Enabling Digital Transformation in Mining

AXON digital platform

User Manual

Revision A, March 2019

AXON
core
MST
MST
AXON
edge
MST
AXON
power
MST

Revision History

Revision	Change		Date
A	Initial release		March 2019

Copyright and Disclaimer

Copyright

Published in Sydney by: Mine Site Technologies Pty Ltd (MST Global)

ABN: 93 002 961 953 ACN: 002 961 953

Global Head Office: Level 5, 113 Wicks Road, North Ryde, NSW 2141 Australia

Telephone: +61 (0)2 9491 6500

MST Global reserves the right to make changes to specifications and information in this manual without prior notice. MST Global accepts no responsibility for any errors or omissions contained in this manual.

This publication is subject copyright. No part of it may in any form or by any means (electronic, mechanical, microcopying, photocopying, recording or otherwise) be reproduced, stored in a retrieval system or transmitted without prior written permission of the copyright owner. Enquiries should be addressed to MST Global.

Warning

Unauthorised reproduction of, alteration of contents, or distribution to third parties, in whole or in part is an infringement of copyright MST Global will actively pursue any breach of its copyright.

Disclaimer

Information contained in this document has been developed by Mine Site Technologies Pty Ltd (MST Global). Every care has been taken by the staff of MST to ensure the content of this manual is relevant and up to date at the time of publication. Content is subject to change without notice. Technical updates as associated with this manual will be supplied to the customer at MST Global's earliest convenience.

This manual is published and distributed on the basis that the publisher is not responsible for the results of any actions taken by users of the information contained in this manual. MST Global does not accept responsibility for errors or damages resulting from misrepresentation, misinterpretation or deviation from instructions by any person in regard to the information contained in this manual. The information is supplied on the condition that the recipient will make their own determination as to the suitability of the information for their purposes prior to use.

Contact Information

Australia
Sydney
Level 5, 113 Wicks Road
North Ryde
Sydney NSW 2113
Tel: +61 (0)2 9491 6500

United States
Denver
13301 W 43rd Drive
Golden, Denver
Colorado 80403
Tel: +1 303 951 0570

Tuscon
Tel: +1 520 495 0185

Chile
Santiago
Vitacura 2771, 0f 503
Las Condes,
Santiago 7550134
Tel: +56 (2) 2 656 7673

Russia
Moscow
Office 318a
Lesnaya, 43
Moscow 127055
Tel: +7 (499) 978 72 11

South Africa
Centurion
Unit 1, Oxford Office Park
3 Bauhinia St
Gauteng 0046
Tel: +27 (0) 12 345 6100

China
Hangzhou
Building 5
1413 Moganshan Road
Hangzhou 310011
Tel: +86 571 8580 3320 Ext 206

About This Manual

This manual describes features and functions of the MST AXON Digital Platform product family. It provides information about hardware, installation, configuration and how to troubleshoot any issues. You will find it easier to use the manual if you are familiar with networking systems and have an understanding of electronics in a network environment.

Conventions used in the manual

This publication uses the following conventions to highlight and convey information:

- Text that requires input from an operator is boldfaced.
- Operator interface screen control names are boldfaced.
- Keyboard input keys are CAPITALISED.

Icons

Icons are used in the manual to highlight specific information as shown the table below.

Icon	Description
👆 **NOTE:**	The NOTE icon indicates important information or references to the user.
! **IMPORTANT:**	The IMPORTANT icon contains information to prevent damage to the product and injury to the user.
✋ **CAUTION:**	The CAUTION icon indicates to stop and pay attention or an action not to be performed.

Additional Support

For additional support please visit our website www.mstglobal.com

NOTE: The information provided in this document ("Information") is presented in good faith and believed to be correct as at the date of this document. MST makes no representations as to the accuracy or completeness of the Information. The Information is supplied on the condition that the recipient will make their own determination as to the suitability of the Information for their purposes prior to use. Under no circumstances will MST be responsible for any damages whatsoever resulting from the use of, or reliance upon, the Information.

Contents

Chapter 1: Understanding AXON Digital Platform

Mine Site Technologies' AXON Family of hardware products consists of the AXON Core unit and a number of expansion modules that can be added to it.

There is also a substantial external software offering (sold separately) that complements and expands AXON hardware, making it a true Digital Platform for mine digitization, automation and productivity enhancement. Please contact MST for more information in relation to the associated MST software products.

Currently, in addition to AXON Core, MST offers AXON Air, daisy-chainable, Wi-Fi Access Point with tracking capability. Two more modules will be added to the family within the next six months.

1.1 Typical System Layout

An example of a typical AXON system deployment is shown on the *Figure 1* below.
The first AXON Core in line connects to an Ethernet switch and a power supply via a JB11 junction box. All subsequent units are connected in series down the mine tunnel by the composite cable. Optional extension modules and radios, such as AXON Air Wi-Fi access points, are fitted as required. When the mine tunnel splits into different sections, an additional AXON Core is branched out from the main network. AXON Core or AXON Air devices can also be positioned in Wi-Fi 'hot spots' such as crib areas and refuge bays. One of the AXON Core devices on the diagram has an optional PoE+ and power distribution module attached to it, allowing for a bigger number of client devices (such as cameras) to be connected.
A client device can connect to the network wirelessly when in proximity of AXON Air or directly to AXON Core via a CAT5 cable.

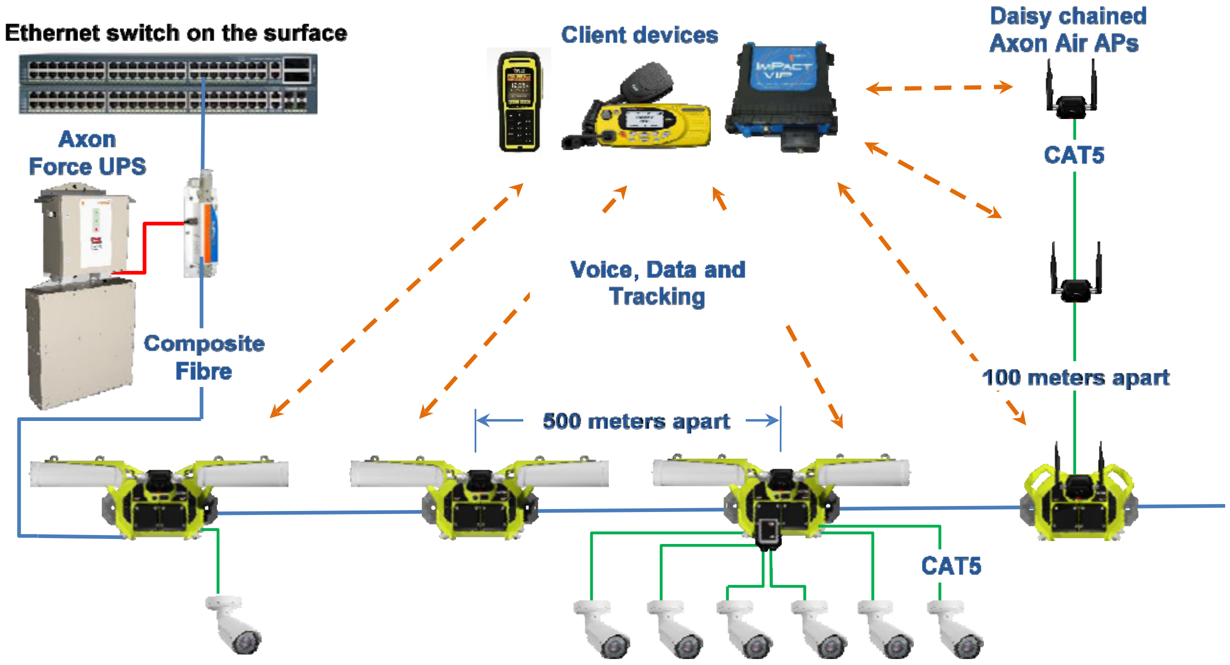


Figure 1: AXON system layout

Chapter 2: AXON Core unit

Topics:

- Hardware Overview
- Connectivity

This chapter presents the features and functions of the AXON Core unit and shows how it integrates within a network.

Mine Site Technologies' AXON Core is the main building block of the MST AXON product family. It consists of a managed fibre optic Ethernet switch with several PoE+ outputs, power management circuitry for client devices and two sockets for external expansion modules. AXON Core provides wired network access for mining environments that do not require Intrinsically Safe equipment.

AXON Core has the following key features:

- Three, Fibre Optic, Full duplex, Gigabit Ethernet ports
- Four 1Gbps copper Ethernet ports with Power over Ethernet (PoE+) supply capability.
- Two sockets for external expansion modules (PoE, managed power, automation control, sensors, etc.)
- Rigid hard plastic enclosure, suitable for mining environment, sealed to comply with an Ingress Protection rating of IP65
- Composite cabling system incorporating fibre optic data and DC power
- Low power design, with a wide input voltage from 20-60VDC
- VLAN (IEEE 802.1Q) protocol support
- RSTP (802.1W) protocol support
- LLDP (802.1AB) protocol support
- MST Device Discovery protocol support
- SNMP (read only) protocol support
- QoS (P802.1p) protocol support

For detailed specifications on AXON Core, see AXON Core Specifications.

2.1 Hardware Overview

The features and functions of AXON Core are illustrated in *Figure 2: AXON Core layout* and the accompanying table.

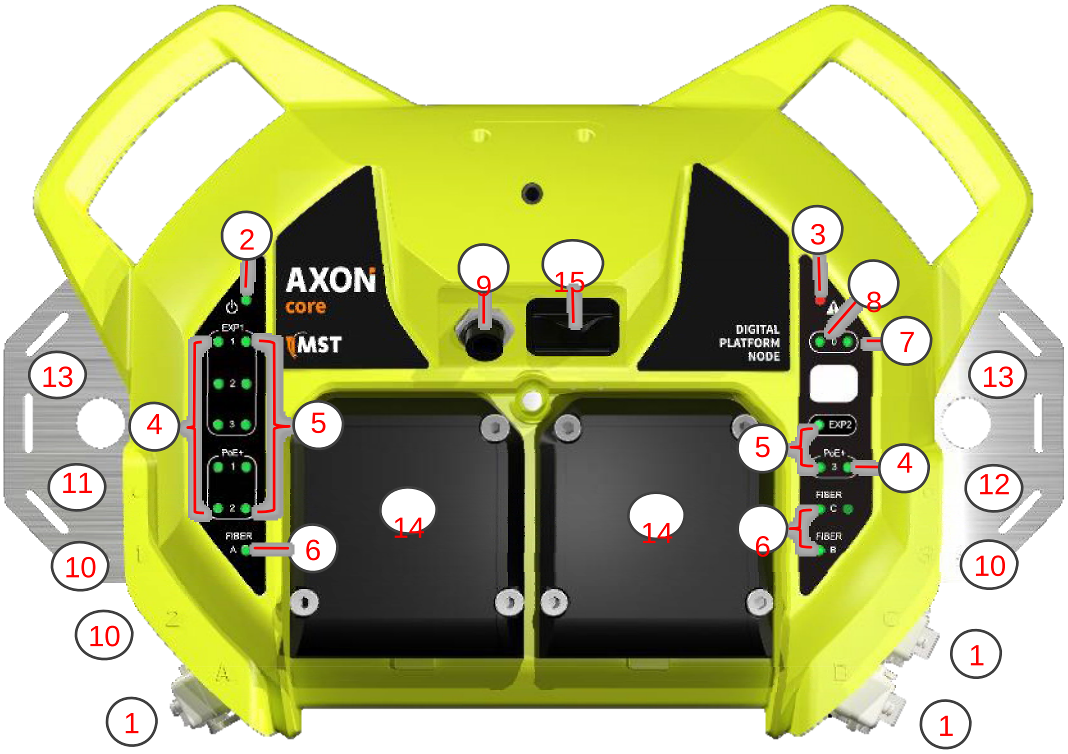


Figure 2: AXON Core layout

Key	Description	Function
1	Composite (fibre + power) cable port	Connector for data transmission and / or DC power distribution. There are three ports: A, B and C
2	Power and Status LED	Power and Status LED
3	Power warning LED	Power warning LED
4	PoE+ port status dual colour LEDs	PoE+ port status dual colour LEDs
5	PoE+ port activity LEDs	PoE+ port activity LEDs
6	Fibre port status LEDs	Fibre port status LEDs
7	Radio port status LED	Radio port status LED
8	Radio port activity LED	Radio port activity LED
9	PoE+ AXON Air port	PoE+ port typically used by AXON Air module. It can also be used for other purposes
10	PoE+ Ethernet ports	External Ethernet port with IEEE 802.3at PoE+ supply capability for powering client devices.

11	Factory defaults button	Factory reset button for the unit. Pressing it for 5…15 seconds will cause factory reset
12	Reset button (RED)	Pressing this button will cause switch core reset without losing the device configuration.
13	Mounting holes	Rear mounting bracket with holes for mounting AXON Core on the wall or roof.
14	Covered Expansion Socket	Expansion socket covered with a protective cover.
15	SD card	Inserting a card from another switch and power cycling AXON Core will install switch configuration stored on the card

2.3 Connectivity

AXON Core has three types of network connections:

- Composite Fibre Ports
- Ethernet Ports
- Expansion interfaces

2.3.1 Composite Fibre Ports

AXON Core unit has three composite fibre port connectors with a crush protection cover. Each connector consists of two electrical contacts and a duplex LC single mode optic fibre (SMOF) receptacle as shown in *Figure 3: Composite fibre ports.*

NOTE: A protective cover or a mating cable connector must be attached to unused ports to maintain the IP65 (Ingress Protection) rating of the unit

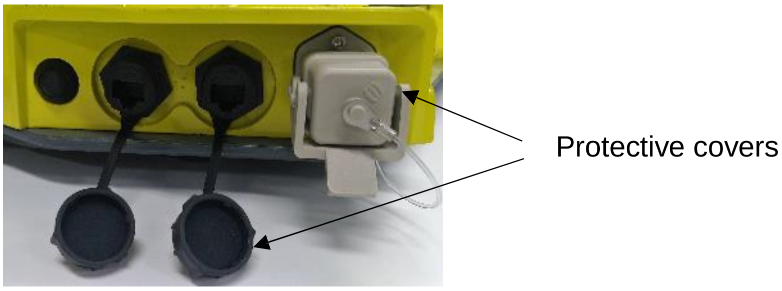


Figure 3: Composite fibre ports

Each port can be connected in one of the following ways:

Port connection	Description
DC power only connection	A DC power cable to connect the PSU to the electrical contacts on an AXON Core. By convention, this cable is connected to port A.

Fibre only connection	A fibre optic cable terminated to the fibre contacts of the AXON Core composite connector.
Fibre and DC power connection	A composite cable providing fibre optic connectivity and power to AXON Core.

Fibre optic cabling provides numerous benefits over Ethernet cabling, with superior signal integrity and no signal interference from high-powered electronics. It also enables units to be spaced over longer distances without the distance limitation of Ethernet cabling.

By default, port A is configured as the upstream port and ports B, C as the downstream ports. The difference between upstream and downstream ports is the orientation of the fibre that is used for transmitting and receiving data. This is illustrated *in Figure 4: Fibre orientation of Upstream and Downstream ports.*

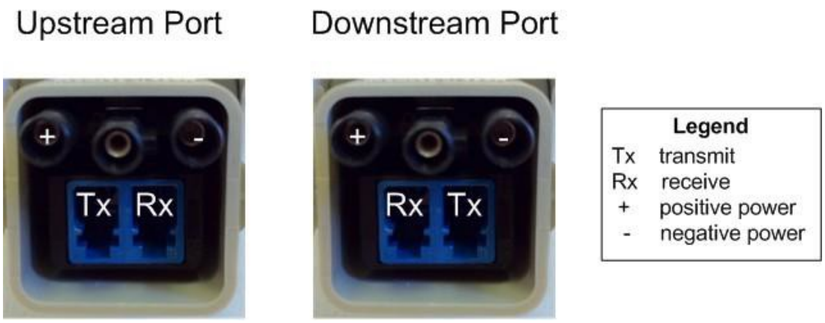


Figure 4: Fibre orientation of Upstream and Downstream ports

Due to the difference in the fibre orientation, MST composite cable and fibre optic cable can only be connected between ports on AXON Core devices marked with a tick in the matrix below.

	Port A	Port B	Port C
Port A	✗	✓	✓
Port B	✓	✗	✗
Port C	✓	✗	✗

Single- and Multi-Mode Cables

AXON Core is supplied from the factory with 1000BASE-LX single-mode SFP modules. Customers wishing to interface to other cable standards, e.g. 100BASE-FX single or multi-mode, should contact MST to arrange replacement of the appropriate SFP modules.

NOTE: If replacing the single-mode SFP modules with multi-mode modules, the single-mode patch lead between the SFP module and the MST Composite Cable connector on the inside of the housing needs to be replaced with a multi-mode patch lead.

JB11 junction boxes can be connected inline between any two units in the chain to supply power. There is no need to isolate AXON Core units to a single power source.

IMPORTANT: If an SFP is changed, the device must be rebooted or reset to detect the change.

2.3.2 Copper Ethernet Ports

AXON Core has four external Copper Ethernet ports that enable connection to other networking devices.

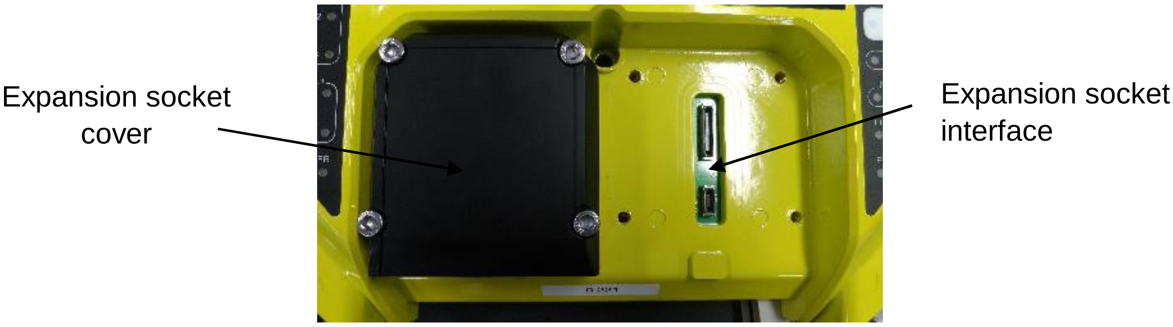
The four Ethernet ports also provide IEEE 802.3at PoE+ (Power over Ethernet) injector functionality, allowing a single cable to be used for data and power to network devices. Each Ethernet port's functionality can be configured by the web browser interface, or by centralised configuration management.

One of these four ports, located on the top of AXON Core, will typically be used for AXON Air module connection, but can also be used for any other purpose. Similarly, any of the other PoE+ ports can be used to connect AXON Air module.

For more information on configuring Ethernet ports, see Chapter 7: Configuration Using the Web Interface

2.3.3 Expansion sockets

AXON Core has two expansion sockets on its front panel that allow adding optional expansion modules to it.



Chapter 3: AXON Air module

Topics:

- Hardware overview
- Daisy Chaining of AXON Air units

This chapter presents the features and functions of the AXON Air module and shows how it integrates with the AXON Core unit and the network.

Mine Site Technologies' AXON Air is a key member and an important building block within the MST AXON family of products, it provides wireless network access for mining environments that do not require Intrinsically Safe equipment and consists of a Wi-Fi Access Point and 2-port Ethernet switch for daisy chaining. AXON Air supports meshing (802.11s protocol) and can be used as a mesh gateway or a wireless bridge between two wired subnets.

AXON Air has the following features:

- One Wi-Fi Radio, 802.11 a/b/g/n, 2 x 2 MIMO, 2.4 or 5Ghz
- 6 x SSIDs
- VLAN (IEEE 802.1Q) protocol support
- LLDP (802.1AB) protocol support
- SNMP (read only) protocol support
- QoS (P802.1p) protocol support
- WEP/ WPA/ WPA2 security protocols support
- Two 1Gbps Ethernet ports with proprietary Power over Ethernet power supply capability
- The unit gets its power from the upstream PoE ports and passes it through to the next access point in the chain via the downstream port. AXON Air negotiates a PoE+ Class 4 power requirement, whilst drawing 4W nominally.
- Rigid hard plastic enclosure, suitable for mining environment sealed to comply with an Ingress Protection rating of IP65

For detailed specifications on AXON Air, see AXON Air Specifications

3.1 Hardware Overview

The features and functions of AXON Air are illustrated in *Figure 2: AXON Air layout* and the accompanying table.

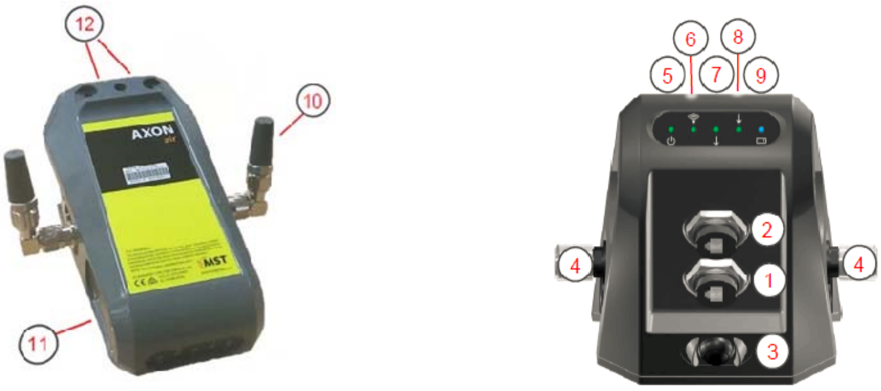


Figure 2: AXON Air layout

Key	Description	Function
1	Upstream PoE+ Ethernet port	1xGbps Ethernet port with IEEE 802.3at PoE+ input capability
2	Downstream PoE+ Ethernet port	1xGbps Ethernet port with IEEE 802.3at PoE+ supply capability for powering next-in-line AXON Air unit
3	Default configuration button	Pressing the button for 10 or more seconds and power cycling AXON Air at the same time will cause factory reset
4	Antenna connector	N-type female Antenna connectors
5	Power On LED	Power On LED
6	Wi-Fi Activity LED	Wi-Fi Activity LED

7	Downstream PoE LED	Downstream PoE activity LED
8	Upstream PoE LED	Upstream PoE activity LED
9	Tracking activity LED	Tracking activity LED
10	External Antenna	External 2.5dB, omnidirectional antenna
11	Antenna swivel mounting area	Mounting area used to accommodate optional antenna swivel mechanism (sold separately).
12	Mounting holes	Two mounting holes on the top of the module

3.3 Daisy Chaining of AXON Air units

Each AXON Air features a two-port Ethernet switch, which enables daisy chaining of individual AXON Air units via a CAT5 cable. The maximum distance in between AXON Air nodes in such scenario is 100 meters. A maximum of three AXON Air units can be daisy chained together.

The unit gets its power from one of its upstream PoE port and passes it through to the next access point in the chain via the downstream port. AXON Air negotiates a PoE+ Class 4 power requirement, whilst drawing 4W nominally.

The AXON Air operational parameters can be configured through its own web browser interface or via the centralised configuration management. For more information, see Chapter 7: Configuration Using the Web Interface

Chapter 4: Network System Design

Topics:

This chapter describes network system design for underground mines.

A MST System Engineer will usually design and preconfigure a network based on the requirements and layout of each mine site. This will involve a visual inspection of the mine site to identify user areas, and determine access point locations. A RF (Radio Frequency) site survey is also conducted to understand the behaviour of radio waves in the mine. The following factors help determine network design:

Wireless coverage requirements of the mine

- Quantity and type of wireless client devices connected to the network
- Wired client devices connected to the network and their location
- Interconnection to the mine's existing corporate network
- Policies for network protocol between networks
- Cabling requirements
- Antenna types to use with each unit and mounting method for each antenna
- Mounting location and installation method for each network device.

4.1 Installation Types and Coverage

Wireless network coverage can be described as:

- **Wi-Fi hotspot** — Network coverage is provided in key areas, such as crib areas and refuge bays.
- **Full coverage** — Seamless wireless coverage by strategically placing AXON Air units so their radio fields overlap.

An AXON Air can communicate at wireless distances of 150-300 metres, depending on the chosen antenna,geometry and geology of the mine.

4.2 Power Requirements

The power requirements for a network are unique to each site installation. Determining power requirements can be complex and is dependent on various factors such as the number of AXON Core units, PoE devices, branches in the network and composite cable lengths.

NOTE: A site inspection conducted by a MST System Engineer will help determine the power requirements for your network.

AXON Core is designed to operate at a wide voltage range, from a minimum of 20VDC up to 60VDC. Each AXON Core in a network can internally step up the incoming voltage to 48VDC in order to supply power to its connected PoE devices. AXON Core needs to receive a minimum input of 20VDC to power PoE devices.

56VDC power supplies are used for large networks to maximise the distance between power supplies. For instances where the AXON Core switches are deployed in isolation or in remote location a 24V DC UPS can be used.

External power supply recommendations:

Using Uninterrupted Power Supplies is not mandatory; however, it will increase the uptime and protect the network from power surges and fluctuations. Fluctuations may cause damage to the network and auxiliary equipment. The recommended UPS is AXON Force UPS.

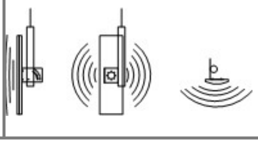
4.3 Choosing Antennas

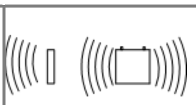
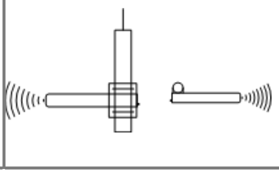
Antennas are connected via N-Type connectors to each AXON Air to provide wireless network coverage. The type of wireless coverage, surrounding geology, tunnel topology and surface of the roadway/tunnel are all factors that will determine the choice of antenna. A minimum of two antennas is required for each AXON Air. There two most popular directional antenna patterns:

- **Omnidirectional antennas** — radiate equally in all directions for a short range, providing immediate coverage in an open area.
- **Directional antennas** — radiate in a specific direction over a longer range. A higher gain antenna will have a longer range and is more directional. It is important that directional antennas are aligned properly between AXON Air units to ensure continuous coverage between units.

The antenna radiation pattern and polarisation need to be considered to provide suitable wireless coverage in an area.

Antennas commonly used with AXON Air are shown below.

Antenna Type	Illustration	Description
Omnidirectional 2.5dbi rubber whips		A lower gain antenna that radiates equally in all directions. It provides direct coverage in an open area.
Panel antenna		A panel antenna is a directional antenna, with a wide horizontal beamwidth and narrower vertical beamwidth. They are suited for covering an open area in one direction.

Diversity panel antenna		A diversity panel antenna contains two panel antennas in one housing with a 90° rotation between them. It is used for providing better signal reception in difficult areas, and more accurate Wi-Fi tag location when Wi-Fi tracking is implemented. Diversity antennas use both antenna connections on a WAC.
Yagi directional antenna		A Yagi antenna is high gain directional antenna. They are ideally suited for line of sight tunnel communications. Yagi antennas need to be aimed accurately and avoid obstacles in their RF beam path.

4.4 Placement of AXON Air units

In underground environments, many factors can influence finding a suitable location for mounting of the AXON Air access point and antennas connected to it. This document will only consider the signal propagation aspects, see AXON Air Mounting Options for more advice.

4.5 Placement of Antennas

It is recommended to attach the antennas directly, or with a short good quality coaxial cable, to the access point. The antenna can be connected up to 20m away from the access point when at minimum CNT or LMR 400 antenna cable is used. At 2.4 GHz the loss of this cable is approximately 2.1 dB per 10m. It will reduce the effectiveness of the antenna however it may be acceptable with the use a of high gain antenna. The coaxial connection should be kept as short as possible to minimise signal attenuation. Larger antennas / longer cable feeds can require line amplifiers, and possibly bi-directional splitter / combiners for dual antenna systems.

In surface installation to ensure EN 60950-1 compliance, AXON Air, the antenna and all cabling must be installed in a location that eliminates the chance of the system being struck by lightning. If an antenna needs to be installed in a location where it could be struck by lightning, then an appropriate lightning arrestor must be placed in-line with the antenna and cabling such that AXON Air is not subject to overvoltage due to lightning.

Antenna placement underground is dependent on the surrounding geology, tunnel topology and stratum type. The recommended placement of antennas is as follows:

Tip 1: Directionality

Antennas should be mounted and angled to give optimum transmission along curves and dips as shown below in *Figure 5: Angling antennas.*

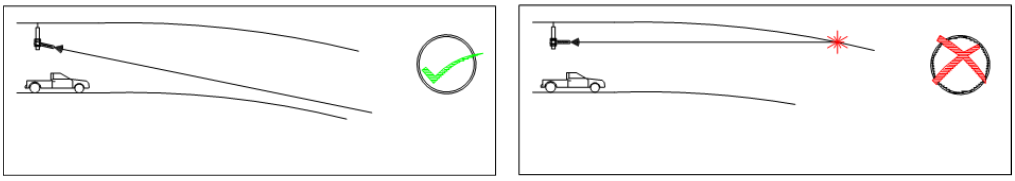


Figure 5: Angling antennas

Tip 2: Obstructions

Antennas should be mounted to avoid signal obstruction from rock, vehicles, equipment and machinery as shown in *Figure 6: Antenna mounting to avoid obstructions*.

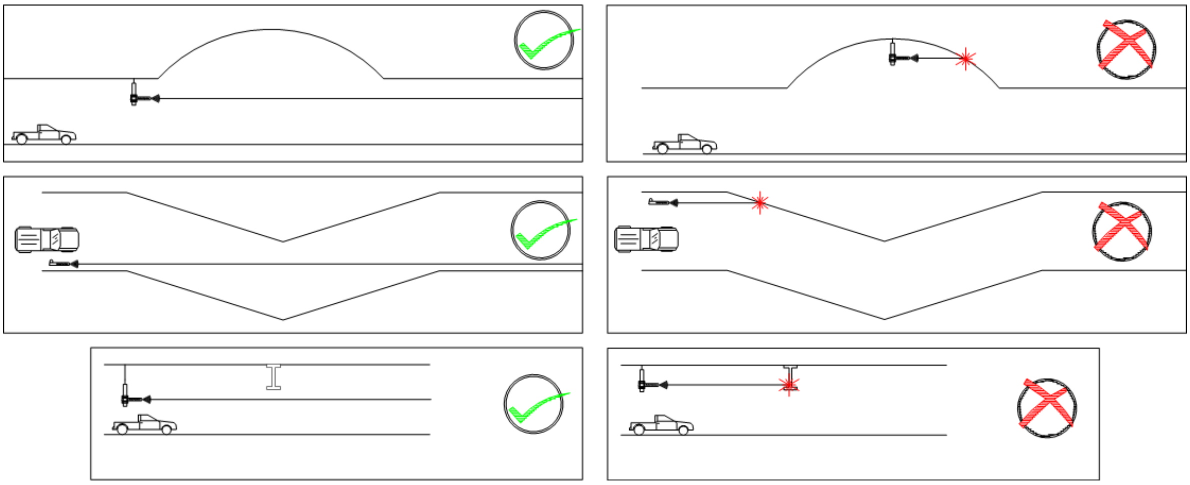


Figure 6: Antenna mounting to avoid obstructions Tip 3: RF Field Overlap

Multiple antennas should be mounted to avoid crossing signal paths as shown in *Figure 7: Antenna directivity.*

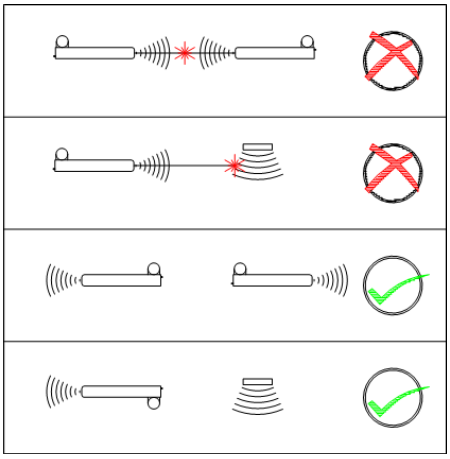


Figure 7: Antenna directivity

The positioning of the antennas is crucial when Wi-Fi tags are used for asset tracking and location services. Wi-Fi tags will not be read when there are antenna standing wave nulls. Antennas need to be positioned to have best reception of tag messages. For Antenna mounting options, see Antenna Mounting Options

4.6 Determining distance between AXON Air modules

Line of Sight Distances

In line of sight, each AXON Air has a maximum wireless range of 300 metres (984 feet) using high gain directional antennas. AXON Air units are generally installed with a 100 metre (328 feet) overlap of the radio field as shown in *Figure 8: Wireless channel layout and distances around curves*

This ensures sufficient coverage between AXON Air units.

AXON Air units within range of each other must be configured with different Wi-Fi channels. By default every fifth channel is used (channels 1, 6 and 11) to prevent signal overlap, minimising the possibility of inter-modulation or interference. There are circumstances in which the configuration may allow all radios to be operating on the same channel. Rapid handover and mobile device battery consumption may improve in this configuration.

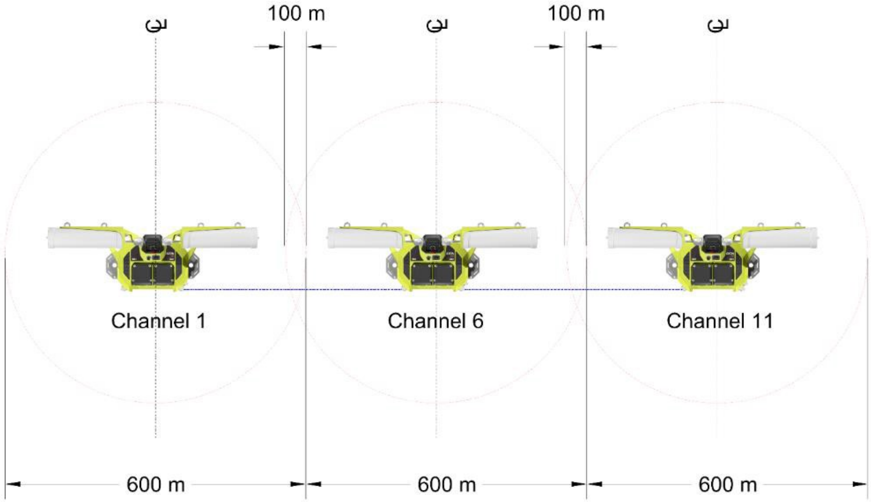
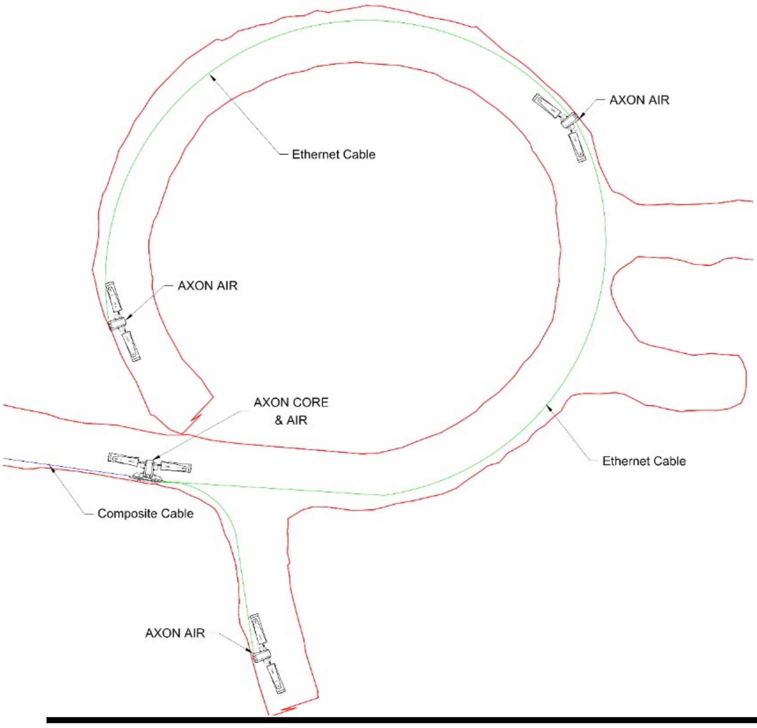


Figure 8: Wireless channel layout and distances around curves

In situation where line of sight (LoS) between the receiving device and AXON Air cannot be achieved due to the physical layout of the tunnel, the distance between the AP's may need to be reduced. Below is a typical example of such situation. The AXON Air AP's are spaced 100 m apart to overcome the curvature of the spiral decline



There are many variances in a tunnel, which influence the RF signal propagation, the size and curvature being the most prevalent. The surface of the walls, steel mesh, water and objects in the RF path are all factors to take into consideration when planning the system design. Another important factor to consider is movement of vehicles, large vehicle such as trucks can shadow a large area of the section of the tunnel, effectively blocking the roadway and the RF path. In many cases, it is advantageous to trial a section to get a better understanding of the Wi-Fi propagation in the specific environment. A Wi-Fi survey is a good measure to insure good coverage.

Chapter 5: Installation

Topics:

This chapter describes mounting options, installation schemes, and antenna and cable connections. Fibre connector assembly and cable termination are beyond the scope of this manual.

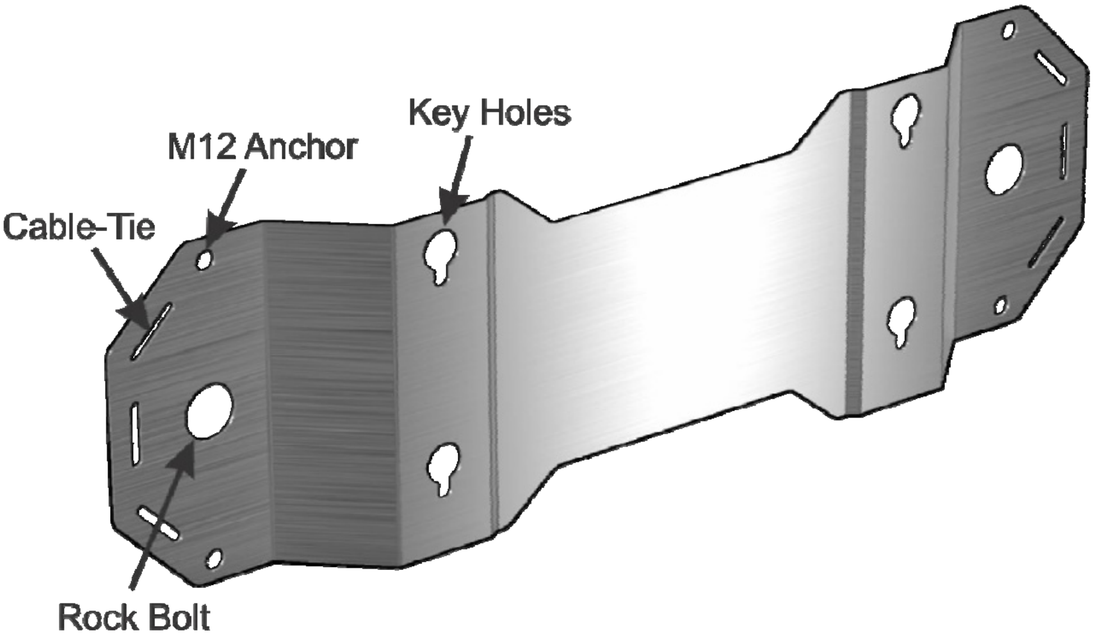
IMPORTANT: The electronic components in each AXON Core have been designed to be isolated from the enclosure and local electrical earth. This ensures there is no current passing between grounds of different potentials (known as galvanic isolation). Galvanic isolation must always be maintained, with the AXON Core ground terminals isolated from electrical earth, and all antenna and antenna cable connections properly insulated.

