duplex	
SFP Port Auto Mdix	<input type="radio"/> Disabled <input checked="" type="radio"/> 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	
<input type="button" value="Submit Updated System Configuration"/> <input type="button" value="Reset Form"/>		

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

- Update the attributes
 - When optical SFP module is installed ([Table 172](#)).
 - When copper SFP module is installed ([Table 170](#))
- To save changes, click **Submit Updated System Configuration**.

Table 169 SFP Configuration (Optical module) attributes

Attribute	Meaning
SFP Port Auto Negotiation	Disabled: Configuration of the Ethernet interface is forced. This is to be used as a last resort only if auto-negotiation fails. Enabled: Configuration of the Ethernet interface is automatically negotiated (default). This is the preferred setting.

Table 170 SFP Configuration (copper SFP module) attributes

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

TDM Configuration page



Note

The TDM service is not supported in the HCMP topology.

Menu option: **System > Configuration > TDM Configuration** ([Figure 160](#)).

Use this page to control how the unit handles E1 or T1 channels over the wireless bridge.

This page is only available when the TDM interface is enabled and the unit is rebooted ([Interface Configuration page on page 6-16](#)).

Procedure:

- Update the attributes ([Table 171](#)).
- To save changes, click **Submit Updated TDM Configuration**.

Figure 160 TDM Configuration page (T1 option shown)

TDM		
This page controls the telecoms configuration of the wireless unit.		
Attributes	Value	Units
TDM Interface Control	T1	
TDM Local MAC Address	00:00:00:00:00:00	
TDM Remote MAC Address	00:00:00:00:00:00	
License Max Number Of TDM Channels	8	
TDM Enabled Channels	3	
TDM Channel Line Code 1	B8ZS or HDB3 ▾	
TDM Channel Line Code 2	B8ZS or HDB3 ▾	
TDM Channel Line Code 3	B8ZS or HDB3 ▾	
TDM Channel Cable Length 0	<input checked="" type="radio"/> 41 <input type="radio"/> 81 <input type="radio"/> 122 <input type="radio"/> 162 <input type="radio"/> 200	meters
TDM Channel Cable Length 1	<input checked="" type="radio"/> 41 <input type="radio"/> 81 <input type="radio"/> 122 <input type="radio"/> 162 <input type="radio"/> 200	meters
TDM Channel Cable Length 2	<input checked="" type="radio"/> 41 <input type="radio"/> 81 <input type="radio"/> 122 <input type="radio"/> 162 <input type="radio"/> 200	meters
TDM Channel Loopback 1	<input checked="" type="radio"/> None <input type="radio"/> Copper <input type="radio"/> Wireless	
TDM Channel Loopback 2	<input checked="" type="radio"/> None <input type="radio"/> Copper <input type="radio"/> Wireless	
TDM Channel Loopback 3	<input checked="" type="radio"/> None <input type="radio"/> Copper <input type="radio"/> Wireless	
Lowest TDM Modulation Mode	BPSK 0.63	
<input type="button" value="Submit Updated TDM Configuration"/> <input type="button" value="Reset Form"/>		

Table 171 TDM Configuration attributes

Attribute	Meaning
TDM Interface Control	Display only. Defined in Table 154 .
TDM Local MAC Address	Display only. MAC address of the local NIDU.
TDM Remote MAC Address	Display only. MAC address of the remote NIDU.
License Max Number of TDM Channels	Display only. Defined in Table 154 .
TDM Enabled Channels	Display only. Defined in Table 154 .
TDM Channel Line Code n	Defined in Table 154 .
TDM Channel Cable Length n	Defined in Table 154 .
TDM Channel Loopback n	Select the loopback status of TDM channel "n" (where "n" is in the range 1 to 8). None: Normal operation, no testing is required. Copper: Sends the TDM data received from the local transceiver and NIDU back on the same TDM channel. This may be used in conjunction with a Bit Error Rate Tester to confirm that the correct connections have been made between the transceiver, NIDU and ODU. This mode cannot be used for resistance tests, as it is only capable of looping back valid TDM signals. Wireless: Sends the TDM data received from the wireless link back across the link on the same TDM channel. The link may be checked using, for example, a Bit Error Rate Tester to ensure that no errors are detected.
Lowest TDM Modulation Mode	Display only. Defined in Table 154 .

Authorization Control page

Menu option: **System > Configuration > Authorization Control** ([Figure 161](#)).

Authorization control is used when Access Method is configured to **Group Access**, and Encryption Algorithm is configured to **TLS-RSA**. In the HCMP topology, Group Access is the only Access Method supported. In the PTP topology, Group Access is available only with the Group Access license. The Authorization Control page is hidden if it is not applicable.

When Authorization Method is configured to Whitelist, the ODU will connect only if the authenticated MAC address of the remote unit is in the list of authorized ODUs. With the Blacklist option, the ODU will always connect unless the authenticated MAC address has been added to a list of unauthorized ODUs.

The Authorization Control page allows up to 32 MAC addresses to be entered.

Authorization Control does not require an AES license.

Procedure:

- Select **Whitelist** or **Blacklist**
- Update the MAC Addresses
- To save changes, click **Submit Configuration**.

Figure 161 Authorization Control page

Authorization

Whitelist must be configured for proper operation.

Entry	MAC Address	Enabled
1	00:04:56: 58 : 00 : c0	<input checked="" type="checkbox"/>
2	00:04:56: 58 : 00 : b6	<input checked="" type="checkbox"/>
3	00:04:56: 58 : 00 : 5b	<input checked="" type="checkbox"/>
4	00:04:56: 58 : 00 : 67	<input checked="" type="checkbox"/>
5	00:04:56: 58 : 00 : 6c	<input checked="" type="checkbox"/>
6	00:04:56: 58 : 00 : 85	<input checked="" type="checkbox"/>
7	00:04:56: 58 : 00 : c4	<input checked="" type="checkbox"/>
8	00:04:56: 58 : 01 : 43	<input checked="" type="checkbox"/>
9	00:04:56: 00 : 00 : 00	<input type="checkbox"/>
10	00:04:56: 00 : 00 : 00	<input type="checkbox"/>
29	00:04:56: 00 : 00 : 00	<input type="checkbox"/>
30	00:04:56: 00 : 00 : 00	<input type="checkbox"/>
31	00:04:56: 00 : 00 : 00	<input type="checkbox"/>
32	00:04:56: 00 : 00 : 00	<input type="checkbox"/>

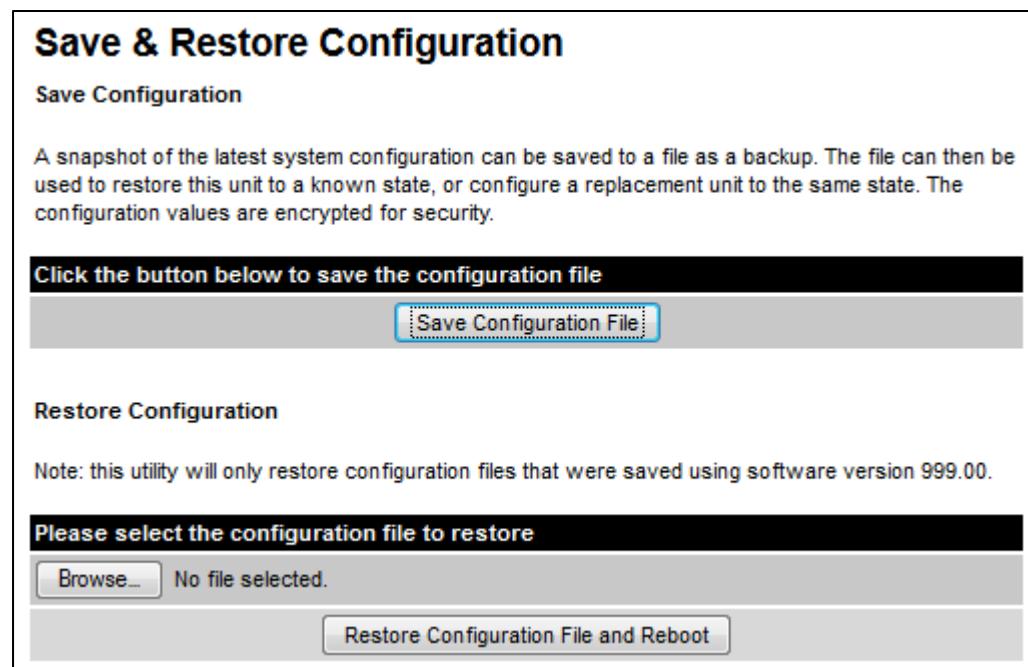
Clear Configuration

Submit Configuration **Reset Form**

Save and Restore Configuration page

Menu option: **System > Configuration > Save And Restore** (Figure 162).

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 162 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

Save 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

Browse... No file selected.

Restore Configuration File and Reboot

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 670 unit, ensure that a valid license key is installed (with optional capabilities enabled where appropriate).

**Note**

The stored configuration must be restored in a unit configured for the same topology

For example, if a unit configured as HCMP needs to be restored to a PTP configuration, the following steps must be taken:

- First, go through the Installation Wizard, change the Wireless Topology to PTP and reboot the unit.
- After the reboot and while the unit is in PTP mode, go to Save/Restore Configuration page, restore the desired PTP configuration and reboot.
- When the unit has completed the reboot, the configuration has been fully restored.

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:

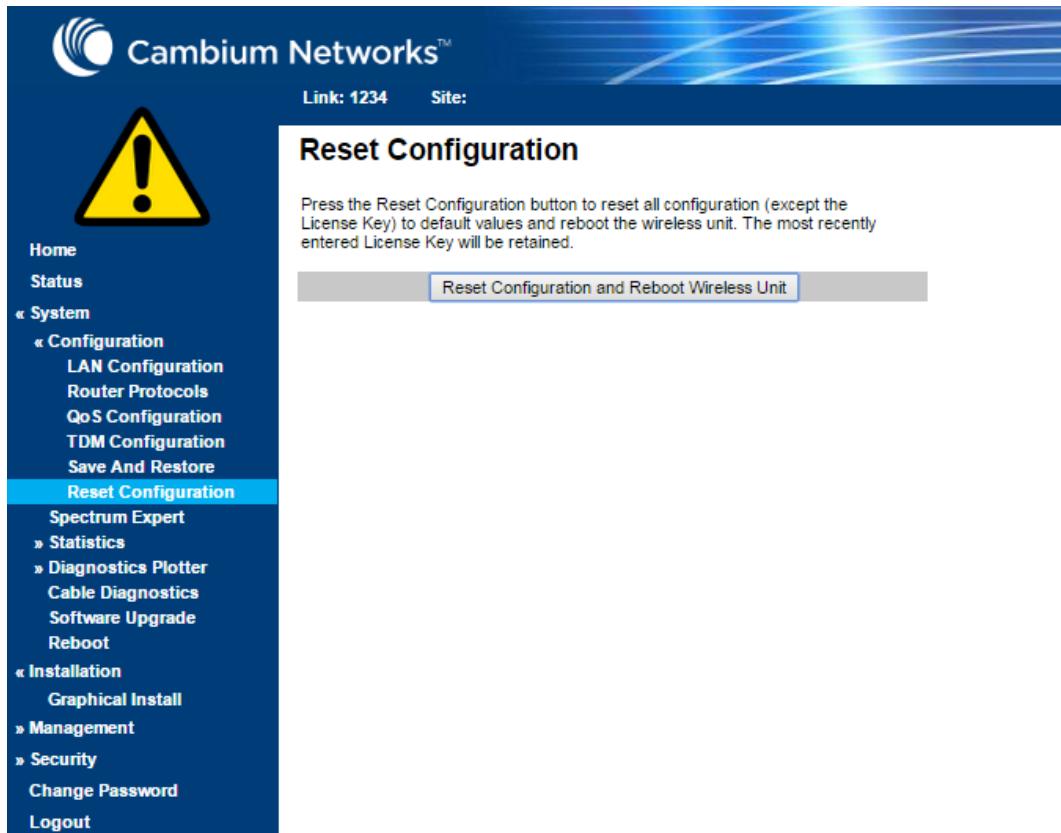
- To save the configuration:
 - Click **Save Configuration File**.
 - Save the file. The default filename is in the format **MAC-mm-mm-mm_IP-iii-iii-iii.cfg**, where **mm-mm-mm** is MAC address of unit and **iii-iii-iii-iii** is Internet address of unit.
- To restore the configuration:
 - Click **Browse**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

Reset Configuration page

Menu option: **System > Configuration > Reset Configuration**. Use this page to reset the ODU configuration to default settings, retaining the most recently entered License Key (Figure 163).

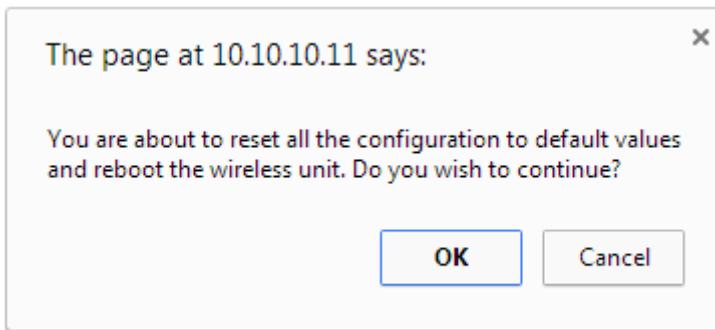
The Reset Configuration page resets the configuration to default settings. After successful execution of Reset Configuration, the ODU reboots and is then accessible via the default IP address (i.e. 169.254.1.1).

Figure 163 Reset Configuration page



Procedure:

- Click **Reset Configuration**. The user pop up box is displayed to reconfirm:



- Click **OK** to restore configuration to the default settings and reboot of unit.

Further reading

For information about...	Refer to...
Erase Configuration	Use this option to erase the entire configuration of the unit. Refer to Resetting all configuration data on page 7-82.

Software Upgrade page

Menu option: **System > Software Upgrade** ([Figure 164](#)).

Use this page to upgrade the unit to a new version of PTP 670 operational software.

Figure 164 Software Upgrade page



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 670 Series](#).

- If the support web page contains a later Software Version than that installed on the PTP 670 unit, perform the procedure below.

Procedure:

- 1 Save the system configuration; see [Save and Restore Configuration page](#) on page 6-64.
- 2 On the Cambium Support web page, select the latest PTP 670 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

© 2000-2015 Cambium Networks Limited. All rights reserved.
Software Version: 45700-00-04

Uploaded software image description

© 2000-2015 Cambium Networks Limited. All rights reserved.
Software Version: 45700-00-05

[Program Software Image into Non-Volatile Memory](#)

 [Back](#)

- 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

© 2000-2015 Cambium Networks Limited. All rights reserved.
Software Version: 45700-00-05

[Reboot Wireless Unit](#)

 [Back](#)

- 6 Click **Reboot Wireless Unit**, then click **OK** to confirm. The unit reboots with the new software installed.
- 7 Save the post-upgrade system configuration; see [Save and Restore Configuration page](#) on page 6-64.

Management menu

This section describes how to configure web-based management of the PTP 670 unit.

Web-Based Management page

Menu option: **Management > Web** ([Figure 165](#)).

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

Figure 165 Web-Based Management page

Web-Based Management

Attributes	Value	Units
HTTPS Access Enabled	<input type="radio"/> No <input checked="" type="radio"/> Yes	
HTTPS Port Number	443	
HTTP Access Enabled	<input type="radio"/> No <input checked="" type="radio"/> Yes	
HTTP Port Number	80	
Telnet Access Enabled	<input type="radio"/> No <input checked="" type="radio"/> Yes	
Telnet Port Number	23	
Access Control	<input type="radio"/> Disabled <input checked="" type="radio"/> 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	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
SNMP Control Of Passwords	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
TFTP Client	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Debug Access Enabled	<input checked="" type="radio"/> No <input type="radio"/> Yes	
Cross Site Request Forgery Protection	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
<input style="margin-right: 10px;" type="button" value="Submit Updated Configuration"/> <input type="button" value="Reset Form"/>		



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. ([Enter HTTPS Configuration](#) on page [6-109](#)).

Procedure:

- Review and update the attributes ([Table 172](#)).
- To save changes, click **Submit Updated Configuration**.

Table 172 Web-Based Management attributes

Attribute	Meaning
HTTPS Access Enabled	Only displayed when HTTPS is configured. No: The unit will not respond to any requests on the HTTPS port. Yes: The unit will respond to requests on the HTTPS port.
HTTPS Port Number	Only displayed when HTTPS is configured. The port number for HTTPS access. A value of zero means the wireless unit uses the default port.
HTTP Access Enabled	No: The unit will not respond to any requests on the HTTP port. Yes: The unit will respond to requests on the HTTP port. Remote management via HTTPS is not affected by this setting.
HTTP Port Number	The port number for HTTP access. A value of zero means the wireless unit uses the default port.
Telnet Access Enabled	No: The unit will not respond to any requests on the Telnet port. Yes: The unit will respond to requests on the Telnet port.
Telnet Port Number	The port number for Telnet access. A value of zero means the wireless unit uses the default port.
Access Control	Enables or disables access control to web-based management by Internet Address.
Access Control Internet Address 1/2/3	A list of up to three IPv4 or IPv6 Addresses permitted to perform web-based management. Only displayed when Access Control is set to Enabled .
SNMP Control of HTTP And Telnet	Disabled: Neither HTTP nor Telnet can be controlled remotely via SNMP. Enabled: Both HTTP and Telnet can be controlled remotely via SNMP.
SNMP Control of Passwords	Enabled: Passwords for identity-based user accounts in the web-based interface can be updated via SNMP. This option can be used together with SNMPv3 to provide a secure means to update passwords from a central network manager. Disabled: Passwords for identity-based user accounts can be updated only via the web-based interface (default).
TFTP Client	Disabled: The unit will not respond to any TFTP software download requests. Enabled: Software can be downloaded via TFTP, as described in Upgrading software using TFTP on page 6-127 .
Debug Access Enabled	Yes: Cambium Technical Support is allowed to access the system to investigate faults.

Attribute	Meaning
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 166) or **Enabled** (Figure 167).

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 reset from the Zeroize CSPs page ([Zeroize CSPs page](#) on page 6-117).

Figure 166 Local User Accounts page (Identity Based User Accounts disabled)

Local User Accounts

Local User Account Management

Attributes	Value	Units
Identity Based User Accounts	<input checked="" type="radio"/> Disabled <input type="radio"/> 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	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	
<input type="button" value="Submit User Account Updates"/> <input type="button" value="Reset To Factory Defaults"/>		

Figure 167 Local User Accounts page (Identity Based User Accounts enabled)

Local User Accounts						
Local User Account Management						
Attributes	Value	Units				
Identity Based User Accounts	<input type="radio"/> Disabled <input checked="" type="radio"/> 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	<input checked="" type="radio"/> Timeout <input type="radio"/> Disable Account					
Login Attempt Lockout Period	1	minutes				
Password Expiry Action	<input checked="" type="radio"/> Force Password Change <input type="radio"/> Disable Account					
Password Complexity Configuration						
Minimum Password Length	Off ▾ characters					
Password Can Contain User Name	<input type="radio"/> No <input checked="" type="radio"/> 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	<input checked="" type="radio"/> No <input type="radio"/> Yes					
Minimum Characters That Must Change	Off ▾ characters					
Password Reuse	<input checked="" type="radio"/> Permitted <input type="radio"/> Prohibited					
Special Characters	!#%&(*+,.-/;<=>?@[{}]^_`{})~					
<input type="button" value="Set Default Complexity"/> <input type="button" value="Set Best Practice Complexity"/>						
User	Name	Role	Password	Password Confirm	Force Password Change	Disable
1	security	Security Officer	<input type="checkbox"/>	<input type="checkbox"/>
2	admin	System Administrator	<input type="checkbox"/>	<input type="checkbox"/>
3	readonly	Read Only	<input type="checkbox"/>	<input type="checkbox"/>
4	readonly2		<input type="checkbox"/>	<input checked="" type="checkbox"/>
5	readonly3		<input type="checkbox"/>	<input checked="" type="checkbox"/>
6	readonly4		<input type="checkbox"/>	<input checked="" type="checkbox"/>
7	readonly5		<input type="checkbox"/>	<input checked="" type="checkbox"/>
8	readonly6		<input type="checkbox"/>	<input checked="" type="checkbox"/>
9	readonly7		<input type="checkbox"/>	<input checked="" type="checkbox"/>
10	readonly8		<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="button" value="Submit User Account Updates"/> <input type="button" value="Reset To Factory Defaults"/>						

Procedure:

- Choose whether to set Identity Based User Accounts to **Disabled** or **Enabled**.
- Review and update the Local User Account Management attributes (Table 173).
- If Identity Based User Accounts is set to **Enabled**:
 - Review and update the Password Complexity Configuration attributes (Table 174). 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 175).
- If any attributes have been updated, click **Submit User Account Updates**.

Table 173 Local User Account Management attributes

Attribute	Meaning
Identity Based User Accounts	Disabled: Access to the web interface is controlled by a single system administration password. Enabled: Up to 10 users may access the unit.
Auto Logout Period	The time without user activity that elapses before a user is automatically logged out (minutes). A value of zero disables this feature.
Minimum Password Change Period	The minimum time that elapses before a user is allowed to change a password (minutes). A value of zero disables this feature.
Password Expiry Period	The time that elapses before a password expires (days). A value of zero disables this feature.
Maximum Number of Login Attempts	The maximum number of login attempts (with incorrect password) that are allowed before a user is locked out. Also, the maximum number of password change attempts before a user is locked out.
Login Attempt Lockout Action	Only displayed when Identity Based User Accounts is Enabled . Timeout: When a user is locked out, the user is allowed to log in again after a specified period. Disabled: When a user is locked out, the user is disabled.
Login Attempt Lockout Period	Only displayed when Identity Based User Accounts is Disabled . The time that elapses before a locked out user is allowed to log in again (minutes). Only displayed when Login Attempt Lockout Action is set to Timeout .
Password Expiry Action	Only displayed when Identity Based User Accounts is Enabled . The action to be taken by the PTP 670 when a password expires.

Table 174 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
Match Reversed Patterns	No: Reversed patterns are not checked. Yes: Reversed patterns are checked. For example, if Maximum Repeated Pattern Length is set to 3 and Match Reversed Patterns is set to Yes , then AB1221BA will be rejected.	Yes
Minimum Characters That Must Change	The minimum number of password characters that must change every time a password is updated.	4
Password Reuse	Permitted: A user may reuse a previous password. Prohibited: A user must not reuse a previous password.	Prohibited

Attribute	Meaning	Best practice
Special Characters	User defined set of special characters used in password construction. The only characters permitted in a password are: (a-z), (A-Z), (0-9) and any of the special characters entered here.	!"%&'()*+-,.:/;<=>?

Table 175 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 174).
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 168](#)).

Use this page to configure RADIUS authentication. RADIUS authentication is only available when PTP 670 is configured for Identity-based User Accounts and when RADIUS servers are connected to the network.

Figure 168 RADIUS Configuration page

RADIUS Configuration		
Attributes	Value	Units
RADIUS Client	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	
RADIUS Primary Server	<input checked="" type="radio"/> Server 1 <input type="radio"/> Server 2	
RADIUS Primary Server Dead Time	5	minutes
RADIUS Server Retries	2	
RADIUS Server Timeout	3	seconds
Authentication Method	<input checked="" type="radio"/> CHAP <input type="radio"/> 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		
Submit RADIUS Configuration		



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 176](#)).
- Click **Submit RADIUS Configuration**.

Table 176 RADIUS Authentication attributes

Attribute	Meaning
RADIUS Client Enabled	Enabled: PTP 670 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 670 will retry after a RADIUS server fails to respond to an initial request.
RADIUS Server Timeout	Time (in seconds) the PTP 670 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.
RADIUS Server Shared Secret Confirm	Shared secret confirmation.

Webpage Properties page

Menu option: **Management > Web > Web Properties** ([Figure 169](#)).

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

Figure 169 Webpage Properties page

Webpage Properties

Properties

Attributes	Value	Units
Web Properties	<input checked="" type="checkbox"/> View Summary and Status pages without login <input type="checkbox"/> Disable Spectrum Expert (use old Spectrum Management)	
Distance Units	<input checked="" type="radio"/> Metric <input type="radio"/> Imperial	
Use Long Integer Comma Formatting	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Transmitter Mute Control	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	
Transmitter Channels Control	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	
Auto Logout Period	10	minutes
Browser Title	\$productName	
<input type="button" value="Apply Properties"/> <input type="button" value="Reset Form"/>		

Procedure:

- Update the attributes (Table 177).
- Click Apply Properties.

Table 177 Webpage Properties attributes

Attribute	Meaning
Web Properties	<p>View Summary and Status pages without login:</p> <ul style="list-style-type: none"> 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 7-19. <p>Disable Spectrum Expert (use old Spectrum Management):</p> <ul style="list-style-type: none"> If not ticked (the default setting), the System Menu includes Spectrum Expert (not Spectrum Management). If ticked, the System Menu includes Spectrum Management (not Spectrum Expert).
Distance Units	<p>Metric: Distances are displayed in kilometers or meters.</p> <p>Imperial: Distances are displayed in miles or feet.</p>
Use Long Integer Comma Formatting	<p>Disabled: Long integers are displayed thus: 1234567.</p> <p>Enabled: Long integers are displayed thus: 1,234,567.</p>
Transmitter Mute Control	<p>Disabled: Hides the Enable Transmission attribute.</p> <p>Enabled: Shows the Enable Transmission attribute (System Configuration page on page 6-39).</p>

Attribute	Meaning
Transmitter Channels Control	Disabled: Hides the Transmitter Channels attribute. Enabled: Shows the Transmitter Channels attribute (Wireless Configuration page on page 6-25 , and System Configuration page on page 6-39).
Send HTTPS Close Notify Alerts	Only displayed when HTTPS is configured. Controls whether or not the HTTPS server sends TLS Close Notify Alerts before it shuts down each socket. Disabled: TLS Close Notify Alerts are not sent before closing each socket. This is the default because these alerts can cause problems with some browsers (e.g. Internet Explorer) Enabled: TLS Close Notify Alerts are sent before closing each socket.
Auto Logout Period	Only displayed if role-based user accounts are in use. Automatic logout period in minutes. If there is no user activity within this time, the user is required to log in again. Think this is only displayed when not using identity based user accounts.
Browser Title	By default, web browser tab titles display PTP 670 model, page title and IP address in the following format: "Cambium PTP 45670 – " & pageName & " (IP = " & ipAddress & ")" To change the default text, enter simple text and optional variables (prefixed with a \$ character). The full list of variables is in Table 178 .

Table 178 Browser Title attribute variables

Variable	Meaning
\$siteName	Site Name, as set in the System Configuration page (Table 159).
\$linkName	Link Name, as set in the System Configuration page (Table 159).
\$masterSlaveMode	Master Slave Mode, as set in the Step 2: Wireless Configuration page (Table 155).
\$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 159): <ul style="list-style-type: none">• 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 160).
\$ipv6Address	IPv6 Address of the ODU, as set in the LAN Configuration page (Table 160).

Variable	Meaning
\$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 160).
\$sysName	Sys Name for this SNMP managed node, as set in the Step 2: SNMP MIB-II System Objects page (Table 184).
\$productName	The product variant, for example Cambium PTP 670 . Not updateable.
\$pageName	Name of the page currently being browsed.

Email Configuration page

Menu option: **Management > Email** (Figure 170). Use this page to enable the PTP 670 to generate Simple Mail Transfer Protocol (SMTP) email messages to notify the system administrator when certain events occur.

Figure 170 Email Configuration page

Email Configuration

Attributes	Value	Units
SMTP Email Alert	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
SMTP Enabled Messages	<input checked="" type="checkbox"/> Wireless Link Up Down <input checked="" type="checkbox"/> Channel Change <input checked="" type="checkbox"/> DFS Impulse Interference <input type="checkbox"/> Enabled Diagnostic Alarms <input type="checkbox"/> Main PSU Port Up Down <input type="checkbox"/> Aux Port Up Down <input type="checkbox"/> SFP Port Up Down <input type="checkbox"/> NIDU Lan Port Up Down	
SMTP Server Internet Address	<input type="text"/>	
SMTP Server Port Number	<input type="text" value="25"/>	
SMTP Source Email Address	<input type="text"/>	
SMTP Destination Email Address	<input type="text"/>	
Send SMTP Test Email	<input type="checkbox"/> Yes	
<input type="button" value="Submit Updated Configuration"/> <input type="button" value="Reset Form"/>		

Procedure:

- Update the attributes (Table 179).
- 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 179 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 670 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 670 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 171).

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

Figure 171 Diagnostic Alarms page

Diagnostic Alarms		
Attributes	Value	Units
	<input checked="" type="checkbox"/> Regulatory Band	
	<input checked="" type="checkbox"/> Install Status	
	<input checked="" type="checkbox"/> Install Arm State	
	<input checked="" type="checkbox"/> Unit Out Of Calibration	
	<input checked="" type="checkbox"/> Maximum Link Range Exceeded	
	<input checked="" type="checkbox"/> Incompatible Regulatory Bands	
	<input checked="" type="checkbox"/> Incompatible Master And Slave	
	<input checked="" type="checkbox"/> Port State	
	<input checked="" type="checkbox"/> No Wireless Channel Available	
	<input checked="" type="checkbox"/> SNTP Synchronization Failed	
	<input checked="" type="checkbox"/> Wireless Link Disabled Warning	
	<input checked="" type="checkbox"/> TDD Synchronization Alarm	
	<input checked="" type="checkbox"/> Link Mode Optimization Mismatch	
	<input checked="" type="checkbox"/> Syslog Disabled Warning	
	<input checked="" type="checkbox"/> Syslog Local Nearly Full	
	<input checked="" type="checkbox"/> Syslog Local Wrapped	
	<input checked="" type="checkbox"/> Syslog Client Disabled Warning	
	<input checked="" type="checkbox"/> Data Bridging Status	
	<input checked="" type="checkbox"/> Remaining Full Capacity Trial Time	
	<input checked="" type="checkbox"/> Capacity Variant Mismatch	
	<input checked="" type="checkbox"/> TDM Alarms	

Procedure:

- Tick the required alarms. These alarms are described in [Alarms](#) on page 7-20.
- Click **Submit Updated Configuration**.

Time Configuration page

Menu option: **Management > Time** ([Figure 172](#) and [Figure 173](#)). Use this page to set the real-time clock of the PTP 670.

Setting the real-time clock manually

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

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

Procedure:

- Set SNTP State to **Disabled** ([Figure 172](#)).
- Review and update the manual clock attributes ([Table 180](#)).
- Click **Submit Updated Configuration**.

Figure 172 Time Configuration page (SNTP disabled)

Attributes	Value	Units
SNTP State	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	
Set Time	00 : 00 : 00	
Set Date	2005 <input type="button" value="▼"/> Jan <input type="button" value="▼"/> 1 <input type="button" value="▼"/>	
Local Time Settings		
Time Zone	GMT 00.00 <input type="button" value="▼"/>	
Daylight Saving	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	
<input type="button" value="Submit Updated Configuration"/> <input type="button" value="Reset Form"/>		

Table 180 Manual clock attributes

Attribute	Meaning
SNTP State	Disabled: the PTP 670 will keep time without connecting to a networked time server.
Set Time	Set hours, minutes and seconds.
Set Date	Set year, month and day.
Time Zone	Set the time zone offset from Greenwich Mean Time (GMT). To set the clock to UTC time, set Time Zone to GMT 00.00 .
Daylight Saving	Disabled: There is no offset for daylight saving time. Enabled: System clock is moved forward one hour to adjust for daylight saving time. To set the clock to UTC time, set Daylight Saving to Disabled .

Setting the real-time clock to synchronize using SNTP

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

Procedure:

- Set the SNTP State attribute to **Enabled** ([Figure 173](#)).
- Review and update the SNTP clock attributes ([Table 181](#)).
- Click **Submit Updated Configuration**.

Figure 173 Time Configuration page (SNTP enabled)

Time Configuration		
Attributes	Value	Units
SNTP State	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
SNTP Primary Server	<input checked="" type="radio"/> Server 1 <input type="radio"/> 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	01-Jan-2005 00:02:57: OK.	
SNTP Server Internet Address	169.254.1.110	
SNTP Server Port Number	123	
SNTP Server Authentication Protocol	<input checked="" type="radio"/> None <input type="radio"/> 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	<input checked="" type="radio"/> None <input type="radio"/> MD5	
SNTP Server Key Identifier	1	
Server Key	-----	
Server Key Confirm	-----	
Status		
SNTP Sync	In Sync	
SNTP Last Sync	17-Feb-2014 10:36:22	
System Clock	17-Feb-2014 10:36:24	
Local Time Settings		
Time Zone	GMT 00:00 ▾	
Daylight Saving	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	
<input type="button" value="Submit Updated Configuration"/> <input type="button" value="Reset Form"/>		

Table 181 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.
SNTP Sync	This shows the current status of SNTP synchronization. If No Sync is displayed, then review the SNTP Server Internet Address and Port Number. A change of state may generate an SNMP trap or SMTP email alert.
SNTP Last Sync	This shows the date and time of the last SNTP synchronization.
System Clock	This displays the local time, allowing for the Time Zone and Daylight Saving settings.
Local Time Settings:	
Time Zone	Set the time zone offset from Greenwich Mean Time (GMT). To set the clock to UTC time, set Time Zone to GMT 00.00 .

Attribute	Meaning
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 174](#)).

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

Figure 174 Syslog Configuration page

Syslog Configuration

Attributes	Value	Units
Syslog State	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Syslog Client	<input type="radio"/> Disabled <input checked="" type="radio"/> 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	
<input type="button" value="Submit Updated Configuration"/> <input type="button" value="Reset Form"/>		



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 6-84](#)).

Procedure:

- Update the attributes ([Table 182](#)).
- Click **Submit Updated Configuration**.

Table 182 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	The IPv4 or IPv6 Address of the syslog server.
Internet Address	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 175](#)).

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

Figure 175 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	
Continue to SNMP Wizard		

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 176).

