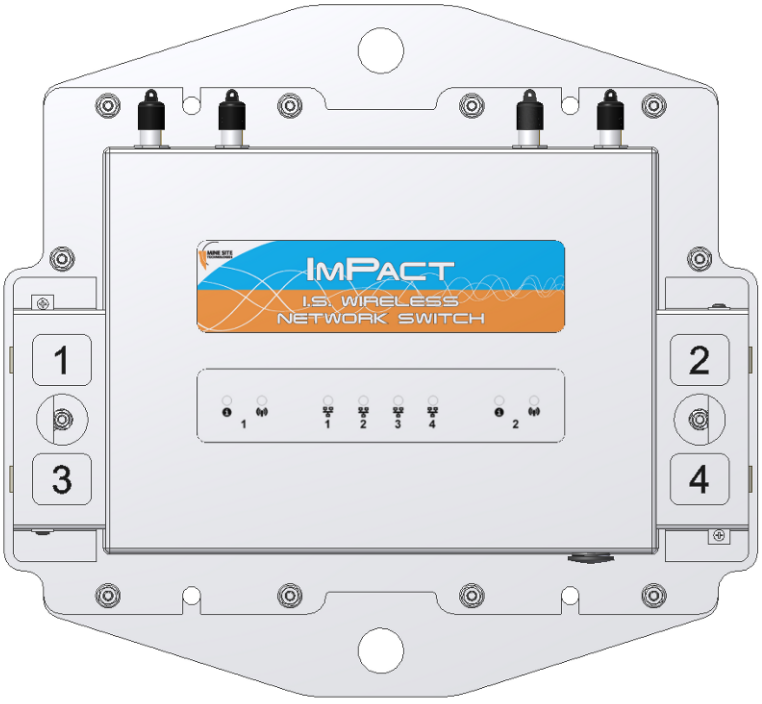
MINE SITE TECHNOLOGIES

Global Leader in Mining Communications

NS40 I.S. Wireless Network Switch

User Manual



Contents

Revision History

Revision	Change	Date
A	User manual for NS40 hardware rev. D and firmware 0.9.36	June 2011
B	Revision for firmware 1.2.0	August 2011

Contact Information

AUSTRALIA

Sydney
25-27 Whiting Street
Artarmon NSW 2064 AUSTRALIA
Tel: +61 2 9437 4399

CANADA

Sudbury
1085 Kelly Lake Road
Sudbury Ontario P3E 5P5 CANADA
Tel: +1 705-675 7468

CHINA

Hangzhou
4th Floor, Building 1
No. 5 Xianghong Road
Hangzhou CHINA 310011
Tel: +86 571 85803320x206

UNITED STATES

Denver
13301 W 43rd Drive
Golden Colorado 80403 USA
Tel: +1 303-951 0570

About This Manual

This manual describes features and functions of the NS40 Intrinsically Safe Wireless Network Switch. It provides information about hardware installation, operation, 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.minesite.com.au*.

Chapter 1

I.S. Wireless Network Switch

Topics:

The Mine Site Technologies Intrinsically Safe Wireless Network Switch (NS40) consists of a managed fibre optic Ethernet switch and two 802.11b/g wireless access points. It provides wired and wireless network access in hazardous coal mining environments. The NS40 forms part of the ImPact Intrinsically Safe Communications System, providing the network infrastructure where voice, tracking, video, process control and data applications are used to enhance mining safety and communication.

The NS40 has the following features:

- Four fibre optic fast Ethernet ports
- Two 802.11b/g wireless access points
- Powder-coated stainless steel enclosure complying to IP65 standards
- AeroScout Tag reading capability for real time tracking of assets and personnel
- Composite cabling that incorporates both power and fibre optic connectivity
- Low power design operating from 8 to 15.1VDC for Intrinsically Safe mining environments
- Rapid Spanning Tree Protocol for network redundancy.

1.1 Hardware Overview

The features and functions of the NS40 are illustrated in *Figure 1: NS40 hardware* and the accompanying table.

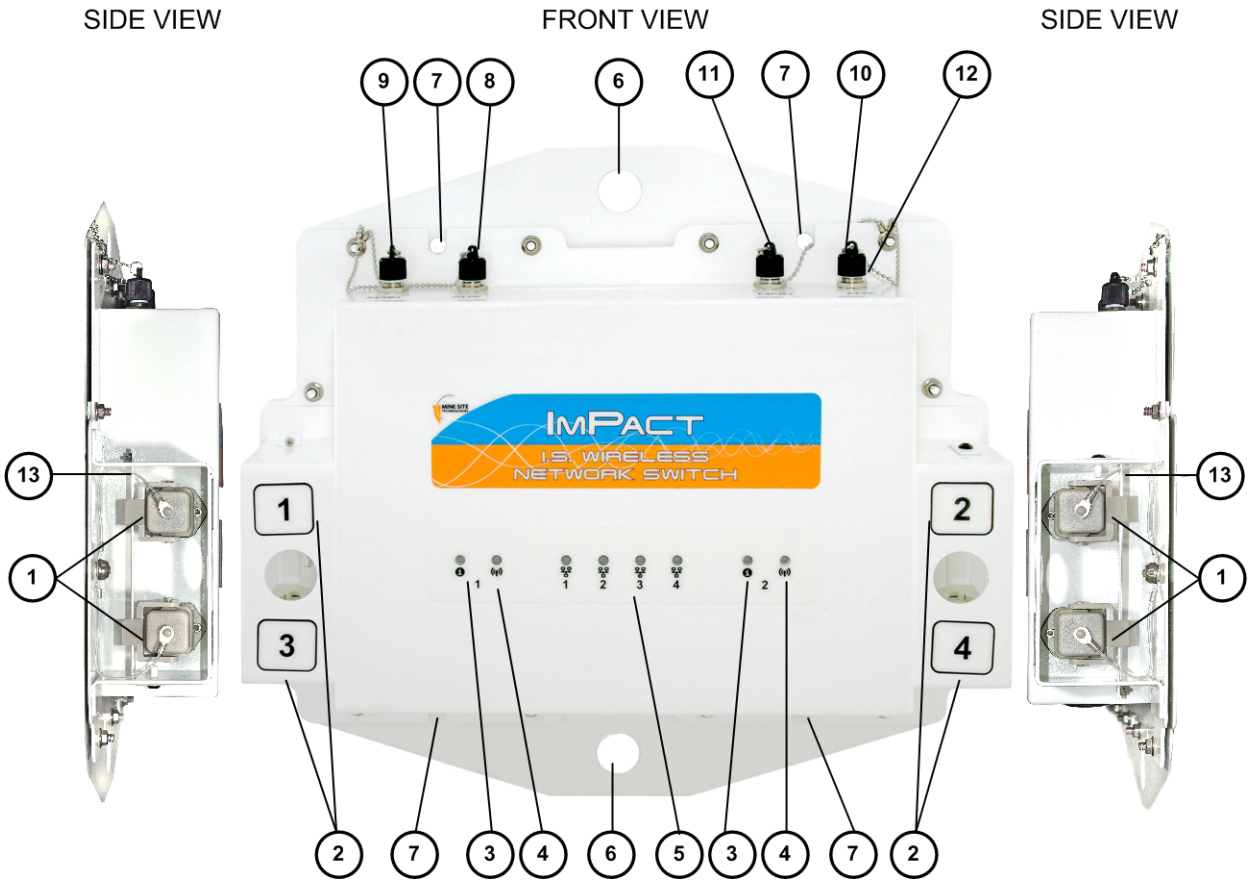


Figure 1: NS40 hardware

Key	Description	Function
1	Composite fibre port.	Power and / or fibre optic connectivity via composite cable, fibre optic cable or DC power cable.
2	Composite fibre port number.	By default, composite fibre port 1 is the upstream port.
3	Status indicator LED for each CPU.	The status LEDs indicate the following:

LED status	Indication
Off	CPU is not running.
Blinking slowly	CPU is operating.
Blinking fast	CPU is booting up.

<table>
<tr><th>Key</th><th>Description</th><th>Function</th></tr>
<tr><td>4</td><td>Wi-Fi indicator LED for each CPU.
  </td><td>Wi-Fi LEDs indicate the following:<table><tr><th>LED status</th><th>Indication</th></tr><tr><td>Off</td><td>Wireless radio is disabled.</td></tr><tr><td>On</td><td>Wireless radio is enabled.</td></tr><tr><td>Flashing</td><td>Transmitting or receiving data.</td></tr></table></td></tr>
<tr><td>5</td><td>Composite fibre port link / Activity LEDs.
  </td><td>The fibre port LEDs indicate the following:<table><tr><th>LED status</th><th>Indication</th></tr><tr><td>Off</td><td>Fibre transceiver is disabled or has not established a link to the next device.</td></tr><tr><td>On</td><td>Fibre transceiver is enabled and has established a link to the next device.</td></tr><tr><td>Flashing</td><td>Transmitting or receiving data.</td></tr></table></td></tr>
<tr><td>6</td><td>25mm diameter mounting hole.</td><td>NS40 mounting point.</td></tr>
<tr><td>7</td><td>10mm diameter mounting hole.</td><td>NS40 mounting point.</td></tr>
<tr><td>8</td><td>Receive (Rx) antenna port for wireless radio 1.</td><td>RP-TNC jack for connecting an antenna to wireless radio 1.</td></tr>
<tr><td>9</td><td>Transmit (Tx) and receive (Rx) antenna port for wireless radio 1.</td><td>RP-TNC jack for connecting an antenna to wireless radio 1.</td></tr>
<tr><td>10</td><td>Receive (Rx) antenna port for wireless radio 2.</td><td>RP-TNC jack for connecting an antenna to wireless radio 2.</td></tr>
<tr><td>11</td><td>Transmit (Tx) and receive (Rx) antenna port for wireless radio 2.</td><td>RP-TNC jack for connecting an antenna to wireless radio 2.</td></tr>
<tr><td>12</td><td>Antenna port protective cap.</td><td>Protective cap when antenna ports are not in use.</td></tr>
<tr><td>13</td><td>Composite fibre port retention arm.</td><td>Protective arm to lock fibre port covers and cable connectors.</td></tr>
</table>

1.2 System Layout Overview

NS40s are used to form a network system known as the ImPact Intrinsically Safe Communications System. Each NS40 is placed at a location where data, voice, and tracking applications are required.

An Intrinsically Safe network consists of a number of cells. Each cell consists of:

- A power supply unit (PSU)
- Up to four NS40s
- A pair of antennas for each 802.11b/g wireless access point
- Interconnection cables consisting of power cables, fibre optic cables, composite cables and coaxial cables

- Antenna splitter boxes
- Junction boxes that are used to join composite cable lengths greater than 325m.

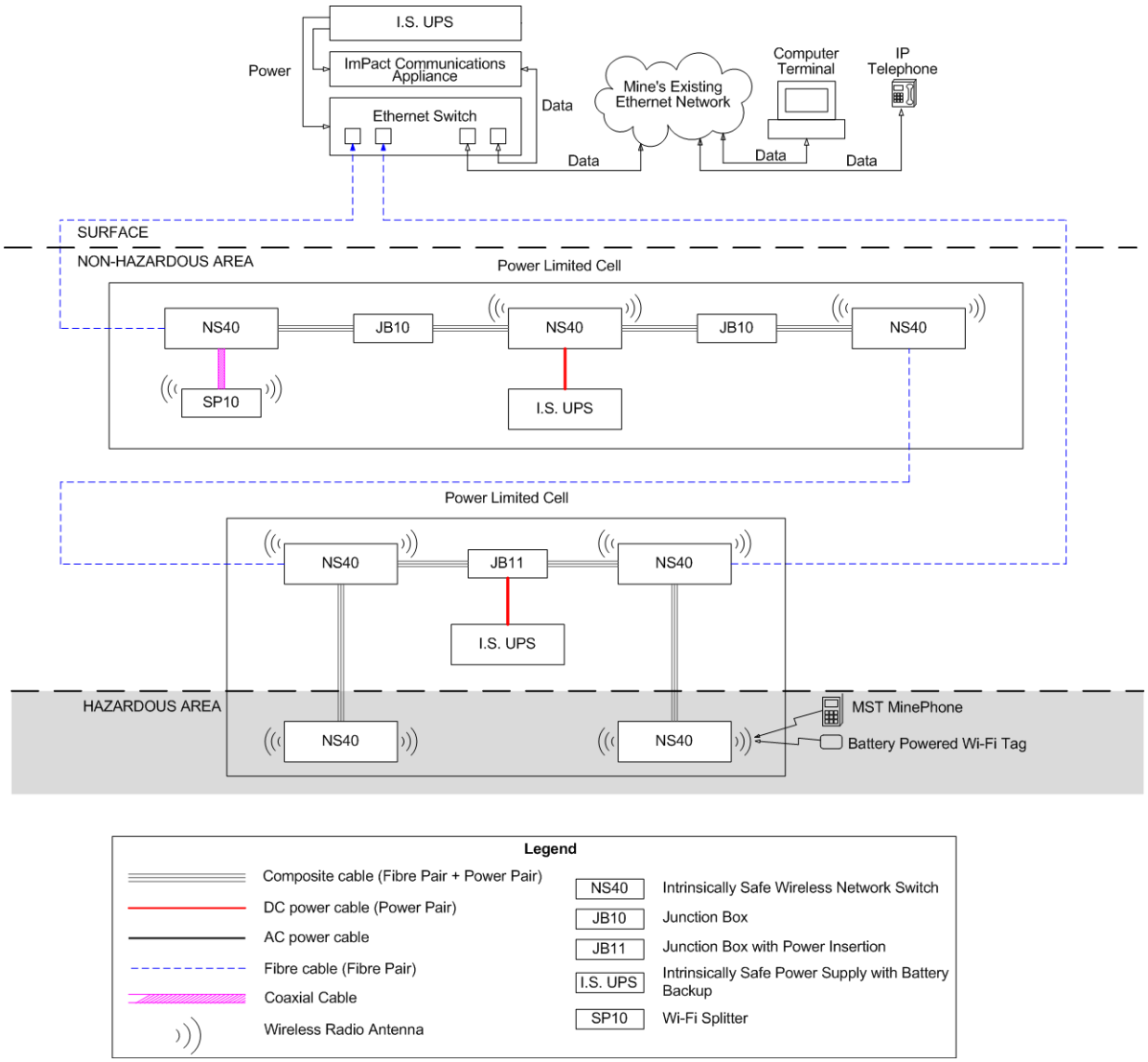


Figure 2: An example of an Intrinsically Safe network

The Intrinsically Safe design of the network requires each cell to be individually powered and that electrical power must not travel between them. Fibre optic cables is used to connect between cells to provide network connectivity as shown in *Figure 2: An example of an Intrinsically Safe network*.

Cells can be connected in a loop configuration to provide multiple redundant network paths to the surface. The NS40 supports Rapid Spanning Tree Protocol (RSTP), which monitors these loops and can redirect data traffic if an active link fails.

1.3 Connectivity

The NS40 has two types of network connections:

- Composite fibre ports
- Wireless access points.

1.3.1 Composite Fibre Ports

Each side of an NS40 unit has two 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 each port to maintain the IP65 (Ingress Protection) rating of the unit. Leaving a port uncovered whilst an NS40 is operating breaches the IP65 rating and consequently the Intrinsic Safety Certification.

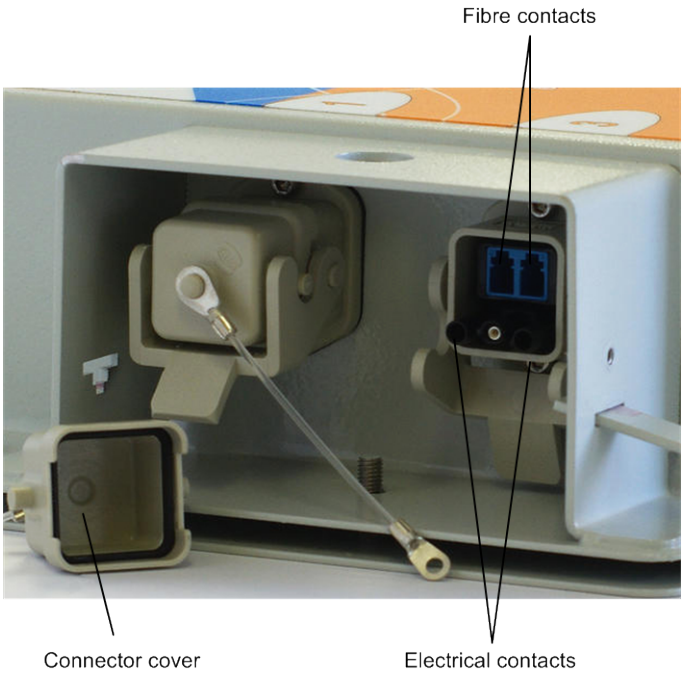


Figure 3: Composite fibre ports

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 NS40 within a cell. By convention, this cable is connected to port 4.
Fibre only connection	A fibre optic cable terminated to the fibre contacts of the NS40 composite connector.
Fibre and DC power connection	A composite cable providing fibre optic connectivity and power to the NS40 in a cell.

Fibre optic cabling provides numerous benefits over Ethernet cabling, with superior signal integrity and no signal interference from high powered electronics. It also enables NS40s to be spaced over longer distances without the distance limitation of Ethernet cabling.

By default port 1 is configured as the upstream port and ports 2, 3 and 4 as the downstream ports. The difference between upstream and downstream ports is the orientation of the fibre that is used for transmitting data and the fibre used for receiving data. This is illustrated in *Figure 4: Fibre orientation of Upstream and Downstream ports*.

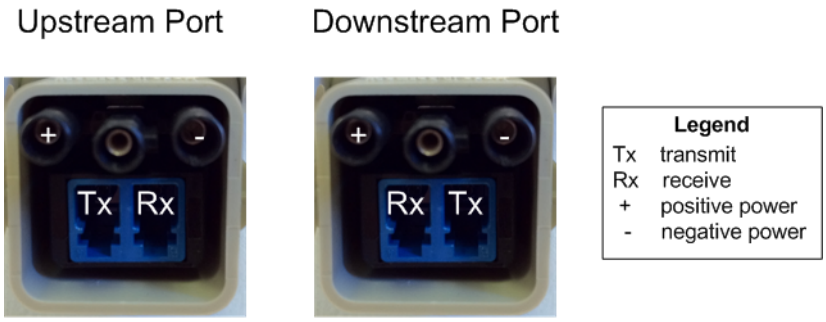


Figure 4: Fibre orientation of Upstream and Downstream ports

Due to the difference in the fibre orientation, MST composite cable and fibre optic cable can only be connected between ports on NS40 devices marked with a tick in the matrix below.

	Port 1	Port 2	Port 3	Port 4
Port 1	✗	✓	✓	✓
Port 2	✓	✗	✗	✗
Port 3	✓	✗	✗	✗
Port 4	✓	✗	✗	✗

1.3.2 Wireless Access Points

The NS40 has two 802.11 b/g radios allowing up to two wireless access points. Each wireless access point is managed by a CPU and can be enabled or disabled through the web browser interface. For more information, see *Configuring Wireless Interface Settings* on page 52.

Chapter 2

Installing I.S. Wireless Network Switches

Topics:

This chapter describes mounting and installation of NS40s, antennas, and connection of cables. Fibre plug assembly and cable termination are beyond the scope of this manual.

Important:

The electronic components in an NS40 are designed to be isolated from the enclosure and local electrical earth. This is known as galvanic isolation and ensures there is no current passing between grounds of different potential. In the event of a short circuit to earth, galvanic isolation allows all devices within a cell to be intrinsically safe as there are no loops for current to flow. Galvanic isolation must always be maintained in the following manner:

- All NS40 circuitry isolated from the enclosure (and electrical earth)
- Use of approved Intrinsically Safe Uninterruptible Power Supply (I.S. UPS)
- All antenna and coaxial cable connections properly insulated.

2.1 Pre-Installation Planning

A detailed design study of a mine must be conducted by an MST System Engineer to determine specific network requirements and design before installation. 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
- Access to Intrinsically Safe power
- Interconnection to the mine's existing corporate network
- Policies for network protocols between networks
- Cabling requirements
- Antenna types to use with each unit, whether antenna splitters are required, and mounting method for each antenna
- Mounting location and installation method for each NS40.

2.2 Mounting an I.S. Wireless Network Switch

The mounting location of each NS40 should be free from debris, and should not be an obstruction to vehicles, machinery, vent tubing, piping and cables. It can be mounted horizontally or vertically.

The NS40 has mounting points shown in *Figure 5: NS40 mounting points* providing several installation options. The 10mm and 25mm diameter mounting holes allow the NS40 to be cable-tied to the mesh in a mine tunnel. The 25mm diameter mounting holes also allow the NS40 to be secured to rock bolts in the mine rock face.