5.1 AXON Core Mounting Options

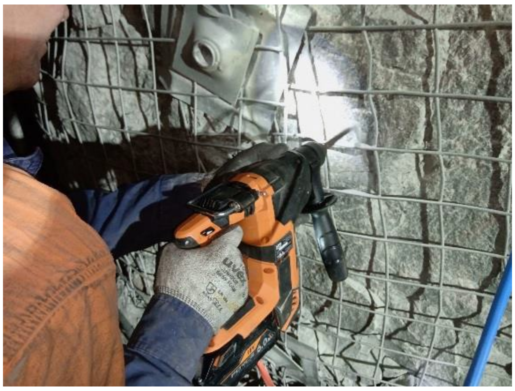
Standard mounting options for AXON Core are described in the table below.

The mounting plate for AXON Core is designed for ease of installation and future convenient removal/replacement. The key holes in the mounting plate allow AXON Core to be attached or removed from the plate with ease; there is no need to remove the mounting plate when exchanging an AXON Core in place of a new one.

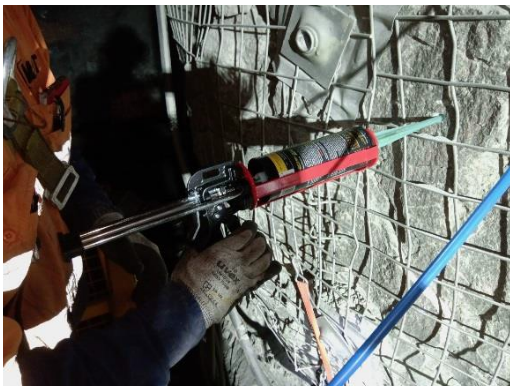
Application	Installation
Mounting the AXON Core Mounting plate to a rock bolt	The AXON Core mounting plate has two 25mm holes to mount it to a rock bolt on the mine's rock face. It is secured to the rock bolt with a 25mm nut.
Mounting the AXON Core Mounting plate with 12 mm rock anchor or threaded bar.	Drill 13 mm hole and use appropriate chemical anchor to secure the anchor rod
Mounting AXON Core to the mesh	The four corner mounting points on a mounting plate can be cable-tied to the mesh in a mine tunnel.



The AXON Core mounting plate

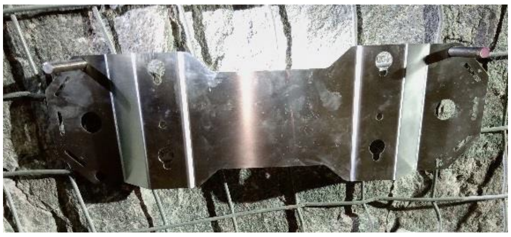


Step 1. Drill 13 mm hole

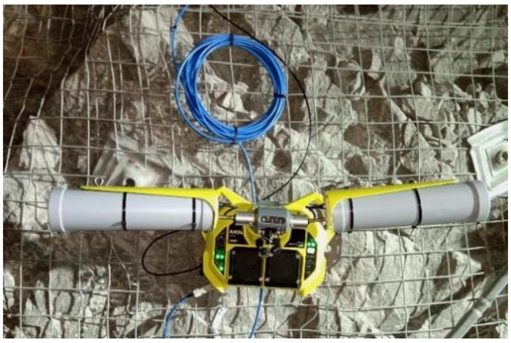


Step 2. Inject glue

Plate Step 3. Insert both Anchors



Step 4. Mount the AXON Core



Step 5. install AXON Core & Air

The AXON Core mounting plate can be mounted in various convenient ways. On this picture you can see a preferred way of using two 12 mm chemical anchors.

Any combination may be used to fix the plate e.g. 24 mm rock bolt and 12mm chem anchor.

CAUTION: The above mounting method maybe not suitable for your particular situation. If in doubt consult with your Geo-Technical team or your supervisor.

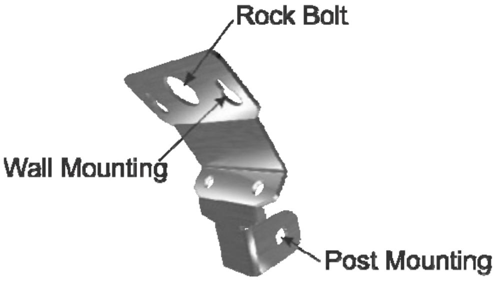
5.2 AXON Air Mounting Options

The AXON Air wireless access point is commonly mounted onto the AXON Core unit as depicted at Step 5 in the previous paragraph. There will be situations where it is advantageous to mount AXON Air in a different location to AXON Core or where AXON Core is not required, e.g. when AXON Air is chained to another AXON Air. For this purpose, a separate mounting plate is included with AXON Air.

A convenient way to mount AXON Air is to use a mounting post as shown on the photo below. The procedure is similar to the AXON Core mounting method shown above. The 12mm threaded anchor (W-MNT-025) is glued into a hole in the rock wall and the yellow mounting post (W-MNT-019) with AXON Air attached to it is screwed on top of the anchor. A M12 nut can be used to counter lock the pole, stopping it from spinning, if required.

The mounting plate has two key holes that are used for wall or rock face mounting.

AXON Air Mounting Bracket



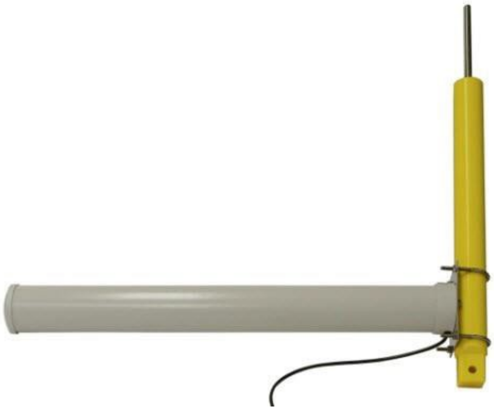
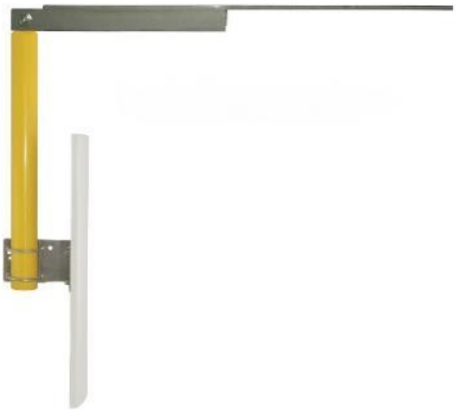
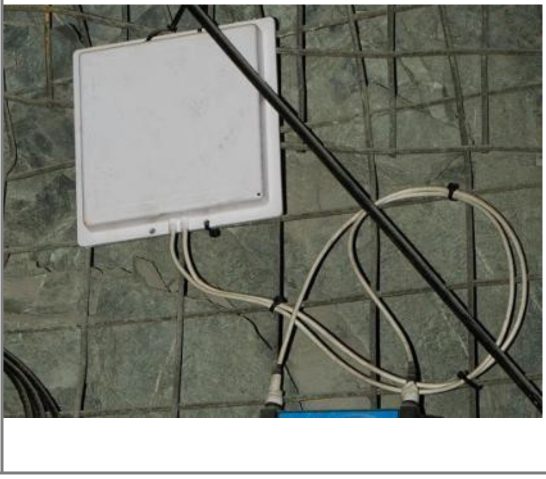
Note: When mounting AXON Air wireless access points, it is important to consider the distance from the antenna to surrounding objects. As a rule generally, antenna should not be placed within 400 mm of RF reflecting objects or materials that contain metal.

CAUTION: The above mounting method maybe not suitable for your particular situation. If in doubt consult with your Geo-Technical team or your supervisor.

5.3 Antenna Mounting Options

Antenna mounting is dependent on the location and coverage required. Examples of antenna installation options are described and illustrated in the table below.

Mounting Option	Description	Picture
Omni directional antenna directly attached to AXON Air	AXON Air is supplied with 2x 2.5 dBi Omni directional antennas. Which install directly to the enclosure.	
Directional Helical antenna 15 dBi (Poynting) directly attached to AXON Air	Example of a directional Helical antenna directly attached to AXON Air. This is the preferred mounting method and has the advantage of a short RF cable.	

Mounting a Yagi antenna or panel antenna to the mine tunnel roof.	In instances where it is required to separate the antenna from AXON Air, an antenna can be connected via an (up to) 20 m Coaxial cable. A hole is drilled into the tunnel roof and the mounting pole is secured using chemset adhesive. The Yagi antenna is attached to the mounting pole using U-clamps	
Mounting a Yagi antenna or panel antenna at a portal	In situation where the drilling is not possible or prohibited, specialised mounts can be manufactured.	
Mounting a panel antenna on the rock face or mesh	The panel antenna is cable tied to the mesh, ensure the antenna is not obstructed by objects and avoid mounting it close (400 mm or less) to large steel structures.	

5.4 Installation Schemes

The installation and placement of antennas and AXON Core units will depend on the wireless coverage type, rock type and tunnel topology. A few examples of installation schemes in a mine are described and illustrated in the following sections.

5.4.1 Installation in a Straight Drive

An example of a straight drive installation scheme is shown in *Figure 9: Installation scheme in a straight drive.*

In this example, multiple AXON Core units are fitted with AXON Air access points utilising 15dBi helical antenna. This creates constant coverage as may be required by a vehicle traveling along the roadway.

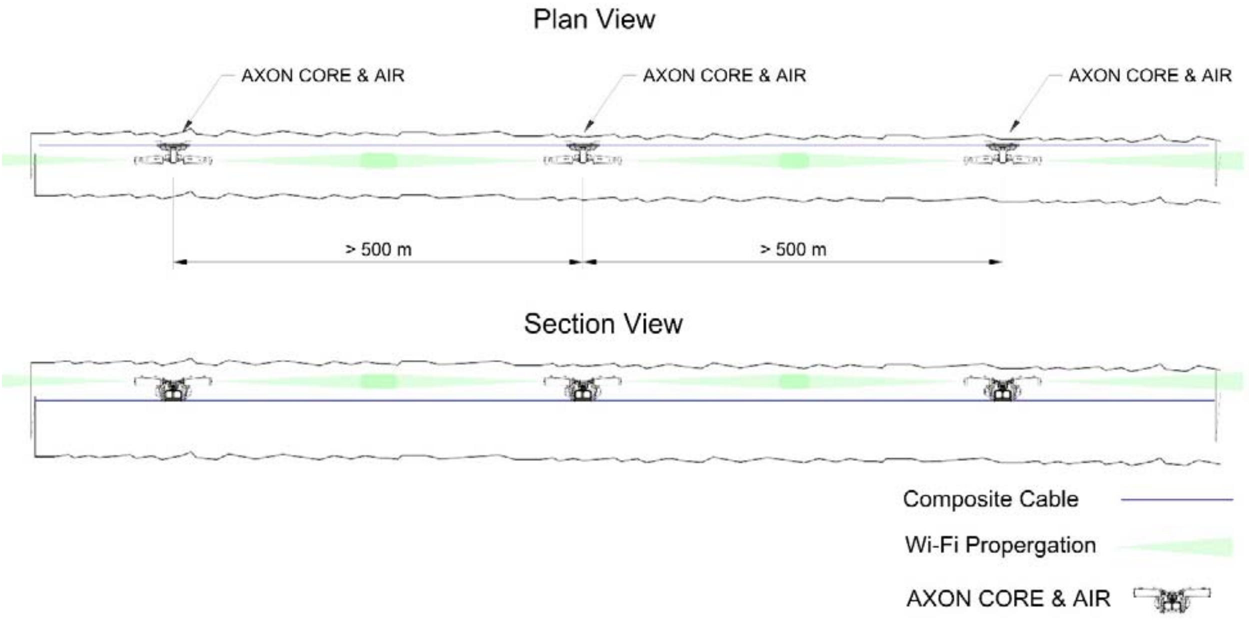


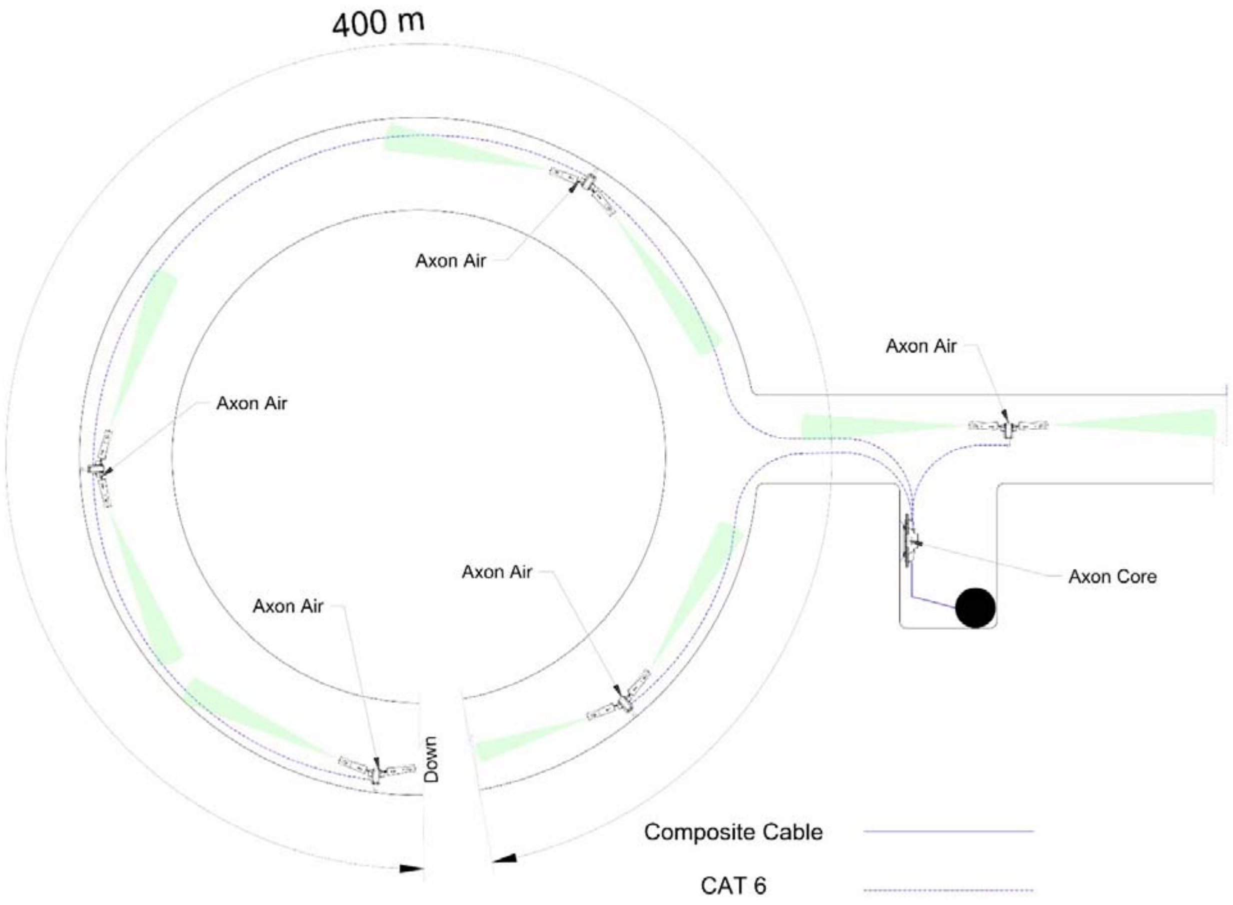
Figure 9: Installation scheme in a straight drive

5.4.2 Installation in a no line of sight scenario

A curved decline installation scheme as shown in Figure 10

One of the advanced futures of AXON Air is the ability to be powered from another AXON Air. This adds great flexibility in network design. In the example below a AXON Core network switch is collocated in the electrical cuddy, this is convenient as the composite cable can be run through a borehole from the surface and then further to the lower levels. It is not recommend to chain more than 3 AXON Air units from one PoE+ port on AXON Core. The maximum length of Ethernet cable between AXON Air units is 100 meters, this gives 300 meters if 3 units were chained.

Figure 10: Installation scheme in a curved decline



5.4.3 Installation in large underground openings, e.g. Crusher Building.

In large openings, it is advantageous to use omni-directional or semi-directional antenna. The example here shows AXON Core unit with AXON Air module providing wireless network coverage and PoE connectivity. AXON Core functionality is expanded with two optional (soon to be released) plugin modules. First called AXON Control providing automation capability and the second called AXON Power, which expands the total number of AXON Core PoE ports to seven.

On the diagram below, there are six IP cameras connected to AXON Core, two of which monitor the crusher and the other four monitor trucks reversing towards the crusher. AXON Control module connects to the sensor measuring the temperature of the main bearing of the crasher, it also drives the crusher dust suppression solenoid valve via one of its relay outputs. The automation logic, driving the relay is enabled by the MST SENSA Director software. The dust suppression is turned on only when a truck is present.

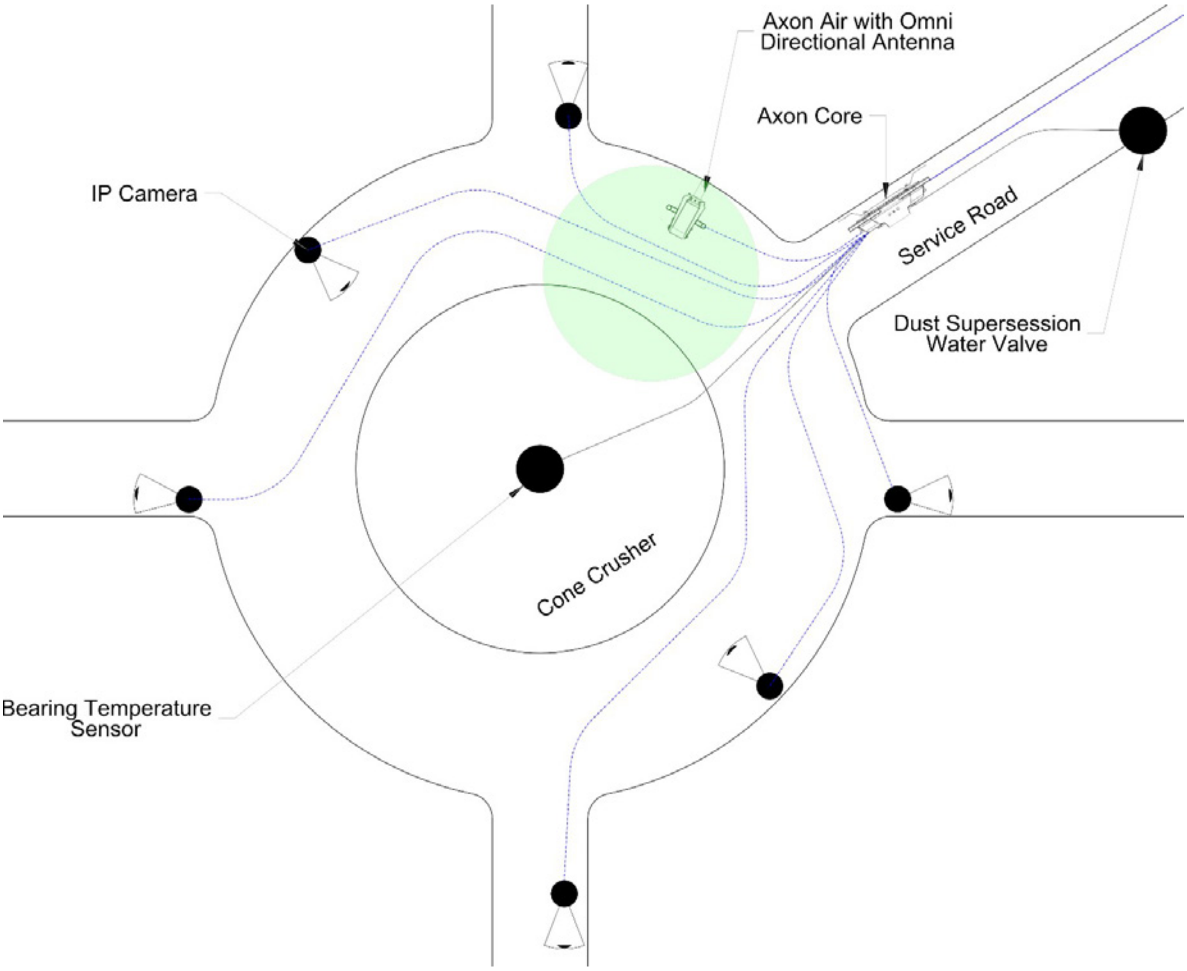

Axon Air with Omni Directional Antenna
Axon Core
IP Camera
Service Road
Dust Supersession Water Valve
Cone Crusher
Bearing Temperature Sensor

Figure 11: Installation scheme in a Crusher Building

5.4.4 Installation at an Intersection

An example installation scheme for an intersection is shown in *Figure 12: Installation Scheme at an intersection.*

At intersection where fibre connection is required to be continued in all directions, two AXON Core Nodes are required. The distance from the intersection depends on the specific requirements.

It may be appropriate to move one AXON core with AXON Air attached to it (B) as far as 400 m into the northern spore roadway and the other (A) in the orthogonal direction closer to the intersection.

A traffic light solution can be implemented if an optional AXON Control module is used inside of the unit (A). It can be programmed to operate independently of the network.

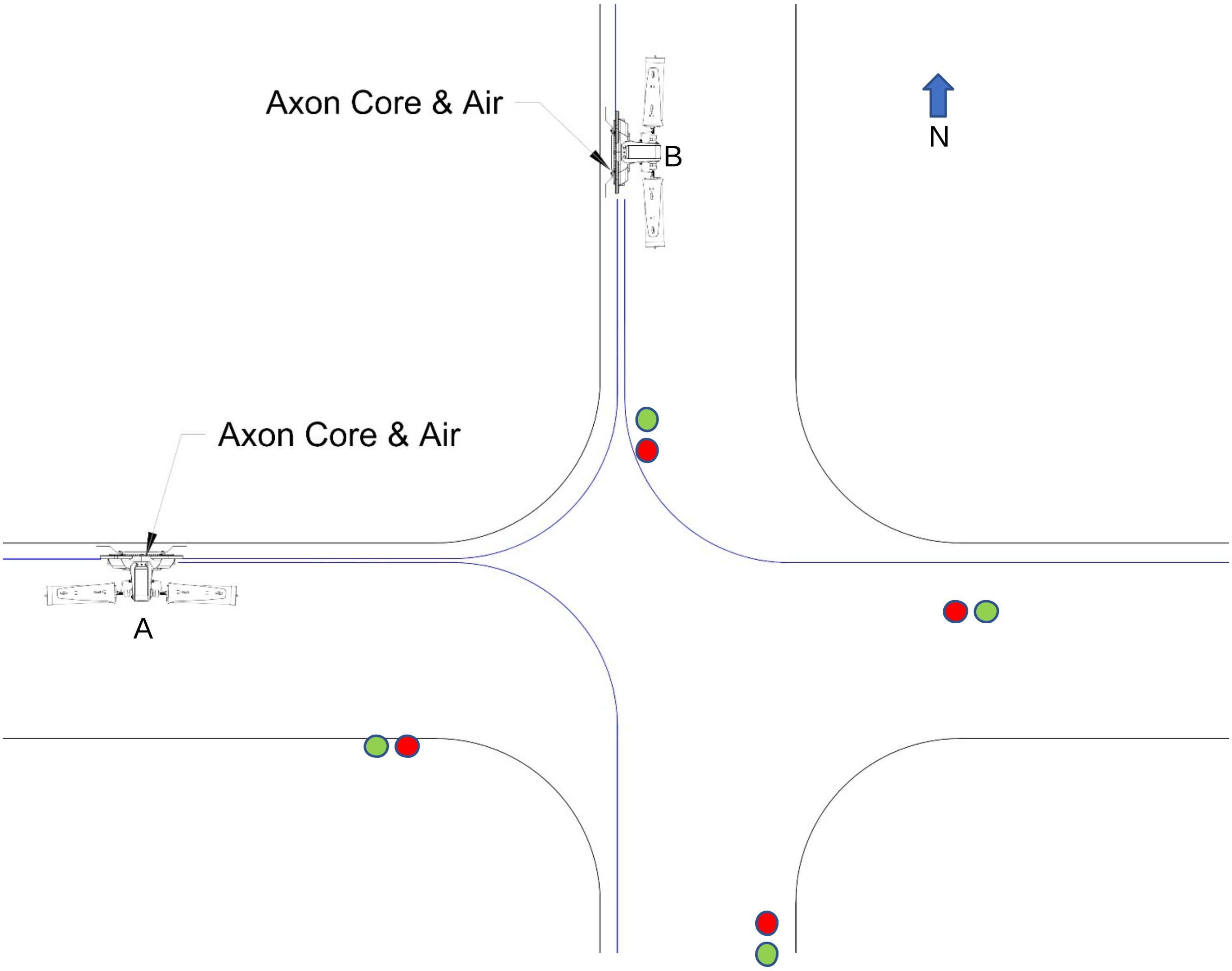


Figure 12: Installation Scheme at an intersection

5.5 Connecting Power to AXON Core

The AXON family of products includes three ruggedized mining uninterrupted power supplies, for full composite cable installation in operational areas AXON Force is an ideal UPS. The main electrical benefit is that the output power is 56V DC constant, regardless if mains power is available or not. Most common UPSs will supply 56V DC if mains power is on; however, the output voltage will drop back to 48 V DC when mains power is off. This means that the DC power design has to consider worst-case scenario.

MST strongly recommends the use of UPS in underground implementation, as it will ensure clean reliable DC power and guarantied uptime.

Composite cable can be inserted into other AXON Cores while the system is powered; this allows the system to be expanded as necessary. Power usage levels should be evaluated prior to adding more units downstream to ensure that the voltage rail does not drop too low. A minimum of 20VDC is required for AXON Core to supply PoE to other devices. If the voltage drops below 20V, additional power is required.

> The DC power system is dose not allows more than one DC Supply/UPS to be connected to the same composite cable. This is referred to as “cell” cells are interconnected via optical fibre connection only. This typical for DC systems. If double redundant power is required, please contact MST.

Connect the composite fibre/power cable to a DC power source with correct termination. Note that the DC supply must be between 20 and 60VDC. Refer to the power supply requirements Section 4.2.

Turn on the DC power supply and verify that the green power light is on. If there is no green light, refer to Troubleshooting Guide.

5.6 Handling composite cable during installation

The composite cable is ruggedly built for the mining environment. However the following precautionary measures should be noted during installation:

- Never pull or create tension on the cable. Unreel the cable from the cable reel, or allow the weight of the cable to unreel as the vehicle is moving as shown in Figure 13: Handling composite cable.
- Do not bend the cable at sharp angles; excessive bending can fracture or break the fibre optic cable.
- Do not step on the cable.

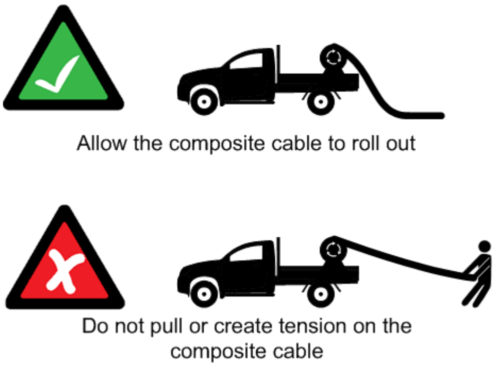

Allow the composite cable to roll out
Do not pull or create tension on the composite cable

Figure 13: Handling composite cable

5.7 Connecting Composite Cable to AXON Core

A composite cable is connected to the fibre port of AXON Core. Once connected, it will auto detect devices and their settings.

IMPORTANT: Protect all connectors and sockets from dust and grit, with minimal exposure during installation. Any unused sockets must be covered by the supplied dust caps at all times during installation. Any unused sockets must be covered by the supplied dust caps at all times.

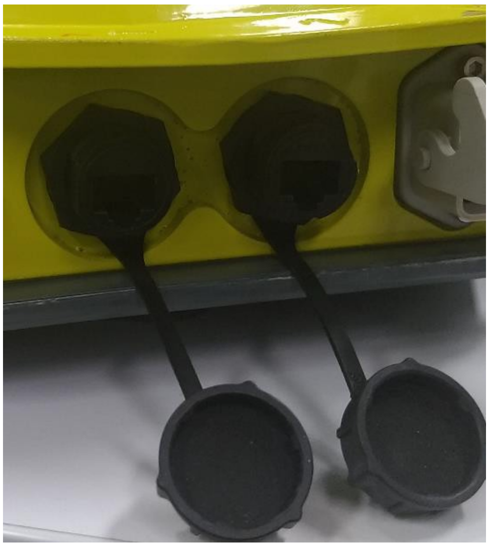
Branch fibre network out requires simply connecting composite cables to the additional fibre ports. The connected fibre ports will cause the corresponding fibre port LEDs to become active. If you are adding AXON Core units to an existing system, please consult your MST System Engineer to ensure power requirements are being met.

5.8 Standard Composite and Fibre Cable Lengths

While custom cable runs can be made where necessary, it is faster and cheaper to use standard cable lengths supplied by MST. Please contact MST for the latest listing of available cable lengths.

5.9 Connecting Ethernet Cable to AXON Core

The external Ethernet ports are located on the underside of AXON Core, and are used to connect to Ethernet devices (such as computers, Ethernet controlled PLCs, hard-wired Ethernet Phones and IP video devices). An Ethernet cable with a RJ45 connector is used to connect PoE devices. Ethernet cables are required to meet specifications for use in a mining environment in Ethernet Cable Specifications

Procedure	Illustration
1. Unscrew the protective cover on the Ethernet port. 2. Insert the Ethernet cable (with a bayonet back-shell) 3. Align the protective cover on the cable to the notch in the mating jack on AXON Core, and twist to lock the connector into the Ethernet port 4. Securely fasten the cable lead against the wall/ceiling. **IMPORTANT:** ❗ Check that all unused Ethernet ports remain protected with the supplied covers.	

5.10 Connecting Antennas to AXON Air

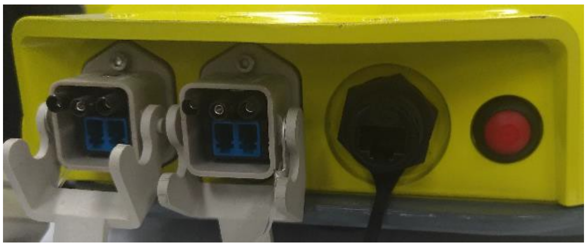
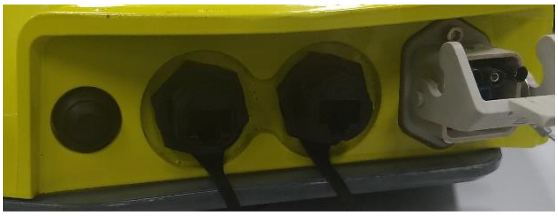
Antennas can be connected directly to the coaxial (RP-TNC) jacks on the unit or mounted remotely by using coaxial cables. Coaxial cable length should be kept as short as possible (ideally less than 10m) to minimise signal loss.

❗ **IMPORTANT:** All cable and antenna connections must be electrically insulated using self-amalgamating rubber tape.

To ensure EN 60950-1 compliance, AXON Air, the antenna and all cabling must be installed in a location that eliminates the chance of the system being struck by lightning. If an antenna needs to be installed in a location where it could be struck by lightning, then an appropriate lightning arrestor must be placed in-line with the antenna and cabling such that AXON Air is not subject to overvoltages due to lightning.

5.11 Manual Reset and Reboot

The AXON Core switch fabric can be manually reset or the whole device can be loaded with default settings as described below.

Description	Picture
Locate and identify the switch Reset Button (RED). Press and release to reset the switch core	
Description	**Picture**
Locate and identify the Default Factory Settings Button (BLACK). To reset AXON Core to factory default settings, press and hold the button for 5 …15 seconds.	

Chapter 6: Understanding VLANs

Topics:

- Understanding Trunk and Access Ports
- VLANs and Wireless Networks
- Native VLAN

This chapter explains the principles behind a Virtual Local Area Network (VLAN). It is important to understand VLANs to properly configure the network and power distribution module.

A VLAN is a collection of nodes grouped according to their function or application, rather than their physical location. They are grouped in order to separate and prioritise data within a network, as shown in *Figure 14: VLANs.* VLANs are created when multiple applications, such as voice, telemetry, data and video, are required in a mining network.

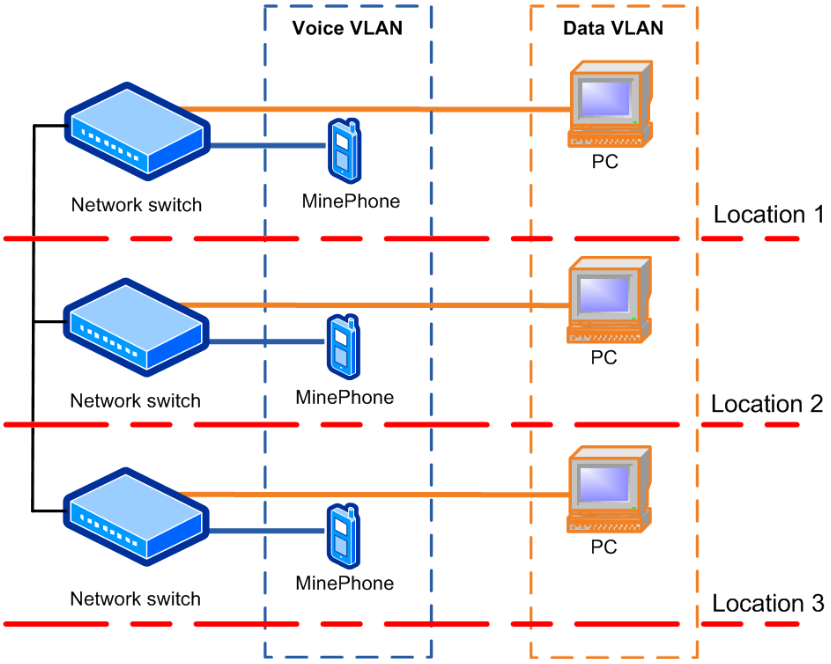


Figure 14: VLANs

6.1 Understanding Trunk and Access Ports

VLANs can be assigned to trunk ports and access ports on a network. These two types of allocation determine how data is transmitted and relayed.

6.1.1 Trunk Ports

Trunk ports typically provide a connection between network switches, and can carry data for multiple VLANs. They will only transmit frames (packets of data) that belong to the port's assigned VLANs. To identify the VLAN of each frame, a network switch adds a tag to the frame (known as 802.1Q trunking). The tag contains the following information:

- **VLAN ID** — allows the network switch receiving a frame to identify the VLAN it belongs to.
- **Priority ID** — allows the network switch to prioritise distribution when multiple frames are being transmitted. Priority ID ranges from 0-7, where 7 is the highest priority.

When a network switch receives a tagged frame, the tag is read to determine the VLAN it belongs to. The tag is removed and distributed to devices connected on the same VLAN.

When the network switch receives multiple frames, it will prioritise the distribution of frames based on the Priority ID in the VLAN ID tag. For more information on configuring VLANs, see Defining VLANs

6.1.2 Access Ports

Access ports connect client devices such as PCs and laptops to the network switch, and can only be assigned to a single VLAN. Access ports can only send and receive untagged frames, with those frames allocated to the relevant VLAN inside the switch. Any tagged frames sent to an access port will be dropped.

An example of VLAN traffic flow through trunk and access ports is shown in *Figure 15: VLAN traffic flow* and described below.

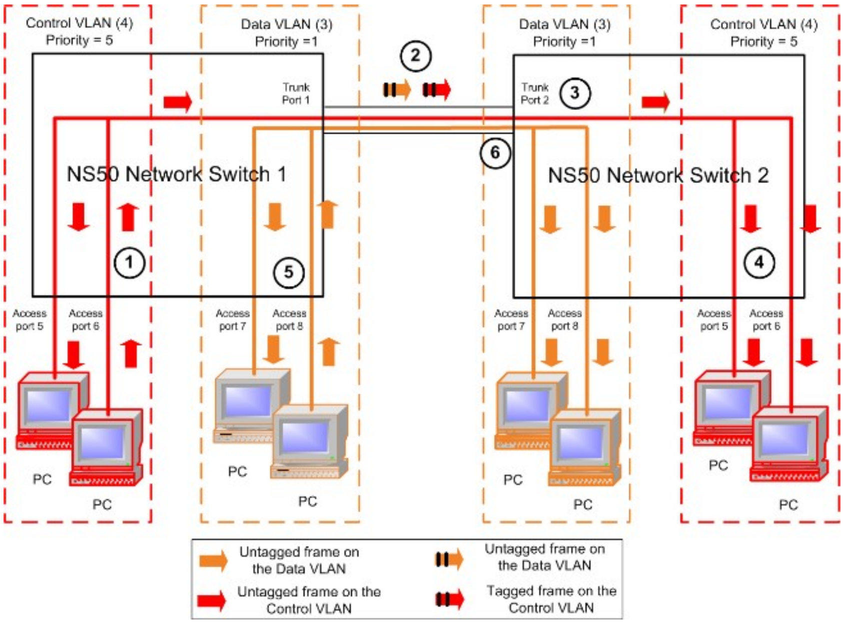


Figure 15: VLAN traffic flow

1. A PC sends an untagged frame into access port 6 (Control VLAN) on network and power distribution module 1. The frame is sent to other access ports on the Control VLAN (access port 5).
2. network and power distribution module 1 tags the frame with VLAN ID = 4 and Priority = 5 and sends it through the trunk ports to network and power distribution module 2.
3. network and power distribution module 2 receives the tagged frame, and identifies the frame belonging to the Control VLAN.
4. network and power distribution module 2 removes the tag and sends the frame to all ports on the Control VLAN (access ports 5 and 7).
5. If network and power distribution module 1 receives multiple frames, they are tagged and sent via trunk ports to network and power distribution module 2.
6. network and power distribution module 2 receives the frames and prioritises distribution.