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

Figure 176 Step 1: SNMP Configuration page (for SNMPv3)

Attributes	Value	Units
SNMP Minimum Privilege Level	<input type="radio"/> System Administrator <input checked="" type="radio"/> Security Officer	
SNMP State	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
SNMP Access Control	<input type="radio"/> Disabled <input checked="" type="radio"/> 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	<input type="radio"/> v1/2c <input checked="" type="radio"/> v3	
SNMP Security Mode	<input checked="" type="radio"/> MIB-based <input type="radio"/> Web-based	
SNMP Engine ID Format	<input type="radio"/> MAC Address <input type="radio"/> IPv4 Address <input checked="" type="radio"/> Text String <input type="radio"/> IPv6 Address	
SNMP Engine ID Text		
SNMP Port Number	161	

Next >>

Procedure:

- Set SNMP State to **Enabled**.
- Set SNMP Version to **v3**. The page is redisplayed with SNMPv3 attributes.
- Update the attributes (Table 183).
- Click **Next**.

Table 183 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 173).
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 6-94 .
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 177](#)).

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

Figure 177 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	

Back **Next**

Procedure:

- Update the attributes ([Table 184](#)).
- 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 6-94](#).
 - If **MIB-based**, go to [Confirm SNMP Configuration \(for SNMPv3\) on page 6-98](#).

Table 184 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 178).

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 185).
- Click **Next**.

Figure 178 Step 3: SNMP User Policy Configuration page (for SNMPv3)

Step 3: SNMP User Policy Configuration

Attributes	Value	Units
System Admin Policy		
Security Level	<input type="radio"/> No Auth No Priv <input type="radio"/> Auth No Priv <input checked="" type="radio"/> Auth Priv	
Authentication Protocol	MD5	
Privacy Protocol	DES	
Read Only Policy		
Security Level	<input type="radio"/> No Auth No Priv <input type="radio"/> Auth No Priv <input checked="" type="radio"/> Auth Priv	
Authentication Protocol	MD5	
Privacy Protocol	DES	
◀◀ Back		Next ▶▶

Table 185 Step 3: SNMP User Policy Configuration attributes (for SNMPv3)

Attribute	Meaning
Security Level	<p>Defines the security level and associated protocols that are required to allow SNMP users to access the PTP 670.</p> <p>No Auth No Priv: Users are not required to use authentication or privacy protocols.</p> <p>Auth No Priv: Users are required to use only authentication protocols.</p> <p>Auth Priv: Users are required to use both authentication and privacy protocols.</p>
Authentication Protocol	<p>The authentication protocol to be used to access the PTP 670 via SNMP.</p> <p>This is disabled when Security Level is set to Auth No Priv.</p> <p>MD5: Message Digest Algorithm is used.</p> <p>SHA: NIST FIPS 180-1, Secure Hash Algorithm SHA-1 is used.</p>

Attribute	Meaning
Privacy Protocol	The privacy protocol to be used to access the PTP 670 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 179).

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 179 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				
Reset To Default Settings						
◀◀ Back				Next ▶▶		

Procedure:

- Update the individual user attributes (Table 186) for up to 10 SNMP users.
- Click **Next**.

Table 186 Step 4: SNMP User Accounts Configuration attributes (for SNMPv3)

Attribute	Meaning
Name	Name to be used by the SNMP user to access the system.
Role	Selects which of the two web-based security profiles are applied to this user: System administrator or Read only . Select Disabled to disable the SNMP account.
Auth/Priv	Indicates whether the Passphrase applies to authentication or privacy protocols.
Passphrase	The phrase to be entered by this SNMP user to access the system using an authentication or privacy protocol. Length must be between 8 and 32 characters. May contain spaces. The Auth Passphrase is hidden when Security Level for this user's Role is set to No Auth No Priv . The Priv Passphrase is hidden when Security Level for this user's Role is set to No Auth No Priv or Auth No Priv .
Passphrase Confirm	Passphrase must be reentered to confirm it has been correctly typed.

Step 5: SNMP Trap Configuration (for SNMPv3)

Menu option: **Management > SNMP**. Part of the SNMP Wizard ([Figure 180](#)).

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 180 Step 5: SNMP Trap Configuration page (for SNMPv3)

Step 5: SNMP Trap Configuration

Attributes	Value	Units
SNMP Enabled Traps	<input checked="" type="checkbox"/> Cold Start	
	<input checked="" type="checkbox"/> Wireless Link Up Down	
	<input checked="" type="checkbox"/> Channel Change	
	<input checked="" type="checkbox"/> DFS Impulse Interference	
	<input type="checkbox"/> Enabled Diagnostic Alarms	
	<input checked="" type="checkbox"/> Authentication Failure	
	<input type="checkbox"/> Main PSU Port Up Down	
	<input type="checkbox"/> Aux Port Up Down	
	<input type="checkbox"/> SFP Port Up Down	
Trap Receiver 1		
SNMP Trap Receiver Enabled	<input type="radio"/> Disabled <input checked="" type="radio"/> 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	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
SNMP Trap Internet Address	2001:DB8::17	
SNMP Trap Port Number	162	
SNMP Trap User Account	User 2: readonly	▼
 Back		Next 

Procedure:

- Update the attributes ([Table 187](#)).
- Click **Next**.

Table 187 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 181).

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

Figure 181 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		
SNMP Trap Receiver Enabled	Disabled	
<input style="border: 1px solid black; border-radius: 5px; padding: 2px 10px; width: 100%;" type="button" value="Confirm SNMP Configuration and Reboot"/>		
◀◀ Back		

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 175](#)).

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 182](#)).

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

Figure 182 Step 1: SNMP Configuration page (for SNMPv1/2c)

Step 1: SNMP Configuration		
Attributes	Value	Units
SNMP Minimum Privilege Level	<input type="radio"/> System Administrator <input checked="" type="radio"/> Security Officer	
SNMP State	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
SNMP Access Control	<input type="radio"/> Disabled <input checked="" type="radio"/> 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	<input checked="" type="radio"/> v1/2c <input type="radio"/> v3	
SNMP Community String	public	
SNMP Port Number	161	

Next >>

Procedure:

- Set SNMP State to **Enabled**.
- Set SNMP Version to **v1/2c**. The page is redisplayed with SNMPv1/2c attributes.
- Update the attributes ([Table 188](#)).
- Click **Next**.

Table 188 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 173).
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 670 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 177](#)). Use this page to enter details of the SNMP managed node. Update the attributes ([Table 184](#)) and click **Next**.

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

Menu option: **Management > SNMP**. Part of the SNMP Wizard (Figure 183).

Figure 183 Step 3: SNMP Trap Configuration page (for SNMPv1/2c)

Step 3: SNMP Trap Configuration		
Attributes	Value	Units
SNMP Trap Version	<input type="radio"/> v1 <input checked="" type="radio"/> v2c	
SNMP Enabled Traps	<input checked="" type="checkbox"/> Cold Start	
	<input checked="" type="checkbox"/> Wireless Link Up Down	
	<input checked="" type="checkbox"/> Channel Change	
	<input checked="" type="checkbox"/> DFS Impulse Interference	
	<input type="checkbox"/> Enabled Diagnostic Alarms	
	<input checked="" type="checkbox"/> Authentication Failure	
	<input type="checkbox"/> Main PSU Port Up Down	
	<input checked="" type="checkbox"/> Aux Port Up Down	
	<input type="checkbox"/> SFP Port Up Down	
Trap Receiver 1		
SNMP Trap Receiver Enabled	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
SNMP Trap Internet Address	2001:DB8::16	
SNMP Trap Port Number	162	
Trap Receiver 2		
SNMP Trap Receiver Enabled	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
SNMP Trap Internet Address	1.11.100.17	
SNMP Trap Port Number	162	
<input style="float: left; margin-right: 10px;" type="button" value="Back"/> <input style="float: right;" type="button" value="Next"/>		

Procedure:

- Update the attributes (Table 189).
- Click **Next**.

Table 189 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 184).

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

Figure 184 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	
<input type="button" value="Confirm SNMP Configuration and Reboot"/>		
◀◀ Back		

Procedure:

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

Security menu

This section describes how to configure security options using the Security Wizard.



Caution

Ensure that the operator's security requirements are configured before connecting the PTP 670 to the network. Otherwise, security may be compromised.

Preparation

Obtain the necessary cryptographic material as described in:

- [Using the Security Wizard](#) on page [3-56](#).
- [Planning for wireless encryption](#) on page [3-57](#).
- [Planning for HTTPS/TLS operation](#) on page [3-59](#).
- [Planning for protocols and ports](#) on page [3-60](#).

Ensure that the ODU has the AES license. If necessary, order the necessary AES capability upgrade, generate a license key ([Generating license keys](#) on page [6-3](#)) and enter it on the Software License Key page ([Software License Key page](#) on page [6-13](#)).

On the Local User Accounts page ([Local User Accounts page](#) on page [6-72](#)), 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 185](#)). Use this page to review the current security configuration of the unit.

Figure 185 Security Configuration Wizard page

Security Configuration Wizard		
This page shows a summary of the current security configuration. Press the 'Continue to Security Wizard' button below to change this configuration.		
Security configuration		
Attributes	Value	Units
Key of Keys	Not configured	
DRNG Entropy	Not configured	
User Defined Security Banner		
Require Acknowledgement Of Notices	No	
Display Login Information	No	
HTTPS Access Enabled	No	
Encryption Algorithm	TLS RSA	
TLS Minimum Security Level	None	
Device Certificate	Factory	
Authorization Method	Blacklist	
HTTP Access Enabled	Yes	
HTTP Port Number	80	
Telnet Access Enabled	No	
SNMP Control Of HTTP And Telnet	Enabled	
SNMP Control Of Passwords	Disabled	
TFTP Client	Enabled	
Debug Access Enabled	Yes	
Cross Site Request Forgery Protection	Enabled	
Continue to Security Wizard		

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

Security options

Menu option: **Security**. Part of the Security Wizard (Figure 186).

Select optional security features.

Keys of Keys, Entropy, and HTTP and Telnet Options are always enabled.

Set the remaining options to **No** to disable the associated feature, or set to **Yes** to enable the associated feature. Enabled features are configured in the remaining pages of the Security Wizard.

Figure 186 Security Options page

Select Security Configuration Options

This page enables or disables the security features in the ODU. Key of Keys, Entropy, and HTTP and Telnet Options are always enabled. Enabled features are configured later in the Security Wizard.

Click on Next to continue.

Key of Keys	Yes
Entropy	Yes
Security Banner	<input checked="" type="radio"/> Yes <input type="radio"/> No
Login Information	<input checked="" type="radio"/> Yes <input type="radio"/> No
HTTPS Configuration	<input checked="" type="radio"/> Yes <input type="radio"/> No
Wireless Security	<input checked="" type="radio"/> Yes <input type="radio"/> No
HTTP and Telnet Options	Yes

Next 

Key of Keys

Menu option: **Security**. Part of the Security Wizard (Figure 187 and Figure 188).

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 187 Key of Keys page

Enter Key of Keys

Key Of Keys
Confirm Key Of Keys

 **Back** **Next** 

Figure 188 Key of Keys page with configured value

Enter Key of Keys

Enter a 256-bit random number formatted as 64 hexadecimal characters.
For example: FDDFF8E045AFD2B8C83E19424D8AE9FBE8A31C227155647634079641EAE34995.

Use a different Key of Keys on each ODU. The Key of Keys is used to encrypt Critical Security Parameters (CSPs) stored in the unit's non-volatile memory. If the Key of Keys is changed, all of the remaining CSPs must be re-entered.

Click on Next to continue.

Click next to use the new Key of Keys

Thumbprint Algorithm: SHA-1

Thumbprint: *** 77 cf 12 1f**

Key Of Keys
Confirm Key Of Keys

Back **Next**

**Caution**

Erasing or changing the key of keys resets all CSPs.

Procedure:

- If the Keys of Keys has already been configured, check the SHA-1 thumbprint, otherwise
- Enter and confirm the generated Key of Keys.
- Click **Next**.

Entropy

Menu option: **Security**. Part of the Security Wizard ([Figure 189](#) and [Figure 190](#)).

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

Figure 189 Entropy page

Enter Random Number Entropy Input

Enter a 512-bit random number formatted as 128 hexadecimal characters. For example:
368BF4EE0E771421FD4CE5F8D7E6E7C82AE547D6B852F71A2A850443024625FAD2328F6BAB601102D9455C72CDD5A2FC5BEB64EE26EB846A58A6A268967EA5FE.

Use a different Entropy Input on each ODU. The Entropy Input is used to seed the unit's random number generator.

Click on Next to continue.

Entropy Input
Confirm Entropy Input

Back **Next**

Figure 190 Entropy page with configured value

Enter Random Number Entropy Input

Enter a 512-bit random number formatted as 128 hexadecimal characters. For example:
368BF4EE0E771421FD4CE5F8D7E6E7C82AE547D6B852F71A2A850443024625FAD2328F6BAB601102D9455C72CDD5A2FC5BEB64EE26EB846A58A6A268967EA5FE.

Use a different Entropy Input on each ODU. The Entropy Input is used to seed the unit's random number generator.

Click on Next to continue.

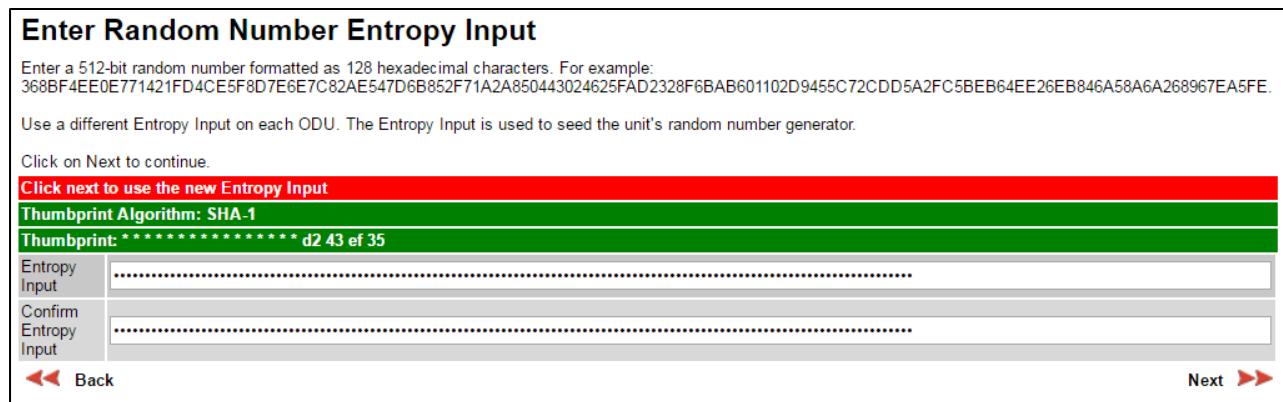
Click next to use the new Entropy Input

Thumbprint Algorithm: SHA-1

Thumbprint: *** d2 43 ef 35**

Entropy Input
Confirm Entropy Input

Back **Next**

**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**.

Enter User Security Banner

Menu option: **Security**. Part of the Security Wizard (Figure 191).

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

Figure 191 Enter User Security Banner page

Enter User Security Banner

Enter banner text to be displayed when users log in to web-based management. Select Yes to require the user to acknowledge the security banner.

Click on Next to continue.

Usage Summary	28 of 1499 characters used
User Defined Security Banner	Text for the Security Banner
Require Acknowledgement Of Notices	<input type="radio"/> No <input checked="" type="radio"/> Yes

Back **Next**

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

Text for the Security Banner

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**.

Enter Login Information Settings

Menu option: **Security**. Part of the Security Wizard (Figure 192).

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

Figure 192 Enter Login Information Settings page

Enter Login Information Settings

Login Information provides details of the most recent successful login and unsuccessful login attempts. An example of Login Information is shown below. Click on Next to continue.

Attributes	Value	Units
Display Login Information	<input type="radio"/> No <input checked="" type="radio"/> Yes	

Back **Next**

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

Successful login	
Time Of Last Login	14-Jun-2017 14:04:15
Internet Address Of Last Login	169.254.1.100
Unsuccessful login attempts	
Number Of Unsuccessful Login Attempts	1
New Unsuccessful Login Attempts	0
Time Of Last Unsuccessful Login Attempt	14-Jun-2017 14:04:13
Internet Address Of Last Unsuccessful Login Attempt	169.254.1.100

Procedure:

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

Enter HTTPS Configuration

Menu option: **Security**. Part of the Security Wizard (Figure 193 and Figure 194).

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

Figure 193 Enter HTTPS Configuration page

Enter HTTPS Configuration

Upload the RSA Private Key and Public Certificate for the HTTPS interface using 2048-bit key size and SHA256. The certificate subject must be the ODU's IP Address, for example 169.254.1.1. Input must be in Distinguished Encoding Rules (DER) format.

Click on Next to continue.

HTTPS Port Number	443	
TLS Private Key	Choose File key-1119.der	DER format
TLS Public Certificate	Choose File cert-1119.der	DER format

Back **Next**

Figure 194 Configured HTTPS Configuration page

Enter HTTPS Configuration

Upload the RSA Private Key and Public Certificate for the HTTPS interface using 2048-bit key size and SHA256. The certificate subject must be the ODU's IP Address, for example 169.254.1.1. Input must be in Distinguished Encoding Rules (DER) format.

Click on Next to continue.

HTTPS Port Number	443		
Click next to use the key from file key-1119.der			
Thumbprint Algorithm: SHA-1			
Thumbprint: ***** a1 56 78 e1			
TLS Private Key	Choose File	No file chosen	DER format
Click next to use the certificate from file cert-1119.der			
Thumbprint Algorithm: SHA-1			
Thumbprint: ***** 81 3c 09 25			
TLS Public Certificate	Choose File	No file chosen	DER format
Back		Next	

**Caution**

If the certificates expire, your web browser will display security warnings. Always investigate the cause of security warnings, and rectify errors in the content or expiry of certificates where necessary. Do not accept or ignore web browser security warnings.

Procedure:

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

Configure Wireless Security

Menu option: **Security**. Part of the Security Wizard ([Figure 195](#) to [Figure 199](#)).

Use this page to enable device authentication and authorization, and AES encryption of the wireless link. Wireless link encryption key is used to encrypt all traffic over the PTP 670 wireless link.

Figure 195 Wireless Link Encryption Settings, TLS-RSA

Enter Wireless Link Encryption Settings

Wireless Security provides device authentication and privacy at the wireless interface. Select the same Encryption Algorithm for the local and remote ODUs.

With the TLS RSA option select "Factory" to use the factory-installed key and certificate or "User" to provide a user-generated key and certificate in a later page.

Select the minimum security level that can be allowed in the link.

With the TLS PSK options, provide a pre-shared key in a later page.

Click on Next to continue.

Attributes	Value	Units
Encryption Algorithm	<input type="radio"/> None <input checked="" type="radio"/> TLS RSA <input type="radio"/> TLS PSK 128-bit <input type="radio"/> TLS PSK 256-bit	
Device Certificate	<input checked="" type="radio"/> Factory <input type="radio"/> User	
TLS Minimum Security Level	AES 256-bit TLS RSA ▾	
Rekey Interval	1440	minutes

 Back

Next 

Figure 196 Wireless Link Encryption Settings, User-supplied device certificates

Enter User Device Certificates

Upload the RSA Root CA, Private Key and Public Certificate for device authentication using 2048-bit key size and SHA256. The certificate subject must be the ODU's Unit ESN as 12 hexadecimal characters without punctuation. For example 000456500EF3. The Root CA certificate must form a valid certificate chain with the Public Certificate for the remote ODU. Input must be in Distinguished Encoding Rules (DER) format.

Click on Next to continue.

Device Root CA	<input type="button" value="Choose File"/> No file chosen	DER format
Device Private Key	<input type="button" value="Choose File"/> No file chosen	DER format
Device Public Certificate	<input type="button" value="Choose File"/> No file chosen	DER format

 Back

Next 

Figure 197 Wireless Link Encryption Settings, Authorization Control

Enter Authorization settings

Whitelist must be configured for proper operation.

Authorization Method Whitelist Blacklist

Whitelist data entry

Entry	MAC Address	Enabled
1	00:04:56: 58 : 00 : c0	<input checked="" type="checkbox"/>
2	00:04:56: 58 : 00 : b6	<input checked="" type="checkbox"/>
3	00:04:56: 58 : 00 : 5b	<input checked="" type="checkbox"/>
4	00:04:56: 58 : 00 : 67	<input checked="" type="checkbox"/>
5	00:04:56: 58 : 00 : 6c	<input checked="" type="checkbox"/>
6	00:04:56: 58 : 00 : 85	<input checked="" type="checkbox"/>
7	00:04:56: 58 : 00 : c4	<input checked="" type="checkbox"/>
8	00:04:56: 58 : 01 : 43	<input checked="" type="checkbox"/>
9	00:04:56: 00 : 00 : 00	<input type="checkbox"/>
30	00:04:56: 00 : 00 : 00	<input type="checkbox"/>
31	00:04:56: 00 : 00 : 00	<input type="checkbox"/>
32	00:04:56: 00 : 00 : 00	<input type="checkbox"/>

Buttons: Clear Configuration, Submit Configuration, Reset Form

Navigation: Back, Next

Figure 198 Wireless Link Encryption Settings, TLS-PSK

Enter Wireless Preshared Key

Enter a 128-bit random number formatted as 32 hexadecimal characters. For example: A6ECBDCAD706A0CFFB3C5CC3E954AE3E.
Use the same Pre-shared Key for the local and remote ODUs. The Pre-shared Key is used to encrypt and decrypt data at the wireless interface.

Click on Next to continue.

Pre-shared Key
Confirm Pre-shared Key

Buttons: Back, Next

Figure 199 Wireless Link Encryption Settings, TLS-PSK

Enter Wireless Preshared Key

Enter a 128-bit random number formatted as 32 hexadecimal characters. For example: A6ECBDCAD706A0CFFB3C5CC3E954AE3E. Use the same Pre-shared Key for the local and remote ODUs. The Pre-shared Key is used to encrypt and decrypt data at the wireless interface.

Click on [Next](#) to continue.

Click next to use the new Wireless Encryption Key

Thumbprint Algorithm: SHA-1

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

Pre-shared Key	*****
Confirm Pre-shared Key	*****

[Back](#) [Next](#)

Procedure:

- Select the applicable value in the Encryption Algorithm field.
- For TLS-RSA, select Factory or User device certificates.
- For User device certificates, install Private Key, Public Certificate and Root CA certificate.
- For TLS-RSA and Group Access, configure the Whitelist or Blacklist
- For TLS-PSK, configure the pre-shared key. If a valid encryption key exists, then an SHA-1 thumbprint of the key is displayed. If this key is correct, then take no action.
- Click **Next**.

HTTP and Telnet options

Menu option: **Security**. Part of the Security Wizard (Figure 200).

Use this page to configure network management of the PTP 670 using one or more of the following methods: HTTPS, HTTP, Telnet or SNMP.

Figure 200 HTTP and Telnet Settings page

Enter HTTP and Telnet Settings

Configure HTTP, Telnet, TFTP and Debug Access.

WARNING: Management access will be impossible if HTTP, HTTPS and SNMP are all disabled.

To regain access, operate the ODU in recovery mode

WARNING: Management access will be impossible if HTTP, HTTPS and SNMP are all disabled. To re-gain access, operate the ODU in recovery mode and select "Reset IP and Ethernet Configuration". Click on Next to see a summary of the security configuration.

Attributes	Value	Units
HTTP Access Enabled	<input type="radio"/> No <input checked="" type="radio"/> Yes	
HTTP Port Number	80	
Telnet Access Enabled	<input checked="" type="radio"/> No <input type="radio"/> Yes	
SNMP Control Of HTTP And Telnet	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
SNMP Control Of Passwords	<input checked="" type="radio"/> Disabled <input type="radio"/> Enabled	
TFTP Client	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Debug Access Enabled	<input type="radio"/> No <input checked="" type="radio"/> Yes	
Cross Site Request Forgery Protection	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	

Back

Next

**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).

Review and update the HTTP and Telnet attributes ([Table 190](#)) and click **Next**.

Table 190 HTTP and Telnet attributes

Attribute	Meaning
HTTP Access Enabled	No: The unit will not respond to any requests on the HTTP port. Yes: The unit will respond to requests on the HTTP port. Remote management via HTTPS is not affected by this setting.
HTTP Port Number	The port number for HTTP access. Zero means use the default port.
Telnet Access Enabled	No: The unit will not respond to any requests on the Telnet port. Yes: The unit will respond to requests on the Telnet port.
Telnet Port Number	The port number for Telnet access. Zero means use the default port.

Attribute	Meaning
SNMP Control of HTTP And Telnet	Disabled: Neither HTTP nor Telnet can be controlled remotely via SNMP. Enabled: Both HTTP and Telnet can be controlled remotely via SNMP.
SNMP Control of Passwords	Enabled: Passwords for identity-based user accounts in the web-based interface can be updated via SNMP. Use this with SNMPv3 to provide secure password updating from a central network manager. Disabled: Passwords for identity-based user accounts can be updated only via the web-based interface (default).
TFTP Client	Enabled: The unit will respond to TFTP software download requests.
Debug Access Enabled	Yes: Cambium Technical Support is allowed to access the system to investigate faults.
Cross Site Request Forgery Protection	Enabled: The system is protected against cross-site request forgery attacks at the web-based interface.

Confirm Security Configuration

Menu option: **Security**. Part of the Security Wizard ([Figure 201](#)).

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

Figure 201 Confirm Security Configuration page

Confirm Security Configuration		
Press the button to confirm the security configuration and reboot the ODU.		
Attributes	Value	Units
Key of Keys	Modified	
DRNG Entropy	Modified	
User Defined Security Banner		
Require Acknowledgement Of Notices	No	
Display Login Information	Yes	
HTTPS Access Enabled	Yes	
HTTPS Port Number	443	
Private Key	Modified	
Public Certificate	Modified	
Encryption Algorithm	TLS PSK 128-bit	
Wireless Encryption Key	Modified	
HTTP Access Enabled	Yes	
HTTP Port Number	80	
Telnet Access Enabled	No	
SNMP Control Of HTTP And Telnet	Enabled	
SNMP Control Of Passwords	Disabled	
TFTP Client	Enabled	
Debug Access Enabled	Yes	
Cross Site Request Forgery Protection	Enabled	
Confirm Security Configuration and Reboot		
 Back		

Procedure:

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

**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 202](#)).

Use this page if it is necessary to reset the security configuration to default values.

Figure 202 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

Zeroize CSPs and Reboot Wireless Unit

Procedure:

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

Aligning antennas

This section describes how to align the antennas for Master and Slave ODUs in the PTP topology, and Slave ODUs in the HCMP topology, using the web interface to assist with alignment, and checking wireless performance after alignment.

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

Starting up the units

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

Procedure:

- 1 Select the unit from which this process is to be controlled; either Master or Slave. This is the “local” unit.
- 2 Check that the management PC is connected to the local unit, powered up and logged on as described in [Connecting to the unit](#) on page 6-4.
- 4 Power up the remote unit.
- 5 Log into the local unit as described in [Logging into the web interface](#) on page 6-6.

Checking that the units are armed

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

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

Procedure:

- Select menu option **Home**. The System Summary page is displayed.
- Check that the Install Arm State is set to **Armed**.
- If the units are not armed, execute the installation wizard as described in [Installation menu](#) on page 6-9.

Aligning antennas

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

Preparation:

Ensure that the following parameters are available:

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

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

If a connectorized ODU is installed at either site with two separate antennas for spatial diversity, refer to [Aligning separate antennas for spatial diversity](#) on page 6-120 before starting alignment.



Note

For improved radio performance, mount the integrated ODU at 45 degrees to the vertical; this ensures that side-lobe levels are minimized for interference transmitted or received at zero elevation.

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



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 6-121
 - [Graphical Install page](#) on page 6-123
- 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 6-123) or by selecting menu option **Status** and monitoring the Receive Power attribute on the System Status page.

- 6 If after repeated attempts to align, the receive level still does not lie within the predicted range, this may be because the data provided to the prediction tool (such as LINKPlanner) is inaccurate. For example estimates of path obstructions, antenna heights or site locations may be inaccurate. Check this data and update the prediction as necessary.
- 7 Once the antennas have been aligned correctly, tighten the integrated ODU (or connectorized antenna) mountings. To ensure that the action of tightening does not alter antenna alignment, continue to monitor received signal level.

Aligning separate antennas for spatial diversity

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

Procedure:

- 1 Connect the horizontal polarization antenna to the ODU, disconnect the vertical polarization antenna, then perform [Aligning antennas](#) on page 6-119.
- 2 Connect the vertical polarization antenna to the ODU, disconnect the horizontal polarization antenna, then perform [Aligning antennas](#) on page 6-119.
- 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 5-59.

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 191](#). 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 191 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:

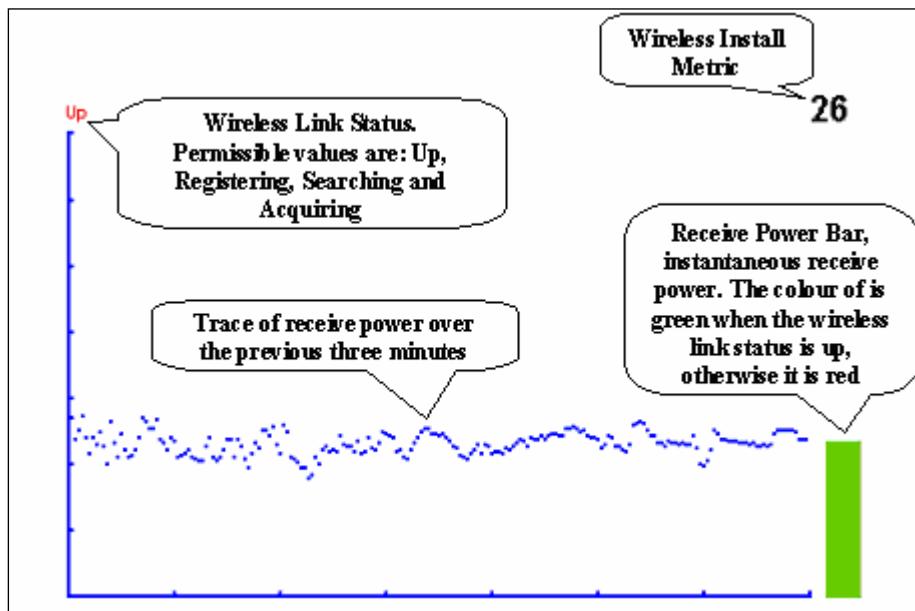
- **Band scan:** When first started up and from time to time, the Master unit will carry out a band scan to determine which channels are not in use. During this time, between 10 and 15 seconds, the Master unit will not transmit and as a consequence of this neither will the Slave unit. During this time 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 670 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 203).

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

Figure 203 Graphical Install page



Procedure:

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



Note

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

Disarming the units

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

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



Note

After 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 129).
- Click **Disarm Installation Agent**. The confirmation page is displayed (Figure 204).

Figure 204 Optional post-disarm configuration

Installation Disarmed

The installation agent has been successfully disarmed.

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

You may also wish to visit the [Spectrum Management](#) page and configure the wireless link channel utilization

Comparing actual to predicted performance

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

Procedure:

- Select menu option **System > Statistics**. The System Statistic page is displayed ([Figure 205](#)).
- Monitor the following attributes:
 - Link Loss
 - Transmit Data Rate
 - Receive Data Rate

Figure 205 Statistics to be monitored after alignment

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

For more information on the System Statistics page, refer to [System Statistics page on page 7-54](#).

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 670, 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 [6-70](#).
- 2 Set tFTP attributes as described in [Table 192](#).
- 3 Monitor tFTP attributes as described in [Table 193](#).
- 4 Reboot the ODU as described in [Rebooting the unit](#) on page [7-84](#).

Table 192 Setting tFTP attributes

Attribute	Meaning
tFTPServerInternetAddress	<p>The IPv4 or IPv6 address of the TFTP server from which the TFTP software upgrade file Name will be retrieved.</p> <p>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:</p> <pre>snmpset_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.11.9.19.0 a 10.10.10.1</pre>
tFTPServerPortNumber	<p>This setting is optional. The port number of the TFTP server from which the TFTP software upgrade file name will be retrieved (default=69).</p>
tFTPSoftwareUpgrade FileName	<p>The filename of the software upgrade to be loaded from the TFTP server.</p> <p>For example, to set the TFTP software upgrade filename on 10.10.10.10 to "B1095.dld", enter this command:</p> <pre>snmpset_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.11.9.7.0 s B1095.dld</pre>
tFTPStartSoftware Upgrade	<p>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.</p> <p>For example, enter this command:</p> <pre>snmpset_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.11.9.8.0 i 1</pre>

Table 193 Monitoring tFTP attributes

Attribute	Meaning
tFTPSoftwareUpgradeStatus	<p>This is the current status of the TFTP software upgrade process. Values:</p> <ul style="list-style-type: none"> idle(0) uploadinprogress(1) uploadsuccesfulprogrammingFLASH(2) upgradesuccesfulrebootorunthenewsoftwareimage(3) upgradefailed(4). <p>For example, enter this command:</p> <pre>snmpget_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.11.9.9.0</pre>
tFTPSoftwareUpgradeStatusText	<p>This describes the status of the TFTP software upgrade process, including any error details.</p> <p>For example, enter this command:</p> <pre>snmpget_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.11.9.10.0</pre>
tFTPSoftwareUpgradeStatusAdditionalText	<p>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.</p> <p>For example, enter this command:</p> <pre>snmpget_d.exe -v 2c -c public 10.10.10.10 .iso.3.6.1.4.1.17713.11.9.11.0</pre>

Chapter 7: Operation

This chapter provides instructions for operators of the PTP 670 wireless Ethernet bridge.

The following topics are described in this chapter:

- [System summary and status](#) on page 7-2
- [Rebooting and logging out](#) on page 7-18
- [Alarms, alerts and messages](#) on page 7-20
- [Spectrum Management](#) on page 7-29
- [Managing security](#) on page 7-53
- [System statistics](#) on page 7-54
- [Recovery mode](#) on page 7-77.