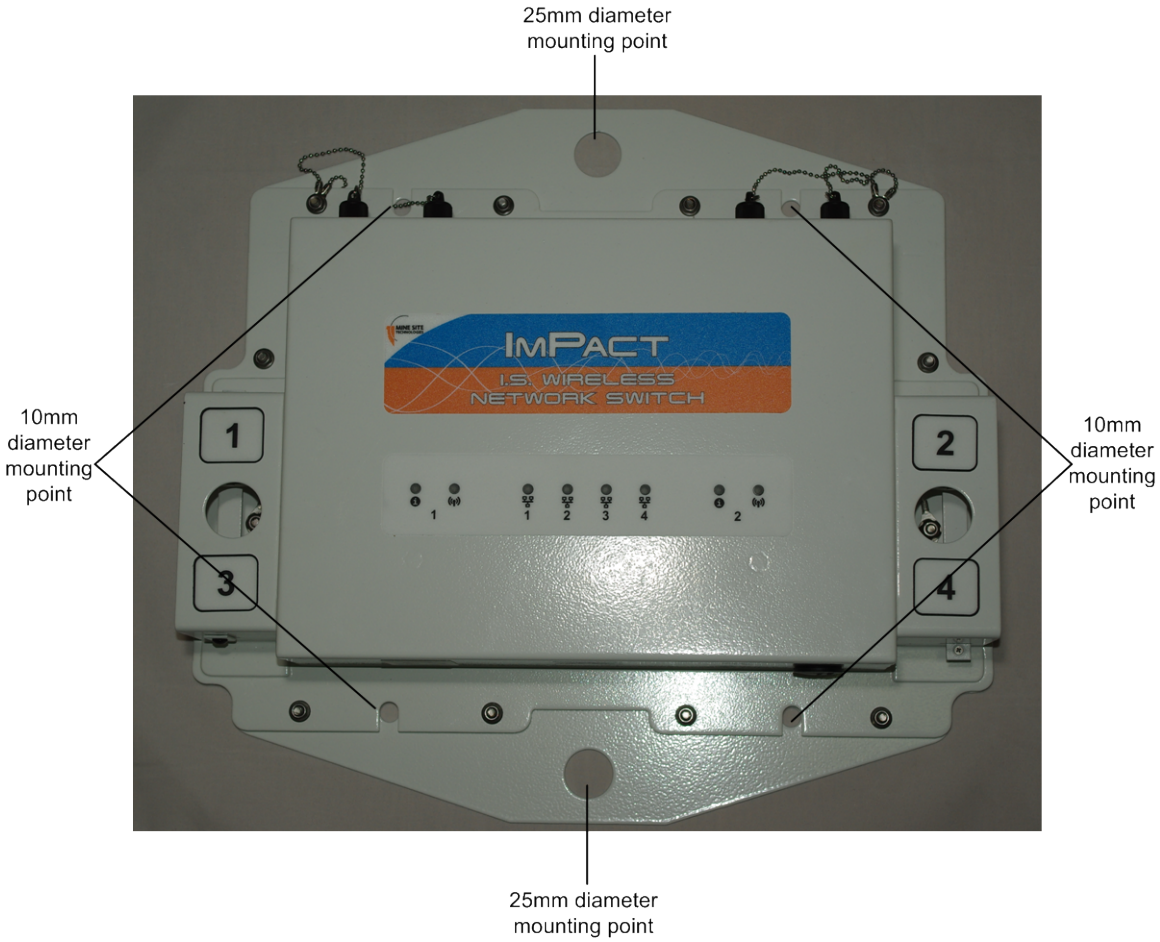


Figure 5: NS40 mounting points

2.3 Cables

An Intrinsically Safe network must only use approved cables for the interconnection of cells and devices. Please consult your MST System Engineer if you have any cabling queries.

Important: Please ensure the power supply is turned off and de-energised before attaching or detaching any cables in a cell.

2.3.1 Power and Data Cables

Cables terminated with a connector which attach to the NS40 ports are described in the table below:

Cable type	Description and function
Composite	A fibre optic cable pair and a DC power cable pair in a single outer jacket as shown in Figure 6. It transfers power and data between an NS40s or an I.S. PSU and the attached network device. The maximum length of composite cable is 325m between NS40 units. Multiple cable lengths can be joined by another NS40 or junction boxes (model no. JB10 or JB11).

Cable type	Description and function
Fibre optic	A fibre optic cable pair in a single outer jacket. This cable transfers data to an NS40 or another network device. Multiple cable lengths can be joined by junction boxes (model no. JB10, JB11 or JB12)
DC power	A DC power cable pair that transfers power between a I.S. PSU and an NS40 or a junction box (JB11).

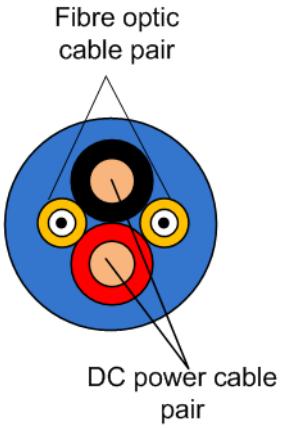
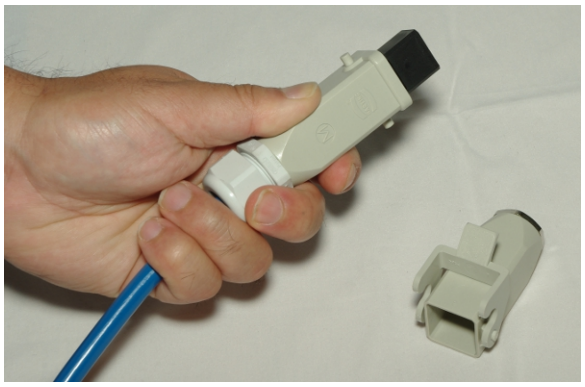
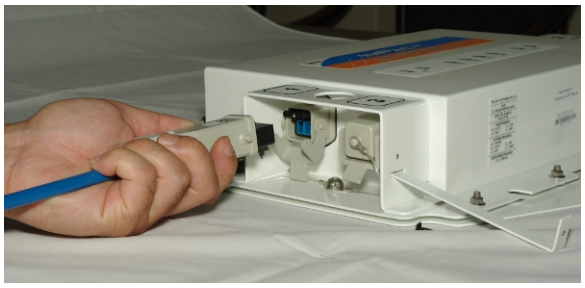
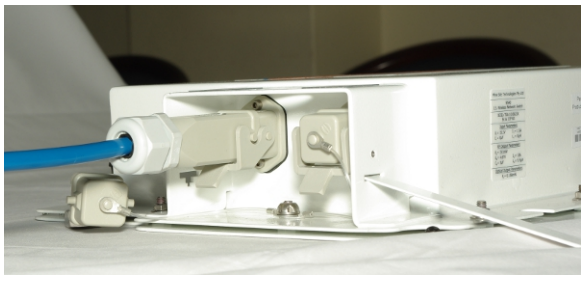
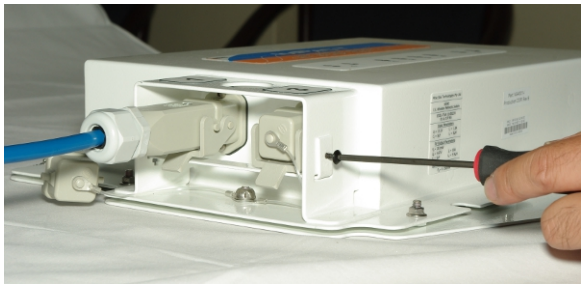


Figure 6: Composite Cable

Installation Procedure

The following procedure demonstrates how composite connector cables are attached to the NS40.

Step	Description	Illustration
1	Insert an allen key (0.125" or 3.18mm hex driver) to remove the hex screw on the retention arm.	
2	Slide out the retention arm from the NS40.	

Step	Description	Illustration
3	Push down on the locking catch for the port and remove the cover.	
4	On the cable, push open the locking catch and remove the connector cover.	
5	Align the pins on the connector to the composite fibre port.	
6	Insert the cable into the composite fibre port, and push the locking catch to the connector. **Important:** Check that all unused composite fibre ports have a cover fitted.	
7	To lock connection, slide the retention arm back into the unit and screw the hex nut tight.	

Extending Cable Runs with Junction Boxes

Power and data cable runs can be extended in a network using junction boxes JB10 and JB11. Junction boxes also provide an inductance barrier, limiting current and voltage to maintain Intrinsic Safety in a network.

The JB11 shown in *Figure 7: JB11 junction box* also has a DC connector. This enables separate fibre optic and power cables to be joined to the JB11, and a composite cable run from the JB11 to the NS40. This frees up ports on the NS40 for connecting other devices.

Figure 7: JB11 junction box

2.3.2 Coaxial cables

Coaxial cables connect an NS40's antenna ports to the antennas to transmit and receive wireless signals. Coaxial cables connect from each of the NS40 antenna ports to either an antenna or a signal splitter, which then connects to multiple antennas.

Use only MST approved low capacitance LMR-400-FR coaxial cable with the system.

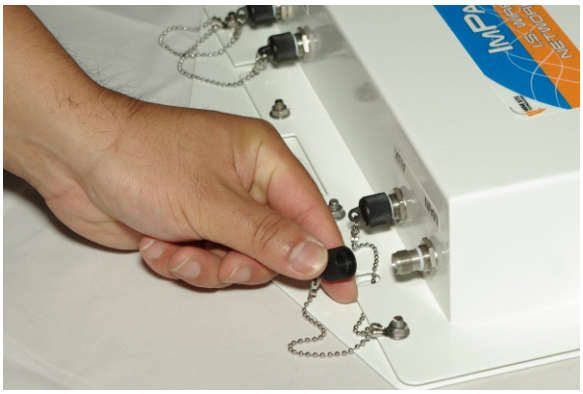
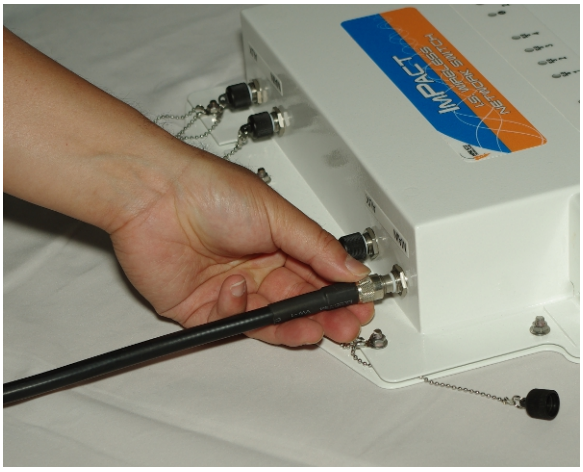
Coaxial cable length should be kept short as possible to minimise signal loss. It is recommended to keep cable length to less than 10 metres. The absolute maximum length is dependent on local compliance approvals. For example, up to 50 metre coaxial cable length is approved in the U.S.A.

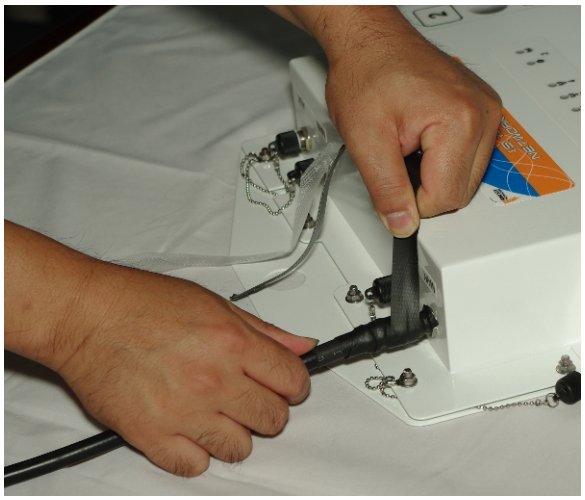
Important:

MST coaxial cables have connector covers that protect the exposed metal of the coaxial connectors. The covers must be in place providing protection to an Ingress Protection (IP20) rating level and galvanic isolation. If coaxial connectors only have metal sleeves, they must be insulated using amalgamated rubber tape.

Installation Procedure

The following procedure demonstrates how coaxial cables are connected and insulated to the NS40.

Step	Description	Illustration
1.	Unscrew antenna cover from the antenna port.	
2.	Connect the coaxial cable connector to the antenna port and tighten the outer metal sleeve slide connector cover over the connection. If the connector has no cover, use the following steps as described below.	
3.	Insulate the connection using self-amalgamating rubber tape. Start at the base of the connection and pull back the rubber tape backing.	
4.	Pull the tape tightly, and tape around the connector at an angle until it is 25mm past the end of the connection.	

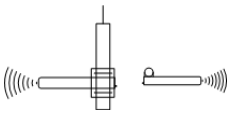
Step	Description	Illustration
5.	Wind the rubber tape at an angle back down towards the base of the connection and cut the tape.	
6.	Cable tie and mount coaxial cables in locations that are free from obstructions. **Important:** Check that all unused antenna ports remain covered with the supplied antenna port covers.	

2.4 Antennas

An NS40 has two antenna ports for each 802.11b/g wireless radio. Antennas are connected to the NS40 to optimise wireless signal coverage in the underground mining environment.

The choice of antenna will depend on wireless coverage, surrounding geology, tunnel topology and stratum type. The antenna types used in a network are described below.

Antenna Type	Illustration	Description
Omndirectional antenna		An antenna that radiates equally in all directions. It provides direct coverage in an open area.
Diversity panel antenna		A diversity panel antenna contains two antennas. It is used for providing better signal reception in difficult areas, and a more accurate AeroScout tag location when Wi-Fi tracking is implemented. Diversity antennas require two antenna connections to the network switch.

Antenna Type	Illustration	Description
Yagi directional antenna		A Yagi antenna is a highly directional antenna providing a very narrow but longer horizontal beamwidth. 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.

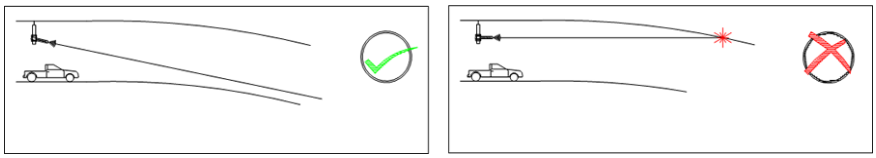
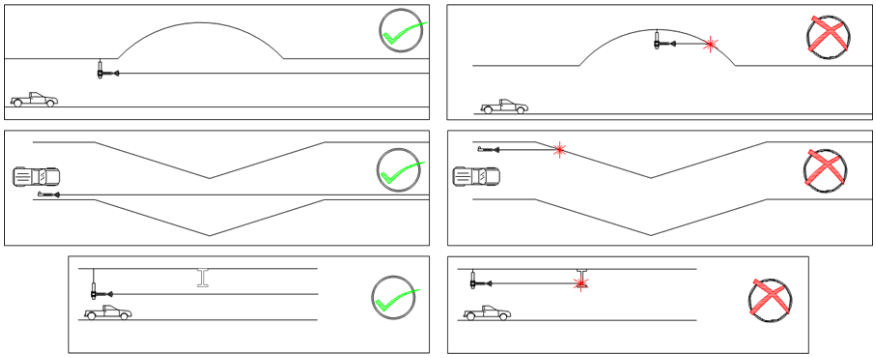
Note: Only approved antenna models can be connected to the NS40. Please consult your MST System Engineer for any queries.

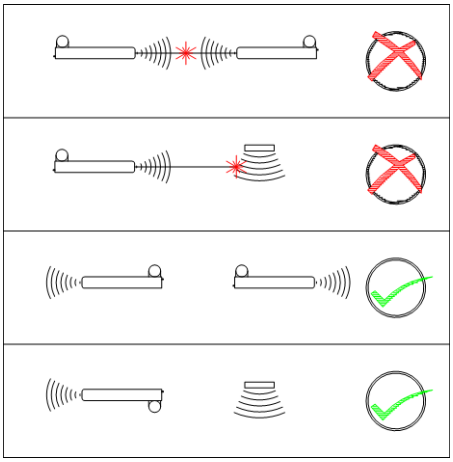
2.4.1 Antenna Placement and Layout

Antennas are usually mounted separately from an NS40 to optimise transmission and avoid any obstructions in a mine tunnel. An antenna splitter can be used connect two antennas to a single antenna port. This provides greater flexibility in the configuration and placement of antennas to improve wireless coverage.

Antenna placement is dependent on the surrounding geology, tunnel topology and stratum type. Antennas can be configured in different layouts to achieve different RF patterns.

The following considerations in the placement of antennas are described and illustrated below.

Scenario	Antenna Placement	Illustration
1.	Antennas should be mounted and angled to give optimum transmission along curves and dips.	
2.	Antennas should be mounted to avoid signal obstruction from rock, vehicles, equipment and machinery.	

Scenario	Antenna Placement	Illustration
3.	Multiple antennas should be mounted to avoid crossing signal paths.	

2.5 Before Powering Up the I.S. Network Switch

After an NS40 is installed, use the following check list before supplying power to the NS40 (and cell).

1. Check that the NS40 mounting is secure and free from obstructions.
2. Check that the antenna mountings are secure and free from obstructions.
3. Check all NS40 ports are protected from coal dust ingress by one of the following:
   - connection to a composite cable
   - connection to a fibre optic cable
   - connection to a DC power cable
   - fitted with a protective cover.
4. Check all antenna ports are protected from electrical contact (to a level of IP20) by one of the following:
   - connection to a coaxial cable, with a protective cover fitted over the connector
   - insulation of the connectors with amalgamated rubber tape
   - fitted with a protective cover (attached to the NS40).

Chapter 3

Understanding VLANs

Topics:

This chapter explains the principles behind Virtual Local Area Networks (VLANs). It is important to understand VLANs to properly configure an NS40.

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. In the context of NS40 devices, VLANs are created to separate multiple applications such as voice, process control, data and video in a mining network.

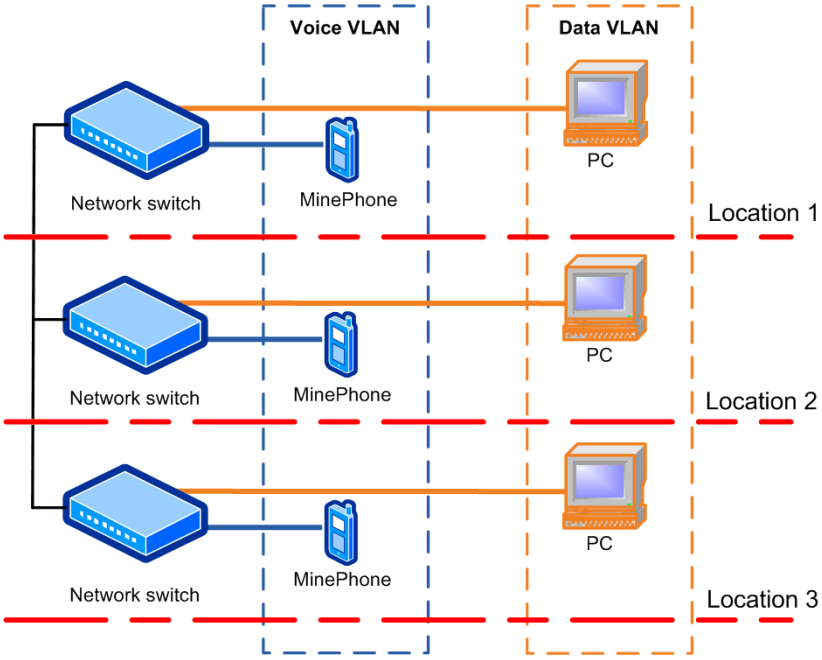


Figure 8: An example of two VLANs distributed across three switches

Figure 8: An example of two VLANs distributed across three switches shows two VLANs distributed across three network switches. PCs can only communicate to other PCs, and MinePhones can communicate to other MinePhones because they are on the same VLAN.

3.1 Understanding Trunk and Access Ports

When VLANs are enabled, network switch ports are assigned to be either trunk ports or access ports. These two types of port allocations determine how data is transmitted and relayed.

3.1.1 Trunk Ports

Trunk ports provide a connection for multiple VLANs between network devices and access points. They will only transmit frames (packets of data) that belong to the assigned VLANs. To identify the frames, a network switch will add a tag (known as an 802.1Q tag) to the frame. The tag contains the following information:

- **VLAN ID** — allows the network switch receiving a frame to identify the VLAN it belongs to for distribution.
- **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. If the switch has devices connected via access ports on the same VLAN, the tag is removed and sent those devices. If the switch has other trunk ports that have the VLAN as a member, the frame is sent with the tag intact.

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 creating VLANs, see *Defining VLANs* on page 61.

3.1.2 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 belonging to the assigned VLAN. Any tagged frames sent to an access port will be dropped.

3.1.3 Port Allocation

Any physical ports on the NS40 can be configured to be a trunk port or access port using the web browser interface. The NS40 default configuration has fibre ports 1-4 allocated as trunk ports as they are usually connected to other NS40s. For more information on defining ports , see *Configuring Composite Fibre Ports* on page 58.

3.2 Wireless MAC VLAN Bridge

VLANs on the wireless network are configured as MAC based VLANs. This means that a wireless device belongs to a VLAN based on its MAC address. A MAC Address Table specifies which MAC addresses belong to a VLAN. If a wireless device has a MAC address that is not defined to a particular VLAN, any frames sent from the device will be allocated to the default VLAN. The MAC address tables and default VLAN can be configured in the web browser interface as described in *Configuring Wireless MAC VLAN Bridge Settings*.

An example of a wireless network is shown in *Figure 9: An example of Wireless MAC VLANs*.