6.1.3 Port Allocation

Physical ports on AXON Core can be configured to be either a trunk port or access port using the web browser interface or editing site configuration files when Trivial File Transfer Protocol (TFTP) is used. AXON Core default configuration has ports 1-8 allocated as trunk ports . Ports 1-4 are usually connected to other AXON Core units, and ports 5-8 are connected to WAPs or other PoE devices. For more information on configuring ports and VLAN membership, see Configuring the VLAN Port Map

6.2 VLANs and Wireless Networks

The network and power distribution module can have up to four wireless Service Set Identifiers (SSIDs) per WAC. Each SSID is associated with a single VLAN and functions as an access port on that VLAN. An example of a wireless network is shown in *Figure 16: An example of VLAN and wireless networks and described below.*

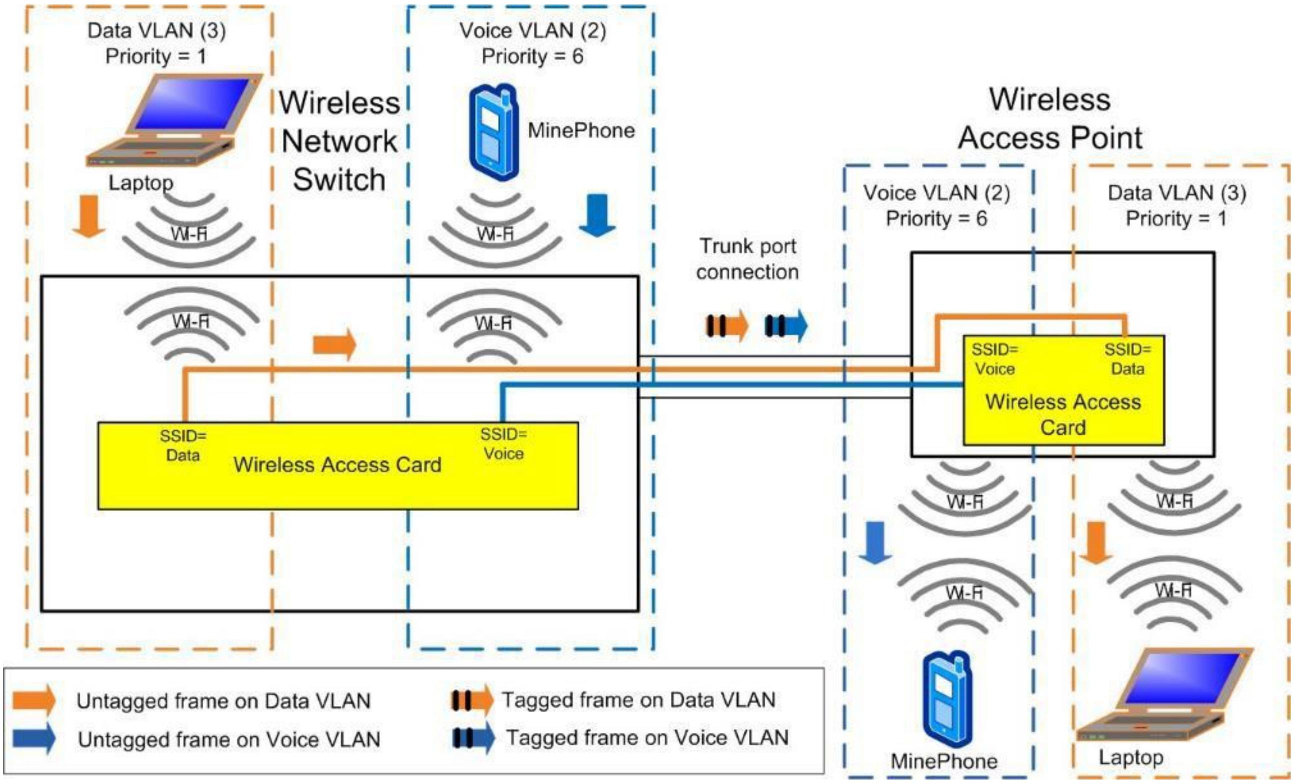


Figure 16: An example of VLAN and wireless networks

1. An untagged frame is sent from a Laptop 1 through a wireless network (SSID = Data) on the network switch.
2. The frame is tagged by the network switch and is sent through the trunk port to the WAP.
3. The WAP identifies the tagged frame as belonging to the Data VLAN and removes the tag.
4. The untagged frame is sent via the wireless network (SSID = Data) to Laptop 2.

6.3 Native VLAN

Trunk ports on the network and power distribution module also support a Native VLAN. The Native VLAN is where untagged frames will be allocated. On the network switch, the native VLAN is always the Infrastructure VLAN. This allows client devices such as PCs or laptops to access and manage the network switch when they are connected via a trunk port.

The Infrastructure VLAN is mandatory in the network switch and cannot be deleted.

An example of native VLAN functionality is illustrated *in Figure 17: An example of native VLAN* and described below.

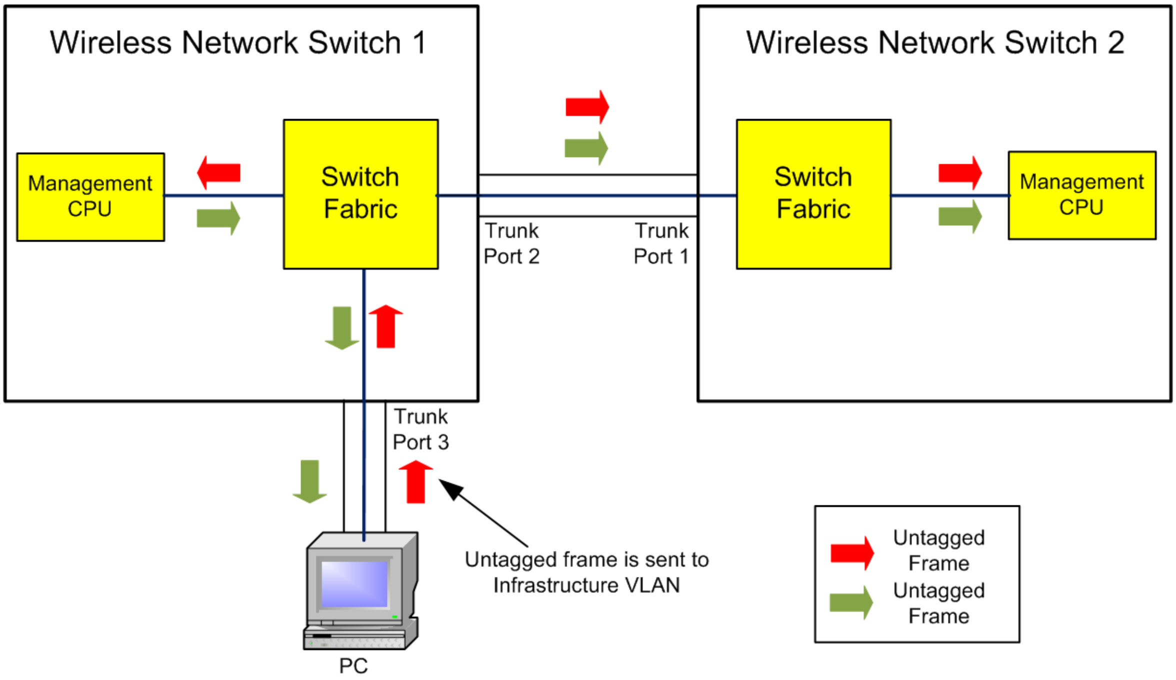


Figure 17: An example of native VLAN

1. The PC sends an untagged frame to Trunk port 3 on network and power distribution module 1.
2. The frame is allocated to the Infrastructure VLAN.
3. The management CPU of network and power distribution module 1 is always an Access port on the Infrastructure VLAN and will receive the frame.
4. The untagged frame would also go to network and power distribution module 2 via the Trunk ports between the network switch units.
5. network and power distribution module 2 allocates the untagged frame to the Infrastructure VLAN.
6. The management CPU of network and power distribution module 2 is always an Access port on the Infrastructure VLAN and will receive the frame.

7. Any frame leaving the Management CPU is placed on the Infrastructure VLAN.
8. All frames on the Infrastructure VLAN are sent out untagged on Trunk ports.

Chapter 7: Configuration Using the Web Interface

Topics:

- Logging in
- Status Tab
- Configuration Tab

This chapter describes how to configure a network device using a web browser. Please note that screenshots may vary slightly from those shown, depending on your current firmware version.

AXON Core and AXON Air have a built-in web-server that is accessible by a PC to configure settings. A PC can access the web browser interface by making a TCP/IP connection to the device. For more information, see Connecting a PC to an Network Device.

The IP address of the network device can be located and configured using the MST Device Scanner tool. For more information on how to use the Device Scanner, see Device Discovery.

7.1 Logging onto the Web Browser Interface

The web browser interface has a login front screen with access at two levels:

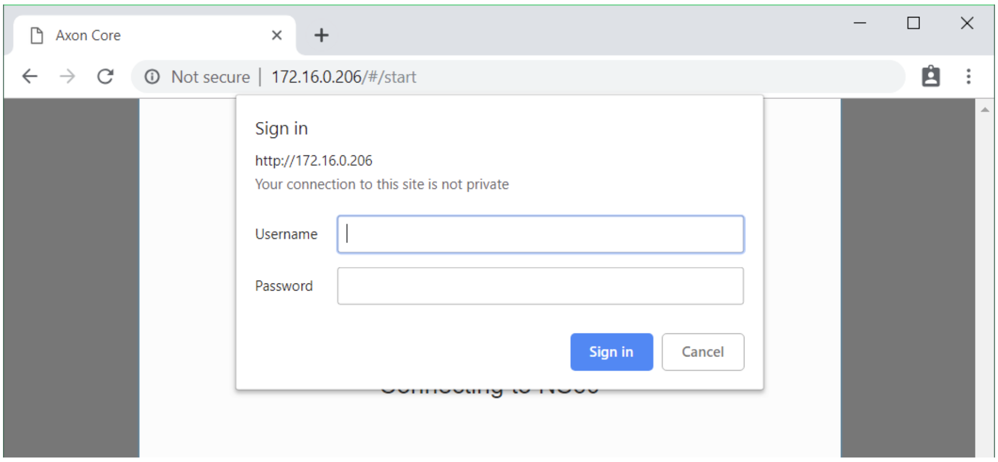
- **ADMIN** — Allows settings to be viewed and modified. The default password is 'admin'.
- **USER** — Allows settings to be viewed but not modified. By default, there is no password.

NOTE:

- By default, AXON Core is configured to use DHCP. To find the IP address of a newly connected device, use the MST Device Scanner.
- Devices running early versions of firmware may default to 192.168.1.100.

To log in to the web browser interface:

1. Launch your web browser and enter **http://<*IP address*>** in the address field.
2. The login screen is displayed.



Sign in

http://172.16.0.206

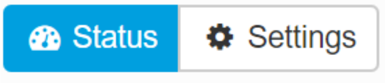
Your connection to this site is not private

Username

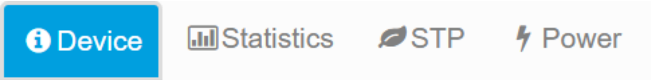
Password

3. In the **Sign in** dialog box, enter **admin** as username and the password. The factory default password is **admin**.
4. Click **Sign In**. The Device Status screen will be displayed.

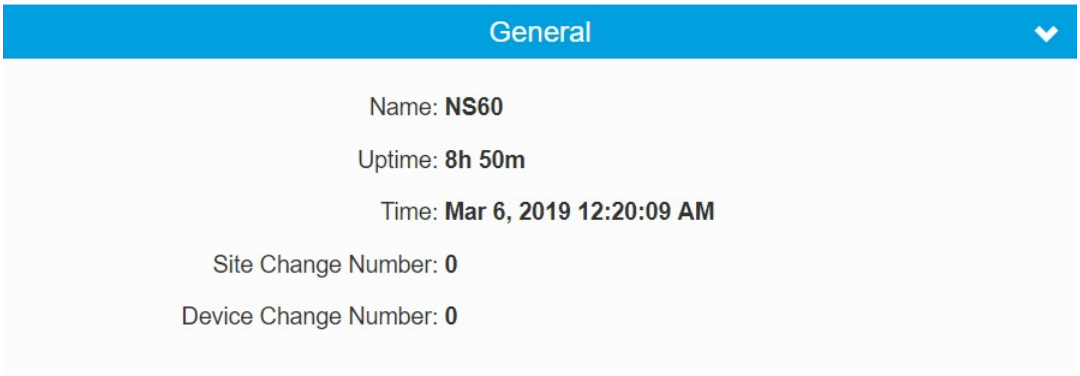
STATUS



1. Device



a. General



Name: **NS60**

Uptime: **8h 50m**

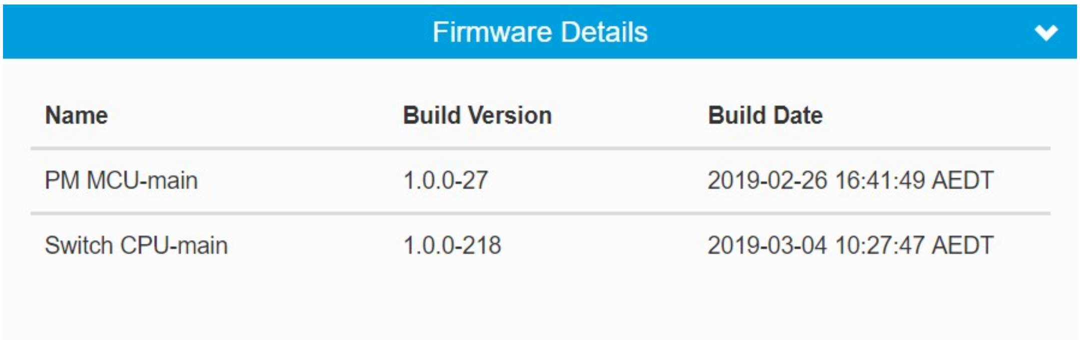
Time: **Mar 6, 2019 12:20:09 AM**

Site Change Number: **0**

Device Change Number: **0**

i. Name – Unique name of the device by which it is known on the network and managements console. OS hostname.
ii. Uptime – Elapsed time since startup
iii. Time – Current time
iv. Site Change Number – Version of the applied site-wide configuration file
v. Device Change Number – Version of the applied device specific configuration file

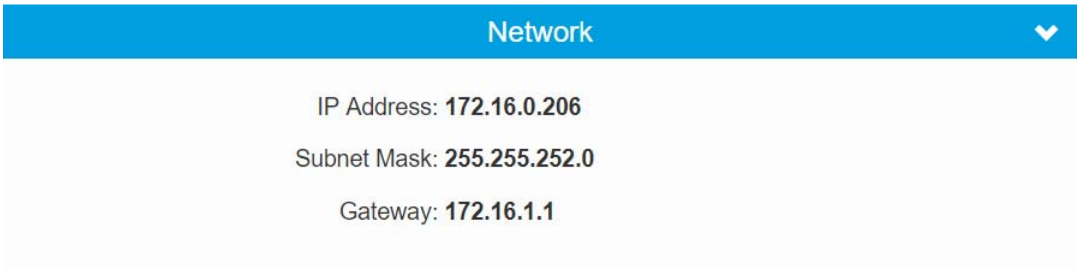
b. Firmware Details



Name	Build Version	Build Date
PM MCU-main	1.0.0-27	2019-02-26 16:41:49 AEDT
Switch CPU-main	1.0.0-218	2019-03-04 10:27:47 AEDT

i. Name – Name of the firmware component
ii. Build version – Unique identifier of the release in the form (major.minor.release-build)

c. Network



Network

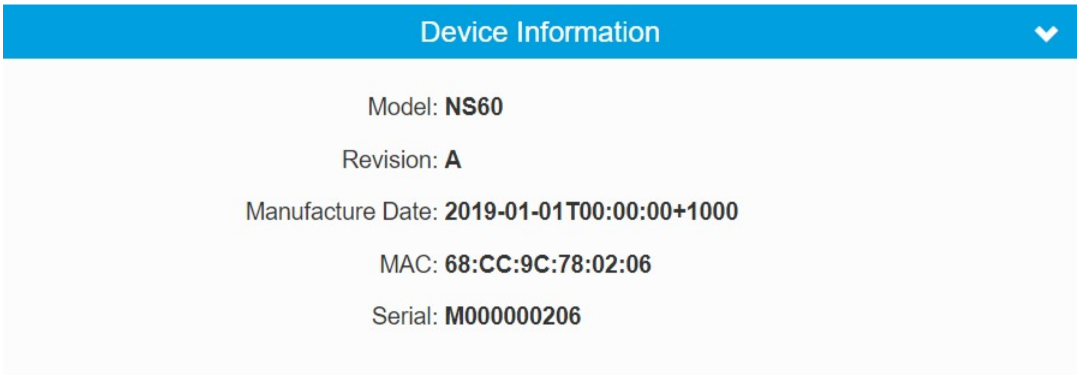
IP Address: **172.16.0.206**

Subnet Mask: **255.255.252.0**

Gateway: **172.16.1.1**

i. IP Address – current management IP address of the device, configured or acquired from DHCP
ii. Subnet mask
iii. Gateway

d. Device Information



Device Information

Model: **NS60**

Revision: **A**

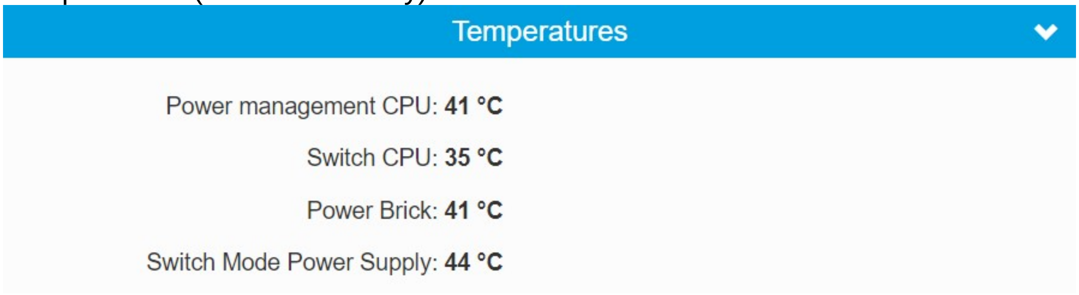
Manufacture Date: **2019-01-01T00:00:00+1000**

MAC: **68:CC:9C:78:02:06**

Serial: **M000000206**

i. Model – Internal MST equipment code
ii. Revision
iii. Manufacture date
iv. MAC
v. Serial

e. Temperatures (AXON Core only)



Temperatures

Power management CPU: **41 °C**

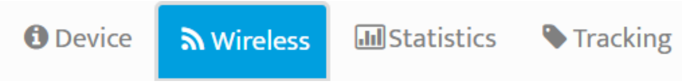
Switch CPU: **35 °C**

Power Brick: **41 °C**

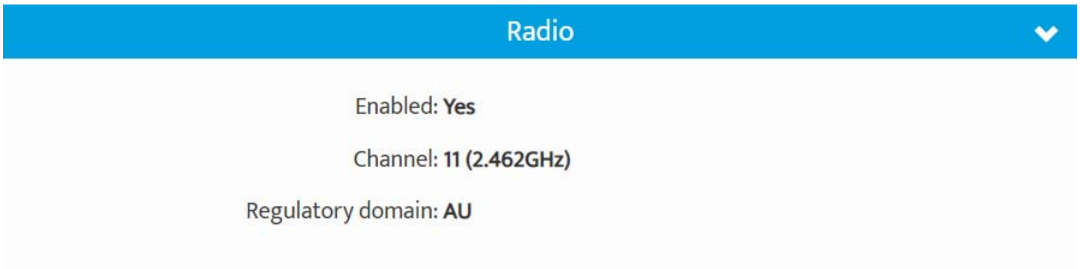
Switch Mode Power Supply: **44 °C**

i. Power management CPU
ii. Switch CPU
iii. Power brick – POE 54V step-up/step-down power supply temperature
iv. Switch mode power supply – 3.3V power supply temperature

2. Wireless (AXON Air only)



a. Radio


Radio

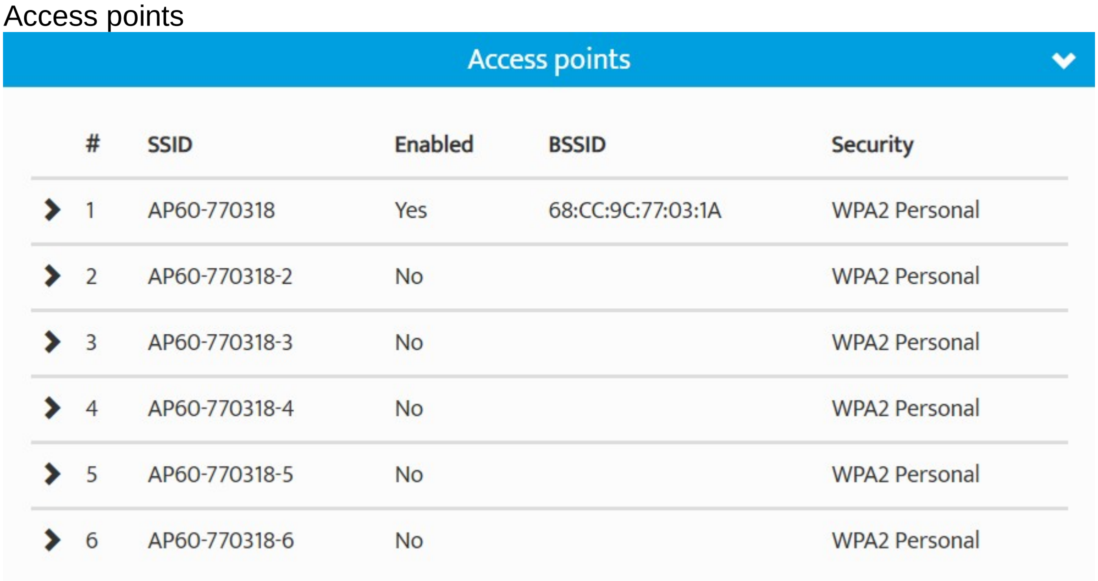
Enabled: **Yes**

Channel: **11 (2.462GHz)**

Regulatory domain: **AU**

1. Enabled – Yes or No
2. Channel – Channel currently in use
3. Regulatory domain – Country code where the device is installed. Determines which channels will be available to comply with local regulation.

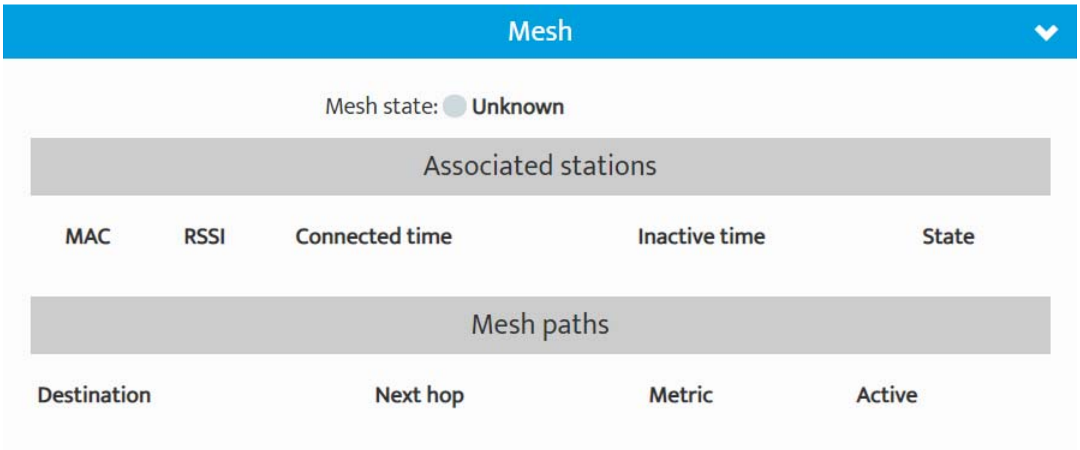
b. Access points


Access points

#	SSID	Enabled	BSSID	Security
1	AP60-770318	Yes	68:CC:9C:77:03:1A	WPA2 Personal
2	AP60-770318-2	No		WPA2 Personal
3	AP60-770318-3	No		WPA2 Personal
4	AP60-770318-4	No		WPA2 Personal
5	AP60-770318-5	No		WPA2 Personal
6	AP60-770318-6	No		WPA2 Personal

1. SSID
2. Enabled
3. BSSID
4. Security

c. Mesh



Mesh state: Unknown

Associated stations

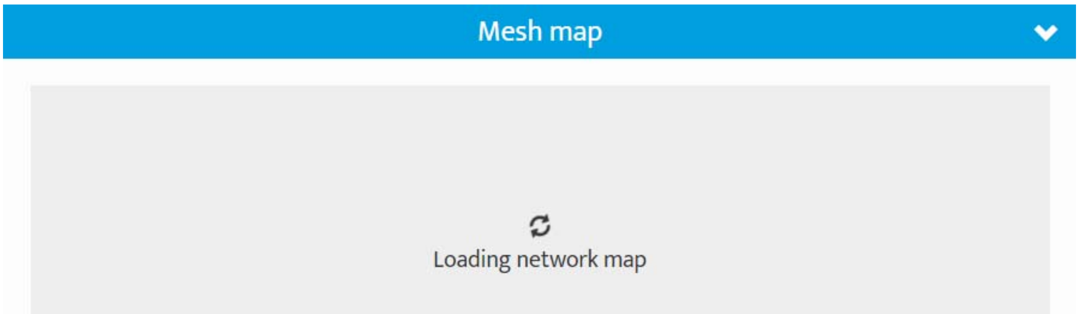
MAC	RSSI	Connected time	Inactive time	State

Mesh paths

Destination	Next hop	Metric	Active

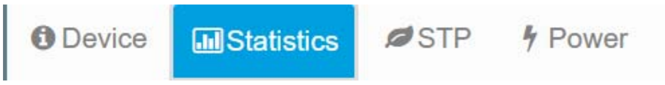
i. Mesh state
ii. Associated stations
iii. Mesh paths

d. Mesh map – displays nodes participating in the mesh with corresponding diagnostic information

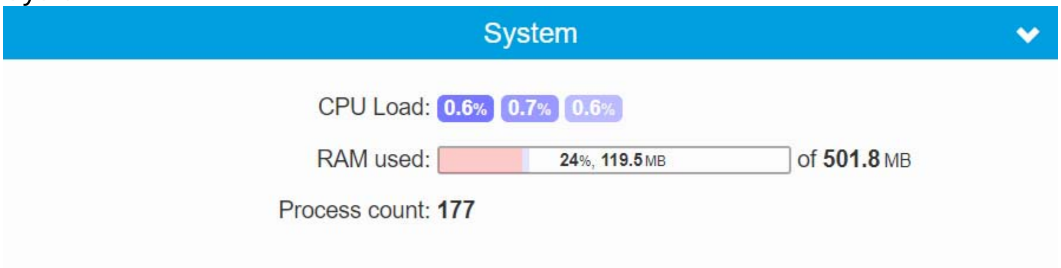


Loading network map

3. Statistics



a. System



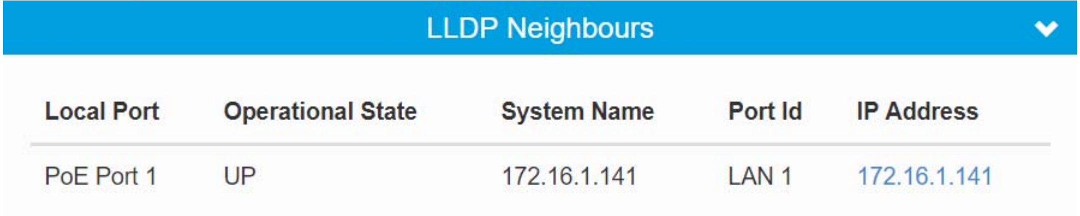
CPU Load: 0.6% 0.7% 0.6%

RAM used: 24%, 119.5 MB of 501.8 MB

Process count: 177

i. CPU load – shows 1 minute, 5 minute and 15 minute CPU load average
ii. RAM used – shows percentage and MB used memory, total available RAM. Mouse over shows free MBs.
iii. Process count

b. LLDP Neighbours – lists all directly connected wired devices

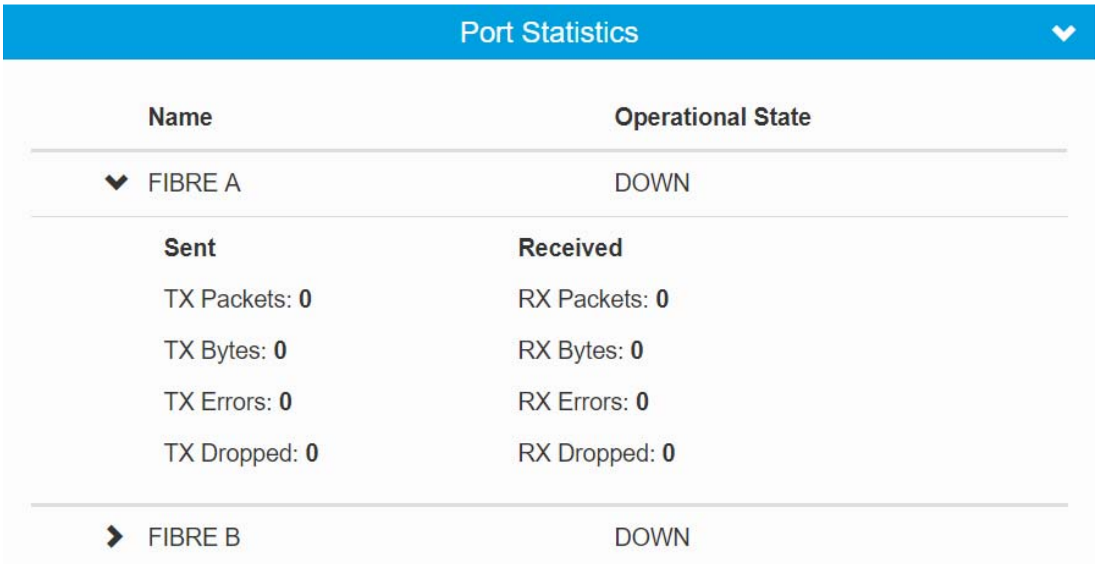


LLDP Neighbours

Local Port	Operational State	System Name	Port Id	IP Address
PoE Port 1	UP	172.16.1.141	LAN 1	172.16.1.141

i. Local port – identifies local port to which a remote device is connected
ii. Operational state – UP or DOWN
iii. System name – the name of the remote host
iv. Port Id –port identifier on the remote system to which the local device is connected
v. IP Address – IP address of the neighbouring device (http link to device management web page)

c. Port Statistics



Port Statistics

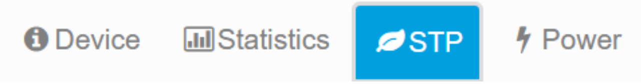
Name	Operational State
FIBRE A	DOWN

Sent	Received
TX Packets: **0**	RX Packets: **0**
TX Bytes: **0**	RX Bytes: **0**
TX Errors: **0**	RX Errors: **0**
TX Dropped: **0**	RX Dropped: **0**

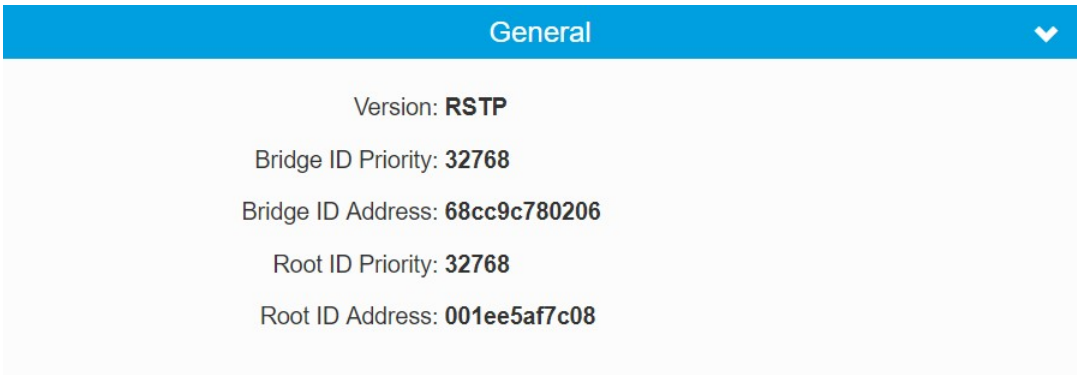
Name	Operational State
FIBRE B	DOWN

i. Name – Local port identifier
ii. Operational state – UP or DOWN
iii. Sent, Received:
    1. TX Packets – number of packets sent and received
    2. TX Bytes – number of bytes sent and received
    3. TX Errors – number of errors sent and received
    4. TX Dropped – number of dropped packets on send and receive

4. STP (AXON Core only)



a. General



Version: **RSTP**

Bridge ID Priority: **32768**

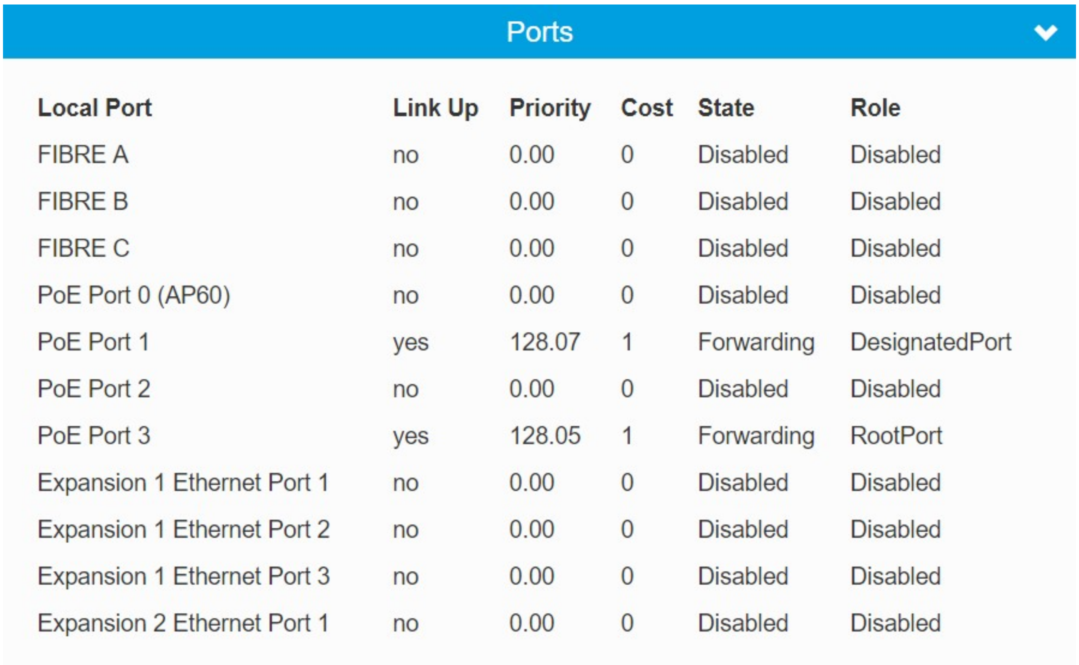
Bridge ID Address: **68cc9c780206**

Root ID Priority: **32768**

Root ID Address: **001ee5af7c08**

i. Version
ii. Bridge ID Priority -
iii. Bridge ID Address
iv. Root ID Priority
v. Root ID Address

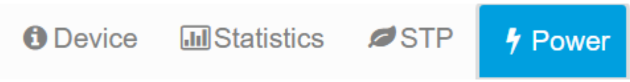
b. Ports



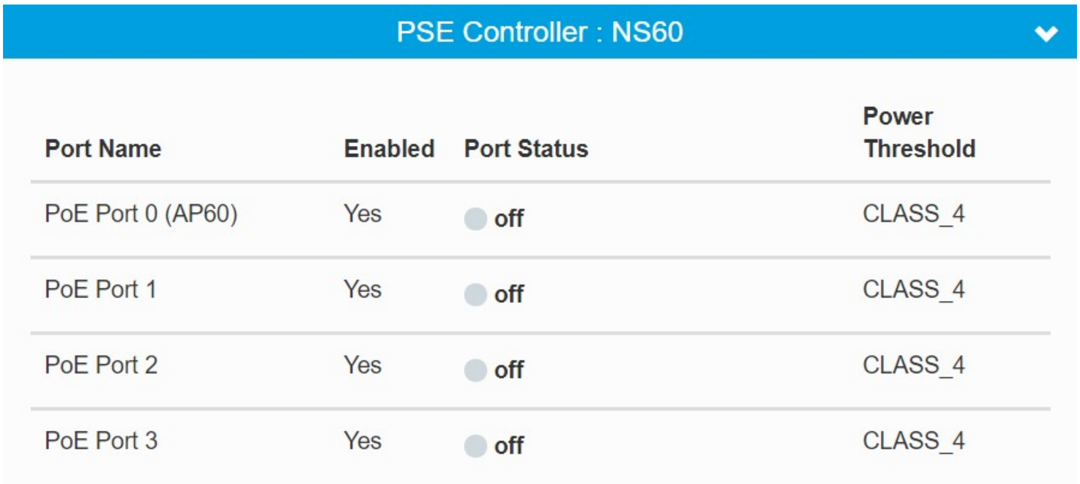
Local Port	Link Up	Priority	Cost	State	Role
FIBRE A	no	0.00	0	Disabled	Disabled
FIBRE B	no	0.00	0	Disabled	Disabled
FIBRE C	no	0.00	0	Disabled	Disabled
PoE Port 0 (AP60)	no	0.00	0	Disabled	Disabled
PoE Port 1	yes	128.07	1	Forwarding	DesignatedPort
PoE Port 2	no	0.00	0	Disabled	Disabled
PoE Port 3	yes	128.05	1	Forwarding	RootPort
Expansion 1 Ethernet Port 1	no	0.00	0	Disabled	Disabled
Expansion 1 Ethernet Port 2	no	0.00	0	Disabled	Disabled
Expansion 1 Ethernet Port 3	no	0.00	0	Disabled	Disabled
Expansion 2 Ethernet Port 1	no	0.00	0	Disabled	Disabled

i. Local Port – port identifier
ii. Link Up – yes/no
iii. Priority –
iv. Cost
v. State – Disable or Forwarding
vi. Role – Disabled, Designated Port or Root Port

5. Power



a. Each Controller

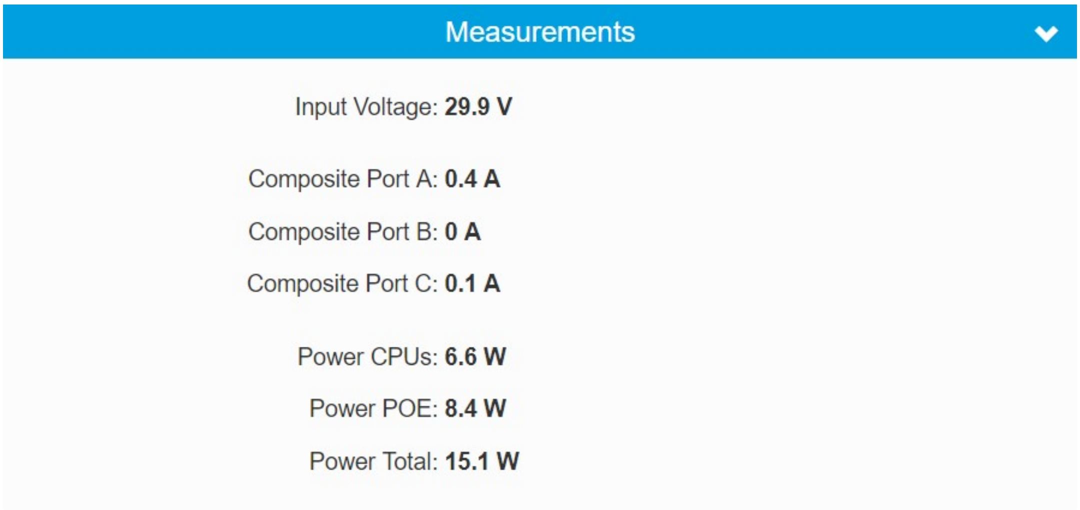


PSE Controller : NS60

Port Name	Enabled	Port Status	Power Threshold
PoE Port 0 (AP60)	Yes	● off	CLASS_4
PoE Port 1	Yes	● off	CLASS_4
PoE Port 2	Yes	● off	CLASS_4
PoE Port 3	Yes	● off	CLASS_4

i. Port Name
ii. Enabled – Yes or No
iii. Port Status – Off (unplugged), Good (plugged in, powered), Failure (tripped, over-current). In case of failure, additional reason for failed status will be shown
iv. Power Threshold – Currently negotiated CLASS for the plugged in device

b. Measurements



Measurements

Input Voltage: **29.9 V**

Composite Port A: **0.4 A**

Composite Port B: **0 A**

Composite Port C: **0.1 A**

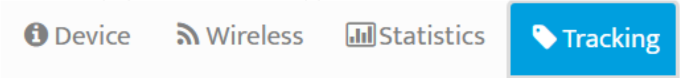
Power CPUs: **6.6 W**

Power POE: **8.4 W**

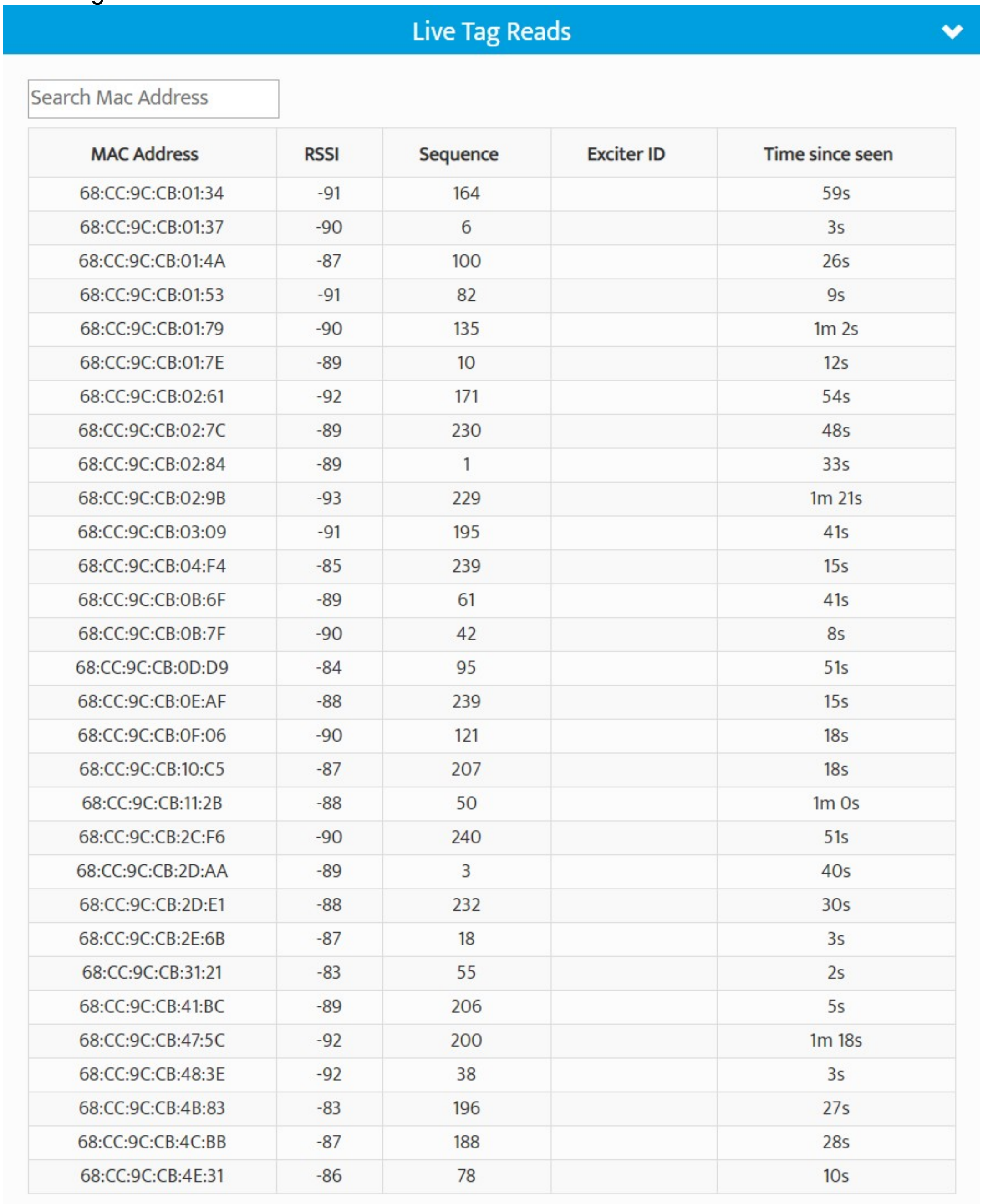
Power Total: **15.1 W**

i. Input Voltage
ii. Composite Port A-C – Current flow through the composite port in Amps. Positive value shows current entering, and negative value shows current leaving the device.
iii. Power CPUs – Current consumption of the management CPU plus the microcontroller
iv. Power POE – Current consumption of all POE devices including voltage step-up / step-down overheads
v. Power Total – Combined total consumption for the whole AXON Core device (CPUs + POE supply).