System summary and status

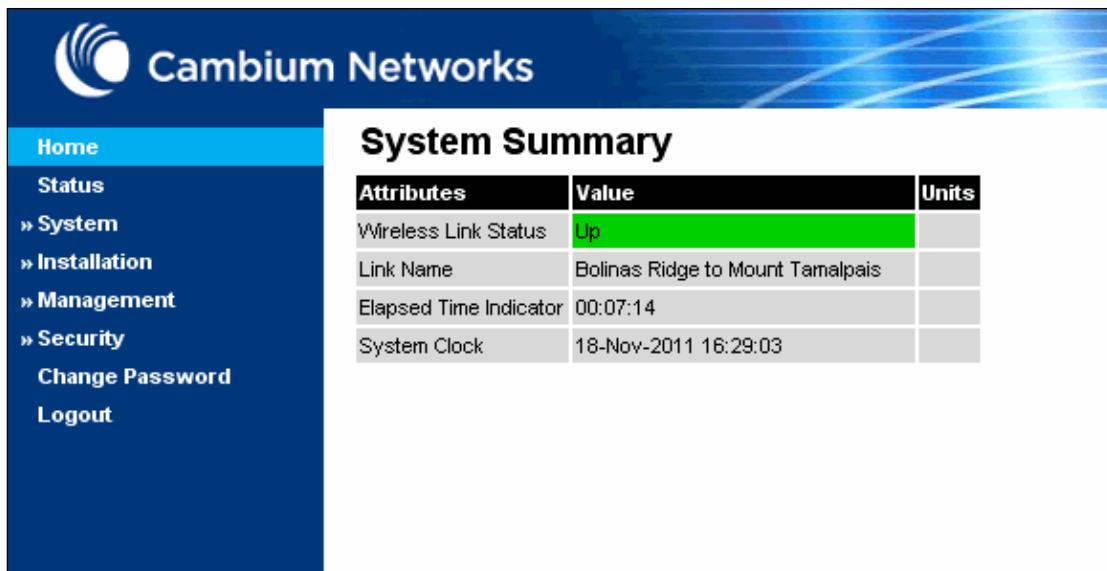
This section describes how to use the summary and status pages to monitor the status of the Ethernet ports and wireless link.

System Summary page

Menu option: **Home** ([Figure 206](#)).

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

Figure 206 System Summary page



Procedure:

- Review the attributes ([Table 194](#)).
- Check that the Wireless Link Status is “Up” on both units. If it is not “Up”, review any uncleared system alarms: these are displayed below the System Clock attribute. For more information, refer to [Alarms](#) on page [7-20](#).

Table 194 System Summary attributes

Attribute	Meaning
Wireless Link Status	Current status of the wireless link. A green background with status text “Up” means that the point-to-point link is established. A red background with suitable status text (for example “Searching”) indicates that the link is not established.
Link Name	The name of the PTP link, as set in the System Configuration page.

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

System Status page

PTP topology

Menu option: **Status** (Figure 207). This page provides a detailed view of the operation of the PTP 670 link from both the wireless and network perspectives.

Figure 207 System Status page (PTP topology)

System Status - Master			
Equipment		Wireless	
Attributes	Value	Attributes	Value
Link Name	Ashburton to Widecombe	Wireless Link Status	Up
Site Name	Ashburton	Maximum Transmit Power	23
Software Version	45700-00-05	Remote Maximum Transmit Power	23
Hardware Version	B0P05.00-C	Transmit Power	23.0, 20.2, -15.0, 23.0
Unit ESN	0004565800D5	Receive Power	-50.7, -97.4, -110.0, -51.4
Unit MSN	2249RN1791	Vector Error	7.2, -0.2, -38.7, -34.2
Regulatory Band	6 - 5.4 GHz Unrestricted EIRP - Development Key	Link Loss	120.5, 18.9, 0.0, 120.5
Elapsed Time Indicator	00:01:51	Transmit Data Rate	3.62, 0.55, 0.00, 3.62
Ethernet / Internet			
Main PSU Port Status	Down	Receive Data Rate	4.73, 0.57, 0.00, 3.62
Main PSU Port Speed And Duplex		Link Capacity Variant	Full
Aux Port Status	Copper Link Up	Link Capacity	7.25
Aux Port Speed And Duplex	1000 Mbps Full Duplex	Transmit Modulation Mode	BPSK 0.63 (15 MHz)
MAC Address	00:04:56:58:00:d5	Receive Modulation Mode	BPSK 0.63 (15 MHz)
Remote MAC Address	00:04:56:58:00:58	Link Symmetry	1 to 1
Remote Internet Address	http://169.254.1.10	Receive Modulation Mode Detail	Restricted Because Installation Is Armed
TDD Synchronization			
TDD Synchronization Interface	Disabled	Range	0.2
Status Page Refresh Period	3600	Seconds	
			<input type="button" value="Update Page Refresh Period"/> <input type="button" value="Reset form"/>

In the PTP topology, the two PTP 670 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.

If TDM is configured, the System Status page displays NIDU LAN Port and TDM attributes (Figure 208).

Figure 208 System Status page with TDM configured

System Status - Master					
Equipment		Wireless			
Attributes	Value	Units	Attributes	Value	Units
Link Name	link5		Wireless Link Status	Up	
Site Name			Maximum Transmit Power	10	dBm
Software Version	50650-G7-B1439+ wdog		Remote Maximum Transmit Power	10	dBm
Hardware Version	B0P03.00-C		Transmit Power	10.0, 10.0, 10.0, 10.0	dBm
Regulatory Band	255 - Development Key		Receive Power	-54.1, -54.3, -54.5, -54.5	dBm
Elapsed Time Indicator	00:08:56		Vector Error	-30.8, -31.9, -32.8, -31.7	dB
Ethernet / Internet					
Main PSU Port Status	Copper Link Up		Link Loss	110.4, 110.3, 110.3, 110.4	dB
Main PSU Port Speed And Duplex	1000 Mbps Full Duplex		Transmit Data Rate	24.22, 24.22, 24.22, 24.22	Mbps
NIDU Lan Port Status	Copper Link Up		Receive Data Rate	24.22, 24.22, 24.22, 24.22	Mbps
NIDU Lan Port Speed And Duplex	1000 Mbps Full Duplex		Link Capacity Variant	Full	
Aux Port Status	Copper Link Up		Link Capacity	48.43	Mbps
Aux Port Speed And Duplex	1000 Mbps Full Duplex		Transmit Modulation Mode	256QAM 0.81 (Dual) (5 MHz)	
SFP Port Status	Fiber Link Up		Receive Modulation Mode	256QAM 0.81 (Dual) (5 MHz)	
SFP Port Speed And Duplex	1000 Mbps Full Duplex		Link Symmetry	1 to 1	
MAC Address	00:04:56:50:00:a9		Receive Modulation Mode Detail	Running At Maximum Receive Mode	
Remote MAC Address	00:04:56:50:02:2e		Range	0.2	km
Remote Internet Address	http://169.254.1.2		TDD Synchronization		
Synchronous Ethernet					
Sync E Tracking State	Free Running		TDD Synchronization Interface	Disabled	
TDM					
TDM Interface Control	E1		TDM Interface Status	OK	
TDM Single Payload Lock	Disabled		TDM Latency	0	μs
TDM Channel Status 1	Up		TDM Channel Status 2	Up	
TDM Channel Status 3	Up		TDM Channel Status 4	Up	
TDM Channel Status 5	Up		TDM Channel Status 6	Up	
TDM Channel Status 7	Up		TDM Channel Status 8	Up	
Status Page Refresh Period	3600	Seconds	<input type="button" value="Update Page Refresh Period"/>		<input type="button" value="Reset form"/>

Procedures:

- Confirm that the Ethernet Link Status attributes are green and set to **Copper Link Up** or **Fiber Link Up**.

HCMP topology

Menu option: **Status** (Figure 209 to Figure 211). This page provides a detailed view of the operation of the PTP 670 link from both the wireless and network perspectives.

Figure 209 System Status page (Master, HCMP topology, Wireless Interface set to a single link)

System Status - High Capacity Multi-Point - Master			
Attributes	Value	Units	
Wireless Interface Selector	Slave_58_01_D5		
Equipment			
Unit Name	Master_AJ		
Site Name			
Software Version	45700-G7PFP-B40+ wdog		
Hardware Version	B0P05.01-C-FPS		
Unit ESN	000456580262		
Unit MSN	2249RS0566		
Regulatory Band	81 - 4.7 GHz- Development Key		
Elapsed Time Indicator	01:12:19		
Ethernet / Internet			
Main PSU Port Status	Copper Link Up		
Main PSU Port Speed And Duplex	1000 Mbps Full Duplex		
Group ID	0		
MAC Address	00:04:56:58:02:62		
Remote Unit Name	Slave_58_01_D5		
Remote MAC Address	00:04:56:58:01:d5		
Remote Internet Address	http://10.10.10.11		
TDD Synchronization			
TDD Synchronization Status	Not Synchronized (No GPS/Sync In)		
Status Page Refresh Period	3600	Seconds	
			Update Page Refresh Period Reset form

Figure 210 System Status page (Master, HCMP topology, Wireless Interface set to “All Wireless Interfaces”)

System Status - High Capacity Multi-Point - Master				
Attributes	Value		Units	
Wireless Interface Selector	All Wireless Interfaces			
Equipment				
Unit Name	Master_AJ			
Site Name				
Software Version	45700-G7PFP-B40+ wdog			
Hardware Version	B0P05.01-C-FPS			
Unit ESN	000456580262			
Unit MSN	2249RS0566			
Regulatory Band	81 - 4.7 GHz - Development Key			
Elapsed Time Indicator	01:13:47			
TDD Synchronization				
TDD Synchronization Status	Not Synchronized (No GPS/Sync In)			
Ethernet / Internet				
Main PSU Port Status	Copper Link Up			
Main PSU Port Speed And Duplex	1000 Mbps Full Duplex			
Group ID	0			
MAC Address	00:04:56:58:02:62			
Remote MAC Address	00:04:56:58:01:d5	Not Available	Not Available	
Remote Internet Address	http://10.10.10.11	Not Available	Not Available	
Wireless				
Remote Unit Name	Slave_58_01_D5	Not Available	Not Available	
Wireless Link Status	Up	Initialising	Searching	
Wireless Encryption	AES 256-bit TLS RSA	None	None	
Maximum Transmit Power	28			dBm
Remote Maximum Transmit Power	28	Not Available	Not Available	dBm
Transmit Power	23.0, -46.2, -35.5, 67.2, 57.89, 2.78, 60.68	23.0, -46.2, -36.6, 67.2, 57.89, 0.00, 0.00	28.0, -109.9, -110.0, 0.0, 0.00, 0.00	0.0, 0.0 dBm
Receive Power				
Vector Error				
Link Loss				
Transmit Data Rate	57.89, 2.78, 0.00	0.00, 0.00	0.00, 0.00	Mbps
Receive Data Rate				
Link Capacity	60.68	0.00	0.00	Mbps
Transmit Modulation Mode	256QAM 0.81 (Dual)	Acquisition	Acquisition	
Receive Modulation Mode	BPSK 0.63	Acquisition	Acquisition	
Channel Bandwidth	40 MHz			
Range	0.2	Not Available	0.0	km
Status Page Refresh Period	3600	seconds		
Updated Page Refresh Period		Reset Form		

Figure 211 System Status page (Slave, HCMP topology)

System Status - High Capacity Multi-Point - Slave					
Equipment		Wireless			
Attributes	Value	Units	Attributes	Value	Units
Link Name			Wireless Link Status	Up	
Site Name	AJ bench		Wireless Encryption	AES 256-bit TLS RSA	
Software Version	45700-G7PFP-B471+ lwdog		Maximum Transmit Power	17	dBm
Hardware Version	B0P05.01-C-FPS		Remote Maximum Transmit Power	24	dBm
Unit ESN	000456580186		Transmit Power	17.0, 12.3, -15.0, 17.0	dBm
Unit MSN	2249RS0201		Receive Power	-55.7, -62.8, -110.0, -57.9	dBm
Regulatory Band	95 - 4.5 GHz - Development Key		Vector Error	7.2, -12.1, -39.0, -25.5	dB
Elapsed Time Indicator	00:02:15		Link Loss	111.9, 34.0, 0.0, 80.9	dB
Ethernet / Internet			Transmit Data Rate	5.18, 1.24, 0.00, 1.90	Mbps
Main PSU Port Status	Copper Link Up		Receive Data Rate	15.45, 3.38, 0.00, 15.45	Mbps
Main PSU Port Speed And Duplex	1000 Mbps Full Duplex		Link Capacity Variant	Full	
Group ID	123		Link Capacity	17.21	Mbps
MAC Address	00:04:56:58:01:86		Wireless Link Availability	100.0000	%
Remote MAC Address	00:04:56:58:02:62		Data Bridging Availability	97.4709	%
Remote Internet Address	http://10.10.10.10		Transmit Modulation Mode	QPSK 0.63 (Single) (20 MHz)	
			Receive Modulation Mode	64QAM 0.92 (Dual) (20 MHz)	
			Dual Payload	Enabled	
			Receive Modulation Mode Detail	Limited By The Wireless Conditions	
			Range	12.1	km
Status Page Refresh Period	3600	Seconds	<input type="button" value="Update Page Refresh Period"/> <input type="button" value="Reset form"/>		

In the HCMP topology, one PTP 670 Series unit is the Master and up to eight PTP 670 Series units are configured as Slaves. The roles of the units in this relationship are displayed in the page title. The master unit will always have the title “ – High Capacity MultiPoint – Master”, and the slave will always have “– High Capacity MultiPoint – Slave” appended to the “Systems Status” page title.

Procedures:

- Only on a device configured as in HCMP mode as a Master, set the Wireless Interface Selector to the Wireless Interface the diagnostic data needs to be displayed for. Note the Remote MAC Address indicates the MAC address of the unit currently connected, if any, to the selected wireless interface.
- Confirm that the NIDU LAN Port Status attribute and the TDM Channel Status are green and set to **Copper Link Up** and **Up** respectively.

Equipment

The Equipment section of the System Status page contains the attributes described in [Table 195](#).

Table 195 System Status attributes - Equipment

Attribute	Meaning
Link Name	The link name is allocated by the system administrator and is used to identify the equipment on the network. The link name attribute is limited to a maximum size of 63 ASCII characters.

Attribute	Meaning
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 670 software installed on the equipment.
Hardware Version	The PTP 670 hardware version. Formatted as "vvvv-C" or "vvvv-I" where vvvv is the version of the printed circuit card. The "-C" suffix indicates a PTP 670 Connectorized unit. The "-I" suffix indicates a PTP 670 Integrated unit.
Unit ESN	The Electronic Serial Number of the ODU.
Unit MSN	The Mechanical Serial Number of the ODU.
Regulatory Band	This is used by the system to constrain the wireless to operate within regulatory regime of a particular band and country. The license key provides the capability to operate in one or more regulatory bands. The Installation Wizard is used to choose one of those bands.
Elapsed Time Indicator	The elapsed time indicator attribute presents the total time in years, days, hours, minutes and seconds since the last system restart. The system can restart for several reasons, for example commanded reboot from the system reboot web page, or a power cycle of the equipment.

Ethernet / Internet

The Ethernet / Internet section of the System Status page contains the attributes described in [Table 196](#).

Table 196 System Status attributes – Ethernet / Internet

Attribute	Meaning
Main PSU Port Status	The current status of the Ethernet link to the PSU port: <ul style="list-style-type: none"> • Green "Copper Link Up": The Ethernet link is established. • Red "Down": The Ethernet link is not established.
Main PSU Port Speed and Duplex	The negotiated speed and duplex setting of the Ethernet link to the PSU port. The speed setting is specified in Mbps.
NIDU LAN Port Status	The current status of the Ethernet link to the NIDU LAN port: <ul style="list-style-type: none"> • Green "Copper Link Up": The Ethernet link is established. • Red "Down": The Ethernet link is not established.
NIDU LAN Port Speed and Duplex	The negotiated speed and duplex setting of the Ethernet link to the NIDU LAN port. The speed setting is specified in Mbps.
Aux Port Status	The current status of the Ethernet link to the Aux port: <ul style="list-style-type: none"> • Green "Copper Link Up": The Ethernet link is established. • Red "Down": The Ethernet link is not established.

Attribute	Meaning
Aux Port Speed and Duplex	The negotiated speed and duplex setting of the Ethernet link to the Aux port. The speed setting is specified in Mbps.
SFP Port Status	The current status of the Ethernet link to the SFP port: <ul style="list-style-type: none"> • Green “Fiber Link Up”: The Ethernet link is established. • Red “Down”: The Ethernet link is not established.
SFP Port Speed and Duplex	The negotiated speed and duplex setting of the Ethernet link to the SFP port. The speed setting is specified in Mbps.
MAC Address	The MAC Address of this unit.
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 160) and IP Address Label (Table 159), this may be either an IPv4 or an IPv6 address.

Wireless

The Wireless section of the System Status page contains the attributes described in [Table 197](#).

Table 197 System Status attributes – Wireless

Attribute	Meaning
Wireless Link Status	The current status of the wireless link: <ul style="list-style-type: none"> • Green “Up”: A point-to-point wireless link is established. • Red “Down”: The wireless link is not established.
Wireless Encryption	For the HCMP topology only, the encryption algorithm used for the wireless link: <ul style="list-style-type: none"> • None: The wireless link is not encrypted. • AES 128-bit TLS RSA: The wireless link is encrypted using the AES TLS RSA algorithm with a 128-bit key. • AES 256-bit TLS RSA: The wireless link is encrypted using the AES TLS RSA algorithm with a 256-bit key.
Maximum Transmit Power	The maximum transmit power that the local wireless unit is permitted to use to sustain a link.
Remote Maximum Transmit Power	The maximum transmit power that the remote wireless unit is permitted to use to sustain a link.
Transmit Power	The maximum, mean, minimum and latest measurements of Transmit Power (dBm). See System histograms on page 7-54 .

Attribute	Meaning
Receive Power	The maximum, mean, minimum and latest measurements of Receive Power (dBm). See System histograms on page 7-54.
Vector Error	<p>The maximum, mean, minimum and latest measurements of Vector Error (dB). See System histograms on page 7-54.</p> <p>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).</p>
Link Loss	<p>The maximum, mean, minimum and latest measurements of Link Loss (dB). See System histograms on page 7-54. The link loss is the total attenuation of the wireless signal between the two point-to-point units.</p> <p>The link loss calculation is:</p> $P_{ll} = P_{T_x} - P_{R_x} + g_{T_x} + g_{R_x} - c_{T_x} - c_{R_x}$ <p>Where:</p> <p>P_{ll} = Link Loss (dB)</p> <p>P_{T_x} = Transmit power of the remote wireless unit (dBm)</p> <p>P_{R_x} = Received signal power at the local unit (dBm)</p> <p>g_{T_x}, g_{R_x} = Antenna gain at the remote and local units respectively (dBi). This is the gain of the integrated or connectorized antenna.</p> <p>c_{T_x}, c_{R_x} = Cable loss at the remote and local units respectively (dB). It is RF cable loss which connects ODU to Connectorized antenna.</p> <p>For connectorized ODUs, the link loss calculation is modified to allow for the increased antenna gains at each end of the link.</p>
Transmit Data Rate	The maximum, mean, minimum and latest measurements of Transmit Data Rate (Mbps). See System histograms on page 7-54.
Receive Data Rate	The maximum, mean, minimum and latest measurements of Receive Data Rate (Mbps). See System histograms on page 7-54.
Link Capacity Variant	Link Capacity Variant is always Full in PTP 670.
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.

Attribute	Meaning
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 198 .
Range	The range between the PTP 670 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 6-78 .

Table 198 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.
Limited By The Wireless Conditions	The radio is running at the maximum achievable modulation mode given the current wireless conditions shown by the vector error. The radio is capable of reaching a higher modulation mode if wireless conditions (vector error) improve.

Synchronous Ethernet



Note

Synchronous Ethernet is available in the PTP topology.

The Synchronous Ethernet section of the System Status page contains the attributes described in [Table 199](#).

Table 199 System Status attributes – Synchronous Ethernet

Attribute	Meaning
Sync E Tracking State	<p>The state of frequency tracking in Synchronous Ethernet. For a list of values and their meanings, see Table 200.</p> <p>In normal operation, with the Synchronous Ethernet feature enabled and a valid timing source present, one end of the link should be in the “Locked Local, Holdover Acquired State”, the other end should be in the “Locked Remote, Holdover Acquired” state.</p> <p>Further status information for the Synchronous Ethernet features is available in the Sync E Status page. See SyncE Status page on page 7-70.</p>

Table 200 Sync E Tracking State values and meanings

Value	Meaning
Disabled	The synchronous Ethernet feature is disabled.
Acquiring Wireless Lock	Synchronous Ethernet is not operational because the wireless link is establishing.
Free Running	Synchronous Ethernet is operational, but with no timing source or history. This is a temporary state.
Locked Local, Acquiring Holdover	Sync E tracking has locked to a synchronisation signal from a cabled Ethernet port on the local ODU. This is a temporary state until the unit has acquired holdover history.
Locked Local, Holdover Acquired	Sync E tracking has locked to a synchronisation signal from a cabled Ethernet port on the local ODU and has acquired holdover history.
Holdover	There is currently no source for the tracking loop, but previously the tracking loop was in a Locked, Holdover Acquired state. The system is using the last known good frequency.
Locked Remote, Acquiring Holdover	The tracking loop has locked to a synchronisation signal from the remote ODU. This is a temporary state until the unit has acquired holdover history.
Locked Remote, Holdover Acquired	The tracking loop has locked to a synchronisation signal from the remote ODU and has acquired holdover history.

TDD Synchronization

The TDD Synchronization section of the System Status page contains the attributes described in [Table 201](#).

Table 201 System Status attributes – TDD Synchronization

Attribute	Meaning
TDD Synchronization Status	The status of TDD synchronization. Displayed at a TDD Master if TDD synchronization is active. For a list of values and their meanings, see Table 202 and Table 203 .

Table 202 TDD Synchronization Status values and meanings for PTP-SYNC

Value	Meaning
Inactive	<p>TDD Synchronization has been administratively disabled.</p> <p>This value is not displayed in the System Status page, but can be determined from the SNMP MIB.</p> <p>TDD Synchronization Status is always in the Inactive state at a TDD Slave unit.</p>
Cluster Timing Master	<p>The ODU has been configured as a Cluster Master with an internal reference, and is communicating correctly with the PTP SYNC unit.</p>
Initialising	<p>The wireless link is down, and the master ODU is attempting to synchronize the TDD frame structure with an external 1 pps reference.</p> <p>Synchronization proceeds more rapidly in this state than in the Acquiring Lock state, because the TDD master does not need to consider the ability of the TDD slave to track changes in frame timing.</p>
PTP-SYNC Not Connected	<p>The ODU is not able to communicate with the PTP SYNC unit.</p>
Locked	<p>The master ODU has locked the TDD frame structure to the 1 pps reference received at the input of the PTP-SYNC unit.</p> <p>The ODU may be a Cluster Master or a Cluster Slave.</p> <p>The ODU is transmitting.</p>
Holdover (No GPS Sync In)	<p>The 1 pps reference has been lost at the input to the PTP-SYNC unit, and the ODU in a free running state.</p> <p>The ODU is transmitting.</p> <p>If the reference input is not restored, the Holdover state will terminate automatically after a period set by TDD Holdover Duration.</p>

Value	Meaning
Holdover	<p>The ODU is a Cluster Slave and the 1 pps reference has been lost at the input to an upstream PTP-SYNC unit. The ODU is locked to an upstream ODU that is in the Holdover (No GPS Sync In) state.</p>
	<p>The ODU is transmitting.</p>
	<p>If the reference input is not restored at the upstream PTP-SYNC unit, the Holdover state will terminate automatically after a period set by TDD Holdover Duration.</p>
Not Synchronized (No GPS Sync In)	<p>The 1 pps reference has been lost at the input to the PTP-SYNC unit and the holdover period has expired.</p> <p>If the ODU is configured for TDD Holdover Mode = Best Effort then the ODU will be transmitting, otherwise it will be muted.</p>
Not Synchronized	<p>The ODU is a Cluster Slave and the 1 pps reference has been lost at the input to an upstream PTP-SYNC unit. The holdover period has expired.</p> <p>If the ODU is configured for TDD Holdover Mode = Best Effort then the ODU will be transmitting, otherwise it will be muted.</p>
Acquiring Lock	<p>The wireless link is up and the master ODU is attempting to synchronize the TDD frame structure with an external 1 pps reference. Frame timing changes at the TDD master are constrained to allow for tracking by the TDD slave.</p> <p>This state is not allowed when TDD Holdover Mode = Strict.</p>

Table 203 TDD Synchronization Status values and meanings for CMM5 or direct connection

Value	Meaning
Inactive	<p>TDD Synchronization has been administratively disabled.</p> <p>This value is not displayed in the System Status page, but can be determined from the SNMP MIB.</p> <p>TDD Synchronization Status is always in the Inactive state at a TDD Slave unit.</p>
Initialising	<p>The wireless link is down, and the master ODU is attempting to synchronize the TDD frame structure with an external 1 pps reference.</p> <p>Synchronization proceeds rapidly in this state because the TDD master does not need to consider the ability of the TDD slave to track changes in frame timing.</p>
Locked	<p>The TDD frame structure is locked to a 1 pps reference from the CMM5 or from the directly-connected partner ODU.</p> <p>The ODU is transmitting.</p>

Value	Meaning
Holdover	<p>The ODU is transmitting.</p> <p>If the reference input is not restored, the Holdover state will terminate automatically after a period set by TDD Holdover Duration.</p>
Not Synchronized	<p>The holdover period has expired.</p> <p>If the ODU is configured for TDD Holdover Mode = Best Effort then the ODU will be transmitting, otherwise it will be muted.</p>

IEEE 1588 Transparent Clock



Note

IEEE 1588 Transparent Clock is available in the PTP topology.

The IEEE 1588 Transparent Clock section of the System Status page contains the attributes described in [Table 204](#).

Table 204 System Status attributes – IEEE 1588 Transparent Clock

Attribute	Meaning
Transparent Clock	Indicates if the IEEE 1588 transparent clock feature is enabled.

TDM



Note

TDM is available in the PTP topology.

The TDM section of the System Status page contains the attributes described in [Table 205](#).



Note

When TDM is enabled and connected at one link end, up to two minutes may elapse before the TDM link is established (this is known as the settling period). Do not attempt to change the TDM configuration during this settling period.

Table 205 System Status attributes – TDM

Attribute	Meaning
TDM Interface Control	The type of TDM interface that is activated (None, E1 or T1). This is set on the Interface Configuration page.
TDM Interface Status	The current status of the Ethernet link between the NIDU (ODU port) and the ODU (PSU port) (OK or Not Connected). <ul style="list-style-type: none"> Green "OK": The Ethernet link is established. Red "Not Connected": The Ethernet link is not established.
TDM Single Payload Lock	The current status of the single payload locking feature: <ul style="list-style-type: none"> "Enabled": The ODU will prevent transition from Single Payload modes to the higher Dual Payload modes. The ODU applies this lock when it calculates that such a transition would pass through modes which cannot carry telecoms data. "Applied": The ODU is actively preventing these transitions. "Disabled": The wireless will transition to the faster Dual Payload modes as soon as the conditions are appropriate.
TDM Latency	The end-to-end latency of the TDM service between TDM ports at the NIDUs (μs).
TDM Channel Status n	The current status of the TDM service between NIDU port "n" at the local NIDU and the corresponding port at the remote NIDU. For a list of values and their meanings, see Table 206 .

Table 206 TDM Channel Status values and meanings

Value	Meaning
Up	TDM data is being bridged between the TDM ports on local and remote NIDUs (green background).
No Signal (Local)	No TDM data is being received at the TDM port on the local NIDU.
No Signal (Remote)	No TDM data is being received at the corresponding TDM port on the remote NIDU.
No Signal (Local and Remote)	No TDM data is being received at the associated TDM ports on local and remote NIDUs.
No Signal (Local and Remote Timing)	No TDM data is being received at the TDM port on the local NIDU. TDM data is being received at the TDM port on the remote NIDU. The modulation mode of the link is too low to support bridging of TDM data in the remote to local direction, but the transmit clock at TDM port of the local NIDU is synchronised to the clock received at the TDM port on the remote NIDU.

Value	Meaning
Remote Timing	TDM data is being received at the TDM port on the local and remote NIDUs. The modulation mode of the link is too low to support bridging of TDM data in either direction. The transmit clocks at the TDM ports on local and remote NIDUs are synchronized to the clocks received at the TDM ports on (respectively) the remote and local NIDUs.
Disabled	The TDM link is not established. This may be because the wireless link is down, or because the TDM service is acquiring synchronization.

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 212](#)).

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

Figure 212 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 213](#)).

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

Figure 213 Reboot Wireless Unit page

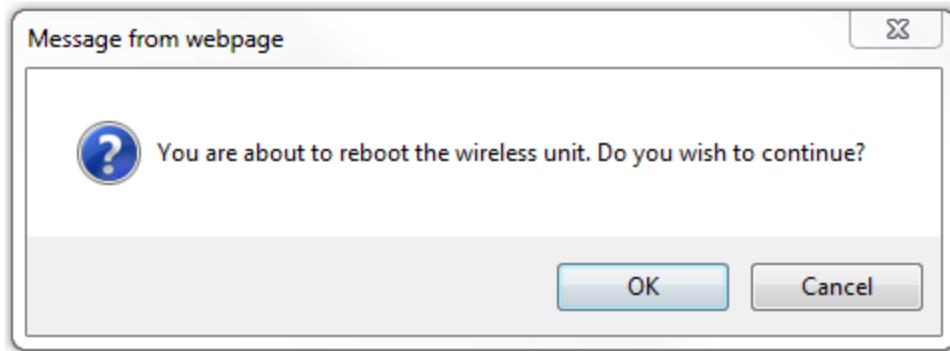
Reboot Wireless Unit	
Use this page to reboot the wireless unit	
Attributes	Value
Previous Reasons For Reset/Reboot	User Reboot - Console (21-May-2013 10:33:21) ▾
<input type="button" value="Reboot Wireless Unit"/>	

Procedure:

- Use the drop-down list to view the Previous Reasons For Reset/Reboot.
- If a reboot is required:
 - Click **Reboot Wireless Unit**. The Reboot Confirmation dialog is displayed ([Figure 214](#)).

- Click **OK**. The reboot progress message is displayed. On completion, the unit restarts.

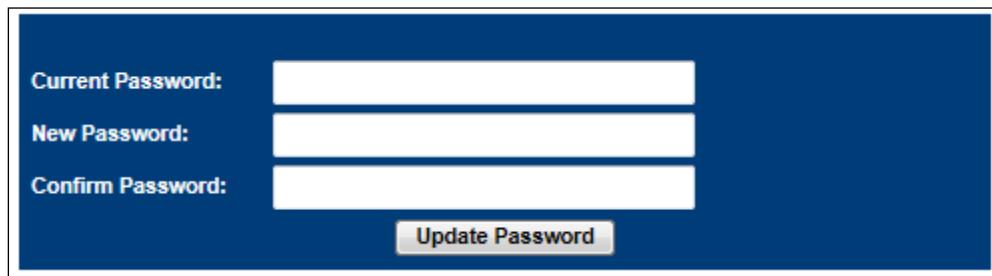
Figure 214 Reboot confirmation pop up



Change Password page

Menu option: **Change Password** ([Figure 215](#)). Use this page to change a personal password.

Figure 215 Change Password page (System Administration example)



A security officer can change the passwords of other users using the User Accounts page, as described in [Local User Accounts page](#) on page [6-72](#).

Procedure:

- Enter and confirm the new password (the default is blank). The new password must comply with the complexity rules ([Table 174](#)).

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 169](#)).

Alarms, alerts and messages

This section describes how to use alarms, alerts and syslog messages to monitor the status of a PTP 670 link.

Alarms

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

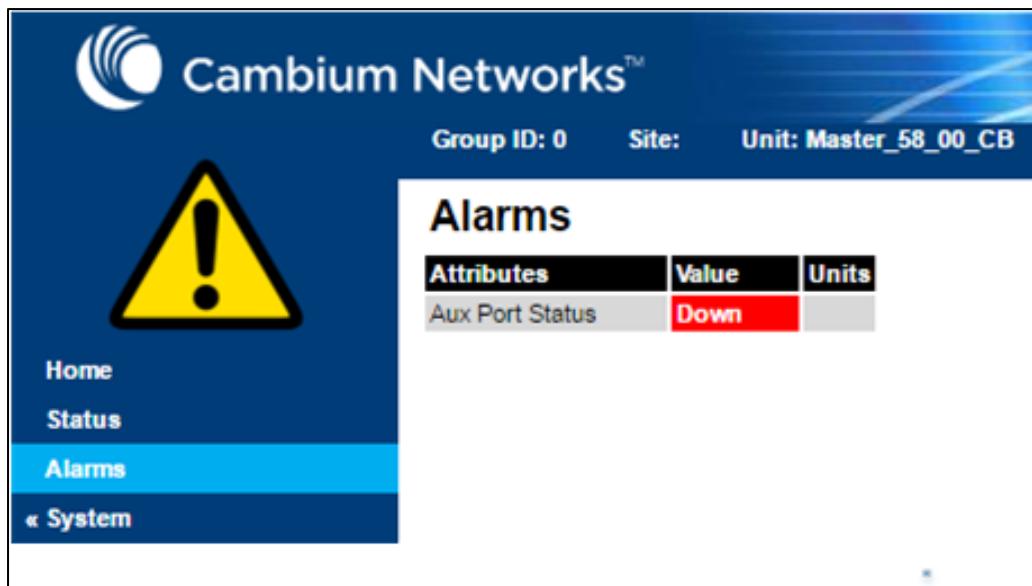
Procedure:

- Click the warning triangle or the menu option **Alarms** to navigate to the Alarms page. The warning triangle and the Alarms menu item are hidden if there are no active alarms.

The example in [Figure 216](#) shows the warning triangle in the navigation bar and an alarm displayed in the Alarms page. The alarms are defined in [Table 207](#).

