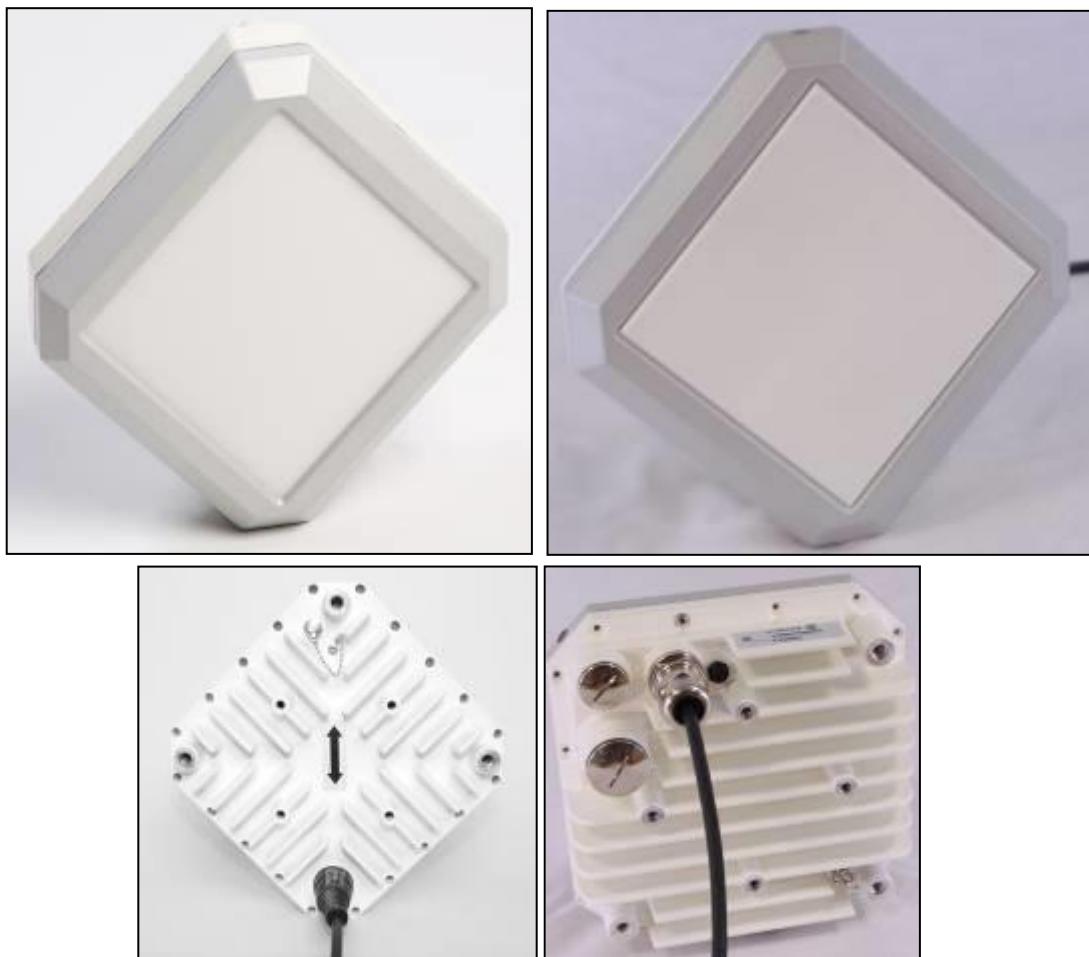


Liberator-V1000

Single-port and Dual-port Installation & User Manual

Revision 04v05
Firmware – v02.01.04.05



Fastback Networks - 2460 N First St., Suite 200, San Jose, CA 95131 U.S.A.
Sub10 Systems Ltd. - Ash House, Canal Way, Kingsteignton, Newton Abbot, Devon, TQ12 3RZ, UK

Document Type	User Manual
Project	Liberator-V1000
Title	V1000 Installation & User Manual
Document Number	FBN-0125_04v05

Version	Date	Description
04v05	21 Dec 2015	Release 02.01.04.05

Purpose & Applicability of This User Manual

This User Manual provides detailed information related to installation and operation of the Liberator V1000 Single-port and Dual-port radios and associated equipment.

Special Considerations and Safety Warnings

Prior to installing and operating this equipment, read all instructions and warning notices marked on the equipment or in accompanying documentation.

Do not attempt to apply power to equipment that shows signs of damage, tampering, or mishandling.

Do not open the equipment or attempt to repair or modify it. Doing so will void the warranty and might create a safety hazard and/or cause the equipment to be out of compliance with regulations.

This equipment should be installed, operated, and serviced only by qualified personnel and in a location where access is restricted to authorized service personnel.

Installation and operation of this equipment should be in compliance with applicable national and local codes.

Ensure that this equipment is grounded at all times in accordance with local codes.

WARNING! Class 1 Laser Product

The Dual-port version of this product may optionally be equipped with small form-factor pluggable (SFP) fibre-optic transceiver connectors for external connection of fibre-optic data cables. Active fibre-optic cables emit radiation invisible to the human eye. **Do not look directly at the end of an active fibre-optic cable or a fibre connector on this product.**

Table of Contents

Purpose & Applicability of This User Manual	3
Special Considerations and Safety Warnings	3
WARNING! Class 1 Laser Product	3
Table of Contents	4
1. INTRODUCTION	6
1.1 Revision	6
1.2 Intended Users & Software Version.....	6
1.3 Safety Information.....	6
1.4 Warranty	7
2. SYSTEM OVERVIEW	8
2.1 Top Level Description	8
2.2 Ethernet Switch.....	10
2.3 Package Contents	11
2.4 Accessories and Spares (<i>available to order as additional parts</i>)	14
3. SITE PLANNING	16
3.1 Terminal Location.....	16
3.2 Line of Sight.....	16
3.3 Link Distance / Link Availability.....	17
3.4 Terminal Mounting Options.....	17
3.5 Lightning Protection Zones	17
3.6 Cabling.....	18
3.7 Co-located Applications	18
4. Installation	19
4.1 Wall Mounts & Mast Mounts.....	19
4.2 Terminal Installation.....	19
4.3 Grounding.....	21
4.4 Cable Installation	21
4.5 Power Injector	22
4.6 Antenna Alignment.....	22
4.7 Factory-Defaulting a Terminal.....	26
4.8 Maintenance.....	27
5. Web Management Interface	28
5.1 Login Page.....	28
5.2 Home Page	29
5.3 Operation.....	30
5.4 Administration	37
5.5 Maintenance.....	65
5.6 Logout.....	72
5.7 Configuration Rollbacks	73
6. SNMP Management Interface	75
6.1 Description of SNMP.....	75
6.2 Administration Management – SNMP – Basic SNMP scripts	76
Appendix A - Technical Information	78
A 1. Troubleshooting	78
1.1 Power and Network Connection.....	78
1.2 Network Configuration	78
1.3 Misalignment	78
1.4 Mixed radio terminals.....	78
1.5 Encryption settings.....	78
A 2. Specifications	79
2.1 Physical Size of ODU Terminal	79

2.2. General System Information - Technical Specifications for V1000:	80
2.3. RSSI DC Voltage vs Received Power	81
Appendix B – Regulatory Information	82
B 1. FCC Statement	82
1.1. Regulatory Statements and Labels.....	82
1.2. Human Exposure to Non-Ionising Radiation in the USA.....	83
B 2. Industry Canada Statement	84
Appendix C – Contact Information	85

1. INTRODUCTION

1.1 Revision

Fastback Networks & Sub10 Systems reserve the right to revise this User Manual and associated documentation periodically without any obligation to provide notification of such revision or changes.

1.2 Intended Users & Software Version

This manual is intended for all installation and service personnel who are involved in the planning, installation, operation and maintenance of the Liberator-V1000 equipment. Although the Liberator-V1000 Link is designed for easy installation and setup, optimum performance can be achieved by following the procedures outlined in this manual. Use of this manual requires that the installer has at least a basic experience and understanding of networking equipment, as well as some familiarity with its configuration and operation. The information covered in this manual should be fully understood prior to installation.

This Manual refers to Liberator-V1000 running Software Version 2.1.4.x. Please ensure that the software on the radio terminals is the latest version on the Fastback Networks website:

<http://www.fastbacknetworks.com>

Please email: support@fastbacknetworks.com if you encounter any issues.

1.3 Safety Information

1.3.1 Grounding

The V1000 radio terminal (outdoor unit) must be properly grounded to protect against lightning strikes. It is the user's responsibility to ensure that the equipment is installed in accordance with national regulations:

USA: Articles 810 & 830 of the National Electric Code ANSI/NFPA No.70-1984

Canada: Section 54 of the Canadian Electrical Code

Other countries may require different regulations. It is recommended that the outdoor unit be installed by a professional installer.

1.3.2 Operation in Hostile Environments

The rated operating temperature of the radio terminal (that is, the outdoor unit or ODU), is from -40°C to +55°C. In normal operation, the radio terminal will be at a higher temperature than the ambient temperature. For safety reasons, if the ambient temperature at the location proposed for the radio terminal is likely to exceed +40°C, then the radio terminal must be mounted in a Restricted Access Location. The Restricted Access Location must only be accessible to authorised maintenance personnel through the use of a tool, lock and key or other security mechanism. The maintenance personnel must be advised that the radio terminal is hot and that safety precautions must be taken: either disconnect power from the radio terminal 1 hour before undertaking maintenance/repair, or else wear protective gloves when handling the radio terminal if power disconnection takes place less than 1 hour before access.

1.3.3 Exposure to Non-Ionising Radiation

All radio transmitters emit non-ionising radiation and have to be assessed for the potential impact of the radiation levels on Human Safety. The radio terminal and antenna should always be mounted in such a way as to prevent human exposure to radio-frequencies, by ensuring that the following minimum safety distances are observed: Safety Distance = 1 metre on boresight. The antennas MUST be positioned to ensure that a minimum separation distance of 1 metre on antenna boresight is maintained between the installer or user and the antennas. The antennas MUST be positioned to ensure that no human being could be reasonably expected to come within 1 metre of the antenna during normal operation of the radio equipment.

1.3.4 Power Supply

The Sub10 Systems PoE++ power injector should always be used to power the Liberator-V1000. If the correct power supply is not used, this may invalidate the safety certification and cause a safety hazard. The mains

power supply is the primary disconnect device for the Liberator-V1000. The installer must ensure that a mains voltage supply cable approved for the country of installation is used.

WARNING: It is strongly advised to first disconnect any network cable attached to the "IN" port of the PoE++ supply before:

- Connecting or disconnecting the PoE++ supply from the mains power
- Connecting or disconnecting the CAT5e cable between the PoE++ supply and the radio terminal (ODU).

1.3.5 Maintenance and Servicing

- Always disconnect the primary power source before undertaking maintenance/repair of the radio terminal (Outdoor Unit).
- At least once per year, each radio terminal (Outdoor Unit) must be inspected for signs of corrosion. Light corrosion is acceptable in extreme environmental conditions (marine-type deployments), but the structural integrity of the Outdoor Unit must not be in doubt. In the unlikely event that significant corrosion is seen, the radio terminal may need to be replaced: in this case, please contact Sub10 Systems for advice.

1.4 Warranty

Sub10 Systems warrants to the original end user (purchaser) that this product is free from any defects in materials or workmanship for a period of up to 24 months (2 years) from the date of shipment to the end user. During the warranty period and upon proof of purchase, should the product show indications of failure due to faulty workmanship and/or materials, Sub10 Systems will, at its discretion, repair or replace the defective products or components without charge for either parts or labor and to whatever extent it shall deem necessary to restore the product or components to full operating condition. Any replacement will consist of a new or remanufactured, functionally equivalent product of equal value, and will be offered solely at the discretion of Sub10 Systems.

This warranty shall not apply if the product is modified (e.g. warranty seal is broken), misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions. To obtain services under this warranty, contact the Sub10 Systems Service Centre. Products must be returned postage prepaid. It is recommended that the terminal be insured when shipped. Any products returned without either proof of purchase or with an outdated warranty will not be repaired or replaced. The customer will be billed for parts and labour. All repaired or replaced products will be shipped by Sub10 Systems to the corresponding return address 'postage paid'. If the customer specifies an alternative return destination where additional costs are incurred, the customer shall bear the cost of the additional return shipment cost. This warranty gives you specific legal rights, and you may also have other rights that vary from country to country.

[Return to Table of Contents](#)

2. SYSTEM OVERVIEW

2.1 Top Level Description

The Liberator-V1000 system operates as a data link in the unlicensed 60 GHz band between 57 GHz and 64 GHz. The antenna radome face measures only 18cm x 18cm (7" x 7"), making it ideal for unobtrusive urban deployments.

The Liberator-V1000 is a Transparent Layer 2 Wireless Ethernet Bridge, and consists of two radio terminals. Each radio terminal is managed individually through a Web Management Interface or via the SNMP management protocol.



Figure 1 - V1000 radio terminal

2.1.1 Versions

There are two versions of the Liberator-V1000:

- The Liberator-V1000 Single-port ODU has a single Gigabit Ethernet copper interface with PoE++ powering.
- The Liberator-V1000 Dual-port ODU has an additional GigE copper interface (data only, non-powered), and also a SFP optical port: only one of these two additional data ports may be used at any one time.

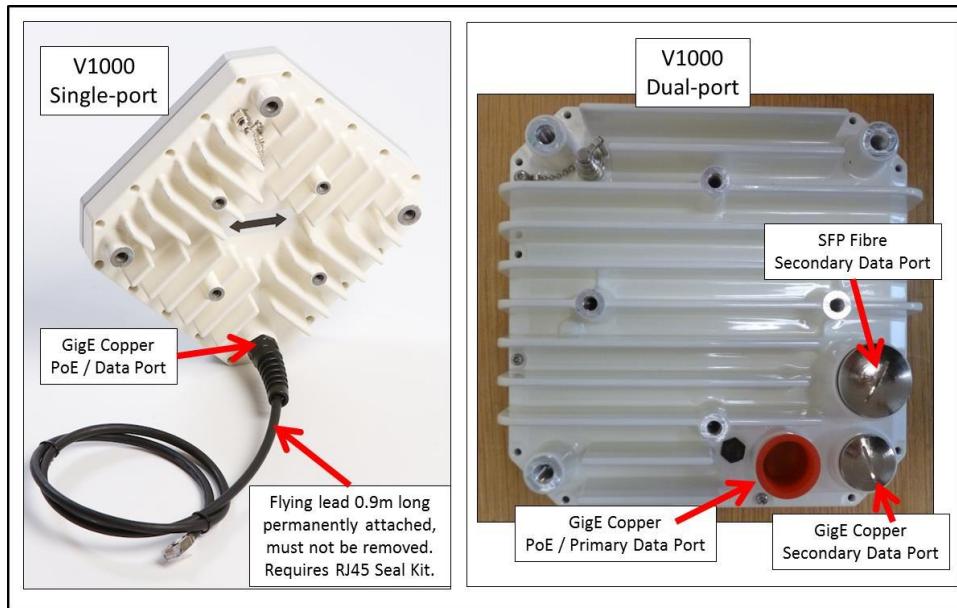


Figure 2 - Liberator-V1000 Single-port and Dual-port versions

Table of differences between Single-port and Dual-port versions of Liberator-V1000:

Feature	Single-port	Dual-port
Software version	All Software releases may be used	Only software releases from 2.1.4.1 onwards may be used
Ports	Single port (PoE & GigE combined)	Primary port: PoE & GigE combined Secondary port copper: GigE data port Secondary port SFP: Optical data port Although both secondary data ports are available on the terminal, only one of the secondary data ports may be used at a time. If both secondary data ports are connected, then the Secondary copper port will have priority and the Secondary SFP port will be inactive. It is not possible to use both secondary data ports at the same time.
RJ45 Seal Kit	Required to connect onto the flying lead.	RJ45 seal kit and rain cover / hood are not needed (not

	The supplied rain cover / hood should always be fitted over the RJ45 seal kit to prevent water ingress.	supplied). The data ports have sockets with water-proof glands instead of a flying lead.
Ice bridge	The radome requires protection from hailstones: recommend to fit standard single-port ice bridge (unless radio terminal is mounted in an exposed / windy location).	The new polycarbonate radome is resistant to hailstone damage. Dual-port ice bridge is an optional accessory. Single-port ice bridge cannot be used.
Alignment scope	Single-port terminal will accept all versions of alignment scope.	Dual-port version will only accept alignment scopes shipped from September 2015 onwards. Older versions of alignment scope are not compatible, and will require a new scope mounting bracket: please contact Fastback Networks Support.
Polarization marking	Arrows on the back of the radio terminal point either vertically or horizontally, and must be in the same orientation at both ends of the link.	Two black dots on the front of each antenna frame: these are either at the top & bottom or else at left & right of the radome, and must be in the same orientation at both ends of the link.
Frequency Channels	Supports 3 non-overlapping channels in both uplink and downlink. All combinations of uplink and downlink channels are allowed.	Supports 4 non-overlapping channels in both uplink and downlink. All combinations of uplink and downlink channels are allowed.
Timing	Basic SyncE	Full SyncE and IEEE 1588v2
Encryption	Most Single-port radios are not hardware-capable for encryption.	All Dual-port radios are hardware-capable for encryption, which is dormant. Dormant encryption can only be enabled with a software licence key, which must be purchased from Fastback Networks.
Inter-operation	A Single-port radio terminal will only make a radio link with another Single-port terminal.	A Dual-port radio terminal will only make a radio link with another Dual-port terminal.

2.1.2 Features & Benefits

- Easy installation – The concept of the Liberator-V1000 Link allows the end user to install it as easily as any other network component. The single cable solution reduces the complexity of the installation. The terminal is connected to the network, monitored and supplied with power through a single outdoor industrial-rated CAT 5e Ethernet cable, which has a solid or multi-braided screen.
- A visual alignment tool together with an alignment bracket allows the user to easily line-up the antennas. Subject to correct installation techniques being used, immediate operation without the need for additional configuration is assured.
- Network performance – Guaranteed 500Mbps, 700Mbps or 1Gbps full-duplex with Licence Key.
- V-band licence-free operation – The system has been approved and can be operated in many countries without needing an individual regulatory licence for each link. Always check in-country regulations which may vary.
- System administration – To monitor the status and the traffic, the user can access the link statistics either via the HTML user interface or by integrating it into a network management tool via SNMP.
- Security – The coding applied to the proprietary radio interface significantly restricts access to the 60 GHz transmitted data. Additionally a high level of data security is inherent in the product via signal absorption by atmospheric oxygen and the use of high gain/narrow beamwidth antennas. The Dual-port version is hardware-capable for upgrade to AES-256 encryption using a licence key.
- The Dual-port version of Liberator-V1000 allows the user to operate with a second data port (either copper or fibre).

2.1.3 Encryption

AES-256 encryption is available via Licence key upgrade, but only in countries where regulations permit, and only on units already fitted with AES-capable hardware (some Single-port and all Dual-port versions). Maximum encrypted capacity is 700Mbps full-duplex.

2.1.4 Applications

- LAN extension
- Redundant access
- Campus connectivity
- Disaster recovery
- Wireless backhaul
- Centralization of IT infrastructure
- Temporary connections during events
- Mesh, hub and spoke configuration

2.2 Ethernet Switch

Each radio terminal includes an Ethernet switch. The first switch port is connected to the physical Ethernet connection to the terminal. The second switch port is connected to the radio modem and the terminal's management agent.

The switch transparently passes all Layer 3 protocol messages. For example, the switch does not implement any kind of Spanning Tree Protocol (STP): it will simply pass all STP messages transparently over the air, but will not perform any routing of data traffic based on the Spanning Tree. This means that all incoming packets on the Ethernet interface are simply passed over the air, without taking any account of STP, and therefore the installer should ensure that there are no data loops in the system, because the switch will not detect the existence of a loop.

The single-port version of Liberator-V1000 does not support MAC address learning, but simply re-directs packets that are addressed to the management agent. All other packets are sent over the radio.

In the dual-port version of Liberator-V1000, the switch is capable of learning up to 1024 MAC addresses to switch between the 2 ports. Any packets addressed to the management agent are redirected, and all other packets are sent over the radio.

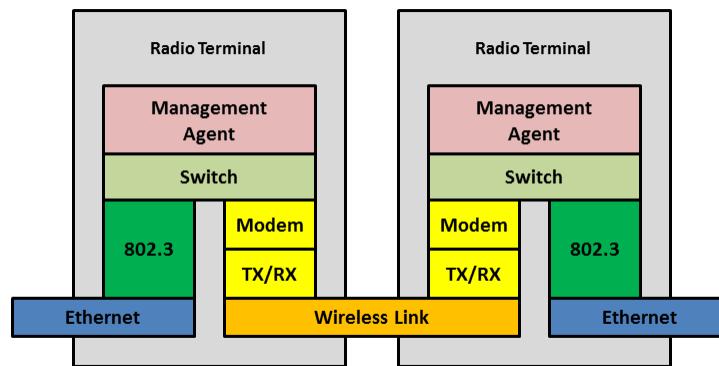


Figure 3 - Network layers of the V1000 system

2.3 Package Contents

A complete link is packed in one box. The box contains the following:

Liberator-V1000 Single-port	Liberator-V1000 Dual-port
Terminal A	Terminal A
Terminal B	Terminal B
2 x Adjustable Alignment Brackets	2 x Adjustable Alignment Brackets
2 x Fixing and Accessory Kit	2 x Fixing and Accessory Kit
1 x Quick Start Guide	1 x Quick Start Guide
2 x Ice bridges	2 x Cable glands for primary port only
2 x RJ45 Seal Kits	1 x voltmeter alignment cable
1 x voltmeter alignment cable	
2 x PoE++ mains power injectors 2 x PoE++ mains power injectors (these may not be included in all kits, please check ordering guide)	



Figure 4 – Contents of V1000 Single-port Link Kit (EU mains plug version), showing parts for one end of the link. Each V1000 Link Kit contains 2 sets of these parts (one set for each end of the link).

NOTE: - In the USA and Canada, the PoE power supply may be ordered separately from the rest of the link kit. Please check the ordering guide for more information.

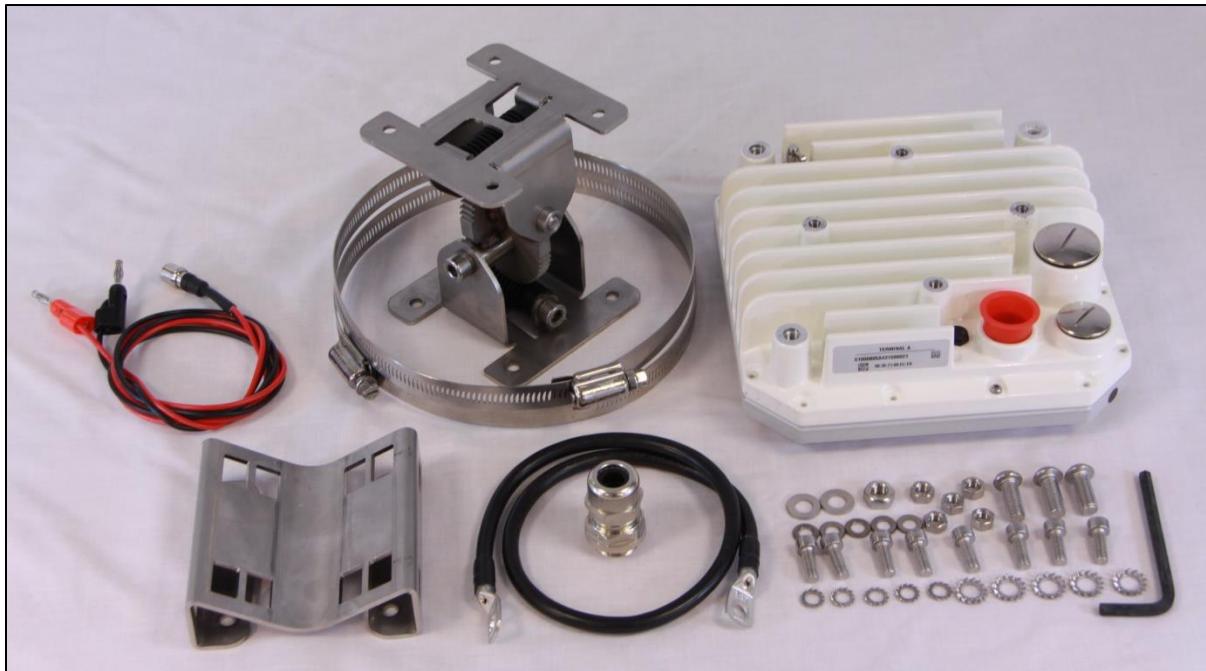


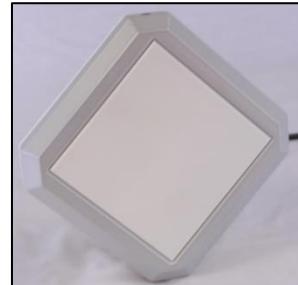
Figure 5 - Contents of V1000 Dual-port Link Kit, showing parts for one end of the link. Each V1000 Dual-port Link Kit contains 2 sets of these parts (one set for each end of the link). Please note that for the Dual-port version, the PoE++ power supply is always ordered separately, and is not included in the standard Link Kit.