6. Tracking (AXON Air only)



a. Live Tag Reads



MAC Address	RSSI	Sequence	Exciter ID	Time since seen
68:CC:9C:CB:01:34	-91	164		59s
68:CC:9C:CB:01:37	-90	6		3s
68:CC:9C:CB:01:4A	-87	100		26s
68:CC:9C:CB:01:53	-91	82		9s
68:CC:9C:CB:01:79	-90	135		1m 2s
68:CC:9C:CB:01:7E	-89	10		12s
68:CC:9C:CB:02:61	-92	171		54s
68:CC:9C:CB:02:7C	-89	230		48s
68:CC:9C:CB:02:84	-89	1		33s
68:CC:9C:CB:02:9B	-93	229		1m 21s
68:CC:9C:CB:03:09	-91	195		41s
68:CC:9C:CB:04:F4	-85	239		15s
68:CC:9C:CB:0B:6F	-89	61		41s
68:CC:9C:CB:0B:7F	-90	42		8s
68:CC:9C:CB:0D:D9	-84	95		51s
68:CC:9C:CB:0E:AF	-88	239		15s
68:CC:9C:CB:0F:06	-90	121		18s
68:CC:9C:CB:10:C5	-87	207		18s
68:CC:9C:CB:11:2B	-88	50		1m 0s
68:CC:9C:CB:2C:F6	-90	240		51s
68:CC:9C:CB:2D:AA	-89	3		40s
68:CC:9C:CB:2D:E1	-88	232		30s
68:CC:9C:CB:2E:6B	-87	18		3s
68:CC:9C:CB:31:21	-83	55		2s
68:CC:9C:CB:41:BC	-89	206		5s
68:CC:9C:CB:47:5C	-92	200		1m 18s
68:CC:9C:CB:48:3E	-92	38		3s
68:CC:9C:CB:4B:83	-83	196		27s
68:CC:9C:CB:4C:BB	-87	188		28s
68:CC:9C:CB:4E:31	-86	78		10s

i. Search Mac Address – type part of the tag MAC address to filter the list
ii. MAC Address – shows the MAC address of the tag recognised
iii. RSSI – Relative Signal Strength Index – the value in dB of the signal strength received

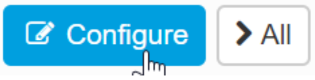
iv. Sequence – the sequence number of the frame broadcast by the tag. Keeps increasing by one with each ‘chirp’ (chirp period is configurable on the tag)

v. Exciter ID – In addition to periodically broadcasting a frame, tags can also broadcast when excited by the vicinity of an exciter in which case the exciter ID will be shown

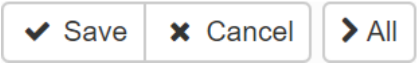
vi. Time since seen – time elapsed since the last time a signal from the tag was received

SETTINGS

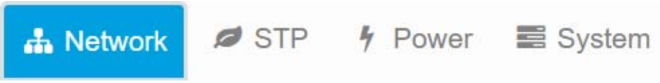
All pages are showing currently configured values. To modify, use Configure button to enter edit mode



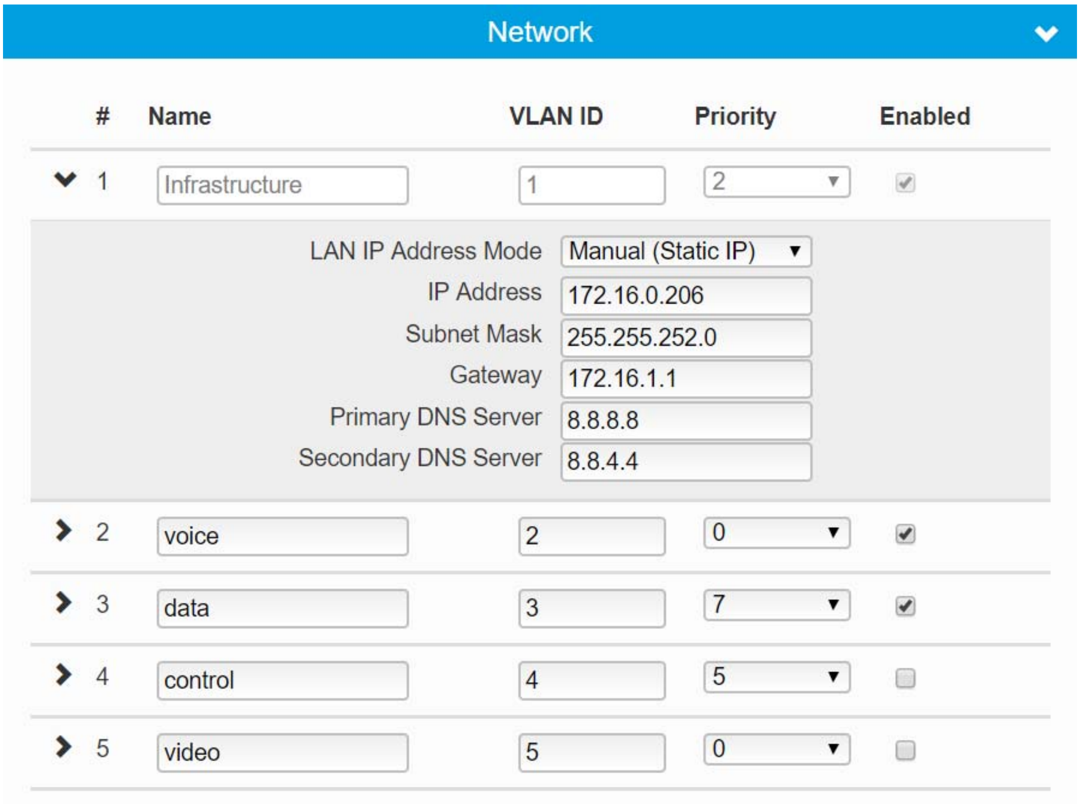
and Save or Cancel to finish.



1. Network



a. Network

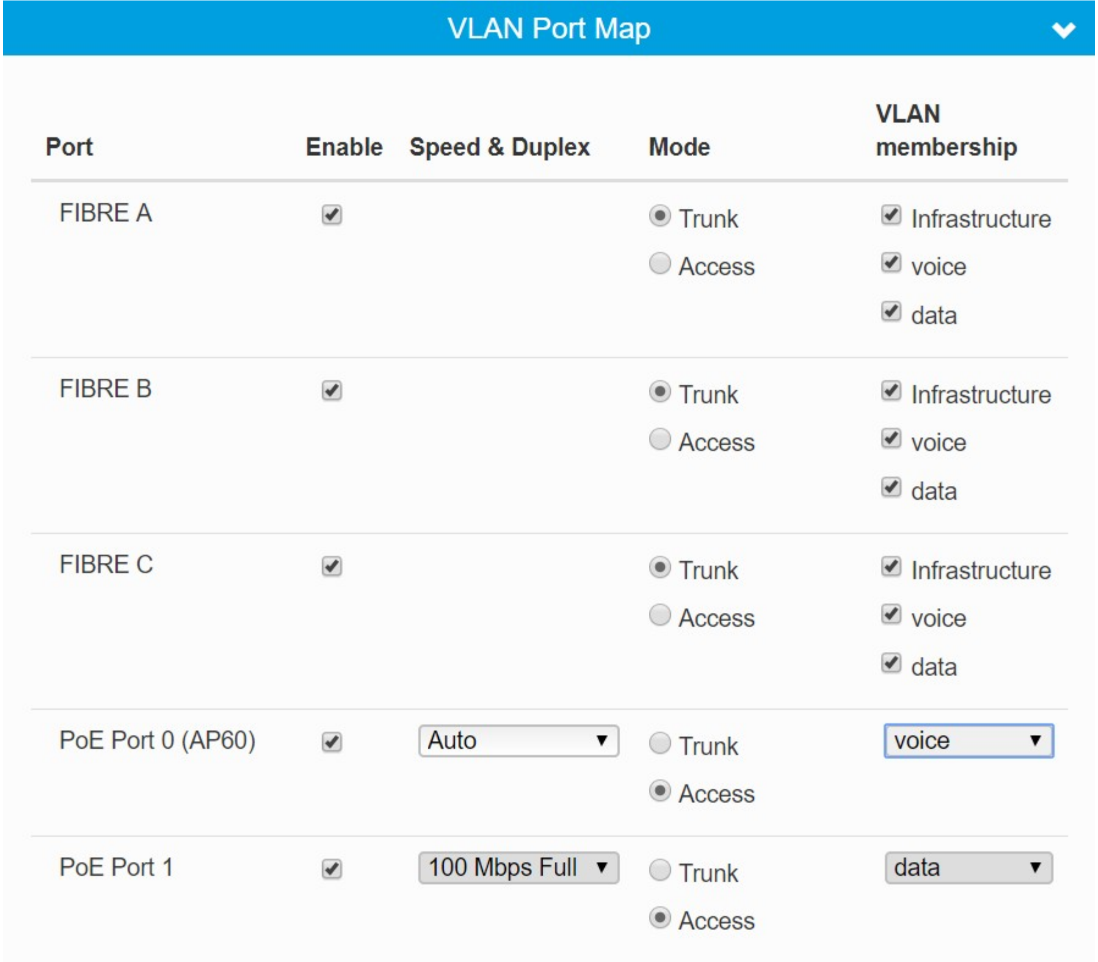


#	Name	VLAN ID	Priority	Enabled
1	Infrastructure	1	2	☑
2	voice	2	0	☑
3	data	3	7	☑
4	control	4	5	☐
5	video	5	0	☐

LAN IP Address Mode: Manual (Static IP)
IP Address: 172.16.0.206
Subnet Mask: 255.255.252.0
Gateway: 172.16.1.1
Primary DNS Server: 8.8.8.8
Secondary DNS Server: 8.8.4.4

i. Name – Descriptive name for easier management (e.g. Infrastructure, Voice, Data, etc.)
ii. VLAN ID – Unique VLAN TAG ID between 1 and 4095
iii. Priority – Value 0 to 7
iv. Enabled – Yes or No

b. VLAN Port Map – Allows port configuration and assigning ports to VLANs

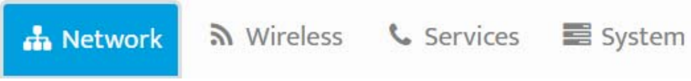


VLAN Port Map

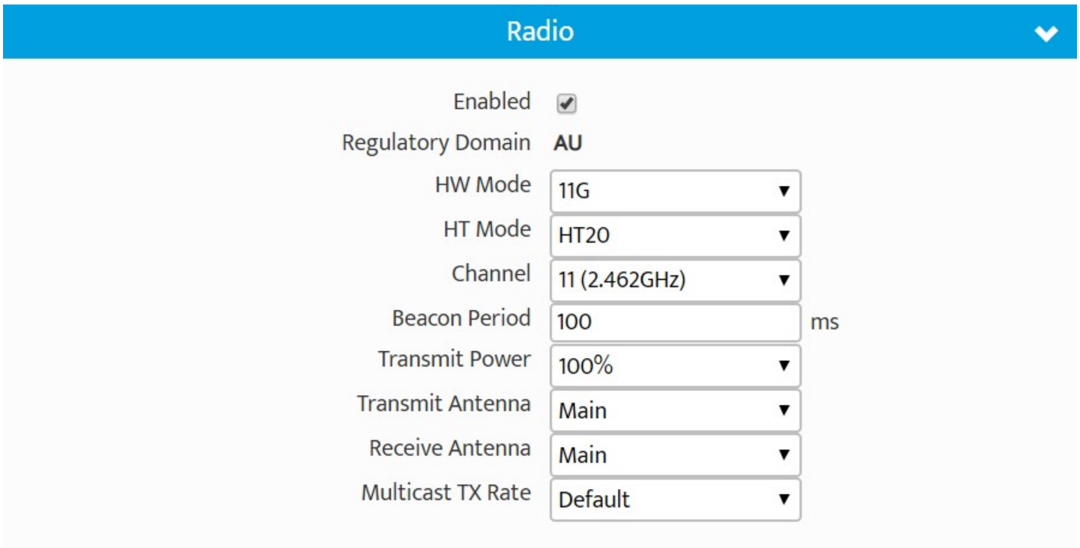
Port	Enable	Speed & Duplex	Mode	VLAN membership
FIBRE A	☑		● Trunk ○ Access	☑ Infrastructure ☑ voice ☑ data
FIBRE B	☑		● Trunk ○ Access	☑ Infrastructure ☑ voice ☑ data
FIBRE C	☑		● Trunk ○ Access	☑ Infrastructure ☑ voice ☑ data
PoE Port 0 (AP60)	☑	Auto ▾	○ Trunk ● Access	voice ▾
PoE Port 1	☑	100 Mbps Full ▾	○ Trunk ● Access	data ▾

i. Port – Local port identifier (Fibre, PoE, Expansion, …)
ii. Enable – Yes or No
iii. Speed & Duplex – Data transfer speeds and Half/Full duplex settings. Default: Auto negotiated.
iv. Mode: Trunk or Access – Traffic send and received from Trunk will contain VLAN tags, traffic on Access port not contain VLAN frames. See VLAN configuration tutorial.

2. Wireless (AXON Air only)

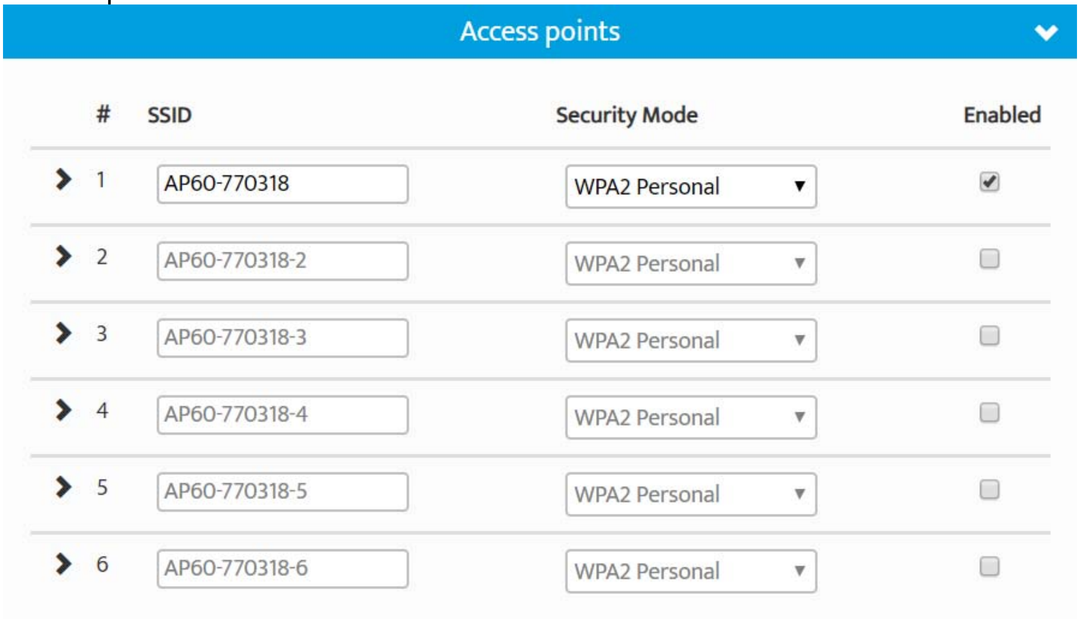


a. Radio



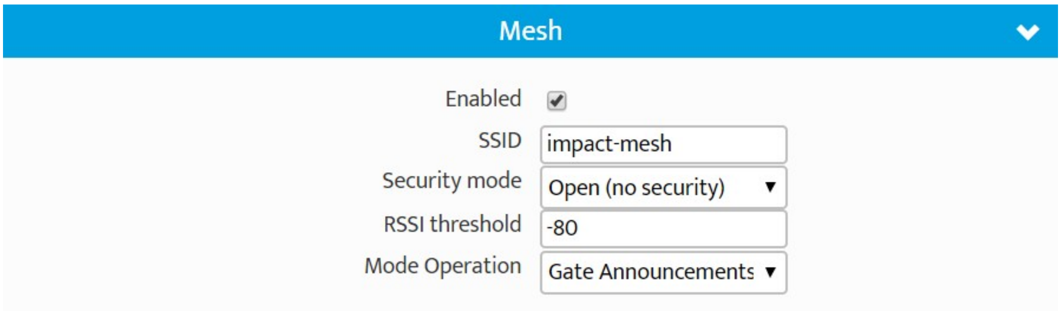
Enabled	☑
Regulatory Domain	**AU**
HW Mode	11G ▼
HT Mode	HT20 ▼
Channel	11 (2.462GHz) ▼
Beacon Period	100 ms
Transmit Power	100% ▼
Transmit Antenna	Main ▼
Receive Antenna	Main ▼
Multicast TX Rate	Default ▼

b. Access points



#	SSID	Security Mode	Enabled
1	AP60-770318	WPA2 Personal ▼	☑
2	AP60-770318-2	WPA2 Personal ▼	□
3	AP60-770318-3	WPA2 Personal ▼	□
4	AP60-770318-4	WPA2 Personal ▼	□
5	AP60-770318-5	WPA2 Personal ▼	□
6	AP60-770318-6	WPA2 Personal ▼	□

c. Mesh

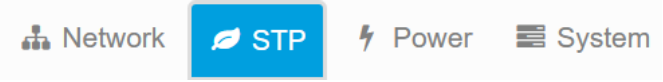


Enabled	☑
SSID	impact-mesh
Security mode	Open (no security) ▼
RSSI threshold	-80
Mode Operation	Gate Announcements ▼

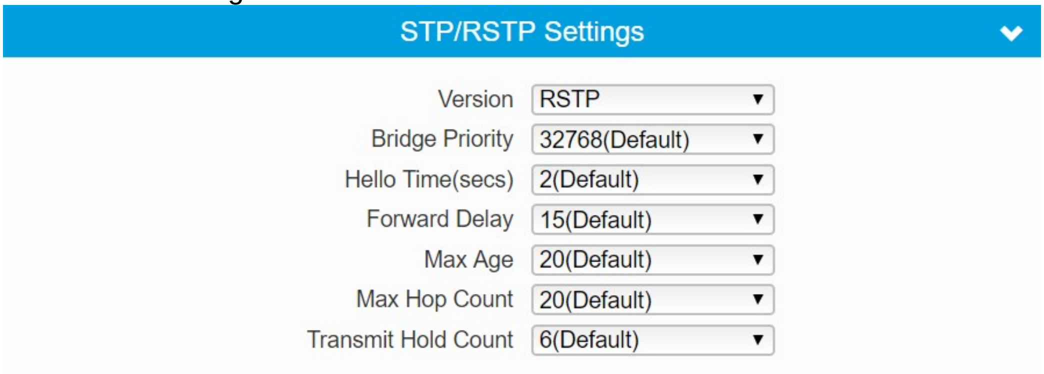
i. Enabled – Yes or No

ii. SSID – The SSID of the mesh network
iii. Security mode – Open (no security) or SAE
iv. Pre-shared key – Password for SAE security
v. RSSI threshold –
vi. Mode operation – None, Gate Announcements or Path Requests & Replies

3. STP (AXON Core only)



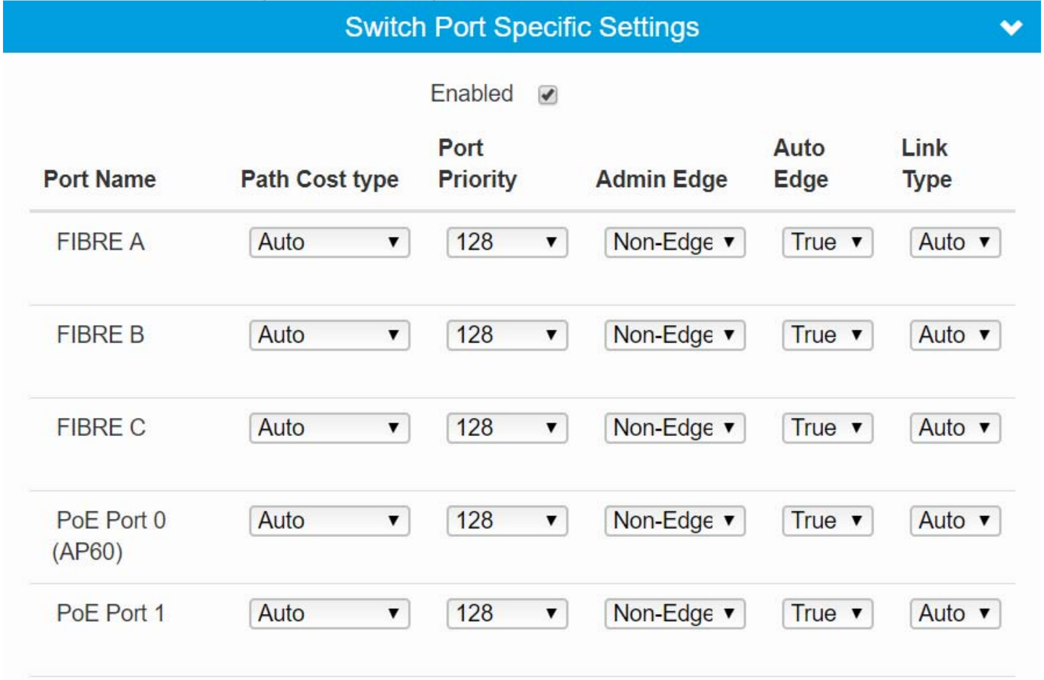
a. STP/RSTP Settings


STP/RSTP Settings

Version	RSTP
Bridge Priority	32768(Default)
Hello Time(secs)	2(Default)
Forward Delay	15(Default)
Max Age	20(Default)
Max Hop Count	20(Default)
Transmit Hold Count	6(Default)

i. Version
ii. Bridge priority
iii. Hello Time
iv. Forward Delay
v. Max Age
vi. Max Hop Count
vii. Transmit Hold Count

b. Switch Port Specific Settings

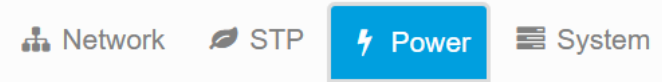

Switch Port Specific Settings

Enabled ☑

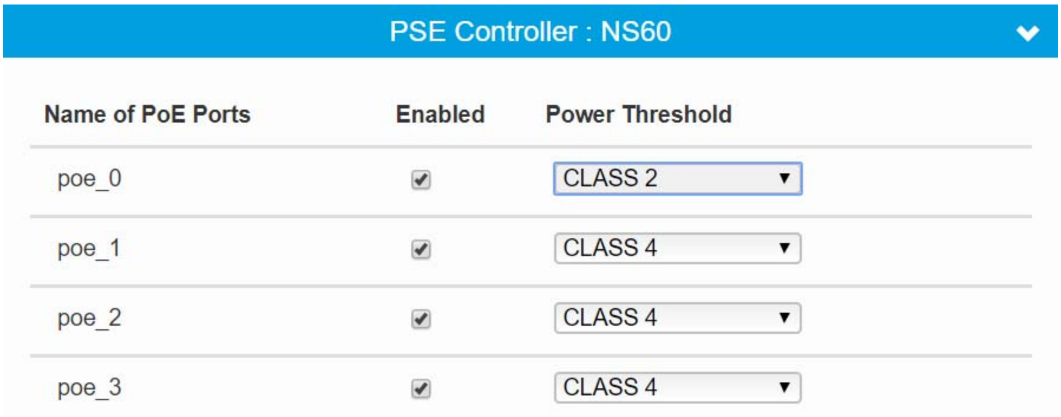
Port Name	Path Cost type	Port Priority	Admin Edge	Auto Edge	Link Type
FIBRE A	Auto	128	Non-Edge	True	Auto
FIBRE B	Auto	128	Non-Edge	True	Auto
FIBRE C	Auto	128	Non-Edge	True	Auto
PoE Port 0 (AP60)	Auto	128	Non-Edge	True	Auto
PoE Port 1	Auto	128	Non-Edge	True	Auto

i. Port Name
ii. Path Cost type
iii. Port Priority
iv. Admin Edge
v. Auto Edge
vi. Link Type

4. Power



a. Each Controller

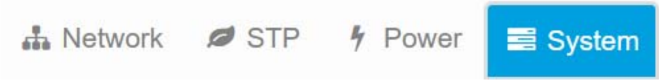


PSE Controller : NS60

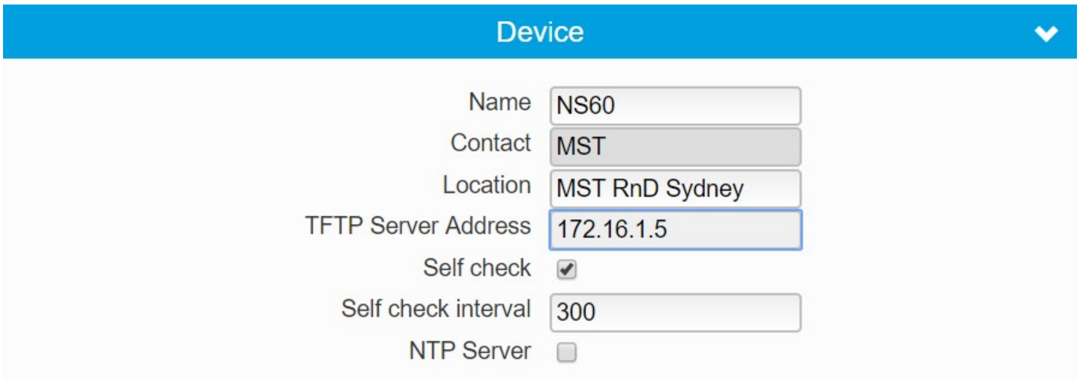
Name of PoE Ports	Enabled	Power Threshold
poe_0	☑	CLASS 2
poe_1	☑	CLASS 4
poe_2	☑	CLASS 4
poe_3	☑	CLASS 4

i. Port Name
ii. Enabled
iii. Power Threshold – Configured maximum allowed power CLASS for the connected device. Higher class allows more power consumption. Use lower class to limit power usage and protect the network.

5. System



a. Device



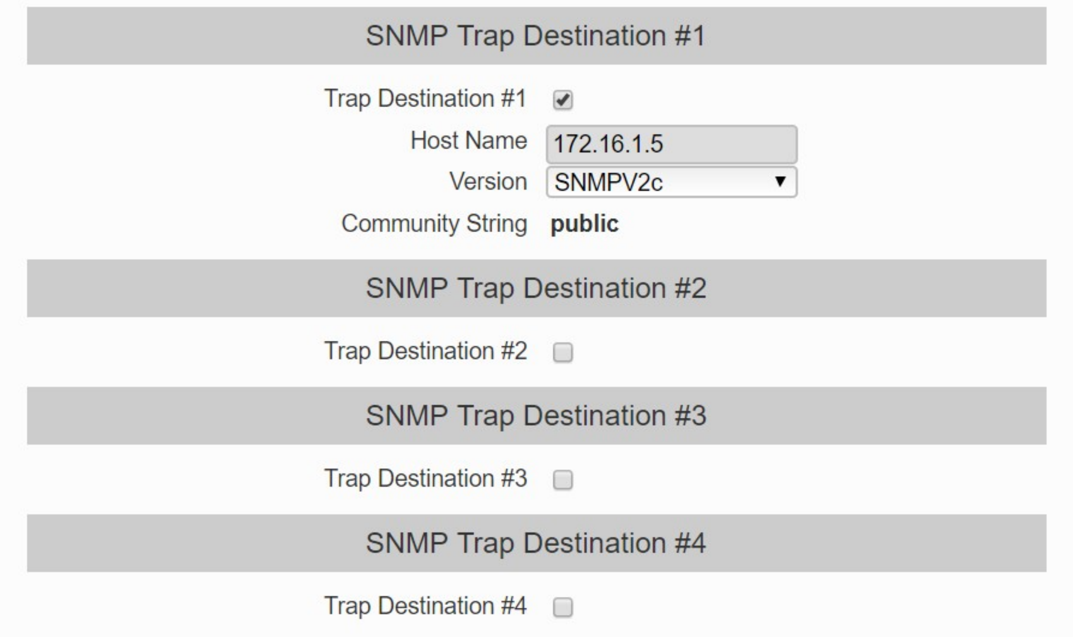
Device

Name	NS60
Contact	MST
Location	MST RnD Sydney
TFTP Server Address	172.16.1.5
Self check	☑
Self check interval	300
NTP Server	□

i. Name – Device hostname by which it is identified on the network and in the ICA management system

ii. Contact – Person responsible, published via SNMP
iii. Location – Device location, published via SNMP
iv. TFTP Server Address – Name or IP address of the central management server which published site-wide and device-specific configuration via TFTP protocol. Usually IP address of ICA.
v. Self check – When enabled, the system periodically contacts TFTP server for updated site and device configuration
vi. Self check interval – number of seconds between configuration update attempts. Applicable when self check enabled.
vii. NTP server – name or IP address of network time protocol server. Used to keep clock accurate. Hint: https://www.ntppool.org/ or IP address of ICA.

b. SNMP Destinations



SNMP Trap Destination #1

Trap Destination #1 ☑
Host Name 172.16.1.5
Version SNMPV2c
Community String **public**

SNMP Trap Destination #2

Trap Destination #2 □

SNMP Trap Destination #3

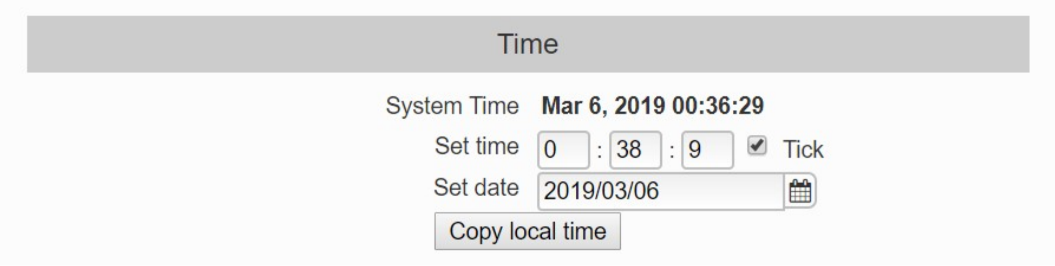
Trap Destination #3 □

SNMP Trap Destination #4

Trap Destination #4 □

i. Enabled
ii. Host name – Name or IP address of host designated to receive SNMP events from this device. Usually an OpenNms service on ICA server.
iii. Version – SNMP protocol version to use. V1 is old and insecure. V2 most widely used, password protected. V3 rather painful to setup, secure.
iv. Community string is always ‘public’, not configurable.

c. Time

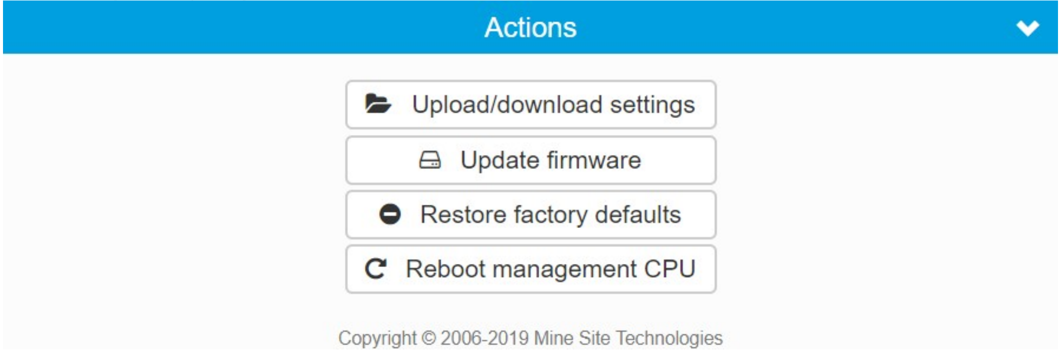


Time

System Time **Mar 6, 2019 00:36:29**
Set time 0 : 38 : 9 ☑ Tick
Set date 2019/03/06

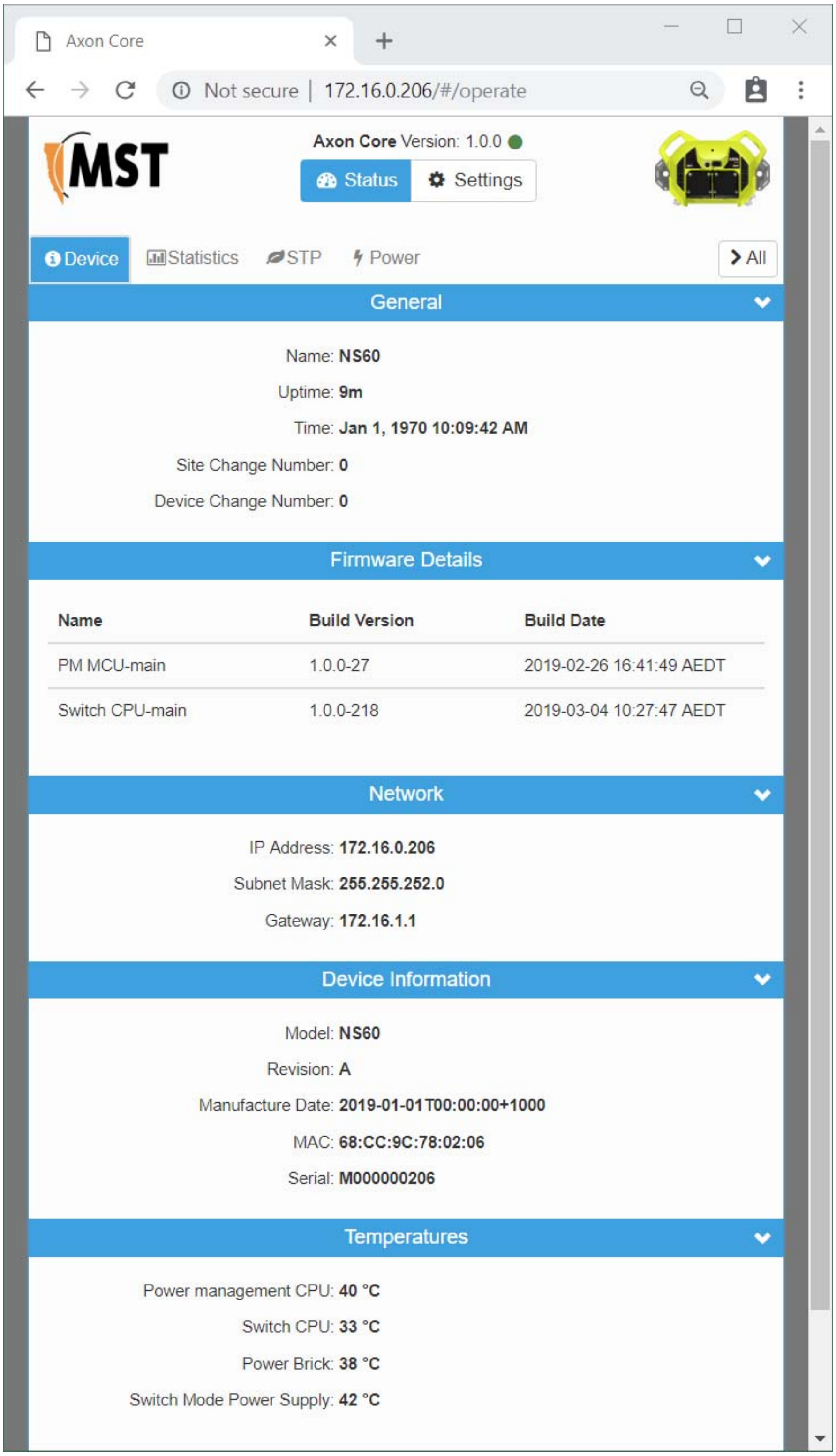
i. Allows configuring device system time. Use tick option to keep updating while waiting to apply. Use 'Copy local time' to use the computer time of the system running the browser session. For best result, use NTP option described above.

d. Actions (Configure)



7.2 Status Screen

After logging on, the **Status** > **Device** screen is displayed by default as shown in



General

Name: NS60

Uptime: 9m

Time: Jan 1, 1970 10:09:42 AM

Site Change Number: 0

Device Change Number: 0

Firmware Details

Name	Build Version	Build Date
PM MCU-main	1.0.0-27	2019-02-26 16:41:49 AEDT
Switch CPU-main	1.0.0-218	2019-03-04 10:27:47 AEDT

Network

IP Address: 172.16.0.206

Subnet Mask: 255.255.252.0

Gateway: 172.16.1.1

Device Information

Model: NS60

Revision: A

Manufacture Date: 2019-01-01T00:00:00+1000

MAC: 68:CC:9C:78:02:06

Serial: M000000206

Temperatures

Power management CPU: 40 °C

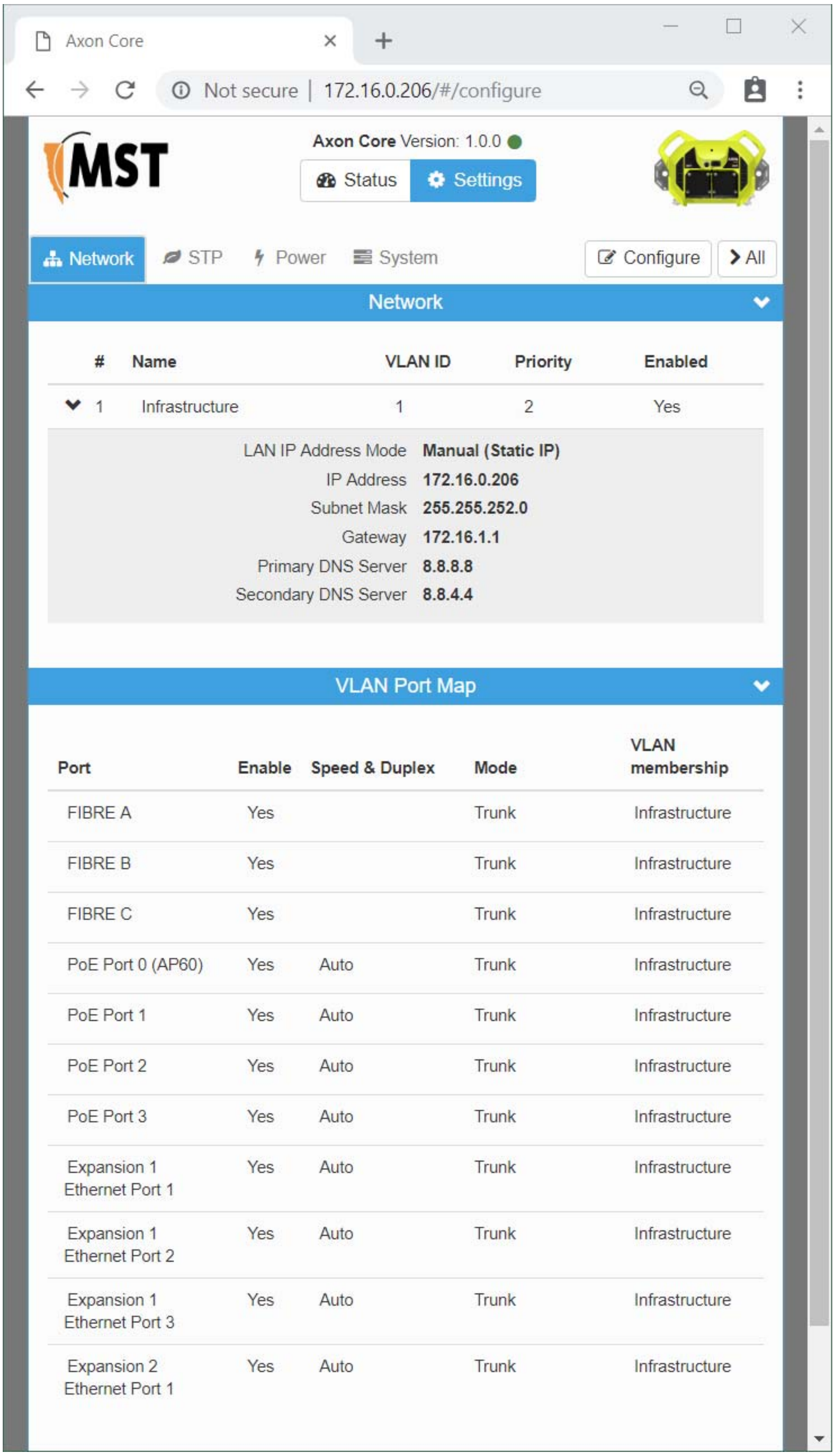
Switch CPU: 33 °C

Power Brick: 38 °C

Switch Mode Power Supply: 42 °C

Figure 1 Default status screen. This screen will be covered later in the chapter.