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

Figure 216 Alarms page



Attributes	Value	Units
Aux Port Status	Down	

Table 207 System alarms

Alarm	Meaning
Aux Port Configuration Mismatch	Ethernet fragments (runt packets) have been detected when the Aux port is in full duplex. This indicates an auto-negotiation or forced configuration mismatch.
Aux Port Disabled Warning	The Aux port link has been administratively disabled via the SNMP Interface.
Aux Port PoE Output Status	The Aux port link is down. The most likely cause is that the unit has no Ethernet cable plugged into its Aux port.
Aux Port Status	The Aux port link is down. The most likely cause is that the unit has no Ethernet cable plugged into its Aux port.
Cable Diagnostics Warning	“Test In Progress” means that the Cable Diagnostics test has been initiated on one or more ports and is in progress.
Capacity Variant Mismatch	The link ends are different capability variants. This is not applicable for PTP 670.
Data Bridging Status	This alarm depends on Lowest Data Modulation Mode. “Disabled” means that the link has stopped bridging Ethernet frames because the Lowest Data Modulation Mode is not being achieved or because the wireless link is down.
Second Data Bridging Status	This alarm depends on Lowest Second Data Modulation Mode. “Disabled” means that the link has stopped bridging Ethernet frames because the Lowest Second Data Modulation Mode is not being achieved or because the wireless link is down.
Install Status	Signaling was received with the wrong MAC address. It is very unusual to detect this, because units with wrongly configured Target MAC Address will normally fail to establish a wireless link. However, rare circumstances may establish a partial wireless link and detect this situation.
Install Arm State	A wireless unit is in installation mode. After installation, the wireless unit should be disarmed. This will increase the data-carrying capacity and stop the installation tone generator. The wireless link is disarmed from the “Installation” process, see Disarming the units on page 6-124.
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.

Alarm	Meaning
Incompatible Master and Slave	The master and slave ends of the wireless link are different hardware products, or have different software versions. It is very unusual to detect this because incompatible units will normally fail to establish a wireless link. However, some combinations may establish a partial wireless link and detect this situation.
Link Mode Optimization Mismatch	The Master and Slave ODUs are configured to use different link mode optimization methods (one is set to IP and the other TDM).
Main PSU Port Configuration Mismatch	Ethernet fragments (runt packets) have been detected when the PSU port is in full duplex. This indicates an auto-negotiation or forced configuration mismatch.
Main PSU Port Disabled Warning	The PSU port link has been administratively disabled via the SNMP Interface.
Main PSU Port Status	The PSU port link is down. The most likely cause is that the unit has no Ethernet cable plugged into its Aux port.
NIDU LAN Port Status	The Ethernet link between the NIDU (LAN port) and the Ethernet network terminating equipment is not established.
No Wireless Channel Available	Spectrum Management was unable to locate a suitable wireless channel to operate on.
Port Allocation Mismatch	The local and remote ODUs have different services configured. The following alarms are raised on the port configuration mismatch - <ul style="list-style-type: none"> Mismatch in Second Data Service: The Second Data Service is configured at the local unit but it is not configured at the remote unit or vice versa. Mismatch in Out of Band Remote Management Service: The Out of Band Management Service is configured at the local unit but it is not configured at the remote unit or vice versa.
Regulatory Band	The installed license key contains an invalid Regulatory Band. The wireless unit is prohibited from operating outside the regulated limits.
Remote Transparent Clock Compatibility	The local and remote units have different IEEE 1588 transparent clock configurations. Both units must have the same configuration for the feature to work correctly.

Alarm	Meaning
SFP Error	<p>A non-OK value indicates that the SFP link is down. There are two possible causes:</p> <ul style="list-style-type: none"> 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.
SNTP Synchronization failed	SNTP has been enabled but the unit is unable to synchronize with the specified SNTP server.
Sync E tracking state	The state of the Synchronous Ethernet feature, if there is a problem.
Syslog Client Enabled/Disabled Warning	The local syslog client has been enabled or disabled.
Syslog Enabled/ Disabled Warning	The local log of event messages has been enabled or disabled.
Syslog Local Nearly Full	The local log of event messages is nearly full.
Syslog Local Wrapped	The local log of event messages is full and is now being overwritten by new messages.
TDM Channel Status n	The Ethernet link between the NIDU (E1/T1 port "n") and the local TDM transceiver is not established.
TDM Channel Loopback n	TDM channel "n" is currently undergoing a loopback test.
TDD Synchronization Alarm	<p>The reference signal for TDD Synchronization is absent and the ODU is now in holdover with more than 80% of the holdover period elapsed (Reference Signal Lost) or the ODU has reached the end of the configured holdover period and may not be correctly synchronized with the remaining units in the wireless network (Synchronization Lost).</p> <p>If TDD Synchronization Alarm = Synchronization Lost and TDD Holdover Mode = Strict, the ODU will be muted and the wireless link will be down.</p>
Transparent Clock Source Port Alarm	If SFP was the selected transparent clock source port but the media did not negotiate to Fiber.

Alarm	Meaning
Unit Out Of Calibration	The unit is out of calibration and must be returned to the factory using the RMA process for re-calibration.
Wireless Link Disabled Warning	The wireless link has been administratively disabled via the SNMP Interface. The wireless interface MIB-II ifAdminStatus attribute has been set to DOWN . To enable the Ethernet interface, set the ifAdminStatus attribute to UP .

Email alerts

The management agent can be configured to generate alerts by electronic mail when certain events occur. The alerts are defined in [Table 208](#).

Table 208 Email alerts

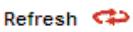
Alert	Meaning
Wireless Link Up Down	There has been a change in the status of the wireless link.
Channel Change	DFS has forced a change of channel.
DFS Impulse Interference	DFS has detected impulse interference.
Enabled Diagnostic Alarms	Diagnostic alarms have been enabled.
Main PSU Port Up Down	There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

Syslog page

Menu option: **Management > Syslog** (Figure 217).

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

Figure 217 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=MeIC; 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 **1-57** describes the system logging feature.
- [Syslog Configuration page](#) on page **6-88** describes how to enable system logging.

Format of syslog server messages

PTP 670 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 = "PTP670" 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:

PTP670: configuration; IP Address; Web user; was=10.10.10.10; now=169.254.1.1;

This is an example of a status message:

PTP670: status; Data Port Status; was=Down; now=Up;

Event messages

Event messages are listed in [Table 209](#). Definition of abbreviations:

SC = ";"

SP = " "

This is an example of an event message:

PTP670: event; auth_login; web user=MarkT; from=169.254.1.1; port=80;
connection=HTTP; authentication=local;

Table 209 Event messages

Facility	Severity	Identifier	Message content
security(4)	warning(4)	auth_idle	"Web user=" user-name SC SP
security(4)	info(6)	auth_login	"from=" IP-address SC SP
security(4)	warning(4)	auth_login_failed	"port=" port-number SC SP
security(4)	warning(4)	auth_login_locked	"connection=" ("HTTP" "HTTPS") SC SP
security(4)	info(6)	auth_logout	"authentication=" ("local" "RADIUS") SC
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

Facility	Severity	Identifier	Message content
security(4)	warning(4)	radius_auth_fail	"RADIUS user=" user-name SC SP "server " ("1" "2") " at " IP-address SP ("failed" "succeeded" "failed (no response)") SC
security(4)	alert(1)	resource_low	"Potential DoS attack on packet ingress " ("warning" "cleared") SC
security(4)	warning(4)	sec_zeroize	"Critical Security Parameters (CSPs) zeroized" SC
local6(22)	warning(4)	snmpv3_asn1	"ASN.1 parse error" SC
security(4)	warning(4)	snmpv3_auth	"Authentication failure" SC
local6(22)	warning(4)	snmpv3_decryption	"Decryption failure" SC
local6(22)	warning(4)	snmpv3_engine_id	"Unknown engine ID" SC
local6(22)	warning(4)	snmpv3_sec_level	"Unknown security level" SC
kernel(0)	warning(4)	sys_reboot	"System Reboot, reason=" reset-reason SC
security(4)	warning(4)	sys_software _upgrade	"Software upgraded from " software- version " to " software-version SC
local6(22)	warning(4)	telnet_idle	"Telnet user=" user-name SC SP
local6(22)	info(6)	telnet_login	"from=" IP-address SC SP "port=" port-number SC
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 "reason=" reason SC
security(4)	info(6)	eap_tls_auth	"MAC=" MAC-address SC "Authentication success" SC "Cipher=" cipher SC cipher = "None" "AES 128-bit TLS RSA" "AES 256-bit TLS RSA"

Facility	Severity	Identifier	Message content
security(4)	warning(4)	eap_tls_auth_failure	"MAC=" MAC-address SC "reason=" eap-tls-auth-reason SC eap-tls-auth-reason = "Authentication timeout" "Authentication error" "Certificates not installed" "Installed certificate has a common name mismatch" "Invalid certificate Root CA" "Installed certificate has invalid key length" "Certificate common name does not match with any entry in whitelist" "TLS handshake failed."
security(4)	info(6)	eap_tls_rekey	"MAC=" MAC-address SC "Rekey success" SC "Cipher=" cipher SC
security(4)	warning(4)	eap_tls_rekey_failure	"MAC=" MAC-address SC "reason=" eap-tls-rekey-reason SC eap-tls-rekey-reason = "Rekey timeout" "Rekey error" "Certificate common name does not match with any entry in whitelist" "TLS handshake failed."

Spectrum Management

This section describes how to use the Spectrum Management pages to monitor the radio spectrum usage of the PTP 670 link.

Spectrum Expert and Spectrum Management pages

There are two alternative web pages providing access to the spectrum monitoring information:

- the Spectrum Expert page, and
- the Spectrum Management page.

The Spectrum Expert page is the default as it is effectively a superset of the Spectrum Management page. However, it makes use of features only available in the most recent web browsers. It also requires additional data to be sent across the wireless link, thus reducing the capacity available for other types of traffic when the page is displayed.



Note

Internet Explorer versions up to and including IE8 do not support the HTTP features used in the Spectrum Expert page.

For these reasons, the PTP 670 Series may be configured to use the Spectrum Management page instead of the Spectrum Expert page. This is done by checking the **Disable Spectrum Expert (use old Spectrum Management)** control in the **Web Property** attribute under the **Management > Web > Web Properties** menu, as shown in [Figure 218](#).

[Figure 218](#) Disabling Spectrum Management page advanced web page

Webpage Properties		
Properties		
Attributes	Value	Units
Web Properties	<input checked="" type="checkbox"/> View Summary and Status pages without login <input checked="" type="checkbox"/> Disable Spectrum Expert (use old Spectrum Management)	
Distance Units	<input checked="" type="radio"/> Metric <input type="radio"/> Imperial	
Use Long Integer Comma Formatting	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Popup Help	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled	
Auto Logout Period	10	minutes
Browser Title	\$productName	
<input type="button" value="Apply Properties"/> <input type="button" value="Reset Form"/>		

**Note**

When configured to use the Spectrum Expert page, the PTP 670 is capable of automatically detecting whether the browser accessing the unit supports the required features. If it does not, the Spectrum Management page will be returned instead of the spectrum Expert page. Internet Explorer 8 is not compatible with the Spectrum Expert page.

Spectrum Expert page

Menu option: **System > Spectrum Expert**

This page is used to view and configure spectrum usage.

The Spectrum Expert page displays the following plots:

- The Local Receive Spectrum, and
- The Peer Receive Spectrum.

The Spectrum Expert page has two display modes:

- Standard Display mode – The ‘Standard’ Display mode is the mode which displays only the operational subband channels (shown in [Figure 219](#)). In this mode, the Extended Spectrum Scanning attribute could be Enabled but the Extended display box could be un-checked.

It has further two types of plot:

- Standard Display mode without realtime line
- Standard Display mode with realtime line

- Extended Display mode – The ‘Extended’ Display Mode shows the entire DSO Full Band range of channels along with highlighted operational channels (shown in [Figure 220](#)). In this mode, the Extended Spectrum Scanning attribute is Enabled.

This mode also has two types of plot:

- Extended Display mode without realtime line
- Extended Display mode with realtime line

The Extended display mode selection checkbox appears when the Extended Spectrum Scanning attribute is set to Enabled.

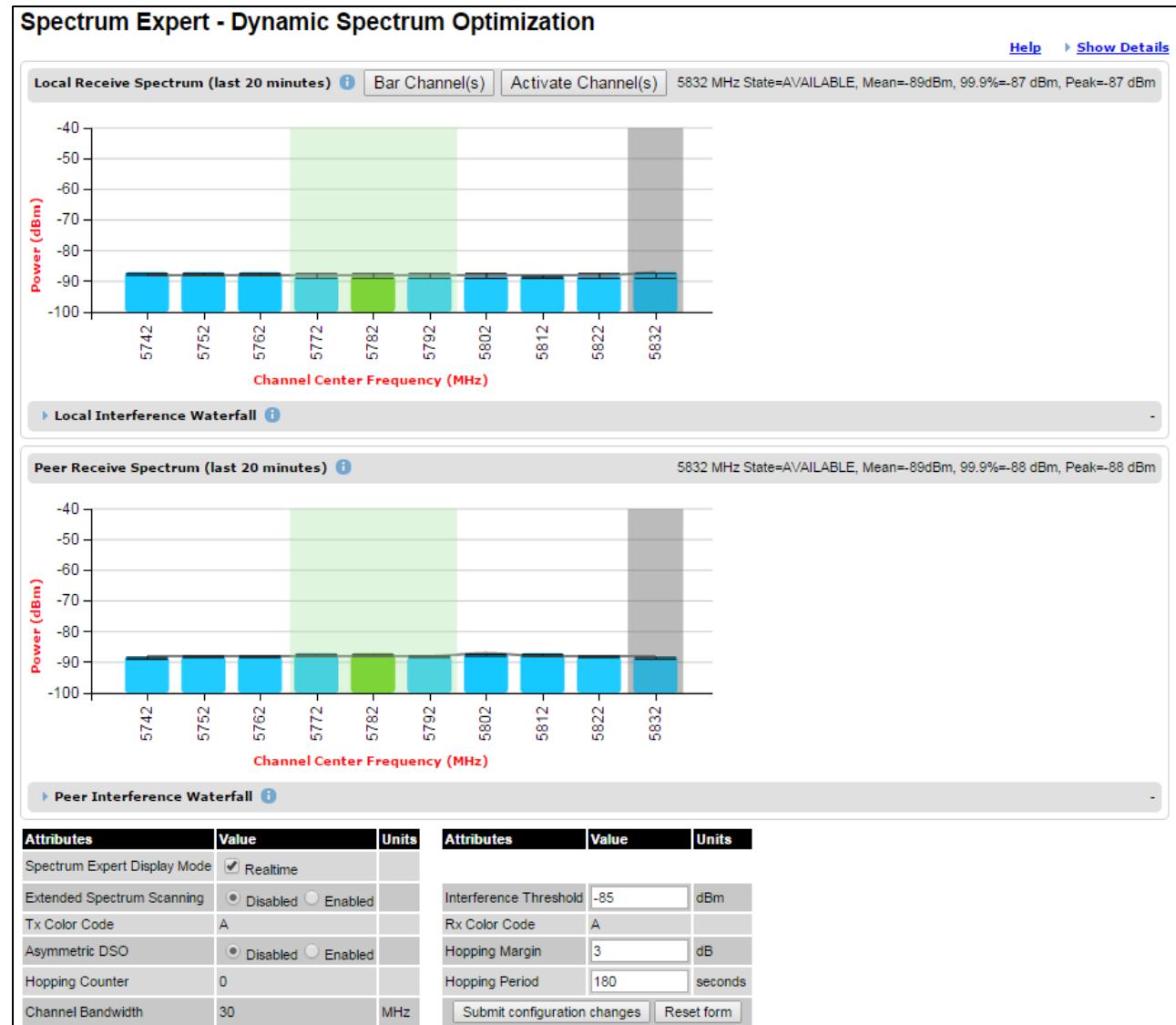
See [Interpreting the receive spectrum plot](#) on page [7-37](#) for details on the how to interpret these plots.

**Caution**

Do not leave the ODU with Extended Spectrum Scanning enabled during normal operation because this adversely affects the DSO response in the operating band.

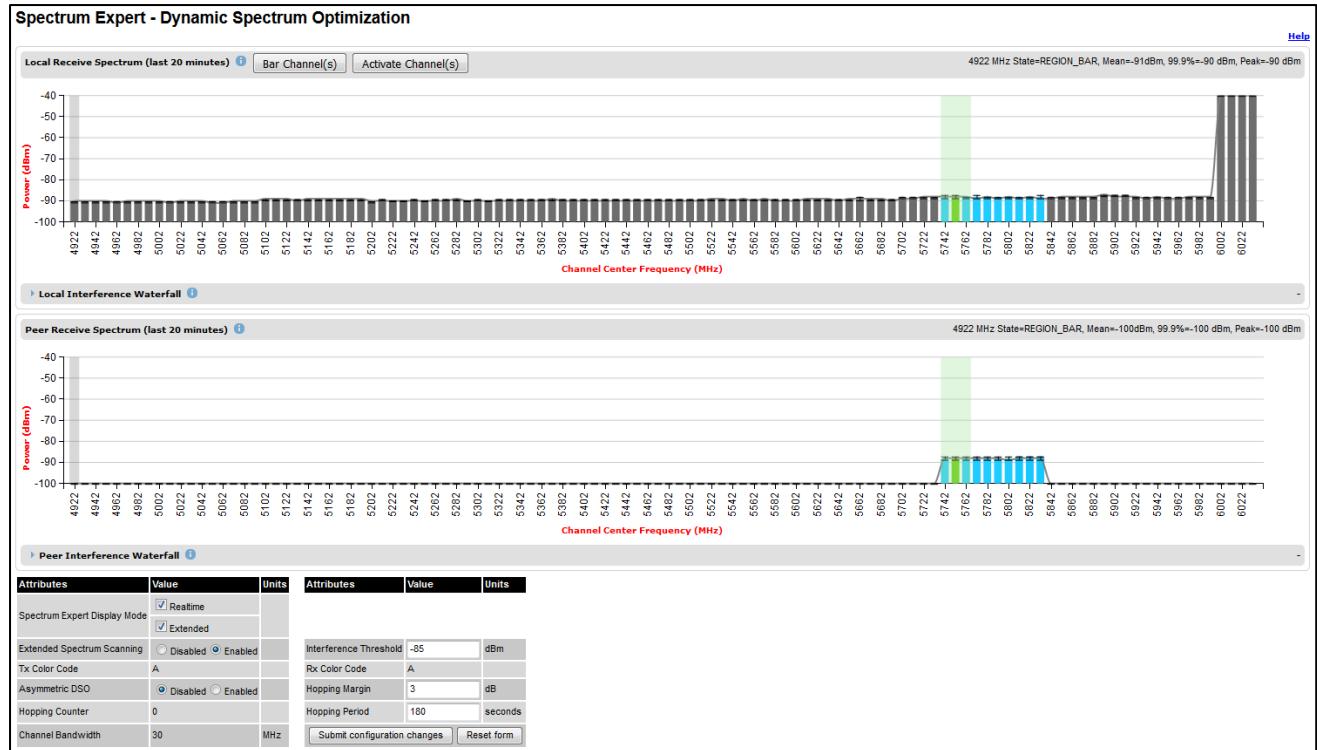
Standard Display mode

Figure 219 Spectrum Expert page – Standard Display mode



Extended Display Mode

Figure 220 Spectrum Expert page – Extended Display mode



Note

Figure 219 shows the default layout for a unit configured as a Master. On a unit configured as Slave, some of the controls at the bottom of the page are not available. In the remainder of this section, the screen shots shown are for the Master Unit.



Note

For Spectrum Expert Extended Display mode, Extended Spectrum Scanning is Enabled and Display mode is set to Extended.

Standard Display with extended layout

The page layout may be changed from the compact layout to the extended layout by clicking on the **Show Details** hyperlink on the top right of the page shown in Figure 219.

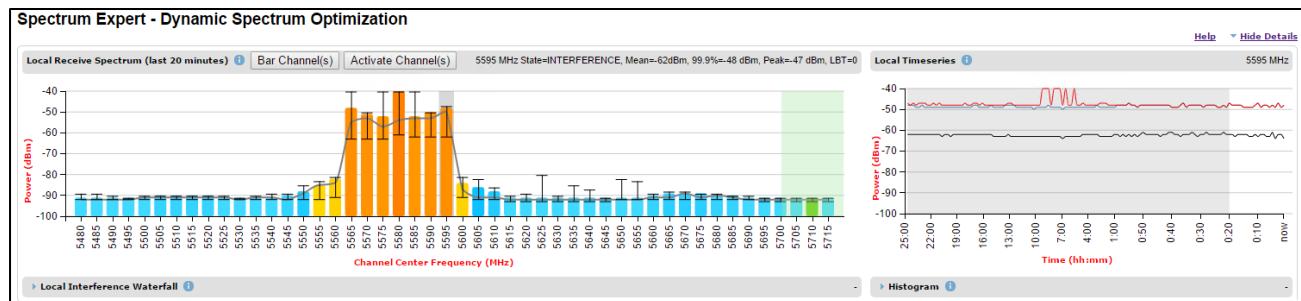
This hyperlink is only visible when the Extended Display checkbox in Spectrum Expert Display Mode is not selected.

A screen shot of the Spectrum Expert page in the extended layout is shown in Figure 221. It displays the following additional plots:

- The Local Timeseries, and
- The Peer Timeseries.

These plots are on the right of the corresponding Receive Spectrum plots. See [Selecting a Channel and a Time period](#) on page 7-45 for details on the timeseries plots.

Clicking on the **Hide Details** hyperlink returns to the compact layout.

Figure 221 Spectrum Expert page with Receive Spectrum and Timeseries for the Local unit

Full layout

The page layout may be extended further to give access to more information on either or both the local and the peer interference spectra.

For the local interference spectrum, clicking on the **Local Interference Waterfall** hyperlink below the Local Receive Spectrum plot shows:

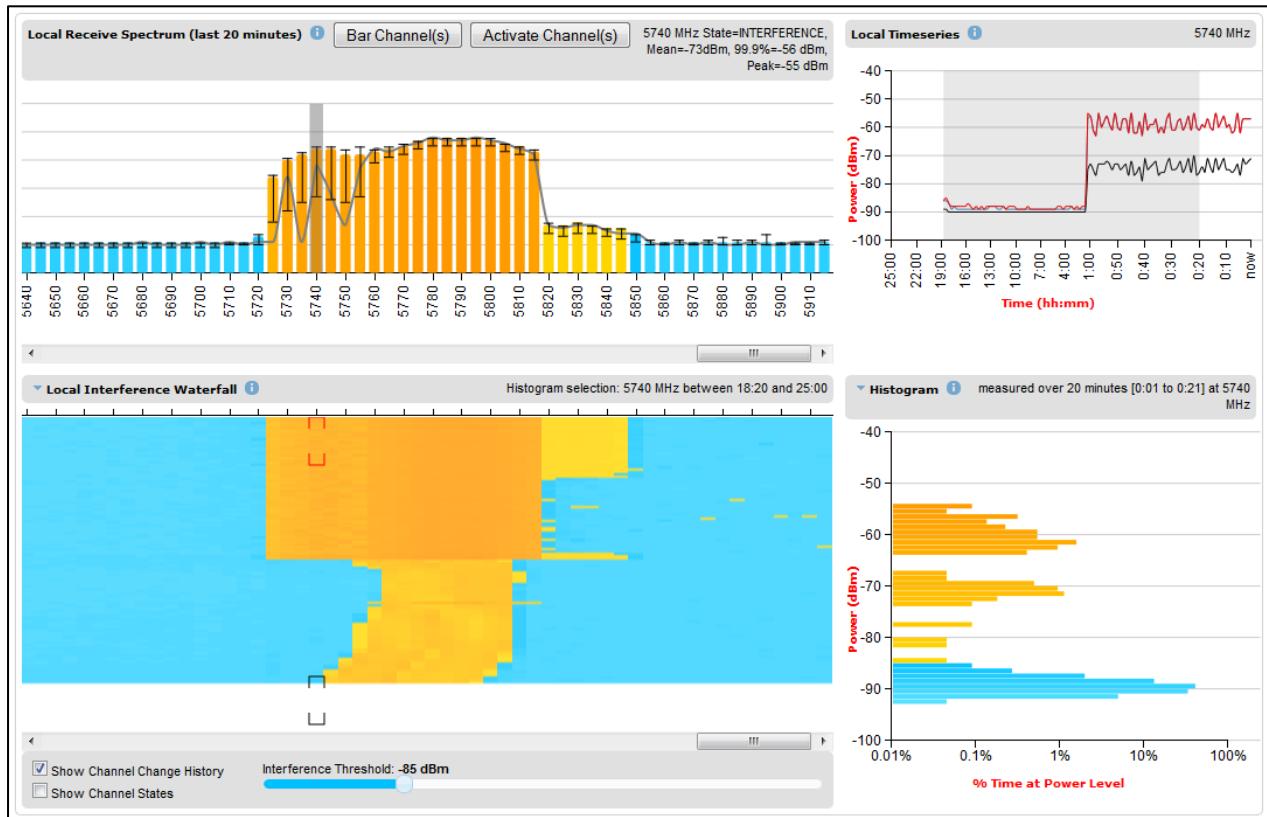
- The Local Interference Waterfall plot, if the Local TimeSeries was not shown (Figure 222), or
- The Local Interference Waterfall and the Histogram plots otherwise (Figure 223).

The same can be done for the peer section of the page.

Details on how to interpret the Interference Waterfall and Histogram plots are provided in sections [Interpreting the Interference Waterfall plot](#) on page 7-47 and [Interpreting the histogram plot](#) on page 7-49 respectively.

Figure 222 Spectrum Expert page showing the Receive Spectrum and Interference Waterfall for the Local unit

Figure 223 Spectrum Expert page showing the Receive Spectrum, Timeseries, Interference Waterfall and Histogram for the Local unit



Spectrum Management page

Menu option: **System > Spectrum Management**

Note that this page is only shown when the Spectrum Expert page has been disabled, as explained in [Spectrum Expert and Spectrum Management pages on page 7-29](#).

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



Note

The extended view is available only in Spectrum Expert, and not in Spectrum Management.

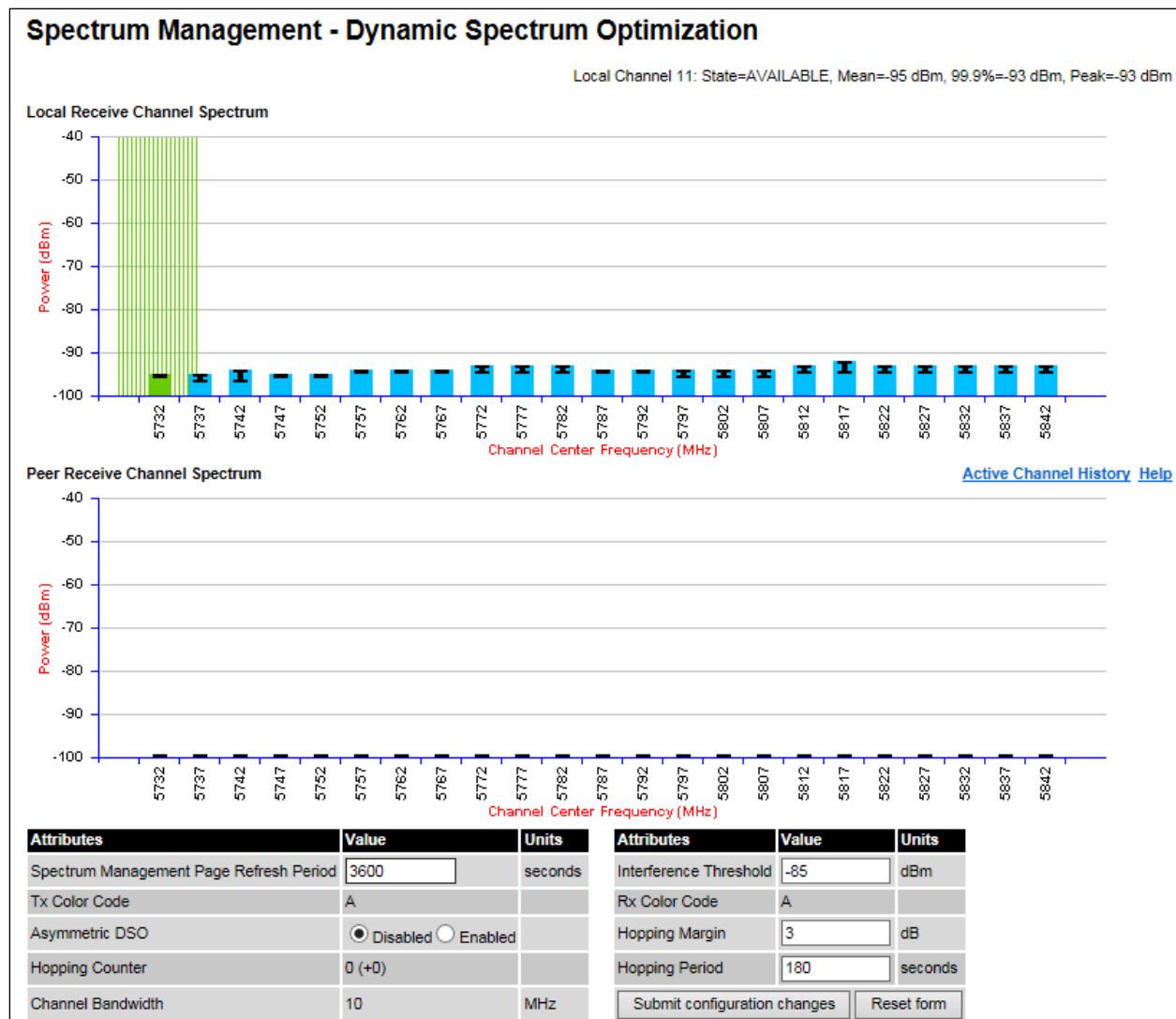
Figure 224 Spectrum Management page (Master unit)

Figure 224 shows the Spectrum Management page layout for a unit configured as a Master. On a unit configured as Slave, some of the controls at the bottom of the page are not available.

Spectrum Management Settings

All spectrum management configuration changes are applied at the master ODU only. These changes are then sent from the master to the slave, so that both master and slave keep identical copies of spectrum management configuration. It is therefore possible to swap master and slave roles on an active PTP 670 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 6-25.

**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 210](#))
- Update the attributes as required. At the slave unit, only Page Refresh Period can be updated.
- To save changes, click Submit configuration changes.

Table 210 Spectrum Management attributes

Attribute	Meaning
Spectrum Expert Display Mode	<p>Realtime: When set to Realtime, an additional line appears on the Receive Spectrum plots showing the most recent measurements of interference level for every channel</p> <p>Extended: Extended Display mode is visible only when Extended Scanning is enabled.</p> <p>This control is available in the Spectrum Expert page only.</p>
Extended Spectrum Scanning	<p>Enabled: Enables scanning of entire DSO full band channels.</p> <p>Disabled: Only the operational subband channels are scanned.</p> <p>This control is available in the Spectrum Expert page only.</p>
Spectrum Management Page Refresh Period	<p>The page refreshes automatically according to the setting entered here (in seconds).</p> <p>This control is available in the Spectrum Management page only.</p>
Hopping Margin	<p>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.</p>
Asymmetric DSO	<p>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.</p>
Spectrum Management Control	<p>Only displayed in radar regions. The options are DFS and DFS with DSO.</p>

Attribute	Meaning
Hopping Period	The Spectrum Management algorithm evaluates the metrics every "Hopping Period" seconds (180 seconds by default) looking for a channel with lower levels of interference. If a better channel is located, Spectrum Management performs an automated channel hop. If SNMP or SMTP alerts are enabled an SNMP TRAP or an email alert is sent warning the system administrator of the channel change.
Hopping Counter (not configurable)	This is used to record the number of channel hops. The number in the (+) brackets indicates the number of channel changes since the last screen refresh.
Interference Threshold	Spectrum Management uses the interference threshold to perform instantaneous channel hops. If the measured interference on a channel exceeds the specified threshold, then DSO will instruct the wireless to immediately move to a better channel. If a better channel cannot be found the PTP 670 Series will continue to use the current active channel. (Default -85 dBm).
Channel Bandwidth (not configurable)	This shows the value of the variable channel bandwidth selected.
Tx Color Code (not configurable)	This shows the Tx Color Code selected during Installation.
Rx Color Code (not configurable)	This shows the Rx Color Code selected during Installation.

Interpreting the receive spectrum plot

The Spectrum Expert page has two graphical plots:

- Local Receive Spectrum
- Peer Receive Spectrum

A more detailed example of one of these plots is shown in [Figure 219](#).

For more information, select the **Help** hyperlink at the top right of the Spectrum Expert page and follow the instructions.

X axis and Y axis

The X-axis shows a stylized view of the selectable wireless channels. Note that the distance between adjacent channels may be smaller than the channel bandwidth. If this is the case, adjacent channels overlap. Channels are displayed separately for clarity. The axis is labeled using the channel center frequencies in MHz. The Y-axis shows the interference power levels from -100 to -40 dBm.

Channel states

The active channel (Channel 9 in [Figure 219](#)) is always marked using hatched green and white lines on the Spectrum Management page or solid green on the Spectrum Expert page. The width of the hatching is directly proportional the channel bandwidth or spectral occupancy of the channel.

The individual channel metrics are displayed using a colored bar and an “I” bar. The colored bar represents the channel state ([Table 211](#)).

Table 211 Channel states represented in the Spectrum Expert plot

Color	State	Meaning
Green	Active	The channel is currently in use, hosting the wireless link.
Orange	Interference	The channel has interference above the interference threshold.
Blue	Available	The channel has an interference level below the interference threshold and is considered by the Spectrum Management algorithm suitable for hosting the Point-to-Point link.
Light Grey	Barred	The system administrator has barred this channel from use. For improved visibility, an additional red “lock” symbol is used to indicate that a channel is barred but The lock is not shown in Extended view.
Red	Radar Detected	A radar signal has been detected and operation on this channel is currently not allowed.
Dark Grey	Region Barred	Extended scanned channels outside the range of configured operational subband channels

Key metrics

The “I” bar and top of the colored bar represent three key metrics ([Table 212](#)). The vertical part of the “I” bar represents the statistical spread between the peak and the mean of the statistical distribution.