2.3.1 Terminals

Each terminal combines the antenna and the transmitter and receiver. Each terminal is connected to the network via an Ethernet cable (to outdoor specification) with RJ-45 connectors. Power is supplied to the terminal through the Ethernet cable.



Figure 6 (a) V1000 Single-port Terminal



(b) V1000 Dual-port Terminal

2.3.2 Alignment Bracket

The alignment bracket facilitates easy radio alignment owing to its independent axes. It has a locking nut on each axis, so that once aligned on one axis, the alignment will not be disturbed by adjustments to the other axis.



Figure 7 – Alignment Bracket

2.3.3 PoE++ Injector

The terminal is powered via an Ethernet cable with a high-power Power-over-Ethernet power supply conforming to “Ultra-PoE” or “PoE++” specifications. It is recommended that the Sub10 Systems PoE++ power injector should always be used to power the Liberator-V1000. If the correct power supply is not used, this may invalidate the safety certification and cause a safety hazard. The mains power supply is the primary disconnect device for the Liberator-V1000. The installer must ensure that a mains voltage supply cable approved for the country of installation is used.

WARNING: It is strongly advised to first disconnect any network cable attached to the “IN” port of the PoE++ supply before:

- Connecting or disconnecting the PoE++ supply from the mains power.
- Connecting or disconnecting the CAT5e cable between the PoE++ supply and the radio terminal (ODU).

Should the network equipment connected to the Liberator-V1000 Link not offer PoE++, a power injector can be inserted in-line with the Ethernet cable.



Figure 8: (a) SL Power PENT 1040B PoE++ power injector



(b) PhiHong POE61W PoE++ power injector

2.3.4 Mast Bracket

The mast bracket is used to mount the bracket onto a mast. The bracket is suitable for any pole diameter from 50 mm to 115 mm (2” to 4.5”).

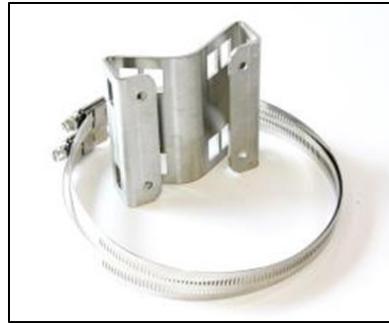


Figure 9 – Mast Bracket

2.4 Accessories and Spares (available to order as additional parts)

The parts listed in this section are not included with each link, but must be ordered separately if required.

2.4.1 Optical Alignment Tool

The optical alignment tool provided is easily mounted on the terminal using the locator pins and large thumbscrew. It enables both ends of the link to be coarsely-aligned quickly, simply and independently. Note that customers who purchased an optical alignment scope for use with Liberator V320 in the past, may find that the scope does not mount onto the V1000 back-housing. An adaptor plate is available for these early-version optical scopes, please contact your distributor, or else Sub10 Systems Customer Support.

The first version of the optical alignment tool only fits the single-port radio. The current version fits both single-port and dual-port radios. Both are shown below.



Figure 10 Optical Alignment Tools

(a) Single-port only

(b) Single & Dual-port

2.4.2 Surge Arrestor

The surge arrestor is placed between the radio head and the Ethernet cable connecting to the PoE and any other network infrastructure. This device helps to reduce the risk of damage from lightning or high-tension overhead equipment.

Note: Fastback Networks / Sub10 Systems does not supply a surge arrestor with each link, but can recommend one on request.



Figure 11 – Surge Arrestor

2.4.3 Wall-Mount Bracket

The wall-mount bracket allows the alignment bracket to be mounted directly onto a flat surface.

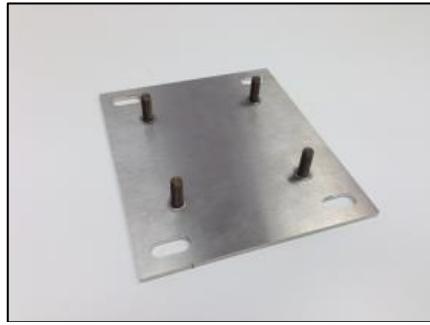


Figure 12

(a) Wall-Mount Plate (Bracket)



(b) Wall-Mount Plate with V1000 Attached

[Return to Table of Contents](#)

3. SITE PLANNING

All installers must perform a full site inspection and plan carefully prior to the physical installation of a Liberator-V1000 link.

This preparation must include:

- Evaluating the most appropriate location for the installation of the terminal.
- Identifying an appropriate mounting structure (wall or mast) for each terminal.
- Planning the cable routing from the network component to the terminal.

3.1 Terminal Location

When selecting the best terminal location the following factors should be considered:

- Accessibility (e.g. How to gain access to a roof)
- Type of mounting (e.g. wall or pole)
- Grounding connection point
- Cable runs (max. 100 m / 328 ft)
- Human safety: Exposure to Non-Ionising Radiation - The Liberator-V1000 terminal should be mounted so that it is always separated from the location of any human being by a distance of at least 1 metre.

3.2 Line of Sight

To ensure a clear line of sight (LOS), there must be no obstructions between the two terminal locations: the first Fresnel Zone should be completely clear of obstacles, see diagram below, with n=1. The required clearance can be established visually, or by using the table below which gives the worst-case clearance at the centre-point of the link. This table is valid for distances greater than about 4 metres from the radio terminal. Note that this is the minimum clearance distance with perfect antenna alignment. It is recommended to use the widest clearance distance around the LOS path as is practically possible.

Table 1 - Fresnel zone clearance for different ranges at 60GHz

Link Distance	Boundary Diameter ($2F_1$)		
100 m	328 ft	0.7 m	2.3 ft
200 m	656 ft	1.0 m	3.3 ft
400 m	1312 ft	1.4 m	4.6 ft
600 m	1968 ft	1.7 m	5.6 ft
800 m	2625 ft	2.0 m	6.6 ft
1000 m	3280 ft	2.2 m	7.3 ft

The figure below shows required clearance at close proximity to the antenna.

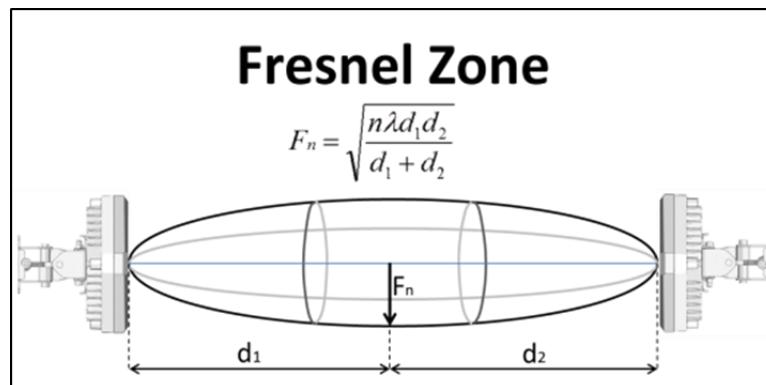


Figure 13 – Fresnel Zone Clearance at 60 GHz

3.3 Link Distance / Link Availability

The link distance is directly related to the weather conditions. Optimum link range and availability is influenced by the following environmental conditions:

- Rainfall - the lower, the better
- Oxygen absorption – This ranges between about 14 and 16 dB/km, depending on temperature and atmospheric pressure An accurate estimation of the total link distance (line of sight) is important in estimating link range and quality. *For the rain regions in your country, see appendix A.4.*

3.4 Terminal Mounting Options

3.4.1 Wall Mounting

The wall mounting location should be strong enough to secure the terminal to the wall, taking into account all foreseeable environmental conditions (e.g. wind, rain, ice).

Depending on the material to which the bracket is mounted, differently-sized mounting hardware may be necessary. To mount the terminals onto the bracket use the enclosed M6 bolts. The bracket allows a tilt angle of +/- 50° in both axes.

3.4.2 Pole Mounting

The mast mount bracket will be needed to mount the terminal onto poles with diameters from 50 mm to 115 mm (2" to 4.5").

3.5 Lightning Protection Zones

In order to protect against lightning strikes damaging the equipment, it is important to choose a mounting position for the radio terminal (ODU), which is located in a "Protected Zone". In order to determine the zone of protection against lightning strikes, the rolling sphere method is commonly-used. In this method, an imaginary sphere is rolled-over the top of the building or mast: regions underneath the lower trajectory of the sphere are in the protection zone, whilst areas above this are in danger of a lightning strike which can damage equipment and be hazardous to life. The imaginary rolling sphere can only be elevated by lightning finials, "air terminations" or adequately-grounded metallic structures, (not simply by the edge of a roof which has no earth bond). The radio terminal should always be installed in a Protected Zone.

The radius of the rolling sphere depends on the level of lightning protection required, which varies between geographical areas. See the table below for details. A commonly used value for the sphere radius is 45 metres, but this will depend on the level of protection needed.

Table 2 - Lightning Protection Levels and Sphere Radius

Lightning Protection Level	Sphere radius (m)	Interception Current (kA)
1	20	2.9
2	30	5.4
3	45	10.1
4	60	15.7

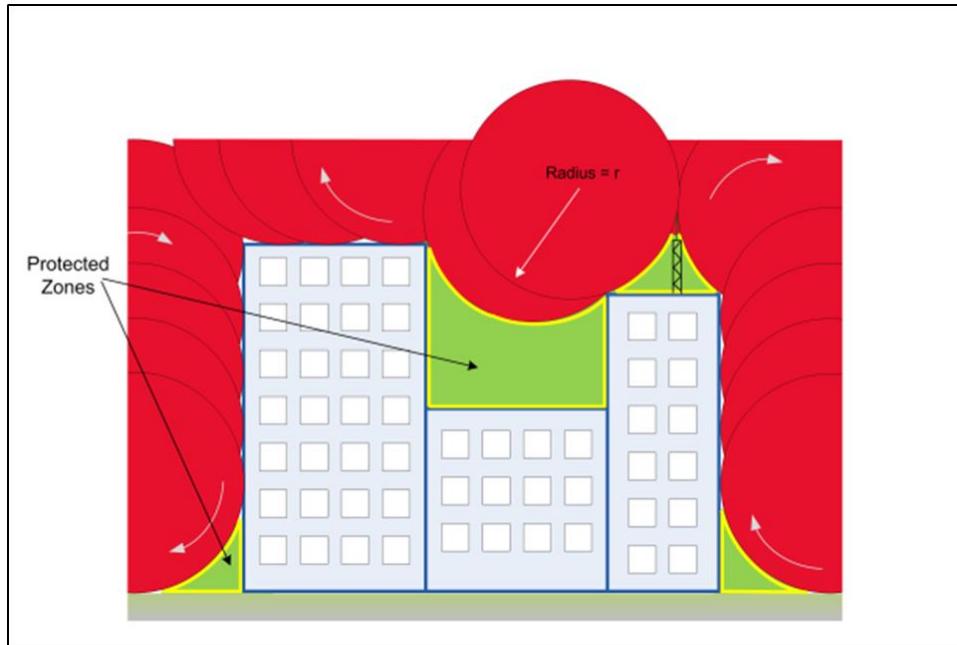


Figure 14 – Rolling Sphere Method for Determining Lightning Protection Zone

3.6 Cabling

The terminal is delivered with an Ethernet cable terminated with a RJ-45 connector. To connect the Liberator-V1000 radio terminal to your network, use a Cat 5e Ethernet cable with a maximum length of 100 metres to the next network node. The recommended cable specifications are:

- CAT5e Cable
- Outdoor Industrial Rated (includes rating for UV protection)
- Solid or Multi-Braided Screen (avoid cables with a metalised plastic foil screen)
- Screened RJ45 Connectors

Since the power is supplied by the Ethernet cable, please make sure that network equipment used supports power over Ethernet to the “Ultra PoE” or “PoE++” specification.

3.7 Co-located Applications

Owing to the compact size of the Liberator-V1000 integrated terminal, it may be used for co-sited applications (see the section titled [Co-located Terminals](#)).

[Return to Table of Contents](#)

4. Installation

Owing to the small size and integrated design of the Liberator-V1000 Link, correct installation and setup is relatively simple. When working on a roof, ladder, mast or staging, please take extreme care, observing all facility and OSHA (or other applicable regulatory agency) required safety precautions.

4.1 Wall Mounts & Mast Mounts

4.1.1 Wall Mount

The wall and mounting screws must be able to support a weight of 11 pounds (5 kg), taking into account associated wind and potential ice loading factors.

4.1.2 Mast Mount

The alignment bracket with V1000 radio terminal attached is shown below.

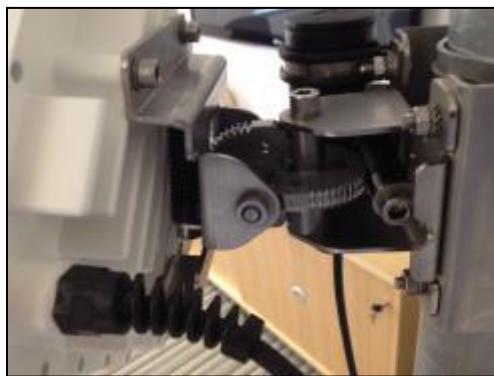


Figure 15 - Alignment bracket

- Ensure that the mast has a diameter of between 50 mm to 115 mm (2" to 4.5"), or else a collar may be required to adapt to the mast bracket.
- Fasten the mast bracket onto the mast using the enclosed stainless steel bands
- Fasten the alignment bracket onto front part of the mast bracket using the enclosed stainless steel screws, nuts and washer (M6 size screws which require a 4.5mm Allen Key tool which is included). To adjust and lock the bracket using the M8 alignment bolts, a 6mm Allen Key tool is required.

NOTE: Do not use zinc-plated screws / bolts as these will corrode and endanger link performance and safety to people and equipment.

4.2 Terminal Installation

4.2.1 Terminal Installation – Polarization

It is important to install the terminal on the bracket with the same orientation (antenna polarization) at both ends of the link. The terminals must be mounted on the brackets in such a way that the polarization arrows point in the same direction: either both ends pointing vertical, or else both ends pointing horizontal (these are actually 45 degree slant polarizations). On Single-port versions, the polarization is indicated by an arrow on the backhousing, as shown below. Note that the "A" terminal has the drop cable entry point on a different corner of the radio housing compared to the "B" terminal.

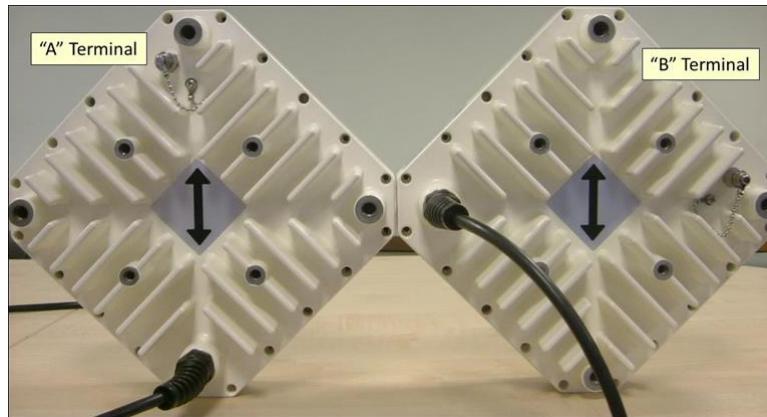


Figure 16 – V1000 Single-port Backhousing with Arrows indicating Polarization Direction

On Dual-port versions, the polarization is indicated by a pair of black dots on the front frame of the antenna face, as shown below.

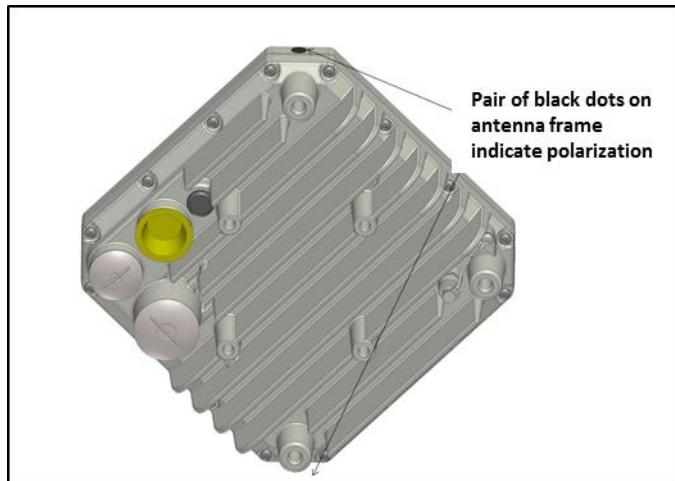


Figure 17 - V1000 Dual-port Backhousing with black dots indicating polarization direction

The terminal must be mounted on the bracket using the enclosed stainless steel screws (M6 x 12).

NOTE: Do not use zinc-plated screws as these will corrode and endanger link performance and safety to people and equipment.

4.2.2 Terminal Installation – Configuration of Co-located Terminals

If radio terminals are sited together in a cluster, configure the links to minimise interference by:

- Swapping Tx High / Low (Swap A and B terminals).
- Swapping polarization (Rotate radio terminals by 90 degrees so that arrows are swapped vertical / horizontal).
- Using different frequencies (Choose from 3 non-overlapping channels on Single-port and 4 non-overlapping channels on Dual-port).
- Physically separating the terminals by at least 1 metre.

For dense networks, especially with multiple clusters terminating on a single building, it is advisable to perform frequency planning prior to installation of the links: Fastback Networks have a planning tool to help with this, or else an industry-standard tool such as Pathloss may be used. Fastback Networks can supply Pathloss configuration files on request.

4.3 Grounding

The terminal must be properly grounded.

Two screws are provided on the rear housing of the terminal to facilitate correct grounding. To fasten the grounding cable onto the terminal, use a screw post and serrated washer combined with an M8 nut.

Connect the terminal to the connection points nearest to the building-to-earth ground point. The grounding conductor must be as short as is practical and should not exceed 6 metres (20 ft). For installations in the USA, refer to Articles 810 and 830 of the National Electrical Code. For installations in Canada, refer to Section 54 of the Canadian Electrical Code. For installations in all other countries, refer to the in-country safety standards and regulatory requirements.



Figure 18 - Grounding post on V1000 terminal

4.4 C able Installation

The length of the cable from the terminal to the next network component may be up to 100 metres (328 ft), but should be kept as short as practical in order to reduce voltage drop and signal loss. All Ethernet cables must be CAT 5e compliant and suitable for outdoor use. The cable must be UV stable and UL approved and must comply with local and/or national building codes. Cables should be shielded for outdoor use.

4.4.1 Terminating the Cat5e cable with the cable gland (Dual-port version only)

When terminating the Cat5e cable with the Dual-port version of V1000, it is important to follow the correct procedure for attaching the cable gland to the Cat5e cable.

- Attach the RJ45 plug to the Cat5e cable, with the metallic screening foil or braid section exposed, starting at 35mm from the end of the RJ45 plug, right up to 50mm from the end of the plug.

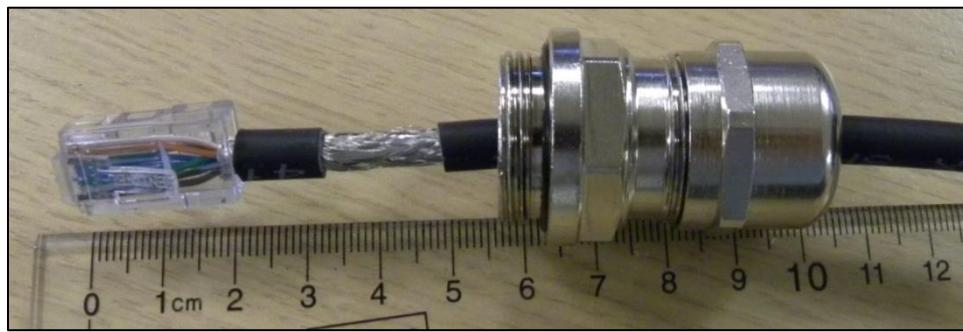


Figure 19 - Expose the cable screen starting at 35mm distance, and running up to 50mm from end of plug

- Push the RJ45 plug into the ODU socket, and make sure that it snaps into position
- Support the Cat5e cable, and gently screw the gland body into the ODU enclosure by hand, until the rubber "O"-ring is flush with the metal enclosure. Tighten the gland body with a 24mm spanner. Do NOT fit the back shell of the gland before the main body of the gland is secure.
- Once the main body of the gland is secure, then tighten the back shell of the gland onto the gland assembly, but do not over-tighten, to avoid damaging the inner seal.

4.4.2 Selecting the correct port for PoE Supply (Dual-port version only)

The Dual-port version of Liberator-V1000 has 3 ports (2 GigE copper ports, and 1 port for fibre SFP which is the largest port aperture). The PoE supply must ONLY be connected to the port marked "PoE" as shown below. The second GigE copper port cannot be used for powering, as it is for data only.

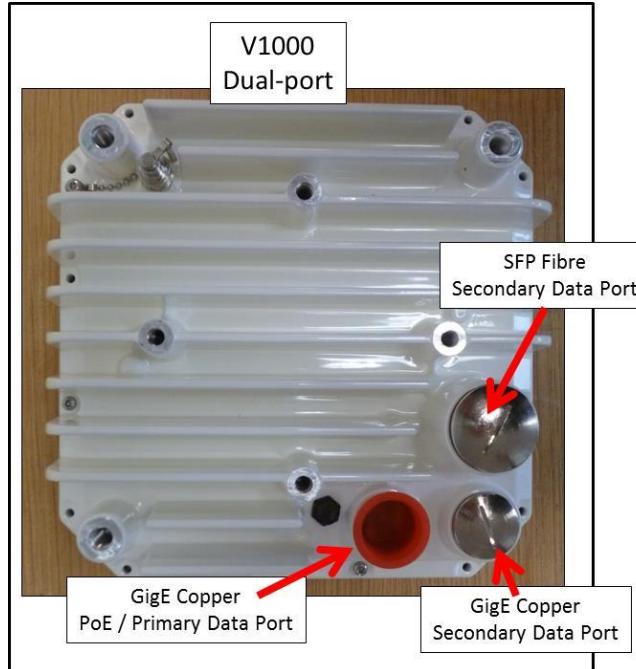


Figure 20 - Port locations on V1000 Dual-port

4.5 Power Injector

The power injector is connected in-line with the data line. The maximum distance between the PoE injector and the Liberator-V1000 Link is 100 metres (328 ft). The PoE injector must be compliant with "Ultra PoE" (PoE++). To check that the injector is functioning correctly, use a PoE Tester.

WARNING: It is strongly advised to first disconnect any network cable attached to the "IN" port of the PoE++ supply before:

- (a) Connecting or disconnecting the PoE++ supply from the mains power
- (b) Connecting or disconnecting the CAT5e cable between the PoE++ supply and the radio terminal (ODU).



Figure 21 (a) - SL Power PENT 1040B PoE++



Figure 21 (b) - PhiHong POE61W PoE++

4.6 Antenna Alignment

Accurate antenna alignment is extremely important to achieve the maximum rain fade margin for the link. One of the Liberator-V1000's biggest advantages is its fast, easy alignment procedure. The terminals can be aligned optically by using an optical alignment tool (shown below). Electrical alignment is then used to optimize performance, using a Digital Voltmeter (DVM) connected to the alignment port on the back housing of the terminal. The first version of optical alignment scope (shown in part (a) of the figure below) can be

used only with a single-port V1000. The current optical alignment scope (shown in part (b) below) can be used with single-port and dual-port V1000.



Figure 22 Optical Alignment Scopes (a) Single-port only (b) Single & Dual-port

Graphs in Appendix A give the required alignment voltage for a given RSSI value and a given range. Note that the values of alignment voltage for a given range are only average values, assume clear air conditions, and will vary slightly with geographic location. Therefore for the most accurate voltage prediction, it is strongly encouraged to use the Liberator-Predict Link Calculator, available from the Fastback Networks website.

The table below shows alignment tolerance in terms of absolute position. However, it should be noted that since all alignment is dependent on the angle subtended at the alignment bracket, the distance of the link is not a factor in determining the required tolerance on the alignment angle, which should be the same for all ranges.

Link Distance		Alignment Positional Accuracy	
100 m	328 ft	0.9 m	2.9 ft
400 m	1312 ft	3.5 m	11.5 ft
600 m	1968 ft	5.2 m	17.2 ft
800 m	2625 ft	7.0 m	22.9 ft

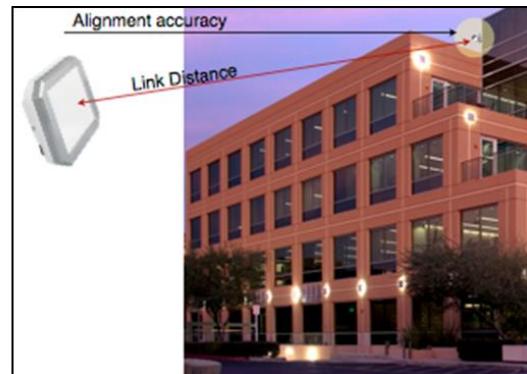


Figure 23 – Alignment Positional Accuracy

4.6.1 Alignment Procedure

The following procedure achieves fast, accurate alignment. For mounting onto the pole, the supplied 4.5 mm Allen key can be used. For fine antenna alignment, a 6mm Allen-Key / T-Bar tool is required (not included) to adjust the M8 alignment bolts.