7.2 Configuration Screen



Axon Core Version: 1.0.0 ●

Network

	#	Name	VLAN ID	Priority	Enabled
⌄	1	Infrastructure	1	2	Yes

LAN IP Address Mode	**Manual (Static IP)**
IP Address	**172.16.0.206**
Subnet Mask	**255.255.252.0**
Gateway	**172.16.1.1**
Primary DNS Server	**8.8.8.8**
Secondary DNS Server	**8.8.4.4**

VLAN Port Map

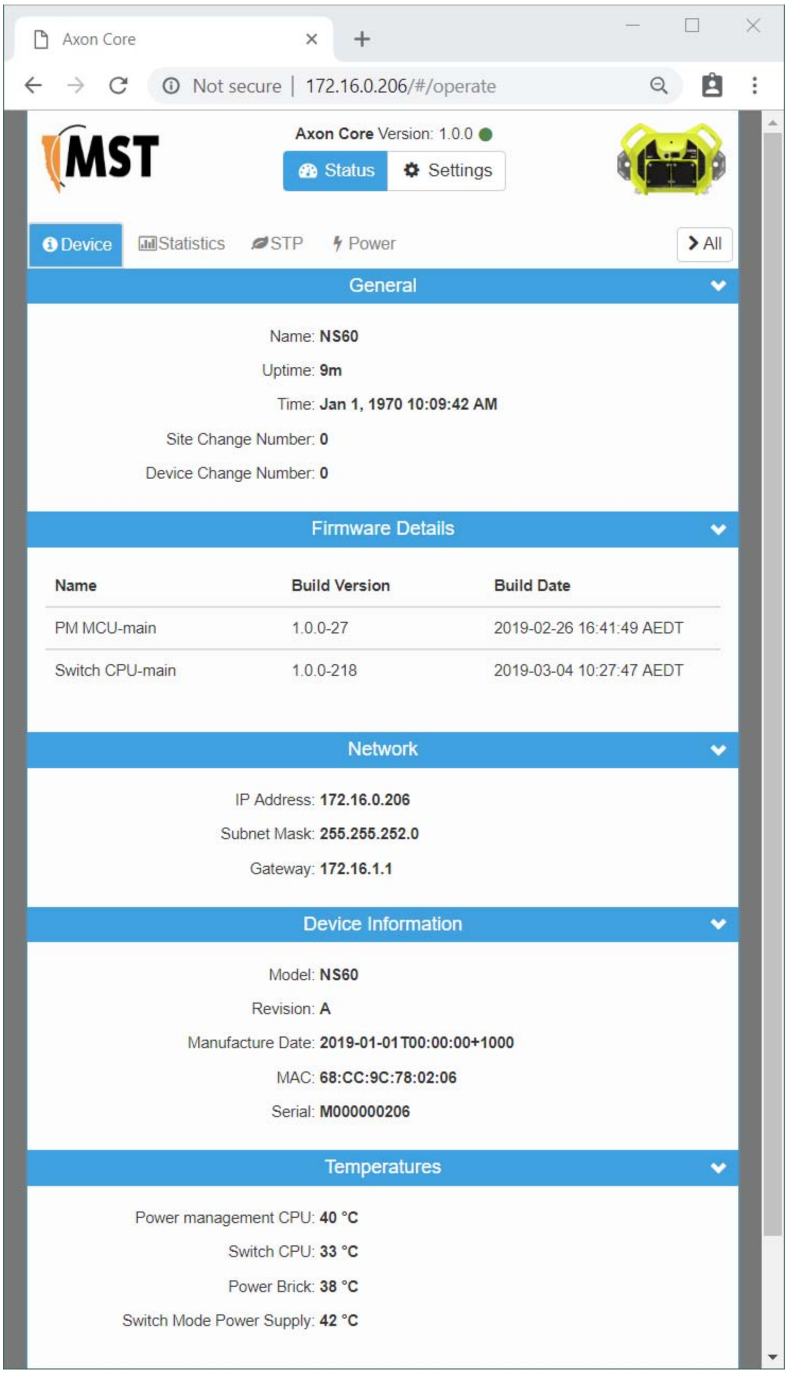
Port	Enable	Speed & Duplex	Mode	VLAN membership
FIBRE A	Yes		Trunk	Infrastructure
FIBRE B	Yes		Trunk	Infrastructure
FIBRE C	Yes		Trunk	Infrastructure
PoE Port 0 (AP60)	Yes	Auto	Trunk	Infrastructure
PoE Port 1	Yes	Auto	Trunk	Infrastructure
PoE Port 2	Yes	Auto	Trunk	Infrastructure
PoE Port 3	Yes	Auto	Trunk	Infrastructure
Expansion 1 Ethernet Port 1	Yes	Auto	Trunk	Infrastructure
Expansion 1 Ethernet Port 2	Yes	Auto	Trunk	Infrastructure
Expansion 1 Ethernet Port 3	Yes	Auto	Trunk	Infrastructure
Expansion 2 Ethernet Port 1	Yes	Auto	Trunk	Infrastructure

Figure 18: Default configuration screen

7.3 Status Tab

7.3.1 Obtaining Device Information

The **Device Info** status screen as shown in *Figure 19: Device Info Status screen* displays system time, firmware version, LAN and wireless LAN summary information.



General

Name: NS60
Uptime: 9m
Time: Jan 1, 1970 10:09:42 AM
Site Change Number: 0
Device Change Number: 0

Firmware Details

Name	Build Version	Build Date
PM MCU-main	1.0.0-27	2019-02-26 16:41:49 AEDT
Switch CPU-main	1.0.0-218	2019-03-04 10:27:47 AEDT

Network

IP Address: 172.16.0.206
Subnet Mask: 255.255.252.0
Gateway: 172.16.1.1

Device Information

Model: NS60
Revision: A
Manufacture Date: 2019-01-01T00:00:00+1000
MAC: 68:CC:9C:78:02:06
Serial: M000000206

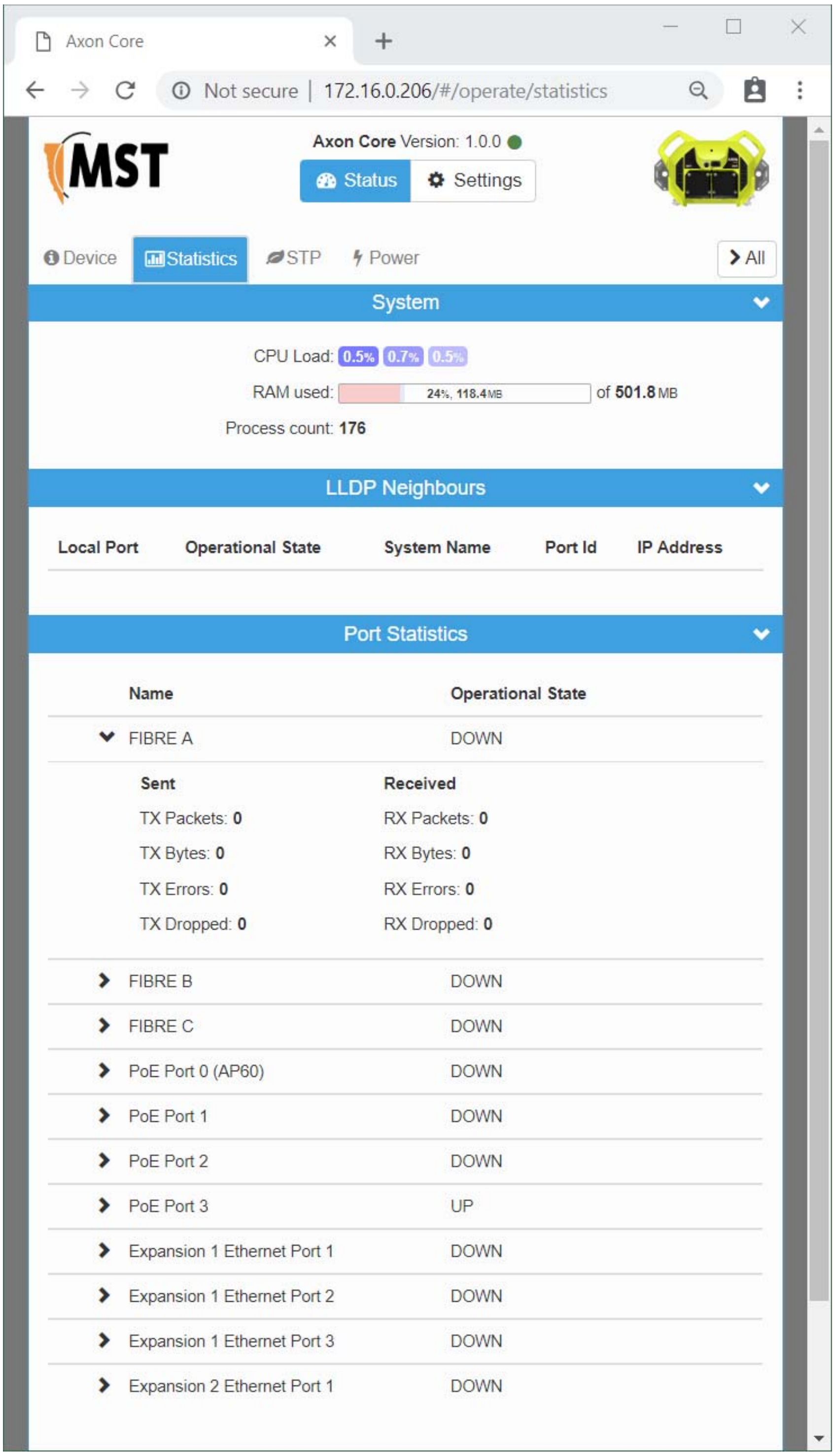
Temperatures

Power management CPU: 40 °C
Switch CPU: 33 °C
Power Brick: 38 °C
Switch Mode Power Supply: 42 °C

Figure 19: Device Info Status screen

7.3.4 Viewing Network Traffic Statistics

The **Statistics** status screen provides network traffic statistics for each network port and for AXON Air each wireless SSID. It shows the number of received and transmitted packets and bytes as well as number of errors and dropped packets.



Axon Core Version: 1.0.0

System

CPU Load: 0.5% 0.7% 0.5%

RAM used: 24%, 118.4MB of 501.8MB

Process count: 176

LLDP Neighbours

Local Port	Operational State	System Name	Port Id	IP Address

Port Statistics

Name	Operational State
FIBRE A	DOWN

Sent	Received
TX Packets: 0	RX Packets: 0
TX Bytes: 0	RX Bytes: 0
TX Errors: 0	RX Errors: 0
TX Dropped: 0	RX Dropped: 0

Name	Operational State
FIBRE B	DOWN
FIBRE C	DOWN
PoE Port 0 (AP60)	DOWN
PoE Port 1	DOWN
PoE Port 2	DOWN
PoE Port 3	UP
Expansion 1 Ethernet Port 1	DOWN
Expansion 1 Ethernet Port 2	DOWN
Expansion 1 Ethernet Port 3	DOWN
Expansion 2 Ethernet Port 1	DOWN

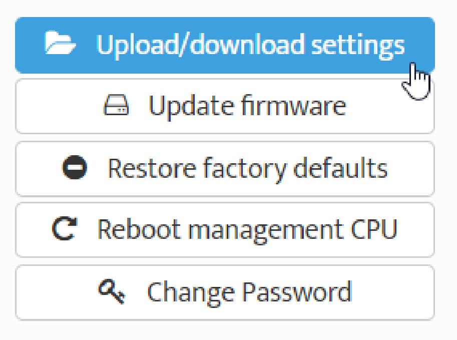
Figure 22: Statistics status screen

7.4 Settings > System > Actions

7.4.1 Upload/download settings

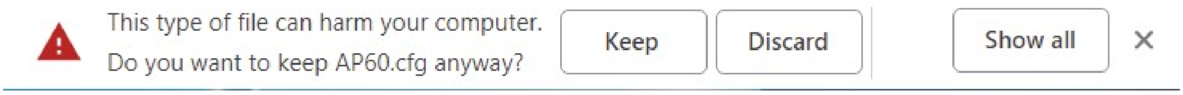
Saving and Restoring Configuration Settings

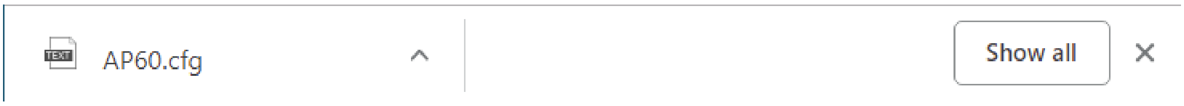
The **System** configuration screen allows network switch settings to be saved as a .cfg file. Saved configuration files can be used to restore settings to the device.



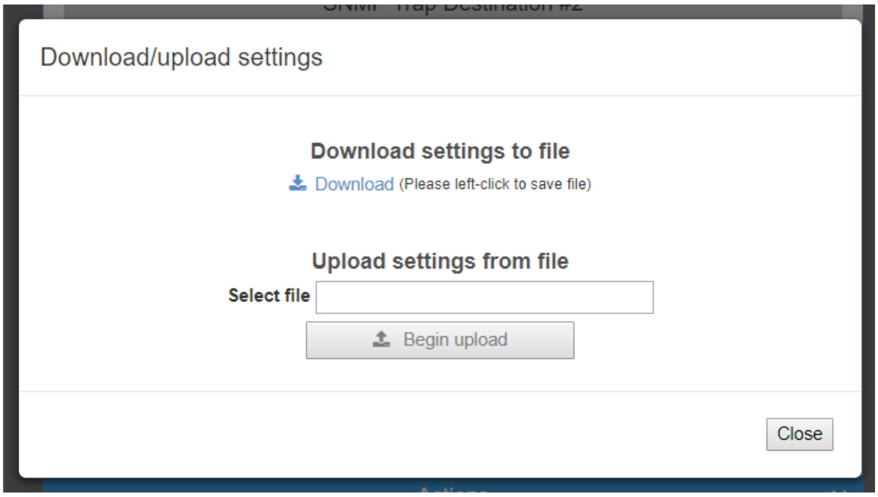
To save device settings, select Download link.

Acknowledge browser warning: -


This type of file can harm your computer.
Do you want to keep AP60.cfg anyway?



To restore the configuration of a device, start with selecting the previously saved .cfg file and then click ‘Begin upload’.

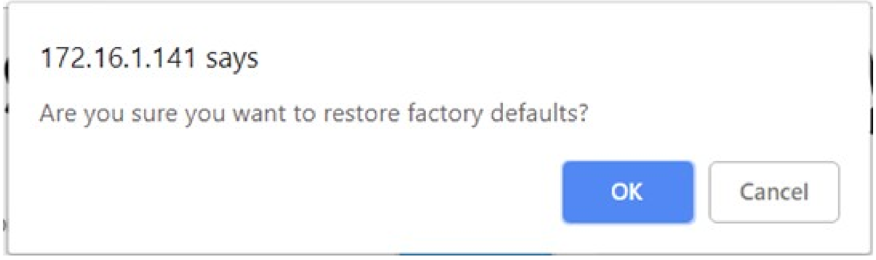

Download/upload settings

Download settings to file

Download (Please left-click to save file)

Upload settings from file

Select file

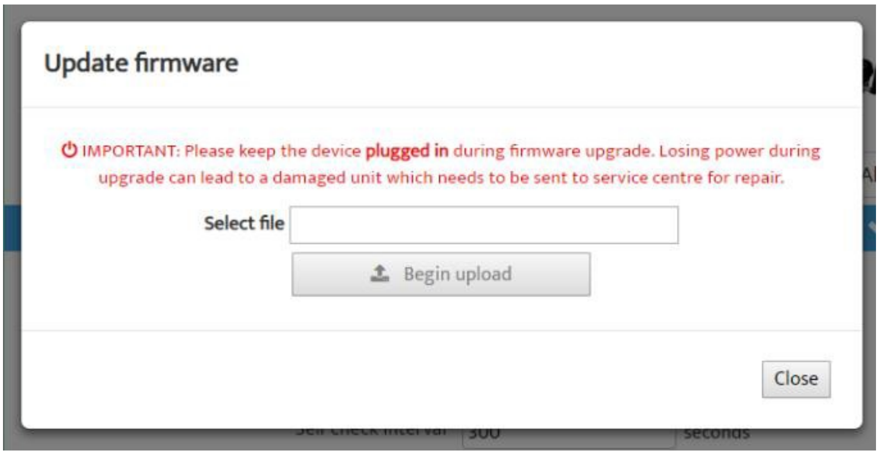

172.16.1.141 says

Are you sure you want to restore factory defaults?

3. Click **Upload settings from file**. The device will upload the configuration file. The device will reboot upon successfully applying configuration.

7.4.2 Update firmware

Select the firmware file provided by MST and click Begin upload.

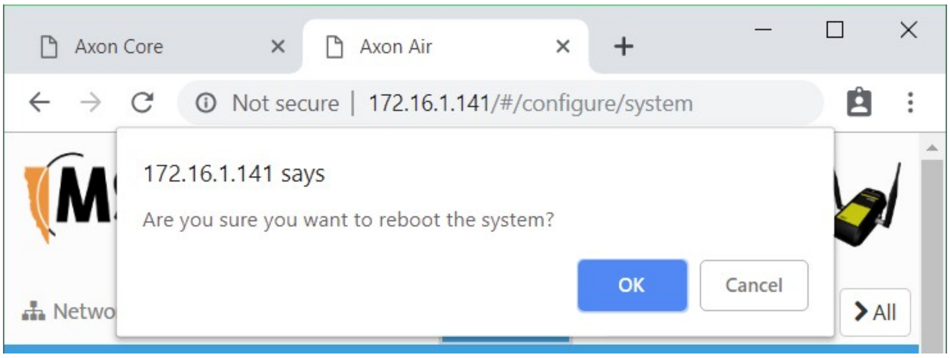

Update firmware

IMPORTANT: Please keep the device **plugged in** during firmware upgrade. Losing power during upgrade can lead to a damaged unit which needs to be sent to service centre for repair.

Select file

DO NOT power off the device during firmware upgrade process. It may lead to a damaged unit which needs to be sent to service for repair.

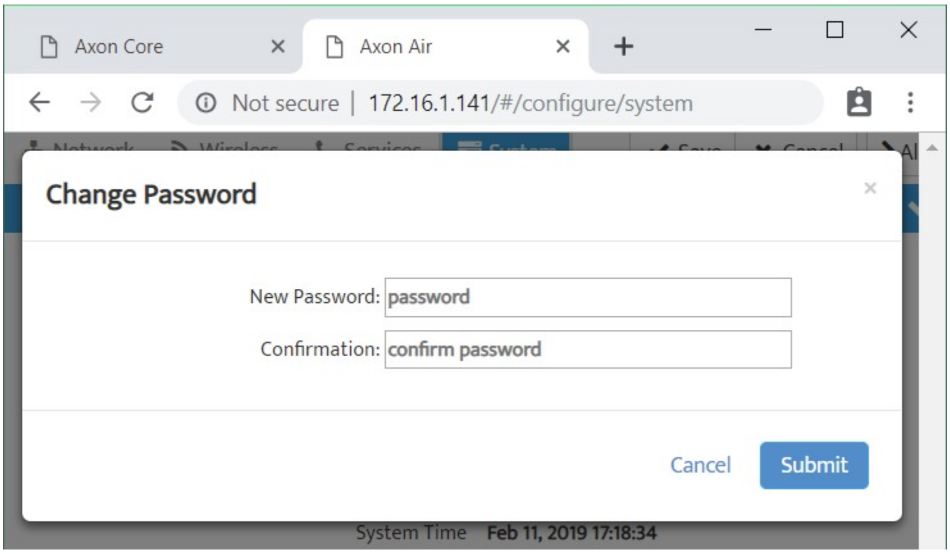
7.4.4 Reboot


172.16.1.141 says

Are you sure you want to reboot the system?

7.4.5 Change password

The administrator login can be configured on the **Change password** action screen.



Change Password

New Password: password

Confirmation: confirm password

System Time Feb 11, 2019 17:18:34

Figure 26: Change password dialog

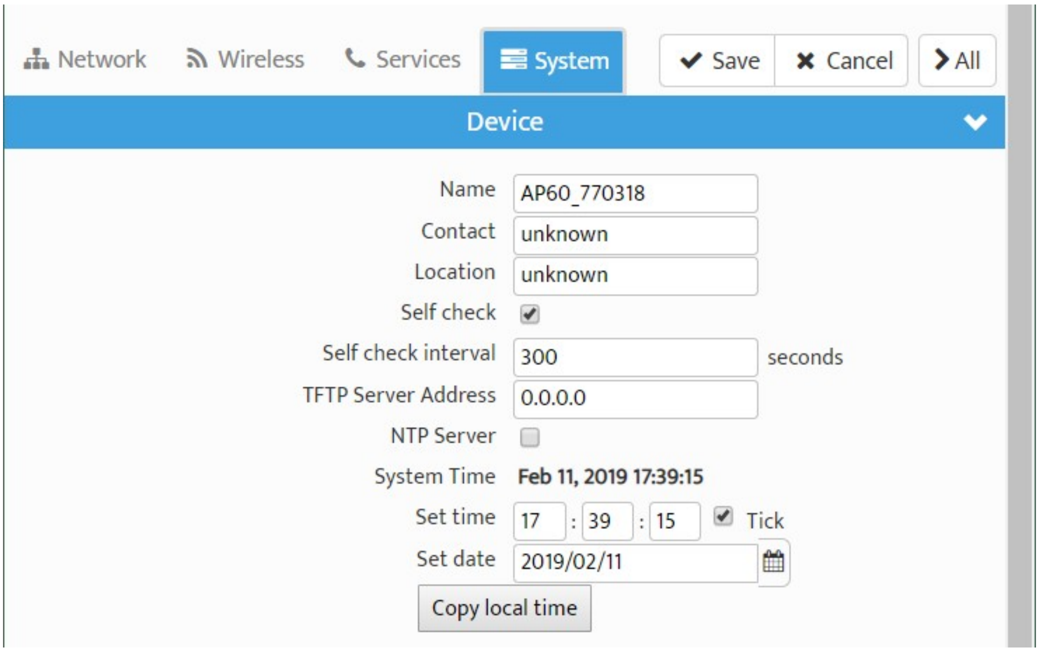
Passwords

The administrator and user password are used to restrict access to the web browser management tool. It is recommended to change the default password (admin).

Enter the same password for New Password and Confirmation, then click Submit.

7.4.2 Setting the Time

The **Time** configuration screen shown in *Figure 27: Time configuration screen* is used to define regional time settings on the device.



Name: AP60_770318

Contact: unknown

Location: unknown

Self check: ☑

Self check interval: 300 seconds

TFTP Server Address: 0.0.0.0

NTP Server: ☐

System Time: Feb 11, 2019 17:39:15

Set time: 17 : 39 : 15 ☑ Tick

Set date: 2019/02/11

Figure 27: Time configuration screen

To set the time configuration settings:

1. Select **Settings** > **System** > **Configure**
2. Click Copy local time to use your computer time to set the time on device. Use ‘Tick’ option to keep counting.
3. Click **Save**.

To enable **Automatic Time Configuration**, tick the **Enable NTP server** checkbox, and enter an NTP server address.

NOTE: If an NTP server is enabled, any manual changes to the time will be overridden the next time the device synchronises with the server. To keep a manually set time, **Enable NTP Server** should be unchecked.

Centralised configuration checklist

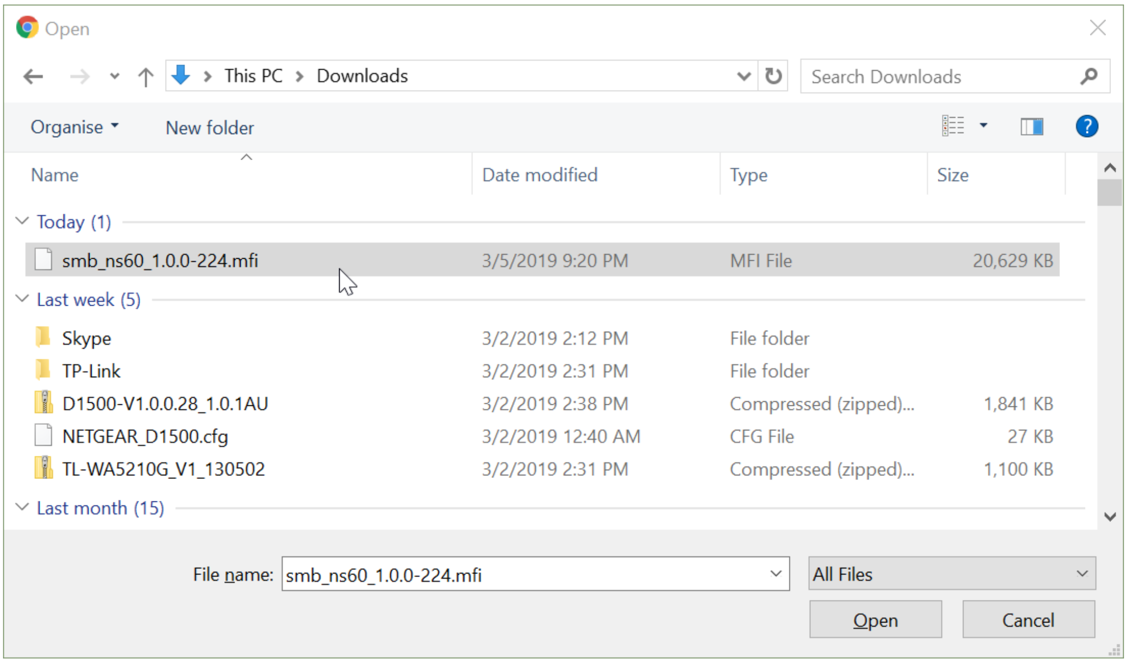
- Confirm all required template settings in the **Configuration** > **AP Config Templates** editor.
- In **Devices** > **Access Points,** select the device, tick the **Manage Configuration** checkbox and select the correct template.
- If required, click **Edit Overridden Parameters** and edit any required parameters for the specific device.
- **Save** the new settings.
- settings.
- Wait for the device's Managed status to change from `PENDING` to `CURRENT`.

NOTE: As a template can be applied to multiple devices, it is fixed to DHCP for networking to avoid address conflicts. If static IP addresses are required, these must be set in the individual devices' overridden parameters.

It is recommended that a client device (PC or laptop) has a wired connection to the network device to upgrade the firmware. Please contact your MST System Engineer for firmware files.

To upgrade the firmware:

1. Click **Choose File**. A dialog box will open.
2. Select the binary (.bin) firmware file and click **Open**.



Open

This PC > Downloads

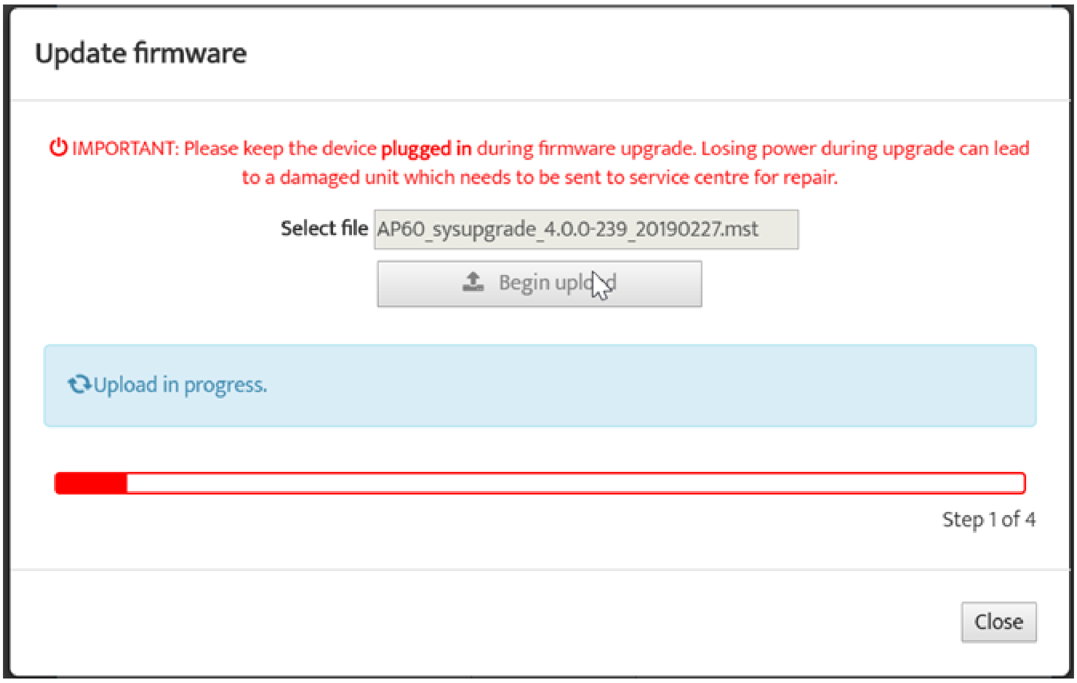
Search Downloads

Name	Date modified	Type	Size
Today (1)			
smb_ns60_1.0.0-224.mfi	3/5/2019 9:20 PM	MFI File	20,629 KB
Last week (5)			
Skype	3/2/2019 2:12 PM	File folder	
TP-Link	3/2/2019 2:31 PM	File folder	
D1500-V1.0.0.28_1.0.1AU	3/2/2019 2:38 PM	Compressed (zipped)...	1,841 KB
NETGEAR_D1500.cfg	3/2/2019 12:40 AM	CFG File	27 KB
TL-WA5210G_V1_130502	3/2/2019 2:31 PM	Compressed (zipped)...	1,100 KB
Last month (15)			

File name: smb_ns60_1.0.0-224.mfi

All Files

3. Click **Upload**, then **OK** on subsequent dialogue boxes to confirm. The firmware will upload to the device.
4. When the firmware has been successfully uploaded, the **UPLOAD SUCCEEDED** screen will appear. The network switch will reboot after 60 seconds.



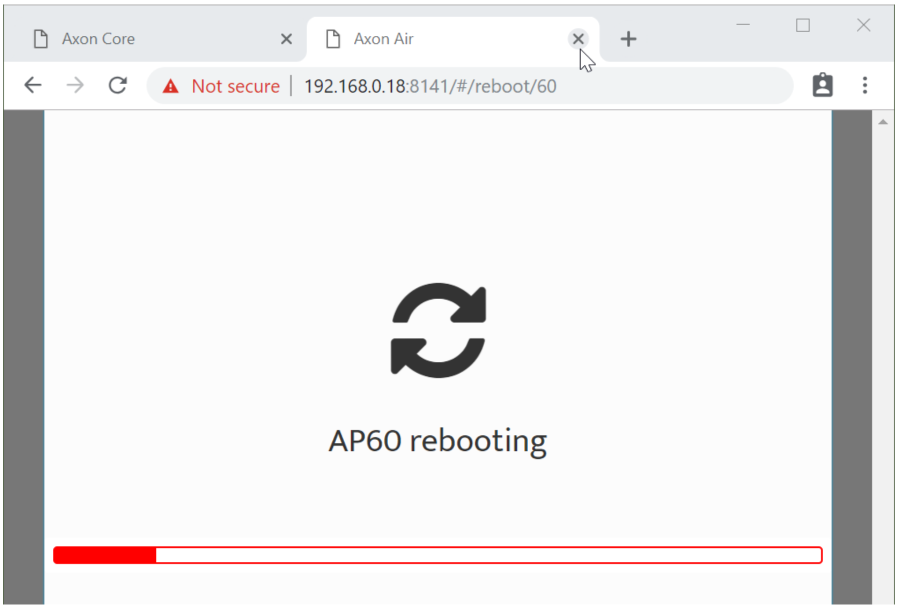
Update firmware

IMPORTANT: Please keep the device **plugged in** during firmware upgrade. Losing power during upgrade can lead to a damaged unit which needs to be sent to service centre for repair.

Select file AP60_sysupgrade_4.0.0-239_20190227.mst

Upload in progress.

Step 1 of 4



AP60 rebooting

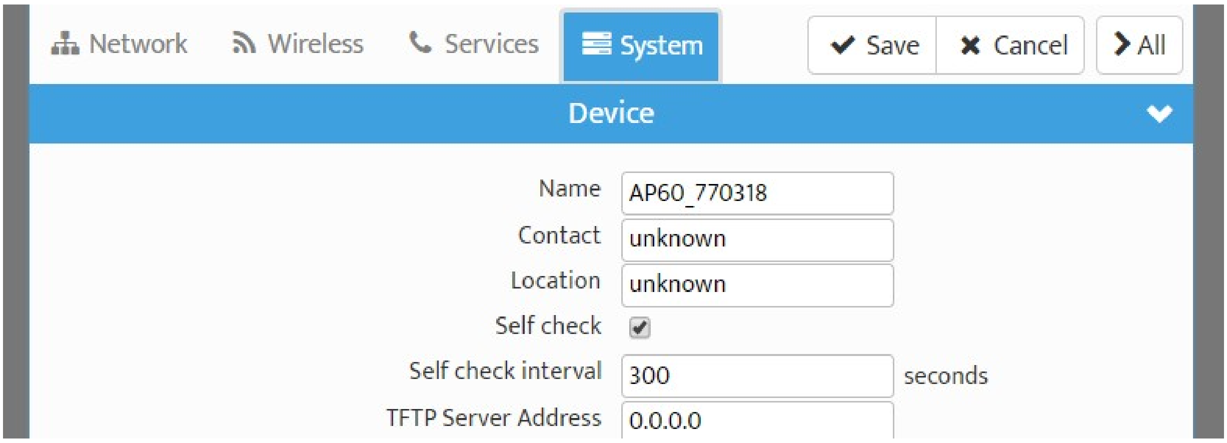
1. Check the device's IP address in the Device Scanner to ensure that it has been correctly updated. This address must match the IP address entered in the AeroScout System Manager for tracking to work.
2. Log back on to the device's web interface and check the **STATUS** > **LOGS** screen for any errors that may need to be addressed.

7.5 Setting Tab

7.5.1 Managing Automatic TFTP Configuration

The **Config Management** screen is used to configure how the device retrieves its configuration from a TFTP server on the network. For more information on TFTP, see Centralised Configuration Management.

NOTE: These settings only affect TFTP configuration from an ICA v1.3.1 or earlier, and 3rd party TFTP servers. If using AP Config Templates from ICA 1.4.0 or later, leave **Self check** disabled



Name: AP60_770318
Contact: unknown
Location: unknown
Self check: ☑
Self check interval: 300 seconds
TFTP Server Address: 0.0.0.0

Self-check Settings

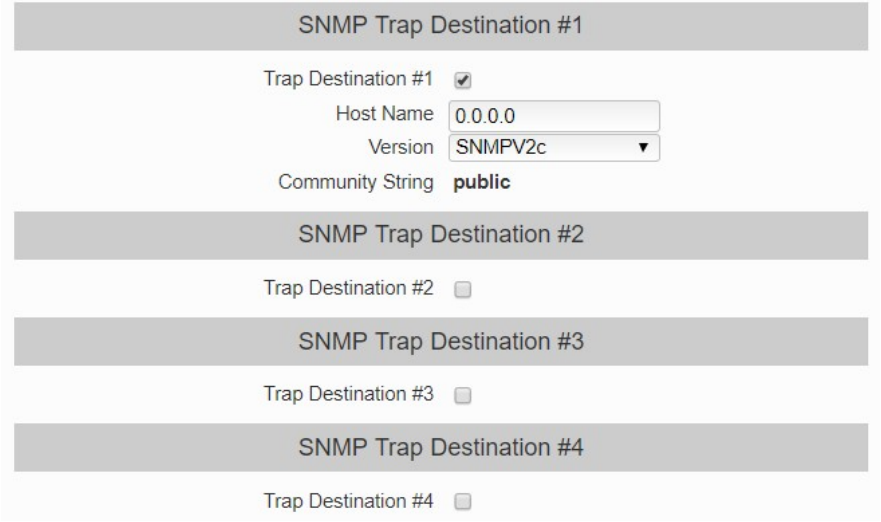
To enable automatic configuration from a TFTP server, tick (enable) the **Self check** checkbox, enter the desired **Self check interval (**default is 300 seconds) and **TFTP Server Address**, then click the **Save**.