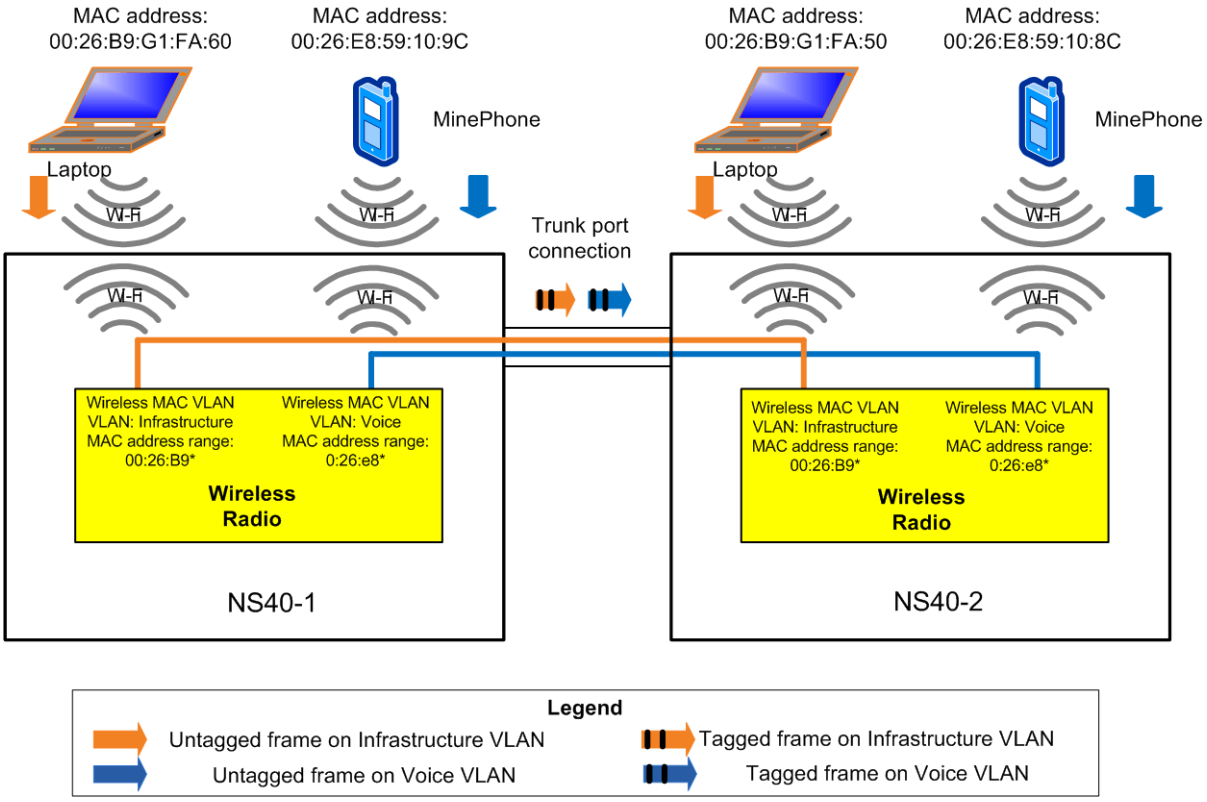
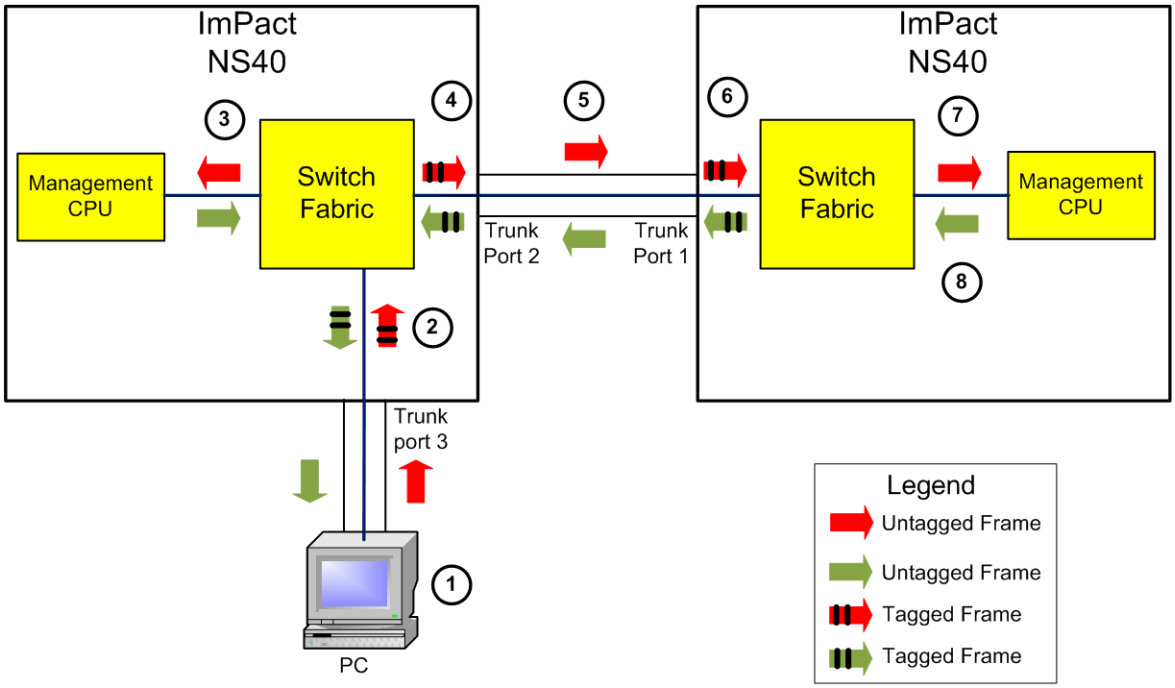


Figure 9: An example of Wireless MAC VLANs

3.3 Native VLAN

Trunk ports on an NS40 support a native VLAN. The native VLAN capability allocates untagged frames received on trunk ports to be associated with the Infrastructure VLAN. This allows client devices such as PCs or laptops to access and manage an NS40.

An example of the native VLAN capability is illustrated in *Figure 10: An example of the native VLAN capability* and described below.



1. Untagged frame is sent into port 3.
2. The switch detects an untagged frame arriving on a trunk port and allocates it to the Infrastructure VLAN.
3. The management CPU is connected to the switch fabric as an access port on the Infrastructure VLAN so it receives the frame without a tag.
4. The frame is sent out port 2 (because it is a trunk port that is a member of the Infrastructure VLAN).
5. Because the frame is on the Infrastructure VLAN, the tag is removed when it is put onto the fibre media between NS40s.
6. The switch detects an untagged frame arriving on a trunk port and allocates it to the infrastructure VLAN.
7. The management CPU is connected to the switch fabric as an access port on the Infrastructure VLAN so it receives the frame without a tag.
8. When the management CPU responds, an untagged frame is sent to the switch fabric (since it is assigned as an access port on the Infrastructure VLAN).

Figure 10: An example of the native VLAN capability

Chapter 4

Configuration using the Web Interface

Topics:

This chapter describes the process for configuring the NS40 using a web browser. All screenshots were generated from devices with firmware version 1.2.0

The NS40 has a built-in web-server accessible by a PC to configure settings. A PC accesses the web browser interface by making a TCP/IP connection to the network switch. For more information on connecting a PC to an NS40, see *Connecting a PC to an I.S. Wireless Network Switch* on page 71.

The IP address of the network device can be located and configured using the UbiDevman device discovery tool. For more information on how to use UbiDevman, see *Discovering Devices on the Network* on page 75.

4.1 Logging onto the Web Interface

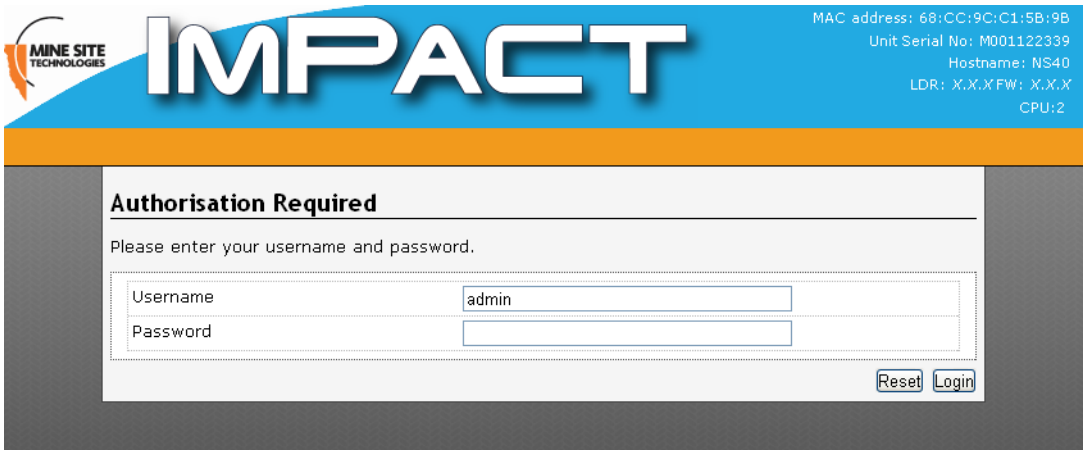
The web browser interface has a login page that requires administrator access. By default the password is 'admin'.

Note: Login and configuration needs to be carried out for each CPU in every NS40 in a network. Each CPU in the NS40 is configured with a different IP address.

To log onto the web browser interface:

1. Launch your web browser and enter **http://<NS40 IP address>** in the address field. The factory default IP address for the NS40 is 192.168.1.90 for CPU 1 and 192.168.1.91 for CPU 2.

2. Press the ENTER key. The NS40 login page is displayed.



3. Enter the username in the **Username** field. The factory default username is **admin**.

4. Type the password in the **Password** field. The factory default password is **admin**.

5. Click **Login**. The configuration home page is displayed.

4.2 Configuration Page

After logging on, the configuration main page is displayed by default as shown in *Figure 11: Default configuration page*.

Figure 11: Default configuration page

The configuration page is divided into four section tabs across the top of the screen:

- **Overview** — web pages to configure language and logout of the web browser.
- **Status** — displays system information, connected devices, wireless clients, system logs, and kernel logs.
- **System** — web pages to configure time, password access, location based services, saving and restoring device configuration, firmware upgrades and rebooting the device.
- **Network** — web pages to configure the LAN interface, wireless network, Wireless MAC VLANs, Spanning tree, VLANs and static routes.

4.2.1 Changes Menu

Any unsaved changes made to the NS40 configuration is displayed at the top right of the configuration page shown in *Figure 12: Unsaved changes drop-down menu*.

Figure 12: Unsaved changes drop-down menu

Clicking **Unsaved Changes** will display a drop-down menu. The drop-down menu actions are described in the table below.

Action	Description
Save & Apply	Saves changes and applies new settings to the device.
Apply	Applies changes to the device.
Revert	Removes any unsaved changes.
Changes	Displays the details of unsaved changes.

4.3 Overview Tab

The **Overview** tab section configures language settings and logs out of the web browser interface.

4.3.1 Setting the Language

The language can be selected from the drop-down menu in the **Language** field as shown in *Figure 13: Language configuration page*. The web browser interface currently only supports English. Future firmware updates will include other languages.

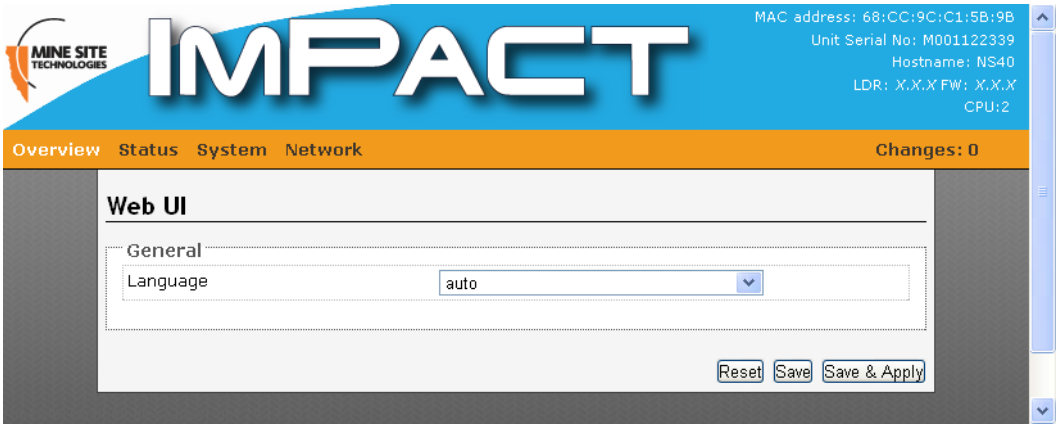


Figure 13: Language configuration page

4.3.2 Logging out of the Web Interface

Clicking **Logout** from the drop-down menu in the **Overview** tab as shown in *Figure 14: Logging out* will logout from the web browser interface.

Figure 14: Logging out

4.4 Status tab

The **Status** tab section contains web pages to configure system information, connected devices, wireless clients, system logs and kernel logs.

4.4.1 Viewing System Status

The **System Status** status page as shown in *Figure 15: System Status page* displays details of the device, system time and current firmware version.

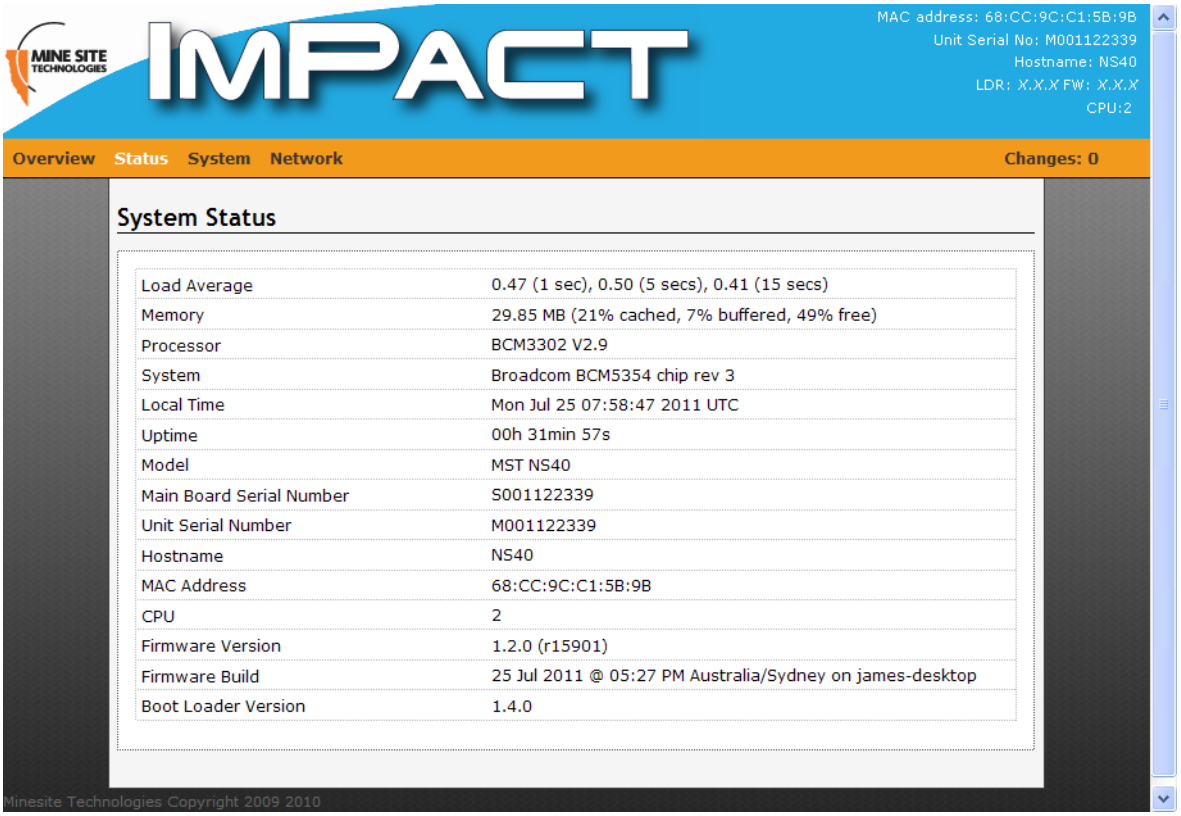


Figure 15: System Status page

4.4.2 Viewing Wireless Networks

The **Networks** page displays information about the wireless network on the NS40 as shown in *Figure 16: Wireless Network status page*.

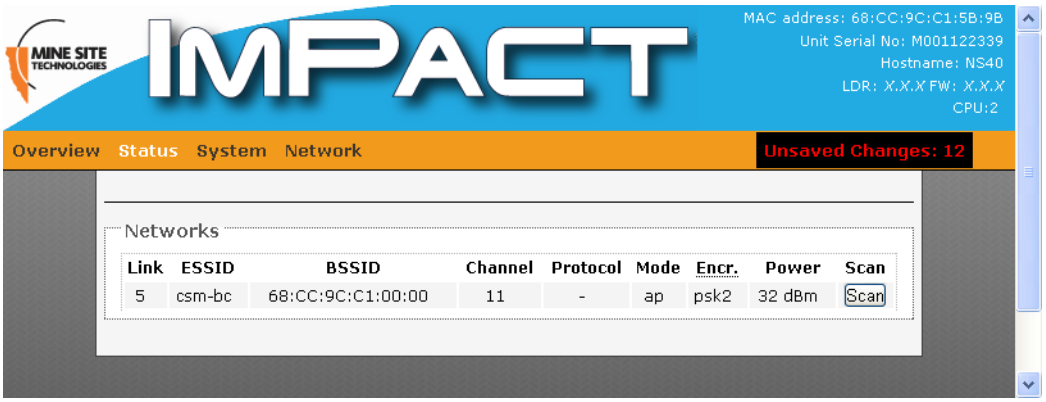


Figure 16: Wireless Network status page

Field	Description
Link	Displays wireless signal strength.
ESSID	Name of the network.
BSSID	Name (MAC address) of the access point.
Channel	Wireless channel allocation.

Field	Description
Protocol	Network protocol used.
Mode	Wireless network mode.
Encryption	Wireless security encryption type.
Power	Display of transmission power.

The page can also display details of surrounding wireless networks as shown in *Figure 17: Results of a sample wireless network scan* by clicking **Scan**.

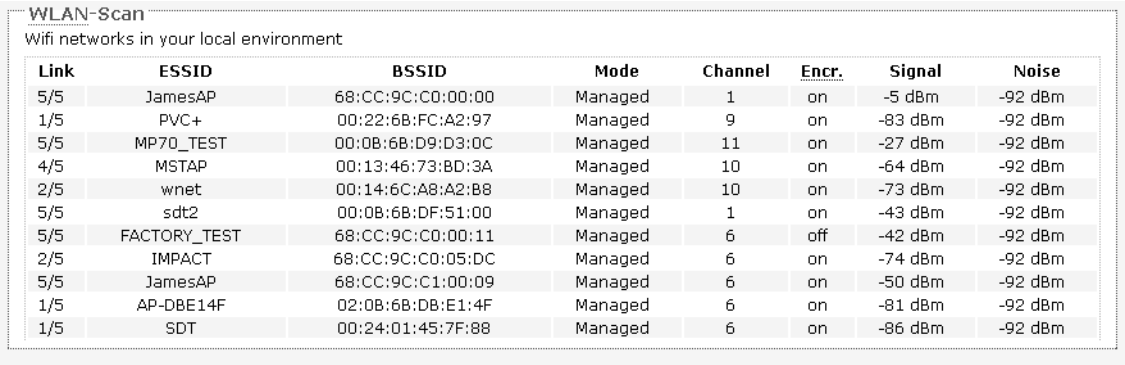


Figure 17: Results of a sample wireless network scan

4.4.3 Viewing AeroScout Status

The **AeroScout Status** page displays AeroScout® tracking engine settings.

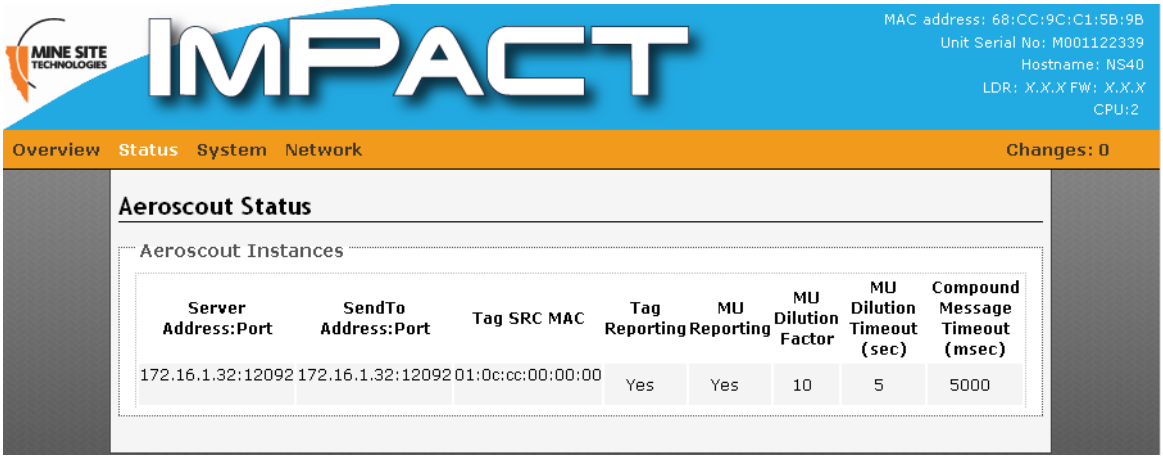


Figure 18: AeroScout Status page

Field	Description
Server Address: Port	IP address and port number of the AeroScout Engine.
SendTo Address: Port	IP address and port number of the AeroScout Engine that an Access Point will send a tag report.
TAG SRC MAC	The MAC address that tag messages are received for.
Tag Reporting	Indicates whether Wi-Fi tag reporting is enabled.