(a) Using the Alignment Bracket

Use a 6mm Allen-Key / T-bar tool to adjust the M8 bolts on the alignment bracket in azimuth and elevation and repeat until fully aligned. Then lock-off using the M8 locking bolts for azimuth and elevation. These steps are illustrated in the figures below.



Figure 24 - (a) Horizontal (azimuth) adjustment screw



Figure 24 - (b) Vertical (elevation) adjustment screw

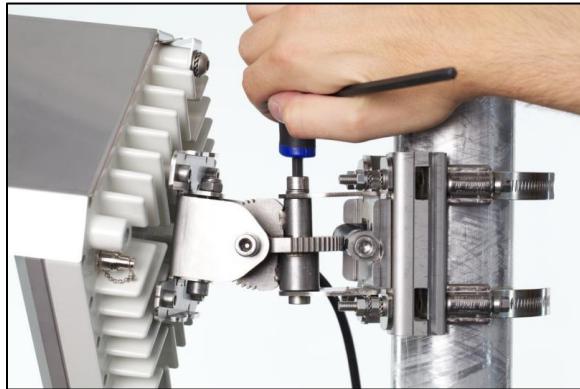


Figure 25 - (a) Locking the horizontal position

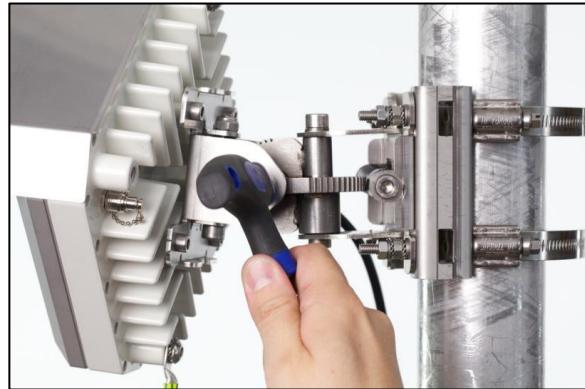


Figure 25 - (b) Locking the vertical position

(b) Optical alignment

- Place the alignment tool on the most accessible corner of the radio unit and ensure good visibility to the opposite terminal by rotating the viewfinder.
- Use a 6mm Allen-Key / T-Bar tool to orientate the bracket in to a position where the alignment scope shows the target location is in the cross hairs.
- Once this is completed correctly at both end, you will be able to measure a Voltage via the DC port (Power Level Alignment)

(c) Alignment using a voltmeter to read RSSI

Following optical alignment, an alignment based on the received power level of each terminal should be performed. Use a voltmeter and cable with a female QMA connector to attach to the QMA connector on the terminal of the procedure for optical alignment, and adjust the alignment bracket to obtain maximum voltage from each terminal.

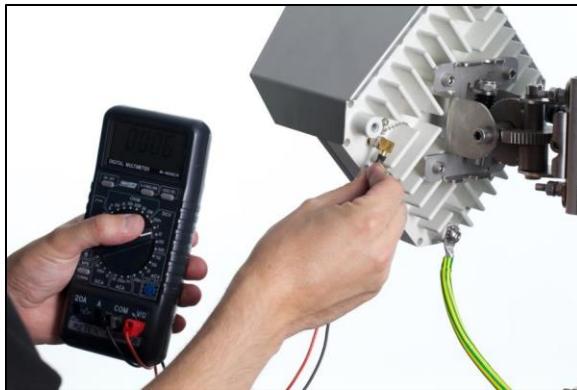


Figure 26 - Connection of a voltmeter for fine alignment on Liberator-V1000

The Alignment Interface is to allow the connection of a voltmeter during terminal installation. During installation a DC voltage between 0.5 and 4V is output, which is proportional to the receive signal strength. The higher the voltage, the higher the receive signal strength (RSSI). See Appendix A.2.3 for graphs of the RSSI voltage.

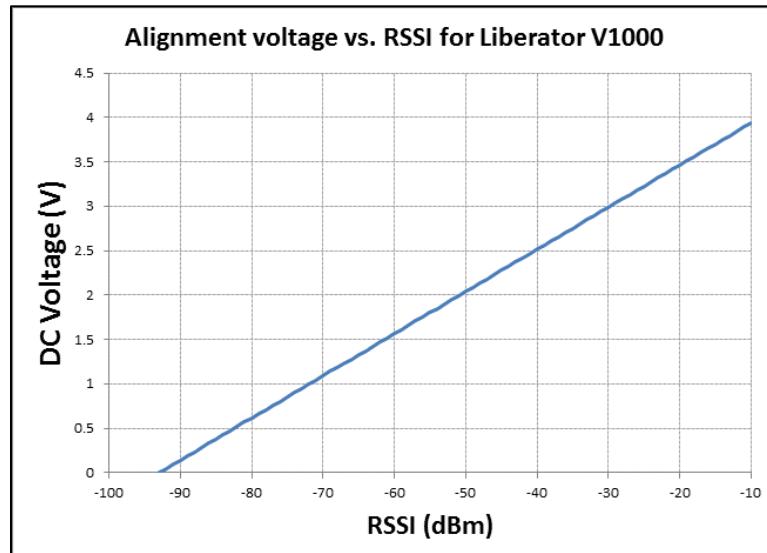


Figure 27 - Alignment voltage vs. RSSI (see Appendix A.2.3)

Follow the scanning pattern example below to find the peak voltage on the voltmeter; you must follow this pattern fully to ensure that you are not aligning on to a side lobe of the antenna. The main beam is **15 dB higher than the side lobes** and in clear line of sight is obvious when found.



Figure 28 – Scan Pattern to Use During Alignment

4.7 Factory-Defaulting a Terminal

Factory-defaulting a terminal may occasionally be necessary to regain access to the unit if the master password is lost, or if it is desired to quickly reset all GUI settings to default.

Note that any Licence Key which has been applied to the terminal will also be lost on factory default, and will need to be re-entered to re-activate the Licensed features.

- (a) The reset procedure below only functions when the terminal is in “Normal” Mode, it will not function when the terminal is in “Alignment” mode. If it is suspected that the terminal is in “Alignment” mode, and does not respond to the reset procedure, then it is necessary to ensure that it is definitely not in “Alignment” mode by either:

1. If the GUI webpage is contactable: Make sure that the alignment cap on the terminal case is closed. Browse to the “Home – Administration – Installation” page on the GUI, and if necessary click on “Change Mode” if the display is showing “Alignment mode”. The terminal should now be in “Normal Mode”, and this should be displayed on the GUI webpage.
2. If the GUI webpage is not contactable: Make sure that the alignment cap on the terminal case is closed. Power cycle the radio terminal, and it should now restart in “Normal Mode” if the alignment cap is already closed when the power is re-applied.

- (b) When it is certain that the radio terminal is in “Normal Mode” (and not “Alignment Mode”), then the following procedure can be used to restore the radio terminal to factory default settings:

Short-out the Alignment interface and then remove and re-apply the short four times with 1 second mark space ratio, as shown below. Shorting-out the alignment port can be achieved either by using the protective Alignment Cap fitted, as this acts as an electrical short-circuit when closed, or else by shorting-out the plugs on the voltmeter alignment cable used for installation. If the radio terminal does not reset itself, it may be that the sequence was counted either too slowly or too quickly: there needs to be 1 second between each short-circuit or open-circuit change, as shown in the timing diagram.

- (c) Note that if the Alignment Cap is disconnected for a period of more than 30 seconds, then the radio terminal will automatically switch into “Alignment Mode”, see (a) above. Therefore it is recommended to always keep the Alignment Cap connected, except when physically aligning the link.

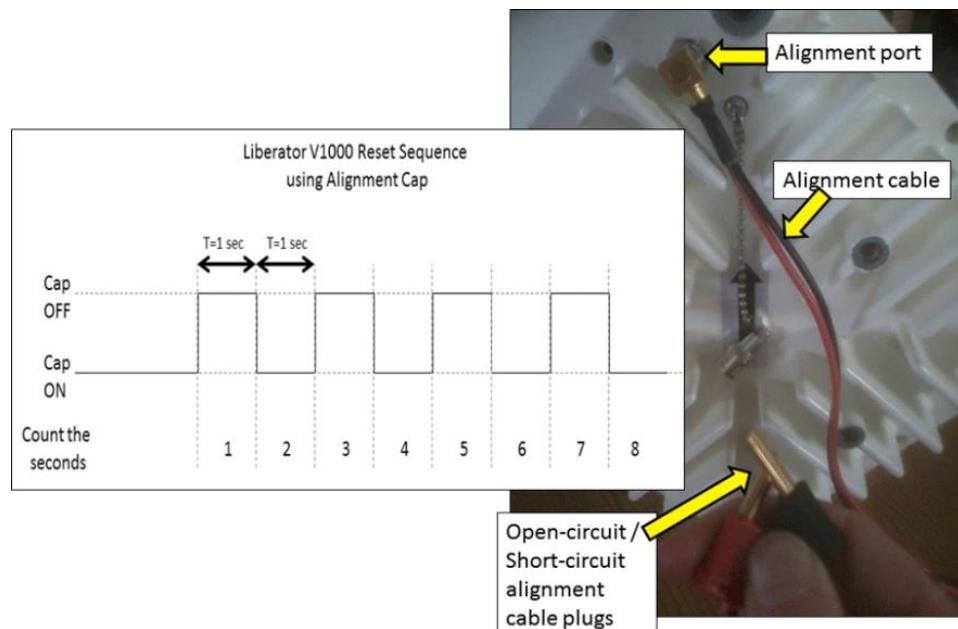


Figure 29 - Reset Sequence Using the Alignment Cap

If the IP address has been lost, then it is possible to re-discover the IP address by using a packet-sniffer tool such as Wireshark, and power-cycling the terminal with Wireshark running (always take care to have the network cable disconnected during the power cycle, and quickly re-connect it immediately after restoring power). A “Gratuitous ARP” containing the IP address will be sent from the terminal on start-up, which can be seen with Wireshark. **Please contact Fastback Networks Support for assistance with factory-defaulting a terminal.**

4.8 Maintenance

Warnings:

- Always disconnect the primary power source before undertaking maintenance/repair of the radio terminal (Outdoor Unit).
- At least once per year, each radio terminal (Outdoor Unit) must be inspected for signs of corrosion. Light corrosion is acceptable in extreme environmental conditions (marine-type deployments), but the structural integrity of the ODU must not be in doubt. In the unlikely event that significant corrosion is seen, the unit may need to be replaced: in this case, please contact Fastback Networks for advice.

[Return to Table of Contents](#)

5. Web Management Interface

Throughout this document, 2 separate screenshots for Single-port and Dual-port will only be shown if there are significant differences between them: otherwise, only one version will be shown.

5.1 Login Page

The screenshot shows the login interface for the Liberator-V1000. At the top left is the Fastback Networks logo with the tagline "intelligent wireless transport". To its right is the text "Liberator-V1000". The main area is a white rectangle containing a black rectangular background. Inside this black area, there are two input fields: "User" with the value "admin" and "Password" with the value "*****". Below these fields is a "Login" button.

Figure 30 - Login Page

The Login Page is used to control access to one or other of the radio terminals. Currently only one user account is supported. This user account has full **Maintenance-Level** privileges.

The default settings for this user account are:

Default IP address (Terminal A):	192.168.0.21
Default IP address (Terminal B):	192.168.0.22

User:	admin
Password:	password

5.2 Home Page

System Information	
Site Name	Sub10
Link Name	Test Link 15
Terminal Name	B
Transmit Modulation Mode	8PSK
Receive Modulation Mode	8PSK
Air Data Rate	1000 Mbps
Regulatory	NON-FCC

System Status	
Radio Interface	Synchronised
Radio Link	Up
Ethernet Interface 1	Up
Ethernet Interface 2	Down

Alarms	
Rx Power Low	Clear
Vector Error High	Clear
MWU Temperature High	Clear
MWU Temperature Low	Clear
Radio Link Down	Clear
Link ID Mismatch	Clear

Figure 31 - Welcome Page

After a successful login the Home Page is displayed. The first box on this page shows the Link Name, Terminal Name, Tx and Rx modulation modes (QPSK or 8PSK), Air Date Rate (either 500Mbps, 700Mbps or 1000 Mbps), and regulatory region (either "FCC" or "NON-FCC"). The second box gives a snapshot of current System Status, and also Alarms. The Status bars are highlighted in GREEN if the Radio Interface, Radio Link and Ethernet Interface are up, otherwise they will be YELLOW for acquiring a radio link, or RED for down. The alarm bars are highlighted in GREEN, YELLOW or RED depending on the status of each alarm.

Following industry standard practice, the menu on the left side of the page has 3 categories:

1. Operation
2. Administration
3. Maintenance

Users having different access privileges may be restricted to only access the Operation, or Operation and Administration pages, whilst the administrator will have full access to all pages. The default setting is a single user with full access privileges (Maintenance-Level privileges).

5.3 Operation

5.3.1 Operation - Radio – Radio Status

The Radio Status page shows the wireless parameters of the link. Parameters displayed are:

- Transmit Power: Transmit power is only displayed in dBm, but the settings available are limited to "High / Medium / Low", as in the table below:

Tx Power Setting	QPSK (700Mbps max) Nominal Average Tx Power into Antenna	8PSK (1Gbps) Nominal Average Tx Power into Antenna
High	+7.5dBm (FCC) and +6 dBm (Rest of World)	+4 dBm
Medium	+3 dBm	-1 dBm
Low	-5 dBm	-5 dBm

- RSSI (dBm): Received power at the antenna port (inside the ODU).
- Vector Error (dB): This is a measure of the signal quality, and should ideally be lower (more negative) than -10dB (the exact value may vary over time).
- MWU Temp (Celsius): This shows the operating temperature of the microwave unit inside the radio
- Air Frame Error Ratio: This shows the % error rate over the air
- Ethernet Rx / Tx (Mbps): This shows the user traffic rate on the Ethernet interface

For each parameter, the local side of the link displays values for the Minimum, Mean, Maximum and Current, while the remote side of the link only displays the Current parameter value. The values may be reset by pressing the "Reset" button (which is useful after a power outage event, for example). The refresh speed can be increased by typing in a smaller number of seconds, as desired, into the "Page Refresh Interval" box, and then pressing the "Change" button.

The screenshot shows the Liberator-V1000 Radio Status page. At the top, there's a red header bar with the Fastback Networks logo and the text "Liberator-V1000". To the right of the header, it says "Logged in as: admin (Maintenance)". Below the header, there's a navigation bar with links for Home, Operation, Radio, and Radio Status. On the left, there's a sidebar with "Radio Status" and "Logout" buttons. The main content area has two tables. The first table, titled "System Information", lists various parameters with their current values: Site Name (Sub10), Link Name (Test Link 15), Terminal Name (B), Transmit Modulation Mode (8PSK), Receive Modulation Mode (8PSK), Air Data Rate (1000 Mbps), and Regulatory (NON-FCC). The second table, titled "Parameter (units)", shows performance metrics with columns for Min, Mean, Max, Snapshot, and Remote Mean. These metrics include Transmit Power (dBm), RSSI (dBm), Vector Error (dB), MWU Temp (Celsius), Air Frame Error Ratio (%), Ethernet Rx (Mbps), and Ethernet Tx (Mbps). At the bottom of the page, there are buttons for "Reset" and "Change", and a text input field for "Page Refresh Interval" with the value "5" and a unit of "seconds".

System Information					
Site Name	Sub10				
Link Name	Test Link 15				
Terminal Name	B				
Transmit Modulation Mode	8PSK				
Receive Modulation Mode	8PSK				
Air Data Rate	1000 Mbps				
Regulatory	NON-FCC				

Parameter (units)	Min	Mean	Max	Snapshot	Remote Mean
Transmit Power (dBm)	4	4	4	4	4
RSSI (dBm)	-43.0	-43.0	-43.0	-43.0	-39.0
Vector Error (dB)	-18.5	-18.5	-18.4	-18.5	-19.0
MWU Temp (Celsius)	48	48	49	49	52
Air Frame Error Ratio (%)	0.0000	0.0000	0.0000	0.0000	0.0000
Ethernet Rx (Mbps)	0.0	0.0	0.1	0.0	0.0
Ethernet Tx (Mbps)	0.0	0.0	0.3	0.0	0.0

Elapsed Time: 02:26:11

Page Refresh Interval seconds.

Figure 32 - Radio Status Page, showing parameter values for both local and remote terminals

5.3.2 Operation - Radio – Radio Statistics

The Radio Statistics page shows the Current Statistics, 1-minute, 15-minute and 24-hour history, see the figures below. It is possible to display each of these time histories in full detail for a selected parameter, and there is a button to allow export of the statistics to a CSV file if desired.

System Information				
Site Name	Sub10			
Link Name	Test Link 15			
Terminal Name	B			
Transmit Modulation Mode	8PSK			
Receive Modulation Mode	8PSK			
Air Data Rate	1000 Mbps			
Regulatory	NON-FCC			

Stat Name	Current	Latest 1m History	Latest 15m History	Last Available 24h History
RxPowerMin	-43.0	-43.0	-43.0	-67.0
RxPowerMax	-43.0	-43.0	-43.0	-67.0
RxPowerAvg	-43.0	-43.0	-43.0	-67.0
TxPowerMin	4	4	4	10
TxPowerMax	4	4	4	10
TxPowerAvg	4	4	4	10
VectErrMin	-18.5	-18.5	-18.5	-2.1
VectErrMax	-18.4	-18.4	-18.4	-1.7
VectErrAvg	-18.5	-18.4	-18.5	-1.9
MWUTempMin	49	48	48	36
MWUTempMax	49	49	49	42
MWUTempAvg	49	48	48	38
RxPkts	41444	287	4380	0
TxPkts	46021	312	4854	0
RxMgtPkts	41120	287	4224	0
TxMgtPkts	41263	282	4231	32
QPSKTo8PSK	1	0	0	0
8PSKToQPSK	0	0	0	0
RxQPSKTime	11	0	0	0
Rx8PSKTime	8730	60	900	0
TxQPSKTime	15	0	0	0
Tx8PSKTime	8726	60	900	0
AFERMin	0.0000	0.0000	0.0000	50.7545
AFERMax	0.0000	0.0000	0.0000	100.0000
AFERAvg	0.0000	0.0000	0.0000	97.8976

Figure 33 - Radio Statistics

System Information			
Site Name	Ash House		
Link Name	Test Link 11		
Terminal Name	B		
Transmit Modulation Mode	8PSK		
Receive Modulation Mode	8PSK		
Air Data Rate	1000 Mbps		
Regulatory	NON-FCC		

Stats 1 Minute Interval History		
Interval	Interval Time (End)	RxPowerMin
1	2015-03-26 18:08:00	-37.5
2	2015-03-26 18:07:00	-37.5
3	2015-03-26 18:06:00	-37.5
4	2015-03-26 18:05:00	-37.5
5	2015-03-26 18:04:00	-37.5
6	2015-03-26 18:03:00	-37.5
7	2015-03-26 18:02:00	-37.5
8	2015-03-26 18:01:00	-37.5
9	2015-03-26 18:00:00	-37.5
10	2015-03-26 17:59:00	-37.5
11	2015-03-26 17:58:00	-37.5
12	2015-03-26 17:57:00	-37.5
13	2015-03-26 17:56:00	-37.5
14	2015-03-26 17:55:00	-37.4
15	2015-03-26 17:54:00	-37.4
16	2015-03-26 17:53:00	-37.4
17	2015-03-26 17:52:00	-37.4
18	2015-03-26 17:51:00	-37.4
19	2015-03-26 17:50:00	-37.5
20	2015-03-26 17:49:00	-37.4
21	2015-03-26 17:48:00	-37.4
22	2015-03-26 17:47:00	-37.4
23	2015-03-26 17:46:00	-37.4
24	2015-03-26 17:45:00	-37.4
25	2015-03-26 17:44:00	-37.5
26	2015-03-26 17:43:00	-37.4
27	2015-03-26 17:42:00	-37.4
28	2015-03-26 17:41:00	-37.4
29	2015-03-26 17:40:00	-37.4
30	2015-03-26 17:39:00	-37.4
31	2015-03-26 17:38:00	-37.4
32	2015-03-26 17:37:00	-38.7

[Export CSV](#)

Figure 34 – One Minute History for RxPowerMin

5.3.3 Operation - Ethernet – Ethernet Status

The Ethernet Status page shows the Ethernet port parameters. By default a radio terminal's Ethernet interface is set to auto-negotiate the Ethernet type and rate. This page indicates the Ethernet line-rate, whether it is active or not, and the auto-negotiation setting. The remote port parameters are also shown, and if there is no Ethernet connected on the remote port, then these will all be red: this is a useful troubleshooting tool, which shows that the remote terminal has no network connection.

The screenshot shows the Liberator-V1000 Ethernet Status page. At the top, there's a header with the Fastback Networks logo and the device name "Liberator-V1000". On the right, it says "Logged in as: admin (Maintenance)". Below the header, there's a navigation bar with links for Home, Operation, Ethernet, and Ethernet Status. A sidebar on the left has "Ethernet Status" and "Logout" buttons.

System Information		
Site Name	Sub10	
Link Name	Test Link 15	
Terminal Name	B	
Transmit Modulation Mode	8PSK	
Receive Modulation Mode	8PSK	
Air Data Rate	1000 Mbps	
Regulatory	NON-FCC	

Ethernet Interface 1	Local	Remote
Link Status	Up	Up
Speed	1000 Mbps	1000 Mbps
Duplex	Full	Full
MDI/MDIX	MDI	MDI
Media	Copper	Copper

Ethernet Interface 2	Local	Remote
Link Status	Up	Down
Speed	1000 Mbps	Unknown
Duplex	Full	Unknown
MDI/MDIX	MDI	Unknown
Media	Copper	Unknown

Figure 35 - Ethernet Status Page

5.3.4 Operation - Ethernet – Ethernet Statistics

The Ethernet Statistics page shows the Current Statistics, 1-minute, 15-minute and 24-hour history. It is possible to display each of these time histories in full detail for a selected parameter.