Change Numbers

The two change numbers shown here are timestamps (formatted as YYYYMMDDhhmmss) showing the last time the device's settings were updated via TFTP. The **Site Change Number** refers to general site settings applied to all devices, whereas the **Device Change Number** refers to specific settings applied to this device.

7.5.2 Configuring SNMP Settings

The **SNMP** screen contains Simple Network Management Protocol settings. SNMP is a protocol used by the ICA and 3rd party SNMP browsers to monitor the status of compatible devices on the network. At present, the ICA only uses this protocol to monitor for Port Up/Port Down errors on AXON Core and is not affected by the settings below.



SNMP Trap Destination #1

Trap Destination #1: ☑
Host Name: 0.0.0.0
Version: SNMPV2c ▾
Community String: public

SNMP Trap Destination #2

Trap Destination #2: □

SNMP Trap Destination #3

Trap Destination #3: □

SNMP Trap Destination #4

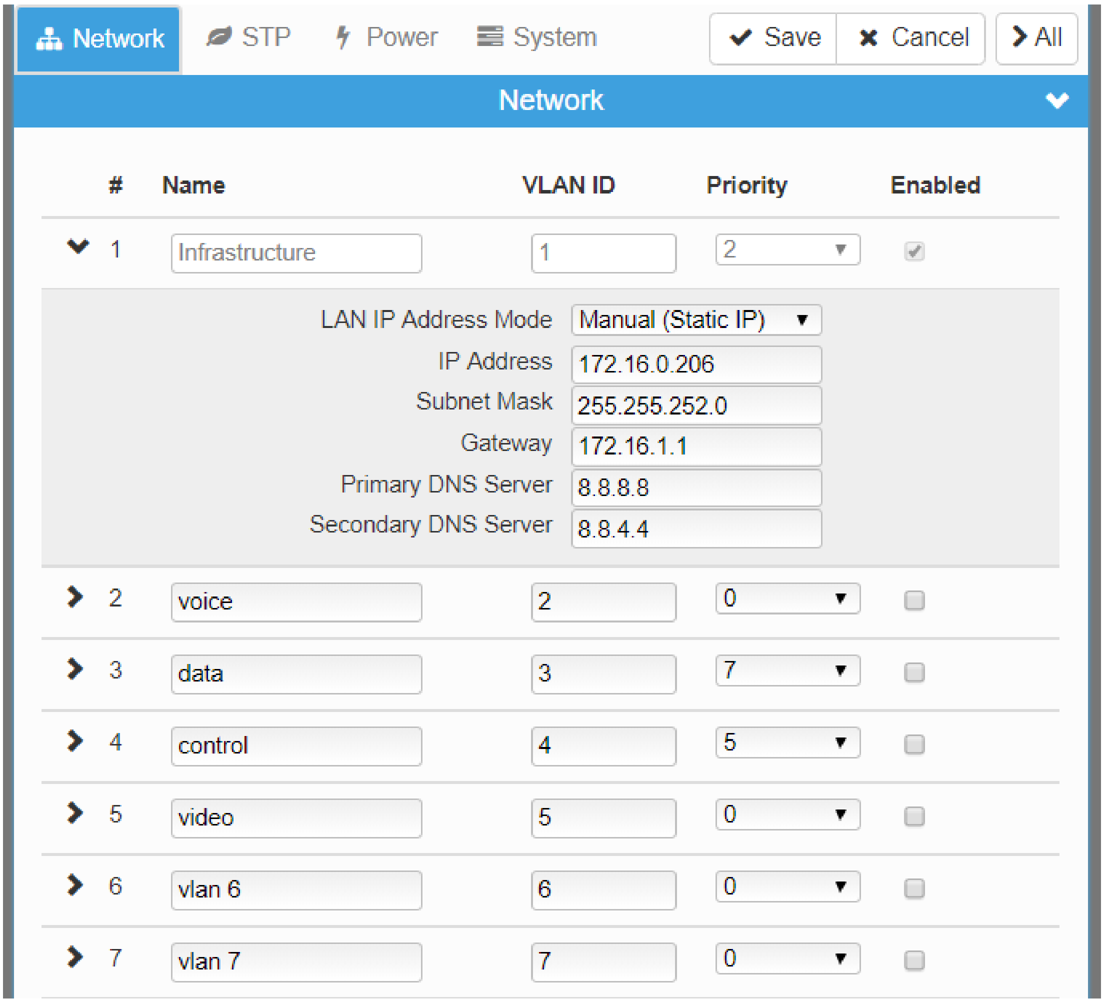
Trap Destination #4: □

The following settings are available, which may affect 3rd party SNMP tools:

- **Name:** The name or ID of the device
- **Contact:** The name of the person to be notified of any alarms
- **Location:** The location of the device
- **Community String:** The group to which the device belongs. Unless otherwise necessary, this is usually left as `public`.

7.5.3 Setting Up the LAN

The LAN configuration screen is shown in *Figure 29: LAN configuration screen.*



#	Name	VLAN ID	Priority	Enabled
1	Infrastructure	1	2	☑
2	voice	2	0	☐
3	data	3	7	☐
4	control	4	5	☐
5	video	5	0	☐
6	vlan 6	6	0	☐
7	vlan 7	7	0	☐

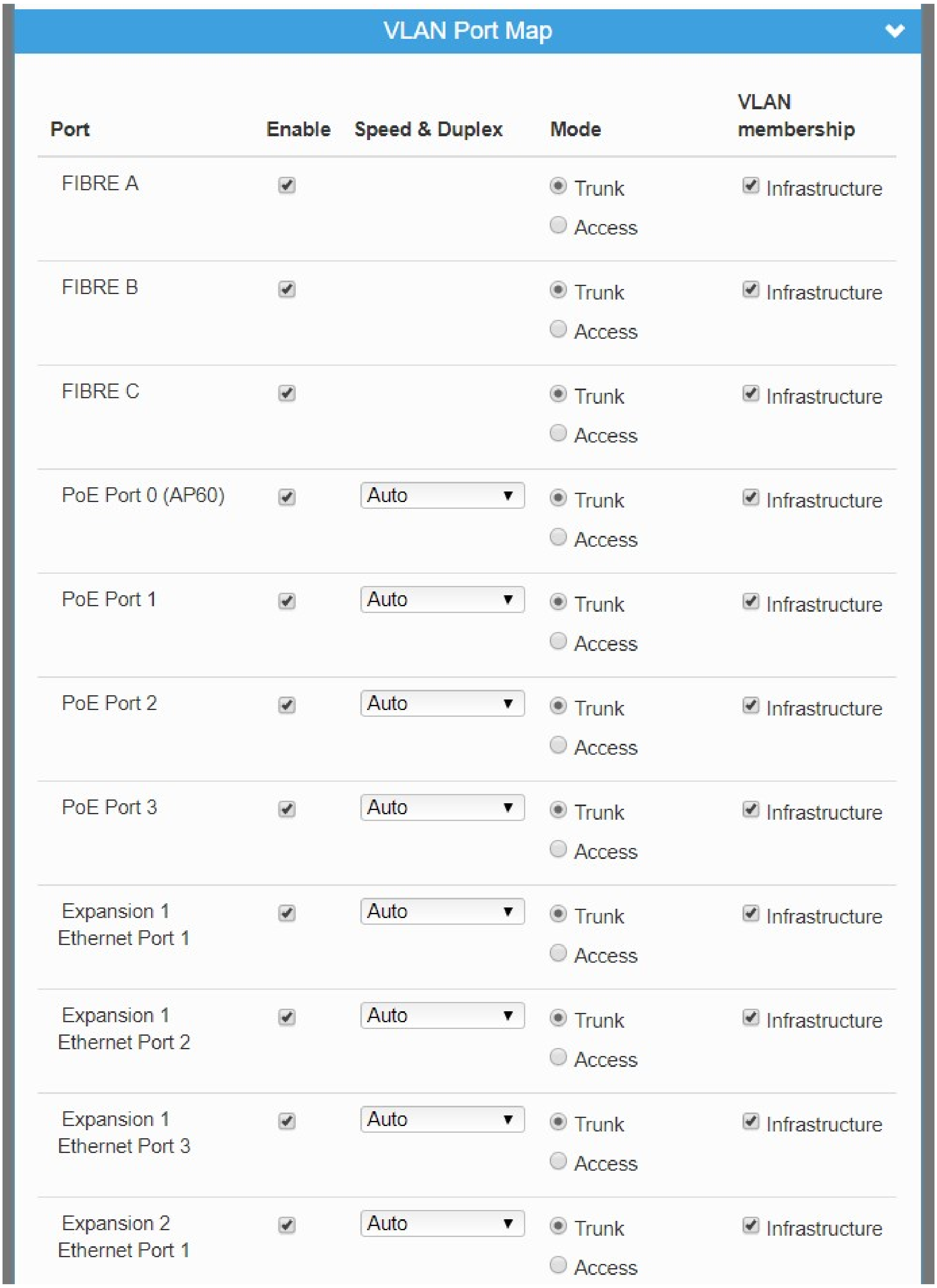
LAN IP Address Mode: Manual (Static IP)
IP Address: 172.16.0.206
Subnet Mask: 255.255.252.0
Gateway: 172.16.1.1
Primary DNS Server: 8.8.8.8
Secondary DNS Server: 8.8.4.4

Figure 29: LAN configuration screen

To edit LAN settings, click in the selected field in the dialog box. LAN settings are described in the table below.

Field	Description	Recommended Settings
Get LAN IP from	DHCP (Dynamic) or Static IP (Manual)	Default is `DHCP`. If `Static IP` is selected, the following fields must be filled in.
IP Address	The IP address of the WAC.	A different IP address is required for each WAC in a network.
Subnet Mask	Identifies the subnet the IP address belongs to for the WAC.	The default subnet mask is 255.255.255.0.
Gateway	The IP address of the default gateway to be used by the WAC.	Settings are dependent on the site's network design.
Primary DNS	The DNS server used by the WAC when looking up host names.	Settings are dependent on the site's DNS design.
Secondary DNS	The backup DNS server used by the WAC when looking up host names.	Settings are dependent on the site's DNS design.
Local Domain Name	Local domain name for the network.	Leave the field blank if you do not wish to add a domain name.

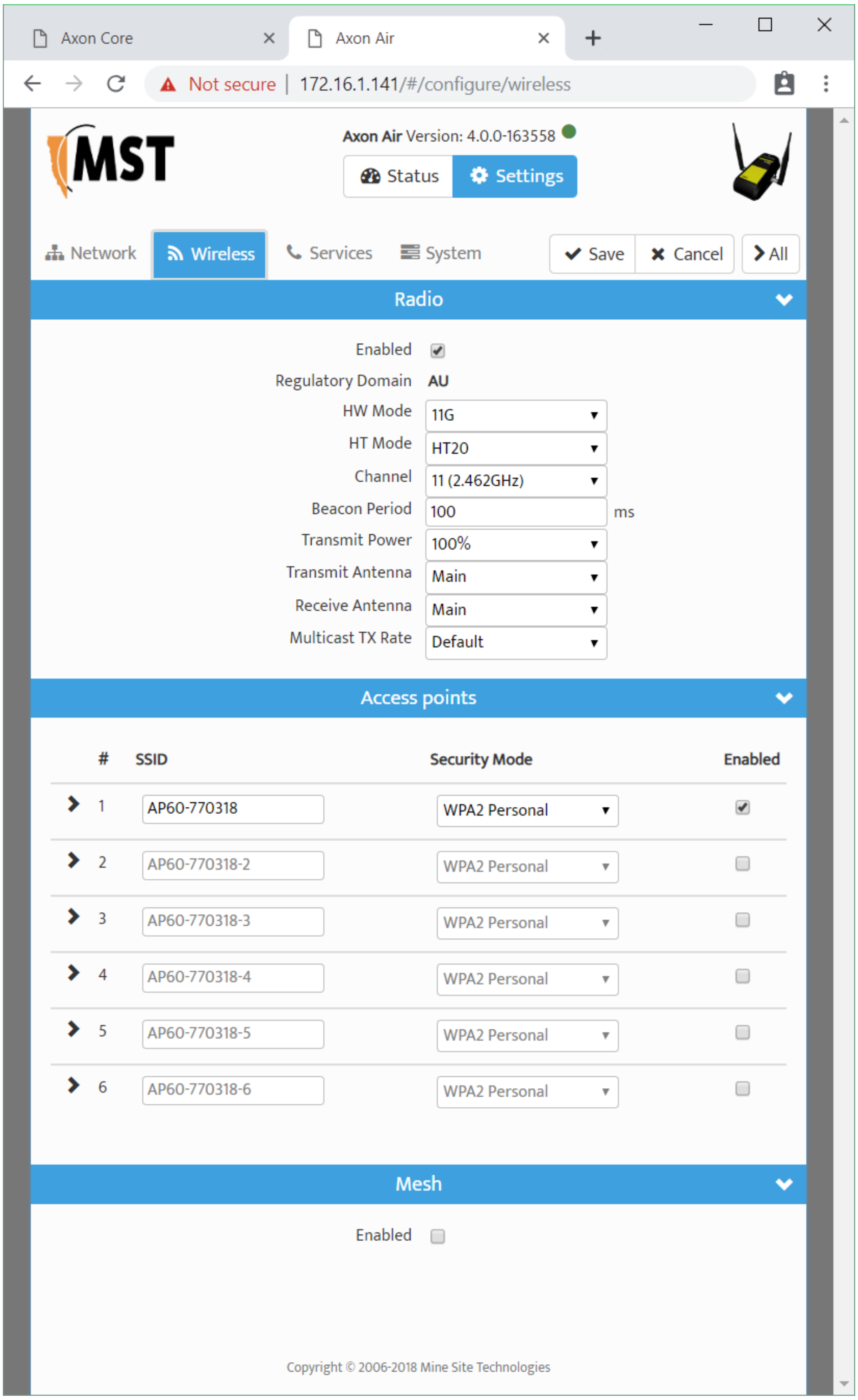
If the device is left on DHCP, only the following fields are shown. These values will function as above, only if they are not defined by the DHCP server.



VLAN Port Map

Port	Enable	Speed & Duplex	Mode	VLAN membership
FIBRE A	☑		● Trunk ○ Access	☑ Infrastructure
FIBRE B	☑		● Trunk ○ Access	☑ Infrastructure
FIBRE C	☑		● Trunk ○ Access	☑ Infrastructure
PoE Port 0 (AP60)	☑	Auto ▼	● Trunk ○ Access	☑ Infrastructure
PoE Port 1	☑	Auto ▼	● Trunk ○ Access	☑ Infrastructure
PoE Port 2	☑	Auto ▼	● Trunk ○ Access	☑ Infrastructure
PoE Port 3	☑	Auto ▼	● Trunk ○ Access	☑ Infrastructure
Expansion 1 Ethernet Port 1	☑	Auto ▼	● Trunk ○ Access	☑ Infrastructure
Expansion 1 Ethernet Port 2	☑	Auto ▼	● Trunk ○ Access	☑ Infrastructure
Expansion 1 Ethernet Port 3	☑	Auto ▼	● Trunk ○ Access	☑ Infrastructure
Expansion 2 Ethernet Port 1	☑	Auto ▼	● Trunk ○ Access	☑ Infrastructure

7.5.4 Configuring Wireless Radio



Axon Air Version: 4.0.0-163558

Radio

Enabled ☑
Regulatory Domain **AU**
HW Mode 11G
HT Mode HT20
Channel 11 (2.462GHz)
Beacon Period 100 ms
Transmit Power 100%
Transmit Antenna Main
Receive Antenna Main
Multicast TX Rate Default

Access points

#	SSID	Security Mode	Enabled
1	AP60-770318	WPA2 Personal	☑
2	AP60-770318-2	WPA2 Personal	□
3	AP60-770318-3	WPA2 Personal	□
4	AP60-770318-4	WPA2 Personal	□
5	AP60-770318-5	WPA2 Personal	□
6	AP60-770318-6	WPA2 Personal	□

Mesh

Enabled □

Copyright © 2006-2018 Mine Site Technologies

The **Wireless Radio** configuration screen configures wireless radio settings as shown in *Figure 30: Wireless radio configuration screen.*

Figure 30: Wireless radio configuration screen

To configure the wireless radio:

1. Select the **Enable Wireless Radio** check box to enable wireless.
2. To change wireless radio settings, edit the required fields. A description and recommended settings are shown below.
3. Click **Save Settings**.

Field	Description	Recommended Settings
Enable Wireless Radio	Used to enable or disable the WAC's radio.	
Region	Limits available channels to those allowed by local regulations	Select the correct region for the site location.
Transmission Rate	Settings to configure how fast data is transmitted.	Leave the default setting as Best (automatic) for data transmission at the best possible speed.
802.11 Mode	A drop-down box to select the 802.11 mode from mixed 802.11g and 802.11b to 802.11g.	If there are 802.11b wireless client devices, leave the setting at Mixed. Select 802.11g for improved performance if all wireless client devices are 802.11g capable.
Super AG Mode	See section below.	See section below.
Transmit Power	Used to control the power delivered via the wireless transmitter.	High - Only drop to Medium or Low if the signal is interfering with other devices.
Transmit Antenna	Defines the antenna to be used for transmission of wireless frames. The options are: Main: The MAIN antenna will always be used for transmission. Aux: The AUX antenna will always be used for transmission. Diversity: The radio will determine the best antenna to use for transmission based on the signal strength of recently received frames from both antennas.	Main

Field	Description	Recommended Settings
Receive Antenna	Defines the antenna to be used for the reception of wireless frames. The options are: Main: The MAIN antenna will always be used for reception. Aux: The AUX antenna will always be used for reception. Diversity: Both antennas will always be used for reception and the received frame with the best signal strength will be used.	`Main`: if a single antenna is fitted. `Diversity`: if antennas are fitted to both of the radio's ports.

IMPORTANT: Ensure that the physical connection of antennas is consistent with the transmit and receive antenna settings. Failure to do so will give poor Wi-Fi performance and reduced tracking accuracy.

Channels

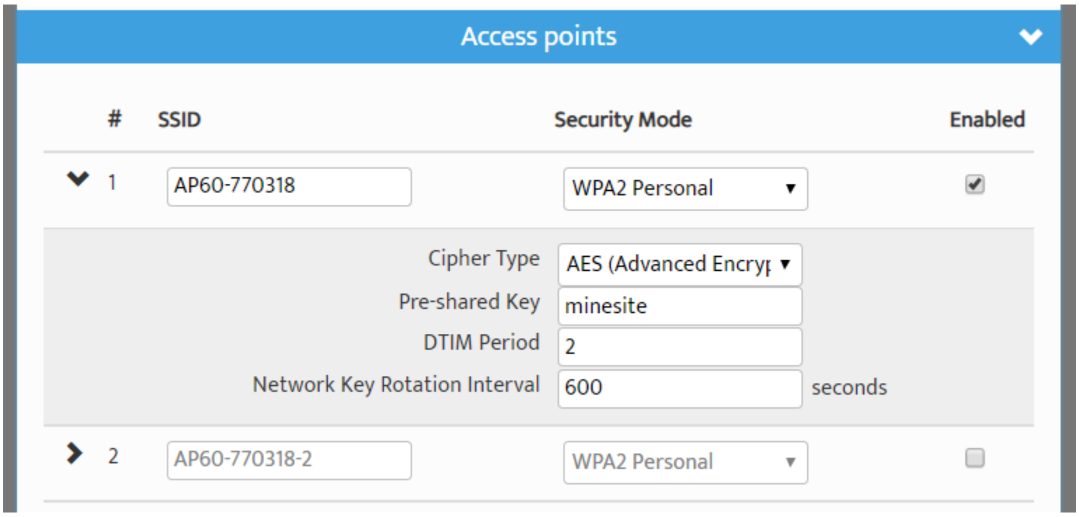
It is recommended that WACs in proximity of each other have different wireless channels (for example, channels 1, 6 and 11). This minimises signal overlap and the possibility of interference.

Advanced Wireless Settings

Field	Description	Recommended Settings
Fragmentation Threshold	Maximum frame size that can be sent without fragmentation.	Default setting is at the maximum size of 2346 and is recommended for most environments.
RTS threshold	Determines what size data packet the low level RF protocol issues to an RTS packet.	Default setting is 2346.
Beacon Period	The amount of time between beacon transmissions.	Default setting is 100ms.
DTIM interval	A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. Wireless clients detect the beacons and awaken on the DTIM interval to receive the broadcast and multicast messages. Valid settings are between 1 and 255.	The recommended DTIM interval is 1.
Burst Time	The time in microseconds which will be used to send data without stopping. Note that other wireless cards in that network will not be able to transmit data for this period.	Default 3000µs (0.3s)
802.11d enable	Wireless specification where configuration occurs at a MAC layer level to comply with country or district rules.	802.11d is not enabled by default.

7.5.5 Configuring Wireless Networks

A WAC can have up to four wireless SSIDs with different performance and security settings. Each can be mapped to different VLANs. The configuration screen is shown in *Figure 31: Wireless Networks configuration screen.*



#	SSID	Security Mode	Enabled
1	AP60-770318	WPA2 Personal	☑
2	AP60-770318-2	WPA2 Personal	□

Cipher Type: AES (Advanced Encry
Pre-shared Key: minesite
DTIM Period: 2
Network Key Rotation Interval: 600 seconds

Figure 31: Wireless Networks configuration screen

Wireless network parameters are described in the table below.

Field	Description	Recommended Settings
Enable	Enables or disables the wireless network.	Click on the Enable check box to enable the wireless network.
SSID	The Wireless Network Name network that will be visible to client devices.	Enter a network name that relates closely to its function. For example, "MST-VOICE".
Security Mode	Four security modes exist: **None**: No wireless authentication is required, and traffic is not encrypted. **WPA2 Personal**: provides a higher level of security and does not use a centralised authentication server. **WPA2 Enterprise**: as per WPA Personal but a RADIUS authentication server is used. (WPA Personal and WPA Enterprise are older versions of the standard and less secure)	**WPA2-Personal** is recommended. Selecting the wireless security mode will display configuration options.

⚠ **Note:** After a unit is reset to factory defaults, it will have a single wireless network on channel 6 with the name "AP------" (the last six digits of the unit's MAC address), WPA2-AES security enabled and the password "minesite".

NOTE: After a unit is reset to factory defaults, it will have a single wireless network on channel 6 with the name "AP------" (the last six digits of the unit's MAC address), WPA2-AES security enable and the password "minesite".

Configuring WPA Settings

WPA provides a higher level of security. WPA-Personal and WPA-Enterprise are variants of Wi-Fi Protected Access (WPA). WPA-Enterprise requires an external RADIUS server.

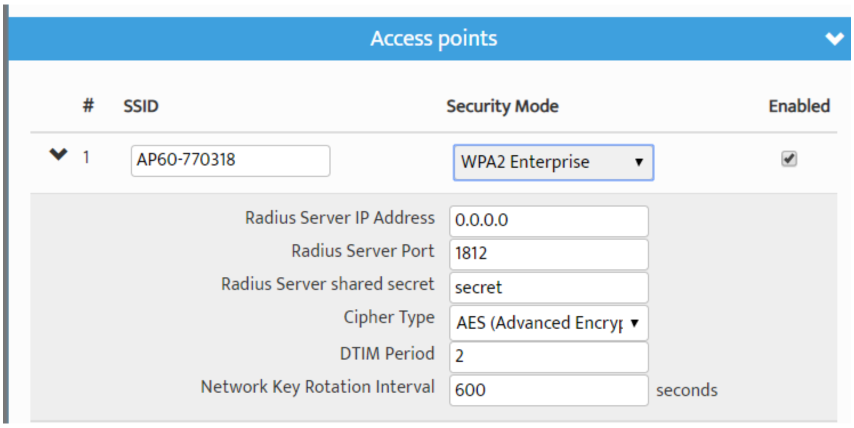
To configure WPA settings:

1. Select the **WPA mode** from the drop-down box.
2. Select the **Cipher Type** from the drop-down box. By default, it is set at **AES**.
3. Enter the **Pre-Shared Key** in the supplied field (applicable to WPA Personal security mode). The key must be at least 8 alphanumeric characters in length.
4. Enter **Network Key Rotation Interval** in the supplied field. By default, it is 600 seconds. This is the amount of time before the group key (used for broadcast and multicast data encryption) is changed.
5. Click Save Settings

Configuring WEP Security Settings

7.5.6 Configuring EAP (Extensible Authentication Protocol)

The **Wireless EAP** configuration screen is used to configure wireless authentication by a RADIUS server (as used by WPA Enterprise). The configuration screen is shown in *Figure 32: Wireless EAP configuration*



#	SSID	Security Mode	Enabled
1	AP60-770318	WPA2 Enterprise ▾	☑

Radius Server IP Address: 0.0.0.0
Radius Server Port: 1812
Radius Server shared secret: secret
Cipher Type: AES (Advanced Encryp ▾
DTIM Period: 2
Network Key Rotation Interval: 600 seconds

Figure 32: Wireless EAP configuration

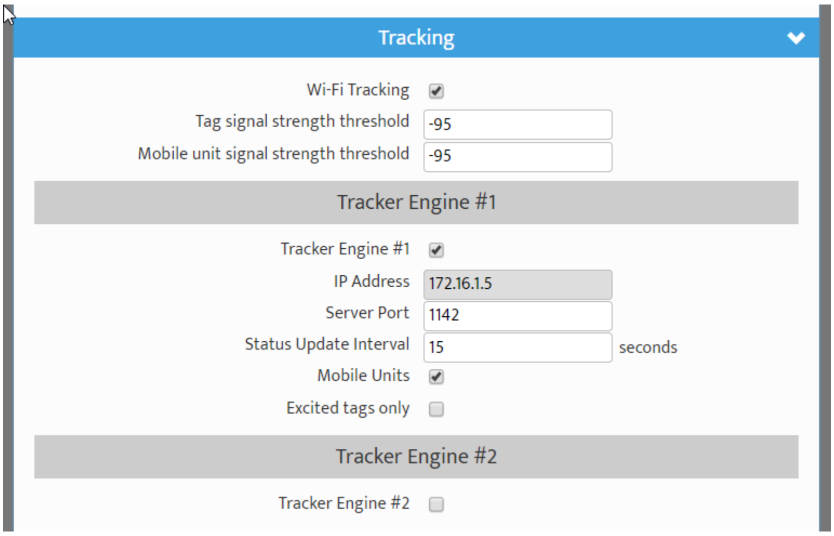
To configure wireless EAP, click on the drop-down boxes in the supplied fields. Click **Save Settings** to save settings. A description of the fields and settings are described in the table below.

Field	Description	Recommended Settings
Authentication Timeout	Amount of time in minutes before a client device is required to re-authenticate.	Setting is at 120 minutes by default.
RADIUS server IP Address	IP address of the authentication server.	This is specific to each site.
RADIUS server Port	Port number used by the access point to connect to the authentication server.	By default the port number is 1812.
RADIUS server Shared Secret	Password used by the access point to access the RADIUS server.	Password that matches with the authentication server.
MAC Address Authentication	Access to the RADIUS server by confirmation of the client device's MAC address.	If selected, the user must always use the same device when connecting to the wireless network.

A second RADIUS server can be configured if the primary server is not available or not responding. This can be configured by clicking on the **Advanced** button.

7.5.7 Configuring Asset Tracking and Location Based Services

The **Tracking** configuration screen establishes where AeroScout tag reports are sent as shown in *Figure 33: Tracking configuration screen.* A network device can communicate with an AeroScout Positioning Engine and / or a MST Tracker Engine. Configuration of the Access Point is not required when communicating with an AeroScout Positioning Engine as the device configuration is performed via AeroScout server tools.



Tracking

Wi-Fi Tracking ☑
Tag signal strength threshold -95
Mobile unit signal strength threshold -95

Tracker Engine #1

Tracker Engine #1 ☑
IP Address 172.16.1.5
Server Port 1142
Status Update Interval 15 seconds
Mobile Units ☑
Excited tags only □

Tracker Engine #2

Tracker Engine #2 □

Figure 33: Tracking configuration screen

If the Access Point is sending tag reports to an MST Tracker Engine, the Tracker Engine's IP address must be entered into each Access Point.

There are four sections on the **Tracking** configuration screen:

Enable

Check **Enable Wi-Fi Tracking** to view other settings.

RSSI Lower Thresholds

These settings are used to control what location reports are sent to the Positioning Engine. If a Wi-Fi tag or mobile unit report is received with an RSSI below the relevant threshold, it is not sent to the Positioning Engine (whether it is an AeroScout Positioning Engine or MST Tracker Engine). The default threshold is -95 dBm, but this can be raised or lowered according to specific site conditions and requirements.

Tracker Engine List

This section is used to configure the MST Tracker Engine(s) that the access point will send information to. The available settings are listed below. Note that data can be passed to up to 2 MST Tracker Engine instances.

Field	Description	Recommended Settings
Enable	Indicates whether the Tracker Engine will be sent data.	On or Off.
IP Address	The IP address of the MST Tracker Engine.	Specific to each site.
Port	The UDP port that the Tracker Engine listens for messages on.	Default is 1142.
Status Update Interval	The period that status reports will be sent from the Access Point to the Tracker Engine. These status reports are used by the Tracker Engine to determine if the Access Point is up or down.	Default is 15 seconds.
AeroScout Tags Enabled MST Wi-Fi Tags Enabled Mobile Units Enabled	Indicates which devices will be tracked by this Access Point.	These options are enabled by default.

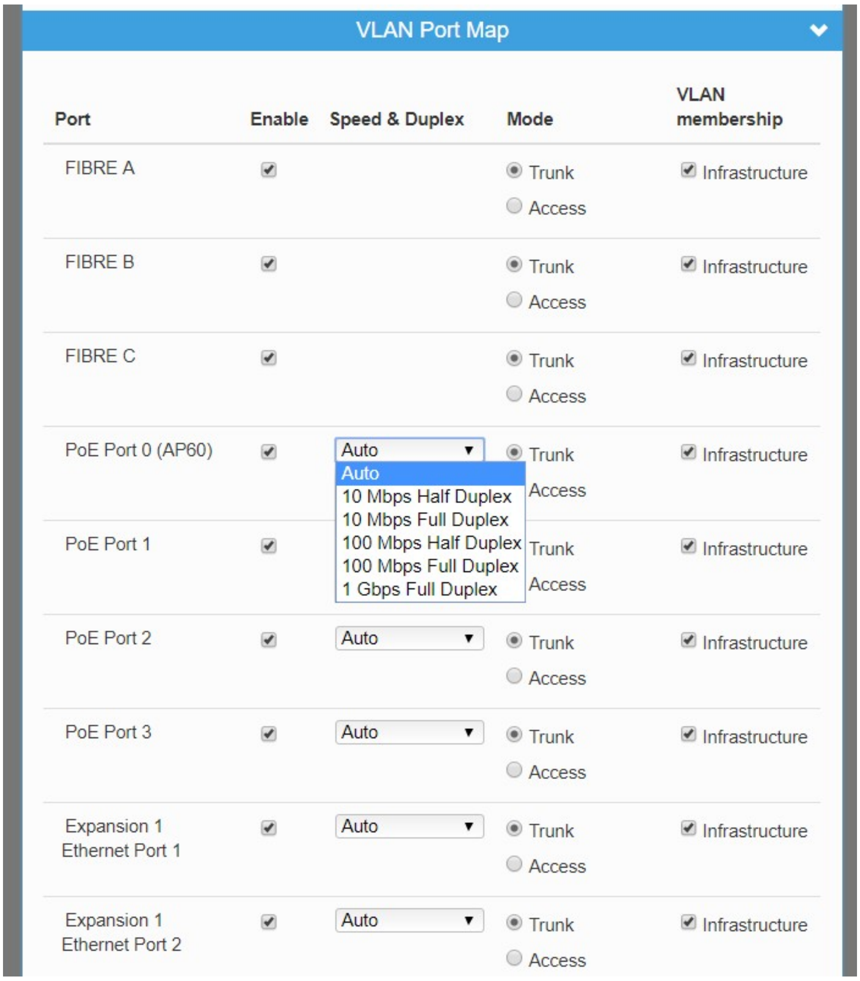
Advanced Settings

Drop non-exciter tag reports - If enabled, the Access Point will only send tag reports when the tag is in an AeroScout Exciter field.

This setting applies to tag reports that are sent to AeroScout Positioning Engines and MST Tracker Engines.

7.5.8 Configuring Ethernet Switch Ports

The WAC in slot 1 (located on the left side of AXON Core) is used for configuration and management of the switch processors in the network switch. It enables the ports on the switch and the 48V rail for the Power over Ethernet (PoE) supply to be configured, as shown in *Figure 34: Switch configuration screen.*



VLAN Port Map

Port	Enable	Speed & Duplex	Mode	VLAN membership
FIBRE A	☑		● Trunk ○ Access	☑ Infrastructure
FIBRE B	☑		● Trunk ○ Access	☑ Infrastructure
FIBRE C	☑		● Trunk ○ Access	☑ Infrastructure
PoE Port 0 (AP60)	☑	Auto ▾ Auto 10 Mbps Half Duplex 10 Mbps Full Duplex 100 Mbps Half Duplex 100 Mbps Full Duplex 1 Gbps Full Duplex	● Trunk Access	☑ Infrastructure
PoE Port 1	☑		Trunk Access	☑ Infrastructure
PoE Port 2	☑	Auto ▾	● Trunk ○ Access	☑ Infrastructure
PoE Port 3	☑	Auto ▾	● Trunk ○ Access	☑ Infrastructure
Expansion 1 Ethernet Port 1	☑	Auto ▾	● Trunk ○ Access	☑ Infrastructure
Expansion 1 Ethernet Port 2	☑	Auto ▾	● Trunk ○ Access	☑ Infrastructure

Figure 34: Switch configuration screen

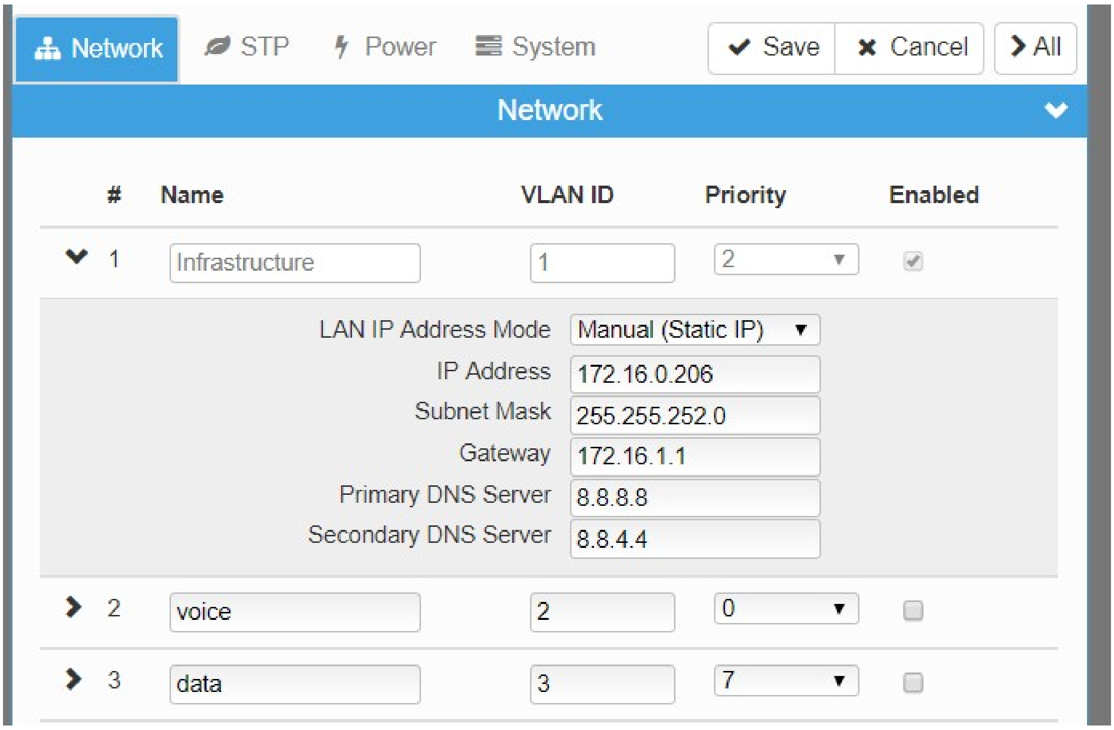
The Switch ports have the following configuration options:

Field	Description	Recommended Settings
Name	Used to provide a convenient name for the port. It is often used to name the device	Naming is specific to each device.

	connected to it. For example, "Level 68 camera".	
Enabled	Enables or disables the port.	On or Off.
Speed & Duplex	Ports 5 thru 8 allow the speed and duplex to be controlled.	Auto is usually the best setting. However, some devices require Speed & Duplex to be hard coded due to poor Auto-negotiation implementations.

7.5.9 Defining VLANs

The **VLAN LIST** screen displays VLANs and the priority that will be assigned to traffic on each VLAN.



#	Name	VLAN ID	Priority	Enabled
1	Infrastructure	1	2	☑
2	voice	2	0	□
3	data	3	7	□

LAN IP Address Mode	Manual (Static IP)
IP Address	172.16.0.206
Subnet Mask	255.255.252.0
Gateway	172.16.1.1
Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.4.4

Figure 36: VLAN list configuration screen

Up to 8 VLANs can be defined with the following parameters:

- **Enable:** Check box to enable the VLAN.
- **ID:** VLAN ID number that is tagged in frames sent through trunk ports.
- **Name:** VLAN name. It should be named to simplify administration.
- **Priority:** Priority ranges from 0-7 (7 being the highest priority) that is assigned to frames on this VLAN.

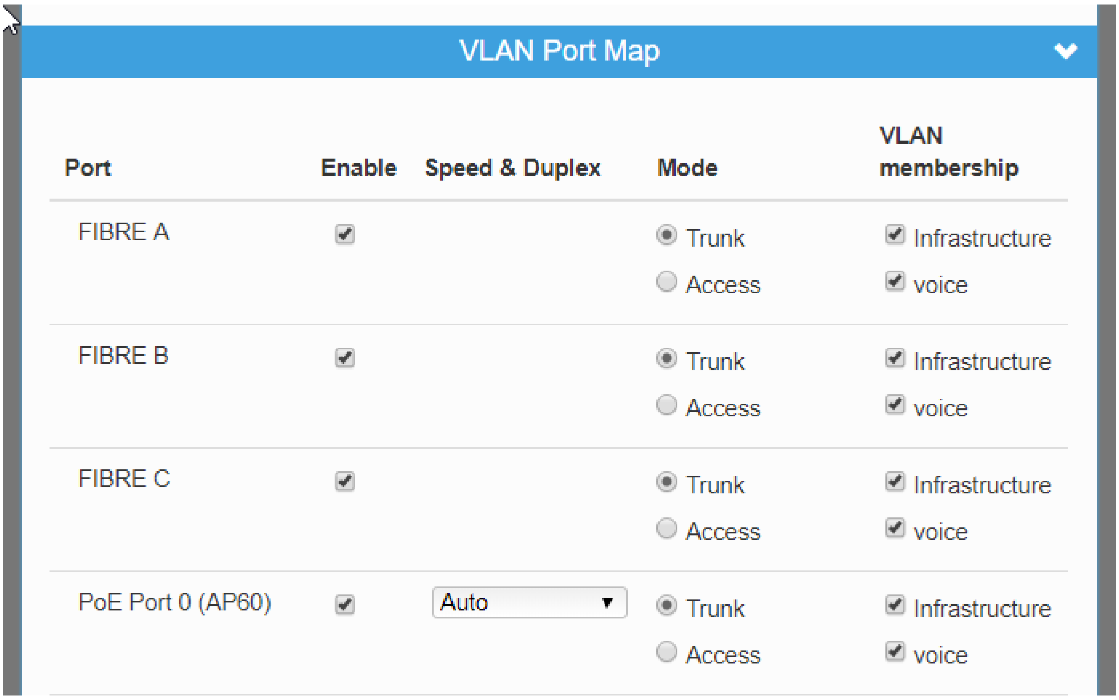
NOTE: The first VLAN (**Infrastructure**) cannot be disabled, because the management CPU is always on this VLAN.