The arithmetic mean is the true power mean and not the mean of the values expressed in dBm. Spectrum Management uses the 99.9% Percentile as the prime interference measurement. All subsequent references to interference level refer to this percentile measurement.

Table 212 Key metrics represented in the Spectrum Expert plot

Metric	Description	How represented
Peak of Means	The largest mean interference measurement encountered during the quantization period. The peak of means is useful for detecting slightly longer duration spikes in the interference environment.	Upper horizontal bar.

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

Spectrum Expert page in fixed frequency mode

When the link is operating in fixed frequency mode, the Spectrum Expert page uses two visual cues ([Figure 225](#)). The main page title has the “Fixed Frequency Mode” suffix and the selected channels are identified by a red capital “F”.

Figure 225 Spectrum Expert page for Fixed Frequency – Standard display mode

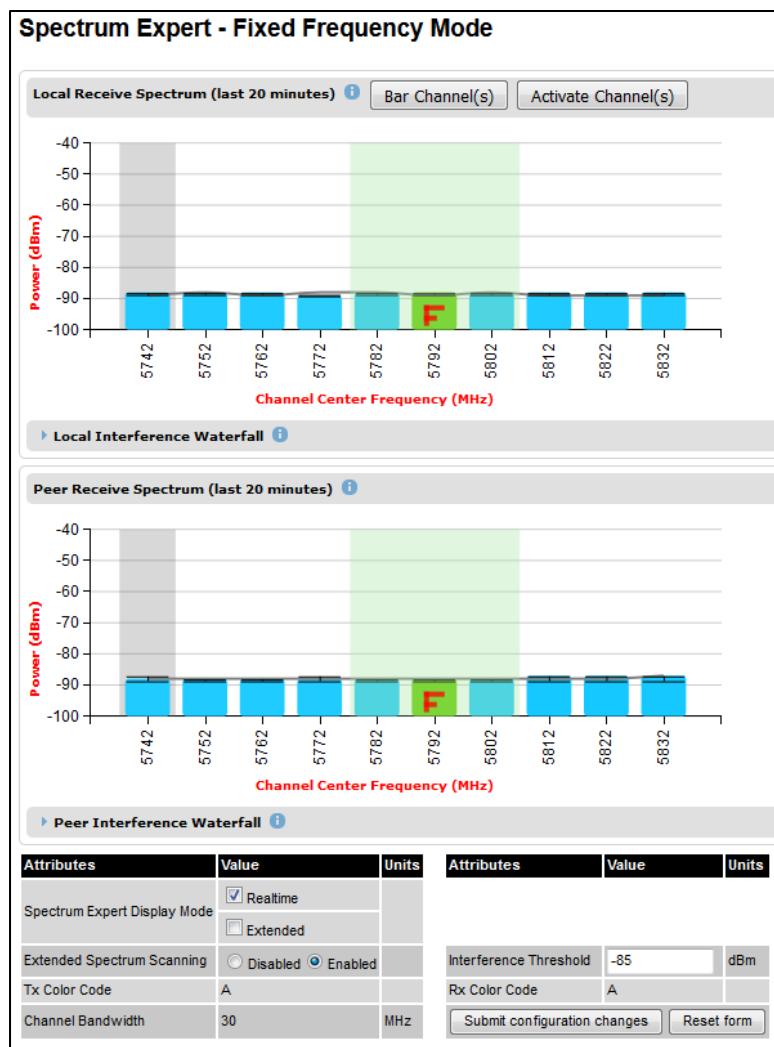
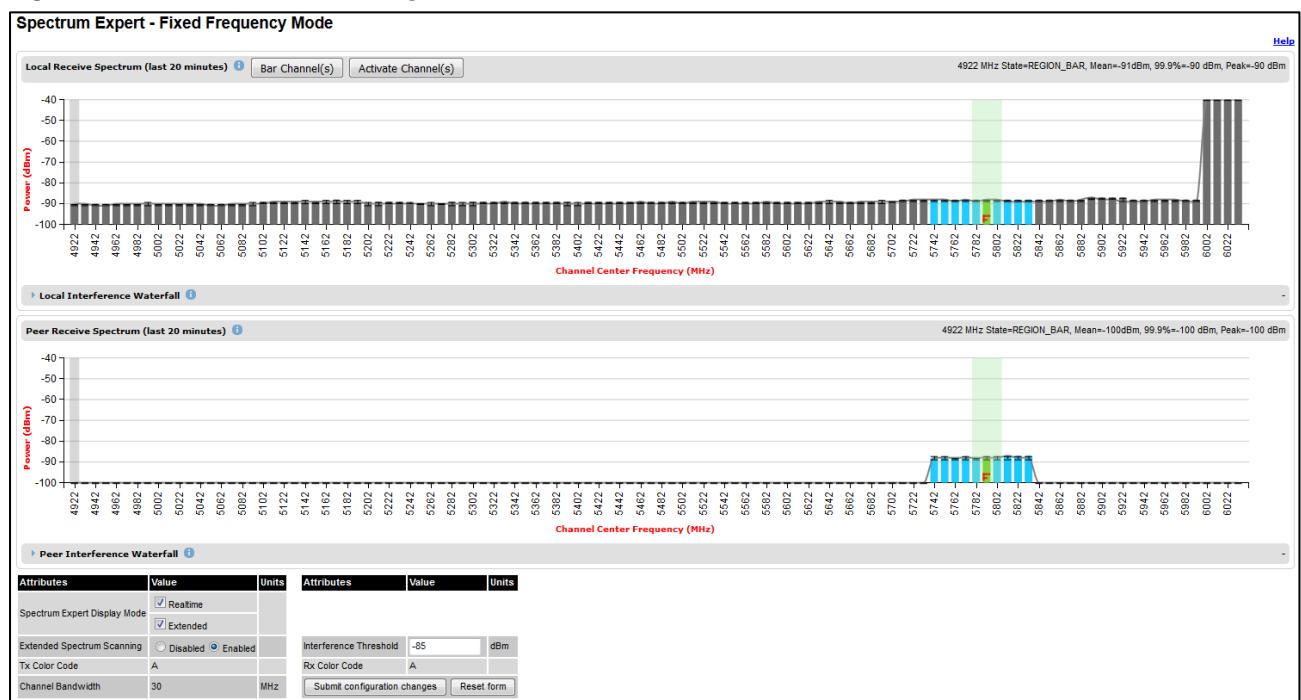


Figure 226 Spectrum Expert page for Fixed Frequency – Extended display mode



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

The only controls available to the master are the Spectrum Expert Display Mode and Interference Threshold attributes. They will have no effect on the operation of the wireless link and will only effect the generation of the channel spectrum graphics.

Spectrum Expert page in radar avoidance mode

When the link is operating in radar avoidance mode, the Spectrum Expert page (Figure 227) 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 213).

Figure 227 Spectrum Expert page with radar avoidance – Standard Display
Spectrum Expert - Radar Avoidance with Dynamic Spectrum Optimization

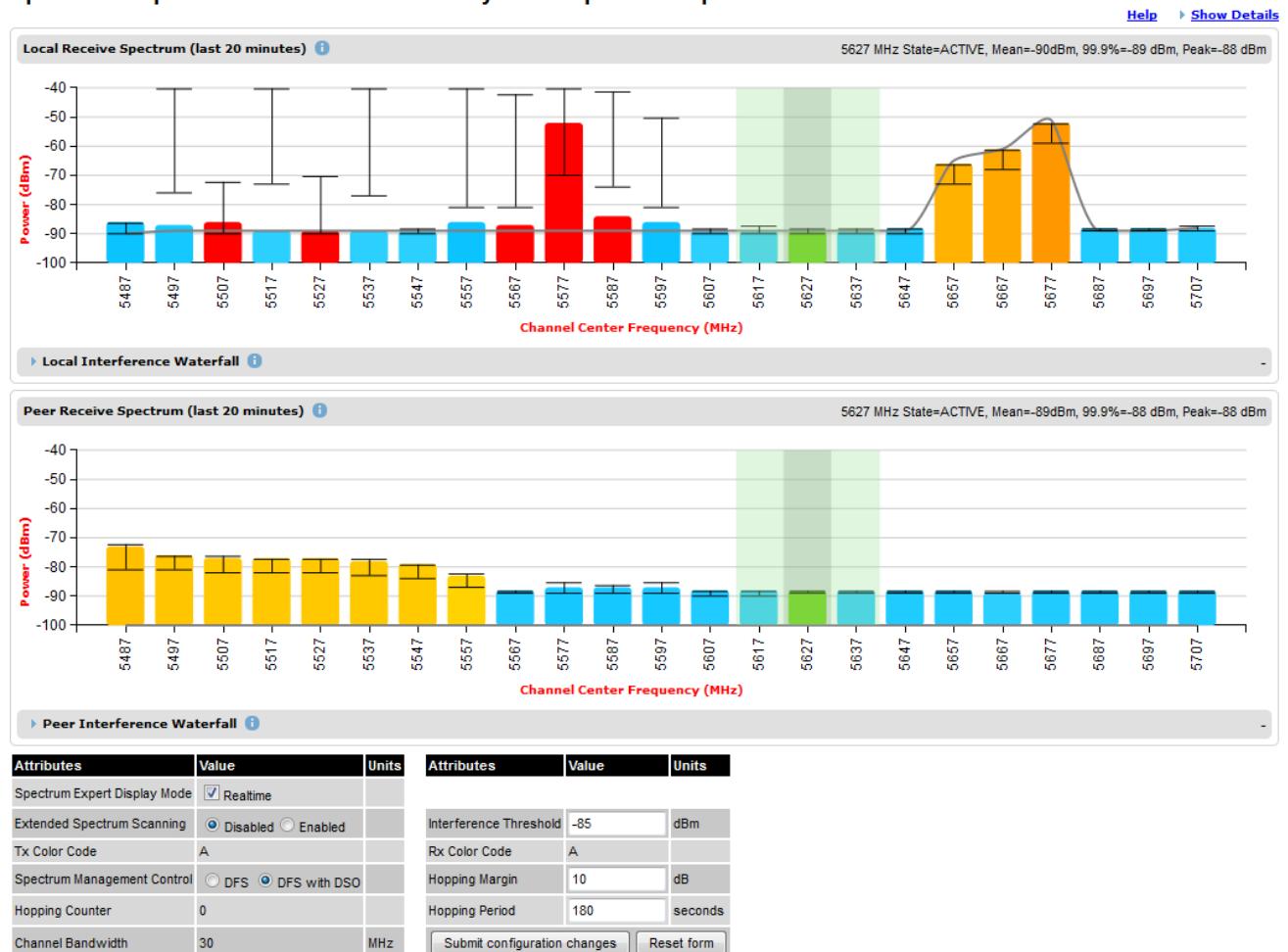
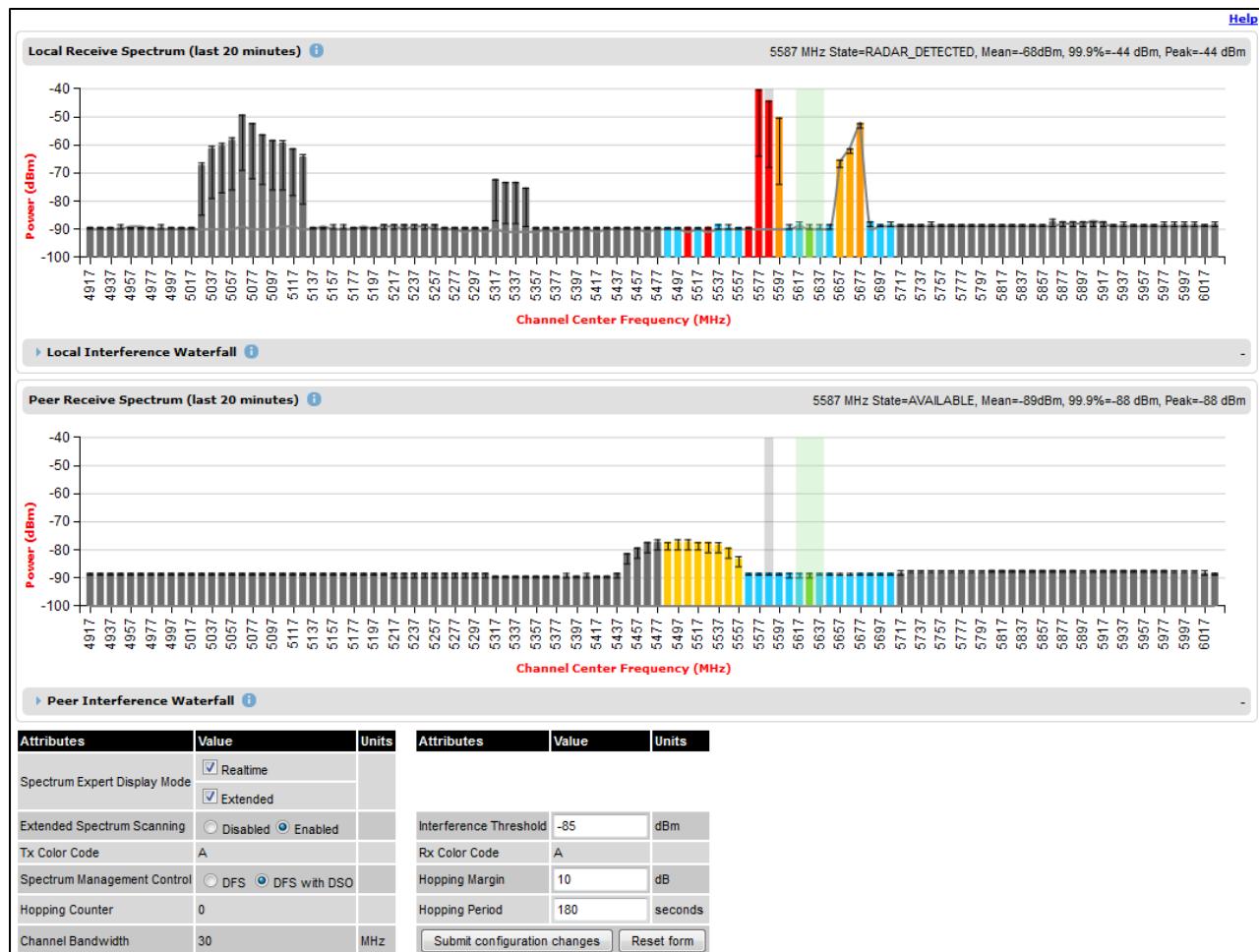


Figure 228 Spectrum Expert page with radar avoidance – Extended Display

When operating with RTTT (Road transport and Traffic Telematics) Avoidance enabled or other regulatory restrictions on channel usage, all channels marked with a “no entry” symbol with their associated statistics colored black are the prohibited channels. These channels are never used to host the wireless link, but CAC measurements are still taken so that adjacent channel biases can be calculated correctly and so the user can see if other equipment is in use.

Table 213 Channel states in the Spectrum Expert plot (radar avoidance)

Color	State and color	Meaning
Green	Active	This channel is currently in use hosting the Point-to-Point wireless link.
Orange	Interference	This channel has interference above the interference threshold
Blue	Available	This channel has an interference level below the interference threshold and is considered by the Spectrum Management algorithm suitable for hosting the Point-to-Point link

Color	State and color	Meaning
Dark grey	Barred	The system administrator has barred this channel from use. Because the low signal levels encountered when a unit is powered up in a laboratory environment prior to installation (which makes the grey of the channel bar difficult to see). An additional red "lock" symbol is used to indicate that a channel is barred.
Light grey	Unavailable	This channel needs to be monitored for one minute and found free of radar signal before it can be used for transmitting.
Red	Radar Detected	Impulsive Radar Interference has been detected on this channel and the channel is unavailable for 30 minutes. At the end of the 30 minute period a Channel Availability Check is required to demonstrate no radar signals remain on this channel before it can be used for the radio link.
Black	Region Bar	This channel has been barred from use by the local region regulator

Barring channels

Procedure:

- Log into the Master unit.
- Select menu option **System > Spectrum Expert**. The Spectrum Expert page is displayed.
- Select one channel by clicking on the graphical display. If required, select additional channels using control clicking, or select a range of channels using shift clicking. The example in [Figure 229](#) shows three channels selected at 4965 MHz, 4970 MHz and 4975 MHz.
- Click on the **Bar Channel(s)** button. A confirmation dialogue is displayed as shown in [Figure 230](#). Click **OK**.
- Barred channels are indicated by the lock symbol as shown in [Figure 231](#) on page [7-45](#).

To activate previously barred channels, select the barred channels and click on **Activate Channel(s)**.



Note

The **Bar Channel(s)** and **Activate Channel(s)** buttons are available on the Master unit, but not on the Slave unit.

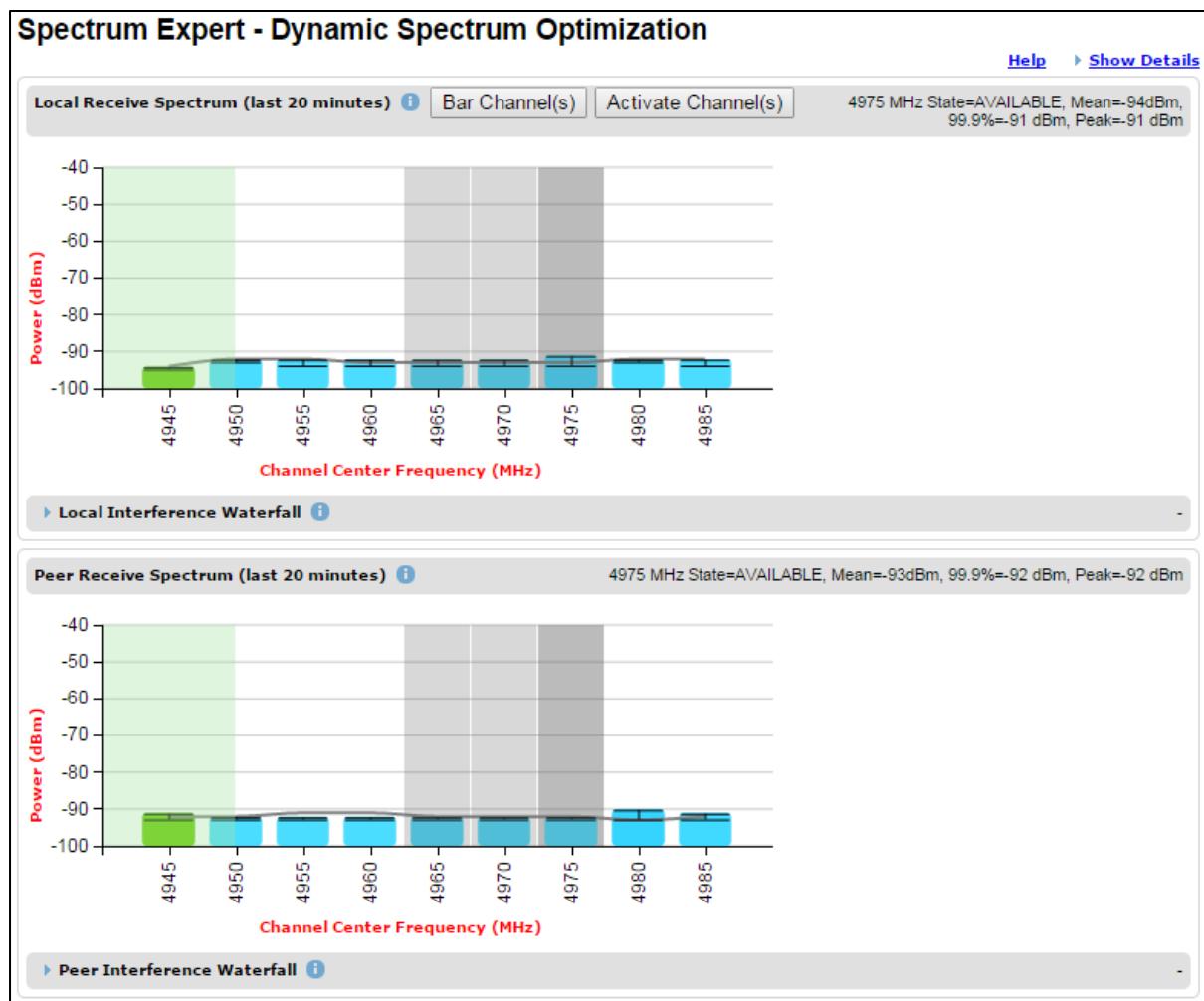
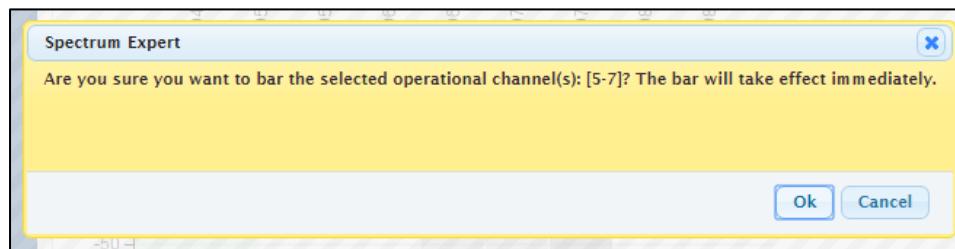
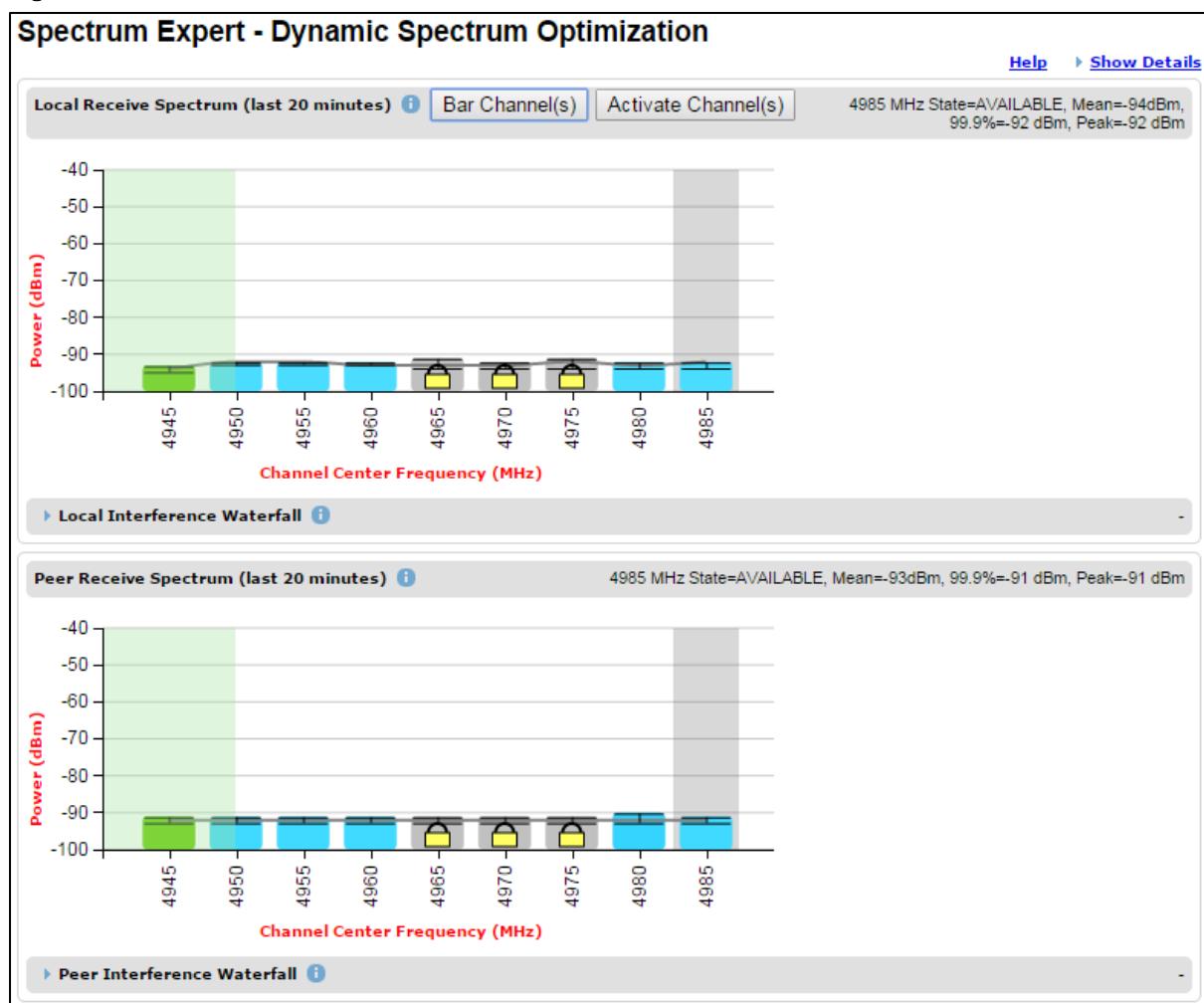
Figure 229 Selecting channels for barring**Figure 230** Channel barring confirmation

Figure 231 Barred channels

Selecting a Channel and a Time period

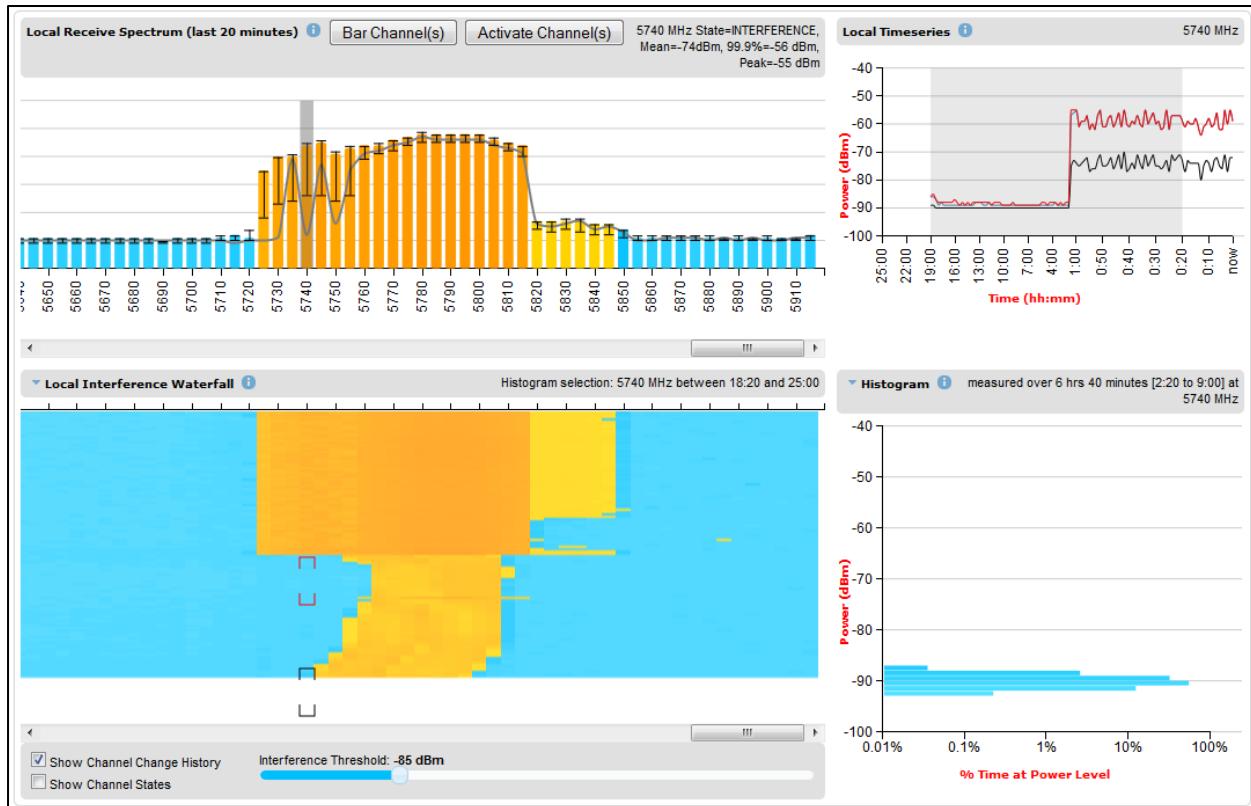
The Timeseries plot uses measurements for the selected channel. The Histogram plot uses measurements for the selected channel and the selected measurement period.

To select a channel, place the cursor in the Receive Spectrum display or the Interference Waterfall display. The Timeseries plot updates automatically to show the data for the selected channel. To select a combination of channel and time period, place the cursor in the Interference Waterfall display. The Histogram plot automatically updates to show data for the selected channel and time period.

The selected channel is shown with a grey background in the Receive Spectrum display and by the horizontal position of square brackets in the Interference Waterfall display. The selected time period is shown by the vertical position of the square brackets.

The Selected Channel is centred on 5740 MHz, and the time period is from 2:20 to 9:00 in the example in [Figure 232](#).

The selected frequency and time period are also displayed in the heading for the Timeseries and Histogram plots.

Figure 232 Selecting a channel on the Receive Spectrum

To freeze the selection of channel and time period, click on the cursor position. The frequency and time period are now fixed until a new combination is selected by clicking in a different location. The frozen time period is shown by red brackets in the Interference Waterfall display.

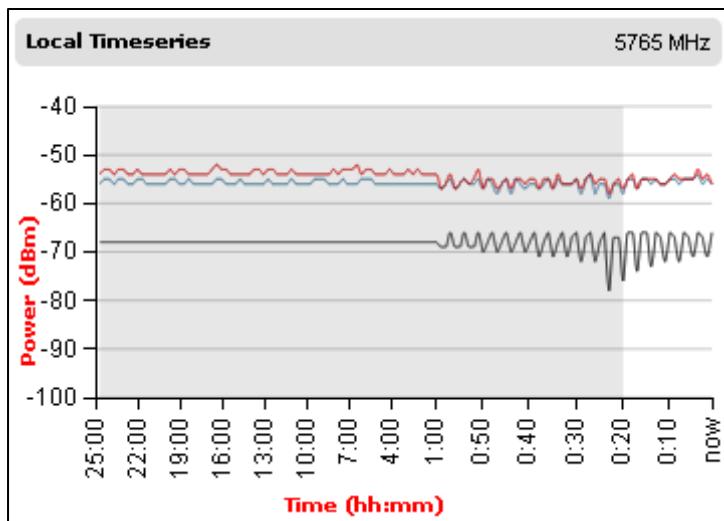
Interpreting the timeseries plot

This plot displays the interference measurements of all previous measurement quantization periods for the selected channel, up to a maximum of 25 h (Figure 233).

The channel is selected as described in [Selecting a Channel and a Time period](#). The center frequency of the selected channel is indicated in MHz at the top right of the Timeseries plot.

The colored lines represent interference measurements, with the color map provided in [Table 214](#).

A white background indicates the measurement period which is used to generate the Receive Spectrum plot. Typically, only the last 20 min are used, although any period of time where the wireless link has been down is excluded.

Figure 233 Spectrum Expert, Timeseries plot**Table 214** Interference represented in the time series plot

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

Interpreting the Interference Waterfall plot

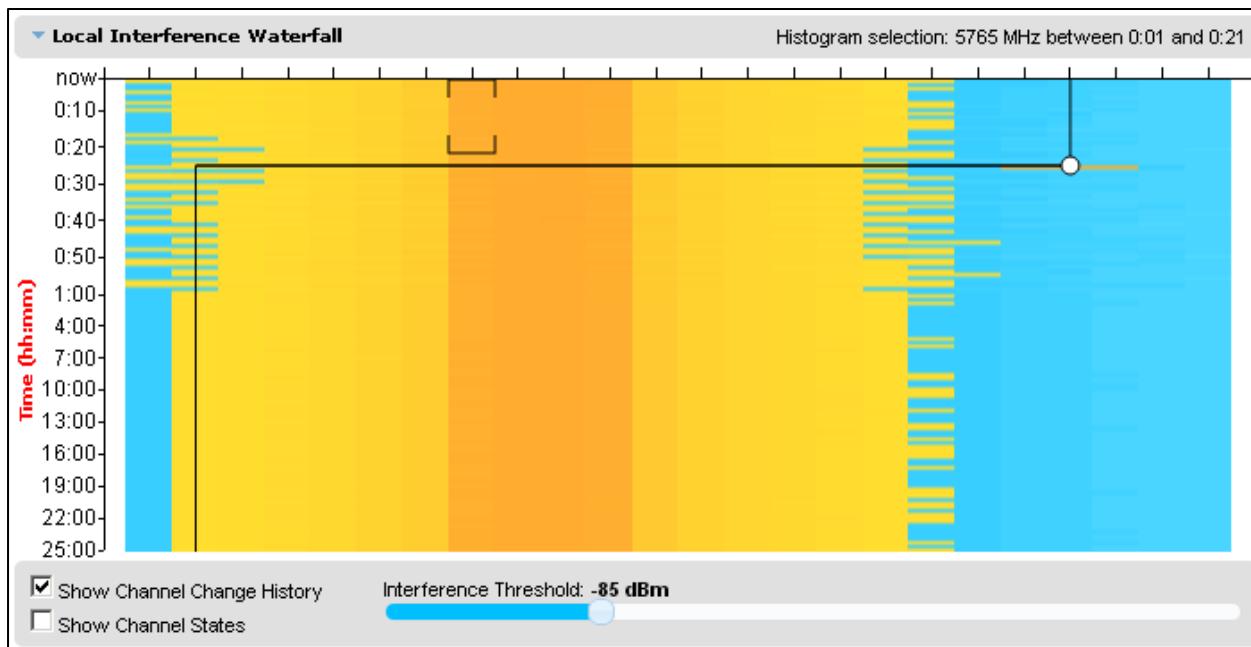
The Interference Waterfall indicates the level of interference for all the channels in the band over the last 25 h. [Figure 234](#) shows a screen capture example.

The channel and measurement period are selected as described in [Selecting a Channel and a Time period](#) on page 7-45. The center frequency of the selected channel and the time period are indicated at the top right of the Interference Waterfall plot.