Ethernet Stats				
System Information				
Site Name				Sub10
Link Name				Test Link 15
Terminal Name				B
Transmit Modulation Mode				8PSK
Receive Modulation Mode				8PSK
Air Data Rate				1000 Mbps
Regulatory				NON-FCC
Stats Current and Latest History				
Stat Name	Current	Latest 1m History	Latest 15m History	Last Available 24h History
RxOctets	1468361	19318	149113	--
RxGoodFrms	15614	172	1572	--
RxBcastFrms	4675	37	450	--
RxMcastFrms	164	18	0	--
RxPauseFrms	0	0	0	--
RxCRCERrs	0	0	0	--
RxAlignErrs	0	0	0	--
RxOversized	0	0	0	--
RxJabberFrms	0	0	0	--
RxUndersized	0	0	0	--
RxFragments	0	0	0	--
RxSOFOvrns	0	0	0	--
TxOctets	2031298	86968	223846	--
TxGoodFrms	10961	147	1102	--
TxBcastFrms	372	12	16	--
TxMcastFrms	158	18	0	--
TxPauseFrms	0	0	0	--
TxDeferred	0	0	0	--
TxCollsn	0	0	0	--
TxSnglCollsn	0	0	0	--
TxMlpCollsn	0	0	0	--
TxExsvCollsn	0	0	0	--
TxLtCollsn	0	0	0	--
TxCsenseErrs	0	0	0	--
Pkts64Octets	5006	49	482	--
Pkts65T127	19833	129	2007	--
Pkts128T255	233	39	1	--
Pkts256T511	653	36	79	--
Pkts512T1023	376	29	50	--
Pkts1024TMax	474	37	55	--
RxMbpsMin	0.0	0.0	0.0	--
RxMbpsMax	0.0	0.0	0.0	--
RxMbpsAvg	0.0	0.0	0.0	--
TxMbpsMin	0.0	0.0	0.0	--
TxMbpsMax	0.2	0.2	0.2	--
TxMbpsAvg	0.0	0.0	0.0	--

[Refresh Stats](#)

Figure 36 - Ethernet Statistics

Receive Modulation Mode	8PSK	
Air Data Rate	1000 Mbps	
Regulatory	NON-FCC	
Stats 1 Minute Interval History		
Stats History Parameter RxOctets ▾		
Interval	Interval Time (End)	RxOctets
1	2000-03-06 13:21:00	53435
2	2000-03-06 13:20:00	19318
3	2000-03-06 13:19:00	17753
4	2000-03-06 13:18:00	40499
5	2000-03-06 13:17:00	27370
6	2000-03-06 13:16:00	38726
7	2000-03-06 13:15:00	35657
8	2000-03-06 13:14:00	8206
9	2000-03-06 13:13:00	8002
10	2000-03-06 13:12:00	8104
11	2000-03-06 13:11:00	8104
12	2000-03-06 13:10:00	8104
13	2000-03-06 13:09:00	8104
14	2000-03-06 13:08:00	8104
15	2000-03-06 13:07:00	8104
16	2000-03-06 13:06:00	8104
17	2000-03-06 13:05:00	8104
18	2000-03-06 13:04:00	8104
19	2000-03-06 13:03:00	8104
20	2000-03-06 13:02:00	8104
21	2000-03-06 13:01:00	8104
22	2000-03-06 13:00:00	8002
23	2000-03-06 12:59:00	8206
24	2000-03-06 12:58:00	8002
25	2000-03-06 12:57:00	8104
26	2000-03-06 12:56:00	8104
27	2000-03-06 12:55:00	8104
28	2000-03-06 12:54:00	8104
29	2000-03-06 12:53:00	8104
30	2000-03-06 12:52:00	8104
31	2000-03-06 12:51:00	8104
32	2000-03-06 12:50:00	8104
33	2000-03-06 12:49:00	8104
34	2000-03-06 12:48:00	8104
35	2000-03-06 12:47:00	8104
36	2000-03-06 12:46:00	8104
37	2000-03-06 12:45:00	8104
38	2000-03-06 12:44:00	8104
39	2000-03-06 12:43:00	8104
40	2000-03-06 12:42:00	8104
41	2000-03-06 12:41:00	8306
42	2000-03-06 12:40:00	8002
43	2000-03-06 12:39:00	8206
44	2000-03-06 12:38:00	8002
45	2000-03-06 12:37:00	8104
46	2000-03-06 12:36:00	8104
47	2000-03-06 12:35:00	8104
48	2000-03-06 12:34:00	8104
49	2000-03-06 12:33:00	8104
50	2000-03-06 12:32:00	8104
51	2000-03-06 12:31:00	8104
52	2000-03-06 12:30:00	8104
53	2000-03-06 12:29:00	8104
54	2000-03-06 12:28:00	8104
55	2000-03-06 12:27:00	8104
56	2000-03-06 12:26:00	8104
57	2000-03-06 12:25:00	8104
58	2000-03-06 12:24:00	8104
59	2000-03-06 12:23:00	8104
60	2000-03-06 12:22:00	8002

[Export CSV](#)

Figure 37 - Ethernet Statistics – 1 minute history for RxOctets

5.3.5 Operation - System Status – System Info

The System Info page provides an overview of the radio link, both on local and remote terminals

System Information		
	Local	Remote
Serial Number	S1000806???????????	S1000805???????????
MAC Address	98:35:71:00:ec:ee	98:35:71:00:ec:e9
IP Address	192.168.0.22	192.168.0.21
Management VLAN	10	Not Set
Site Name	Sub10	Sub10
Link Name	Test Link 15	Test Link 15
Terminal Name	B	A
Link ID		
Terminal Type	B	A
Software Version	xx.xx.xx.xx	xx.xx.xx.xx
Air Data Rate	1000 Mbps	1000 Mbps
Regulatory	NON-FCC	NON-FCC
Current Time	2000-03-06 13:23:14 (Clock)	2000-03-06 18:17:14 (Clock)

Figure 38 - Status – System Info Page

Local & Remote Terminals

- **Serial Number** – Serial number of the local radio terminal
- **MAC Address** – MAC Address of the local radio terminal
- **IP address – IP address of the management agent (very useful if the IP address of the remote terminal has been forgotten)**
- **Management VLAN – VLAN ID of the management agent VLAN (if set)**
- **Site Name** – This is a free-text field that can be used to store the Site Name (optional).
- **Link Name** – This is a free-text field that can be used to store the Link Name (optional).
- **Terminal Name** – This is a free-text field that can be used to store the Terminal Name (optional).
- **Link ID** – The Link ID must be the same at both ends of the link, and should not be used for any other link. *Note that if the Link ID is not the same at both ends of the link, then the radio link may not be established between the 2 ends. A warning message will be displayed if the LinkID is not the same at both ends. Suggest to leave this blank if not required.*
- **Software Version** – Software version running in the active memory bank.
- **Transmit / Receive Modulation Mode** – Modulation modes used in Tx / Rx (QPSK or 8PSK)
- **Air Data Rate** – Capacity (full-duplex) user data rate. This may be increased up to a maximum of 1000Mbps full-duplex by purchasing a licence key upgrade.
- **Regulatory** – The regulatory region is either “FCC” or “NON-FCC”. Only radios marked as “FCC” may be sold and operated in the USA or Canada.
- **Current Time** – The system clock time

5.4 Administration

The Administration pages are only accessible by users having the required access privileges, which are granted by an administrator.

5.4.1 Administration – LAN Interface

By default a radio terminals Ethernet interface is set to auto-negotiate the Ethernet type and rate. This page indicates the Ethernet line-rate and whether it is active or not, and the status of the auto-negotiation. The Ethernet port parameters for the remote end of the link are also shown, and are coloured RED if there is no Ethernet cable connected at the remote end. Dual-port versions display a second box for Ethernet Interface 2.

System Information

Site Name	Sub10
Link Name	Test Link 15
Terminal Name	B
Transmit Modulation Mode	8PSK
Receive Modulation Mode	8PSK
Air Data Rate	1000 Mbps
Regulatory	NON-FCC

Ethernet Interface 1

	Local	Remote
Link Status	Up	Up
Speed	1000 Mbps	1000 Mbps
Duplex	Full	Full
MDI/MDIX	MDI	MDI
Media	Copper	Copper

Ethernet Interface 2

	Local	Remote
Link Status	Up	Down
Speed	1000 Mbps	Unknown
Duplex	Full	Unknown
MDI/MDIX	MDI	Unknown
Media	Copper	Unknown

Switch Mode

Normal ▾

Bypass Mode forces frames on Primary and Secondary ports to be sent over the air interface.
Switching between Primary and Secondary ports is not available in Bypass mode.

Apply

Figure 39 - LAN (Ethernet) Interface

Note: On Dual-port versions, there is an option to choose the Switch Mode as either "Normal" or "Bypass". Bypass mode forces frames on both Primary and Secondary ports to be sent over the air interface, and does not allow traffic to be switched between Primary and Secondary ports. The reason for choosing "Bypass mode" is to allow unicast traffic to traverse across the radio link, even if there is no entry in the Switch Address Lookup Engine. For TCP traffic where bidirectional frames will populate the Switch Address Lookup Engine, it is possible to use "Normal" mode which will also allow switching between Primary and Secondary data ports.

5.4.2 Administration – VLAN Configuration

The user data traffic may be configured to support VLAN tags. Note that for management signalling, the VLAN ID is set on GUI page: “Administration / Management / IP”. When using VLAN’s the VLAN ID may be set to any value from 1 up to 4095.

There are 4 possible scenarios when using VLAN’s:

Case 1: VLAN’s not used

Case 2: VLAN for Management only

Case 3a: VLAN for Management + VLAN’s for User Traffic

Case 3b: VLAN for Management + VLAN’s for User Traffic with Tag / Untag on Default VLAN

NOTE: The “Allowed VLAN’s” table must always list the same set of VLAN ID’s on both ends of the link.

5.4.2.1 Case 1: VLAN’s not used

In this case, VLAN’s are not used, and the VLAN table is empty (or the “Enable VLAN Filtering” box is unticked) on both sides of the link.

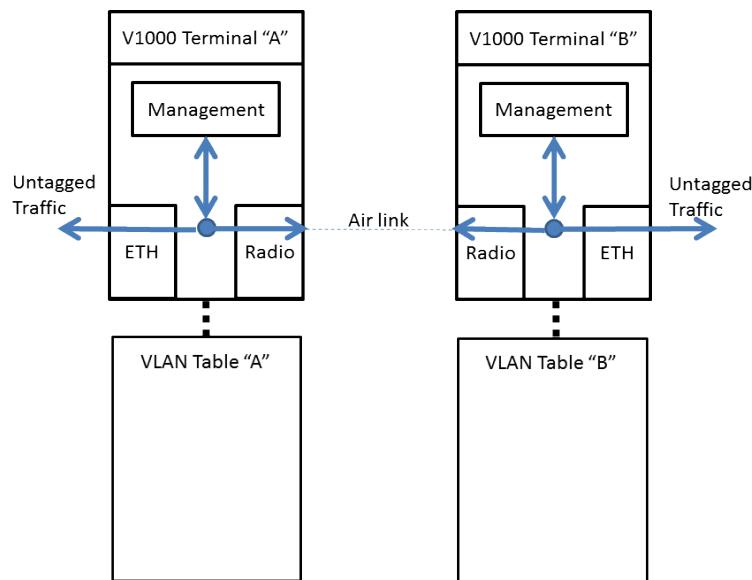


Figure 40 - VLAN’s not enabled (Allowed VLAN tables empty, or not enabled)

5.4.2.2 Case 2: VLAN for Management Only

In this case, VLAN is used for Management only (VLAN ID 99). All User Traffic is accepted, (both Tagged and Untagged), while the VLAN ID 99 is only used for Management traffic. The “Enable VLAN Filtering” box is unticked in the second figure below. Although the VLAN filtering is inactive, the Management VLAN ID 99 is still shown in the “Allowed VLAN’s” table for clarity.

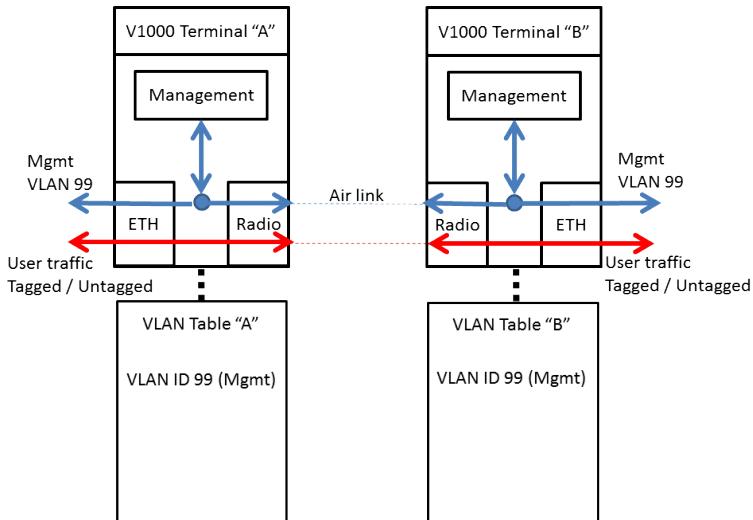


Figure 41 - VLAN 99 used for Management only, with User Traffic both Tagged & Untagged

System Information

Site Name	Ash House
Link Name	Test Link 11
Terminal Name	B
Transmit Modulation Mode	8PSK
Receive Modulation Mode	8PSK
Air Data Rate	1000 Mbps
Regulatory	NON-FCC

VLAN Filtering for User Traffic

VLAN Filtering restricts user traffic to the allowed VLANs only.

Enable VLAN Filtering

VLAN Filtering - Allowed VLANs

Only user traffic tagged with the following VLANs is allowed.

No allowed VLANs.

Allowed VLAN (1 - 4095)

VLAN Filtering - Default VLAN

The Default VLAN is added to all incoming untagged traffic and removed from all outgoing traffic.

Enable Default VLAN
Default VLAN Id
Default VLAN Priority
Default VLAN DEI

Figure 42 - Management VLAN only, with VLAN filtering not enabled

5.4.2.3 Case 3a: VLAN filtering enabled, with VLAN for management

In this case, VLAN's are used, and the VLAN table must contain the same VLAN ID's on both sides of the link. Note that in order to enable VLAN filtering, it is first necessary to set-up the Management VLAN, which is set on GUI page: "Administration / Management / IP". In the figure below, VLAN ID's 10, 11 and 12 are for User Traffic, and VLAN ID 99 is for Management Traffic, and these VLAN ID's are set to the same values on both

ends of the link, also see the GUI screenshot below (the order of VLAN ID's in the "Allowed VLAN's" table does not matter). With this VLAN configuration, only user traffic on VLAN ID's 10, 11 and 12 will be transported across the link, together with Management Traffic on VLAN ID 99, whilst all other traffic will be discarded (packets either untagged or else tagged with any other VLAN ID not listed in the tables).

If the Management VLAN 99 is removed from the "Allowed VLAN's" table, with VLAN filtering enabled, this will still allow management of the local side of the link, but it will prevent management of the remote end of the link, because the Management traffic will be filtered out and therefore not transported over the air to the remote terminal.

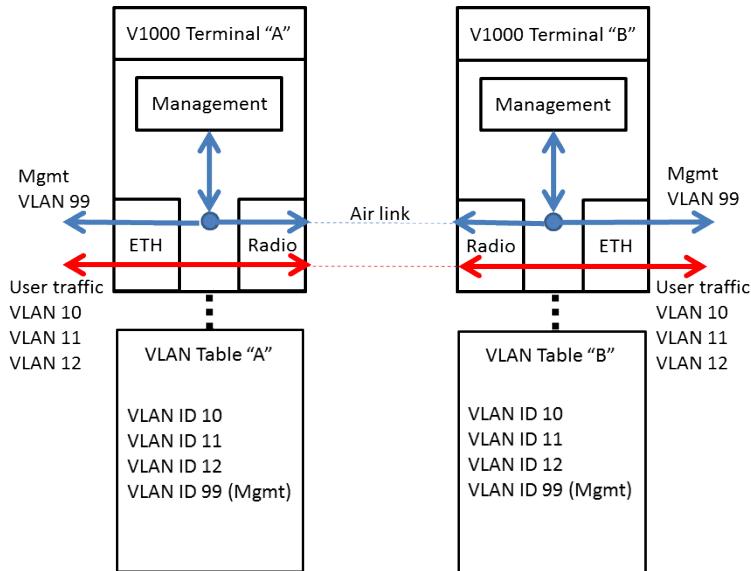


Figure 43 - VLAN filtering with Management VLAN ID 99

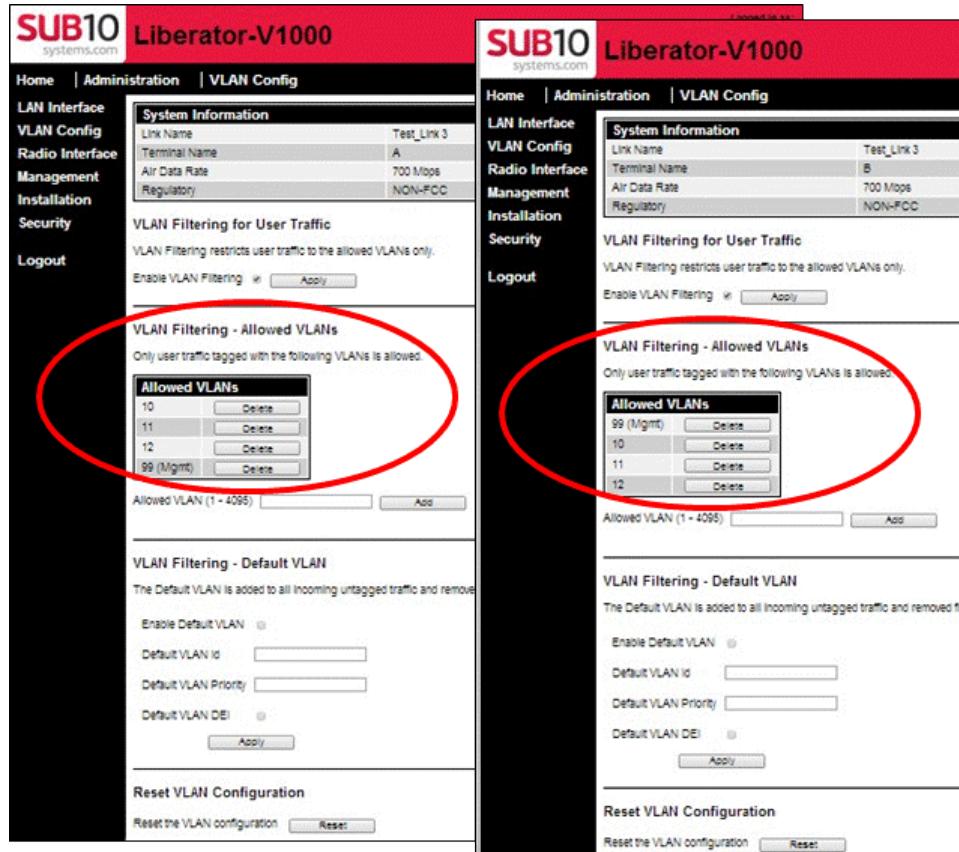


Figure 44 - VLAN filtering with Management VLAN ID 99

5.4.2.4 Case 3b: VLAN's used with VLAN for management and default VLAN (Tag / Untag)

This case is the same as Case 3a, but with the additional step of performing Tag / Untag manipulation on a single VLAN ID only. In this scenario, one of the User Traffic VLAN's is also specified to be the DEFAULT VLAN at one end of the link only: at the end where the DEFAULT VLAN is enabled, all incoming untagged frames into the Ethernet port will be tagged with the VLAN ID of the DEFAULT VLAN before sending over the air to the remote side as Tagged frames. All frames Tagged with the DEFAULT VLAN ID which arrive over the air from the remote terminal will be stripped of their VLAN Tag before being sent out on the Ethernet port as Untagged frames. Note that both ends of the link must contain the same list of VLAN ID's in the "Allowed VLAN's" table, but the DEFAULT VLAN can only be enabled at one end of the link at any one time. See the figures below, where VLAN ID 99 is used for Management, VLAN ID's 10, 11 and 12 for User Traffic, with VLAN ID 10 being set as the DEFAULT VLAN, and therefore performing the Tag / Untag operation on Terminal "B".

Note that it is possible to configure a DEFAULT VLAN ID at both ends of the link, (which may not be identical), but this represents an unlikely network configuration and is therefore normally unnecessary.

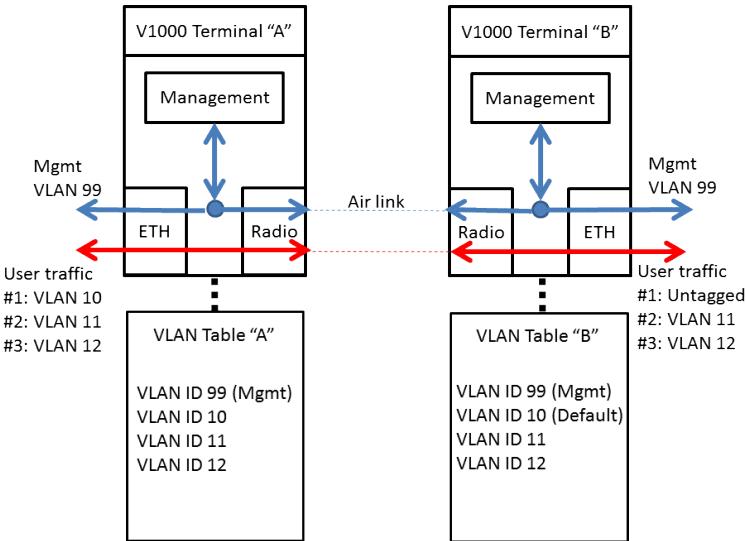


Figure 45 - VLAN filtering with Management VLAN and Tag/Untag on one end (Default VLAN ID 10)

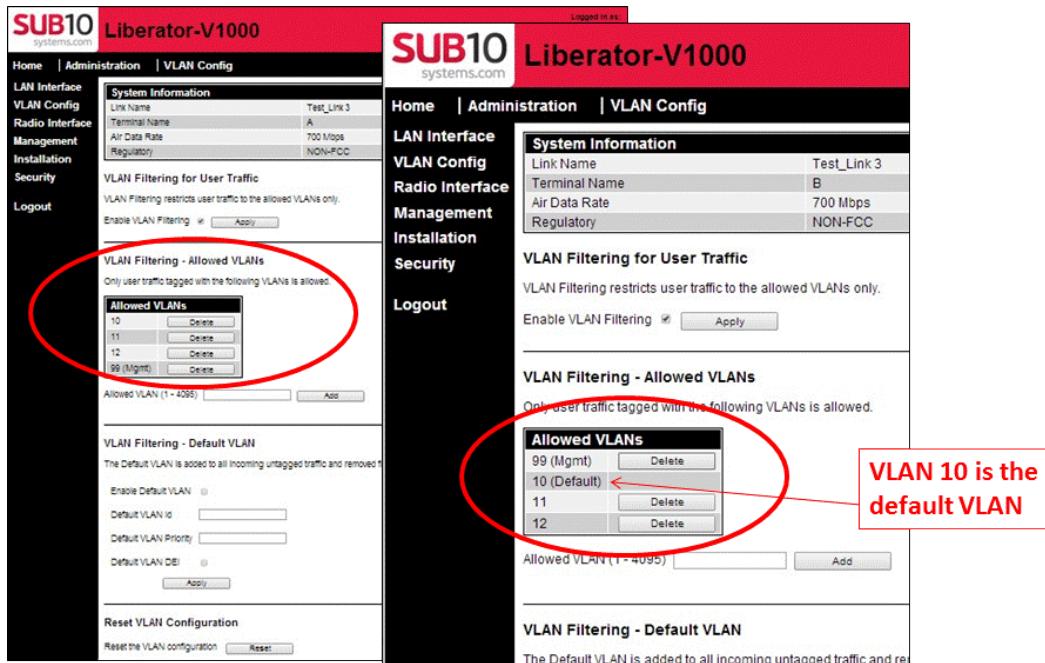


Figure 46 - VLAN filtering with VLAN 10 being default

5.4.3 Administration – QoS

This page is used to control the Quality of Service (QoS) settings. QoS has 8 priority queues, with queue 7 being the highest priority queue. The priority level of an incoming packet is set by the PCP bits of the VLAN, and it is possible to map multiple values of PCP bit settings to a single QoS queue if so desired. The priority level of an incoming packet is set by the PCP bits of the VLAN. The scheduling algorithm is Strict Priority only.

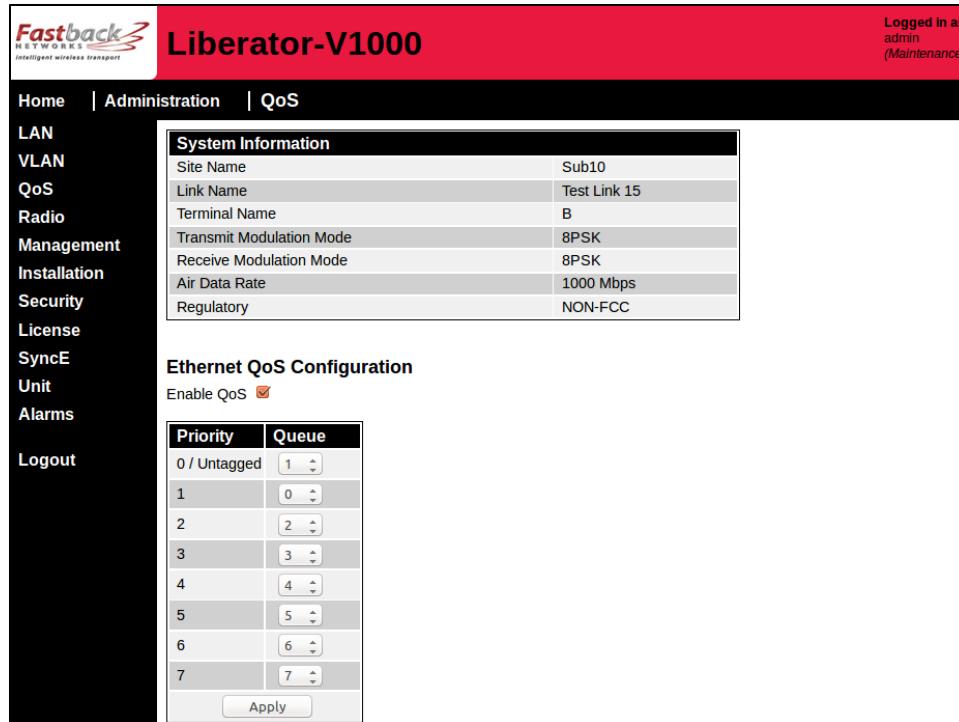


Figure 47 - QoS Settings

After setting the QoS parameters, it is necessary to click on “Apply”, and then to reboot the terminal for any changes to take effect. This allows both terminals to be set to the correct settings before QoS filtering is performed on the traffic.

5.4.4 Administration – Radio

This page is used to control the radio interface: it displays the radio parameters for both the local and remote sides of the link, and allows the user to make changes. Please note that any changes made to either Transmit Power or Channel Selection must be carefully considered before making any changes, as it may result in the radio link going down, and therefore the remote side will no longer be contactable. Firmware version 02.01.03.01 and later supports a rollback feature, so that any changes to certain configurations including Tx Power or Frequency require a confirmation within a pre-defined expiry time (default 3 minutes): this is a failsafe mechanism so that if the requested change caused the link to drop then the setting will automatically be rolled-back to its previous value if left unconfirmed until the expiry time is reached. For a list of all configuration that is subject to confirmation and potential rollback see section [Configuration Rollbacks](#).