Field	Description
MU Reporting	Indicates if reporting of mobile units is enabled.
MU Dilution Factor	Reporting factor of mobile units.
MU Timeout	MU Timeout setting.
Compound Message Timeout	The amount of time (in milliseconds) tag information is compiled before being sent as a packet in the network. This alleviates the volume of network traffic.

4.4.4 Viewing Ports and STP Status

The **Port and STP Status** page displays Spanning Tree Protocol (STP) and the NS40 port status as shown in *Figure 19: Port and STP status page*.

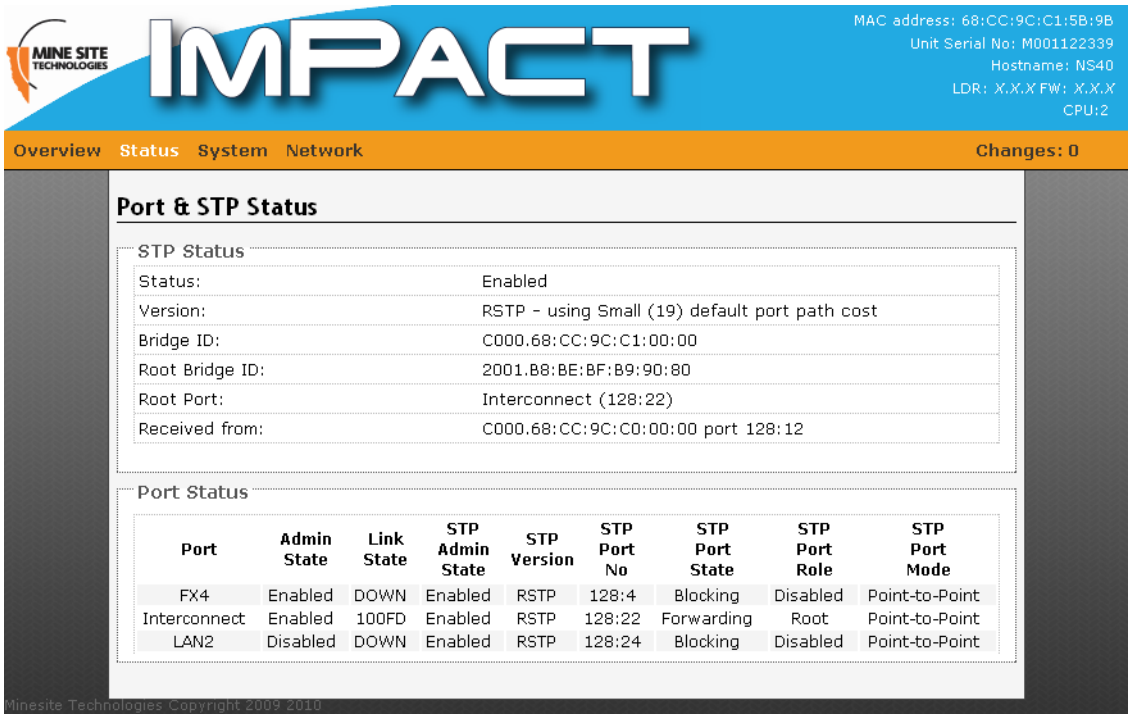


Figure 19: Port and STP status page

The table below describes the fields in the **Port Status** section.

Field	Description
Port	Port name
Admin State	Whether the port is **Enabled** or **Disabled**.
Link State	State and port speed. Values can be link **DOWN**, or up with 10/100/1000 HD (half duplex) or FD (full duplex) depending on port type.
STP Admin State	Spanning Tree Protocol state. Can be **Enabled** or **Disabled**.
STP version	Spanning Tree Protocol version. Can be **STP** or **RSTP**.
STP Port No	Value is displayed as **xxx:yz** where **xxx** = Port priority, **y** = CPU number and **z** = Physical port number.

Field	Description
STP Port State	Shows the current spanning tree state of the port within a spanning tree. Can be **Forwarding**, **Blocking**, **Learning** or **Disabled**.
STP Port Role	The function of the port in STP. Values can be **Backup**, **Alternate**, **Designated**, and **Root**.
STP Port Mode	Values displayed are **Edge**, **Delay-forwarding** and **Point to Point**.

Viewing Interfaces

The **Interfaces** page shows details of the LAN and wireless radio on the NS40 as shown in *Figure 20: Interfaces status page*.

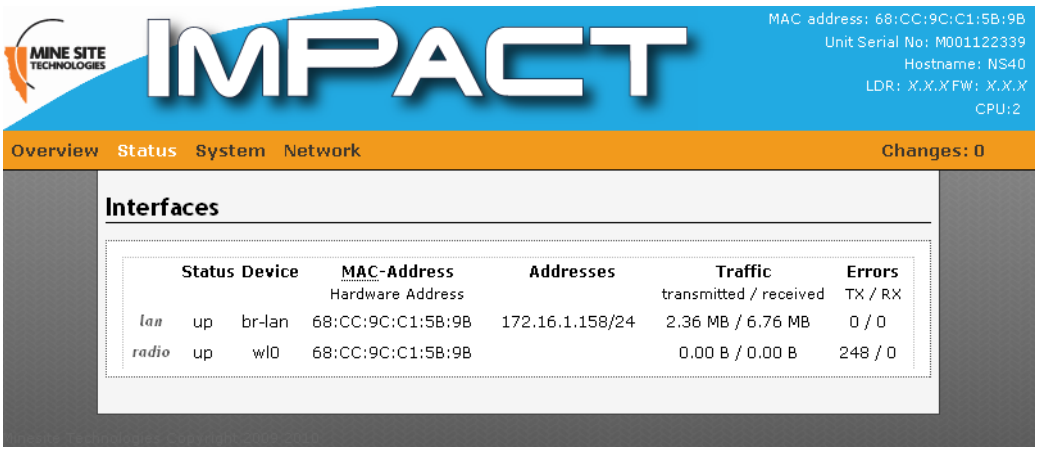


Figure 20: Interfaces status page

Field	Description
Status	Indicates the operating status.
Device	Device name.
MAC Address	The LAN and radio are bridged and will have the same MAC address.
Addresses	Assigned IP address.
Traffic	The amount of data transmitted and received since the last startup of the network switch.
Errors	Displays any transmission or receive errors.

4.4.5 Viewing MAC Address Table

The **MAC Address Table** page maps MAC addresses of devices to the ports on the NS40 where those devices are located. There can be one or a number of MAC addresses bound to the interface depending on the port type and the devices connected.

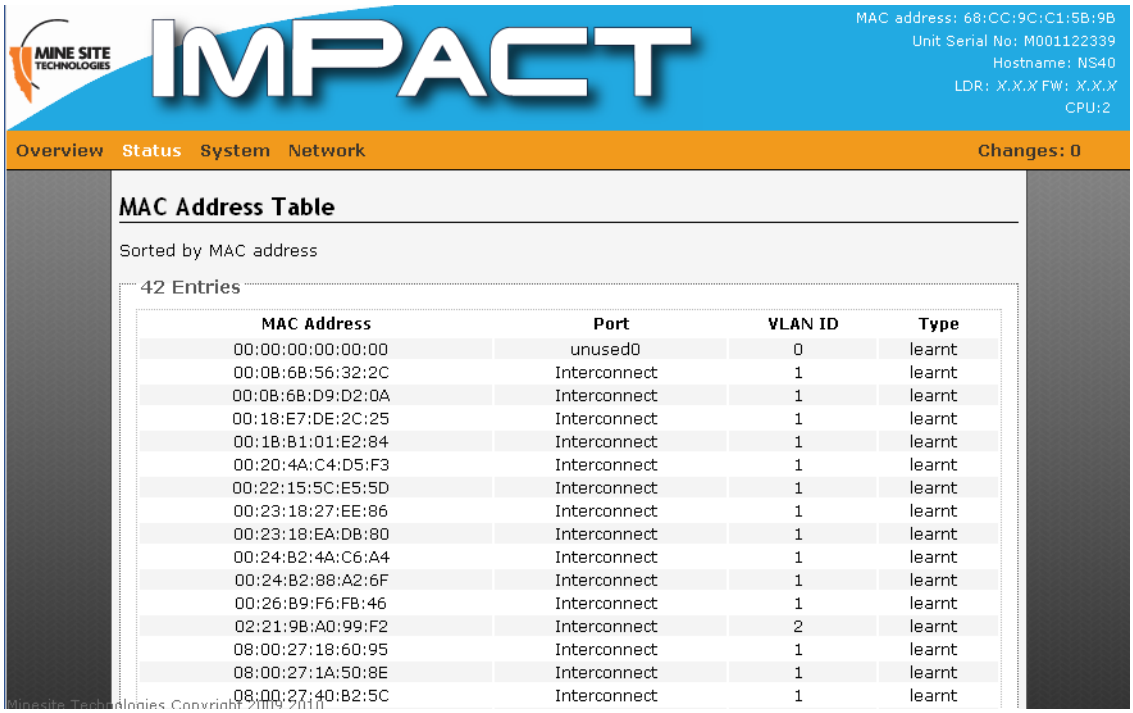


Figure 21: MAC Address Table page

The table below describes the MAC Address Table fields.

Field	Description
MAC Address	MAC Address of the device on the network.
Port	The port type that the device is connected to. This can be Interconnect, FX1-4, LAN1-2, CPU
VLAN ID	The VLAN ID where the device resides.
Type	Can be two values: **learnt** or **static**.

4.4.6 Viewing Routes

The **Routes** status page displays information on local network routes as shown in *Figure 22: Routes status page*.

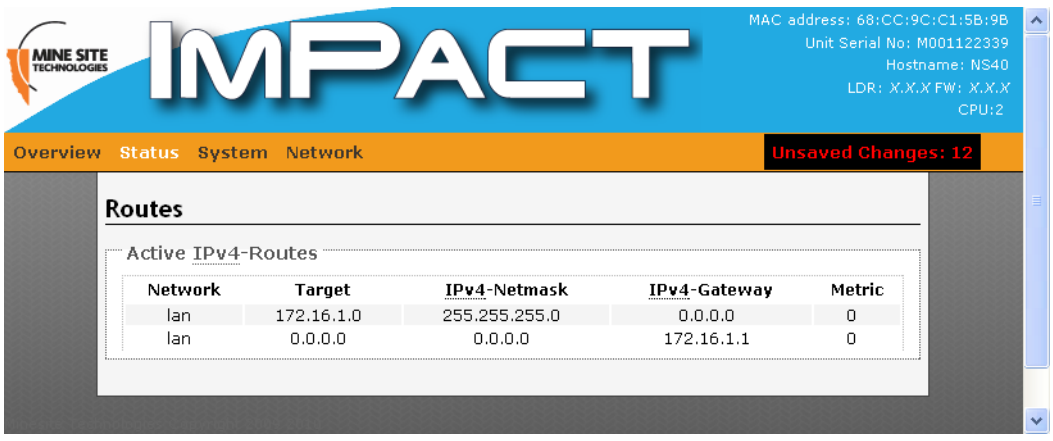


Figure 22: Routes status page

Field	Description
Network	Network type.
Target	Host IP address or network.
Network	Subnet mask of the network.
Gateway	Gateway.
Metric	Weighting factor of a route.

4.4.7 Viewing System logs

The **System log** page displays logged program messages as shown in *Figure 23: System log status page*. Configuring reporting levels for the VLAN Bridge filter and Location Based Services will also determine what is displayed on this page. The system log page is useful for viewing general information, analysis of the switch and debugging messages.

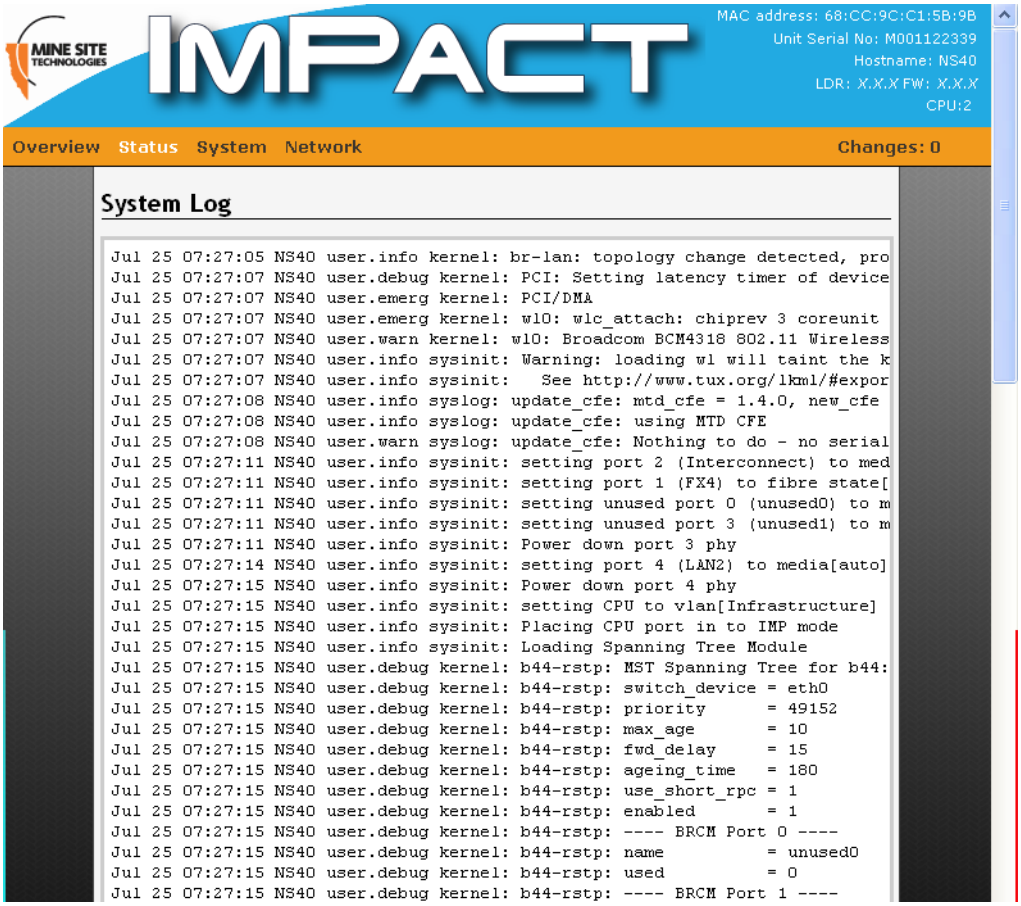


Figure 23: System log status page

4.4.8 Viewing Kernel Logs

The **Kernel Log** page tracks and logs activity of the kernel as shown in *Figure 24: Kernel Log page*.

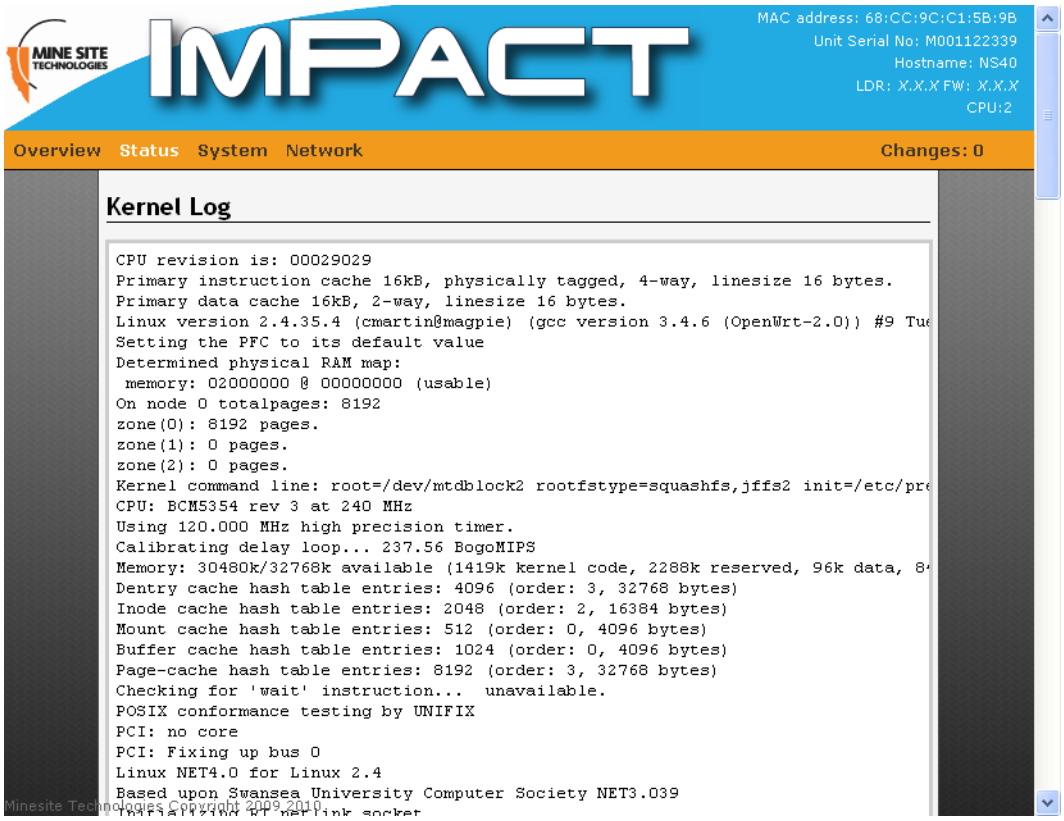


Figure 24: Kernel Log page

4.5 System tab

The **System** tab accesses web pages to configure time, password access, Location Based Services, saving and restoring device configuration, firmware upgrades and rebooting the device.

4.5.1 Changing System Settings

The **System** configuration page configures general system settings as shown in *Figure 25: System page*.

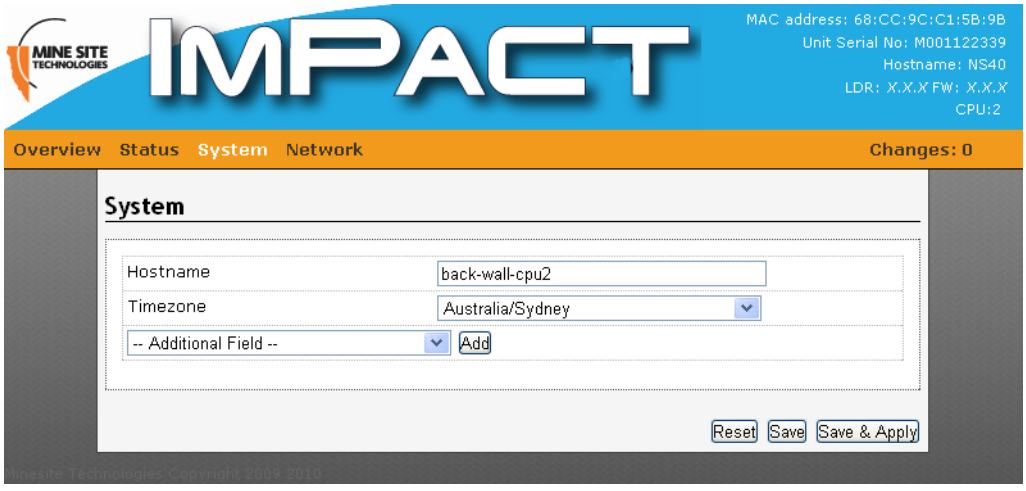


Figure 25: System page

Additional parameters can be displayed and configured from the **Additional Field** drop-down box and clicking **Add**.

The system parameters are described in the table below.

Field	Description
Hostname	Name of the device.
Timezone	A drop-down box to select the country timezone.
External system log server	IP address of the external system log server.
System log buffer size	Buffer size is 16kb by default.
Log output level	0-7 filtering of system log messages.

4.5.2 Changing the System Administrator Password

The administrator login restricts access to the web browser configuration. It is strongly recommended to change the default password when using it for the first time.

Figure 26: Administrator password page

To create a new password:

1. Enter the administrator password in the **Password** and the **Verify Password** fields.
2. Click **Submit**. Administrators will have full access to the web browser interface.

4.5.3 Managing System Processes

The **Processes** page displays and manages system processes in the NS40 as shown in *Figure 27: System processes configuration page*.