The X-axis corresponds to the channel center frequency and is horizontally aligned with the Receive Spectrum plot.

The Y-axis corresponds to the time in the past in hours and minutes, with the most recent period being at the top of the plot.

Each channel and measurement period is indicated using the color scale given in [Table 211](#).

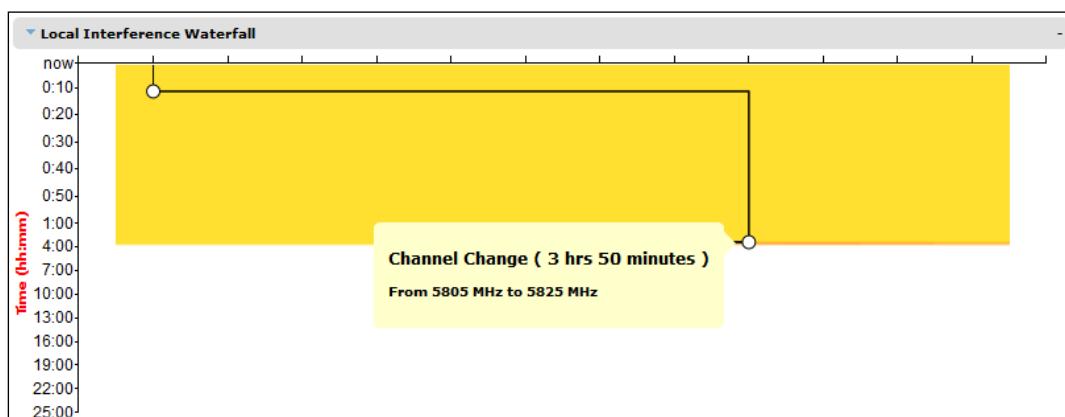
Figure 234 Spectrum Expert, Interference Waterfall plot

Setting the interference threshold

The interference threshold may be set using the sliding control located directly below the Interference Waterfall plot. This is an alternative to the method described in [Spectrum Management Settings](#) on page 7-34. For either method, the change to the Interference Threshold is not taken into account until the Submit button is clicked.

Viewing the active channel history

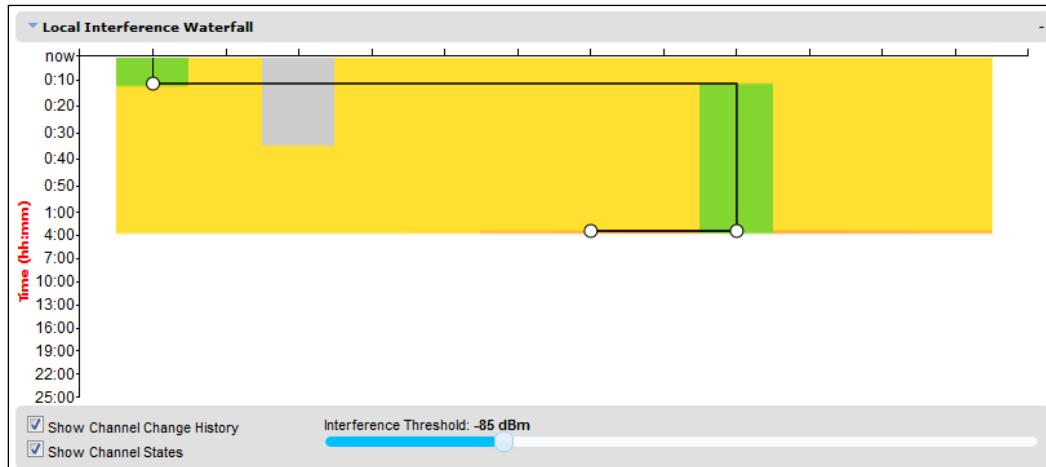
To display the active channel history, tick the Show Channel Change History control right below the Interference Waterfall plot. The active channel history over the last 25 hours is plotted as a black line overlay on the Interference Waterfall plot. A circle is displayed every time the active channel has changed. By hovering above the circle, the reason for the channel change is indicated, as shown in [Figure 235](#).

Figure 235 Spectrum Expert, Interference Waterfall with active channel history

Viewing the channel states

To display the Channel States, tick the Show Channel State control right below the Interference Waterfall plot. Figure 236 shows an example of the Interference Waterfall when the Channel States are displayed. The colors used are defined in [Channel states](#) on page 7-38.

Figure 236 Spectrum Expert page, Interference Waterfall plot with channel states



Interpreting the histogram plot

The histogram plot indicates the percentage of the measurements in the selected measurement period where the interference level for the selected channel is at a given level (Figure 237).

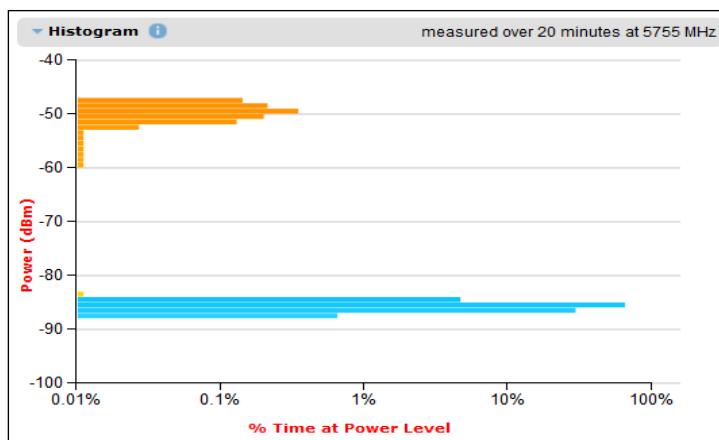
The channel and measurement period are selected as described in [Selecting a Channel and a Time period](#) on page 7-45. The combined selection is indicated graphically by a pair of brackets in the Waterfall plot, and in text form on the top right of the Histogram plot, as shown in Figure 236.

The X-axis corresponds to a percentage of the measurements in the measurement period on a logarithmic scale.

The Y-axis corresponds to actual interference level in dBm.

The bar for each each power level is of the same color as in the Interference Waterfall plot.

Figure 237 Spectrum Expert page, histogram plot



Spectrum Expert example

In this example from a real-world link, shown in [Figure 238](#), the channel at 5740 MHz has been selected for analysis.

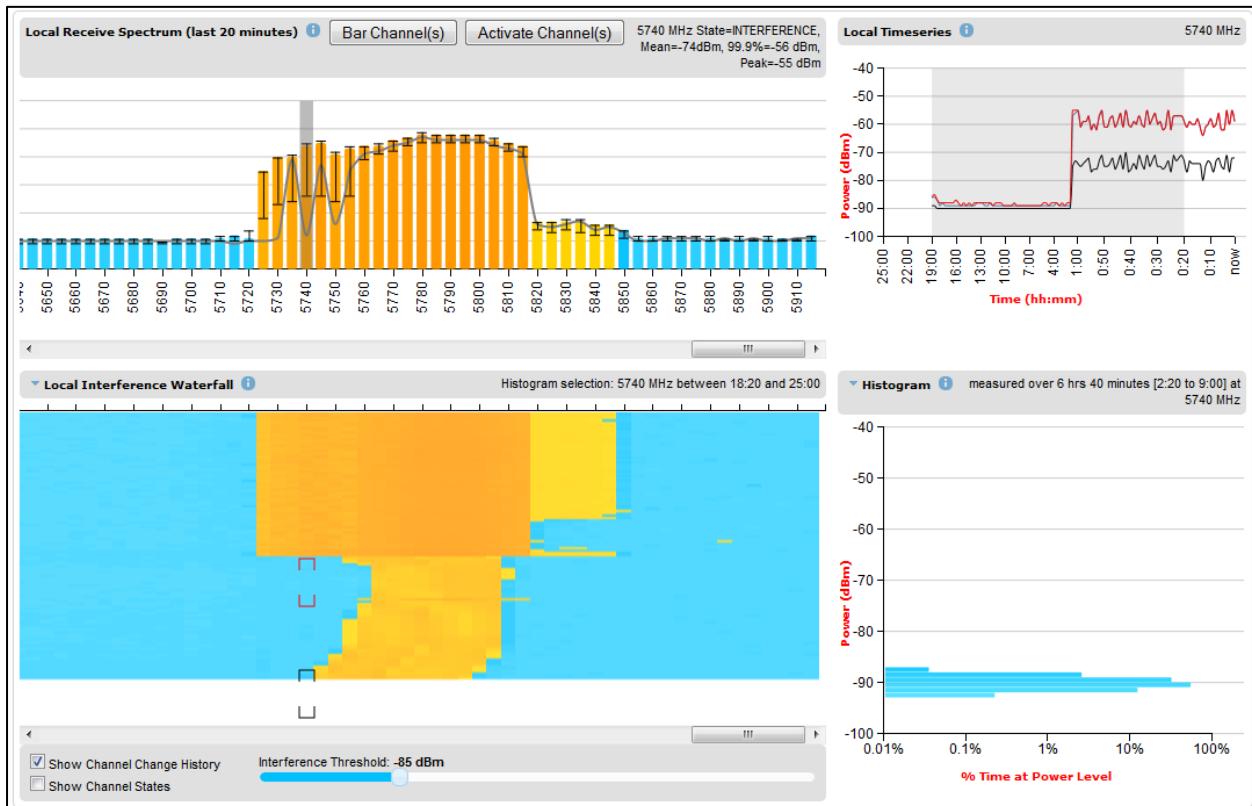
The Spectrum display is based in the most recent 20 minute period. The height of the colored bar in the selected channel shows that the 99.9th percentile of the interference is at about -66 dBm. The orange color of the bar is a reminder that this level is above the interference threshold of -85 dBm.

The upper bar of the “I” bar indicates the peak level of the interference. The lower bar of the “I” bar indicates the mean level of the interference. The height of the “I” bar represents the peak to mean ratio. In this channel, the peak to mean ratio is about 15 dB.

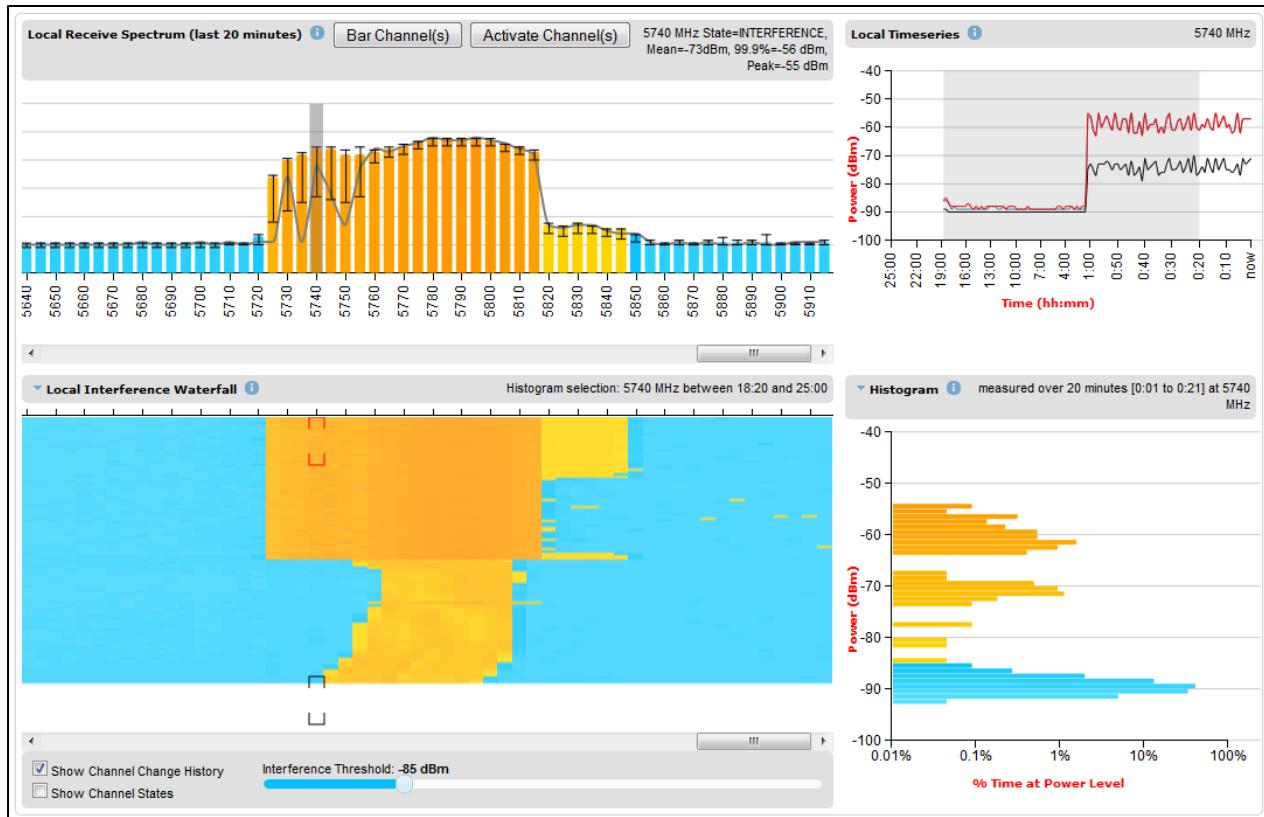
The red and black traces in the Timeseries plot show that the peak and mean interference levels have been maintained at approximately constant levels over a period of about two hours. Before that period, the interference level was considerably lower, at about -90 dBm.

In the Interference Waterfall plot, the selected time period is from 2 hours 20 minutes to 9 hours ago. The plot shows that interference occurred suddenly, across a broad band of channels, shortly after the selected period, or about two hours ago, and that it has been maintained at an approximately constant level since then. The Histogram plot shows that, prior to the onset of interference, the interference level was consistently close to -90 dBm, corresponding to the earlier part of the Timeseries plot.

Figure 238 Spectrum Expert, example 1



In [Figure 239](#), the time period for the Histogram plot has been set to the most recent 20 minutes. The histogram shows that interference levels are distributed over the range of approximately -74 dBm to approximately -54 dBm.

Figure 239 Spectrum Expert, example 2

The interference observed in [Figure 239](#) for the channel at 5740 MHz during the recent two hour period is not compatible with satisfactory operation a PTP 670 link.

The situation is, if anything, even worse in the channel at 5780 MHz, as shown in [Figure 240](#), where the interference level was historically worse, and in the recent period was consistently in the range -52 dBm to -58 dBm.

[Figure 241](#) shows the recent history of the channel at 5835 MHz. In this case, the peak interference is less than -80 dBm. This channel is likely to support satisfactory operation at a receive signal level of -60 dBm or greater.

Figure 240 Spectrum Expert, example 3

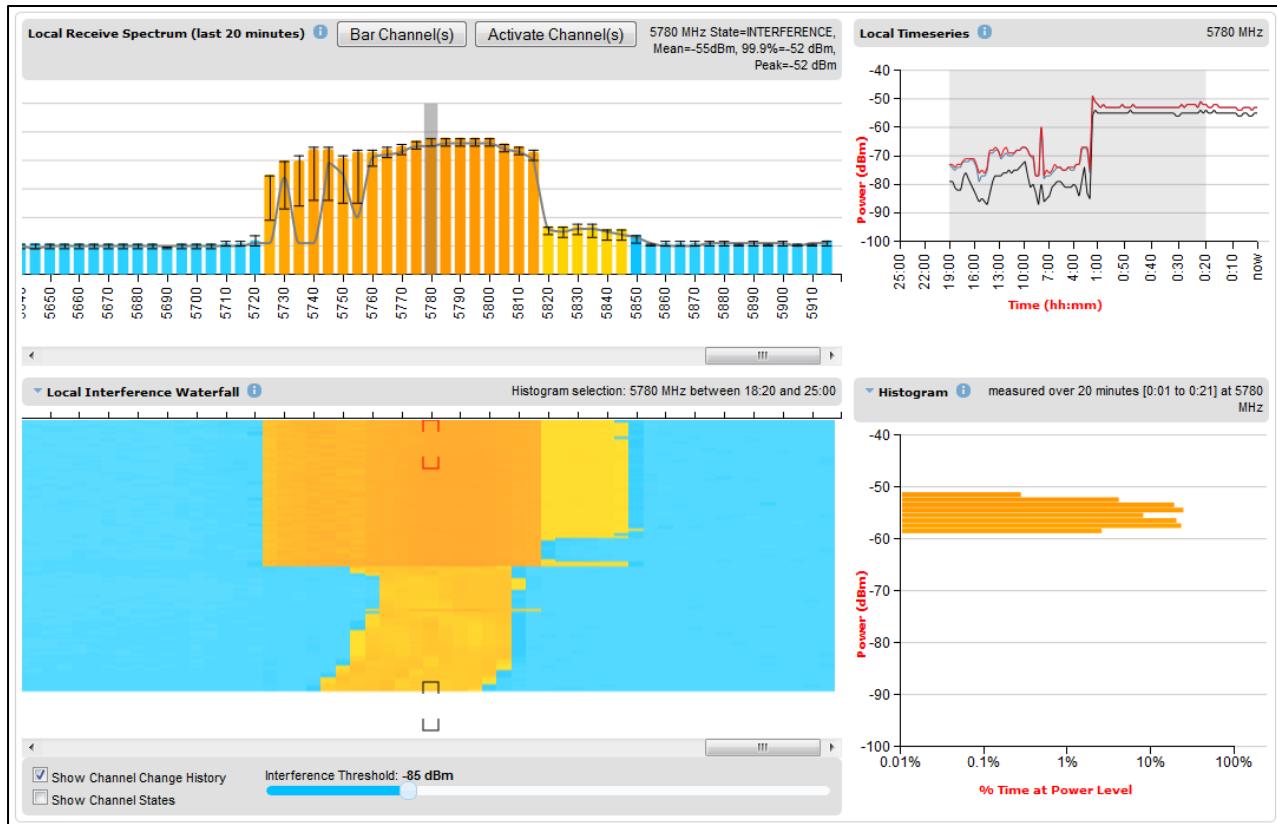
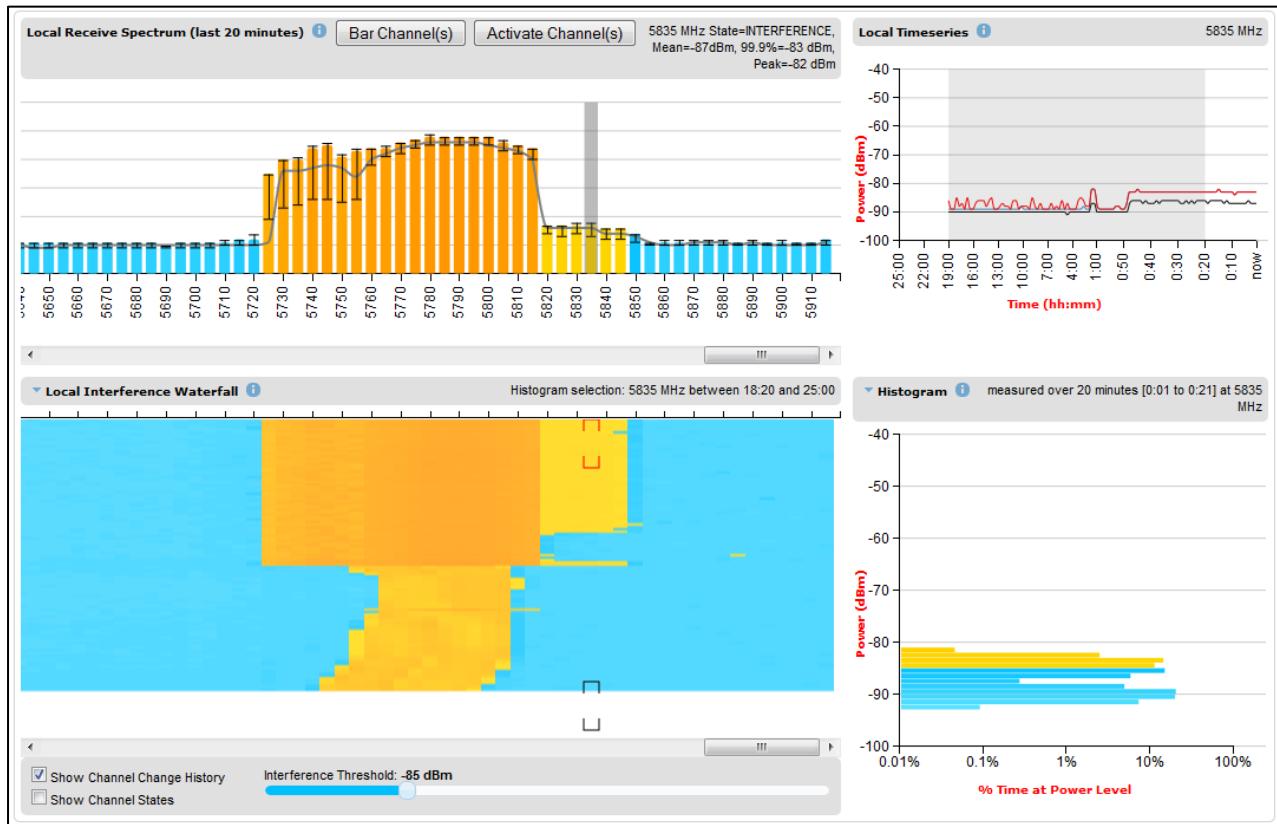


Figure 241 Spectrum Expert, example 4



Managing security

This section describes the procedure for Zeroising critical security parameters.

Other security configuration procedures are described in [Security menu](#) on page 6-103.

Zeroizing critical security parameters

Use this procedure to zeroize Critical security parameters (CSPs) as follows:

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

Procedure:

- On the Security menu, click Zeroize CSPs.
- Click Select Zeroize CSPs and Reboot Wireless Unit.
- Confirm the reboot.



Note

Alternatively, select the Zeroize CSPs option in Recovery mode as described in [Zeroize Critical Security Parameters](#) on page 7-83

System statistics

This section describes how to use the system statistics pages to manage the performance of the PTP 670 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 242](#)) contains eight diagnostic attributes that are presented as arrays of four elements ([Table 215](#)).

Figure 242 System Histograms section of the System Statistics page (PTP topology)

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

Figure 243 System Histograms section of the System Statistics page (HCMP Topology, Wireless Interface Selector set to “All Wireless Interfaces”)

System Statistics				
Attributes	Value			Units
Wireless Interface Selector	All Wireless Interfaces			
Attributes	Value	Value	Value	Units
Remote Unit Name	Slave_58_01_D5	Not Available	Not Available	
System Histograms				
Transmit Power	23.0,	23.0	28.0, 28.0	0.0, 0.0 dBm
Receive Power	-46.2,	-46.2	-109.9, -110.0	0.0, 0.0 dBm
Vector Error	-35.5,	-33.7	0.0, 0.0	0.0, 0.0 dB
Link Loss	67.2,	67.2	0.0, 0.0	0.0, 0.0 dB
Signal Strength Ratio	3.1,	3.2	0.0, 0.0	0.0, 0.0 dB
Transmit Data Rate	57.89,	57.89	0.00, 0.00	0.00, 0.00 Mbps
Receive Data Rate	2.78,	2.78	0.00, 0.00	0.00, 0.00 Mbps
Aggregate Data Rate	60.67,	60.67	0.00, 0.00	0.00, 0.00 Mbps
Histogram Measurement Period	01:00:00			
<input type="button" value="Reset System Histogram Measurement Period"/>				
Attributes	Value			Units
Elapsed Time Indicator	01:21:18			
Statistics Page Refresh Period	3600			seconds
<input type="button" value="Submit Page Refresh Period"/>				

The element arrays represent the following:

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

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

Use the [Diagnostics Plotter page](#) on page 7-73 to plot these attributes against time. Use the [Generate Downloadable Diagnostics page](#) on page 7-75 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 215 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: $\text{Peer_Tx_Power (dBm)} - \text{Local_Rx_Power (dBm)} + 2 \times \text{Antenna_Pattern (dBi)}$
Signal Strength Ratio	<p>The Signal Strength Ratio (calculated over a one hour period) is:</p> $\frac{\text{Power received by the vertical antenna input (dB)}}{\text{Power received by the horizontal antenna input (dB)}}$ <p>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.</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
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 (PTP topology)

The System Counters section of the System Statistics page ([Figure 244](#)) contains Data Port Counters ([Table 216](#)), Management Agent Counters ([Table 218](#)) and Wireless Port Counters and Performance Information ([Table 219](#)).

Figure 244 System Counters section of the System Statistics page

Attributes	Value	Units
Data Port Counters		
Tx Frames	197 (+197)	
Rx Frames	248 (+248)	
Second Data Port Counters		
Tx Frames	14 (+14)	
Rx Frames	3 (+3)	
Management Agent Counters		
Packets To Internal Stack	203 (+208)	
Packets From Internal Stack	293 (+293)	
Wireless Port Counters and Performance Information		
Tx Frames	100 (+100)	
Rx Frames	104 (+104)	
Link Symmetry	1 to 1	
Link Capacity	226.65	Mbps
Transmit Modulation Mode	256QAM 0.81 (Single) (30 MHz)	
Receive Modulation Mode	256QAM 0.81 (Dual) (30 MHz)	
Receive Modulation Mode Detail	Running At User-Configured Max Modulation Mode	
Wireless Link Availability	100.0000	%
Data Bridging Availability	100.0000	%
Byte Error Ratio	1.356e-8	
Counter Measurement Period	00:01:32	
Reset System Counters		

Procedure:

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

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

Table 216 Data Port Counters

Attribute	Meaning
Tx Frames	The total number of good frames the bridge has sent for transmission through the port selected for Data Service
Rx Frames	The total number of good frames the bridge has received through the port selected for Data Service

Table 217 Second Data Port Counters

Attribute	Meaning
Tx Frames	The total number of good frames the bridge has sent for transmission through the port selected for Second Data Service
Rx Frames	The total number of good frames the bridge has received through the port selected for Second Data Service

Table 218 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 219 Wireless Port Counters and Performance Information

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

Attribute	Meaning
Receive Modulation Mode Detail	The receive modulation mode in use. For a list of values and their meanings, see Table 198 .
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 245](#)) contains two attributes ([Table 220](#)).

Figure 245 Other attributes section of the System Statistics page

Attributes	Value	Units
Elapsed Time Indicator	00:07:55	
Statistics Page Refresh Period	3600	seconds
<input type="button" value="Submit Page Refresh Period"/>		

Procedure:

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

Table 220 Other attributes in the System Statistics page

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

Wireless Port Counters page

PTP topology

Menu option: **System > Statistics > Wireless Port Counters** (Figure 246).

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

Figure 246 Wireless Port Counters page (PTP topology)

Wireless Port Counters					
Attributes	Value	Units	Attributes	Value	Units
Tx Frames	132 (+32)		Rx Frames	491 (+387)	
Tx Frames Q0	0 (+0)		Rx Frames With Crc Error	0 (+0)	
Tx Frames Q1	125 (+125)		Rx Frames Q0	0 (+0)	
Tx Frames Q2	0 (+0)		Rx Frames Q1	160 (+160)	
Tx Frames Q3	0 (+0)		Rx Frames Q2	0 (+0)	
Tx Frames Q4	0 (+0)		Rx Frames Q3	0 (+0)	
Tx Frames Q5	0 (+0)		Rx Frames Q4	0 (+0)	
Tx Frames Q6	0 (+0)		Rx Frames Q5	0 (+0)	
Tx Frames Q7	7 (+7)		Rx Frames Q6	0 (+0)	
Tx Drops Q0	0 (+0)		Rx Frames Q7	331 (+331)	
Tx Drops Q1	0 (+0)				
Tx Drops Q2	0 (+0)				
Tx Drops Q3	0 (+0)				
Tx Drops Q4	0 (+0)				
Tx Drops Q5	0 (+0)				
Tx Drops Q6	0 (+0)				
Tx Drops Q7	0 (+0)				
Tx Frames Second Data	3 (+3)		Rx Frames Second Data	198 (+198)	
Tx Drops Second Data	0 (+0)				
Attributes	Value	Units	Attributes	Value	Units
Counter Page Refresh Period	3600	seconds	Counter Measurement Period	00:05:36	
<input type="button" value="Submit Page Refresh Period"/>			<input type="button" value="Reset System Counters"/>		



Note

If the ODU is configured for OOB Remote Management Service, the OOB Management counters will be displayed instead of Second Data counters (i.e. Tx Frames Management → Tx Frames Second Data, Tx Drops Management → Tx Drops Second Data, and Rx Frames Management → Rx Frames Second Data)

Procedure:

- Review the attributes (Table 221).
- 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 221 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.
Rx Frames Second Data	Total number of frames received at the wireless port in the Out-of-Band management queue

HCMP topology

Menu option: **System > Statistics > Wireless Port Counters** (Figure 247 to Figure 249).

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

Figure 247 Wireless Port Counters page (Master, HCMP topology, Wireless Interface Selector set to a single link)

Wireless Port Counters

Attributes	Value	Units
Wireless Interface Selector	Slave_58_01_D5	
Attributes	Value	Units
Tx Frames	75,333 (+0)	
Tx Frames Q0	75,333 (+0)	
Tx Frames Q1	0 (+0)	
Tx Frames Q2	0 (+0)	
Tx Frames Q3	0 (+0)	
Tx Drops Q0	0 (+0)	
Tx Drops Q1	0 (+0)	
Tx Drops Q2	0 (+0)	
Tx Drops Q3	0 (+0)	
Byte Error Ratio	3.574e-9	
Attributes	Value	Units
Counter Page Refresh Period	3600	seconds
<input type="button" value="Submit Page Refresh Period"/>		<input type="button" value="Reset System Counters"/>

Figure 248 Wireless Port Counters page (Master, HCMP topology, Wireless Interface Selector set to All Wireless Links)

Wireless Port Counters				
Attributes	Value			Units
Wireless Interface Selector	All Wireless Interfaces ▾			
Attributes	Value	Value	Value	Units
Remote Unit Name	Slave_58_01_D5	Not Available	Not Available	
Tx Frames	75,333 (+0)	0 (+0)	0 (+0)	
Rx Frames	171,324 (+0)	0 (+0)	0 (+0)	
Rx Frames With Error	3 (+0)	0 (+0)	0 (+0)	
Tx Frames Q0	75,333 (+0)	0 (+0)	0 (+0)	
Tx Frames Q1	0 (+0)	0 (+0)	0 (+0)	
Tx Frames Q2	0 (+0)	0 (+0)	0 (+0)	
Tx Frames Q3	0 (+0)	0 (+0)	0 (+0)	
Tx Drops Q0	0 (+0)	0 (+0)	0 (+0)	
Tx Drops Q1	0 (+0)	0 (+0)	0 (+0)	
Tx Drops Q2	0 (+0)	0 (+0)	0 (+0)	
Tx Drops Q3	0 (+0)	0 (+0)	0 (+0)	
Rx Frames Q0	171,322 (+0)	0 (+0)	0 (+0)	
Rx Frames Q1	0 (+0)	0 (+0)	0 (+0)	
Rx Frames Q2	0 (+0)	0 (+0)	0 (+0)	
Rx Frames Q3	2 (+0)	0 (+0)	0 (+0)	
Byte Error Ratio	3.533e-9	0	0	
Attributes	Value	Units		
Counter Page Refresh Period	3600	seconds		
Counter Measurement Period	01:25:58			
<input type="button" value="Submit Page Refresh Period"/>		<input type="button" value="Reset System Counters"/>		

Figure 249 Wireless Port Counters page (Slave, HCMP topology)

Wireless Port Counters					
Attributes	Value	Units	Attributes	Value	Units
Tx Frames	843 (+70)		Rx Frames	464 (+40)	
Tx Frames Q0	843 (+70)		Rx Frames With Error	0 (+0)	
Tx Frames Q1	0 (+0)		Rx Frames Q0	464 (+40)	
Tx Frames Q2	0 (+0)		Rx Frames Q1	0 (+0)	
Tx Frames Q3	0 (+0)		Rx Frames Q2	0 (+0)	
Tx Drops Q0	0 (+0)		Rx Frames Q3	0 (+0)	
Tx Drops Q1	0 (+0)				
Tx Drops Q2	0 (+0)				
Tx Drops Q3	0 (+0)				
Byte Error Ratio	0				
Attributes	Value	Units	Attributes	Value	Units
Counter Page Refresh Period	5	seconds	Counter Measurement Period	00:04:07	
<input type="button" value="Submit Page Refresh Period"/>			<input type="button" value="Reset System Counters"/>		

Procedure:

- Only on a device configured as in HCMP topology as a Master, select one interface using the Wireless Interface Selector. Note the Remote MAC Address indicates the MAC address of the unit currently connected, if any, to the selected wireless interface.
- Review the attributes ([Table 222](#)).
- 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 222 Wireless Port Counters attributes, HCMP mode

Attribute	Meaning
Tx/Rx Frames	Number of frames transmitted and received over the wireless link.
Rx Frames With Error	Number of received frames with errors.
Tx/Rx Frames Q0...Q3	Number of transmitted and received frames for each Traffic Class.
Tx Drops Q0...Q3	Number of frames discarded for each Traffic Class by taildrop.