The **Transmit Power Limit** section can be used to set the power to either: High, Medium or Low.

Tx Power Setting	QPSK (700Mbps max) Nominal Average Tx Power into Antenna	8PSK (1Gbps) Nominal Average Tx Power into Antenna
High	+7.5dBm (FCC) and +6 dBm (Rest of World)	+4 dBm
Medium	+3 dBm	-1 dBm
Low	-5 dBm	-5 dBm

The transmit power should typically be reduced on shorter links (less than 150 metres) to ensure that the RSSI is not higher than -25dBm wherever possible. Please use the Link Availability Calculator to work out the correct link budget for your link before changing the Transmit Power, which should be the same on both ends of the link. Enabling **ATPC** (Automatic Transmit Power Control), will allow the transmit power to be dynamically adjusted by the radio in response to changing propagation conditions (e.g. rain fade). The transmit power will never move above the level set by the **Transmit Power Limit**. Always press “Submit”

after making any changes to ensure that the change is applied to the radio. ATPC is disabled by default on V1000 radios. ATPC is always disabled when in “Alignment Mode”. Note that in Firmware Release 02.01.03.012, the maximum Tx power in 8PSK mode is +2dBm. The usable range with this Firmware release for 8PSK is from 30 metres up to 450 metres maximum.

The **Modulation Mode** can be used to change modulation mode between fixed QPSK (up to 700Mbps) and 8PSK (1Gbps) AMOD. When 8PSK mode is selected, a slow adaptive modulation (AMOD) algorithm will automatically choose between QPSK and 8PSK according to the changing condition of the radio link. When QPSK mode is selected, AMOD is turned off. The Link Availability of the Modulation Mode may be changed using the drop-down menu to select either “High”, “Medium” or “Low” availability (default is “Medium”). This Availability setting changes the AMOD threshold: if Link Availability is set to “Low” this means that the AMOD threshold is set at a lower level so that the link will transition to 8PSK mode much more easily. If Link Availability is set to “High”, then the link will be biased more to remaining in QPSK mode, and will only transition to 8PSK mode with a much higher incoming signal level.

Note that, on units fitted with AES capable hardware, if a valid AES Licence Key is applied, and AES encryption is activated, the modulation will be locked to QPSK mode only with a maximum throughput rate of 700Mbps. In this case, the AMOD setting options will not be displayed.

If the capacity key is only 700Mbps or lower, then it is recommended to set the modulation mode to QPSK in order to avoid unnecessary changes up to 8PSK mode which will not increase the usable data rate if the Air Data Rate is 700Mbps or less.

The screenshot shows the Liberator-V1000 user interface. At the top, there's a red header bar with the Fastback Networks logo, the device name "Liberator-V1000", and a "Logged in as: admin (Maintenance)" message. Below the header is a black navigation bar with links for Home, Operation, Radio, Ethernet, System, and Logout. The main content area is divided into three sections: "System Information", "System Status", and "Alarms".

System Information	
Site Name	Sub10
Link Name	Test Link 15
Terminal Name	B
Transmit Modulation Mode	8PSK
Receive Modulation Mode	8PSK
Air Data Rate	1000 Mbps
Regulatory	NON-FCC

System Status	
Radio Interface	Synchronised
Radio Link	Up
Ethernet Interface 1	Up
Ethernet Interface 2	Down

Alarms	
Rx Power Low	Clear
Vector Error High	Clear
MWU Temperature High	Clear
MWU Temperature Low	Clear
Radio Link Down	Clear
Link ID Mismatch	Clear

Figure 48 - Home Page showing the Air Data Rate (in this case set to 1000 Mbps)



Liberator-V1000

Logged in as:
admin
(Maintenance)

- [Home](#)
- [Administration](#)
- [Radio](#)

System Information		
Site Name	Sub10	
Link Name	Test Link 15	
Terminal Name	B	
Transmit Modulation Mode	8PSK	
Receive Modulation Mode	8PSK	
Air Data Rate	1000 Mbps	
Regulatory	NON-FCC	

Radio Attributes	Local	Remote
Link	Up	Up
Tx Power Limit	Full	Full
Modulation Mode	8PSK	8PSK
Terminal Type	B	A
Channel Bandwidth (MHz)	500	500
Tx Frequency (GHz)	62.500	58.500
Rx Frequency (GHz)	58.500	62.500

Transmit Power

Enable ATPC (Automatic Transmit Power Control)

Transmit Power Level

Modulation

Maximum Receive Modulation Mode

Availability

Channel Selection

Tx / Rx Frequencies (GHz)

WARNING: Frequency channels selected must comply with in-country radio regulations

Figure 49 - Radio Interface: Transmit Power, ATPC, Modulation Mode, Frequency Channel and Data-rate throttling selections

5.4.4.1 Frequency Selection - The Tx/Rx channels can be selected.

WARNING: it is the responsibility of the installer to ensure that the correct frequency channels are selected in accordance with the in-country radio regulations.

On V1000 Single-port, The “A” end can be set to transmit on 58.5, 59.0 or 59.5GHz and the “B” end to transmit on 61.5, 62.0 or 62.5GHz. The 3 channels on Tx Low and Tx High are non-overlapping.

On V1000 Dual-port, The “A” end can be set to transmit on 58.0, 58.5, 59.0 or 59.5GHz and the “B” end to transmit on 61.5, 62.0, 62.5 or 63.0GHz. The 4 channels on Tx Low and Tx High are non-overlapping.

Radio Attributes		Local	Remote
Link	Up	Up	
Tx Power Limit	High	High	
Modulation Mode	8PSK	8PSK	
Terminal Type	A	B	
Channel Bandwidth (MHz)	500	500	
Tx Frequency (GHz)	59.500	62.000	
Rx Frequency (GHz)	62.000	59.500	

Transmit Power

Enable ATPC (Automatic Transmit Power Control)

Transmit Power Level

Modulation

Maximum Receive Modulation Mode

Availability

Frequency Selection

Tx / Rx Frequencies (GHz)

WARNING: Frequency channels must comply with in-country radio regulations

Maximum Input Data Rate

Data Rate Limit

Figure 50 - Radio interface showing Frequency Selection (V1000 Single-port)

5.4.4.2 Maximum Input Data Rate - The Data Rate Limit can be set to a value less than the Air Data Rate, in order to allow shaping of the input data stream. The Data Rate limit may be set to 100Mbps, 300Mbps, 500Mbps, 700Mbps or 1000Mbps (up to the maximum licensed data rate). Traffic exceeding the rate set will be dropped according to the QoS priorities being used.

The maximum Air Data Rate is set by Capacity Licence Key. If the Air Data Rate only shows 500 Mbps or 700 Mbps, and a higher capacity is desired, the please contact Fastback Networks Support to obtain a Capacity Licence Key. Please include the MAC addresses of both radio terminals, which will be needed to generate the Licence Keys.

Note that on units fitted with AES capable hardware, if a valid AES Licence Key is applied, and AES encryption is activated, the modulation will be locked to QPSK mode only with a maximum throughput rate of 700Mbps. In this case, the AMOD setting options will not be displayed.

The screenshot shows the Liberator-V1000 configuration interface. The top navigation bar includes links for Home, Administration, and Radio. The left sidebar lists various configuration categories: LAN, VLAN, QoS, Radio, Management, Installation, Security, License, SyncE, Unit, Alarms, and Logout. A yellow warning icon with an exclamation mark is positioned on the left side of the main content area.

System Information

Site Name	Ash House
Link Name	Test Link 12
Terminal Name	A
Transmit Modulation Mode	8PSK
Receive Modulation Mode	8PSK
Air Data Rate	1000 Mbps
Regulatory	NON-FCC

Radio Attributes

	Local	Remote
Link	Up	Up
Tx Power Limit	High	High
Modulation Mode	8PSK	8PSK
Terminal Type	A	B
Channel Bandwidth (MHz)	500	500
Tx Frequency (GHz)	59.500	62.000
Rx Frequency (GHz)	62.000	59.500

Transmit Power

Enable ATPC (Automatic Transmit Power Control)

Transmit Power Level

Modulation

Maximum Receive Modulation Mode

Availability

Frequency Selection

Tx / Rx Frequencies (GHz)

WARNING: Frequency channels selected must comply with in-country radio regulations

Maximum Input Data Rate

Data Rate Limit

Figure 51 - Confirmation required or else config change will be rolled-back to previous setting

5.4.5 Administration - Management

5.4.5.1 Administration - Management – IP Configuration

The IP Configuration Page is used to configure the Ethernet interface and Management IP Connectivity.

Figure 52 – IP Configuration

- (a) By default, management connectivity to a terminal is by fixed IPv4 address. The default IP address for an “A” terminal is 192.168.0.21 and the default IP address for a “B” terminal is 192.168.0.22. Changes to the IP address are protected by rollback which requires confirmation within expiry time limit, or else changes will be rolled-back.
- (b) If it is desired to set up a VLAN for management, this should be entered in the “Management VLAN Id” box with a value from 1 up to 4095, and by setting the “Management VLAN Priority” with a value from 0 to 7. Management VLAN priority may take values from 0 to 7, with 0 being lowest priority, and 7 being highest. “DEI” stands for “Drop Eligible Indicator” within IEEE 802.1Q. The option “DEI Enabled” sets the DEI Enabled bit, which indicates to other network devices (such as routers) that this VLAN has low priority, and in case of system overload, these frames may be dropped to reduce congestion. If a Management VLAN is entered, this will be enabled on pressing the “Apply” button: note that this is likely to result in loss of GUI connection to the terminal, and the PC or router will need to be reconfigured to use the same Management VLAN which has just been applied to the terminal. If VLAN Filtering is enabled on GUI page “VLAN Config”, then it is important to make sure that both terminals of the link are configured to use a VLAN for management, and this VLAN is listed in the “Allowed VLAN’s” table.
- (c) When DHCP is selected, the terminal’s IP Address, Subnet Mask and Default Gateway are acquired from a DHCP server. When DHCP is selected these fields are greyed out. When using DHCP the terminal cannot be managed until the DHCP client has started up and acquired an IP Address.

5.4.5.2 Administration Management – SNMP

The SNMP Configuration Page is used to configure the SNMP Agent, see below.

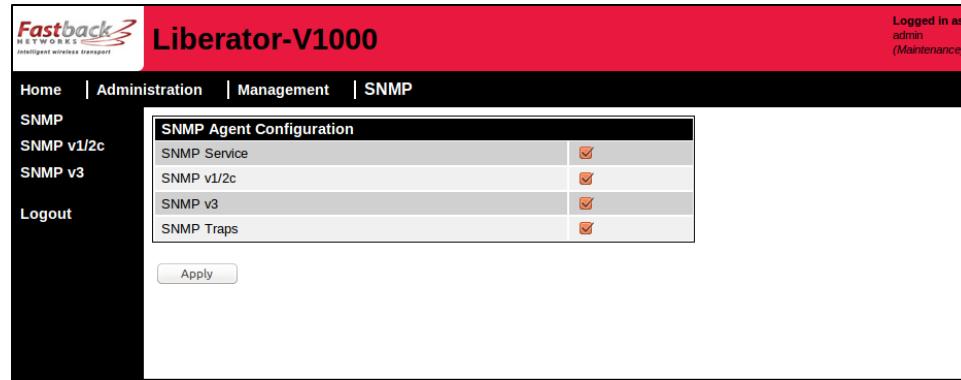


Figure 53 - Configuring SNMP

The SNMP Agent is compatible with SNMPv1, SNMPv2c and SNMPv3.

- SNMP v1/2c** Enables the SNMP v1/2c agent and configuration options.
- SNMP v3** Enables the SNMP v3 agent and configuration options.
- SNMP Traps** The SNMP agent will send traps to the configured trap destinations.

Selection of SNMPv3 requires confirmation, otherwise the setting will be rolled back to its original value after the configured rollback timeout. Note that the SNMP agent is not enabled by default, and it must be enabled from this GUI webpage before it can accept SNMP messages. The settings which must be enabled on the GUI before using SNMP are as follows:

1. Webpage: "*Admin/Management/SNMP*" -> Enable SNMP v1/2c and Traps
2. Webpage: "*Admin/Management/SNMP/SNMPv1/2c*" -> Set Trap destination(s)
3. Webpage: "*Admin/Unit*" -> Enable SNMP Service

5.4.5.3 Administration - Management – SNMP – SNMPv1/2c

Configure the SNMP v1/2c agent community strings and trap destinations.

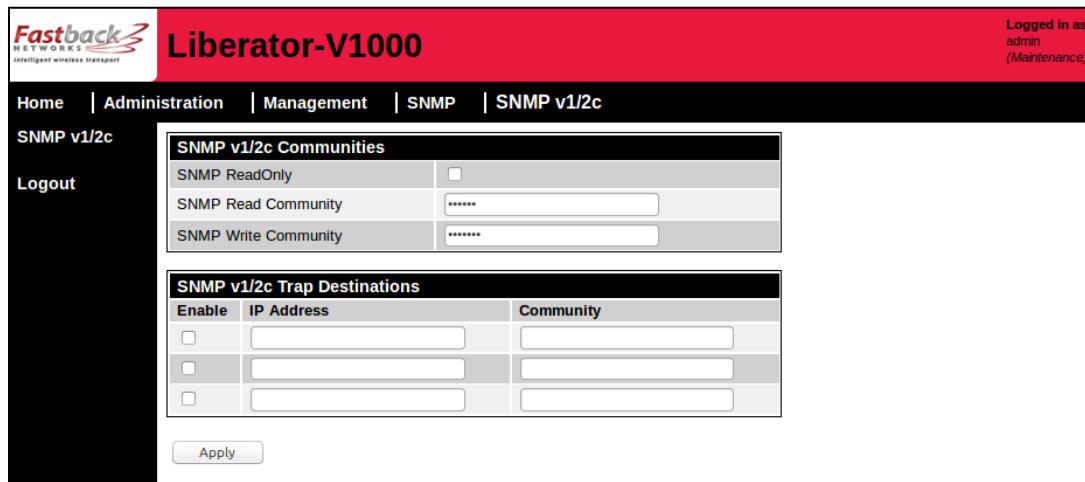


Figure 54 - SNMPv1/v2c settings

- Communities** SNMPv1/v2c community strings for read-only and read-write operations when accessing MIB objects via SNMP.

- **SNMP ReadOnly** A security feature which prohibits SNMP Sets. If this is 'Enabled' all SNMP Set requests will be rejected.
 - **Read Community** The community string used for read access (Get/GetNext). Default setting to use is "public".
 - **Write Community** The community string used for write access (Set). Default setting to use is "private".
 - **Trap Destinations** Up to three destination are possible, each requiring:
 - **IPv4 Address** A valid IP address of the receiving management system.
- Note: The IP address must be valid and reachable.**
- **Community** The trap community string sent in each trap to this destination, this is used by management systems that require authentication of the trap community.

5.4.5.4 Administration - Management – SNMP – SNMPv3

Configure the SNMP v3 agent supports User Based Model (USM) security. Note that the SNMPv3 configuration is only supported through the web GUI and the Sub10 Systems enterprise MIB. The configuration may be viewed but not changed via the standard SNMPv3 MIBs – this will be supported in a later release.

The screenshot shows the 'SNMPv3 Configuration' page of the Liberator-V1000 web interface. The top navigation bar includes links for Home, Administration, Management, SNMP, and SNMP v3. The left sidebar has links for Home, Administration, Management, SNMP, SNMP v3, and Logout. The main content area is titled 'SNMPv3 Configuration' and contains several tables for configuration:

- SNMPv3 Engine Id Configuration:** Includes fields for 'SNMP Engine Id Format' (set to 'Text') and 'SNMP Engine Id Text' (set to 'Sub10Systems').
- SNMPv3 Group Security Policy:** Shows a table with columns for Group, Auth Protocol, and Priv Protocol. Rows include Operation (No Auth, No Priv), Administration (MDS, No Priv), and Maintenance (MDS, DES).
- SNMPv3 Access Security:** Shows a table with columns for Enable, Access Name, and Access Address. It lists three entries: one with 'Enable' checked and two others with 'Access Name' and 'Access Address' fields.
- SNMPv3 User Security:** Shows a large table with columns for Enable, User Name, User Role, Auth Password, Verify Password, Priv Password, and Verify Password. It lists 12 rows, each with 'User Name' and 'User Role' fields.
- SNMPv3 Notification Target Security:** Shows a table with columns for Enable, Name, Target Address, and SNMPv3 User:Group. It lists three entries with 'Name' and 'Target Address' fields.

An 'Apply' button is located at the bottom of the configuration section.

Figure 55 - SNMPv3 settings

- **SNMPv3 Engine Id** - Configure the format of the SNMP v3 Engine Id.
- **SNMP Engine Id Format**
 - IPv4 Address The IPv4 Address of the unit
 - IPv6 Address (Not Available)

- **MAC Address** The MAC address of the unit
- **Text** Plain text up to 18 characters in length.
- **SNMP Engine Id Text** – Plain text up to 18 characters in length if Engine Id format is selected as ‘Text’
- **SNMPv3 Group Security Policy** - Configure authentication and privacy protocols per user group.
- **Auth Protocol**
 - **No Auth** Authentication disabled for the group
 - **MD5** Message Digest algorithm authentication
 - **SHA-1** Secure Hash Algorithm authentication
- **Priv Protocol**
 - **No Priv** Privacy disabled for the group
 - **DES** Data Encryption Standard
 - **AES** Advanced Encryption Standard

AES encryption will only be permitted if the unit has a valid AES encryption license key installed (note that only Dual-port versions and certain Single-port versions are hardware-capable for AES encryption). An AES-256 upgrade may be purchased, which will only be supplied if there is official permission to export AES encryption to the country of operation. If there is no AES license key installed, then the following message is displayed if “AES” is selected:

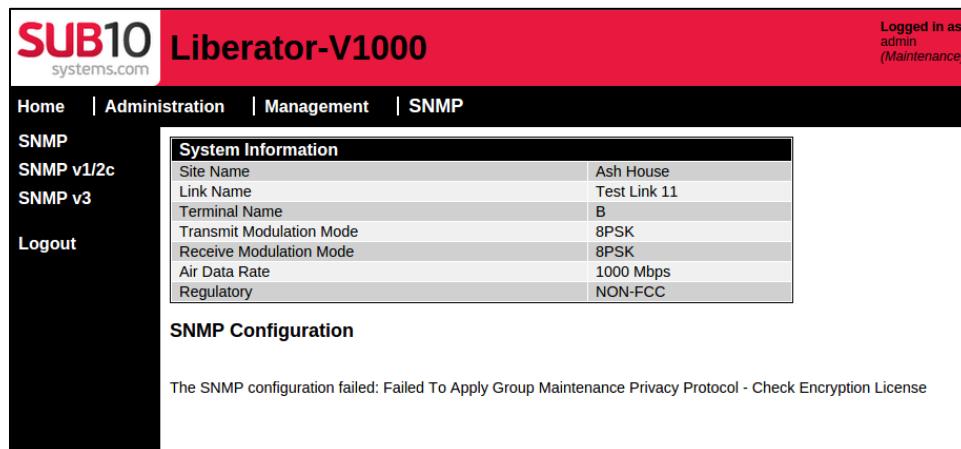


Figure 56 - Error message displayed if “AES” is selected without a valid AES license key.

- **SNMPv3 Access Security** Restricts access to the specified management stations.
 - **Access Name** User defined name up to 32 characters
 - **Access Address** IP Address
- **SNMPv3 User Security** Defines each user (maximum 10) in the user based security model (USM).
 - **User Name** User defined name up to 32 characters
 - **User Role** The user’s group defining the access rights to certain parts of the MIB
 - Operation User has read-only access
 - Administration User has read-write access but cannot upload new firmware or reboot the unit
 - Maintenance Full Access
 - **Auth Password** The password for the configured authentication protocol (not for ‘No Auth’)
 - **Verify Password** Verify the Auth Password
 - **Auth Password** The password for the configured authentication protocol (not for ‘No Priv’)
 - **Verify Password** Verify the Priv Password

Note: The 'User Role' restricts access via VACM (View Based Access Model) which is fixed depending on the user's assigned group.

- **SNMPv3 Notification Target Security** Defines each target for sending SNMP notifications.
 - **Target Name** User defined **name** up to 32 characters.
 - **Target Address** Target IP Address.
- **User:Group** The User and Group used to send the notification.

5.4.6 Administration Management – Time

The Time page is used to set the internal real time clock on the radio terminal. The real-time clock is used to timestamp events in logs and SNMP traps.

The screenshot shows the Liberator-V1000 Time configuration interface. At the top right, it says "Logged in as: admin (Maintenance)". The left sidebar has links for Home, Administration, Management, and Time. Under Time, there are links for IP, SNMP, and Logout. The main content area has three sections: "System Information" (Site Name: Sub10, Link Name: Test Link 15, Terminal Name: B, Transmit Modulation Mode: 8PSK, Receive Modulation Mode: 8PSK, Air Data Rate: 1000 Mbps, Regulatory: NON-FCC), "System Time" (Current Time: Mar 06 13:27:08), and "System Clock". The "System Clock" section contains fields for Date (Year: 2000, Month: 3, Day: 6) and Time (Hours: 13, Minutes: 27, Seconds: 8), with an "Apply" button. Below this is the "NTP Server Configuration" section, which includes an "NTP Enabled" checkbox and fields for "Server 1" and "Server 2".

Figure 57 - Setting the real-time clock manually

The first option is simply to set the System Clock date and time, and press the “Apply” button in the “System Clock” section of the page.

For greater accuracy the operator can synchronise the internal real time clock to an NTP (Network Time Protocol) time server. To enable the use of an NTP time server the operator must tick the “NTP Enabled” box, and also enter the IP address of an accessible NTP time server into the “Server 1” field (and also “Server 2” field if an alternative server is available), and then press the “Apply” button in the “NTP” section of the page.

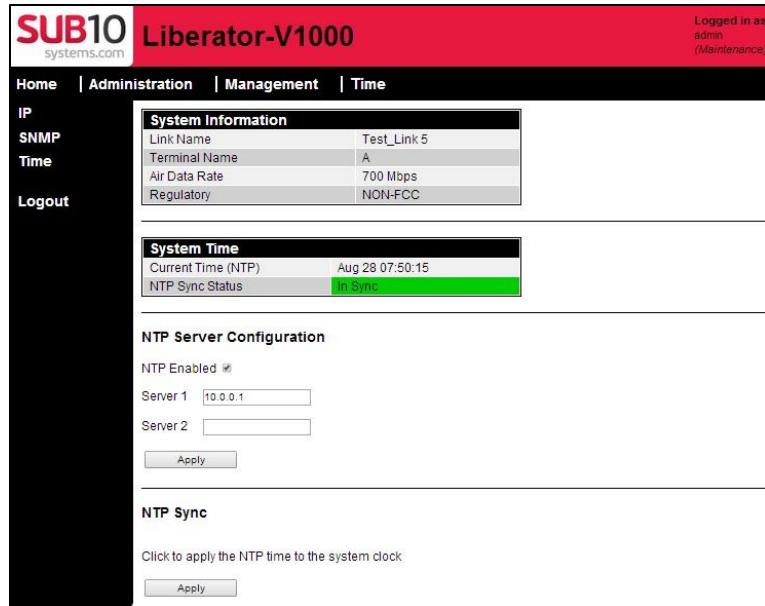


Figure 58 – Using an NTP Server

5.4.7 Administration - Installation

When Alignment mode is selected, the System Mode box displays “Alignment Mode” in YELLOW. The Alignment Voltage indication given is in volts and is the same voltage as can be measured with a voltmeter on the alignment port on the back of the terminal. Note that ATPC is always disabled when in “Alignment Mode”. After alignment is complete, replace the voltage port cap on the back enclosure of the terminal, and click on “Change” to return to Normal mode. The System Mode box displays “Normal” in GREEN. It is also possible to change mode by clicking on the “Change Mode” box on the Installation page. Once back in “Normal Mode”, ATPC will continue to operate if it was previously enabled on the “Radio Interface” page.