By default, VLANs are pre-defined with recommended IDs and priorities. This is based on commonly used applications in mines. Once the VLANs are defined, they can be saved by clicking on the **Save Settings** button.

After the VLANs have been defined, they can be assigned to the wireless networks and switch ports (Network Switch only) on the **VLAN PORT MAP** screen.

7.5.10 Configuring the VLAN Port Map

The **VLAN Port Map** screen assigns the VLAN(s) to each physical switch port, and each wireless network. The screen is shown in *Figure 37: VLAN Port Map screen.*



VLAN Port Map

Port	Enable	Speed & Duplex	Mode	VLAN membership
FIBRE A	☑		● Trunk ○ Access	☑ Infrastructure ☑ voice
FIBRE B	☑		● Trunk ○ Access	☑ Infrastructure ☑ voice
FIBRE C	☑		● Trunk ○ Access	☑ Infrastructure ☑ voice
PoE Port 0 (AP60)	☑	Auto ▾	● Trunk ○ Access	☑ Infrastructure ☑ voice

Physical switch ports can be assigned as Trunk or Access ports. Wireless networks always act as Access ports on the selected VLAN.

Figure 37: VLAN Port Map screen

Chapter 8: Centralised Configuration Management

Topics:

- Devise Management Overview
- TFTP Server Overview
- TFTP Parameters

Centralised configuration management is an alternative configuration method to the web interface. It uses Trivial File Transfer Protocol (TFTP) where devices read and apply configuration files from a TFTP server. It is a faster way to configure a large number of network switches, reducing the potential for human error.

To take advantage of TFTP configuration:

For networks with an ICA v1.4.0 or higher, AP settings can be managed from the ICA Administration console. A customisable **Site Default** template is included at installation, and further templates can be copied from it and modified separately. Additionally, individual APs can have specific settings overridden via the Administration Console.

In this case, the ICA will push configuration changes to the APs, and no local setup is required.

8.1 Device Management Overview

The ICA Administration Console (v1.4.0 and later) supports the creation of Access Point configuration templates. A **Site Default** template is created at installation and applied to all managed devices. New templates can be copied from the **Site Default** and applied to selected devices, and further overrides can also be applied to individual devices.

Some familiarity with the ICA Administration Console is assumed here. For more information, see the

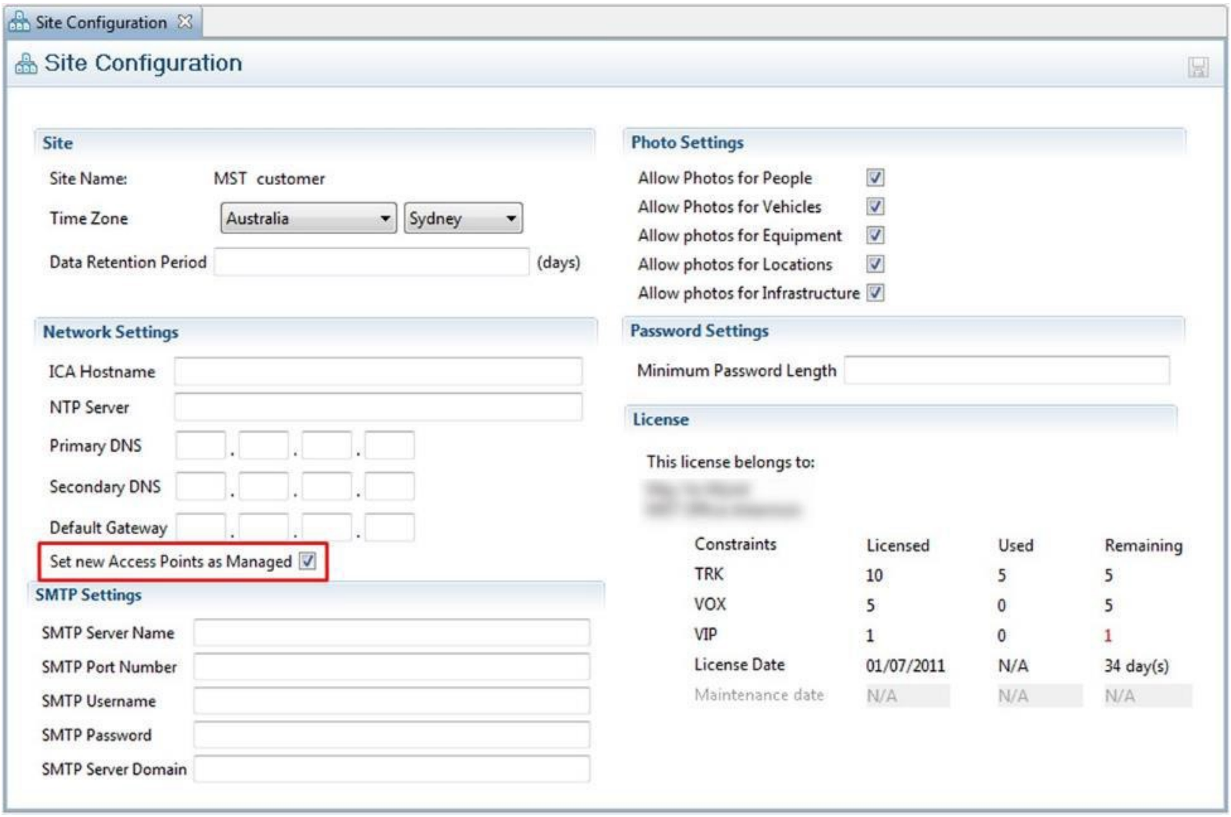
ICA Administration Console User Manual available from MST.

There are three editors in the ICA Administration Console with relevant settings:

- Configuration **>** Site Configuration
- Configuration **>** AP Config Templates
- Devices **>** Access Points

8.1.1 Site Configuration

This editor contains the option to **Set new Access Points as Managed** - If checked, all newly discovered Access Points will be configured according to the **Site Default** template by the ICA. If disabled, new APs must either have their management settings configured in the **Devices** > **Access Points** editor, or be configured manually.



Site

Site Name: MST customer

Time Zone: Australia / Sydney

Data Retention Period: (days)

Network Settings

ICA Hostname

NTP Server

Primary DNS

Secondary DNS

Default Gateway

Set new Access Points as Managed ☑

SMTP Settings

SMTP Server Name

SMTP Port Number

SMTP Username

SMTP Password

SMTP Server Domain

Photo Settings

Allow Photos for People ☑

Allow Photos for Vehicles ☑

Allow photos for Equipment ☑

Allow photos for Locations ☑

Allow photos for Infrastructure ☑

Password Settings

Minimum Password Length

License

This license belongs to:

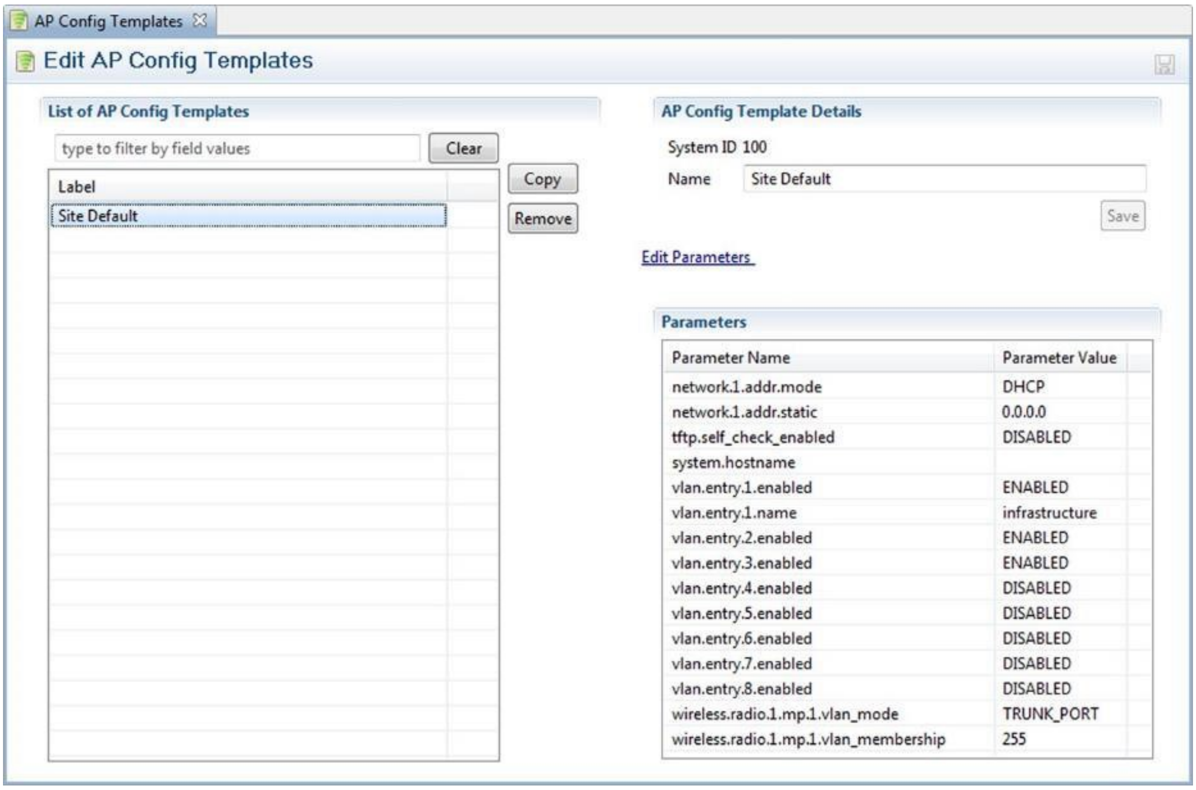
[redacted]

Constraints	Licensed	Used	Remaining
TRK	10	5	5
VOX	5	0	5
VIP	1	0	1
License Date	01/07/2011	N/A	34 day(s)
Maintenance date	N/A	N/A	N/A

8.1.2 AP Config Templates

The ICA is installed with one AP Template: **Site Defaults**. This is a special AP Template which defines the settings that new APs will automatically pick up if **Set new Access Points as Managed** is ticked in the **Site Configuration** editor. This template cannot be deleted, but new templates can be copied from it and modified separately.

NOTE: Once a template is applied to an AP, any manual changes made to settings listed in the template will be reverted automatically to the template default. Settings that are not defined by the template can be changed freely.



Label
Site Default

System ID 100

Name: Site Default

Parameter Name	Parameter Value
network.1.addr.mode	DHCP
network.1.addr.static	0.0.0.0
tftp.self_check_enabled	DISABLED
system.hostname	
vlan.entry.1.enabled	ENABLED
vlan.entry.1.name	infrastructure
vlan.entry.2.enabled	ENABLED
vlan.entry.3.enabled	ENABLED
vlan.entry.4.enabled	DISABLED
vlan.entry.5.enabled	DISABLED
vlan.entry.6.enabled	DISABLED
vlan.entry.7.enabled	DISABLED
vlan.entry.8.enabled	DISABLED
wireless.radio.1.mp.1.vlan_mode	TRUNK_PORT
wireless.radio.1.mp.1.vlan_membership	255

New templates are created by copying an existing template (initially the only one to copy is **Site Defaults**). A copied template will start with the same parameters as the original, but they are not linked, so further changes to one will not affect the other. To create a new template, select another template from the list and click the **Copy** button. To delete a template, click the **Remove** button.

AP Config Template Details

This section contains the details for each template:

- **System ID** is an automatically assigned identifier used by the ICA.
- **Name** - A name or description for the template.
- **Edit Parameters** - Individual parameters can be selected and modified, or ignored, for each template by clicking this link to open the **Parameters** dialogue box (See **Edit Parameters** section below).

Editing Parameters

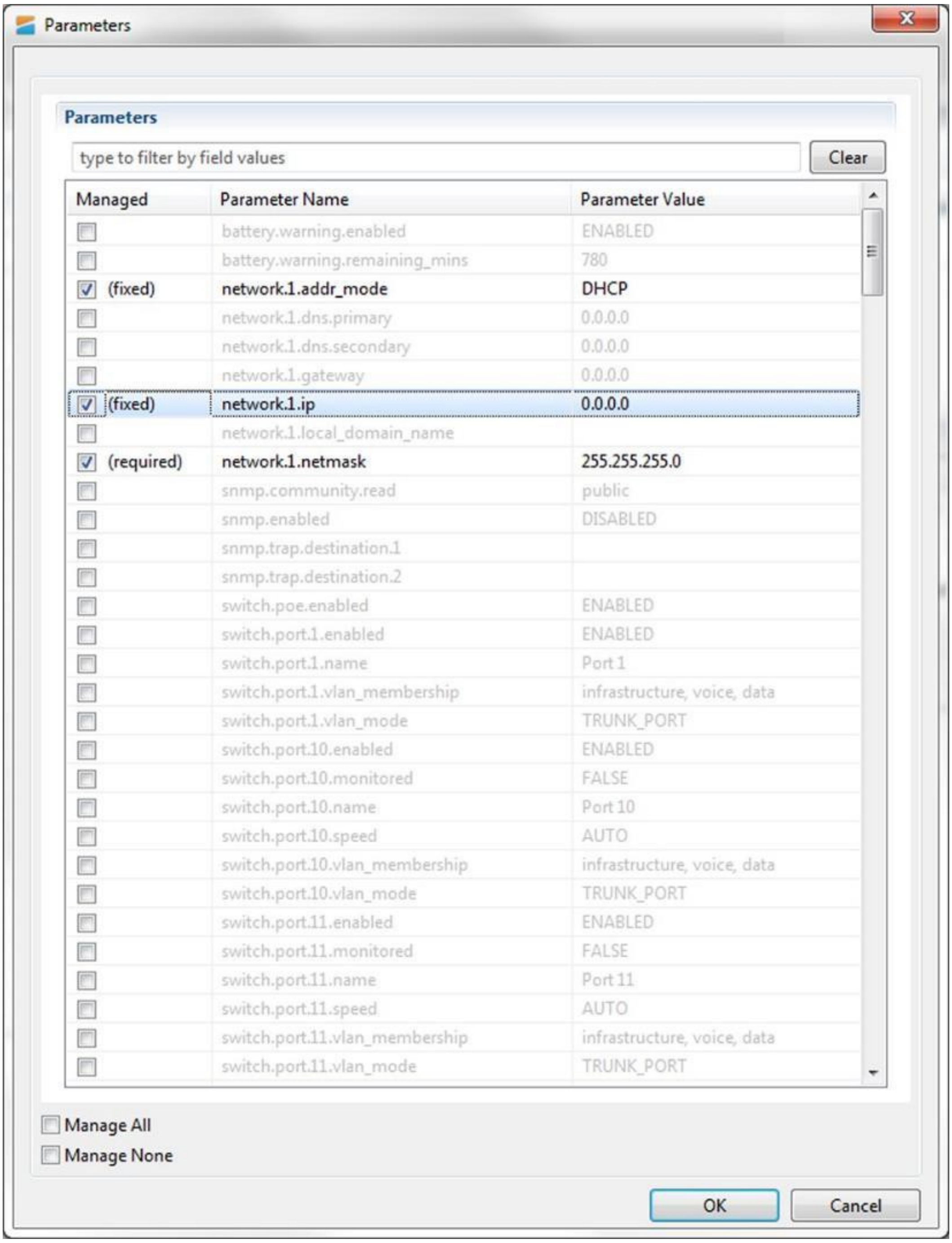
In the **Parameters** dialog box, search for the desired parameter by typing all or part of any of the displayed column values:

- **Managed:** To manage a parameter, tick the checkbox in this column. `Fixed` entries cannot be disabled or changed, while `required` entries can be edited but not disabled. Unmarked entries can be disabled by unticking the checkbox.
- **Parameter Name:** For more information on parameters that affect a specific AP model on the network, see the **TFTP Parameters** section of the user manual for that model.
- **Parameter Value:** To edit a parameter, click on the parameter value and either enter a new value (e.g. names and IP addresses) or select a new value from the dropdown menu (e.g. `ENABLED` / `DISABLED`).

When all required changes have been made, click **OK** to close the dialog box. The **Managed** status of all available parameters can be changed at once using the **Manage All** and **Manage None** checkboxes below the list.

8.1.3 Access Point

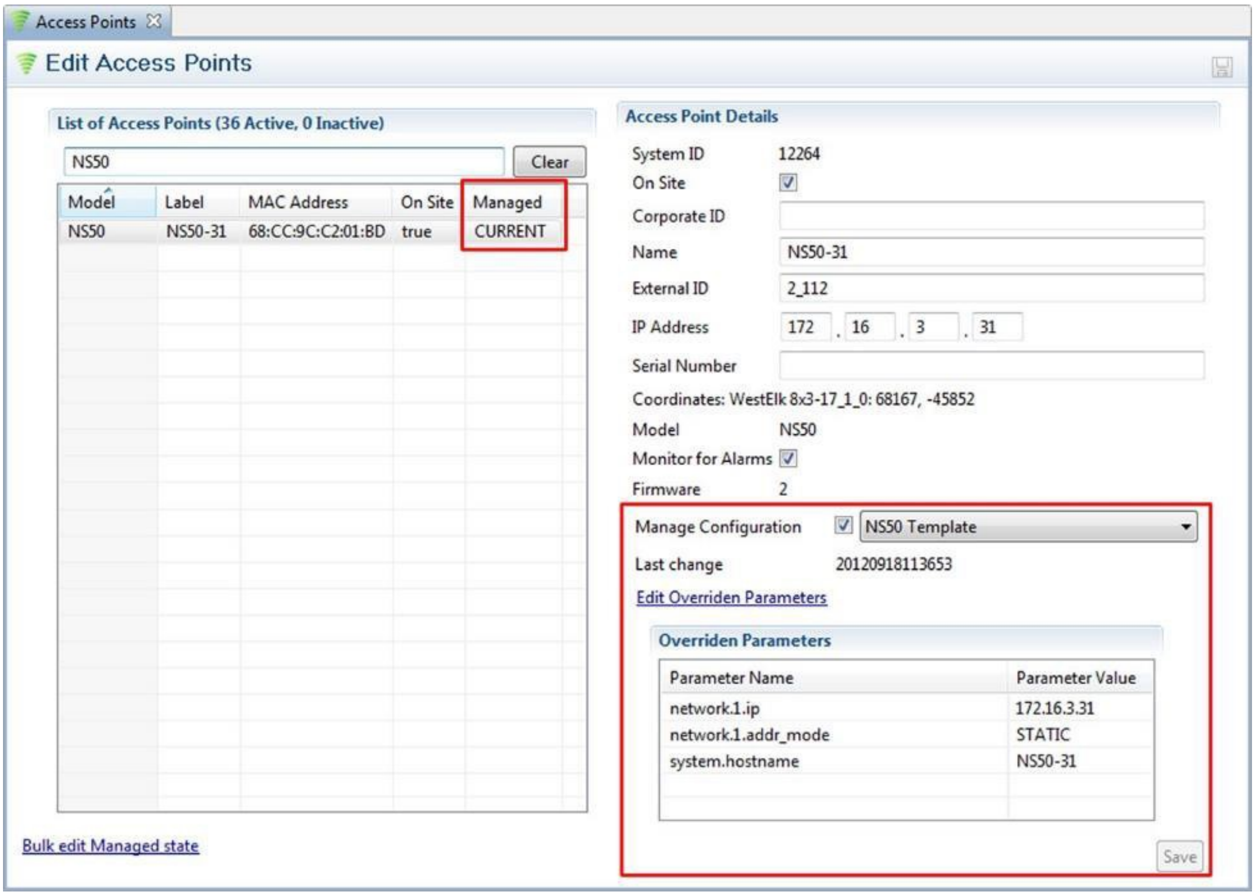
Access Points (APs) become visible to the ICA after the map containing them is first synchronised from AeroScout. Once visible, APs are automatically added to the **List of Access Points**



Managed	Parameter Name	Parameter Value
☐	battery.warning.enabled	ENABLED
☐	battery.warning.remaining_mins	780
☑ (fixed)	network.1.addr_mode	DHCP
☐	network.1.dns.primary	0.0.0.0
☐	network.1.dns.secondary	0.0.0.0
☐	network.1.gateway	0.0.0.0
☑ (fixed)	network.1.ip	0.0.0.0
☐	network.1.local_domain_name	
☑ (required)	network.1.netmask	255.255.255.0
☐	snmp.community.read	public
☐	snmp.enabled	DISABLED
☐	snmp.trap.destination.1	
☐	snmp.trap.destination.2	
☐	switch.poe.enabled	ENABLED
☐	switch.port.1.enabled	ENABLED
☐	switch.port.1.name	Port 1
☐	switch.port.1.vlan_membership	infrastructure, voice, data
☐	switch.port.1.vlan_mode	TRUNK_PORT
☐	switch.port.10.enabled	ENABLED
☐	switch.port.10.monitored	FALSE
☐	switch.port.10.name	Port 10
☐	switch.port.10.speed	AUTO
☐	switch.port.10.vlan_membership	infrastructure, voice, data
☐	switch.port.10.vlan_mode	TRUNK_PORT
☐	switch.port.11.enabled	ENABLED
☐	switch.port.11.monitored	FALSE
☐	switch.port.11.name	Port 11
☐	switch.port.11.speed	AUTO
☐	switch.port.11.vlan_membership	infrastructure, voice, data
☐	switch.port.11.vlan_mode	TRUNK_PORT

☐ Manage All

☐ Manage None



Edit Access Points

List of Access Points (36 Active, 0 Inactive)

NS50

Model	Label	MAC Address	On Site	Managed
NS50	NS50-31	68:CC:9C:C2:01:BD	true	CURRENT

Access Point Details

System ID	12264
On Site	☑
Corporate ID	
Name	NS50-31
External ID	2_112
IP Address	172 . 16 . 3 . 31
Serial Number	

Coordinates: WestElk 8x3-17_1_0: 68167, -45852

Model	NS50
Monitor for Alarms	☑
Firmware	2
Manage Configuration	☑ NS50 Template
Last change	20120918113653

Overriden Parameters

Parameter Name	Parameter Value
network.1.ip	172.16.3.31
network.1.addr_mode	STATIC
system.hostname	NS50-31

List of Access Points

The **Managed** column shows CURRENT for managed devices with up-to-date settings, or PENDING for devices awaiting newly updated settings.

To edit an existing entry: Click on that entry, fill in the relevant fields on the right, then click the **Save** button or press Ctrl+S:

Manage Configuration

To have an AP's configuration managed by the ICA, tick the **Manage Configuration** checkbox, and select the correct template from the dropdown menu.

Last Change shows the time of the last change to the AP's configuration management settings if known, and PENDING if new settings are waiting to be sent.

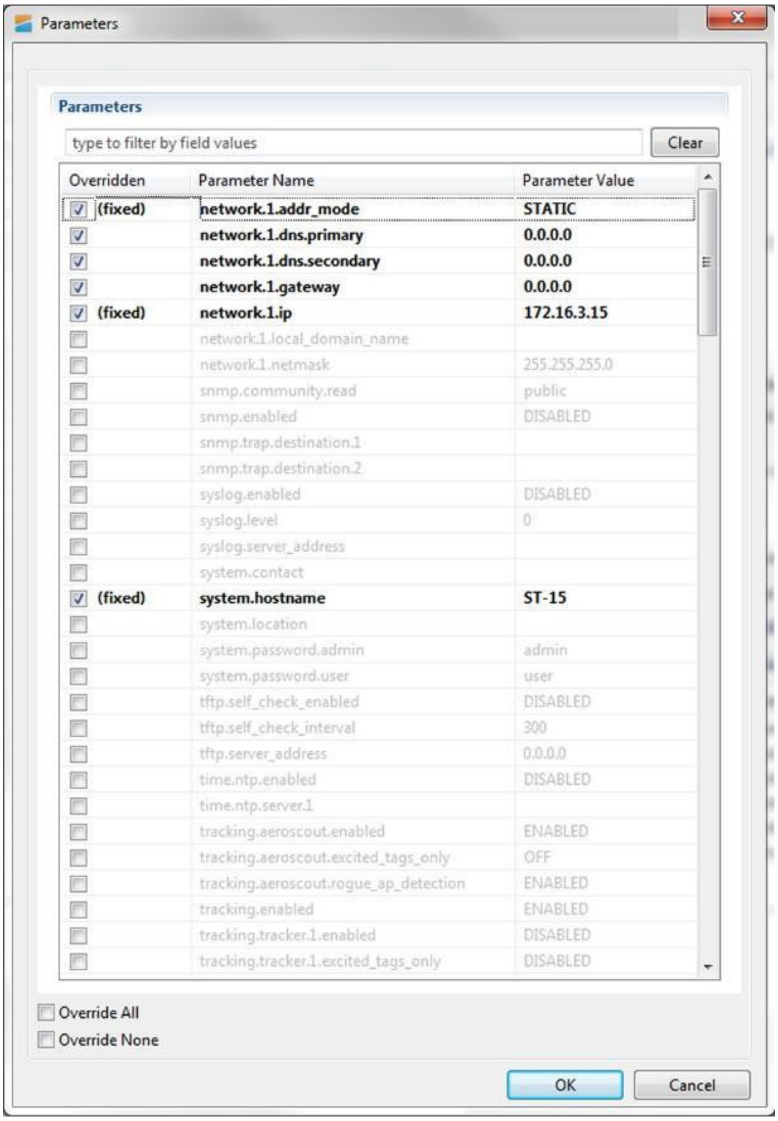
IMPORTANT: If any changes are made to a managed AP's settings via the web interface that conflict with the selected template or overridden parameters (see below), those changes will be automatically reverted by the ICA. Settings that are not defined in the template will be ignored.

Editing Overridden Parameters

Individual parameters specified in a template can be modified for the selected AP. To modify any parameters, click **Edit Overridden Parameters**.

In the **Parameters** dialog box, search for the desired parameter by typing all or part of any of the displayed column values:

- **Overridden:** To override a parameter, tick the checkbox in this column. `Fixed` entries are enabled by default and cannot be disabled or changed. `Required` entries are not enabled by default; once ticked, they can be edited but not disabled. Unmarked entries can be disabled by unticking the checkbox.
- **Parameter Name:** For more information on parameters, see the **TFTP Parameters** section of the user manual for the selected access point.
- **Parameter Value:** To edit a parameter, click on the parameter value and either enter a new value (e.g. names and IP addresses) or select a new value from the dropdown menu (e.g. `ENABLED` / `DISABLED`).



Overridden	Parameter Name	Parameter Value
☑ (fixed)	network.1.addr_mode	STATIC
☑	network.1.dns.primary	0.0.0.0
☑	network.1.dns.secondary	0.0.0.0
☑	network.1.gateway	0.0.0.0
☑ (fixed)	network.1.ip	172.16.3.15
□	network.1.local_domain_name	
□	network.1.netmask	255.255.255.0
□	snmp.community.read	public
□	snmp.enabled	DISABLED
□	snmp.trap.destination.1	
□	snmp.trap.destination.2	
□	syslog.enabled	DISABLED
□	syslog.level	0
□	syslog.server_address	
□	system.contact	
☑ (fixed)	system.hostname	ST-15
□	system.location	
□	system.password.admin	admin
□	system.password.user	user
□	tftp.self_check_enabled	DISABLED
□	tftp.self_check_interval	300
□	tftp.server_address	0.0.0.0
□	time.ntp.enabled	DISABLED
□	time.ntp.server.1	
□	tracking.aeroscout.enabled	ENABLED
□	tracking.aeroscout.excited_tags_only	OFF
□	tracking.aeroscout.rogue_ap_detection	ENABLED
□	tracking.enabled	ENABLED
□	tracking.tracker.1.enabled	DISABLED
□	tracking.tracker.1.excited_tags_only	DISABLED

□ Override All
□ Override None

When all required changes have been made, click **OK** to close the dialog box. The override status of all available parameters can be changed at once using the **Override All** and **Override None** checkboxes below the list.

8.2 TFTP Server Overview

Centralised configuration management using ICA v1.3.1 or earlier, or a 3rd party TFTP server, involves the following steps:

1. Configure a TFTP server on the network. The ICA is preconfigured for this purpose. Configuring a 3rd party server is outside of the scope of this document.
2. Define a site configuration file that contain global settings to all network devices on the site.
3. Define device configuration files that contain specific settings for each device, which override global settings.
4. Apply the configuration files to each device and reboot.

Network devices read and apply the configuration files from the TFTP server as shown below.

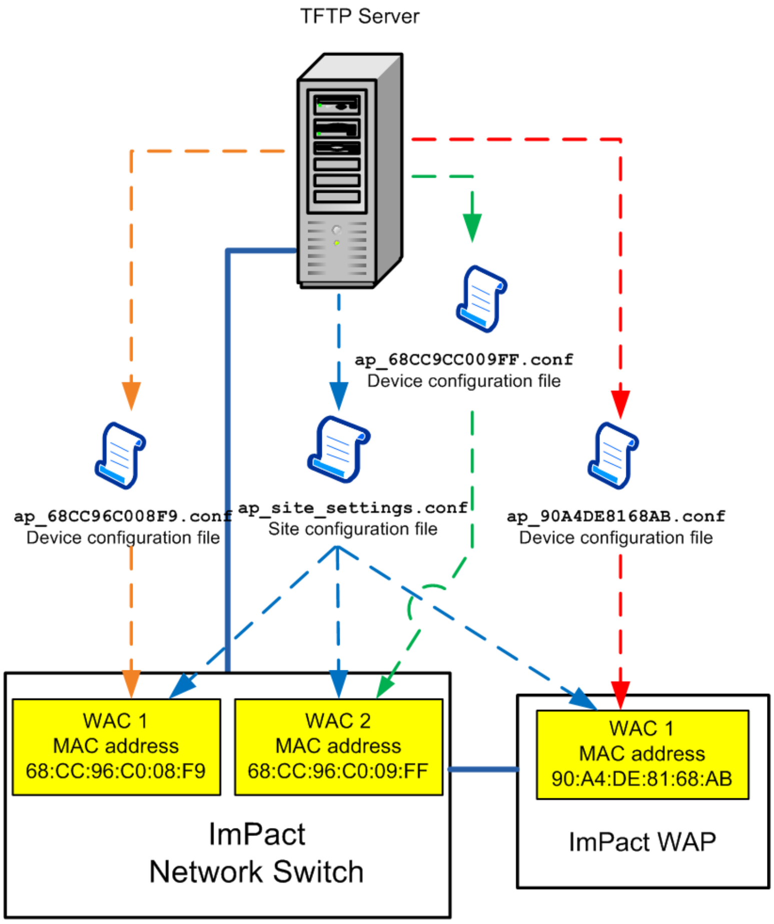


Figure 39: Centralised configuration management

8.2.1 Editing Site Configuration Files

Site configuration files contain common settings for all devices in a network. The site configuration file has the naming convention **ap_site_settings.conf**. This file is retrieved by devices using TFTP.

NOTE: The same site configuration file can be used to configure network switch units and WAPs in a network. When the site configuration file is applied to WAPs, all switch port settings are ignored by the WAP.

The site configuration file can be opened on a PC and edited using a text editor. Parameters are changed by modifying the text and saving the file. A description of the editable parameters are covered in the following sections.

To edit a site configuration file:

1. Open a text file editor on your PC.
2. Locate and open the site configuration file **ap_site_settings.conf**. This is usually stored in the file directory folder of the TFTP server.
    1. Edit the parameters as required.
    2. Save the site configuration file in the directory folder of the TFTP server.

8.2.2 Editing Device Configuration Files

Device configuration files contain settings specific to each WAC in the network device. A device configuration file is created for each WAC. Device configuration files follow the naming convention **ap_MACaddress.conf** where **MACaddress** is the MAC address of the WAC. A device will recognise and apply the device configuration file based on a comparison of the MAC address in the file name.

Note that any parameter from the site configuration file can override parameters in a device configuration file. However, it is recommended that only the settings that are different be entered into the device configuration file in order to make maintenance easier.

A device configuration file configures individual settings for each device as shown below. The device configuration file can be edited using a text editor such as Wordpad or Notepad. The example below includes settings that are commonly over-ridden. All other settings are inherited from the global site configuration file. Comments are prefixed with a hash symbol (#) and are ignored by the device. These are not necessary for configuration but may be included for convenience.

```
# Mine Site Technologies Network and power distribution module ConfigFile

# System
# ======
#
system.hostname=AP57R2 system.location=Mine Location 16

# Wireless Radio Configuration
# ===========================
```

The parameters shown in the example device configuration file are described in the following table.

Section	Parameter	Description	Settings
System	system.hostname	Network switch name.	Each device should have a unique name identifier.
System	system.location	Location name of the network switch.	It is recommended the location name is relevant to the physical location of the device.
Wireless Radio Configuration	wireless.radio.1.channel	Wi-Fi channel that the WAC will operate on.	It is recommended WACs in proximity of each other have assigned channels 1, 6 and 11. This minimises signal overlap and interference.
Power over Ethernet	switch.poe.enabled	Enabling PoE supply on the network switch.	0 = Disabled, 1 = Enabled **NOTE:** This setting is not applicable to WAPs and will be ignored when the file is applied to a WAP.

To edit a device configuration file:

3. Open a text file editor on your PC.
4. Locate and open the device configuration file **ap_MACaddress_settings.conf**. This is usually stored in the file directory folder of the TFTP server.
5. Edit the parameters as required.
6. In the directory folder of the TFTP server, save the file using the naming **ap_MACaddress_settings.conf**, where **MACaddress** is the MAC address of the WAC card to configure.

8.3 TFTP Parameters

Below is a list of configurable parameters for AXON Core, classified by type.

Network

Common LAN settings to all devices on a network as shown below.

Field	Description
network.1.addr.mode	`0:` Static - fixed IP address configured manually on the device `1:` DHCP - IP address assigned automatically
network.1.addr.static	The IP address of the device, if Static.
network.1.netmask	Identifies the subnet the IP address belongs to for the device.

network.1.local_domain_name	The domain name of the local network.
Field	**Description**
network.1.gateway	The IP address of the default gateway.
network.1.dns.primary	The DNS server to be used when looking up host names.
network.1.dns.secondary	The backup DNS server to be used when looking up host names.

Configuration Management

These settings are only required for 3rd party TFTP servers or ICA v1.3.1 and earlier.

Field	Description
tftp.self_check_enabled	`0:` Disabled `1:` Enabled - device will check the TFTP server for changes at startup and every "tftp.self_check_interval" minutes
tftp.self_check_interval	The number of seconds elapsed before checking for new TFTP settings. If zero, do not perform regular checks.
tftp.server_address	The TFTP server address to use. If blank, and in DHCP mode, use the address supplied by DHCP.

System

Network names, contact details and passwords can be edited in the system section of the configuration file as shown below.

Field	Description
system.contact	Contact name for the network devices.
system.location	Location of the network devices.
system.password.admin	Administrator password. The default password is "admin".
system.password.user	User password. The default password is "user".
system.hostname	Device hostname as displayed in the Device Scanner, should be unique for each device.

NTP (Network Time Protocol)

The **Time** section shown below defines NTP (Network Time Protocol) server settings for the network switch.

Field	Description
time.ntp.enabled	`0`: Disabled `1`: Enabled - device will synchronise time with an NTP server (requires network or internet access to an NTP server).
time.ntp.server1	Hostname or IP address of NTP server. For example time.windows.net.

Logging

System message logging settings.

Field	Description
syslog.enabled	`0`: Disabled `1`: Enabled
syslog.server_address	The hostname or IP address of the syslog server
syslog.level	All messages from 0 to the selected number will be logged. `0`: Emergency `1`: Alert `2`: Critical `3`: Error `4`: Warning `5`: Notice `6`: Informational `7`: Debug

SNMP

Simple Network Management Protocol settings. At present, the ICA only uses this protocol to monitor for Port Up/Port Down errors on AXON Core, and is not affected by the settings below, adjust only if required for 3rd party monitoring software.

Field	Description
snmp.enabled	`0`: Disabled `1`: Enabled

Field	Description
snmp.community.read	The SNMP community string for reads. Unless otherwise necessary, this is usually left as `public`.
snmp.trap.destination.1	The hostname or IP address of the primary SNMP trap.
snmp.trap.destination.2	The hostname or IP address of the secondary SNMP trap.

Asset Tracking and Location Servers

This section configures asset tracking and location servers, consisting of AeroScout Positioning Engines or MST Tracker Engines. This is where AeroScout tag and Wi-Fi client device information is sent.

Configuration is not required when communicating with an AeroScout positioning engine.

Field	Description
tracking.enabled	`0`: Disabled `1`: Enabled
tracking.aeroscout.enabled	Tracking of AeroScout tags. `0`: Disabled `1`: Enabled
tracking.aeroscout.rogue_ap_detection	Reports non-compatible access points on the network to the AeroScout Engine. `0`: Disabled `1`: Enabled
tracking.aeroscout.excited_tags_only	Only sends tracking information for detected tags within range of an exciter. `0`: Disabled `1`: Enabled
tracking.rssi_threshold.tag	By default it is set at `-95`. Only tag reports higher than this signal strength threshold will be sent to the positioning engines.
tracking.rssi_threshold.mu	By default it is set at `-95`. The default value should not be changed without understanding the implications. Only Wi-Fi client frames higher than this signal strength threshold will be sent to the positioning engines.

These settings configure up to two MST Tracker Engines that the access point will send information to. The "x" in each parameter is replaced by the tracking engine number.

Field	Description
tracking.tracker.x.enabled	0: Disabled 1: Enabled
tracking.tracker.x.excited_tags_only	Only sends tracking information for detected tags within range of an exciter. 0: Disabled 1: Enabled
tracking.tracker.x.server_address	The IP address of the MST Tracking Engine.
tracking.tracker.x.server_port	UDP port to be used by messages sent to the MST Tracker Engine. Default 1142.
tracking.tracker.x.status_reporting_interval	The period in seconds between status reports being sent to the MST Tracker Engine. These status reports are used to determine Access point availability.

VLAN Configuration

The VLANs section defines VLANs for the devices as shown below. For large networks it is recommended that VLAN settings are applied to all network devices consistently by using centralised configuration management. Up to 8 VLANs can be defined, the "x" in each address is replaced by the VLAN number 1-8. By default, the site configuration file has some VLANs predefined based on commonly used applications. VLAN parameters are described in the table below.

Field	Description
vlan.enabled	0: Disabled 1: Enabled
vlan.entry.x.enabled	0: Disabled 1: Enabled
vlan.entry.x.id	The VLAN ID that will be tagged to frames sent to trunk ports from VLAN *x*.
vlan.entry.x.priority	Priority from 0-7 (with 7 being the highest) that is assigned to frames on VLAN *x*.
vlan.entry.x.name	The administrative name for VLAN *x*.

NOTE: The Infrastructure VLAN cannot be edited or disabled because the management CPU is on this VLAN.

Wireless Radio

General wireless radio settings.