Main Port Counters page (PTP topology only)

Menu option: **System > Statistics > Main Port Counters** ([Figure 250](#)). 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 250 Main Port Counters page (when main port is bridging traffic)

Main Port Counters					
Attributes	Value	Units	Attributes	Value	Units
Tx Octets	684,506 (+684,506)		Rx Octets	398,584 (+398,584)	
Tx Frames	6,177 (+2)		Rx Frames	6,044 (+2)	
Tx Drops	0 (+0)		Rx Frames With Crc Error	0 (+0)	
Tx Broadcasts	5,368 (+5,368)		Rx Broadcasts	5,554 (+5,554)	
Tx IEEE1588 Event Frames	0 (+0)		Rx IEEE1588 Event Frames	0 (+0)	
			Rx Frames Undersize	0 (+0)	
Tx Frames 64 Bytes	5,912 (+5,912)		Rx Frames 64 Bytes	5,968 (+5,968)	
Tx Frames 65 To 127 Bytes	41 (+41)		Rx Frames 65 To 127 Bytes	57 (+57)	
Tx Frames 128 To 255 Bytes	17 (+17)		Rx Frames 128 To 255 Bytes	2 (+2)	
Tx Frames 256 To 511 Bytes	6 (+6)		Rx Frames 256 To 511 Bytes	11 (+11)	
Tx Frames 512 To 1023 Bytes	4 (+4)		Rx Frames 512 To 1023 Bytes	2 (+2)	
Tx Frames 1024 To 1600 Bytes	197 (+197)		Rx Frames 1024 To 1600 Bytes	4 (+4)	
Tx Frames 1601 To Max Bytes	0 (+0)		Rx Frames 1601 To Max Bytes	0 (+0)	
			Rx Frames Oversize	0 (+0)	
			Rx Pause Frames	0 (+0)	
Attributes	Value	Units	Attributes	Value	Units
Counter Page Refresh Period	3600	seconds	Counter Measurement Period	00:08:09	
<input type="button" value="Submit Page Refresh Period"/>			<input type="button" value="Reset System Counters"/>		

Procedure:

- Review the attributes ([Table 223](#)).
- 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 223 Main Port Counters attributes

Attribute	Meaning
Tx/Rx Octets	Total number of octets (bytes) transmitted and received over the interface.
Tx/Rx Frames	Total number of frames transmitted and received over the interface. This includes both good and bad frames.
Tx Drops	Total number of transmit frames dropped.
Rx Frames With Crc Error	Total number of received frames with CRC errors.
Tx/Rx Broadcasts	Total number of good transmitted and received broadcast packets.
Tx/Rx IEEE1588 Event Frames	Only displayed when IEEE 1588 Transparent Clock is enabled.
Tx/Rx Frames TDM	Only displayed when TDM is enabled. Total number of transmitted or received TDM (E1 or T1) frames.
Rx Frames Undersize	Total number of frames received that are less than 64 bytes.
Tx/Rx Frames 64 Bytes	Total number 64 byte frames transmitted and received.
Tx/Rx Frames xxxx to yyyy Bytes	Total number of frames transmitted and received in the size range xxxx to yyyy bytes.
Tx/Rx Frames 1601 to Max bytes	Total number of frames transmitted and received in the size range 1601 to maximum bytes.
Rx Frames Oversize	Total number of frames received that are greater than the maximum number of bytes.
Rx Pause Frames	Total number of received pause frames.

Aux Port Counters page (PTP topology only)

Menu option: System > Statistics > **Aux Port Counters** (Figure 251).

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

Figure 251 Aux Port Counters page (when Aux port is allocated to the Local Management Service)

Aux Port Counters		
Attributes	Value	Units
Tx Frames	568 (+52)	
Tx Drops	0 (+0)	
Attributes	Value	Units
Rx Frames	3 (+0)	
Rx Frames With Crc Error	0 (+0)	
Rx Frames Undersize	0 (+0)	
Attributes	Value	Units
Counter Page Refresh Period	3600	seconds
<input type="button" value="Submit Page Refresh Period"/>		
		<input type="button" value="Reset System Counters"/>

Procedure:

- Review the attributes (Table 224).
- 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 224 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.
Tx Drops	Number of frames dropped due to excessive collision, late collision or frame ageing
Rx Frames Undersize	Number of short frames (<64 Bytes) with or without a valid CRC

SFP Port Counters page (PTP topology only)

Menu option: System > Statistics > **SFP Port Counters** (Figure 252).

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

Figure 252 SFP Port Counters page (when SFP port is allocated to the Local Management Service)

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
Submit Page Refresh Period		Reset System Counters

Procedure:

- Update the attributes ([Table 225](#)).
- 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 225 SFP Port Counters attributes

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

Ethernet Port Counters page (HCMP topology only)

Menu option: **System > Statistics > Ethernet Port Counters** (Figure 253). Use this page to check the performance of all Ethernet. The displayed counters vary depending on which port is being used to bridge the traffic.

Figure 253 Ethernet Port Counters page (HCMP topology)

Ethernet Port Counters					
Main Port Counters			Aux Port Counters		
Attributes	Value	Units	Attributes	Value	Units
Tx Octets	3,465,824 (+0)		Rx Octets	113,761 (+0)	
Tx Frames	2,638 (+0)		Rx Frames	1,464 (+0)	
Tx Broadcasts	0 (+0)		Rx Frames With Error	0 (+0)	
			Rx Broadcasts	0 (+0)	
			Rx Frames Undersize	0 (+0)	
			Rx Frames Oversize	0 (+0)	
SFP Port Counters					
Attributes	Value	Units	Attributes	Value	Units
Tx Octets	0 (+0)		Rx Octets	0 (+0)	
Tx Frames	0 (+0)		Rx Frames	0 (+0)	
Tx Broadcasts	0 (+0)		Rx Frames With Error	0 (+0)	
			Rx Broadcasts	0 (+0)	
			Rx Frames Undersize	0 (+0)	
			Rx Frames Oversize	0 (+0)	
Attributes			Attributes		
Counter Page Refresh Period			Counter Measurement Period		
Submit Page Refresh Period			Reset System Counters		

Procedure:

- Review the attributes (Table 226).
- 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 226 Ethernet Port Counters attributes (HCMP topology)

Attribute	Meaning
Tx/Rx Octets	Total number of octets (bytes) transmitted and received over the interface.
Tx/Rx Frames	Total number of frames transmitted and received over the interface. This includes both good and bad frames.

Attribute	Meaning
Rx Frames With Error	Total number of received frames with CRC errors.
Tx/Rx Broadcasts	Total number of good transmitted and received broadcast packets.
Rx Frames Undersize	Total number of frames received that are less than 64 bytes.
Rx Frames Oversize	Total number of frames received that are greater than the maximum number of bytes.

Management Counters page (HCMP topology only)

Menu option: **System > Statistics > Management Counters** (Figure 254). Use this page to check the performance of all Ethernet. The displayed counters vary depending on which port is being used to bridge the traffic.

Figure 254 Management Counters page (HCMP topology)

Management Counters					
Attributes	Value	Units	Attributes	Value	Units
Tx Frames Management	15,350 (+27)		Rx Frames Management	8,505 (+24)	
Tx Drops Management	0 (+0)				
Attributes	Value	Units	Attributes	Value	Units
Counter Page Refresh Period	5	seconds	Counter Measurement Period	01:53:57	
<input type="button" value="Submit Page Refresh Period"/>			<input type="button" value="Reset System Counters"/>		

Procedure:

- Review the attributes (Table 227).
- 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 227 Management Counters attributes (HCMP topology)

Attribute	Meaning
Tx Frames Management	Total number of frames transmitted over the management interface.
Tx Drops Management	Total number of transmit frames dropped over the management interface.
Rx Frames Management	Total number of frames received over the management interface.

SyncE Status page

Menu option: System > Statistics > **SyncE Status**

Use this page to monitor the state of the Synchronous Ethernet function.



Note

When TDM is enabled ([TDM Configuration page](#) on page 6-62), the following restrictions are automatically applied:

- The SyncE Status page is hidden.
- Main PSU Port Sync E Master Slave Status is set to **Master**.
- Main PSU Port Gigabit Master Slave Status is set to **Master**.

Figure 255 SyncE Status page

SyncE Status					
Attributes	Value	Units	Attributes	Value	Units
Sync E Tracking State	Locked Local, Holdover Acquired				
Main PSU Port					
Main PSU Port Accepted QL Rx	QL-PRC		Main PSU Port Sync E Rx Status	Good	
Main PSU Port QL Rx	QL-PRC		Main PSU Port Sync E Master Slave Status	Slave	
Main PSU Port QL Tx	QL-DNU / QL-DUS		Main PSU Port Gigabit Master Slave Status	Slave	
Aux Port					
Aux Port QL Rx	None		Aux Port Sync E Master Slave Status	Master	
Aux Port QL Tx	QL-PRC		Aux Port Gigabit Master Slave Status	Not Applicable	
SFP Port					
SFP Port QL Rx	None		SFP Port Sync E Master Slave Status	Master	
SFP Port QL Tx	None		SFP Port Gigabit Master Slave Status	Slave	
Page Refresh Period	3	Seconds	Submit Page Refresh Period		

Procedure:

- Review the attributes
- To change the refresh period, update the Page Refresh Period attribute and click **Submit Page Refresh Period**

Table 228 Sync E Status attributes

Attribute	Meaning
Sync E Tracking State	The state of the Synchronous Ethernet state machine. See Table 229 for further details.
Main PSU Port Accepted QL Rx	<p>The “accepted” QL received by the Main PSU Port. This should be the same as Main PSU Port QL Rx, unless:</p> <ul style="list-style-type: none"> • an “Overwrite” has been configured • the system is starting up or recovering from an exception <p>The ODU synchronizes to the best frequency reference as determined by the Port Accepted QL Rx values at the nominated Sync E Slave Ports of local and remote ODUs.</p>
Main PSU Port QL Rx	The QL currently being received at the Main PSU Port
Main PSU Port QL Tx	The QL currently being transmitted at the Main PSU Port
Main PSU Port SyncE Rx Status	The overall status of the incoming synchronous Ethernet signal on the Main PSU port. This port is available as a valid synchronization source if the status is Good . The port may potentially be a valid source in the near future if the status is Wait-to-Restore .
Main PSU Port Sync E Master Slave Status	This attribute indicates if the Main PSU Port is operating as a Synchronous Ethernet master (providing a source of timing for downstream devices) or slave (receiving a source of timing from an upstream device).
Main PSU Port Gigabit Master Slave Status	This attribute indicates if the Main PSU Port’s Gigabit Ethernet physical interface is operating as a master (generating a clock) or slave (locking to a clock generated at the other end of the Ethernet link).
Aux Port QL Rx	The QL currently being received on the Aux Port
Aux Port Accepted QL Rx	The “accepted” QL received by the Aux Port. This should be the same as Aux Port QL Rx, unless the system is starting up or recovering from an exception
Aux Port QL Tx	The QL currently being transmitted at the Aux Port
Aux Port Sync E Master Slave Status	The Aux Port operates as a Synchronous Ethernet master (providing a source of timing for downstream devices).
Aux Port Gigabit Master Slave Status	This attribute indicates if the Aux Port’s Gigabit Ethernet physical interface is operating as a master (generating a clock) or slave (locking to a clock generated at the other end of the Ethernet link).
SFP Port QL Rx	The QL currently being received on the SFP Port

Attribute	Meaning
SFP Port Accepted QL Rx	<p>The “accepted” QL received by the SFP Port. This should be the same as SFP Port QL Rx, unless:</p> <ul style="list-style-type: none"> • an “Overwrite” has been configured • the system is starting up or recovering from an exception <p>The ODU synchronizes to the best frequency reference as determined by the Port Accepted QL Rx values at the nominated Sync E Slave Ports of local and remote ODUs.</p>
SFP Port QL Tx	The QL currently being transmitted at the SFP Port
SFP Port Sync E Master Slave Status	This attribute indicates if the SFP Port is operating as a Synchronous Ethernet master (providing a source of timing for downstream devices) or slave (receiving a source of timing from an upstream device).
SFP Port Gigabit Master Slave Status	<p>This attribute indicates if the SFP Port’s Gigabit Ethernet physical interface is operating as a master (generating a clock) or slave (locking to a clock generated at the other end of the Ethernet link).</p> <p>The Master Slave Status is Not Applicable unless a Copper SFP module is present.</p>

The “Sync E Tracking State” attribute can take the following values:

Table 229 Sync E Tracking State

Value	Meaning
Disabled	The synchronous Ethernet feature is disabled.
Acquiring Wireless Lock	Synchronous Ethernet is not operational because real-time clocks have not completed alignment.
Free Running	Synchronous Ethernet is operational, but with no timing source or history. This is a temporary state.
Locked Local, Acquiring Holdover	Sync E tracking has locked to a synchronisation signal from a cabled Ethernet port on the local ODU. This is a temporary state until the unit has acquired holdover history.
Locked Local, Holdover Acquired	Sync E tracking has locked to a synchronisation signal from a cabled Ethernet port on the local ODU and has acquired holdover history.
Holdover	There is currently no source for the tracking loop, but previously the tracking loop was in a Locked, Holdover Acquired state. The system is using the last known good frequency.
Locked Remote, Acquiring Holdover	The tracking loop has locked to a synchronisation signal from the remote ODU. This is a temporary state until the unit has acquired holdover history.

Value	Meaning
Locked Remote, Holdover	The tracking loop has locked to a synchronisation signal
Acquired	form the remote ODU and has acquired holdover history.

In normal operation, with the Synchronous Ethernet feature enabled and a valid timing source present, one end of the link should be in the “Locked Local, Holdover Acquired State”, the other end should be in the “Locked Remote, Holdover Acquired” state.

The Sync E Tracking State attribute remains in the Acquiring Wireless Lock state for a period of time after the wireless link has established whilst the two ODUs establish precise synchronization. The duration of this period depends on channel bandwidth, varying from less than one minute at 45 MHz, up to two minutes for 5 MHz.

Diagnostics Plotter page

Menu option: **System > Diagnostics Plotter** ([Figure 256](#)).

Use this page to monitor the performance of an operational PTP 670 link over time.

Figure 256 Diagnostic Plotter page (PTP topology)

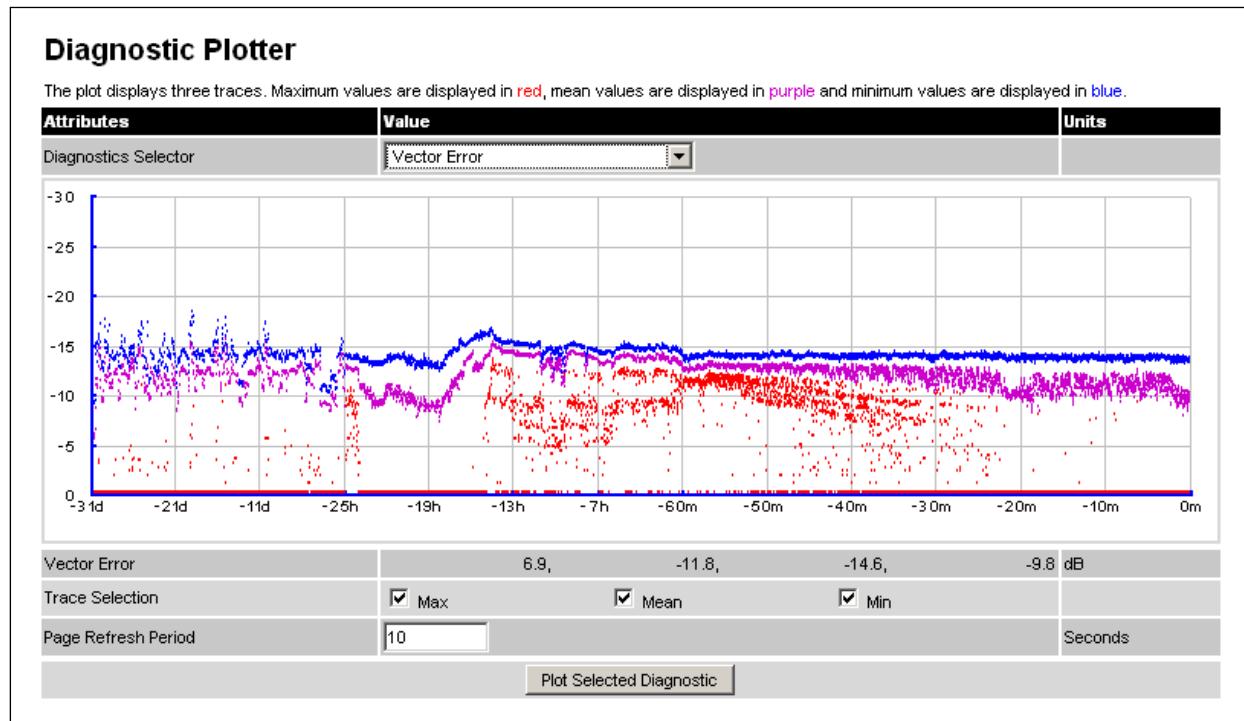
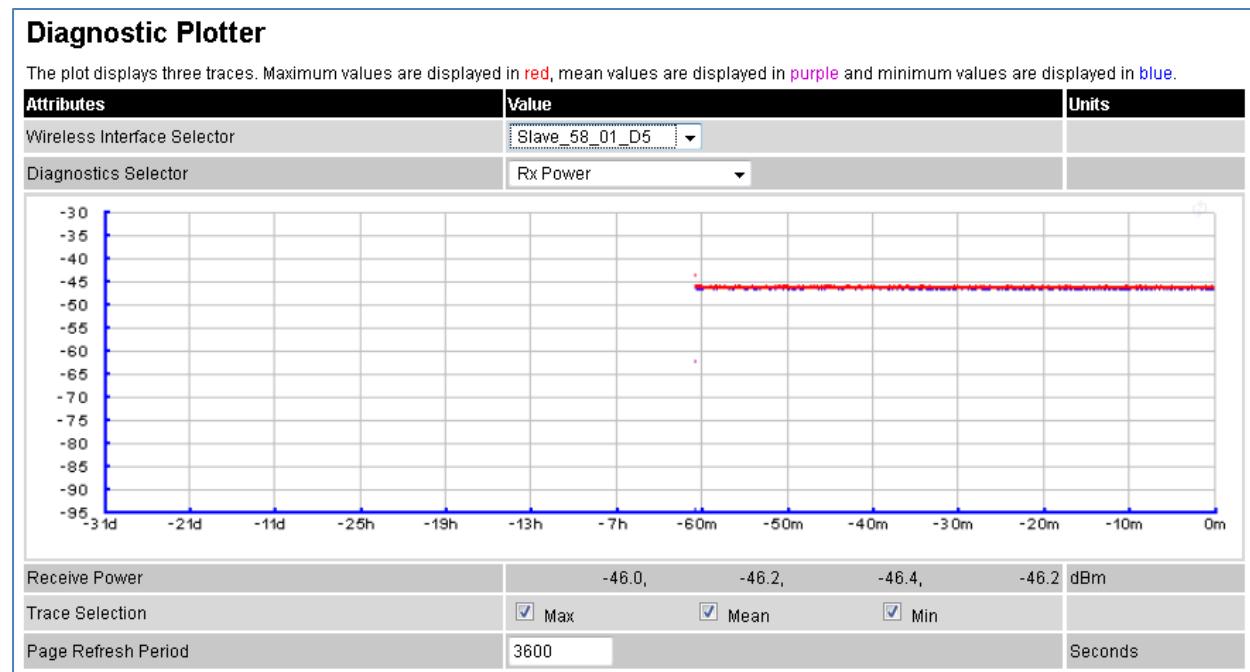


Figure 257 Diagnostic Plotter page (HCMP topology)**Procedure:**

- Only on a device configured as in HCMP topology as a Master, set the Wireless Interface Selector to the Wireless Interface the diagnostic data needs to be displayed for. Note the Remote MAC Address indicated the MAC address of the unit currently connected, if any, to the selected wireless interface.
- Select a diagnostic from the Diagnostics Selector drop-down list. The diagnostics are described in [Table 230](#).
- Tick the required Trace Selection boxes: Max, Mean and Min.
- Update the Page Refresh Period as required. The default period is 3600 seconds (1 hour). To monitor the performance of a link in real time, select a much shorter period, for example 60 seconds.
- Click **Plot Selected Diagnostic**. The selected diagnostic trace is displayed in the graph. Maximum values are displayed in red, mean values are displayed in purple and minimum values are displayed in blue.

Table 230 Diagnostic Plotter attributes

Attribute	Meaning
Vector Error	The vector error measurement compares the received signal IQ modulation characteristics to an ideal signal to determine the composite vector error magnitude.
Tx Power	The transmitter power.
Rx Power	The receive signal strength.

Attribute	Meaning
Signal Strength Ratio	<p>The Signal Strength Ratio is:</p> <p>Power received by the vertical antenna input (dB) – Power received by the horizontal antenna input (dB)</p> <p>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:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
Link Loss	<p>Link loss calculated as follows:</p> $\text{Peer_Tx_Power (dBm)} - \text{Local_Rx_Power (dBm)} + 2 \times \text{Antenna_Pattern (dBi)}$
Tx, Rx, and Aggregate Data Rates	The data rates in the transmit direction, the receive direction and in both directions, expressed in Mbps.
PCB Temperature	The temperature in degrees Celsius measured by a sensor on the printed circuit board of the ODU. The PCB temperature will normally be higher than the ambient temperature.
Tx Link Capacity Utilization	The Tx Link Capacity Utilization measures the percentage of the instantaneous transmit capacity actually used to carry traffic. Note that this percentage is relative to the instantaneous capacity of the link in the transmit direction and that this capacity is dependent over time of the modulation the link operates in.

Generate Downloadable Diagnostics page

Menu option: **System > Diagnostics Plotter > CSV Download** ([Figure 258](#)).

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

Figure 258 Generate Downloadable Diagnostics page

Generate Downloadable Diagnostics

Attributes	Value
Diagnostics Selector	Vector Error <input style="width: 150px;" type="button" value="▼"/>
<input style="width: 200px; height: 30px;" type="button" value="Generate Diagnostics"/>	

Procedure:

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

Recovery mode

This section describes how to recover a PTP 670 unit from configuration errors or software image corruption.

Entering recovery mode

Use this procedure to enter recovery mode manually.

**Note**

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

**Note**

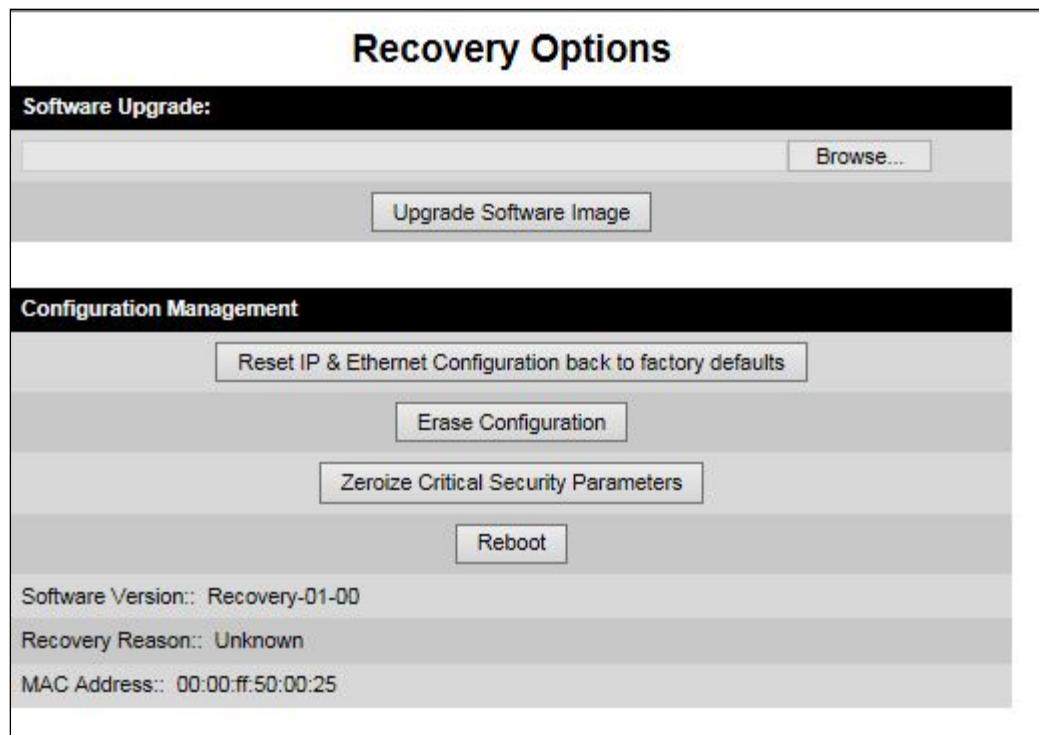
Once the unit has entered recovery, it will switch back to normal operation if no access has been made to the recovery web page within 30 seconds.

Procedure:

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



- 5 Click on the warning page image. The Recovery Option Page is displayed ([Figure 259](#)).
- 6 Review the Software Version and Recovery Reason ([Table 231](#)).
- 7 Select a recovery option ([Table 232](#)).

Figure 259 Recovery Options page**Table 231** 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 232 Recovery Options buttons

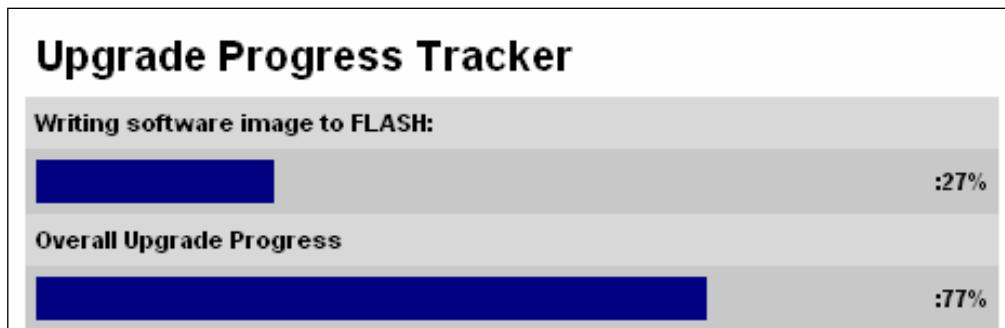
Button	Purpose
Upgrade Software Image	Use this option to restore a working software version when software corruption is suspected, or when an incorrect software image has been loaded. Refer to Upgrading software image on page 7-79.
Reset IP & Ethernet Configuration back to factory defaults	Use this option to reset the IP and Ethernet attributes to factory defaults. Refer to Resetting IP & Ethernet configuration on page 7-80.
Erase Configuration	Use this option to reset the entire configuration of the unit to factory defaults. Refer to Resetting all configuration data on page 7-82.
Zeroize Critical Security Parameters	Use this option to reset the security configuration to default values. Refer to Zeroize Critical Security Parameters on page 7-83.
Reboot	Use this option to reboot the unit. Refer to Rebooting the unit on page 7-84.

Upgrading software image

Use this option to restore a working software image from the Recovery Options page ([Figure 259](#)).

Procedure:

- 1 Click **Browse**.
- 2 Navigate to the required software image. This may be the most recent image if software corruption is suspected, or an older image if an incorrect image has just been loaded. Click on the image and click **Open**.
- 3 Click **Upgrade Software Image**. The Confirmation page is displayed. Click **Program Software Image into Non-Volatile Memory**. The Upgrade Progress Tracker page is displayed:



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



- 5 Click **Reboot Wireless Unit**. When the “**Are you sure?**” message is displayed, click **OK**.
- 6 The unit will now reboot and restart in normal operational mode, and the link should recover. If the unit or link fails to recover, refer to [Testing link end hardware](#) on page [8-7](#).

Resetting IP & Ethernet configuration

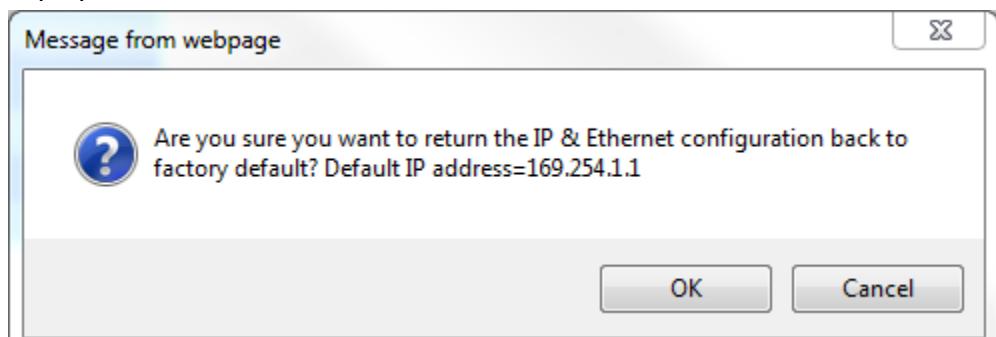
Use this option in the Recovery Options page to reset IPv4, IPv6 and Ethernet configuration to default values ([Figure 259](#)). This procedure resets the IP Version attribute to **IPv4**. It also resets the IPv6 configuration. The reset action affects the following attributes:

- IP Version
- IPv4 Address
- Subnet Mask
- Gateway IP Address
- use VLAN For Management Interfaces
- VLAN Management VID
- VLAN Management Priority
- IPv6 Address
- IPv6 Prefix Length
- IPv6 Gateway Address
- Data Service
- Second Data Service
- Management Service
- Local Management Service
- Data Port Wireless Down Alert
- Management Port Wireless Down Alert
- Main PSU Port Auto Negotiation
- Main PSU Port Auto Neg Advertisement
- Main PSU Port Auto Mdix
- Aux Port Auto Negotiation
- Aux Port Auto Neg Advertisement
- Aux Port Auto Mdix
- Aux Port Power Over Ethernet Output
- SFP Port Auto Negotiation

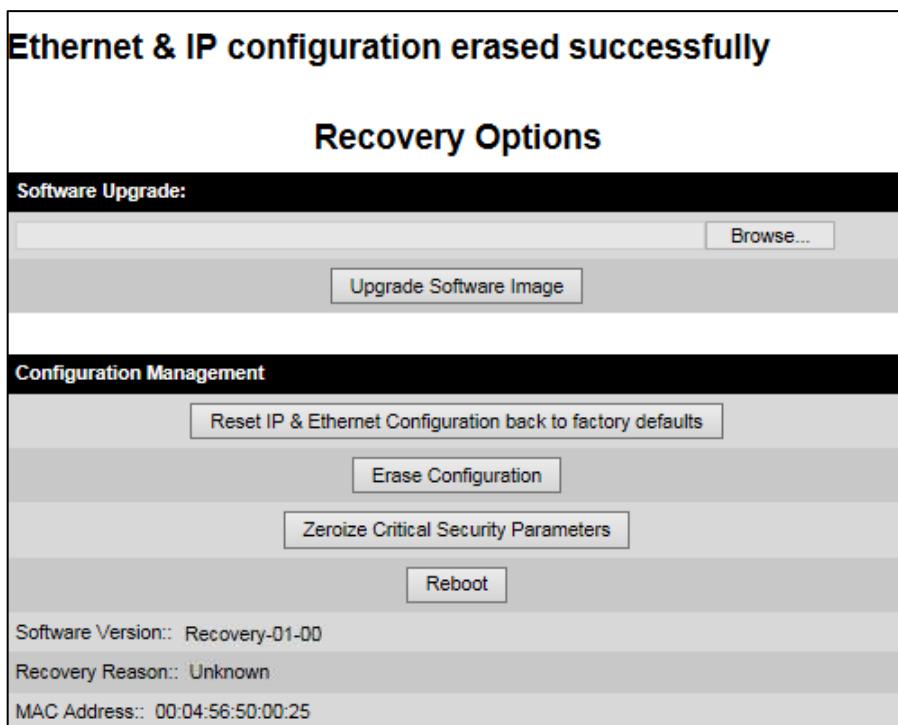
- SFP Port Auto Neg Advertisement
- SFP Port Auto Mdix
- Local Packet Filtering
- NIDU Lan Port Auto Negotiation
- NIDU Lan Port Auto Neg Advertisement
- NIDU Lan Port Auto Mdix
- SNMP Access Control
- Access Control
- IP Address Label

Procedure:

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



- 2 Record the IP address, as it will be needed to log into the unit after recovery.
- 3 Click **OK**. The reset confirmation page is displayed:



- 4 Click **Reboot**. When the “Are you sure you want to REBOOT this unit?” message is displayed, click **OK**.
- 5 The unit will now reboot. The unit should now start up in normal mode but with the IP and Ethernet configuration reset to factory defaults. If the unit fails to recover, refer to [Testing link end hardware](#) on page 8-7 and [Cable Diagnostics](#) on page 8-2.

Resetting all configuration data



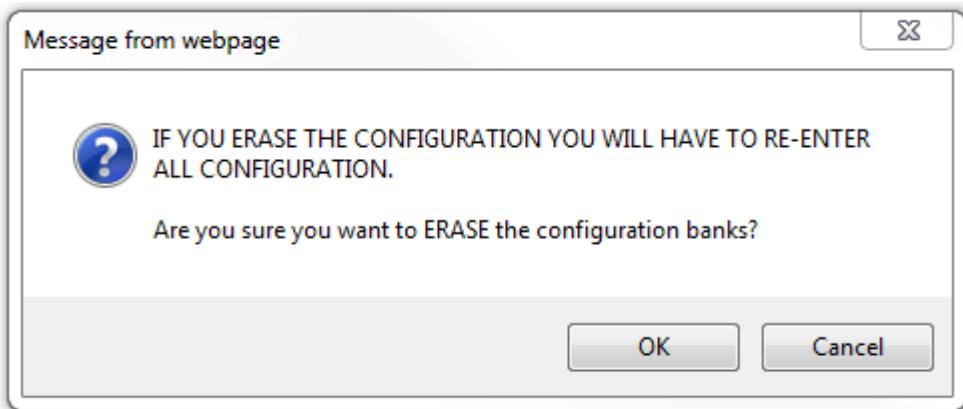
Note

Wireless Topology is not reset by this procedure.