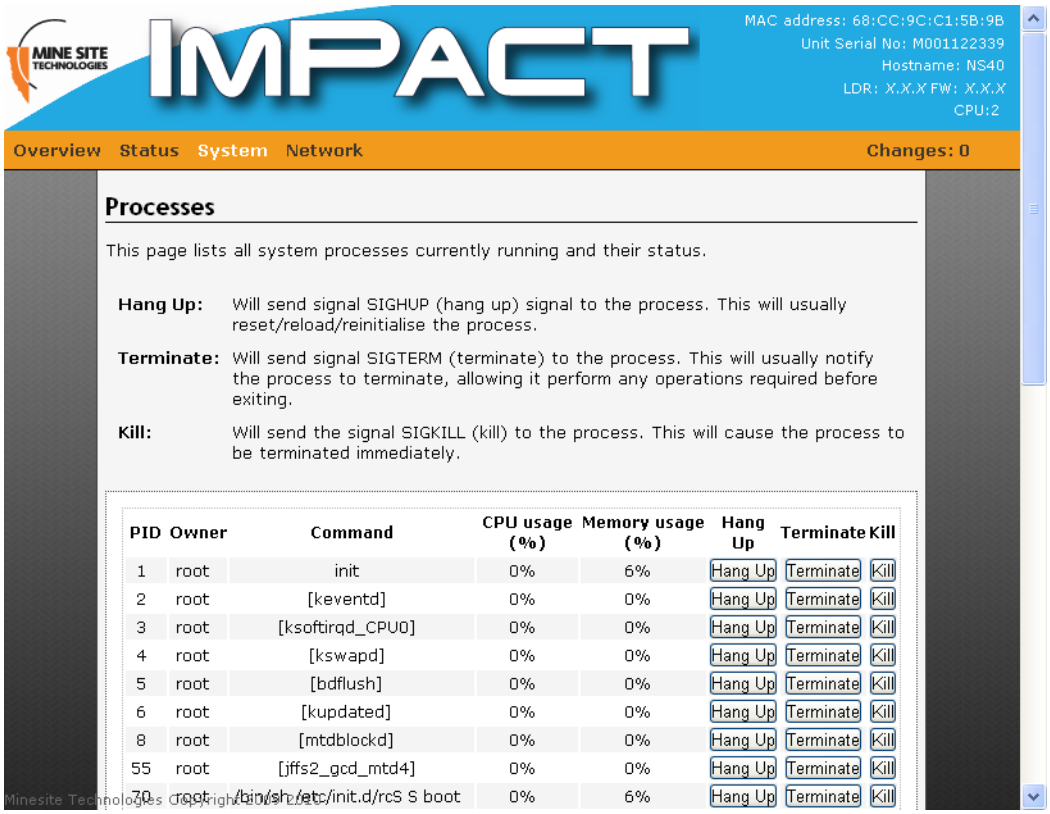


Figure 27: System processes configuration page

Each system process can be stopped by clicking the **Hang Up**, **Terminate** or **Kill** buttons. Stopping system processes is described in the table below.

Process	Description
Hang up	Hang up will either reset, reload or reinitialise the process.
Terminate	Terminate will perform and exit any operations relating to the system process before closing.
Kill	Kill will immediately close the system process.

4.5.4 Configuring Location Based Services

The **Location Based Services** page as shown in *Figure 28: Location Based Services configuration page* establishes where AeroScout tag reports are sent. An NS40 can communicate with an AeroScout Positioning Engine and / or a MST Tracker Engine.

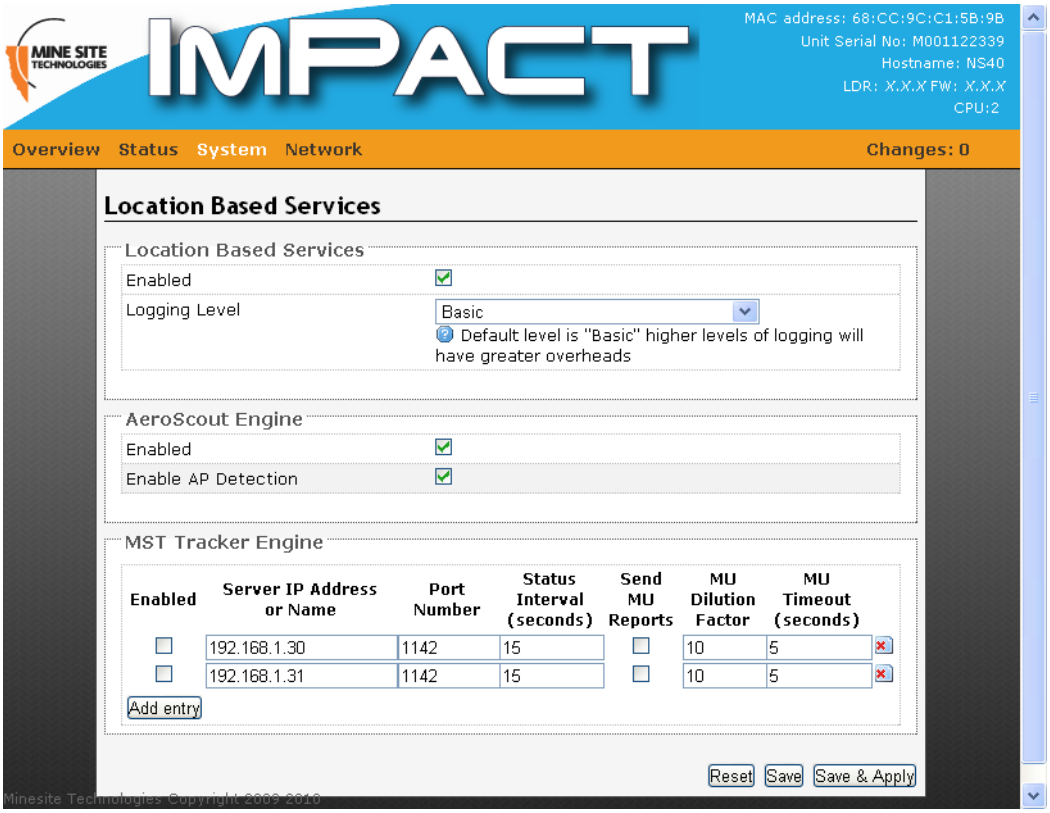


Figure 28: Location Based Services configuration page

A description of the Location Based Services fields are shown in the following table.

Section	Field	Description
Location Based Services	Enabled	Check box that enables the location based services on the NS40.
	Logging Level	The drop-down box selects the level of reporting details to the syslog server. There are four levels of reporting: • Errors & Warnings — the lowest level of reporting which will report any errors or warnings. • Basic — logs start up configuration and any errors and warnings. This is the factory default setting. • Extra Information — reports basic information of the tracking engine, tags and mobile units. • Debug — highest level of reporting which includes detailed information of tag reads. Note that higher levels of reporting will increase the system overhead in the NS40.
AeroScout Engine	Enabled	Enables communication with an AeroScout engine.
	Enable AP Detection	Enables the detection of surrounding Access Points.

The NS40 can have up to two MST Tracker Engines configured. The configuration parameters are described in the table below.

Field	Description
Enabled	Check box to enable the MST Tracker Engine.

Field	Description
Server IP or Name	IP address or server name of the MST tracker engine.
Port Number	Port number of the MST tracker engine. By default the port number 1142.
Status Interval	How often status messages are sent to the MST tracker engine.
Send MU Reports	The check box enables reporting for mobile units (such as the Mine Phone).
MU Dilution Factor	Reporting factor for mobile units. By default the value is 10, where a report is sent for every tenth read of the device.
MU Timeout	If no frames from a mobile unit are received, the server will sent a report based on the MU Timeout setting. By default the value is 5 seconds.

Click **Save** to save settings or **Save & Apply** to instantly apply new settings.

4.5.5 Configuring Network Time

The **Network Time** configuration page defines regional time settings on the NS40 as shown in *Figure 29: Network Time configuration page*.

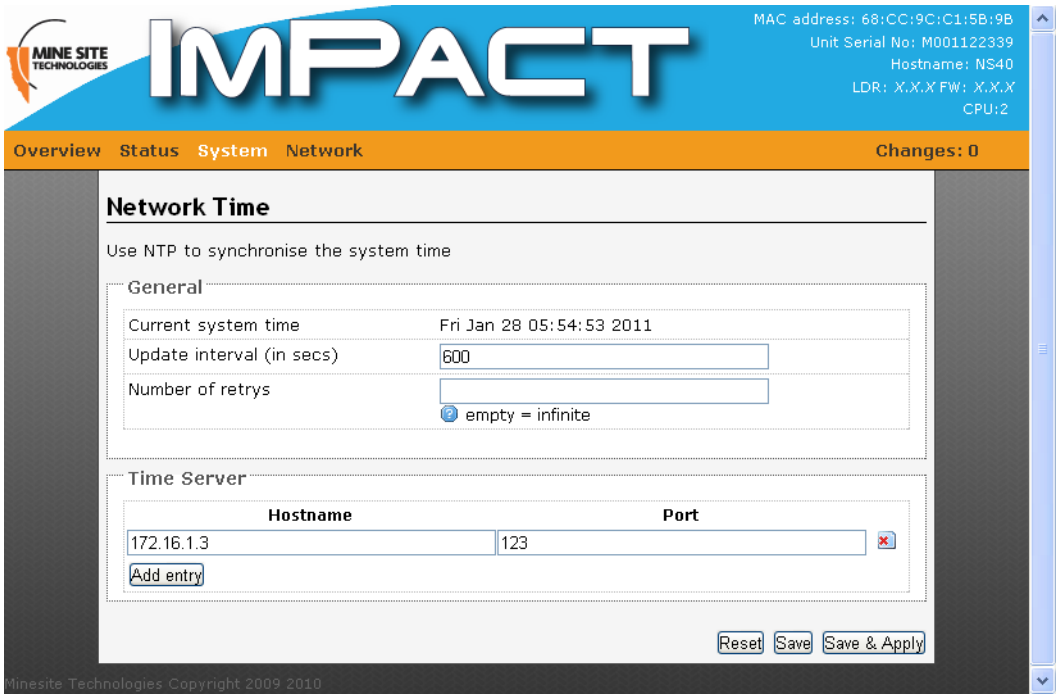


Figure 29: Network Time configuration page

The network time can be synchronised with a Network Time Protocol (NTP) server. The NTP lookup is performed by the switch's management CPU (which resides on the Infrastructure VLAN).

A description of the configuration parameters are shown in the table below.

Section	Field	Description
General	Current System Time	Displays the current system time.
	Update Interval	The frequency that an NS40 will synchronise with the NTP server. 600 seconds is the default setting.

Section	Field	Description
	Count of Time measurements	The number of times the NS40 will try to connect to the NTP server if it cannot make a connection.
Clock Adjustment	Offset Frequency	Average time drift of the NS40 when referenced to a NTP server.

To add an NTP server:

1. Enter the IP address or host name of the NTP server in the **Hostname** field.
2. Enter the port number in the **Port** field.
3. Click **Save** to save settings or **Save & Apply** to save and instantly apply new settings to the device.

4.5.6 Changing the Unit Serial Number

The serial number of the NS40 unit can be entered in the web interface. The unit serial number is on the identification label located on the outside of the NS40 enclosure.

1. Enter the serial number in the supplied field and press reset.
2. The NS40 will reset and may take up to 15 seconds to update. Do not unplug or turn off the power supply until the unit has reset.

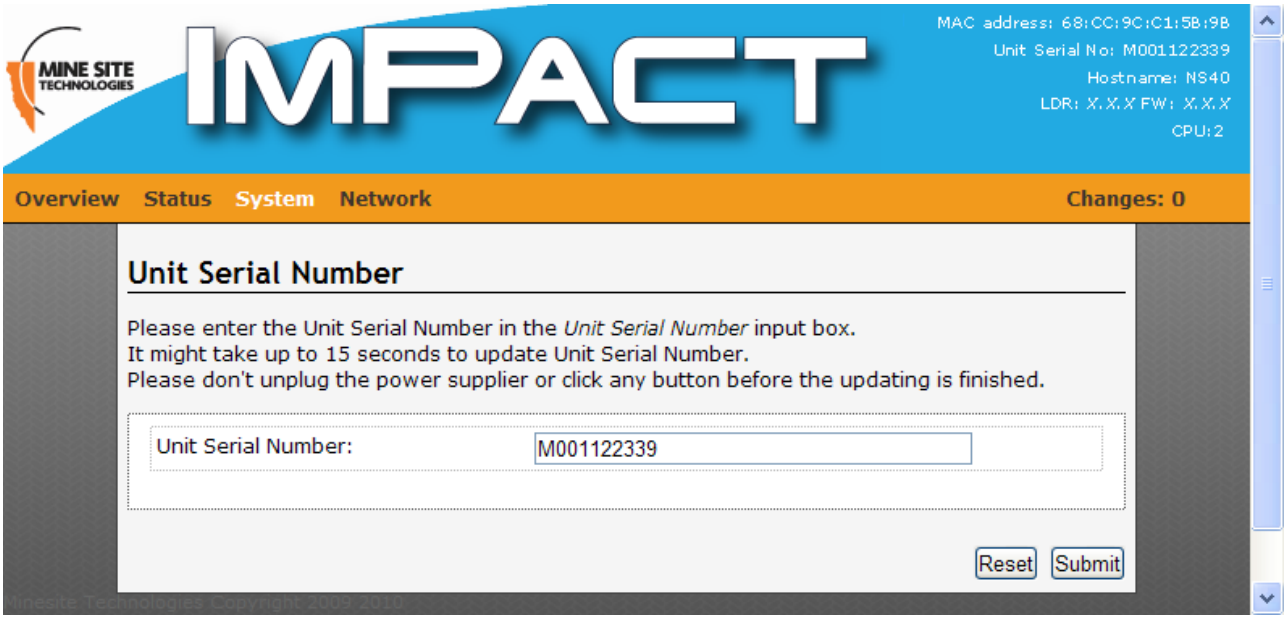


Figure 30: Unit Serial Number page

4.5.7 Backup and Restore Settings

The **Backup / Restore** configuration page shown in *Figure 31: Backup / Restore configuration page* enables the NS40 to save configuration settings, reset to factory default settings and restore saved settings.

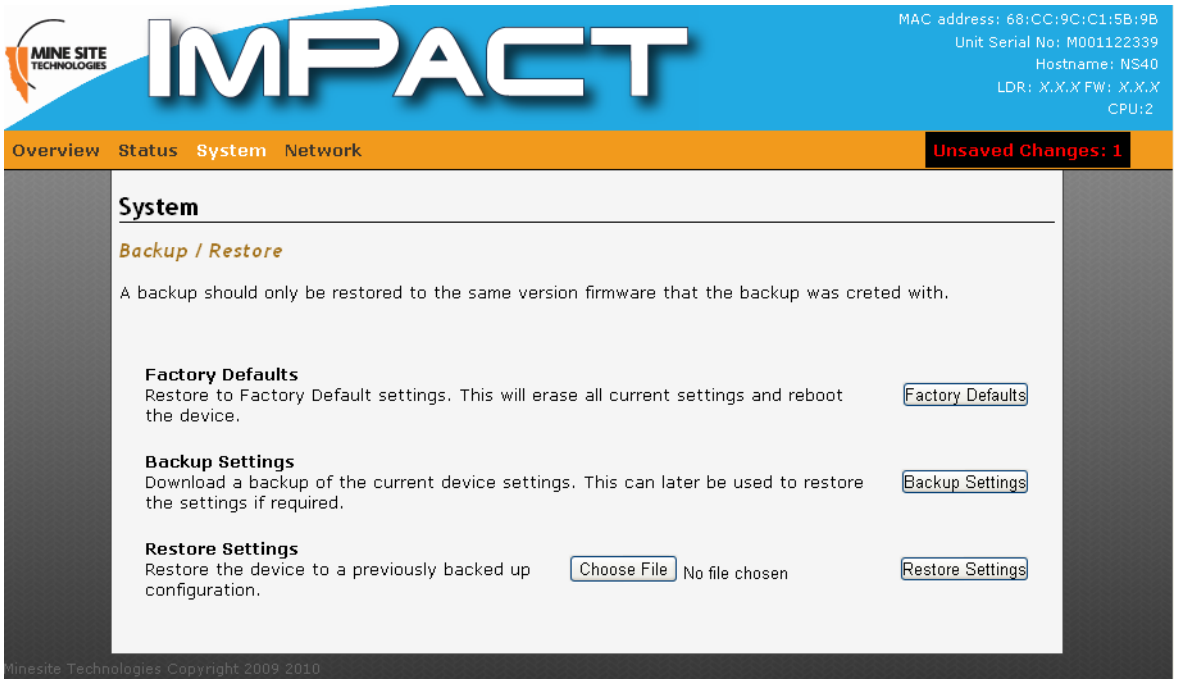
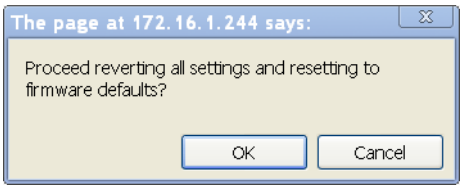


Figure 31: Backup / Restore configuration page

Reset Device to Factory Settings

To restore to factory default settings:

1. Click **Factory Defaults**. A dialog window will appear to confirm to reset the device.



2. Click **OK**. The device will reset.

Backup Device Settings

Configuration settings in the NS40 can be saved and used to restore to the device.

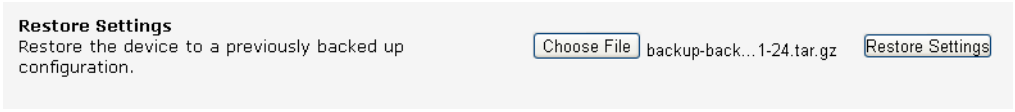
To backup device settings, click **Backup Settings**. Settings are saved and downloaded as a compressed tar.gz file format to your computer.

Restore Saved Settings

Note: Saved device settings should not be restored to a device with earlier firmware version than the backup was made from.

To restore device settings:

1. Click **Choose File**. A dialog window will open.
2. Select the saved settings file tar.gz file from your computer and click **Open**.



3. Click **Restore Settings**. The file will be uploaded and the device will reboot.

4.5.8 Rebooting the Device

The Reboot page as shown in *Figure 32: Reboot configuration page* reboots the device by selecting the **Reboot** button.

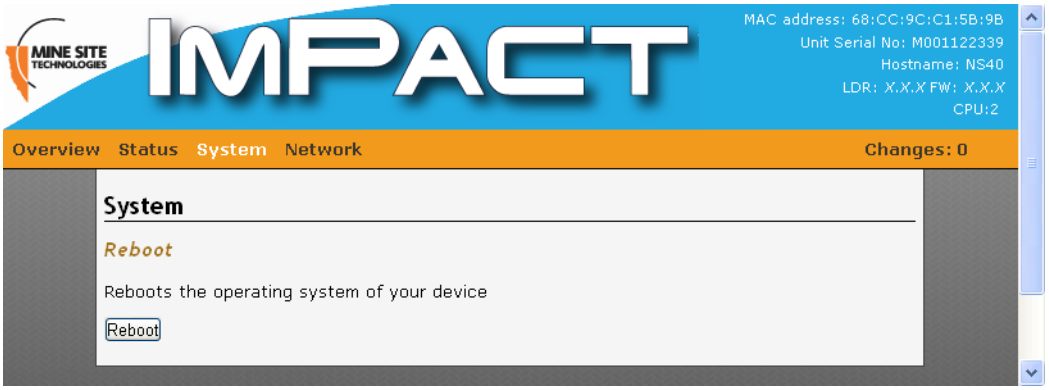


Figure 32: Reboot configuration page

4.6 Network Tab

The network tab accesses web pages to configure the LAN interface, wireless network, Wireless MAC VLANs, Spanning Tree, VLANs and static routes.

4.6.1 Configuring LAN Interface Settings

The **LAN Interface** page shown in *Figure 33: LAN Interface configuration page* configures the LAN settings of the device.

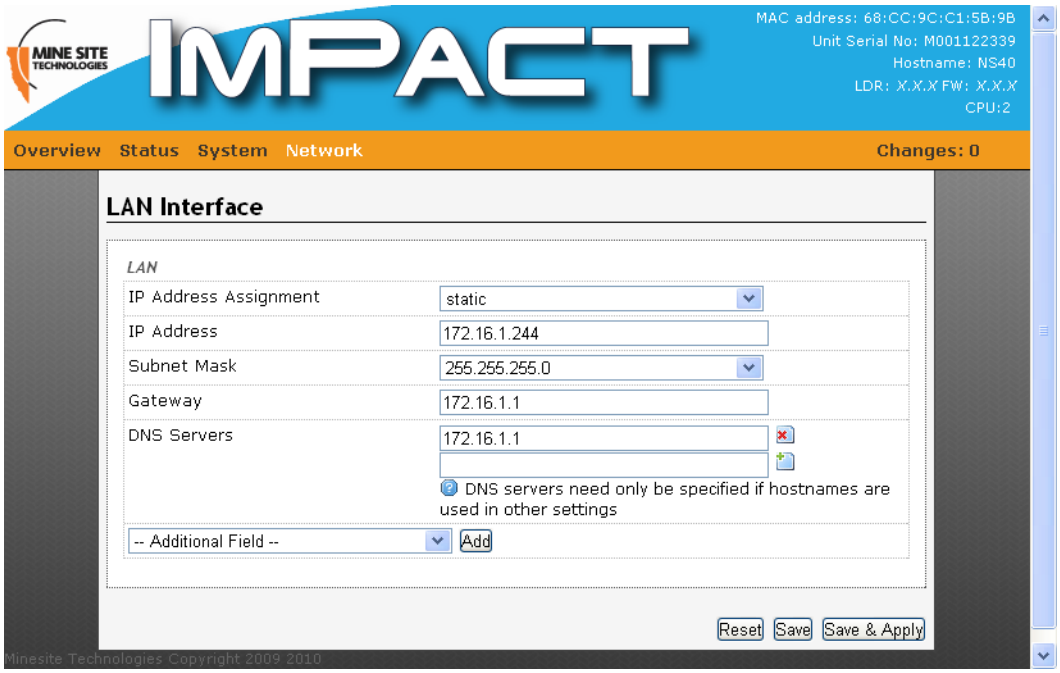


Figure 33: LAN Interface configuration page

To edit LAN settings, click the selected field in the dialog box. Click **Save** to save settings or **Save & Apply** to save and instantly apply settings. LAN settings are described in the table below.