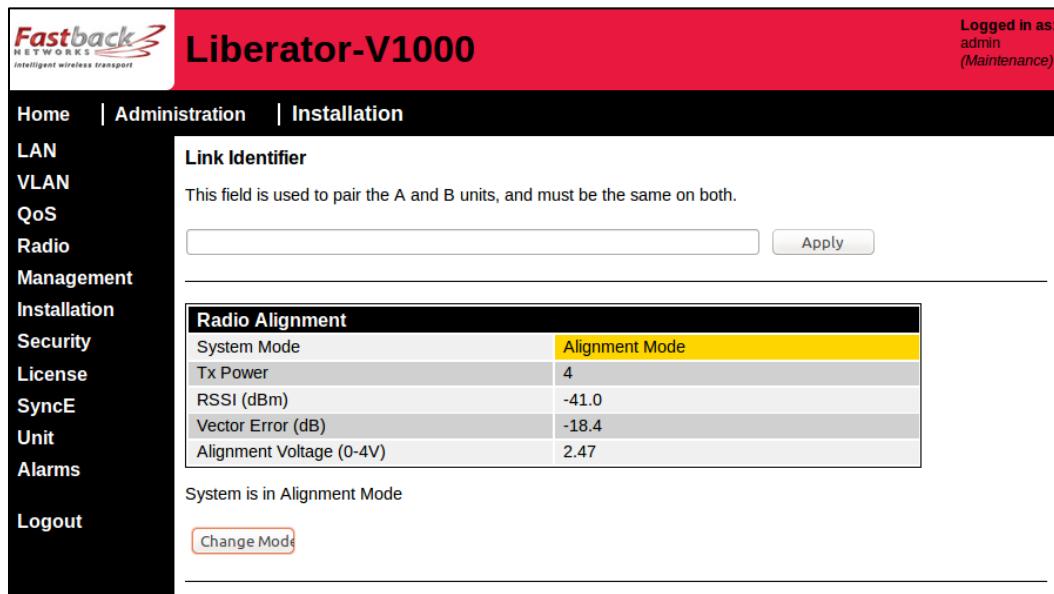


Figure 59 - Installation - Alignment Mode

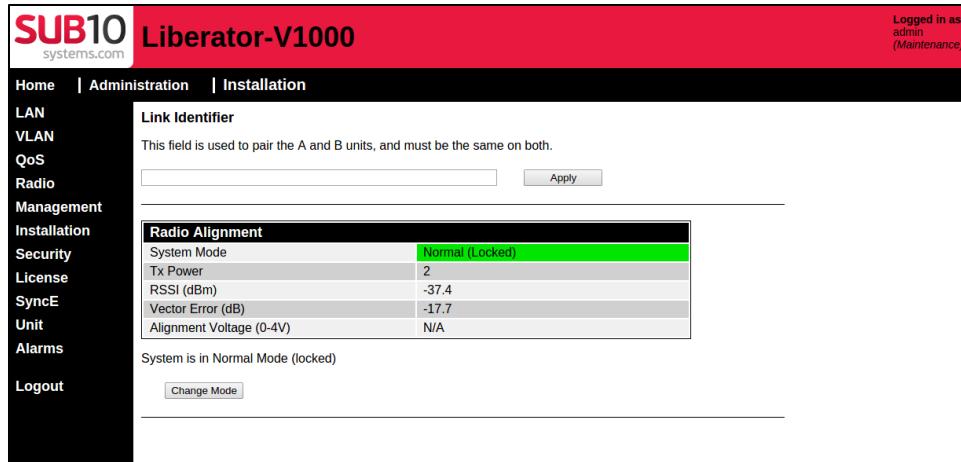


Figure 60 - Installation – Normal Mode

Note: In order to prevent false transitions into alignment mode due to the alignment cap not being correctly fitted and producing a false open-circuit, it is possible to use the GUI button "change mode" to force the unit from Alignment mode into Normal mode: in this case, the System Mode will display "Normal (Locked)" and removal of the alignment cap will not change back to Alignment mode, and there will not be any voltmeter reading available. The only way to unlock the mode to allow Alignment mode again, is to press the "Change Mode" button on the GUI again.

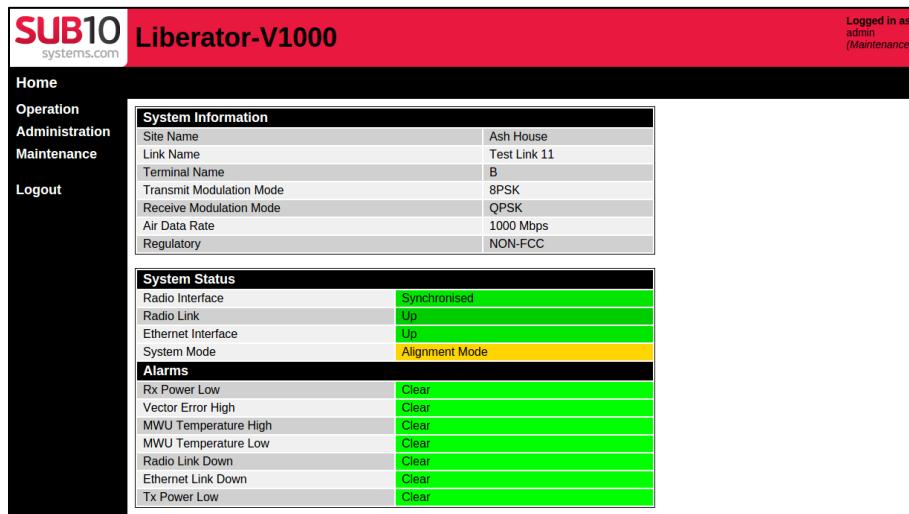


Figure 61 - Home page showing System Mode in Alignment mode

The Installation page also allows the Link Identifier to be set. The Link Identifier should be the same on both ends of the link, or else the link will not be established. In the case of a mismatch in Link Identifier, a warning message will be displayed.

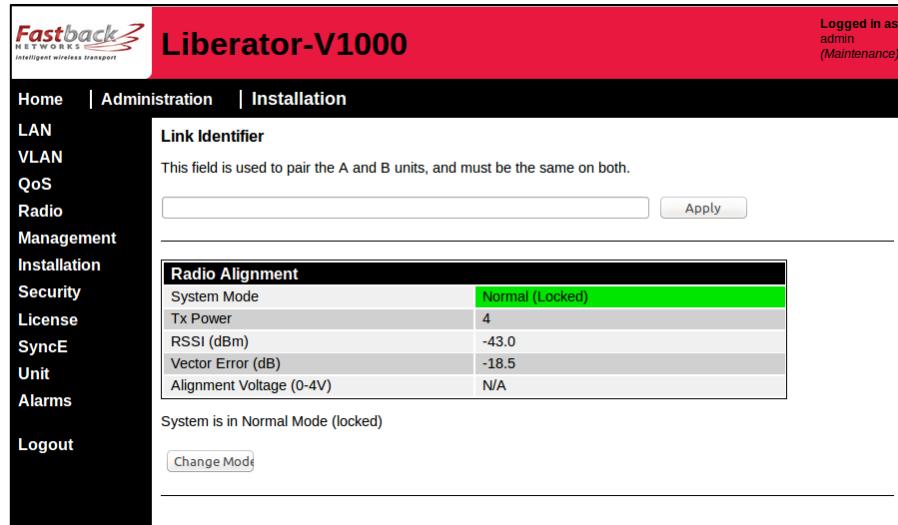


Figure 62 - Normal Mode (Locked)

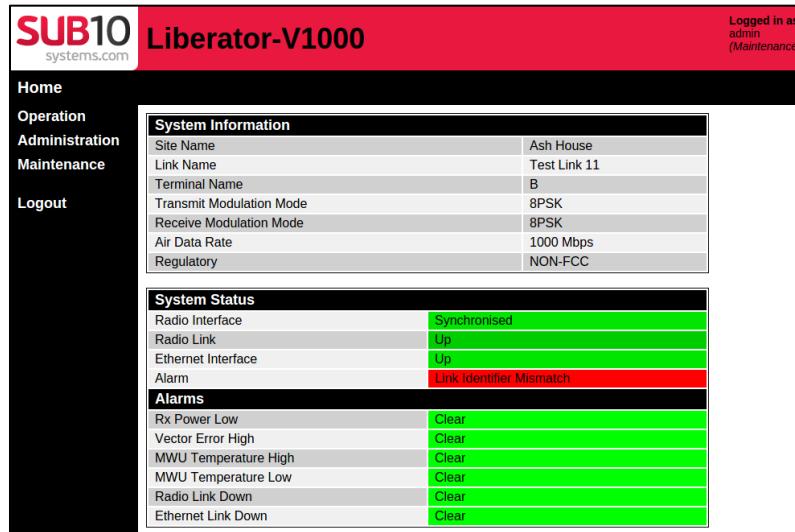


Figure 63 - Mismatch in Link Identifier name results in a warning message

5.4.8 Administration Security – Users

This page shows the users who are registered to use the system, together with their privilege level ("Role"). It is possible to add new users by clicking on "New", and this allows the new username, password and privilege level ("Role") to be set. Note that the password must always be at least 6 characters long.

The screenshot shows the Liberator-V1000 User Management interface. At the top right, it says "Logged in as: admin (Maintenance)". The left sidebar has links for Home, Administration, Security, and Users, with "Users" being the active tab. It also includes links for Encryption and Logout.

System Information

Site Name	Sub10
Link Name	Test Link 15
Terminal Name	B
Transmit Modulation Mode	8PSK
Receive Modulation Mode	8PSK
Air Data Rate	1000 Mbps
Regulatory	NON-FCC

User Management

User	Role	
admin	Maintenance	Modify

Add User

Click to add a new user [New](#)

Reset

Click to reset user accounts to default [Reset](#)

Figure 64 - Security: Users Page

A User's role or password may be modified by clicking the "Modify" button. Please note that after following this process, it is necessary to logout and log back in to the terminal for the new privilege level ("role") to take effect. So for example, if it is desired to elevate a User's privilege level to "Maintenance" in order to allow the User to perform firmware upgrades, the User will not actually benefit from the change until they have logged-out and logged in again.

The screenshot shows the Liberator-V1000 New User creation interface. At the top right, it says "Logged in as: admin (Maintenance)". The left sidebar has links for Home, Administration, Security, and Users, with "Users" being the active tab. It also includes links for Encryption and Logout.

System Information

Site Name	Sub10
Link Name	Test Link 15
Terminal Name	B
Transmit Modulation Mode	8PSK
Receive Modulation Mode	8PSK
Air Data Rate	1000 Mbps
Regulatory	NON-FCC

New User

User Name:

Role:

Password:

Confirm password:

[Submit](#)

Figure 65 - User Access Control Page

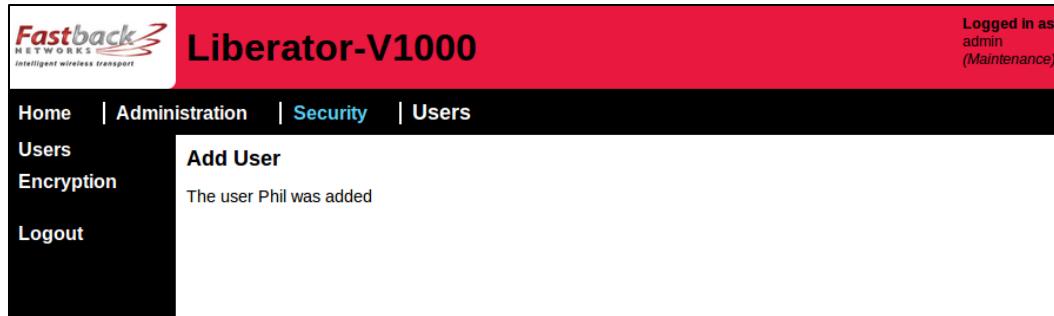


Figure 66 - Confirmation that new user was added

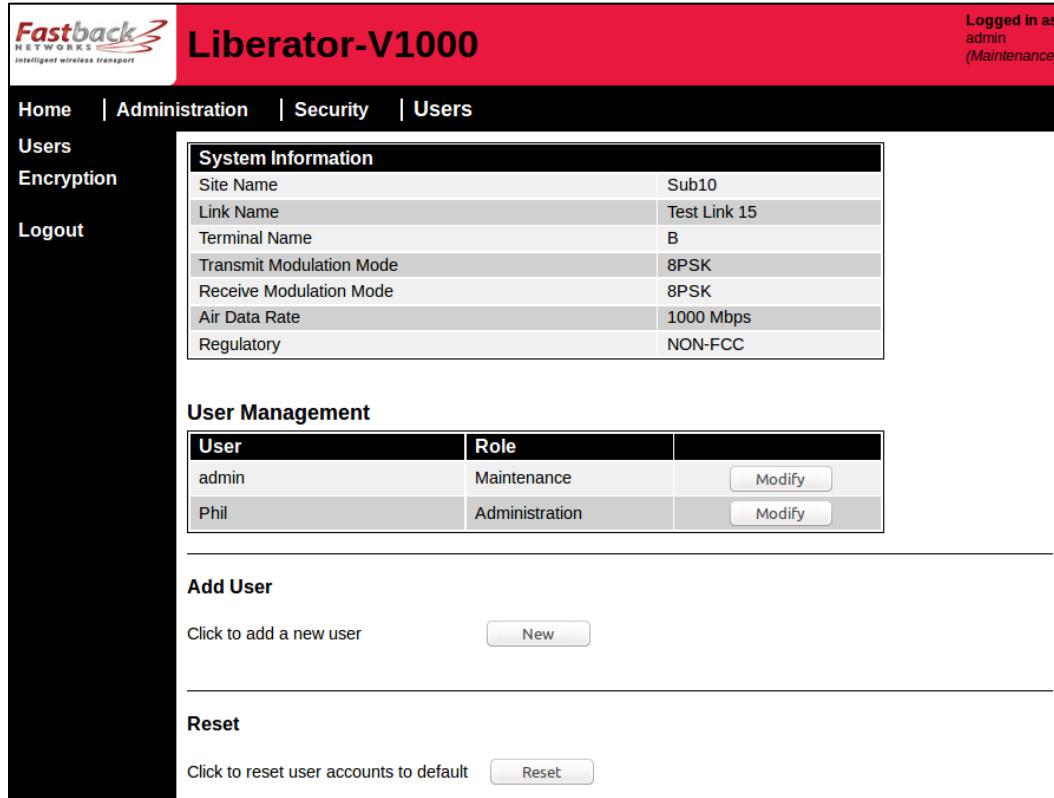


Figure 67 - New User Added

5.4.9 Administration – Security/Encryption

This page is only visible if a valid AES Licence Key has been applied to the terminal. See Section 5.4.10 to apply the Licence Key, which will then make the “Encryption” option visible.

In order to activate the AES encryption after the AES Licence Key has been applied (this procedure MUST be followed at both ends of the link, always update the REMOTE END FIRST):

1. In the “Encryption Algorithm” Drop-down box, select “AES-256”.
2. Enter a new AES 256 Encryption Key. This is a set of alphanumeric characters which MUST be the same at both ends of the link. The user may choose any set of characters they wish from (0 to 9) and (a to z).
3. Enter the same Encryption Key again in the second box to verify that it is correct.
4. Press “Apply” and the Encryption Key will now come into operation, and the data will be encrypted over the air in the transmit direction only.

5. Reboot the unit and click “Confirm” to prevent Rollback to the unencrypted state.
6. Note that the link can then only be re-established if the remote terminal is also set with the same Encryption Key (this means that it is necessary to make this change on the remote end of the link FIRST).

Notes:

1. If one terminal is reset to Factory Default, then its Licence Keys will be lost and AES encryption will be automatically de-activated, and this means that it will not be able to re-establish a link if the remote end is still running with AES encryption activated. In this case, it will be necessary to either de-activate the AES encryption on the remote end, or else to re-apply the AES Licence Key and re-activate the encryption on the end which had been reset to Factory Default. In this case it will be necessary to use the same AES 256 Encryption Key on both ends of the link.
2. The maximum capacity of the link when AES encryption is activated is 700Mbps full-duplex in the current software release. The AMOD settings on the radio page will not be displayed when AES encryption is activated.
3. A new encryption key will only be active after a reboot, and in this case always remember to click “Confirm” on each unit after reboot, to prevent automatic rollback to the previous state.

The screenshot shows the Liberator-V1000 web interface. At the top, there's a red header bar with the Fastback Networks logo and the text "Liberator-V1000". On the right of the header, it says "Logged in as: admin (Maintenance)". Below the header, there's a black navigation bar with links for Home, Administration, Security, and Encryption. The main content area has a sidebar on the left with links for Users, Encryption, and Logout. The main content area is titled "Wireless Encryption" and contains a table with two rows: "Encryption Status" (Algorithm: None, Key: No key entered). Below the table, there's explanatory text: "This will encrypt the airside data transmitted across the link.", "Encryption keys entered must be the same on both ends of the link.", and "Both ends of the link must be restarted before a key change will take effect.". There are dropdown menus for "Encryption Algorithm" (set to AES-256) and "Encryption Key" (containing four asterisks), and a text input field for "Confirm Encryption Key" (also containing four asterisks). A "Apply" button is at the bottom of the form.

Figure 68 - Enable AES-256 encryption, enter the desired encryption key (twice), and press Apply

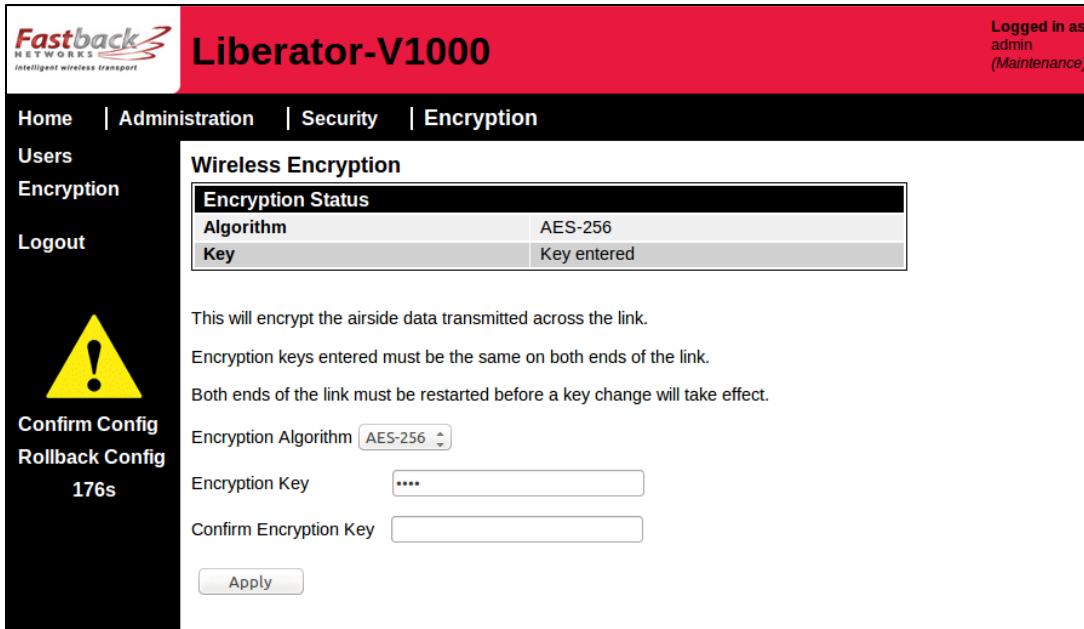


Figure 69 - Press Confirm to accept change and avoid rollback

5.4.10 Administration - License

This page allows License Keys (including AES Licence Keys) to be entered. The License Key is locked to the MAC address of the radio terminal, so the License Key can only be used on the radio terminal with the corresponding MAC address.

Note that AES Licence Keys can be used only if the hardware version is AES capable. All Dual-port versions are hardware-capable of AES, but only certain Single-port versions are hardware-capable of AES.

Please contact Fastback Network Support to obtain a License Key, the MAC addresses of both radio terminals will be required in order to generate the Licence Keys. Copy and Paste the License Key into the entry box, and press "Submit". If there is an error message saying "Error: key not applied", then it is likely that the MAC address is not correct, in this case double-check that the correct License Key has been applied to the radio terminal, and if the error message persists then please contact Fastback Networks Support.

After a valid AES Licence Key has been correctly uploaded to a V1000 unit which has hardware capable of AES, then a new page "Encryption" will appear. This Encryption page is not visible until a valid AES Licence Key has been applied to the terminal. Note that the terminal will require a reboot before the entered Licence Key is activated.

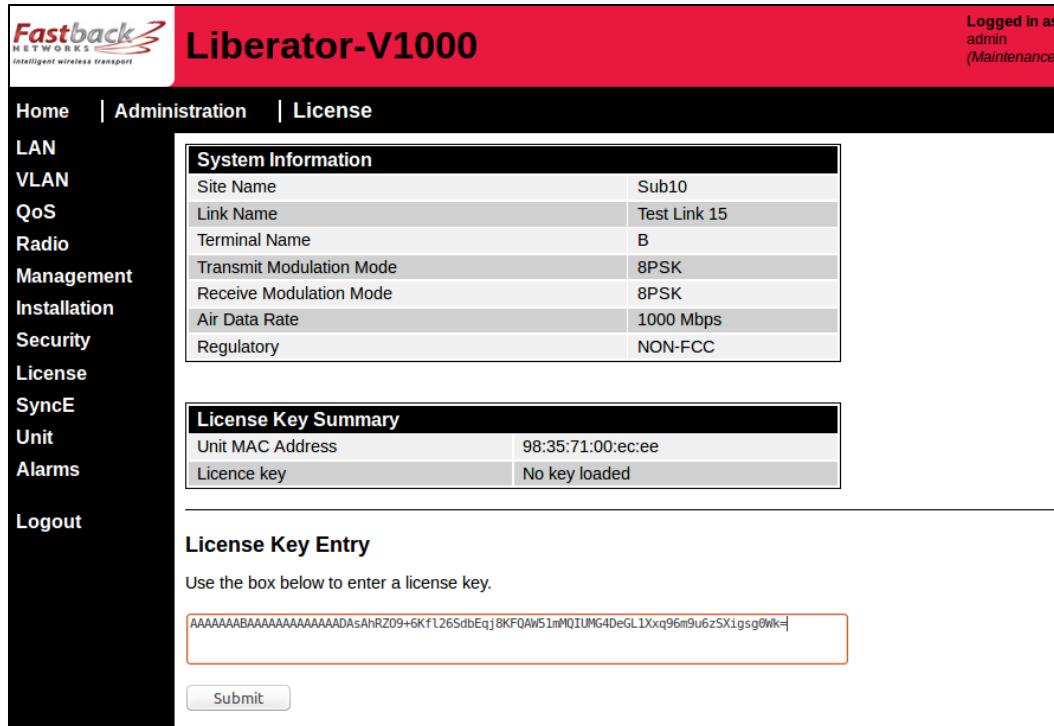


Figure 70 - License Key Entry Page

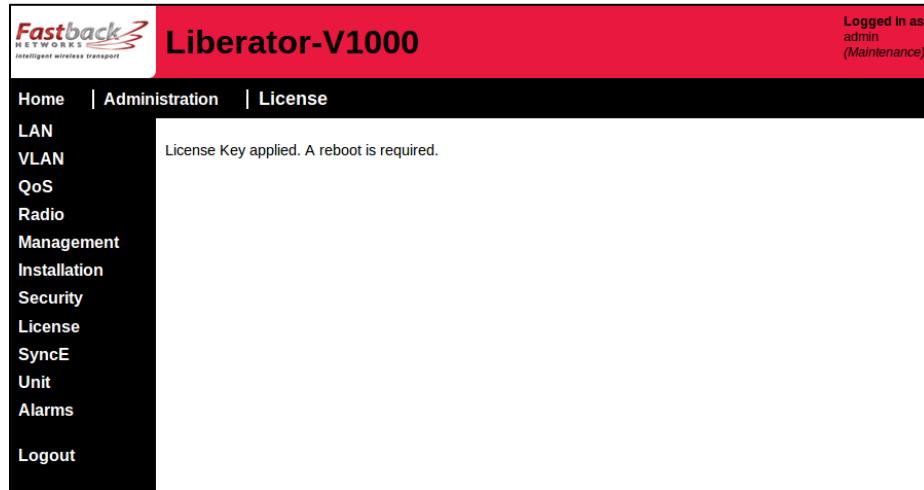


Figure 71 - A reboot is required to apply the Licence Key

5.4.11 Administration - Timing

This page allows the Timing parameters to be configured (SyncE only on Single-port versions, and both SyncE and IEEE1588v2 on Dual-port versions). Note that setting of these parameters should only be performed by a trained installer, as incorrect configuration may result in the link being dropped.

SyncE mode may be configured as either:

- **None:** This is the default setting, SyncE is disabled. This is the recommended setting unless a Primary Reference Clock input is available.
- **Provider:** Use this setting if a Primary Reference Clock or other Synchronous Ethernet timing signal is available on the Ethernet port. Note that only one end of the link may be configured as SyncE “Provider”, and the remote end must be configured as “Consumer” in this case.

- **Consumer:** Use this setting if the remote end of the link is to be configured as “Provider”. Note that only one end of the link may be configured as SyncE “Consumer”.

The screenshot shows the Liberator-V1000 web interface. The top navigation bar includes the Fastback Networks logo, the device name "Liberator-V1000", and a "Maintenance" link. The left sidebar lists various menu items: Home, Administration, Timing, LAN, VLAN, QoS, Radio, Management, Installation, Security, License, Timing Unit, Alarms, and Logout. The main content area is titled "Timing Status" and contains a table with four rows and three columns: SyncE Mode (Local: None, Remote: None), SyncE Status (Local: Disabled, Remote: Disabled), 1588 Local Mode (Local: None, Remote: None), and 1588 Local Status (Local: Locked, Remote: Locked). Below this is a section titled "Synchronous Ethernet" with a dropdown menu set to "Consumer". A note states: "Select "None" at both ends if there is no primary SyncE reference clock available. Select "Provider Primary" only if the Primary Ethernet port timing is driven by a primary SyncE reference clock. Select "Provider Secondary" only if the Secondary Ethernet port timing is driven by a primary SyncE reference clock. Select "Consumer" only if the remote end of the link is a Provider. Only one end can be a Provider. Only one end can be a Consumer." A red warning message at the bottom of this section reads: "Warning: You may lose contact with the unit if you are not connected to a SyncE compatible source." The next section is titled "1588" with a dropdown menu set to "Transparent". A note states: "The clock setting must be replicated at the other end of the link. One end of the link must be set as SyncE Consumer when using a "Transparent" clock." At the bottom of the page is an "Apply" button.