Field	Description	Settings
wireless.radio.1.enabled		• 0: Disabled • 1: Enabled
wireless.radio.1.beacon_period	The amount of time between beacon transmissions.	Default 100ms
wireless.radio.1.region	Limits available channels to those allowed by local regulations.	• Israel • USA • Hong Kong • Canada • Australia • Japan
		• Singapore • Korea • Latin America • Venezuela • World
wireless.radio.1.channel		Default 6.
wireless.radio.1.transmit_power	Percentage of Tx output power from the wireless transmitter.	Default 100, lower only if device is interfering with other wireless signals.
wireless.radio.1.antenna.tx	Antenna for transmission of wireless frames.	• 1: Main • 2: Aux • 3: Diversity
wireless.radio.1.antenna.rx	Antenna for reception of wireless frames.	• 1: Main • 2: Aux • 3: Diversity
wireless.radio.1.auto_channel_select.enabled	Enables automatic channel selection for wireless radio	• 0: Disabled • 1: Enabled
wireless.radio.1.auto_channel_select.channel_list	A comma separated list of available Wi-Fi channels	e.g. 1,6,11

Wireless Network Configuration

Each WAC in a device can have up to four wireless SSIDs, each with different security settings and different mappings to VLANs.

Field	Description	Settings
wireless.radio.1.ap.x.enabled	Enables or disables the wireless network.	0: Disabled 1: Enabled
wireless.radio.1.ap.x.ssid	The name of the wireless network visible to client devices.	Choose a network name that relates closely to its function. For example "MST-VOICE".
wireless.radio.1.ap.x.invisibility	Enables or disables visibility of the wireless network to anyone within range.	Click on the Visible option button to enable wireless network visibility.
wireless.radio.1.ap.x.dtim_interval	A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. Wireless clients detect the beacons and awaken on the DTIM interval to receive the broadcast and multicast messages.	Valid settings are between 1 and 255. The recommended DTIM interval is 1.
wireless.radio.1.ap.x.vlan_membership	The VLAN assigned to devices on the wireless network. VLANs are defined in the VLAN configuration section of the site configuration file.	VLAN range from 1-8.
wireless.radio.1.ap.x.security_mode	Three selectable wireless security modes: WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. WPA-Enterprise requires a RADIUS authentication server.	1: Open 2: WEP 3: WPA-Personal 4: WPA-Enterprise

The following settings configure options specific to WEP or WPA security; only the options specific to the chosen security mode need be configured.

Field	Description	Settings
wireless.radio.1.ap.x.wep.auth		1: Open 2: Shared key
wireless.radio.1.ap.x.wep.keylen	The WEP key length, longer is more secure	0: Short Key (64 bit) 1: Long Key (128 bit)
wireless.radio.1.ap.x.wep.use_key		1-4 Determines which of the following preconfigured keys to use
wireless.radio.1.ap.x.wep.key.1	The first WEP key	e.g. mine1
wireless.radio.1.ap.x.wep.key.2	The second WEP key	e.g. mine2
wireless.radio.1.ap.x.wep.key.3	The third WEP key	e.g. mine3
wireless.radio.1.ap.x.wep.key.4	The fourth WEP key	e.g. mine4
wireless.radio.1.ap.x.wpa.mode	The WPA mode.	1: WPA 2: WPA/WPA2 3: WPA2 Only (recommended)
wireless.radio.1.ap.x.wpa.cipher	The encryption type	1: TKIP 2: AES 3: TKIP/AES
wireless.radio.1.ap.x.wpa.rekey_time	The WPA group rekey interval	e.g. 3600s
wireless.radio.1.ap.x.wpa.psk	The Pre-Shared Key for WPA-Personal mode	e.g. password123

Wireless EAP Configuration

The **Wireless EAP** section is used to configure the RADIUS server as shown below. This is applicable for wireless networks configured with WPA Enterprise security mode. A primary and secondary (backup) RADIUS server can be set up and configured. A description of the editable parameters are shown in the following table. The "x" in each parameter below should be replaced with "primary" or "secondary".

Field	Description	Settings
wireless.eap.reauth_time	Amount of time in minutes before a client device is required to re-authenticate.	Setting is at 120 minutes by default.
wireless.eap.x.auth_mac	Access to the RADIUS server by confirmation of the MAC address of the client device.	0: Disabled 1: Enabled
wireless.eap.x.server_address	The IP address of the authentication server.	default 0.0.0.0
wireless.eap.x.server_port	The port number used to connect to the authentication server.	By default the port number is 1815.
wireless.eap.x.shared_secret	Password used by the Access point to access the RADIUS server.	Password that matches with the authentication server.

WDS

The Wireless Distribution System (WDS) allows network devices to connect wirelessly where a fibre or ethernet connection is not practical. Up to six peered devices can be configured.

Field	Description	Settings
wireless.radio.1.wds.enabled	Enables the WDS network	0: Disabled 1: Enabled
wireless.radio.1.wds.ssid	The SSID of the network	
wireless.radio.1.wds.security_mode	Three selectable wireless security modes: WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. WPA-Enterprise requires a RADIUS authentication server.	1: Open 2: WEP 3: WPA-Personal 4: WPA-Enterprise
wireless.radio.1.wds.wep.auth		1: Open 2: Shared key

Field	Description	Settings
wireless.radio.1.wds.wep.keylen	The WEP key length, longer is more secure	`0`: Short Key (64 bit) `1`: Long Key (128 bit)
wireless.radio.1.wds.wep.use_key		`1-4` Determines which of the following preconfigured keys to use
wireless.radio.1.wds.wep.key.1	The first WEP key	e.g. `mine1`
wireless.radio.1.wds.wep.key.2	The second WEP key	e.g. `mine2`
wireless.radio.1.wds.wep.key.3	The third WEP key	e.g. `mine3`
wireless.radio.1.wds.wep.key.4	The fourth WEP key	e.g. `mine4`
wireless.radio.1.wds.wpa.mode	The WPA mode.	`1`: WPA `2`: WPA/WPA2 `3`: WPA2 Only (recommended)
wireless.radio.1.wds.wpa.cipher	The encryption type	`1`: TKIP `2`: AES `3`: TKIP/AES
wireless.radio.1.wds.wpa.rekey_time	The WPA group rekey interval	e.g. `3600s`
wireless.radio.1.wds.wpa.psk	The Pre-Shared Key for WPA-Personal mode	e.g. `password123`

For the following peer-specific settings, the "x" is replaced with 1-6.

Field	Description	Settings
wireless.radio.1.wds.peer.x.enabled		`0`: Disabled `1`: Enabled
wireless.radio.1.wds.peer.x.name	The name of the port or peered device	e.g. `WDS Port x`
wireless.radio.1.wds.peer.x.mac	The MAC address of the peered device	e.g. `00:00:00:00:00:00`

Switch Configuration

These settings control switch ports 1-8 and assign VLANs. The following settings are available for all ports. Note that the x in each parameter is replaced by the relevant port number.

Field	Description
switch.port.x.enabled	0: Disabled 1: Enabled
switch.port.x.name	The name of the port
switch.port.x.vlan_mode	1: ACCESS_PORT 2: TRUNK_PORT
switch.port.x.vlan_membership	Bitmask of the VLAN ID of which the port is a member.

Additionally, ports 5-8 include the following:

Field	Description
switch.port.x.speed	1: 10 HALF 2: 10 FULL 3: 100 HALF 4: 100 FULL 5: 1000 HALF 6: 1000 FULL 7: AUTO

PoE (Power Over Ethernet)

This setting controls the 48VDC PoE supply feature, and is enabled by default.

Field	Description
switch.poe.enabled	0: Disabled 1: Enabled

Appendix A: Troubleshooting Guide

This chapter assists in the diagnosis and resolution of problems with AXON Core and AXON Air installation and operation.

Problem	Possible Causes	Solution
PoE devices are not operational.	Insufficient power supplied to AXON Core to power PoE devices.	Measure voltage supplied to AXON Core. If the voltage measures less than 20VDC, a JB11 junction box is required to enable the measurement.
	The PoE rail is not enabled.	Enable the PoE feature in the web browser interface.
PoE status LED turned orange	Power management system detected that the associated client device has exceeded its declared power consumption	Check the associated PoE port power allocation via AXON core webpage. If incorrect PoE power limit has been assigned previously change the assignment. Check if the client device is faulty.
LEDs on the network and power distribution module are not on.	AXON Core has no power.	Check if power is connected from either the composite cable or the test / configuration jig to AXON Core. Verify the network switch is connected to an operational power supply. Test the power supply is supplying the correct voltage/current for AXON Core. Check there is sufficient power available if extending AXON Core infrastructure.
The fibre activity light is not on.	AXON Core fibre connector is not connected.	Verify the fibre link is connected and active.
The wireless network cannot be configured from AXON Air web browser interface.	There is a network access issue.	Check that AXON Core is properly installed, LAN connections are connected properly and the unit is powered on. If the PC uses a fixed (static) IP address, check that it is using an IP address within the IP range of the network switch. Check that the VLAN settings on the devices upstream on the network are not restricting access.

Power supply instability.	Incorrect Earthing scheme.	Check AXON Air antennas are insulated from ground. Check PCB in the network switch has a floating earth (not grounded).
	There are too many network devices on the one power supply.	Add additional power supplies. Isolate network segments so that in event of power supply failure, an overload condition is avoided.
Signal loss in the fibre optic cable.	Composite connector or fibre port is dirty.	Check the connectors and fibre ports are clean. Clean using alcohol wipes or fibre optic cleaning kits. NB: Do not use air spray as the compressor oil can leave residue.
The Internet or the LAN cannot be accessed with a wireless-capable PC.	There is a configuration problem with the PC.	Re-boot the computer with the wireless adapter that has had TCP/IP changes applied to it. The computer with the wireless adapter may not have the correct TCP/IP settings to communicate with the network. Restart the computer and check the network settings. If this is not resolved, try changing the DHCP setting to obtain an IP address automatically. Check AXON Core default configuration against the configuration of other devices on the network.
	The port on AXON Core is disabled.	Check the port activity light is on. If the light is not on, connect a PC to the network switch to access the web browser interface. Go to the Basic>Switch screen and check the port is enabled.
	VLAN(s) on the port are not properly configured.	Connect a PC to another port on the network switch to access the network. In the web browser interface, check that VLAN membership is assigned to the port for Internet / LAN access.

Appendix B: Composite Cable Testing

This appendix describes fibre optic cable continuity and testing. Fibre optic cable testing includes visual inspection and power loss testing.

B1: Visual Inspection of the Fibre Optic Cable

Fibre optic cable can be inspected by visually tracing and inspecting the connector.

Visual Tracing

Checking for continuity diagnoses whether the fibre optic cable is damaged or broken. A visible light "fibre optic tracer" or "pocket visual fault locator" connected to a fibre optic connector.

Attach a fibre optic cable to the visual tracer and look at the other end to see if light is transmitting through the fibre.

If there is no light, there is a damaged or broken section of the fibre in the composite cable.

Visual Connector Inspection

A visual inspection of the fibre optic termination is usually carried out using a fibre optic microscope. It is important the fibre termination has a clean, smooth, polished, and scratch free finish. Any signs of cracks, chips or dirt will affect connectivity.

B2: Measuring and Testing for Power Loss

Measuring power and loss requires a Optical Time-Domain Reflectometer (OTDR) with a suitable adapter matching the fibre optic connector being tested.

To measure power in fibre optic cable:

1. Set the OTDR to ‘dBm’ and set the wavelengths according to the fibre optic cable being tested.
2. Attach the OTDR to the fibre optic cable at the receiving end to measure the output.
3. Compare the output with a reference test cable.

To measure power loss in fibre optic cable:

1. Set the power meter to ‘dB’ for a relative power range and select the wavelength required for the test.
2. Perform a single-ended loss test by connecting the cable to be tested to the reference cable and measuring power loss at the receiving end.
3. Perform a double-ended loss test by attaching the cable between two reference cables that are attached to the source and to the OTDR. If high losses are measured, reverse the cable and test in the opposite direction using the single ended test.

A guideline on power losses are shown in the table below.

Component	Power loss
Connector	0.5 dBi
Multi-mode fibre	1 dBi / km @ 1300nm
Single-mode fibre	0.5 dBi / km @ 1300nm 0.4 dBi / km @ 1550nm

Appendix C: Ethernet Cable Specifications

Ethernet cable must conform to the following specifications when connecting to network devices:

- Polyethylene jacket
- 5.0-6.5mm outer diameter
- Stranded cable for lengths less than 30m
- Solid core cable for lengths greater than 30m

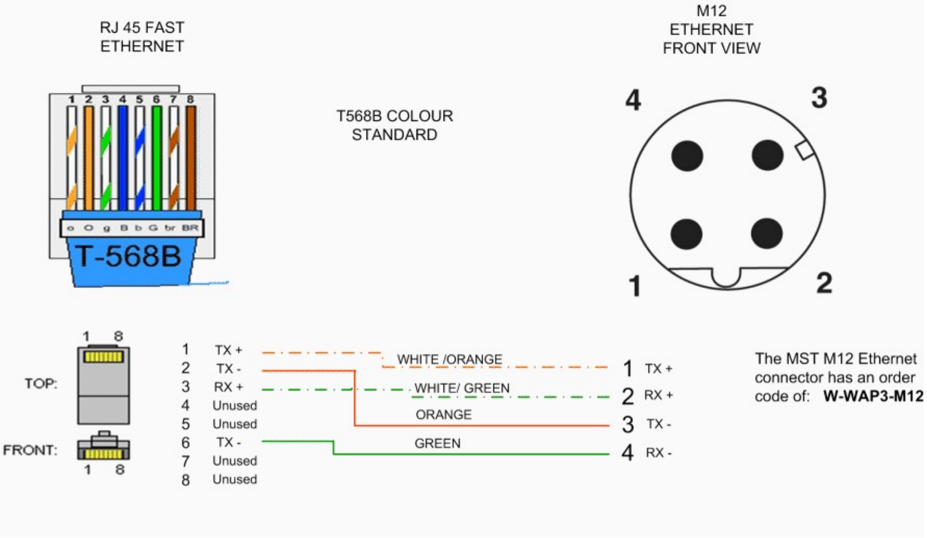
Cable and Parts Description

Description	Order Code
Bayonet back-shell for RJ45 connector	W-AXON Core-RJ45-PLUG

The choice of RJ45 crimp will depend on the type of wire used (stranded or solid core). Generic brand crimps may be used.

NOTE: Both solid and stranded core RJ45 connectors at AXON Core end require a bayonet back-shell.

RJ45 to M12 Ethernet Cable Wiring Diagram



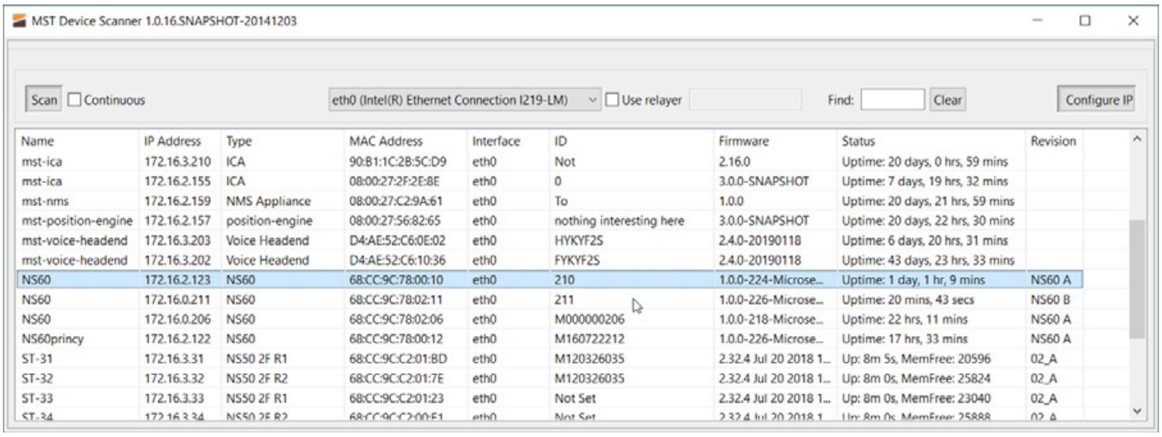
The MST M12 Ethernet connector has an order code of: **W-WAP3-M12**

Appendix D: Device Discovery

The MST Device Scanner can be used to discover and change the IP address of devices from any PC connected to the same network. Upon opening, the Device Scanner will automatically scan

for devices.

To use the Device Scanner, navigate to the folder where the program is stored, and double click devicescanner.exe**.**



MST Device Scanner 1.0.16.SNAPSHOT-20141203

Name	IP Address	Type	MAC Address	Interface	ID	Firmware	Status	Revision
mst-ica	172.16.3.210	ICA	90:B1:1C:2B:5C:D9	eth0	Not	2.16.0	Uptime: 20 days, 0 hrs, 59 mins	
mst-ica	172.16.2.155	ICA	08:00:27:2F:2E:8E	eth0	0	3.0.0-SNAPSHOT	Uptime: 7 days, 19 hrs, 32 mins	
mst-nms	172.16.2.159	NMS Appliance	08:00:27:C2:9A:61	eth0	To	1.0.0	Uptime: 20 days, 21 hrs, 59 mins	
mst-position-engine	172.16.2.157	position-engine	08:00:27:56:82:65	eth0	nothing interesting here	3.0.0-SNAPSHOT	Uptime: 20 days, 22 hrs, 30 mins	
mst-voice-headend	172.16.3.203	Voice Headend	D4:AE:52:C6:0E:02	eth0	HYKYF2S	2.4.0-20190118	Uptime: 6 days, 20 hrs, 31 mins	
mst-voice-headend	172.16.3.202	Voice Headend	D4:AE:52:C6:10:36	eth0	FYKYF2S	2.4.0-20190118	Uptime: 43 days, 23 hrs, 33 mins	
NS60	172.16.2.123	NS60	68:CC:9C:78:00:10	eth0	210	1.0.0-224-Microse...	Uptime: 1 day, 1 hr, 9 mins	NS60 A
NS60	172.16.0.211	NS60	68:CC:9C:78:02:11	eth0	211	1.0.0-226-Microse...	Uptime: 20 mins, 43 secs	NS60 B
NS60	172.16.0.206	NS60	68:CC:9C:78:02:06	eth0	M000000206	1.0.0-218-Microse...	Uptime: 22 hrs, 11 mins	NS60 A
NS60princy	172.16.2.122	NS60	68:CC:9C:78:00:12	eth0	M160722212	1.0.0-226-Microse...	Uptime: 17 hrs, 33 mins	NS60 A
ST-31	172.16.3.31	NS50 2F R1	68:CC:9C:C2:01:BD	eth0	M120326035	2.32.4 Jul 20 2018 1...	Up: 8m 5s, MemFree: 20596	02_A
ST-32	172.16.3.32	NS50 2F R2	68:CC:9C:C2:01:7E	eth0	M120326035	2.32.4 Jul 20 2018 1...	Up: 8m 0s, MemFree: 25824	02_A
ST-33	172.16.3.33	NS50 2F R1	68:CC:9C:C2:01:23	eth0	Not Set	2.32.4 Jul 20 2018 1...	Up: 8m 0s, MemFree: 23040	02_A
ST-34	172.16.3.34	NS50 2F R2	68:CC:9C:C2:00:F1	eth0	Not Set	2.32.4 Jul 20 2018 1	Up: 8m 0s, MemFree: 25888	02_A

The Device Scanner shows the columns of information for discovered devices:

Name - The hostname of the device. For AXON Core, the default name is `AXONCore_` and last three bytes of the device’s MAC address in hex (e.g. AXONCore_00013F). Device name can be changed.

IP Address - This can be set remotely via Web UI.

Type - The device type or model. AXON Core units will identify as NS60 and AXON Air units will identify as AP60 model.

MAC Address - The MAC address of the device.

Interface - The network interface via which the Device Scanner is communicating with the device.

ID - The serial number on the device casing.

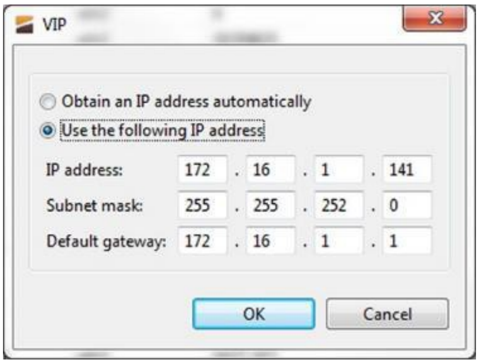
Firmware - The version number of the firmware running on the device.

Status - The uptime of the device. This can be used to easily determine which devices have recently been connected to the network.

Revision - The hardware revision of the device.

To manually discover new devices after the program has been opened, click the **Scan** button. To allow the Device Scanner to continually check for new devices, tick the **Continuous** checkbox.

To change the IP address or settings of a device, click the **Configure IP** button. This will open a dialogue box allowing you to set the device to **Obtain an IP address automatically** using DHCP, or to manually set an IP address, Subnet Mask and Default Gateway with the **Use the following IP address** option



VIP

○ Obtain an IP address automatically

● Use the following IP address

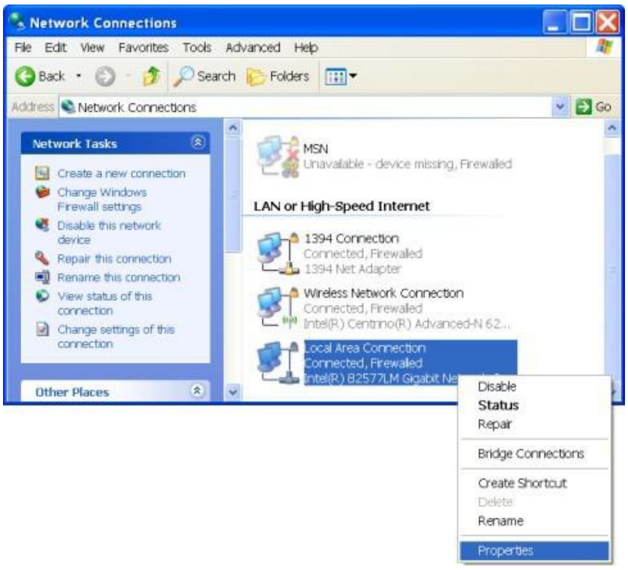
IP address: 172 . 16 . 1 . 141

Subnet mask: 255 . 255 . 252 . 0

Default gateway: 172 . 16 . 1 . 1

Appendix E: Connecting a PC to an Network Device

1. This Appendix specifies how to set up a PC connection (with Windows XP operating system) to connect to an AXON Core or AXON AIR.
2. Connect a PC to the device's Ethernet port with an Ethernet cable. If the PC is already part of the network, note its TCP/IP configuration settings.
3. Click Start > Control Panel. Open Network Connections.



MSN
Unavailable - device missing, Firewalled

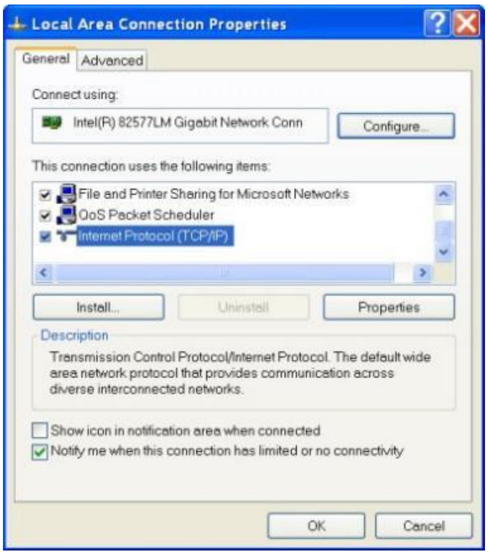
LAN or High-Speed Internet

1394 Connection
Connected, Firewalled
1394 Net Adapter

Wireless Network Connection
Connected, Firewalled
Intel(R) Centrino(R) Advanced-N 62...

Local Area Connection
Connected, Firewalled
Intel(R) 82577LM Gigabit Ne...

Right-click Local Area Connection and select Properties. The Local Area Connection Properties window will open



Connect using:

Intel(R) 82577LM Gigabit Network Conn

This connection uses the following items:

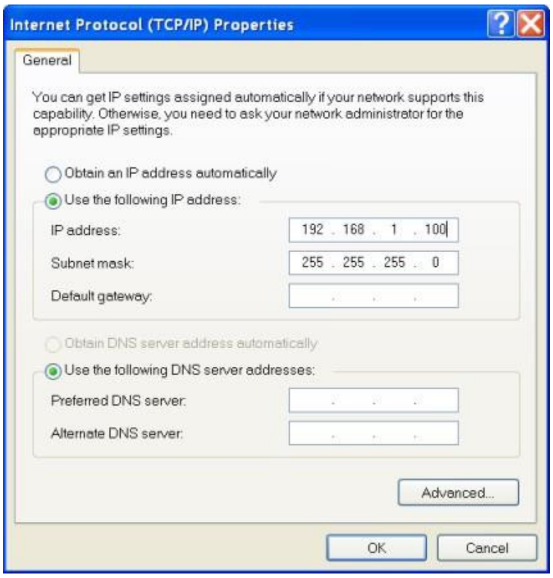
☑ File and Printer Sharing for Microsoft Networks
☑ QoS Packet Scheduler
☑ Internet Protocol (TCP/IP)

Description

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

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

4. On the General tab, scroll down to Internet Protocol (TCP/IP), then click Properties. The Internet Protocol (TCP/IP) Properties dialog box is displayed.



Internet Protocol (TCP/IP) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

5. Click the Use the following IP address option button.
6. In the IP address field, enter a fixed (static) IP address within the Subnet range of the target device's IP address (for example **192.168.1.100**).
7. In the Subnet mask field, enter **255.255.255.0**. Click **OK**

Appendix F: Maintenance Check List

It is recommended all AXON Core and AXON Air units, antennas, cables and connectors are inspected at regular intervals. A maintenance checklist is provided below.

Inspection	Action
Power	Verify the voltage at each AXON Core is above 20VDC (using the web browser interface).
Structural	Inspect the outer case for any structural damage.
	Check the case is firmly closed.
	Check there is no excessive damage or markings to paintwork.
Composite cables	Check all composite cables are connected and secure.
Coaxial cables	Check coaxial cable connections are securely fastened and properly insulated to AXON Air unit.
	Check the coaxial cable for any damage.
Antennas	Check the antennas for any damage.
	Check the antennas' connections to the coaxial cable for any damage to the insulation or connection.
	Check the antennas' directional alignment.
Ethernet connections (PoE)	Check all Ethernet cable connections are secure.
	Check dust covers are present and secure on unused Ethernet ports.
LEDs	Check the power LED is lit green.
	Check the status LEDs are blinking green and there are no orange LED lights
Testing RF TX path for AXON Air	Stand 50M away from AXON Air. Using a MinePhone handset, verify the signal strength is within specification. (Refer to commissioning data).
Testing RF RX path for AXON Air	Stand 50M away from AXON Air with two MST RFID tags. Open AXON Air web browser interface and select the “Tracking” web page. Verify that the two tags have been detected by the network switch and check the received signal strength is within specification (Refer to commissioning data).

Appendix G: Acronyms

Acronym	Meaning
AC	Alternating Current
AP	Access Point
DC	Direct Current
IP address	Internet Protocol address
IPxx	Ingress Protection rating
MAC address	Media Access Control address
MST	Mine Site Technologies
NS	Network Switch
PoE	Power Over Ethernet
PSU	Power Supply Unit
RF	Radio Frequency
SSID	Service Set Identifier.
SFP	Small Form-factor Pluggable (optical transceiver module)
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
WAC	Wireless Access Card
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WNS	network and power distribution module
WPA	Wi-Fi Protected Access

Appendix H: AXON Core Specifications

General

Dimensions	360mm x 507mm x 146mm (H x W x D) – without mounting bracket
Weight	9.0kg packaged
Connectivity	3 x MST composite fibre ports (1000BASE-LX) 4 x IEEE 802.3at PoE+ ports (1000BASE-T) 2 x MST Expansion Slots (proprietary modular interfaces) 1 x DataKey RUGGEDrive slot (configuration management port) 1 x Mechanical mount to support an MST AXON Air wireless module
Enclosure Ingress Protection (IP) rating	SMC enclosure, sealed to comply with an Ingress Protection standard rating of IP65
Operating Temperature	0ºC to 50ºC (operating) -20ºC to 80ºC (storage)
Operating Humidity	5- 95%

Power

Supply Voltage	20-60 VDC operation
External Power Supply Recommendations	AC to DC power supply with galvanically isolated output(s) 56VDC output(s) (nominal) With 6A breaker/fusing in line with each 56V output

		Power Consumption	
Part Number	**Configuration**	**Idle (W)**	**Maximum (W)**
AXON Core	56VDC input voltage, No AXON Air or PoE+ devices connected	10.50	12.50
AXON Core + AXON Air (locally mounted)	56VDC input voltage, 1 x AXON Air (zero metres of CAT5 cable)	14.50	18.50
AXON Core + AXON Air (remotely mounted)	56VDC input voltage, 1 x AXON Air (100 metres of CAT5 cable)	14.52	18.55
AXON Core + 2 AXON Air (daisy chained)	56VDC input voltage, 1 x AXON Air (100 metres of CAT5 cable) + 1 x daisy chained AXON Air (100m CAT5)	18.62	24.77
AXON Core + 3 AXON Air (daisy chained)	56VDC input voltage, 1 x AXON Air (100 metres of CAT5 cable) + 1 x daisy chained AXON Air (100m CAT5) +	22.84	31.30

	1 x daisy chained AXON Air (100m CAT5)		

Copper Ethernet Port

Crossover	Auto MDI/MDIX crossover
Auto negotiation	10BASE-T / 100BASE-TX / 1000BASE-T

Network Information

Network Protocols	IEEE 802.3 Ethernet • 802.3i 10BASE-T, • 802.3u 100BASE-TX, • 802.3x Full Duplex and flow control, • 802.3z 1000BASE-X (Ethernet over fibre), • 802.3ab 1000BASE-T (Ethernet over twisted-pairs), • 802.3at Power over Ethernet enhancements (PoE+) • 802.3az Energy Efficient Ethernet. IEEE 802.1 LAN/MAN/WAN • 802.1Q VLAN, • 802.1p Quality of Service (QoS), 8 traffic classes, o Automatic 802.1p tagging based on 802.1Q VLAN ID, • 802.1D spanning tree, • 802.1w rapid spanning tree, • 802.1AB Link Layer Discovery Protocol (LLDP). SNMP – Simple Network Management Protocol (Read Only) MST Device Discovery Protocol

Appendix I: AXON Air Specifications

General

Dimensions	115mm x 135mm x 242mm (H x W x D) – without mounting bracket
Weight	700g
Connectivity	2 x IEEE 802.3at PoE+ ports (1000BASE-T) 2 x IEEE 802.11a/b/g/n antenna ports (2x2 MIMO) using 50Ω N-Type Female connectors 1 x Mechanical mount compatibility with the MST AXON Core
Enclosure Ingress Protection (IP) rating	SMC enclosure, sealed to comply with an Ingress Protection standard rating of IP65
Operating Temperature	0ºC to 50ºC (operating) -20ºC to 80ºC (storage)
Operating Humidity	5- 95%

Power

Power Requirement	PoE+ Class 4 (negotiated) 4W nominally, 6W peak.
Power pass-through (daisy chaining)	Up to PoE+ Class 4 (negotiated) *Notes:* *- Up to 3 x AP60 units may be daisy chained together (using CAT5 cable).* *- Maximum CAT5 cable lengths between daisy chained units is 100 metres.* *- The available power at the downstream port should be expected to be approximately 6W less than the power present at the upstream port.*

Wireless

Wireless Connectivity	1 x IEEE 802.11a/b/g/n wireless access point 2.4 or 5GHz with 2x2 MIMO 6 x SSIDs IEEE 802.11s Meshing
Network Protocols	IEEE 802.3 Ethernet • 802.3i 10BASE-T, • 802.3u 100BASE-TX, • 802.3x Full Duplex and flow control, • 802.3z 1000BASE-X (Ethernet over fibre), • 802.3ab 1000BASE-T (Ethernet over twisted-pairs), • 802.3at Power over Ethernet enhancements (PoE+) • 802.3az Energy Efficient Ethernet.

	IEEE 802.1 LAN/MAN/WAN • 802.1Q VLAN, • 802.1p Quality of Service (QoS), 8 traffic classes, o Automatic 802.1p tagging based on 802.1Q VLAN ID, • 802.1D spanning tree, • 802.1w rapid spanning tree, • 802.1AB Link Layer Discovery Protocol (LLDP). SNMP – Simple Network Management Protocol (Read Only) MST Tracking Protocol MST Device Discovery Protocol Aeroscout Compatible
Wi-Fi Security	WPA Personal [†] WPA Enterprise [†] WPA2 Personal [†] WPA2 Enterprise [†] [†] supports options for AES or TKIP encryption
Compatibility	Inter-operable with 802.11a/b/g/n compliant products
Modulation	DSSS (DBPSK, DQPSK, CCK) OFDM (BPSK, QPSK, 16-QAM, 64-QAM)
Permitted WLAN channels by region	IEEE 802.11b/g/n (2.4GHz channels) Australia 1-13 Canada 1-11 China 1-11 Europe 1-13 Japan 1-14 (802.11b), 1-13 (802.11g/n) USA 1-11 IEEE 802.11a/n (5GHz channel frequencies) Australia Contact MST for latest details Canada China Europe Japan USA
RF output power (maximum)	802.11a: +16dBm 802.11b: +20dBm 802.11g: +20dBm 802.11n: +20dBm (in 2.4GHz bands) 802.11n: +16dBm (in 5GHz bands)

Receive sensitivity (typical)	2.4GHz Receive Sensitivities: CCK, 1Mbps -98dBm CCK, 11Mbps -91dBm OFDM, 6Mbps -94dBm OFDM, 54Mbps -80dBm HT20, MCS0, 1 stream, 1 Tx, 1 Rx -94dBm HT20, MCS7, 1 stream, 1 Tx, 1 Rx -77dBm HT20, MCS8, 2 stream, 2 Tx, 2 Rx -93dBm HT20, MCS15, 2 stream, 2 Tx, 2 Rx -74dBm HT40, MCS0, 1 stream, 1 Tx, 1 Rx -92dBm HT40, MCS7, 1 stream, 1 Tx, 1 Rx -75dBm HT40, MCS8, 2 stream, 2 Tx, 2 Rx -91dBm HT40, MCS15, 2 stream, 2 Tx, 2 Rx -70dBm 5GHz Receive Sensitivities: 6Mbps -95dBm 54Mbps -80dBm HT20, MCS0, 1 stream, 1 Tx, 1 Rx -96dBm HT20, MCS7, 1 stream, 1 Tx, 1 Rx -77dBm HT20, MCS8, 2 stream, 2 Tx, 2 Rx -93dBm HT20, MCS15, 2 stream, 2 Tx, 2 Rx -74dBm HT40, MCS0, 1 stream, 1 Tx, 1 Rx -91dBm HT40, MCS7, 1 stream, 1 Tx, 1 Rx -72dBm HT40, MCS8, 2 stream, 2 Tx, 2 Rx -90dBm HT40, MCS15, 2 stream, 2 Tx, 2 Rx -69dBm

Compliance

NOTE: Please contact MST for the latest available compliance information if required.

Appendix J: Hardware Warranty

Mine Site Technologies Pty Ltd (MST Global) provide a 12-month warranty for hardware supplied to the original purchaser. MST Global warrants that the hardware supplied will be free from material defects in workmanship and materials from the date of original purchase.

MST Global will repair or replace the defective hardware during the warranty period at no charge to the original owner. Such repair or replacement will be rendered by MST Global. MST Global may in its sole discretion replace the defective hardware (or any part thereof) with a reconditioned product or parts that MST Global determines is substantially equivalent (or superior) to the defective hardware. Repaired or replacement hardware will be warranted for the remainder of the original warranty period from the date of original purchase. All hardware (or part thereof) that is replaced by MST Global shall become the property of MST Global upon replacement.

Appendix K: AXON AIR Installation Addendum

Professional installation

AXON Air device must be installed by professionals. It is strictly forbidden to be installed and maintained by non-professionals.

Application: Outdoor operation in 5150 – 5250 MHz band
Country: United States of America

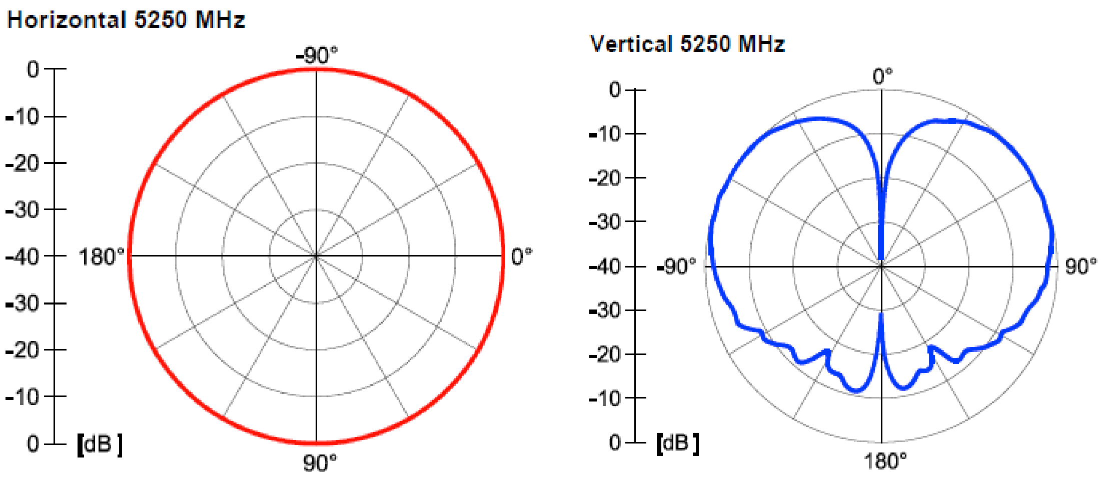
When the frequency band 5150 – 5250 MHz is used outdoors in the U.S.A, the FCC mandates that it is necessary to keep the energy radiated above 30 degrees from the horizon below 21 dBm EIRP. This can be obtained using the following guidance.When device installed outdoors level to the horizon, (i.e. - antenna point towards down towards the earth), the device operates in compliance with FCC rules without any adjustment of output power.

Maximum EIRP in 5150 – 5250 MHz band = 17 dBm + Antenna Gain
Maximum EIRP in 30 degree from Horizontal = 17 dBm + 3 dBi = 20 dBm

When the device is installed outdoors at an angle to the horizon, power must be reduced to insure the energy radiated above 30 degrees from the horizon remains under 21 dBm EIRP.

AXON AIR maximum device tx power is 17dBm and the default antenna gain is 2.5 dBi(0dB+2.5dBi) in all degree. The device operates in compliance with FCC rules without any adjustment of output power when use default antenna.

Elevation Pattern:



Degree Above Horizon (A)	Output Power Reduction
A<30	>=0 dB
A>30	>=0 dB

MST Global

Mine Site Technologies Pty Ltd (MST Global) is a tier one provider of communications networks and operational optimisation solutions, which assist the mining, resources and industrial sectors to optimally manage core business operations. Established in Australia over 25 years ago and with a global reach across six continents, the company specialises in the design, manufacture, deployment and support of critical technologies for communications, automation-enablement, production optimization, vehicle and personnel tracking, and safety in hazardous environments both underground and on the surface.

A pioneering force within the mining industry, MST Global has over 600 deployments at mine sites worldwide. Customers across the globe trust MST Global solutions to help optimise output, minimise cost and reduce risk, resulting in a compelling ROI on technology investments.

MST Global subsidiary Nixon Communications provides specialist surface radio and networking services throughout Australia.

Connecting your mine to the future.
Contact your local office today.

www.mstglobal.com
solutions@mstglobal.com

Australia
Sydney
Tel: +61 (0)2 9491 6500

United States
Denver
Tel: +1 303 951 0570

United States
Tucson
Tel: +1 520 495 0185

Chile
Santiago
Tel: +56 9 7772 3819

Russia
Moscow
Tel: +7 (499) 978 72 11

South Africa
Centurion
Tel: +27 (0) 12 345 6100

China
Hangzhou
Tel: +86 571 8580 3320 Ext 206