Field	Description	Recommended Settings
IP Address Assignment	Static or DCHP can be assigned to the device.	When the DHCP setting is selected, all static configuration fields are removed from the page.
IP Address	The IP address of the CPU in the device.	The default IP address for CPU 1 is 192.168.1.90 and CPU 2 is 192.168.1.91. Assigning a different IP address is required for each management CPU.
Subnet Mask	Identifies the subnet the IP address belongs to for the CPU in the device.	By default the subnet mask is 255.255.255.0.
Gateway	The IP address of the default gateway to be used by the device.	n/a.
DNS servers	The DNS servers used by the managment CPU when looking up host names.	Settings are dependent on the local domain name registration.
MTU	Maximum transmission size (MTU) is the largest packet size (in bytes) a network can transmit.	The MTU in the device is automatically configured based on the protocol configuration. It can be manually configured if required.

4.6.2 Configuring Wireless Interface Settings

The **Wireless Interface** configuration page configures wireless settings for the NS40 as shown in *Figure 34: Wireless Interface configuration page*.

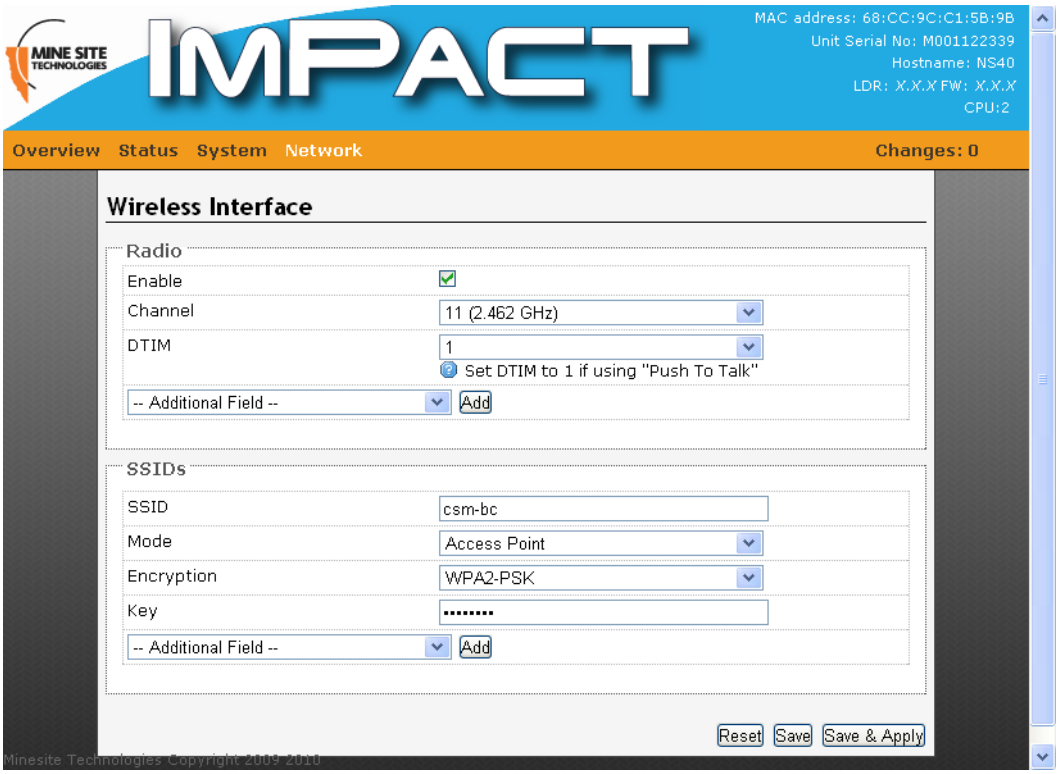


Figure 34: Wireless Interface configuration page

To configure wireless settings on the device:

1. Select the **Enable** check box to enable wireless.
2. Click on the drop-down boxes in the supplied fields.
3. For additional configuration options, click on the **Additional Field** drop-down menu. The radio parameters and settings are described in the table below.
4. Click **Save** to save settings or **Save & Apply** to save and instantly apply new settings to the device.

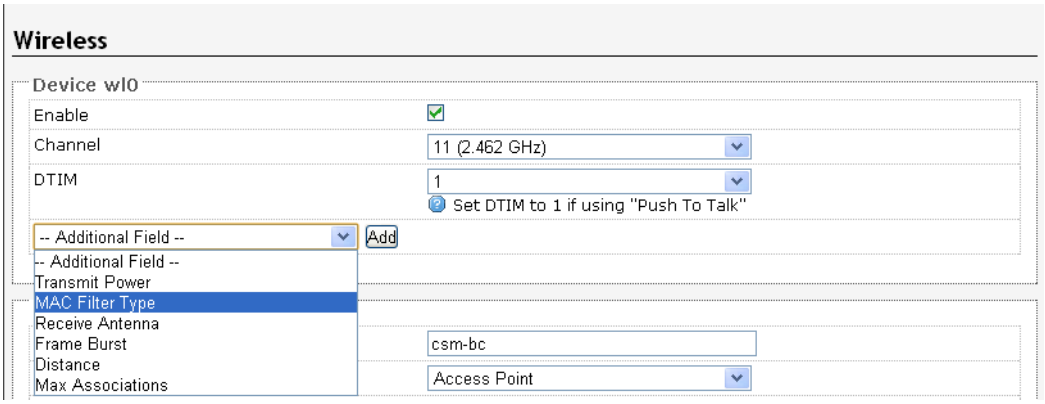
Field	Description	Recommended Settings
Enable	Check box to enable or disable wireless radio.	n/a.
Channel	A drop-down box to select the channel the wireless radio will operate on the NS40.	It is recommended wireless radios in proximity of each other have a different wireless channel. This minimises signal overlap and the possibility of interference.
DTIM	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.	By default the DTIM interval is 1.
Transmit Power	Used to control the range of the wireless performance.	High.
MAC filter type	Listed MAC addresses can enabled (or disabled) for wireless network access.	n/a.

Field	Description	Recommended Settings
Receive Antenna	Defines the antenna mode for wireless frame reception.	By default the Receive antenna is set to Diversity.
Max Associations	The maximum number of devices that can simultaneously connect to the access point.	n/a.

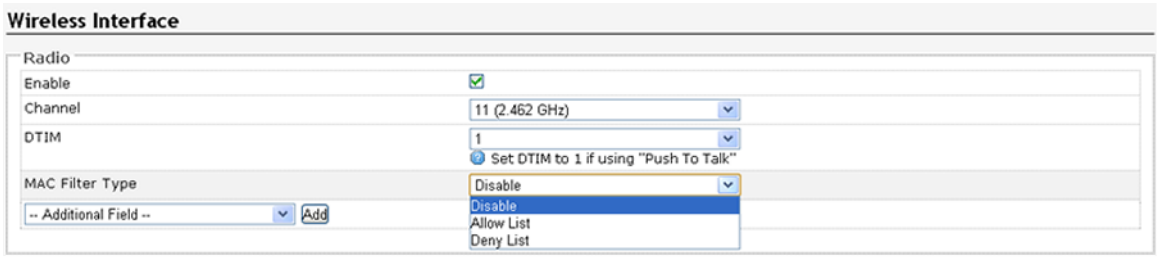
MAC address filtering

To enable MAC address filtering:

1. In the **Device** section, select **MAC Filter Type** from the **Additional Field** drop-down box.



2. The MAC Filter Type and MAC list menu fields are displayed. By default, MAC address filtering is disabled.



3. Select **Allow List** on the drop-down box.

4. Enter the MAC address to allow network access in the **MAC List** field. To add MAC addresses, click on the icon for MAC address fields.

5. Select **Deny List** from the MAC filter type drop-down menu.
6. Enter the MAC address in the **MAC List** field to deny access to the network. To add MAC addresses, click on the icon for MAC address fields.

7. Click **Save** to save settings or **Save & Apply** to save and instantly apply new settings to the device.

Configuring SSID

The NS40 has a SSID which is configured in the **Wireless Interface** page as shown in *Figure 34: Wireless Interface configuration page*.

A description of the configuration parameters are described in the table below.

Field	Description
SSID	The name of the wireless network visible to client devices.
Mode	There are several wireless network modes to select from the drop-down menu: • Access point • Ad-Hoc • Client • Wireless Distribution System (WDS)

Encryption	Three wireless security modes are available:
	• WEP is the original wireless encryption standard.
	• WPA provides a higher level of security than WEP.
	  • WPA- PSK does not require an authentication server.
	  • WPA-EAP requires a RADIUS authentication server.
	• WPA2 provides a higher level of security than WPA.
	  • WPA2-PSK does not require an authentication server.
	  • WPA2-EAP requires a RADIUS authentication server.

Hide SSID	Enables or disables visibility of the wireless network.
Isolate Clients	When enabled, client devices are prevented from accessing other client devices on the same wireless network.
Multi-Media Extensions	A 802.11e standard for multimedia and VOIP applications. By default this feature is disabled.

Configuring WEP Security Settings

To configure WEP security settings:

1. Select the WEP mode from the **Encryption** drop-down box.
2. Enter a password in the **Key** field.
3. Select Default WEP Key from the drop-down box.
4. Click **Save** to save settings or **Save & Apply** to save and instantly apply settings to the device.

Configuring WPA-PSK and WPA2-PSK Settings

WPA and WPA2 provide stronger security encryption than WEP.

To configure settings:

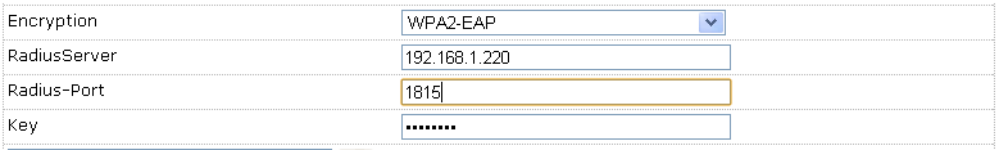
1. Select the WPA-PSK or WPA2-PSK mode from the **Encryption** drop-down menu.
2. Enter the Pre-Shared Key in the **Key** field. The key must be at least 8 alphanumeric characters in length.

3. Click **Save** to save settings or **Save & Apply** to save and instantly apply settings to the device.

Configuring Wireless Extensible Authentication Protocol (EAP)

WPA-EAP and WPA2-EAP requires a RADIUS server for authentication. To configure wireless EAP:

1. Select the WPA-EAP or WPA2-EAP mode from the **Encryption** drop-down box.



2. In the **RadiusServer** field, enter the RADIUS server's IP Address.
3. In the **Radius-Port** field, enter the RADIUS port number.
4. Enter the Pre-Shared Key in the **Key** field. The key must be at least 8 alphanumeric characters in length.
5. Click **Save** to save settings or **Save & Apply** to save and instantly apply settings to the device.

4.6.3 Configuring Wireless MAC VLAN Bridge Settings

Setting up a Wireless MAC VLAN Bridge requires assigning a MAC address or MAC address range for wireless devices to a VLAN. A wireless device whose MAC address does not match the MAC address(es) defined in the Wireless MAC VLANS will have traffic allocated to the Default VLAN.

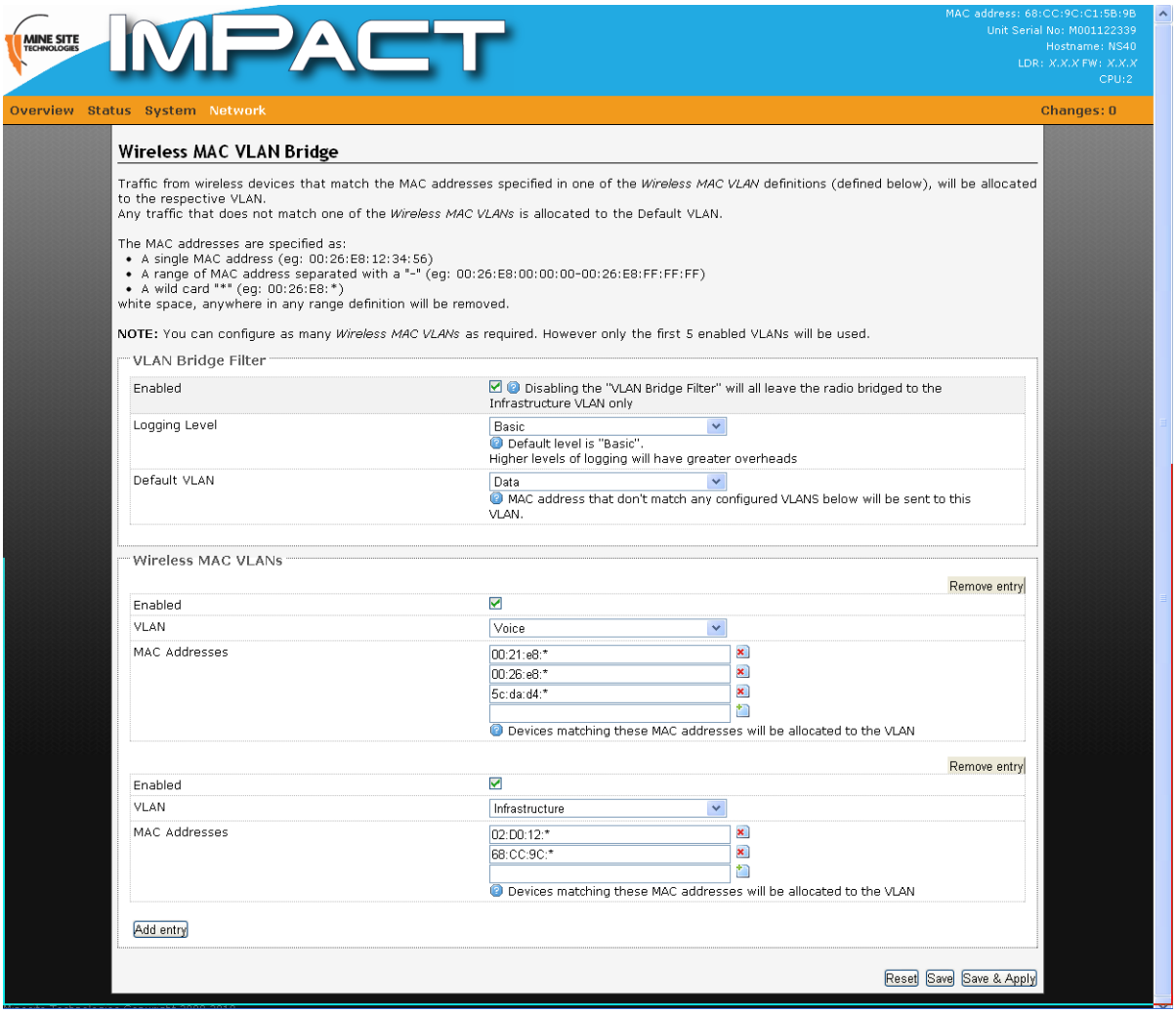


Figure 35: Wireless MAC VLAN Bridge page

Up to five Wireless MAC VLANs can be used in the NS40. The VLAN Bridge Filter parameters are described in the table below.

Field	Description
Enabled	Check box to enable the VLAN bridge filter. If it is disabled the radio is bridged to the Infrastructure VLAN.
Logging Level	The drop-down box selects the level of reporting details to the syslog server. There are four levels of reporting: • **Errors & Warnings** — lowest level of reporting which will report any errors or warnings. • **Basic** — logs starts up configuration and any errors and warnings. This is the factory default setting. • **Extra Information** — reports basic information of the tracking engine, tags and mobile units. • **Debug** — highest level of reporting which includes detailed information of AeroScout tag reads. Note that higher levels of reporting will use more system overhead in the NS40.

Field	Description
Default VLAN	Any client devices with MAC addresses that do not match the defined Wireless MAC VLANs will have traffic directed to the default VLAN. The drop-down box provides a selection of the default VLAN.

Creating Wireless MAC VLANs

To create a Wireless MAC VLAN:

1. In the Wireless MAC VLANs section, click **Add Entry**.
2. Click the **Enable** check box.
3. Select the VLAN from the drop-down box.
4. In the MAC address field, enter the MAC address or MAC address range (separated with a "-"). An "*" after the MAC address denotes all wireless devices with a MAC address complying to the first few hexadecimal digits (see Figure 35).
5. Click to add a field, and enter another MAC address or MAC address range .
6. Click **Save** to save settings or **Save & Apply** to save and instantly apply settings to the device.

4.6.4 Configuring Composite Fibre Ports

The **Ports** page enables and assigns composite fibre ports to be either in trunk or access mode as shown in *Figure 36: Ports configuration page*. A trunk port is a member of all enabled VLANs whilst an access port is a member of only one VLAN. For more information on trunk ports and access ports, see *Understanding Trunk and Access Ports* on page 30.

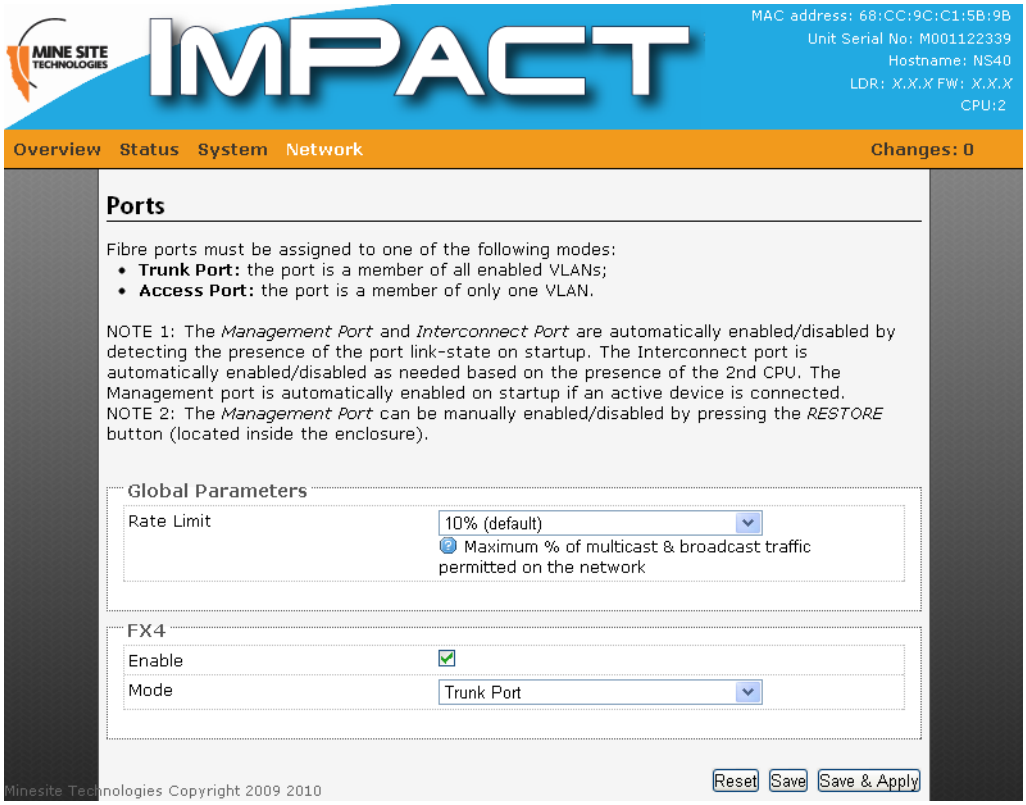
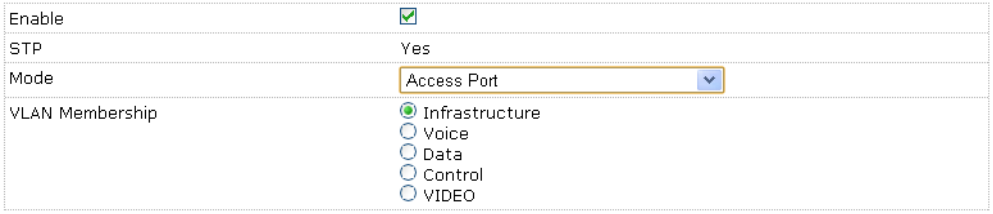


Figure 36: Ports configuration page

To configure the composite fibre port(s):

1. Select the **Enable** check box to enable the fibre port.
2. In the **Mode** field, select trunk port or access port from the drop-down box.
3. If the fibre port is selected as a Trunk port, it will be a member of all enabled VLANs. If it is selected as an access port, select a VLAN membership.