Timing Status		
	Local	Remote
SyncE Mode	None	None
SyncE Status	Disabled	Disabled
1588 Local Mode	None	None
1588 Local Status	Locked	Locked

Synchronous Ethernet

Consumer

Select "None" at both ends if there is no primary SyncE reference clock available.
Select "Provider Primary" only if the Primary Ethernet port timing is driven by a primary SyncE reference clock.
Select "Provider Secondary" only if the Secondary Ethernet port timing is driven by a primary SyncE reference clock.
Select "Consumer" only if the remote end of the link is a Provider.
Only one end can be a Provider. Only one end can be a Consumer.

Warning: You may lose contact with the unit if you are not connected to a SyncE compatible source.

1588

Transparent

The clock setting must be replicated at the other end of the link.
One end of the link must be set as SyncE Consumer when using a "Transparent" clock.

Apply

Figure 72 - Timing Configuration Page (SyncE and 1588)

On the Dual-port version, it is necessary to choose the timing source port if Provider is selected (Primary or Secondary port for the Provider).

On the Dual-port version only, IEEE1588 mode may be configured as either:

- None (1588 not active)
- Transparent (1588v2 Transparent Clock, requiring that one end of the link must be configured with SyncE setting as “Consumer”).

5.4.12 Administration - Unit

This page allows the user to change the Site Name, Link Name, Terminal Name and also enable / disable the rollback function and the rollback timeout period. Always press “Apply” so that changes will take effect. The SNMP Service box must also be ticked on this page, in order to allow use of SNMP.

Unit Configuration	
Site Name	Sub10
Link Name	Test Link 15
Terminal Name	B
Enable Rollbacks	<input checked="" type="checkbox"/>
Rollback Timeout	180

Services	
SNMP	<input checked="" type="checkbox"/>

Figure 73 - Setting the Rollback function



Figure 74 - Icon Displayed When Rollback Is Enabled and a Critical Change Is Made on the GUI, showing timer countdown

5.4.13 Administration - Alarms

The unit has a number of default alarms which cannot be removed from the display (but can be disabled), and in addition the user can specify extra alarms: these can be added on the “Alarm Management” page, but they only take effect after pressing the “Apply” button. For each alarm, the type and severity can be changed, and there is also an option for sending a trap to SNMP and/or to Syslog. The “Alarm Management” page allows the user to create and configure alarms, see below.

The screenshot shows the Liberator-V1000 web interface under the 'Alarm Management' tab. On the left, a sidebar includes links for Home, Administration, Alarms, Alarm Management, Threshold Management, and Logout. The main content area is titled 'Alarm Management' and contains a table titled 'Alarm Names, Measurements and Notifications'. The table has columns for Alarm Name, Enable Alarm, Measured Object, Alarm State, Alarm Type, Severity, SNMP, Syslog, and Delete Alarm. It lists several fixed alarms: Rx Power Low, Vector Error High, MWU Temperature High, MWU Temperature Low, Radio Link Down, and Link ID Mismatch. Below the table are 'Apply' and 'Refresh' buttons. At the bottom, there's an 'Add New Alarm' section with a text input field containing 'RadioReceivePower', a dropdown menu, and an 'Add' button.

Alarm Name	Enable Alarm	Measured Object	Alarm State	Alarm Type	Severity	SNMP	Syslog	Delete Alarm
Rx Power Low	<input checked="" type="checkbox"/>	RadioReceivePower	Clear	RadioAlarm	Critical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Vector Error High	<input checked="" type="checkbox"/>	RadioVectorError	Clear	RadioAlarm	Critical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
MWU Temperature High	<input checked="" type="checkbox"/>	MicroWaveUnitTemperature	Clear	UnitAlarm	Major	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
MWU Temperature Low	<input checked="" type="checkbox"/>	MicroWaveUnitTemperature	Clear	UnitAlarm	Major	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Radio Link Down	<input checked="" type="checkbox"/>	RadioLinkStatus	Clear	RadioAlarm	Critical	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Link ID Mismatch	<input checked="" type="checkbox"/>	RadioLinkIdMismatch	Clear	RadioAlarm	Warning	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Figure 75 - Alarm Management

An alarm is based on the monitoring and comparison of a measured object with configured thresholds. An alarm is persistent in that it can exist in a raised state until it is later cleared. The attributes of an alarm for example the action taken, frequency of monitoring and values of thresholds are fully configurable.

The unit has a number of fixed alarms by default. The attributes of a fixed alarm can be configured except for the name and the monitored object; a fixed alarm cannot be deleted. In addition to fixed alarms the user can create user defined alarms. A user defined alarm is fully configurable including the name and measured object.

5.4.13.1 Alarm Names, Measurements and Notifications - Configure alarm attributes.

- **Alarm Name** – Identifies the alarm (cannot change fixed alarm names)
- **Enable Alarm**
 - Enabled Measured object is monitored and alarm state will be raised or cleared according to configured thresholds
 - Disabled Measured object is not monitored, and alarm state is unknown
- **Measured Object** The parameter in the unit subject to monitoring and threshold comparison
- **Alarm State** Colour coded state showing severity for raised alarms
- **Alarm Type** Defines the type of alarm Unit, Radio or Ethernet and defines type of SNMP trap sent
- **Alarm Severity** The severity indicates the importance of the alarm
- **Measured Object** The parameter in the unit subject to monitoring and threshold comparison
- **SNMP** An SNMP trap is sent when alarm state changes
- **SysLog** A line of Syslog is written when alarm state changes
- **Delete** Delete the alarm (only user defined alarms can be deleted)

A user-defined alarm can be added by selecting the name of the alarm and the measured object. The following example adds a user defined alarm to monitor the previous 15m average Radio Rx Power.

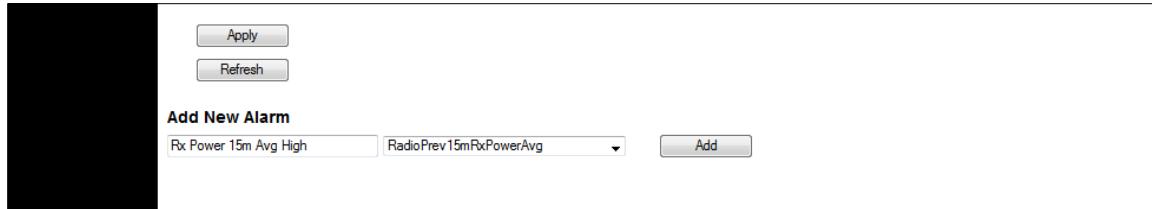


Figure 76 - Add User Defined Alarm

The new alarm is added to the Alarm Management table allowing alarm attribute configuration, note that monitoring interval and thresholds must be configured using the 'Alarm Threshold Management' GUI.

IMPORTANT: Before enabling the alarm it is recommended that the user configures the monitoring interval and threshold crossing attributes, because otherwise initial alarms may be raised and/or cleared using the default monitoring interval and threshold values, and this could result in initial spurious and incorrect alarm states. See 'Threshold Management' for configuration.

Alarm Management with a new alarm added to the table.

Alarm Name	Enable Alarm	Measured Object	Alarm State	Alarm Type	Severity	SNMP	Syslog	Delete Alarm
Rx Power Low	<input checked="" type="checkbox"/>	RadioReceivePower	Clear	RadioAlarm	Critical	<input type="checkbox"/>	<input type="checkbox"/>	
Vector Error High	<input checked="" type="checkbox"/>	RadioVectorError	Clear	UnitAlarm	Critical	<input type="checkbox"/>	<input type="checkbox"/>	
MWU Temperature High	<input checked="" type="checkbox"/>	MicroWaveUnitTemperature	Clear	UnitAlarm	Warning	<input type="checkbox"/>	<input type="checkbox"/>	
MWU Temperature Low	<input checked="" type="checkbox"/>	MicroWaveUnitTemperature	Clear	UnitAlarm	Warning	<input type="checkbox"/>	<input type="checkbox"/>	
Radio Link Down	<input checked="" type="checkbox"/>	RadioLinkStatus	Clear	RadioAlarm	Critical	<input type="checkbox"/>	<input type="checkbox"/>	
Ethernet Link Down	<input checked="" type="checkbox"/>	EthLinkStatus	Clear	EthernetAlarm	Warning	<input type="checkbox"/>	<input type="checkbox"/>	
Rx Modulation QPSK	<input checked="" type="checkbox"/>	RadioRxModulationMode	Clear	RadioAlarm	Major	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> Delete
Rx Power 15m Avg High	<input type="checkbox"/>	RadioPrev15mRxPowerAvg	Unknown	RadioAlarm	Warning	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/> Delete

Figure 77 - New Alarm Configure Attributes

Please also note that 'Alarm Type' configuration selects the type of SNMP notification sent when the alarm state changes. For further alarm behaviour configuration select 'Threshold Management'.

The alarms page: "Threshold Management" allows the user to configure monitoring intervals and threshold crossing behaviour.

Each alarm is listed as in 'Alarm Management'. The user is able to configure the behaviour of each alarm, see below.

Alarm Monitoring and Thresholds												
	Alarm Name	Measured Object	Observed Value	Monitor Interval (secs)	Raise Intervals	Clear Intervals	Raise Operation	Raise Threshold	Clear Operation	Clear Threshold	Alarm State	Alarm Time
Logout	Rx Power Low	RadioReceivePower	-41.0	1	3	5	LessThanOrEqual	-60.0	GreaterThan	-58.0	Clear	2000-03-06 13:31:10
	Vector Error High	RadioVectorError	-18.3	1	3	5	GreaterThanOrEqual	-12.0	LessThan	-14.0	Clear	2000-03-06 13:31:10
	MWU Temperature High	MicroWaveUnitTemperature	49	3	3	5	GreaterThanOrEqual	70	LessThan	68	Clear	2000-03-06 13:31:18
	MWU Temperature Low	MicroWaveUnitTemperature	49	3	3	5	LessThanOrEqual	-30	GreaterThan	-28	Clear	2000-03-06 13:31:18
	Radio Link Down	RadioLinkStatus	Up	5	3	3	NotEqual	radioLinkStateUp	Equal	radioLinkStateUp	Clear	2000-03-06 13:31:20
	Link ID Mismatch	RadioLinkIdMismatch	False	30	2	2	Equal	true	NotEqual	true	Clear	2000-03-06 13:32:00

Figure 78 - Alarm Threshold Management

5.4.13.2 Alarm Monitoring and Thresholds - Configure alarm monitoring and threshold attributes.

- **Alarm Name** Identifies the alarm
- **Measured Object** The parameter in the unit subject to monitoring and threshold comparison
- **Observed Value** The value of the measured object which caused the last alarm state change
- **Monitor Interval** The frequency in seconds that the measured object is checked against the configured thresholds
- **Raise Intervals** The number of consecutive monitoring intervals required where the observed measured object value has crossed the raise threshold before the alarm is finally raised.
- **Clear Intervals** The number of consecutive monitoring intervals required where the observed measured object value has crossed the clear threshold before the alarm is finally cleared.
- **Raise Operation** The comparison operator used when comparing the measured object's value against the raise threshold for determining the alarm is in the raised state.
- **Raise Threshold** The raise alarm threshold value
- **Clear Operation** The comparison operator used when comparing the measured object value against the clear threshold for determining the alarm is in the cleared state.
- **Clear Threshold** The clear alarm threshold value
- **Alarm State** Colour coded state showing severity for raised alarms
- **Alarm Time** The time of the last alarm state change

Note: For a measured object based on statistical history (e.g. 1m, 15m etc..) it does not make sense to set the monitoring interval to a value less than the update frequency of the statistic, e.g. for 15m stats set monitoring interval to 900 seconds.

5.5 Maintenance

The Maintenance pages are only accessible by users having the required access privileges, which are granted by an administrator.

5.5.1 Maintenance - Firmware Upgrade

This section allows the operator to upgrade a radio terminal's firmware. There are 2 memory banks. The firmware upgrade process will upload the new firmware to the INACTIVE memory bank. Therefore, before

performing a firmware upload, first be sure that a stable firmware version is in the ACTIVE memory bank. Click on the “Change” button in the “Switch bank” section to swap the active and inactive banks if necessary. The “Copy” button in the “Duplicate bank” section allows a firmware version to be copied into both banks if desired.

Firmware upload uses HTTP, simply choose the filename and press “Upload”. There is also the option to upload a firmware file using a TFTP server: in this case it is necessary to set-up a TFTP server, and then select the server IP address and filename.

The screenshot shows the Liberator-V1000 Firmware Upgrade interface. At the top right, it says "Logged in as: admin (Maintenance)". The left sidebar has links for Home, Maintenance, Firmware, Syslog, System config, Reboot, and Logout. The main content area has a red header bar with "Liberator-V1000". Below it, there's a "System Information" table:

Site Name	Sub10
Link Name	Test Link 15
Terminal Name	B
Transmit Modulation Mode	QPSK
Receive Modulation Mode	QPSK
Air Data Rate	1000 Mbps
Regulatory	NON-FCC

Below this is a "Firmware Banks" section with a table:

Bank	Version	Status	Selected
1	xx.xx.xx.xx	Inactive	
2	xx.xx.xx.xx	Running	selected

A note below the table says: "The firmware in bank 2 will be loaded following the next restart."

There are sections for "Switch bank" (with a "Change" button) and "Duplicate bank" (with a "Copy" button). Under "Upload New Firmware", there's a "Select a file to upload to the inactive bank" field with a "Browse..." button (showing "No file selected") and an "Upload" button. Under "Upload Firmware Via TFTP", there are fields for "Server IP" and "File Name", each with an "Upload" button below it.

Figure 79 - Firmware Upgrade page

Once initiated the firmware upgrade process should not be interrupted. Interrupting the process could result in a corrupt firmware image and a non-operational radio terminal.

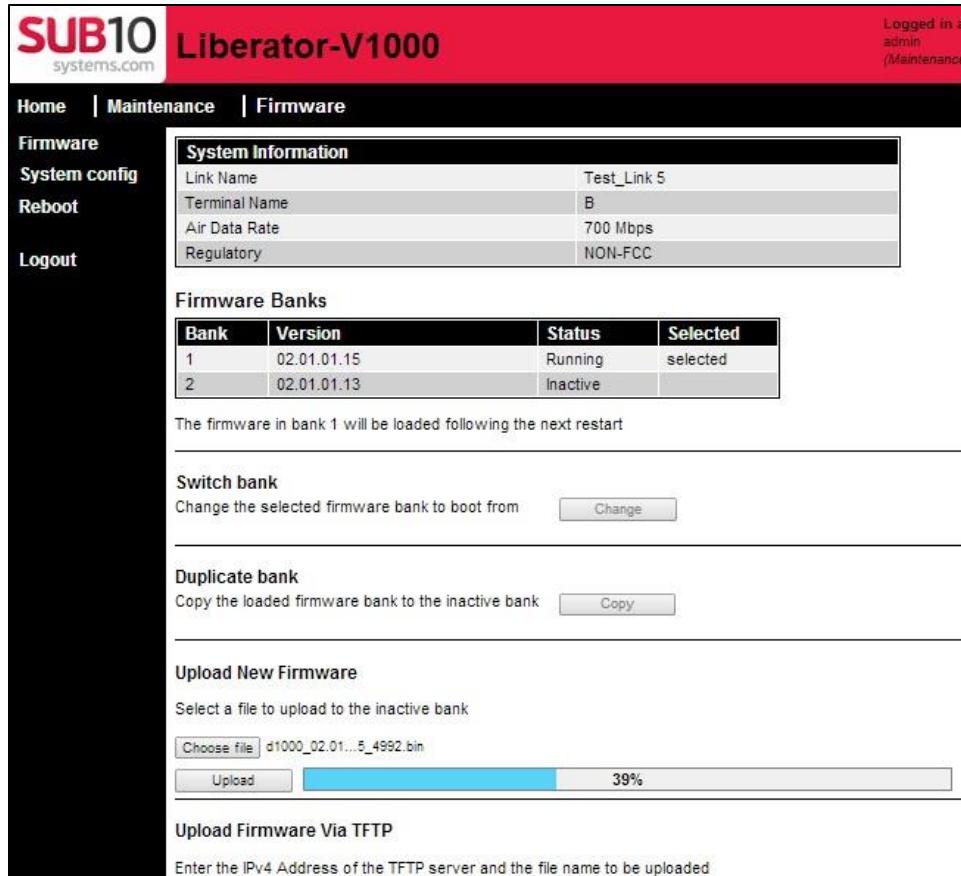


Figure 80 - Wait until Firmware has been uploaded

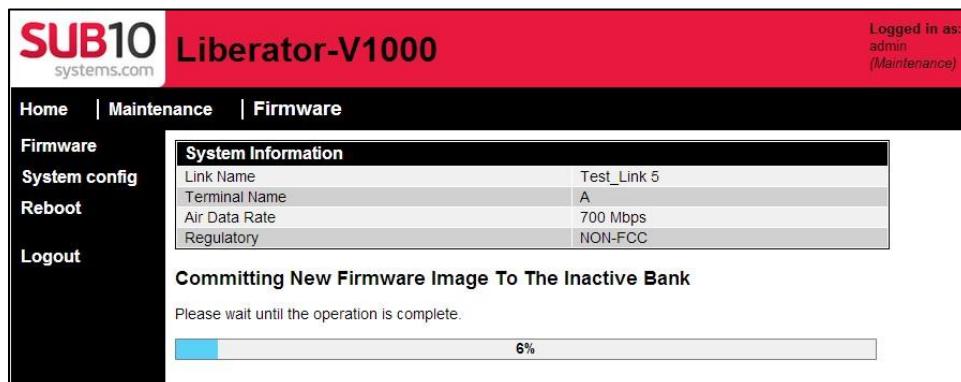


Figure 81 - Wait until Firmware has been committed to the Inactive Bank

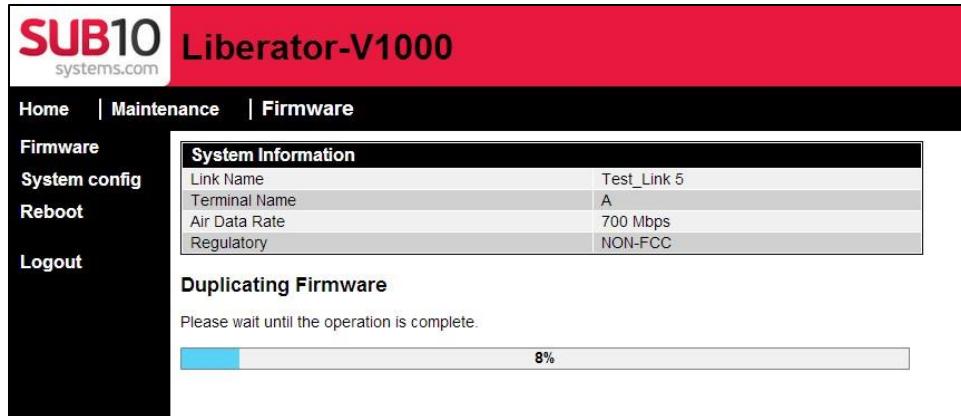


Figure 82 - Copy the Loaded Firmware to Inactive Bank

IMPORTANT : Note that after switching banks and rebooting, the rollback function will require confirmation to be made. Upon the next reboot and login the confirm / rollback option will appear.



If the bank change is not confirmed within the rollback expiry time after reboot (default 3 minutes), then the rollback function will rollback the change made to the Firmware bank which will cause the unit to reboot back to the original bank – this is a failsafe mechanism to protect the radio link in case the link does not re-establish after the Firmware bank change has been made.

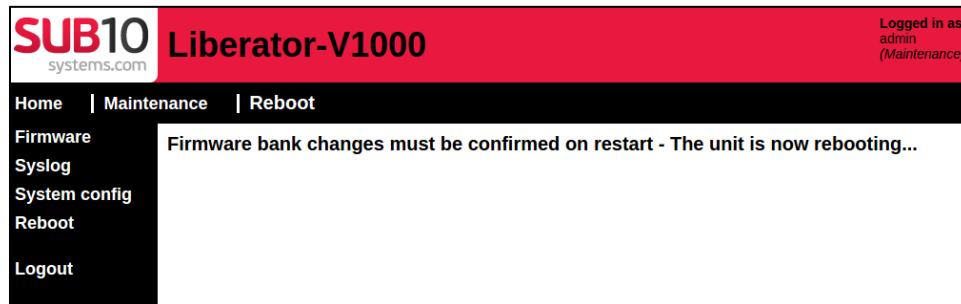


Figure 83 - Changes to Firmware Banks must be confirmed after reboot

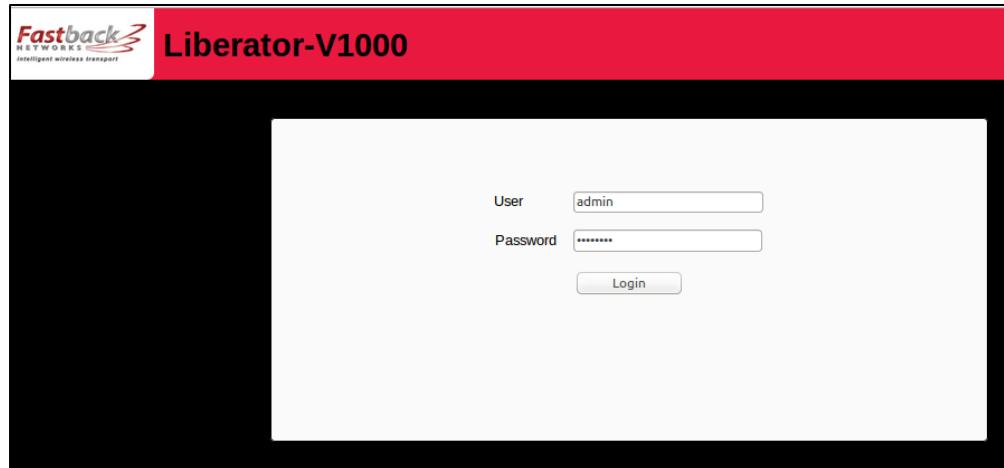


Figure 84 - Login page following reboot

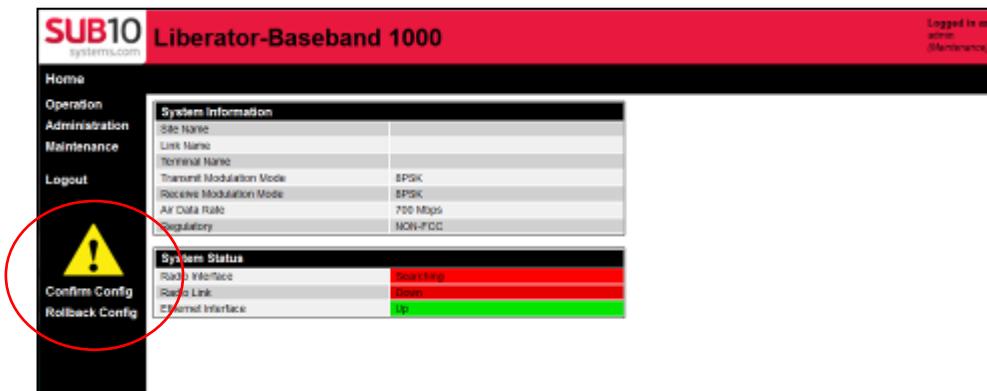


Figure 85 - Confirm / Rollback option appears on login following a switch bank and reboot

5.5.2 Maintenance – Syslog

The Syslog file can be viewed, and a copy can be saved (using the web browser cut-and-paste keys) for sending to Fastback Networks support in the case of any errors. It is always useful to check the Syslog file to be sure that the correct software version is running on the unit.