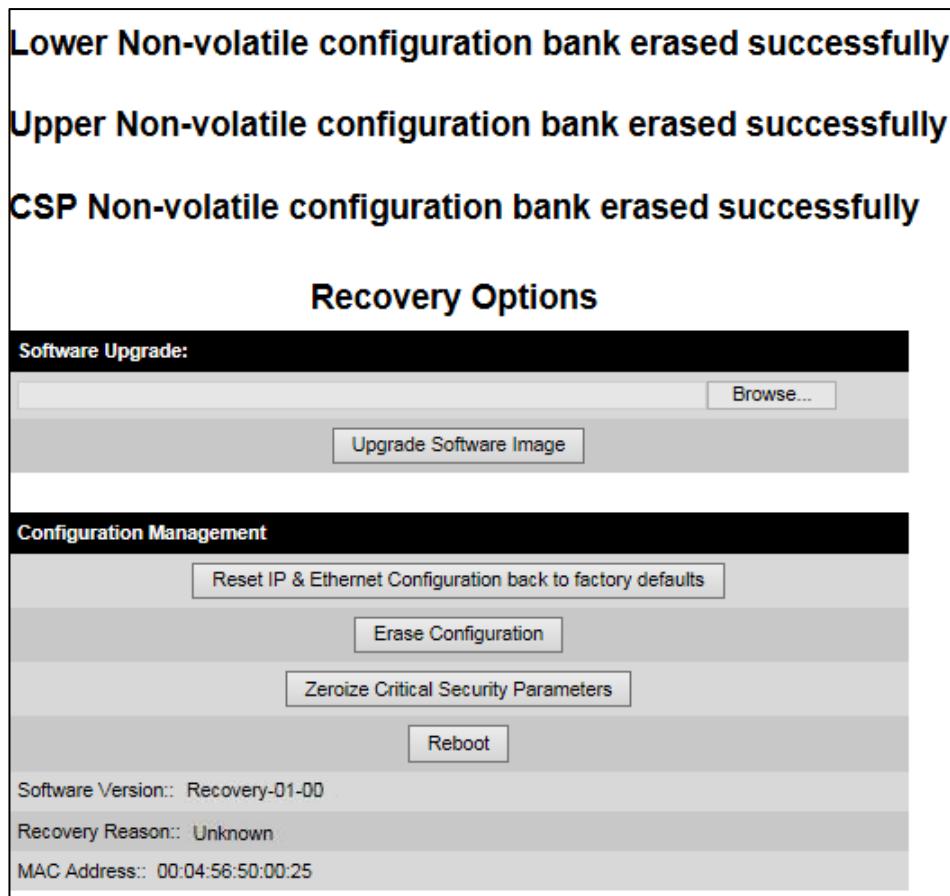
Use this option in the Recovery Options page to reset the entire configuration of the unit (including IP, Ethernet and CSPs) to default values ([Figure 259](#)).

Procedure:

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



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



- 3 Click **Reboot**. When the confirmation message is displayed, click **OK**.
- 4 The unit reboots and starts up in normal mode but with all configuration reset to default values. If the unit fails to start up, refer to [Testing link end hardware](#) on page [8-7](#) and [Cable Diagnostics](#) on page [8-2](#).

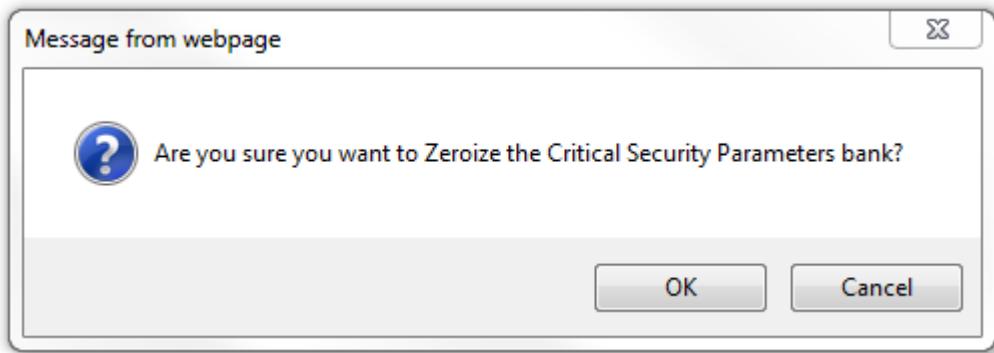
Zeroize Critical Security Parameters

Use this option in the Recovery Options page to reset the security configuration of the unit to default values ([Figure 259](#)). This action includes the following attributes:

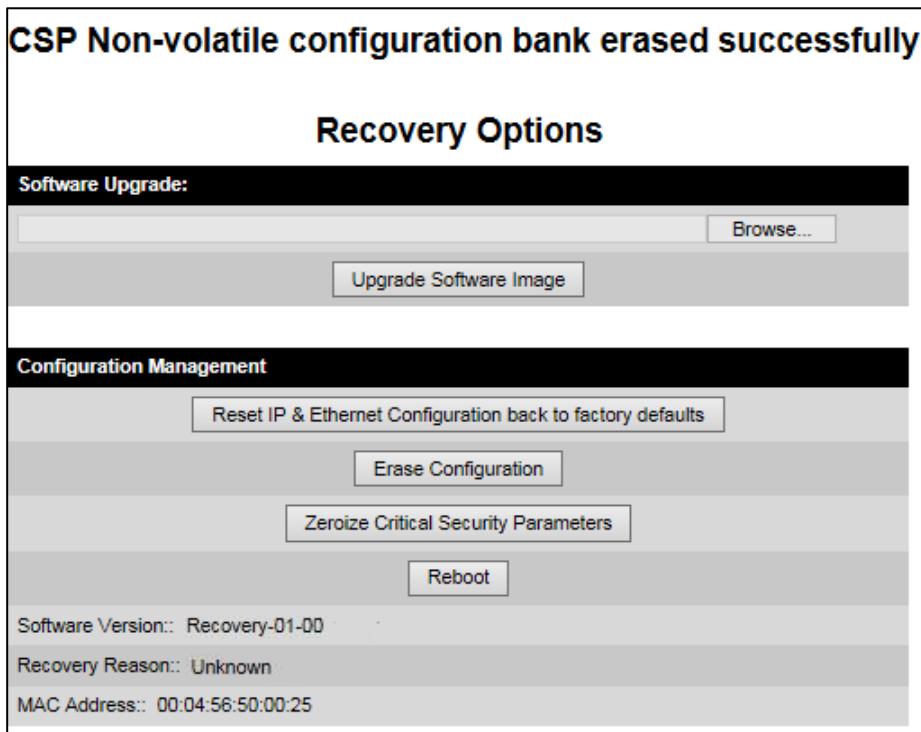
- Key of Keys
- Local User Accounts Names, Roles and Passwords
- Encryption Algorithm
- Wireless Encryption Key
- HTTPS Private Key
- HTTPS Public Key Certificate
- Random Number Generator Entropy
- HTTP Access Enabled
- HTTP Port Number

Procedure:

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



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



- 3 Click **Reboot**. When the "Are you sure you want to REBOOT this unit?" message is displayed, click **OK**.
- 4 The unit will now reboot. The unit should now start up in normal mode but with the security configuration reset to default values. If the unit fails to recover, refer to [Testing link end hardware](#) on page 8-7 and [Cable Diagnostics](#) on page 8-2.

Rebooting the unit

Use this option to reboot the unit from the Recovery Options page ([Figure 259](#)).

Procedure:

- Click **Reboot**.

- When the “Are you sure you want to REBOOT this unit?” message is displayed, click **OK**. The unit will now reboot. The unit should now start up in normal operational mode. If the unit fails to start up, refer to [Testing link end hardware](#) on page 8-7.

Chapter 8: Troubleshooting

This chapter contains procedures for identifying and correcting faults in a PTP 670 link. These procedures can be performed either on a newly installed link, or on an operational link if communication is lost, or after a lightning strike.

The following topics are described in this chapter:

- [Cable Diagnostics](#) on page 8-2 describes how to perform cable diagnostics test to detect cabling related faults.
- [Testing link end hardware](#) on page 8-7 describes how to test the link end hardware, either when it fails on startup, or after a lightning strike.
- [Testing the radio link](#) on page 8-13 describes how to test the link when there is no radio communication, or when it is unreliable, or when the data throughput rate is too low.
- [Testing PTP-SYNC](#) on page 8-15 describes how to test the PTP-SYNC unit and its connections when the PTP-SYNC LEDs do not illuminate correctly, or when a synchronization fault is suspected.
- [Testing a TDM link](#) on page 8-18 describes how to check the NIDU LEDs and how to perform a TDM loopback test.

Cable Diagnostics

This section describes how to diagnose cable faults.

The Cable Diagnostics feature may be used to test Ethernet cables connected to the Main PSU port and the Aux port. The feature uses Time Domain Reflectometry (TDR) technology to test individual twisted pairs in the cable, to identify open circuit and short circuit faults, and indicate the approximate location of the fault:

- Open circuit – An open circuit is detected when the impedance is greater than 300 ohms.
- Short circuit – A short circuit is detected when the impedance is less than 33 ohms.
- Approximate location of the fault - The fault location is reported as a distance from the ODU along the cable, and is accurate to +/- 2 meters (6.5 feet).



Note

- The cable diagnostics results are provided only as a guide.
- The feature reliably detects all open circuit and short circuit faults in cable pairs, but it is not possible to reliably detect short circuit faults between wires in different cable pairs. Except for that specific circumstance, an OK result for all pairs means the cable is good.
- The presence of LPUs can affect the accuracy and reliability of the results.

Before initiating the test, confirm that all outdoor drop cables (that is those that connect the ODU to equipment inside the building) are specified as supported, as defined in [Outdoor copper Cat5e Ethernet cable](#) on page [2-31](#).

Test scenarios

The Cable Diagnostics test may be performed in following scenarios:

Scenarios	Actions
Main PSU port "Down"	<p>Check for physical Ethernet cable connectivity between Power over Ethernet (PoE) and Customer Data Network (or LAN).</p> <p>If the cable connectivity is OK, Perform Cable Diagnostics test.</p>
Aux port "Down"	<p>Check for physical Ethernet cable connectivity between ODU and Customer Data Network or Management Agent.</p> <p>If the cable connectivity is OK, Perform Cable Diagnostics test.</p>
Main PSU or Aux port is "Up" but the Ethernet speed is noticed slow	<p>There is a possibility that one or more cable pairs have intermittent contact with the RJ45 connector pin. This could result in intermittent communication errors.</p> <p>Follow procedure Ethernet packet test.</p> <p>If Ethernet Rx Crc and Align counter is greater than ten (>10), Perform Cable Diagnostics test.</p>

Scenarios	Actions
	If Packet Error Rate is greater than 1 in 1 million, Perform Cable Diagnostics test .
	If Number of lost packets are less than two (<2) after performing Test ping packet loss , perform Cable Diagnostics test .
	Otherwise check the ODU's parameter configurations.

Cable Diagnostics test

Menu option: **System > Cable Diagnostics**

The Cable Diagnostics feature determines a fault in a cable and its approximate location based on Time Domain Reflectometry (TDR).

When the test is initiated for the selected port(s), the ODU sends a known signal (+1V) over the twisted pair cable. The transmitted signal will travel down the cable until it reflects off a fault. The magnitude of the reflection and the time it takes for the reflection to come back can be used to calculate the distance to the fault on the cable. For example, a +1V reflection will indicate an open close to the PHY and a -1V reflection will indicate a short close to the PHY.

Based on the returned signal, the radio identifies the cable status and estimates the distance of the fault. The result of the cable test will be displayed.

The cable diagnostics test can be carried out for Main PSU and AUX ports. This test is not supported for SFP port.



Caution

- On the Main PSU port, the presence of LPUs can affect the accuracy of the cable diagnostics results for some cable configurations. When a fault is detected, the feature reports the distance corresponding to the final TDR signal reflection. In configurations where there is a short cable from the ODU to the first LPU (< 2m), and a moderately long cable to the second LPU (30m), the final TDR signal reflection may come from one of the LPUs itself, rather than the fault. For example, a fault in the first short cable may be reported at or near the second LPU.
- On the Aux port, the presence of LPUs can affect the reliability of the cable diagnostics results for many cable configurations. Frequently, open circuit faults may be reported when the cable is OK, and fault distances may be reported corresponding to the LPU locations. Cable diagnostics tests on the Aux port should be repeated a number of times to establish a pattern.



Note

All cable diagnostics results should be verified with an external cable tester before remedial action is taken.

All four twisted pairs of the cable are tested separately and results are displayed for each pair.

The pin to pair mapping of a cable is shown in [Table 233](#).

Table 233 Pin to pair mapping of a cable (T568B termination)

Pin	Pair	Wire	Color (Supplied cable)	Color (Conventional)	Pins on plug face
1	2	1	Light Orange	White/Orange	
2	2	2	Orange	Orange	
3	3	1	Light Green	White/Green	
4	1	2	Blue	Blue	
5	1	1	Light Blue	White/Blue	
6	3	2	Green	Green	
7	4	1	Light Brown	White/Brown	
8	4	2	Brown	Brown	

Procedure

- 1 Select ports for cable diagnostics test:

Cable Diagnostics

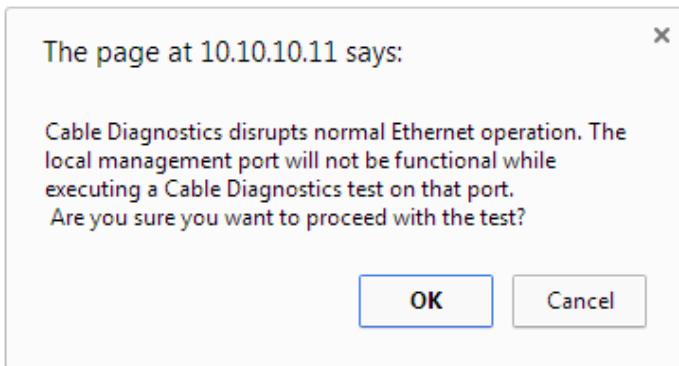
This feature uses Time Domain Reflectometry (TDR) technology to identify open circuit and short circuit faults in individual twisted pairs of Ethernet cables connected to the Main PSU port and the Aux port, and indicate the approximate distance to the fault

Attributes	Value	Units
Cable Diagnostics Ports	<input checked="" type="checkbox"/> Main PSU Port <input type="checkbox"/> Aux Port	
Start Test		

- 2 Click "Start Test" button to begin the test:

Start Test

- 3 The confirmation pop up box is displayed. Click the "OK" button to proceed with the test:



**Note**

The Local Management port connection will be lost when the local management port is under test. However the management port will be accessible when the other ports are under test.

4 On completion of the test, the web page is refreshed automatically, and the results are displayed:

Cable Diagnostics Results

The cable diagnostics results are provided only as a guide. The presence of LPUs can affect the accuracy and reliability of the results (see the User Guide for more details).

 All cable diagnostics results should be verified with an external cable tester before remedial action is taken.

Main PSU Port

Attributes	Value	Units
Last Test Time	01-Jan-1970 00:06:53	
Cable Pair	Results	Distance to Fault
Pair 1	Short Circuit	6
Pair 2	OK	
Pair 3	OK	
Pair 4	Short Circuit	6
		meters

Aux Port

Attributes	Value	Units
Last Test Time		
Cable Pair	Results	Distance to Fault
Pair 1	Not Tested	
Pair 2	Not Tested	
Pair 3	Not Tested	
Pair 4	Not Tested	

**Note**

The last test performed results are shown for user reference purpose.

Table 234 Cable Diagnostics attributes

Attribute	Meaning
Cable Diagnostics Ports	Select ports on which Cable Diagnostics must be executed.
Last Test Time	The date and time when a Cable Diagnostics test was last executed successfully.
Cable Pair	The result of the most recent execution of cable diagnostics on a cable pair.

Attribute	Meaning
	There are four twisted pairs in each Cat5 cable. The cable diagnostics test is performed on each pair of the cable.
Results	OK: Reported when the test is passed for a respective cable pair. Open Circuit: Reported when the impedance is greater than 330 ohms. Short Circuit: Reported when impedance is less than 33 ohms.
Distance	The estimate of the distance from the ODU to the fault detected on the cable pair during the most recent execution of Cable Diagnostics. Fault in cables longer than 160 meters (525 feet) may not be detected. The error margin is +/- 2 meters (6.5 feet).
Units	Unit of cable length in meters.

Testing link end hardware

This section describes how to test the link end hardware when it fails on startup or during operation.

Before testing link end hardware, confirm that all outdoor drop cables, that is those that connect the ODU to equipment inside the building, are of the supported type, as defined in [Outdoor copper Cat5e Ethernet cable on page 2-31](#).

AC Power Injector 56V LED sequence

When the AC Power Injector 56V 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 5-21](#).

AC+DC Enhanced Power Injector 56V LED sequence

For the AC+DC Enhanced Power Injector 56V, the expected power-up LED sequence is:

- The Power (green) LED illuminates steadily.
- After about 45 seconds, the Ethernet (yellow) LED blinks slowly 10 times.
- The Ethernet (yellow) LED illuminates steadily, then blinks randomly to show Ethernet activity.

If this sequence does not occur, take appropriate action depending on the LED states:

- [Power LED is off on page 8-7](#)
- [Power LED is blinking on page 8-8](#)
- [Ethernet LED did not blink 10 times on page 8-8](#)
- [Ethernet LED blinks ten times then stays off on page 8-9](#)
- [Ethernet LED blinks irregularly on page 8-9](#) (for example a short blink followed by a long blink)
- [Power LED is on, Ethernet LED blinks randomly on page 8-9](#)

If a fault is suspected in the ODU-PSU drop cable, perform [Test resistance in the drop cable on page 5-21](#).

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 5-21.

Power LED is blinking

Meaning: The PSU is sensing there is an overload on the ODU port; this could be caused by a wiring error on the drop cable or a faulty ODU.

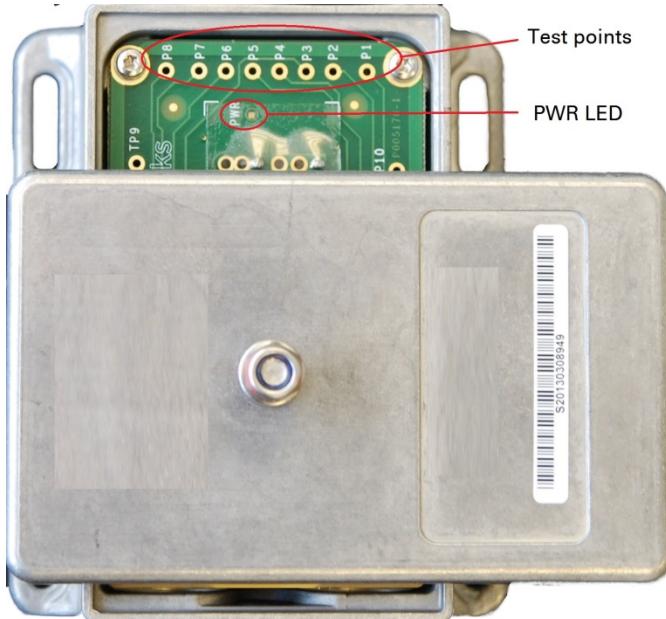
Action: Remove the ODU cable from the PSU. Check that pins 4&5 and 7&8 are not crossed with pins 1&2 and 3&6. Check that the resistance between pins 1&8 is greater than 100K ohms. If either check fails, replace or repair the ODU cable.

Ethernet LED did not blink 10 times

Meaning: The ODU flashes the LED on the AC+DC Enhanced Power Injector 56V 10 times to show that the ODU is powered and booted correctly.

Action:

- 1 Remove the ODU cable from the PSU. Examine it for signs of damage. Check that the ODU cable resistances are correct, as specified in [Test resistance in the drop cable](#) on page 5-21. If the ODU cable is suspect, replace it.
- 2 Use the LPU (if installed) to check that power is available on the cable to the ODU. Access the connections by rotating the LPU lid as shown (slacken the lid nut but do not remove it):



- 4 Check that test point P1 on the LPU PCB corresponds to pin 1 on the RJ45. Repeat for points P2 to P8. This test is only valid if both the PSU and the ODU are disconnected.
- 5 Reconnect the ODU cable to the PSU.
- 6 Check that the PWR LED near the top right of the LPU PCB is illuminated to indicate power in the Ethernet cable.
- 7 If any test fails, replace or repair the cable that connects the PSU to the LPU or ODU.

Ethernet LED blinks ten times then stays off

Meaning: There is no Ethernet traffic between the PSU and ODU.

Action: The fault may be in the LAN or ODU cable:

- Confirm that Ethernet traffic is connected to the AC+DC injector LAN port, confirm the cable is not faulty, replace if necessary.
- If the LAN connection to the AC+DC Power Injector 56V is working, check the drop cable is correctly wired using a suitable cable tester. Repeat the drop cable tests on page [Test resistance in the drop cable](#) on page 5-21.

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 7-77.

Power LED is on, Ethernet LED blinks randomly

Meaning: Both LEDs are in their normal states, implying that the PSU is receiving power from the AC/DC outlet and there is normal Ethernet traffic between the PSU and ODU.

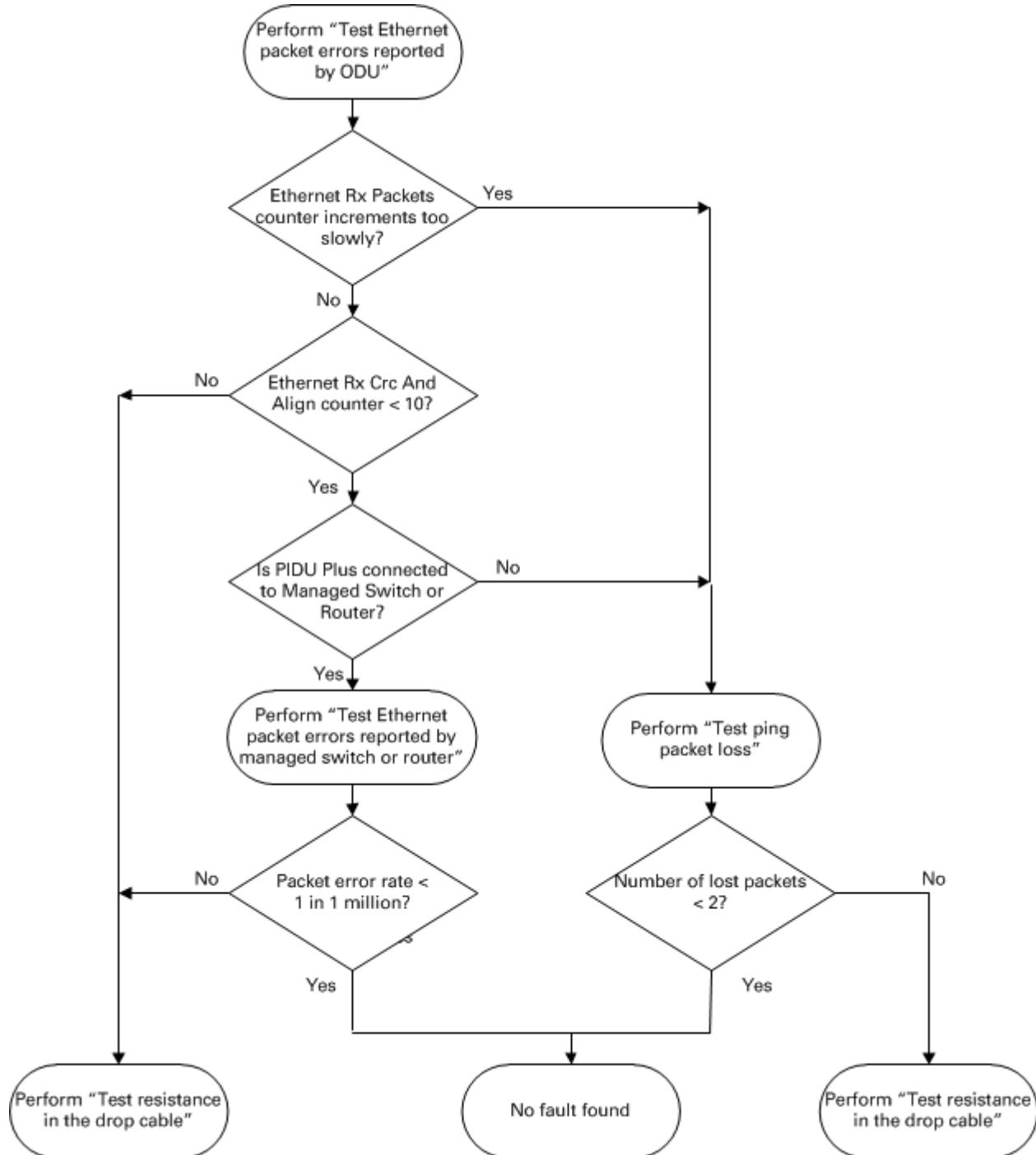
Action: If, in spite of this, a fault is suspected in the link end hardware:

- If the Ethernet connection to the network is only 100BASE-TX, when 1000BASE-T is expected: remove the ODU cable from the PSU, examine it, and check that the wiring to pins 4&5 and 7&8 is correct and not crossed.
- Perform [Ethernet packet test](#) on page 8-10.

Ethernet packet test

Follow the Ethernet packet test flowchart (Figure 260) and procedures below.

Figure 260 Ethernet packet test flowchart



Test Ethernet packet errors reported by ODU

Log into the unit and click **Administration**, **Statistics**, **Detailed Counters**. Click **Reset System Counters** at the bottom of the page and wait until the Ethernet Rx Packets counter has reached 1 million (the count will only update when the page is refreshed. If the counter does not increment or increments too slowly, because for example the PTP 670 is newly installed and there is no offered Ethernet traffic, then abandon this procedure and consider using the procedure [Test ping packet loss](#) on page 8-11).

Read the Ethernet Rx Crc And Align counter. The test has passed if this is less than 10.

Test Ethernet packet errors reported by managed switch or router

If the ODU is connected to a managed Ethernet switch or router, it may be possible to monitor the error rate of Ethernet packets. Please refer to the user guide of the managed network equipment. The test has passed if the rate of packet errors reported by the managed Ethernet switch or router is less than 10 in 1 million packets.

Test ping packet loss

Using a computer, it is possible to generate and monitor packets lost between the PSU and the ODU. This can be achieved by executing the Command Prompt application which is supplied as standard with Windows and MAC operating systems.



Caution

This procedure disrupt network traffic carried by the PTP 670 under test:

Procedure:

- 1 Ensure that the IP address of the computer is configured appropriately for connection to the PTP 670 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 670 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 670 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 670 unit is interfering with radio or television reception (this can be determined by turning the equipment off and on), attempt the following corrective actions:

- Realign or relocate the antenna.
- Increase the separation between the affected equipment and antenna.
- Connect the ODU and PSU power supply into a power outlet on a circuit different from that to which the receiver is connected.
- Contact Cambium Point-to-Point for assistance.

Testing PTP-SYNC

This section describes how to test the PTP-SYNC unit and its connections when the PTP-SYNC LEDs do not illuminate correctly, or when a synchronization fault is suspected.

Checking the PTP-SYNC LEDs

If a fault is suspected in the PTP-SYNC or GPS hardware, check the PTP-SYNC LED states and use [Table 235](#) to choose the correct test procedure.

Table 235 PTP-SYNC indicator LED states

LED	State	Description and test procedure
GPS	Off	No GPS satellite data being received at the GPS/SYNC IN port. Refer to GPS LED does not illuminate or blink on clustered units on page 8-16.
	On steady or blink	GPS satellite data being received.
SYNC	Off	No data being received at the SYNC OUT port.
	On steady or blink	Data being received at the SYNC OUT port. The SYNC LED does not normally illuminate, even in cluster configurations.
STATUS	Off	No power. Refer to LEDs do not illuminate on page 8-15.
	On steady	Power but no satellite lock. Refer to STATUS LED is on steady on page 8-16.
	Blink	Power and satellite lock at either the GPS/SYNC IN or 1PPS IN port.
ODU	Double blink	Possible fault in GPS/SYNC IN or 1PPS IN cables. Refer to STATUS LED double-blinks on page 8-16.
	Off	No signal being received from the ODU. Refer to ODU LED does not illuminate within 90 seconds on page 8-16.
	On	Communication with the ODU is established.
	Blink red	Error in communication with ODU. Refer to ODU LED blinks red on page 8-16.

LEDs do not illuminate

Meaning: The PTP-SYNC unit is not powered up.

Action: Ensure that there is a cable connection between the PSU ODU interface and the PIDU IN interface of the PTP-SYNC unit. Confirm that the PSU is powered up.

STATUS LED is on steady

Meaning: There is power but no satellite lock. This probably indicates that a 1 pps synchronization pulse is not detected by the PTP-SYNC unit.

Action: Depending on system configuration, take one of the following actions:

- System using a GPS receiver module - Ensure that there is a cable connection between the PTP-SYNC GPS/SYNC IN interface and the LPU, also that there is a cable connection between the LPU and the GPS receiver module. Check that the GPS receiver module has an uninterrupted view of the sky.
- System using an alternative 1 pps timing source - Ensure that there is a cable connection between the PTP-SYNC GPS/SYNC IN or 1PPS IN interface and the 1 pps timing source.
- On cluster slave units – Ensure that there is a cable connection between the slave GPS/SYNC IN interface and the SYNC OUT interface of the preceding unit in the chain.

STATUS LED double-blinks

Meaning: There may be a fault in the GPS/SYNC IN or 1PPS IN cables.

Action: Check the GPS wiring in accordance with [Table 50](#).

ODU LED does not illuminate within 90 seconds

Meaning: There may be no communication between PTP-SYNC and ODU.

Action: Ensure that the PTP-SYNC ODU OUT interface is connected to the ODU (and LPUs if installed) via the drop cable.

ODU LED blinks red

Meaning: Error in communication with ODU. Possible causes are: fault in the ODU or PSU cable, maximum recommended cable lengths exceeded, or TDD synchronization is not enabled at the ODU.

Action: Confirm that the ODU and PSU cables are not too long: see [Ethernet standards and cable lengths on page 2-30](#). Check the ODU cable wiring by following the procedure described in [Test resistance in the drop cable on page 5-21](#).

GPS LED does not illuminate or blink on clustered units

Meaning: This indicates a fault only when the timing source is a GPS receiver.

Action: [Table 236](#) describes the action to be taken depending upon the behavior of the GPS LEDs at the master and slave(s).

Table 236 Clustered PTP-SYNC units - GPS LEDs Fault-finding

Cluster timing source	GPS LED on master	GPS LED on slave(s)	Diagnosis
GPS receiver providing NMEA data	Blink	Blink	OK
	Off	Any	Fault in GPS unit or GPS cable
	Blink	Off	Fault in daisy chain cable
Alternative 1PPS source, no NMEA data	Off	Off	OK
	Off	On	Fault in alternative 1PPS source
One ODU is cluster timing master	Off	Off	OK

Testing a TDM link

This section describes how to check the NIDU LEDs and how to perform a TDM loopback test.

Checking the NIDU LEDs

If a fault is suspected in the NIDU, check the NIDU LED states and use [Table 237](#) to choose the correct test procedure.

Table 237 NIDU indicator LED states

Port	LED	State	Description and test procedure
LAN	Green	On steady	Normal state: Ethernet 1000BaseT signal detected.
		Off	Abormal state: Ethernet signal detected but not 1000BaseT.
	Amber	Blink	Normal state: data activity detected.
		On steady	Abormal state: alarm signal received.
ODU	Green	On steady	Normal state: Ethernet 1000BaseT signal detected
		Off	Abormal state: Ethernet signal detected but not 1000BaseT.
	Amber	Blink	Normal state: data activity detected.
		On steady	Abormal state: alarm signal received.
E1/T1	Green	On steady	Normal state: TDM signal detected
	Amber	Blink	Normal state: TDM data activity detected.
	Amber	On steady	Abnormal state: no TDM data activity detected.

Performing a TDM loopback test

The loopback test allows a TDM data stream to be looped back at the copper or wireless interface. A typical T1 or E1 installation test includes a copper loopback on the local unit followed by a wireless loopback on the remote unit.



Note

The TDM Configuration page is only available when the TDM interface is enabled and the unit is rebooted ([Interface Configuration page](#) on page [6-16](#)).

Procedure:

- Select menu option **System > Configuration > TDM Configuration** ([Figure 160](#)).
- Set the TDM Channel Loopback n attribute (where “n” is in the range 1 to 8) to **Copper** or **Wireless** ([Table 171](#)).
- Click **Submit Updated TDM Configuration**.
- Perform loopback tests. The System Summary page displays alarms indicating the presence of loopbacks on each affected TDM channel ([Alarms](#) on page [7-20](#)).
- Set the TDM Channel Loopback n attribute (where “n” is in the range 1 to 8) to **None** ([Table 171](#)).
- Click **Submit Updated TDM Configuration**.

Checking for 1000BASE-T operation

If the ODU port has negotiated a link at 100BASE-T, the NIDU will not send or receive TDM data and will not bridge customer data traffic. Check that the Ethernet drop cable between the ODU and the PSU, and the network cable between the PSU and the NIDU have successfully negotiated operation at 1000BASE-T. On the System Status page, review Main PSU Port Speed and Duplex ([Figure 208](#)) and confirm that it is set to **1000 Mbps Full Duplex**.

Glossary

Term	Definition
AES	Advanced Encryption Standard
ANSI	American National Standards Institution
ARP	Address Resolution Protocol
ATPC	Automatic Transmit Power Control
Aux	Auxiliary
BBDR	Broadband Disaster Relief
BPSK	Binary Phase Shift Keying
BW	Bandwidth
CFM	Connection Fault Management
CHAP	Challenge Handshake Authentication Protocol
CSP	Critical Security Parameter
DC	Direct Current
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol
DSCP	Differentiated Services Code Point
DSO	Dynamic Spectrum Optimization
EAPS	Ethernet Automatic Protection Switching
EIRP	Equivalent Isotropic Radiated Power
EMC	Electromagnetic Compatibility
EMD	Electro-Magnetic Discharge
EPL	Ethernet Private Line
ETSI	European Telecommunications Standards Institute
EU	European Union
FAQ	Frequently Asked Question
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
GARP	Generic Attribute Registration Protocol

Term	Definition
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
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transmission Unit
NA	Neighbor Advertisement
NIDU	Network Indoor Unit
NLOS	Non-Line-of-Sight
NMEA	National Marine Electronics Association

Term	Definition
NS	Neighbor Solicitation
NTP	Network Time Protocol
NUD	Neighbor Un-reachability Detection
ODU	Outdoor Unit
OFDM	Orthogonal Frequency Division Multiplex
OOB	Out-of-Band
PC	IBM Compatible Personal Computer
PIDU	Powered Indoor Unit
POE	Power over Ethernet
PSU	Power Supply Unit
PTP	Point-to-Point
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
R-APS	Ring Automatic Protection Switching
RADIUS	Remote Authentication Dial-In Service
RAM	Random Access Memory
RF	Radio Frequency
RFC	Request for Comments
RoW	Rest of World
RMA	Return Material Authorization
RSSI	Received Signal Strength Indication
RSTP	Rapid Spanning Tree Protocol
SELV	Safety Extra Low Voltage
SFP	Small Form-factor Pluggable
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

Term	Definition
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