4. Click **Save** to save settings or **Save & Apply** to save and instantly apply settings to the device.

Rate Limit

The **Rate Limit** field restricts the percentage of network bandwidth for broadcast and multicast traffic. This is a secondary feature apart from Rapid Spanning Tree Protocol to assist with network traffic loops.

To configure:

1. Select the rate limit from the drop-down box. By default the rate is 10%.
2. Click **Save** to save settings or **Save & Apply** to save and instantly apply settings to the device.

4.6.5 Configuring Rapid Spanning Tree Protocol

The NS40 supports Rapid Spanning Tree Protocol (RSTP), a protocol that prevents bridge loops and automatically determines an alternate network path if an active link fails. The **Spanning Tree** configuration page is shown in *Figure 37: Spanning Tree configuration page*.

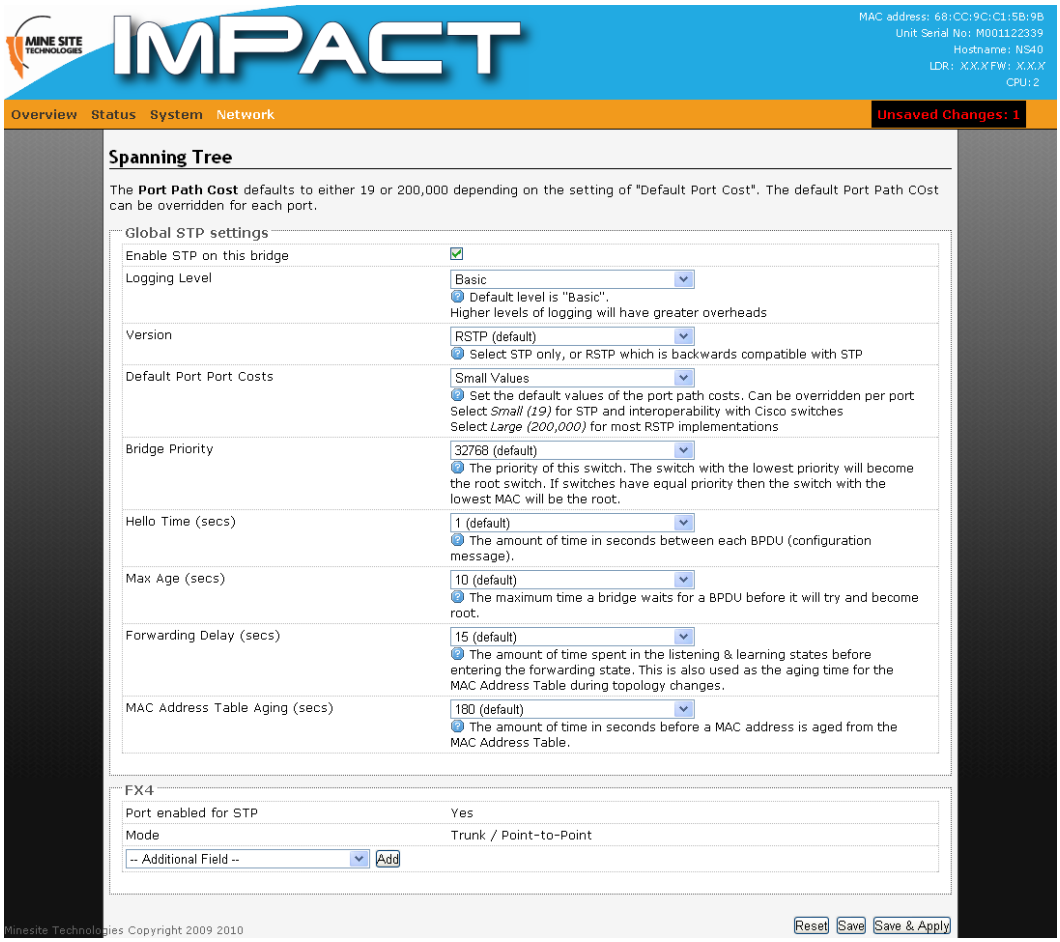


Figure 37: Spanning Tree configuration page

A description of the STP parameters are described in the table below.

Section	Field	Description	Default Settings
Global STP settings	Enable STP on this bridge	Check box to enable STP on the network switch.	On
	Logging Level	Selects the reporting level to the syslog server.	Basic
	Version	Selects RSTP or STP. RSTP is backwards compatible with STP.	RSTP
	Default Port Costs	Sets the default values of the port path costs. Small values is applicable when RTP is used and Cisco brand Switches (even when RSTP is implemented). Large values is applicable when RSTP is implemented.	Small
	Bridge Priority	The priority of the switch. The switch with lowest priority in a network will be the root switch.	32768
	Hello Time	The amount of time in seconds when Bridge Protocol Data Units (BPDUs) are sent. BPDUs exchange information about bridge IDs and root path costs.	1
	Max Age	The amount of time a bridge will wait for a BDPU before it becomes a root bridge.	10

Section	Field	Description	Default Settings
	Forwarding Delay	The amount of time spent in the listening and learning state before entering the forwarding state. This is also used as the aging time for the MAC Address Table during topology changes.	15
	MAC Address Table Aging	The amount of time in seconds before a MAC address is aged from the MAC Address Table. This will assist in minimising traffic across a network.	180
FX*x* (Composite fibre port)	Enable STP	Enables STP on the composite fibre port.	On
	Mode	Port mode of the composite fibre port. This can be configured in **Network > Ports**.	n/a
	Port Priority	Port priority value. A port allocated with the lowest priority value in a network will be the designated root port.	128
	Port cost	The defined port cost that overrides the Default Port Cost.	n/a

4.6.6 Managing Simple Network Management Protocol

The NS40 has Simple Network Management Protocol (SNMP) for monitoring client devices on a network. The **SNMP** page shown in *Figure 38: SNMP page* has a **Trap Destination** field which define the IP address(es) of the host (such as the ImPact Communication Appliance (ICA)) for sending trap information.

SNMP Trap enables client devices to sent messages to the host when there are significant events. Currently link up / down messaging is supported.

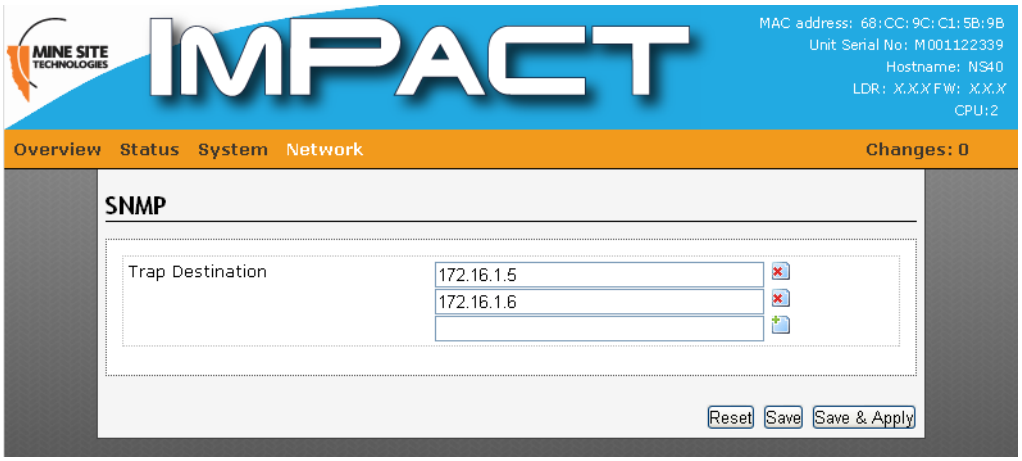


Figure 38: SNMP page

To enter SNMP Trap destination(s):

1. Enter the IP address(es) in the supplied field.
2. To add a IP address field, click . To delete a field, click
3. Click **Save** to save settings or **Save & Apply** to save settings and reboot the switch.

4.6.7 Defining VLANs

VLANs can be defined on the VLAN list page as shown in *Figure 39: VLAN list page*. The VLAN page displays VLANs, their ID and priorities that will be assigned to each VLAN. By default the NS40 has VLANs defined with recommended IDs and priorities. This is based on commonly used applications in mining environments.

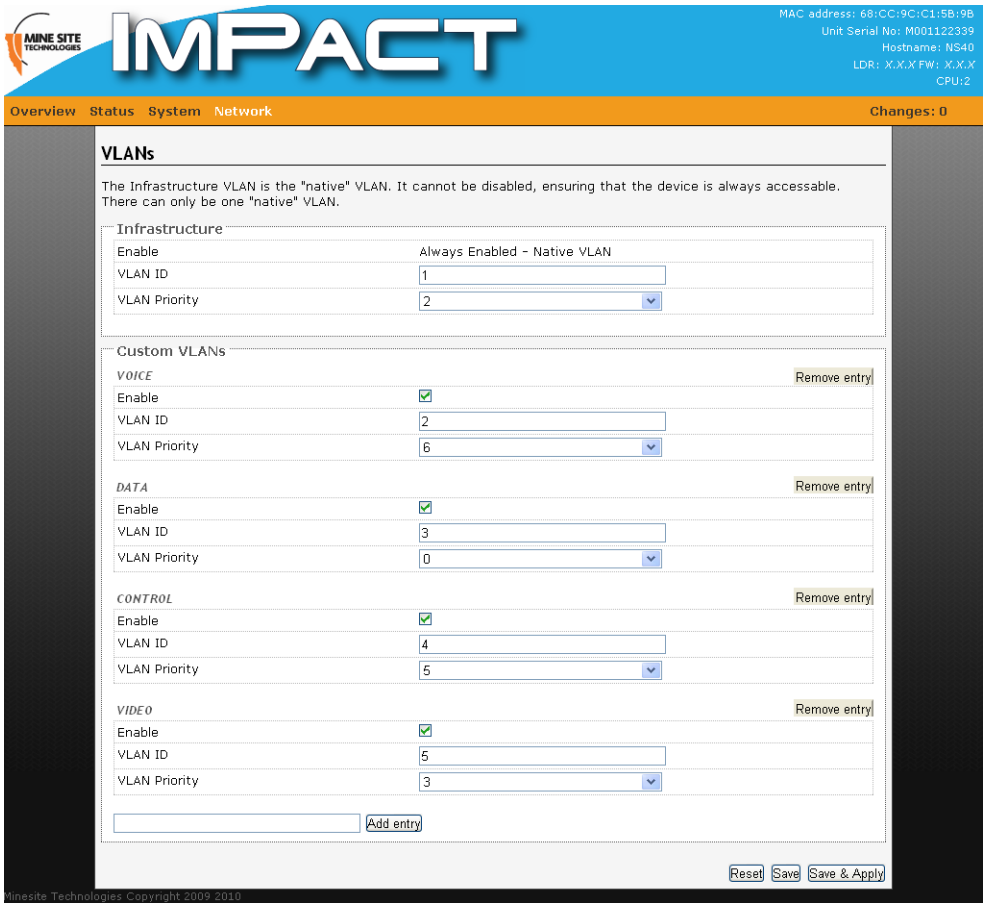
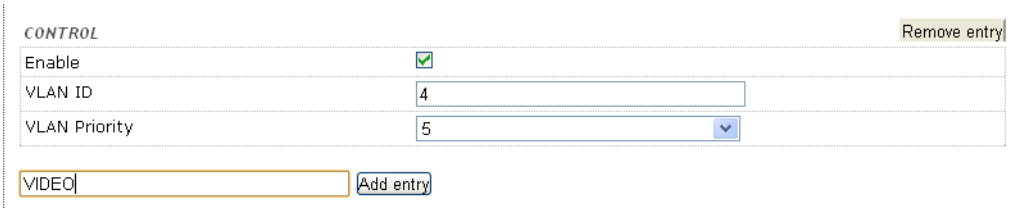


Figure 39: VLAN list page

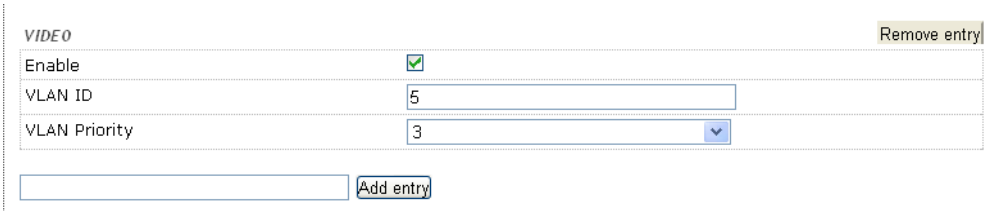
Note: The Infrastructure VLAN cannot be disabled because the management CPU is on this VLAN. This enables client devices to access and manage the network switch.

Up to 16 VLANs can be created. To create a VLAN:

1. Type the name of the VLAN and click **Add entry**. The VLAN parameter fields will appear.



2. By default the **Enable** check box is selected.



3. Enter the VLAN ID number. The VLAN ID is tagged to frames sent to and from trunk ports.
4. Select the **VLAN Priority** from the drop-down menu. Priority ranges from 0-7 (7 being the highest priority) that is assigned to frames tagged with the VLAN ID.

5. Click **Save** to save settings or **Save & Apply** to save and instantly apply settings to the device.

Note:

To configure VLANs, it is recommended to understand the principles of VLANs. For more details on VLANs, see *Understanding VLANs* on page 29.

4.6.8 Adding Static Routes

The Routes page as shown in *Figure 40: Static Routes configuration page* can add static routes which enables network traffic to reach another network.

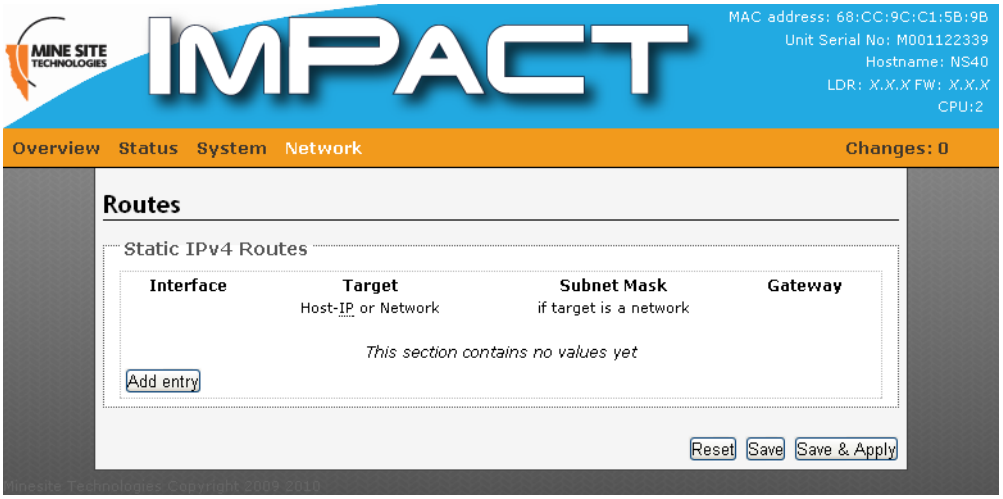
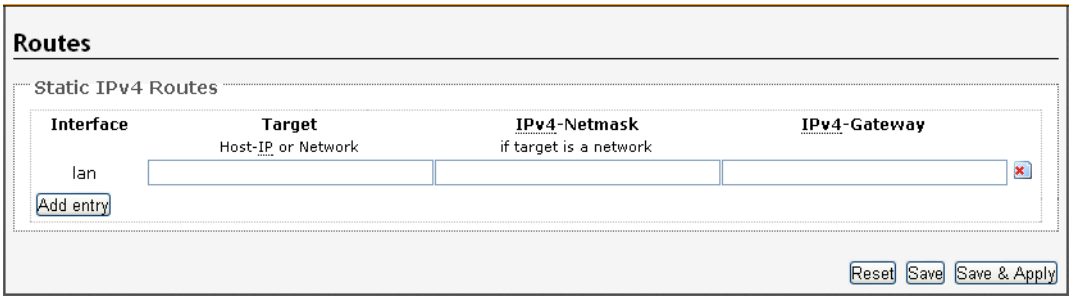


Figure 40: Static Routes configuration page

To add a static route:

1. Click **Add Entry**. A LAN entry is displayed.



2. Enter the network IP address in the **Target** field.
3. Enter the Subnet mask in the **Netmask** field.
4. Enter the Gateway in the **Gateway** field.
5. Click **Save** to save settings or **Save & Apply** to save and instantly apply settings to the device.

Appendix
A

Troubleshooting Guide

This appendix will help diagnose and solve any issues with NS40 installation and operation.

Problem	Possible Causes	Solution
The status light on the NS40 is not blinking when powered up.	Insufficient power supplied to the NS40.	Configuration and power to the cell will need to be revised. Please consult your MST System Engineer to assist. A site survey is conducted to determine power requirements for a system design or modifications.
	NS40 needs to the rebooted.	Reboot the device in the web browser interface under **System > Reboot**.
LEDs on the wireless network switch are not on.	The NS40 has no power.	• Check that power is connected from either the composite cable, DC power cable to the NS40 in the cell. • Verify the network switch is connected to an operational power supply. • Check the power supply is operating as manufacturer's instructions.
The composite fibre port activity light is not on.	The NS40 fibre connector is not connected.	Verify the composite fibre port link is connected and active.
The wireless network cannot be configured from the web browser interface.	There is a network access issue.	• Check that the NS40 is properly installed, all cable connections are connected properly and the unit is powered on. • Check that the VLAN settings on the devices upstream on the network are not restricting access.
Power supply instability.	Incorrect earthing scheme.	Check antennas are insulated from ground.
Client devices cannot connect to the wireless network.	Incorrect Wireless MAC VLAN Bridge settings.	Using the web browser interface under **Network > Wireless MAC VLAN Bridge**, check the MAC address of the device is configured and assigned to the correct VLAN.
	MAC filter settings.	Using the web browser interface under **Network > Wireless Interface**, check the device's MAC address is not denied in the MAC filter settings.
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. Refer to Appendix A for fibre optic cable testing.
Poor wireless coverage or loss of data frames.	Antennas not positioned correctly.	Check antennas are free from obstructions and positioned for optimum transmission. See 2.4.1 Antenna placement and layout.
	A problem with coaxial cable connections.	Check all coaxial cable connections to the NS40, antennas and any antenna splitter boxes.

Problem	Possible Causes	Solution
	Client device(s) may be continually sending multi-cast data frames using up network bandwidth.	Check client devices are not continually sending multi-cast data frames.
PC cannot access device when connected using a media converter.	The port on the NS40 is disabled.	Check the port activity light on the NS40 is on. Connect to the web browser interface and go to the **Network** > **Ports** page 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

Acronyms

Acronym	Meaning
AC	Alternating Current
DC	Direct Current
I.S.	Intrinsically Safe
MAC address	Media Access Control address
MST	Mine Site Technologies
PSU	Power Supply Unit
RF	Radio Frequency
STP	Spanning Tree Protocol
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

Appendix
C

Composite Cable Testing

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

C.1 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.

1. Attach a fibre optic cable to the visual tracer and look at the other end to see if light is transmitting through the fibre.
2. If there is no light, there is a damaged or broken section of the fibre component 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.

C.2 Measuring and Testing for Power Loss

Measuring power and loss requires a Optical time-domain reflectometer (OTDR) with a suitable custom 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
Single-mode fibre	0.5 dBi / km @ 1300nm 0.4 dBi / km @ 1550nm

Appendix
D

Connecting a PC to an I.S. Wireless Network Switch

This Appendix specifies how to set up and connect a PC (with a Windows XP operating system) to the ImPact NS40.

In an existing network, a PC can be connected by an Ethernet cable to the surface network switch. The network switch either incorporates or is connected to a media converter which converts Ethernet cabling to fibre optic cabling to the NS40s. Alternatively a PC can use a media converter to directly connect to the port of an NS40, with a power supply connected to another port.

Note when connecting fibre cable to the NS40, composite fibre port 1 is the default upstream port. The fibre transmit (Tx) and receive (Rx) configuration is wired differently to the downstream ports as illustrated in *Figure 41: NS40 Fibre port wiring configuration*.

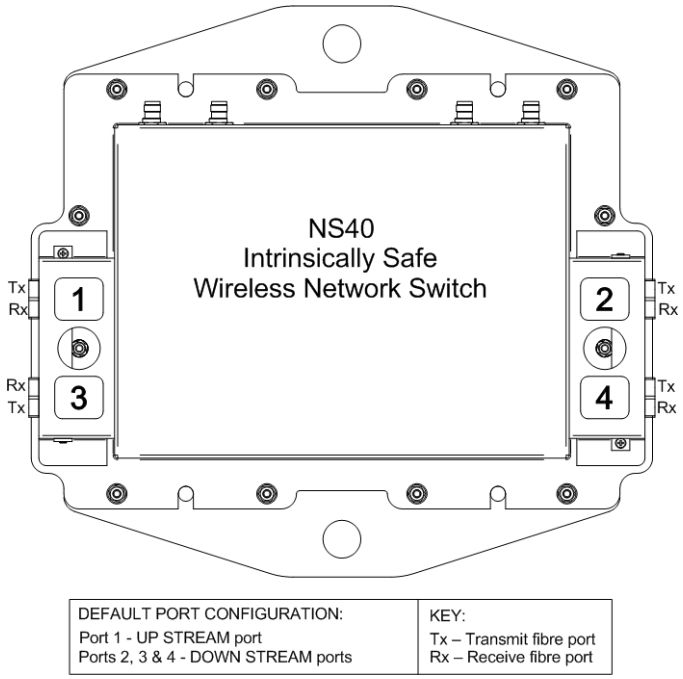
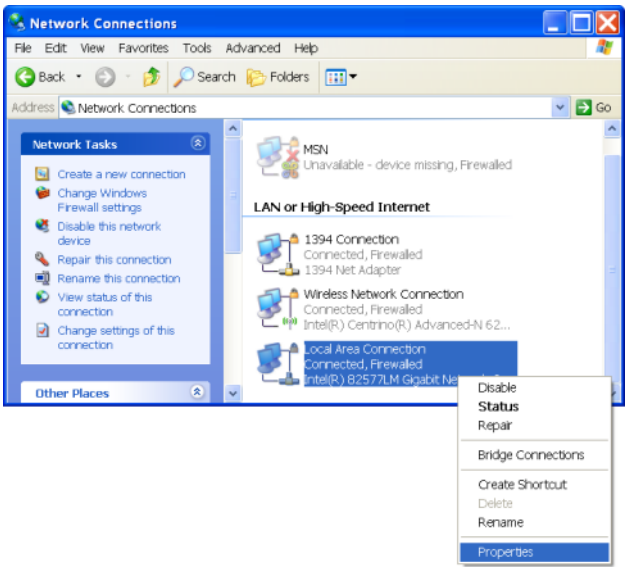


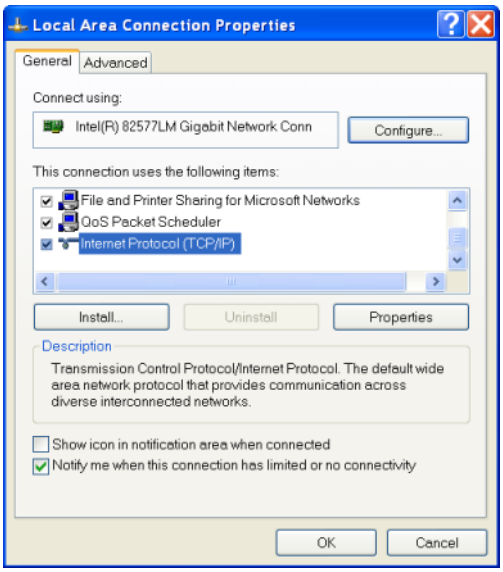
Figure 41: NS40 Fibre port wiring configuration

Procedure

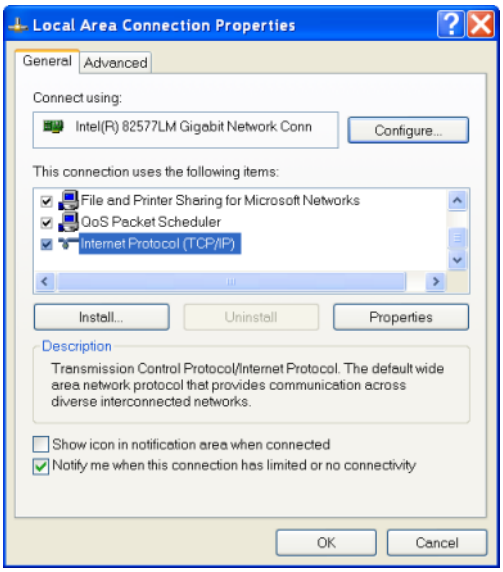
1. Connect a PC to an NS40 as described above. If the PC is already part of the network, note its TCP/IP configuration settings.
2. Click **Start** > **Control Panel**. Open **Network Connections**.



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



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.



5. Click the **Use the following IP address** option button.
6. In IP address field enter a fixed (static) IP address within range of the NS40 IP address (for example **192.168.1.100**).
7. In the Subnet mask field, enter **255.255.255.0**. Click **Ok**.

Appendix
E

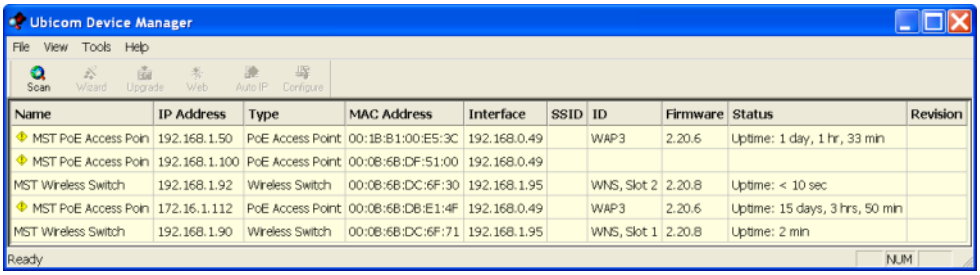
Discovering Devices on the Network

The Ubicom Device Manager is a PC software application used to detect devices and configure their IP addresses. It is used when firmware upgrades on NS40 units have reset default IP settings. The tool should be run on a PC connected on the same network segment as the device.

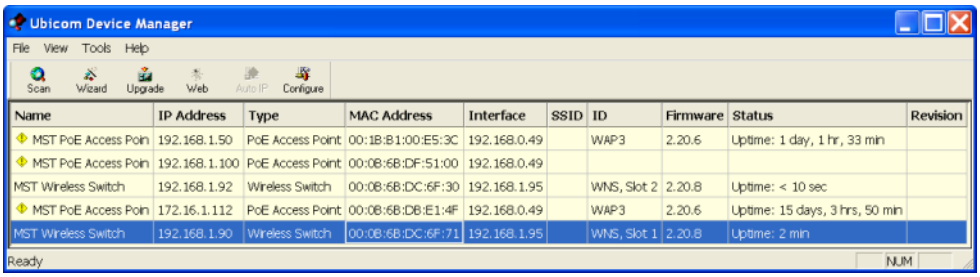
Note: The management CPU in an NS40 responds to the Device Manager tool. A PC running the tool must be on the Infrastructure VLAN.

To use the Device Manager to discover / configure device IP settings:

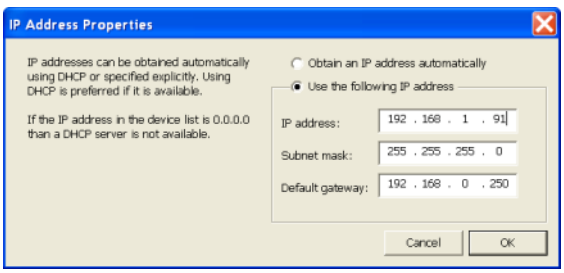
1. Locate and open the folder on your PC where the Device Manager tool is located.
2. Double-click the UbiDevman icon to launch.



3. The **Ubicom Device Manager** window is displayed and an automatic scan is initiated. Click the **Scan** icon at any time to re-scan the network for devices.



4. Note the MAC address to identify the network device to edit, and click on the row to highlight it.
5. Click on the **Configure** icon. The **IP Address Properties** dialog box is displayed.



6. Select the **Use the following IP address** option button and fill in the IP address, Subnet mask and Default settings.
7. Click **OK** to close the dialog box and save changes. The **Device Manager** will rescan devices on the network.
8. Select **File** menu and **Exit** or click [**X**] to close the **Device Manager** tool.

Note:

UbiDevman keeps running in the background after it is closed on PC's with Windows Vista and 7 operating systems. Shut it down from the **Windows Task Manager** before running it again.

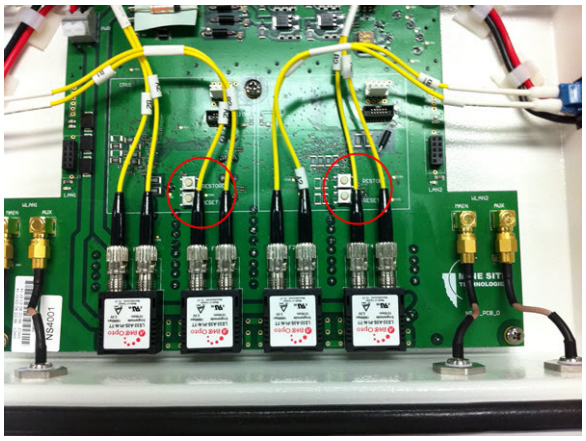
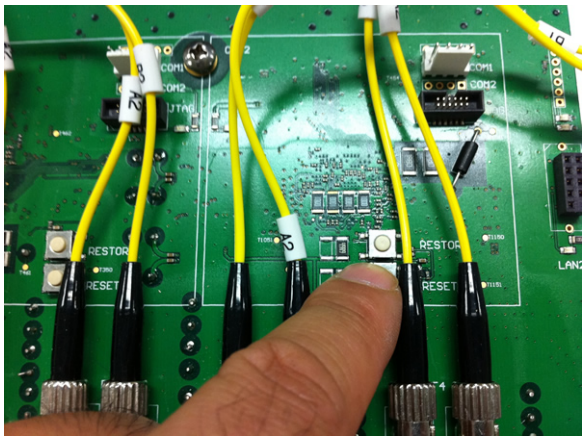
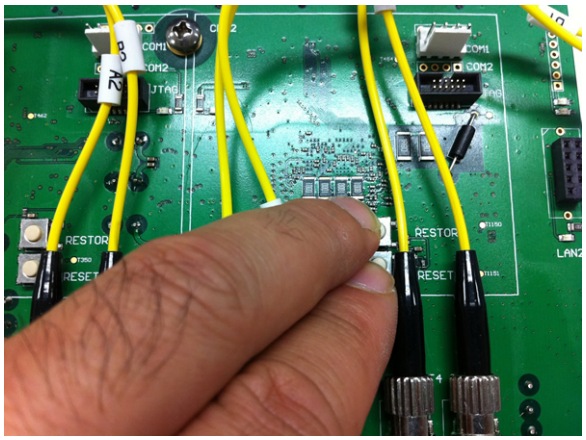
Appendix
F

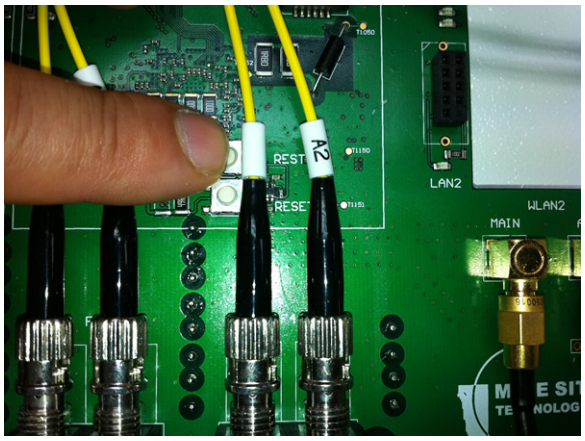
I.S. Wireless Network Switch Reset and Reboot

This appendix describes rebooting the NS40 and resetting to factory default settings. It can also be carried out using the web browser interface.

Important: The NS40 is designed to meet Intrinsic Safety requirements. Opening the NS40 in hazardous environments is a breach of Intrinsic Safety and will void the warranty. Please consult your MST System Engineer first before opening a NS40.

Step	Procedure	Picture
1	Insert an Allen key (0.125" or 3.18mm hex driver) to remove the hex screw and pull out the retention arm.	
2	Remove the nuts with a 5/16" socket wrench.	
3	Remove the two security nuts (between the composite fibre ports) with a socket wrench and remove lid.	

Step	Procedure	Picture
4	Remove lid and place upside down, locating the **RESET** and **RESTORE** buttons on the PCB.	
5	To reboot the NS40, press **RESET** whilst it is powered. Repeat the process for the other CPU.	
6	To restore to factory default settings: • Hold **RESTORE** and press **RESET** whilst the NS40 is powered. • Alternatively if the device is not powered, hold **RESTORE** and apply power. Repeat the process for the other CPU.	

Step	Procedure	Picture
7	To turn the Management port on and off, press **RESTORE** whilst the NS40 is powered.	
8	Put the lid back on the NS40, applying Loctite 222 thread lock to all screw threads before reattaching nuts and securing the retention arms.	

Appendix G

I.S. Wireless Network Switch Specifications

General

Dimensions	410mm x 380mm x 80mm
Enclosure Ingress Protection (IP) rating	IP65 (Powdercoated stainless steel enclosure)
Operating Temperature	0ºC to 40ºC
Maximum Operating Humidity	90%

Power

Maximum supply voltage	15.1VDC
Maximum input current	1.5A DC
Protection	Ex ia Group 1

Composite Fibre Ports

Composite fibre ports	4 x 100BASE-FX single mode transceivers
Connector Ingress Protection (IP) Rating	IP65

Network Information

Network architecture	Access Point, client and WDS mode
Network protocol	IEEE 802.3, 802.3u, 802.3x 802.1Q Automatic 802.1p priority based on 802.1Q VLAN ID
Redundancy	Rapid Spanning Tree Protocol

Wireless Radio

Wireless radio ports	2 x IEEE 802.11 b/g wireless access ports
Standards Compliance	IEEE 802.11b (up to 11Mbps) IEEE 802.11g (up to 54Mbps) IEEE 802.11i (security – WPA2) IEEE 802.11e (QoS – WMM)

	AeroScout Compatible
Wi-Fi security	64/128-bit WEP, WPA-PSK, WPA2-PSK, WPA- Enterprise, WPA2-Enterprise, Radius with 802.1x , MAC Address Filtering Block SSID Broadcast
Radio data rate	54, 48, 36, 24, 18, 12, 11, 9, 6, 5.5, 2 and 1 Mbps, Auto Fall-Back
Compatibility	Fully inter-operable with 802.11b/g compliant products
Frequency band	2.4 – 2.4835 GHz
Wireless Modulation	CCK (802.11b) DSSS / OFDM (802.11g)
Operation channels	1, 6, 11
Transmit power	Maximum approved 24dBm (251mW)
Receive sensitivity	1 Mbps: -95dBm (802.11b) 11 Mbps: -90dBm (802.11b) 5 Mbps: -90dBm (802.11g) 54 Mbps: -74dBm (802.11g)

Certifications

International Electrotechnical Commission (IEC)	Ex ia — IECEx TSA 10.0022X
Mining Safety and Health Administration (MSHA)	Ex ia — 23-A100003-0 (Group 1 for coal mining environment)

Appendix
H

Maintenance Checklist

It is recommended that a visual inspection of all NS40s, antennas, cables and connectors are carried out at regular intervals. A maintenance checklist is provided below.

Inspection	Action
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.
	Check there is no damage to the decal on the enclosure
Composite cables	Check all composite cables are connected and secure.
	Check the composite connector retention arm is secured to the enclosure.
	Check dust covers are on all unused composite fibre ports.
Power Supply	Check power supply as per manufacturer's recommendations.
Coaxial cables	Check coaxial cable connections are securely fastened and properly insulated to the NS40.
	Check the coaxial cable for any damage.
	Check the coaxial cable run has no kinks.
Antennas	Check the antennas for any damage.
	Check all antenna connections are properly insulated with connector covers or amalgamated rubber tape.
	Check the antennas' connections to the antenna cable.
	Check the antennas' directional alignment.
Display LEDs	Check the power LED is lit green.
	Check the status LED is blinking green (at approximately a 1 second interval).

If faults are found, please refer to maintenance procedures or consult your MST Support Engineer.

Appendix I

MSHA and IEC Approvals

Table 1: I.S. Wireless Network Switch

Mining Safety and Health Administration (MSHA)	Certification: Ex ia — 23-A100003-0 (Group 1 for coal mining environment)
International Electrotechnical Commission (IEC)	Certification: Ex ia — IECEx TSA 10.0022X
IEC Entities	Input Parameters Ui = 15.1V Ii = 1.5A Ci = 5uF Li = 0uH
	RF Output Parameters Po = 251mW Uo = 4.67v Io = 10A Co = 5uF Lo = 5.9uH
	Optical Output Parameters Po = 0.158mW

Table 2: JB10 and JB11 Junction Box

Mining Safety and Health Administration (MSHA)	Certification: Ex ia — 23-A100003-0 (Group 1 for coal mining environment)
International Electrotechnical Commission (IEC)	Certification: Ex ia — IECEx TSA 10.0022X
IEC Entities	Input Parameters Ui = 15.1V Ii = 1.5A Ci = 5uF Li = 0uH
	Optical Output Parameters P = 0.158mW

Symbol	Term	Definition
U_i	Maximum input voltage	Maximum voltage (peak AC or DC) that can be applied to the connection facilities of the apparatus without invalidating the type of protection.
I_i	Maximum input current	Maximum current (peak AC or DC) that can be applied to the connection facilities of the apparatus without invalidating the type of protection.
C_i	Maximum internal capacitance	Maximum equivalent internal capacitance of the apparatus which is considered as appearing at the connection facilities.
L_i	Maximum internal inductance	Maximum equivalent internal capacitance of the apparatus which is considered as appearing across the connection facilities.
P	Maximum output power	Maximum electrical power that can be taken from the apparatus.
U	Maximum output voltage	Maximum voltage (peak AC or DC) that can appear at the connection facilities of the apparatus at any applied voltage up to the maximum voltage.
I	Maximum output current	Maximum current (peak AC or DC) in apparatus which is considered as appearing at the connection facilities.
C	Maximum external capacitance	Maximum capacitance that can be connected to the connection facilities of the apparatus without invalidating the type of protection.
L	Maximum external inductance	Maximum value of inductance that can be connected to the connection facilities of the apparatus without invalidating the type of protection.

Appendix
J

Warranty and License Agreement

J.1 Hardware Warranty

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

Mine Site Technologies 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 Mine Site Technologies. Mine Site Technologies may in its sole discretion replace the defective hardware (or any part thereof) with a reconditioned product or parts that Mine Site Technologies 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 Mine Site Technologies shall become the property of Mine Site Technologies upon replacement.

J.2 Software End User License Agreement

IMPORTANT: PLEASE READ CAREFULLY BEFORE USING THIS EQUIPMENT.

Mine Site Technologies End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Mine Site Technologies. Mine Site Technologies (MST) firmware may include associated software components, media, printed materials and electronic documentation. By installing, copying or otherwise using MST firmware, you agree to be bound by the terms of this EULA. This license agreement represents the entire agreement concerning the program between you and Mine Site Technologies, and it supersedes any prior proposal, representation or understanding between the parties. If you do not agree to the terms of this EULA, do not install or use the software.

1. GRANT OF LICENSE

The MST firmware is licensed as follows:

(a) Installation and Use

Mine Site Technologies grants you the right to install and use copies of the MST firmware on associated MST hardware.

(b) Backup Copies

You may also make copies of the MST firmware if necessary for backup and archival purposes.

2. DESCRIPTION OF OTHER RIGHTS AND LIMITATIONS

(a) Maintenance of Copyright Notices

You must not remove or alter any copyright notices on any and all copies of the MST firmware.

(b) Distribution

You may not distribute copies of MST firmware to third parties.

(c) Prohibition on Reverse Engineering, Decompilation, and Disassembly

You may not reverse engineer, decompile, or disassemble the MST firmware.

(d) Rental

You may not rent, lease, or lend MST firmware.

(e) Support Services

Mine Site Technologies may provide you with support services related to the MST firmware. Any supplemental activation codes provided to you shall be considered part of the MST firmware and subject to the terms and conditions of this EULA.

(f) Compliance with Applicable Laws

You must comply with all applicable laws regarding use of the MST firmware.

3. TERMINATION

Without prejudice to any other rights, Mine Site Technologies may terminate this EULA if you fail to comply with the terms and conditions of this EULA. In such event, you must destroy all copies of the MST firmware in your possession.

4. COPYRIGHT

All title, including but not limited to copyrights, in and to the MST firmware and any copies thereof are owned by Mine Site Technologies. All title and intellectual property rights in and to the content which may be accessed through use of the MST firmware is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants you no rights to use such content. All rights not expressly granted are reserved by Mine Site Technologies.

5. NO WARRANTIES

Mine Site Technologies disclaims any warranty for the MST firmware. The MST firmware is provided 'as is' without any warranty of any kind, including but not limited to any warranties of merchantability, non-infringement, or fitness fora particular purpose. Mine Site Technologies does not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained within the MST firmware. Mine Site Technologies makes no warranties respecting any harm that may be caused by the transmission of a computer virus, worm, time bomb, logic bomb, or other such computer program. Mine Site Technologies disclaims any warranty or representation to authorised users or to any third party.

6. LIMITATION OF LIABILITY

In no event shall Mine Site Technologies be liable for any damages (including, without limitation, lost profits, business interruption, or lost information) rising out of 'authorised users' use of or inability to use the MST firmware, even if Mine Site Technologies has been advised of the possibility of such damages. In no event will Mine Site Technologies be liable for loss of data or for indirect, special, incidental, consequential (including lost profit), or other damages based in contract, tort or otherwise. Mine Site Technologies shall have no liability with respect to the content of the MST firmware or any part thereof, including but not limited to errors or omissions contained therein, libel, infringements of rights of publicity,

privacy, trademark rights, business interruption, personal injury, loss of privacy, moral rights or the disclosure of confidential information.

Index

P

R

S

T

U

V

W

Y