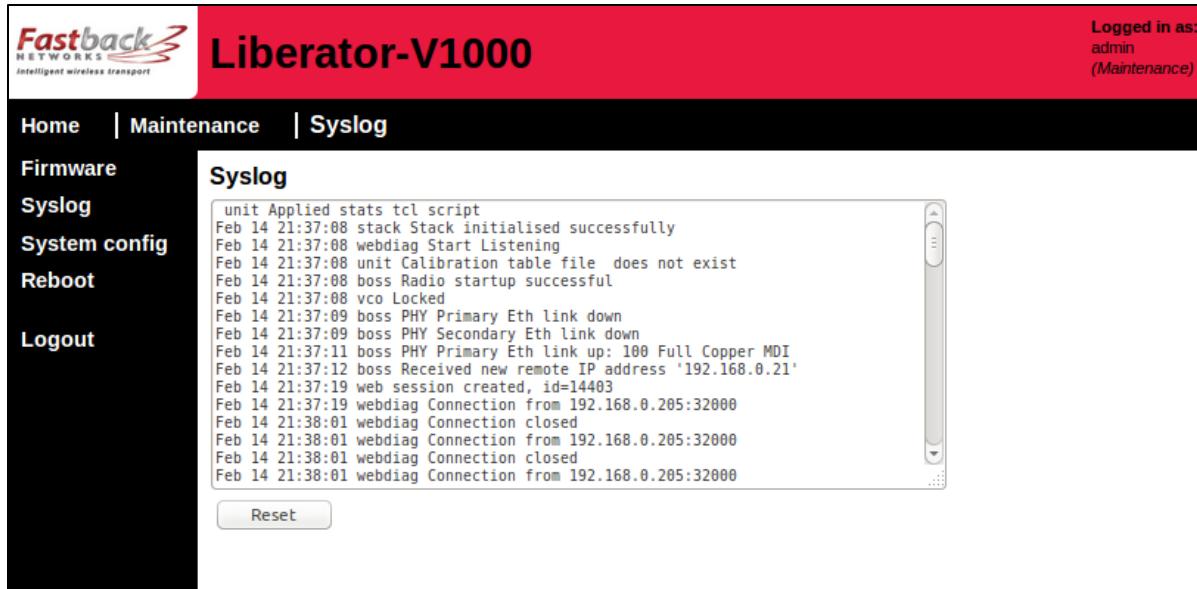


Figure 86 - Syslog page for sending to Fastback Networks support (use cut-and-paste)

5.5.3 Maintenance – System Configuration

The System Configuration page is used to Download (save) the existing user configuration, and also to Upload a previously-saved user configuration. This is very useful when a customer needs to configure multiple links with the same settings. There are also options to reset the statistics and counters, and also the alarms.

Fastback NETWORKS Intelligent wireless transport

Liberator-V1000

Logged in as:
admin
(Maintenance)

Home | Maintenance | System config

Firmware

Syslog

System config

Reboot

Logout

System Configuration

Configuration File Upload

Upload and process configuration (Only previously downloaded files are accepted). Requires a reboot.

No file selected.

Configuration File Download (Downloaded filenames contain the MAC address).

Download the configuration.

Reset Configuration

Click to reset the configuration to factory defaults.

Reset Statistics and Counters

Select Stats to Reset.

Reset Alarm Configuration

Select type of Alarm Configuration to reset.

Figure 87 - System Configuration page

5.5.4 Maintenance - Reboot

This page allows the user to reboot either the local or the remote radio terminal, by clicking on "Reboot". It is important to first check the Terminal Name on the top of this, page to ensure that the intended radio terminal is being rebooted (either the local or the remote end).

System Information	
Site Name	Sub10
Link Name	Test Link 15
Terminal Name	B
Transmit Modulation Mode	QPSK
Receive Modulation Mode	QPSK
Air Data Rate	1000 Mbps
Regulatory	NON-FCC

Reboot

Click to reboot the local unit

Click to reboot the remote unit

Figure 88 - Reboot page

Firmware bank changes must be confirmed on restart.
After a successful upgrade and reboot of a new firmware, it is recommended to duplicate the new firmware to the inactive bank.

The unit is now rebooting...

Figure 89 - Unit Rebooting

5.6 Logout

This page allows the user to Logout securely, and is necessary when multiple user accounts have been configured. Simply click "OK" to confirm that you wish to Logout.

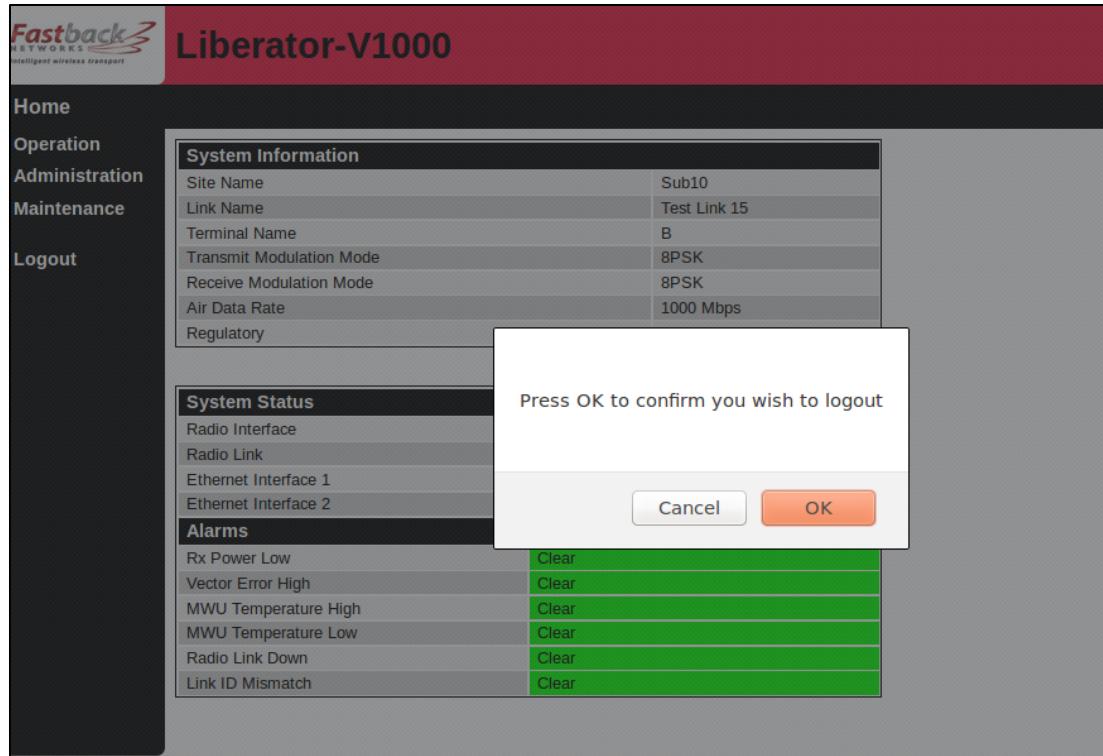


Figure 90 - User Account Logout Page

5.7 Configuration Rollbacks

Critical configuration items which may cause communication loss either over the management or radio link are subject to user confirmation via the web GUI. If a configuration confirmation is not received within a timeout period the configuration is rolled back to the previous values.

Rollbacks can be enabled or disabled and the rollback timeout can be configured using the Administration->Unit web GUI, see section 5.4.10. The confirmation/Rollback feature operates on configuration whether being changed from the Web GUI or over SNMP.

The table below lists all the configuration that requires a confirmation. If confirmation or rollback is not provided either via the GUI or via SNMP it will be reset to the previous values after the configured timeout. Confirmation or Rollback over SNMP is achieved by setting the MIB object 'sub10UnitMgmtTransaction'. The transaction status can be read by getting the MIB object 'sub10UnitMgmtTransactionStatus' (See Sub10 Systems enterprise MIB for more details).



<u>Configuration Item</u>	<u>Web Page</u>	<u>MIB Object</u>
Use DHCP	Administration / Management / IP	sub10UnitMgmtIpDhcp
IP Address	Administration / Management / IP	sub10UnitMgmtIpAddress
Subnet Mask	Administration / Management / IP	sub10UnitMgmtIpSubnetMask
Default Gateway	Administration / Management / IP	sub10UnitMgmtIpDefGateway
Enable VLAN Management	Administration / Management / IP	sub10UnitMgmtVlanState
Management VLAN Id	Administration / Management / IP	sub10UnitMgmtVlanId
Management VLAN Priority	Administration / Management / IP	sub10UnitMgmtVlanPriority
Management VLAN DEI	Administration / Management / IP	sub10UnitMgmtVlanDEI
SNMP	Administration / Unit	sub10UnitMgmtServiceSnmp
Read Community	Administration / Management / SNMP	sub10UnitMgmtSnmpReadCommunity
Write Community	Administration / Management / SNMP	sub10UnitMgmtSnmpWriteCommunity
Synchronous Ethernet	Administration / SyncE	sub10UnitMgmtSyncEMode
Encryption	Administration / Security / Encryption	sub10UnitMgmtEncryptMode
Enable VLAN Filtering	Administration / VLAN	sub10EthMgmtVlanFiltering
Allowed VLAN	Administration / VLAN	sub10EthMgmtVlanAllowedId
Enable Default VLAN	Administration / VLAN	sub10EthMgmtVlanDefaultEnabled
Default VLAN Id	Administration / VLAN	sub10EthMgmtVlanDefaultId
Default VLAN Priority	Administration / VLAN	sub10EthMgmtVlanDefaultPriority
Default VLAN DEI	Administration / VLAN	sub10EthMgmtVlanDefaultDEI
Enable ATPC	Administration / Radio	sub10RadioMgmtAPCMode
Transmit Power level	Administration / Radio	sub10RadioMgmtTxPowerLimit
Maximum Modulation Mode	Administration / Radio	sub10RadioMgmtModulationMode
Tx/Rx Frequencies	Administration / Radio	sub10RadioMgmtTxRxFreq
Switch Bank & Reboot ¹	Maintenance / Firmware	sub10UnitMgmtFirmwareSelectBank / sub10UnitMgmtFirmwareAction=fmw Reboot(2)

Table 3 - Configuration Confirmation / Rollback Table

[Return to Table of Contents](#)

¹ The configuration rollback option is required after a bank change and reboot. Upon the next restart login to the unit's web GUI to view the confirm / rollback option. **IMPORTANT NOTE:** A rollback (manually or automatic after timeout) after a firmware bank change and reboot will cause the unit to switch back to the original bank and reboot the unit again.

6. SNMP Management Interface

6.1 Description of SNMP

Note that the SNMP agent is not enabled by default, and it must be enabled from this GUI webpage before it can accept SNMP messages. The settings which must be enabled on the GUI before using SNMP are as follows:

Webpage: "*Admin/Management/SNMP*" -> Enable SNMP v1/2c and Traps

Webpage: "*Admin/Management/SNMP/SNMPv1/2c*" -> Set Trap destination(s)

Webpage: "*Admin/Unit*" -> Enable SNMP Service

The SNMP Agent is compatible with SNMPv1 and SNMPv2c. The SNMP Configuration is as follows:

- **Enable Agent** The agent will respond to SNMP v1/2c requests GET/SET/GET-NEXT and GET-BULK
- **Enable Traps** The agent will send traps to the configured trap destinations.
- **Trap Destinations** Up to three destination are possible, each requiring:
- **IPv4 Address** A valid IP address of the receiving management system.

Note: The IP address must be valid and reachable.

- **Community** The community string sent in each trap to this destination, this is used by management systems that require authentication using the trap community string.
- **Communities** SNMPv1/v2c community strings for read-only and read-write operations when accessing MIB object via an SNMP management system.
- **Read Community** The community string used for read access
- **Write Community** The community string used for write access

The following MIBs should be loaded into communicating network management tools:

Table 4 - V1000 MIB Compliance Table

MIB	Module	Usage
RFC1213-MIB	MIB-II	Standard MIB-II
IF-MIB	ifMIB	For SNMPv2c linkUp, linkDown notifications only interfaces supported as part of MIB-II.
SNMP-v2-MIB	snmpMIB	System group including SNMP resources. SNMP Traps including well known traps e.g coldStart.
SUB10SYSTEMS-MIB-201509240000Z.mib	Sub10Systems	The Sub10 Systems enterprise MIB for CM, FM and PM network management.
liberator-v320	LIBERATOR-MIB	Sub10 Systems V320 enterprise MIB for backwards compatibility. Note: V320 MIB compatibility mode is disabled by default. It can be enabled by setting the SUB10SYSTEMS-MIB object <i>sub10UnitMgmtSnmpV320Mib = stateEnabled(1)</i>

6.2 Administration Management – SNMP – Basic SNMP scripts

The following scripts give examples of SNMP usage

Firmware Upload (Prep)

*set sub10UnitMgmtFirmwareUplSvrIp = (The ip address of a tftp server which the unit will use to get the firmware image from)
 set sub10UnitMgmtFirmwareUplImage = (String firmware image name)*

Firmware Upload (Command)

set sub10UnitMgmtFirmwareAction = fmwUploadInactiveBank(4) (Uploads from the above tftpserver and loads into the inactive bank)

Firmware Upload (Monitoring the progress)

get sub10UnitMgmtFirmwareActStatus (values will change in order as the upload progresses as follows)...

*fmwUploadingImage(6)
 fmwUploadingImageComplete(7)
 fmwValidatingImage(10)
 fmwImageValidateSuccess(11)
 fmwUploadWritingBank(8)
 fmwUploadWritingBankComplete(9)
 mwUploadSuccess(1)*

Error states

*fmwUploadFailed(2)
 fmwUploadTimeout(3)
 fmwUploadFileNotFound(4)
 fmwUploadInvalid(5)
 fmwImageValidateFailed(12)*

During sub10UnitMgmtFirmwareActStatus = fmwUploadWritingBank(8)....

get sub10UnitMgmtFirmwareActProgress (An incrementing % from 0 - 100 indicating the progress of the bank writing)

The Bank being loaded

get sub10UnitMgmtFirmwareToBank

Change Bank and Reboot

set sub10UnitMgmtFirmwareSelectBank = (1 or 2) which is the inactive bank and should be the same as sub10UnitMgmtFirmwareToBank set during the upload.

set sub10UnitMgmtFirmwareAction = fmwReboot(2) (the unit will now reboot so you will lose connectivity - Check for ColdStart Trap from the Unit)

On successful restart Confirm Firmware Upgrade (important to do within 3 minutes)

get sub10UnitMgmtTransactionStatus

If the value = transStatusActive(2)

set sub10UnitMgmtTransaction = transactionCommit(2) (This confirms the upgrade and avoids rollback to previous firmware after 3 minutes)

get sub10UnitMgmtTransactionStatus (should be = transStatusCommitted(3))

License

set sub10UnitMgmtLicenseKey

Encryption

set sub10UnitMgmtEncryptKey = (The user input string as currently entered in the GUI)

set sub10UnitMgmtEncryptMode = encryptNone(0) or encryptAES256CBC(1)

Also recommend setting the following

sub10UnitMgmtTerminalName (unique to unit)

sub10UnitMgmtLinkName (unique to Link - this is not the LinkId)

sub10UnitMgmtSiteName (unique to geographical site)

sub10UnitMgmtContactName (usually same in all units but dependent on customer's support process)

[Return to Table of Contents](#)

Appendix A - Technical Information

A 1. Troubleshooting

This chapter provides solutions to problems that can occur during the installation and operation of the Liberator-V1000. It covers various aspects of installation and network setup.

Note: Each of the following points must be checked at both ends of the link. Start by running the entire procedure on one side (e.g. Terminal A). If this does not solve the problem, repeat all the steps at the opposite terminal.

1.1. Power and Network Connection

You must verify that the terminal is connected to the power. The PoE injector must be installed and plugged in. Go to the terminal, disconnect the RJ-45 connector and verify if there is power in the cable using a PoE++ tester.

WARNING: It is strongly advised that the mains power supply should be disconnected before making or breaking the CAT5e drop-cable connection between the PoE++ supply and the radio terminal (Outdoor Unit). If it is not possible to disconnect the mains power before making or breaking the CAT5e drop-cable connection between PoE++ and radio terminal, then ALWAYS first disconnect any network cable attached to the "IN" port of the PoE++ supply.

Take the network cable and plug it into a notebook or a network testing device and verify that there is a valid network connection. If there is any problem, please replace the cable and validate the connection again.

1.2. Network Configuration

Check that the PC's IP address is in the same range and subnet as the Liberator-V1000.

Note: The default IP address of the Liberator-V1000 is 192.168.0.21 and 192.168.0.22 for terminal A and B respectively. All terminals on the network must have a unique IP address in the same range, e.g. 192.168.0.X. Any terminal with identical IP addresses will not be visible on the network. They must all also have the same subnet mask (e.g. 255.255.255.0).

Ping the terminal to make sure that the Liberator-V1000 is responding. On a Windows PC, go to Start → Run → Type "Command" → Type "ping 192.168.0.21/22". A successful ping will generate four replies. As soon as the network configuration is correct you can access the GUI (Graphical User Interface) and check the settings according to the section titled "Factory-Defaulting a Terminal".

If a Management VLAN is enabled, then it will be necessary to set-up the communicating PC / laptop / network device with the same VLAN ID, in order to communicate with the V1000 management agent.

1.3. Misalignment

On the Installation screen you see the signal strength in dBm (e.g. -30 dBm). The correct RSSI value can be obtained from the Sub10 Systems Link Availability Calculator. If the value is more than 5dB below the Link Availability Calculator value, then the antenna is not properly aligned to receive the signal. You therefore need to re-align the terminal to its opposite terminal (please follow the instructions in the section titled "Antenna Alignment").

1.4. Mixed radio terminals

It is not possible to mix Single-port and Dual-port terminals.

1.5. Encryption settings

If AES encryption is used, then it must be enabled on both ends of the link, and the same encryption key used on both ends, or else no data will pass over the link.

A 2. Specifications

2.1. Physical Size of ODU Terminal

All dimensions are in millimetres. Dimensions are approximate with accuracy limited to +/- 3mm, and should be used for information purposes only.

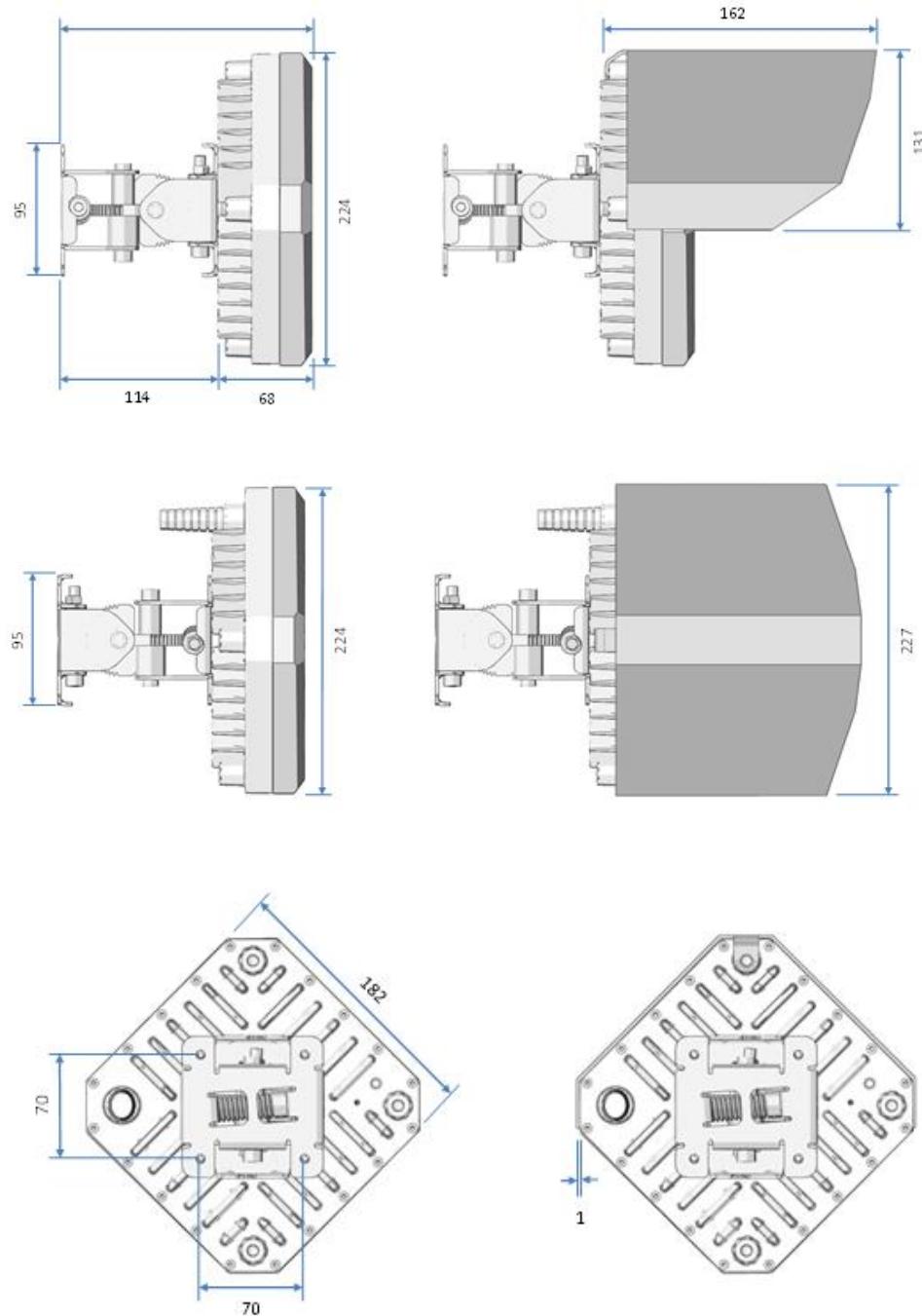


Figure 91 Dimensions of Single-port radio terminal in mm.

The Dual-port radio terminal has the same outer dimensions.

Liberator-V1000 User Manual
Appendix A – Technical Information

2.2. General System Information - Technical Specifications for V1000:

Modulation	QPSK and 8PSK
Range	QPSK: up to 800m, 8PSK up to 450m
Ethernet throughput (full duplex)	700Mbps QPSK and 1Gbps 8-PSK (Licence Key may be required)
Max Tx Power (at antenna port)	QPSK: +7.5dBm (FCC) and +6dBm (Rest of World)
Channel width	500 MHz
Antenna gain	38 dBi
FEC	Reed-Solomon
Availability	Up to 99.999% (use Liberator-Predict Link Availability Calculator)
MTBF	25 years
Wind load	160 km/h (operating) and 200 km/h (survival)
Ethernet frame size	64 up to 2048 Bytes (current software) and up to 9600 Bytes (future)
Latency	< 250 microseconds (single-trip delay)
VLAN support	IEEE 802.1Q
QoS	8 queues using VLAN PCP bits (current software) Flow control, 802.1p, DiffServ (future software release)
QoS Scheduling	SP (current software), WFQ (future software release)
Network management	SNMP v1, v2c and SNMP v3
Encryption	AES-256 encryption upgradeable with licence key in countries where authorised. Requires an AES Licence Key and AES-capable hardware. Max encrypted capacity is 700Mbps full-duplex.
GUI	HTTP web-browser (current software)
Interface	1000 Base-T
Drop cable	Cat5e, 100 metres max length
Connector	Single-port version: RJ45 plug (outdoor Gigabit Ethernet seal kit included) Dual-port version: 2 x GigE copper ports, and 1 x optical SFP port
Voltage alignment port	Waterproofed QMA socket
ODU Terminal dimensions	182 x 182 x 68mm
Power supply	Power Over Ethernet ("Ultra-PoE" / PoE++), consumption 35W
Operating temperature	-40°C to +55°C
Environmental	IP66 and IP67 (waterproof and dustproof)
Regulatory approvals	Safety: IEC60950-1/-22 and EN50385(2002) EMC: EN301 489-1/-4 Radio: EN302 217-3 FCC: CFR 47, Part 15 approved IC: In process for certification
Regulatory information	Emission designator: 500MG1D ETSI Spectral Efficiency Class: Class 2 (QPSK) and Class 3 (8PSK)

Please use the Liberator Predict Link Availability Calculator (free download from the Fastback Networks website), for a prediction of the V1000 link performance at your precise geographic location.

2.3. RSSI DC Voltage vs Received Power

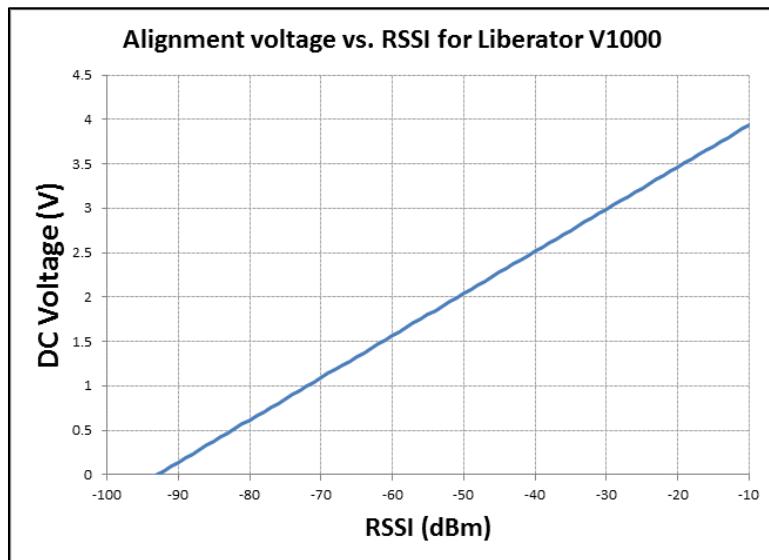


Figure 92 - Alignment voltage measured on Voltmeter for a given RSSI

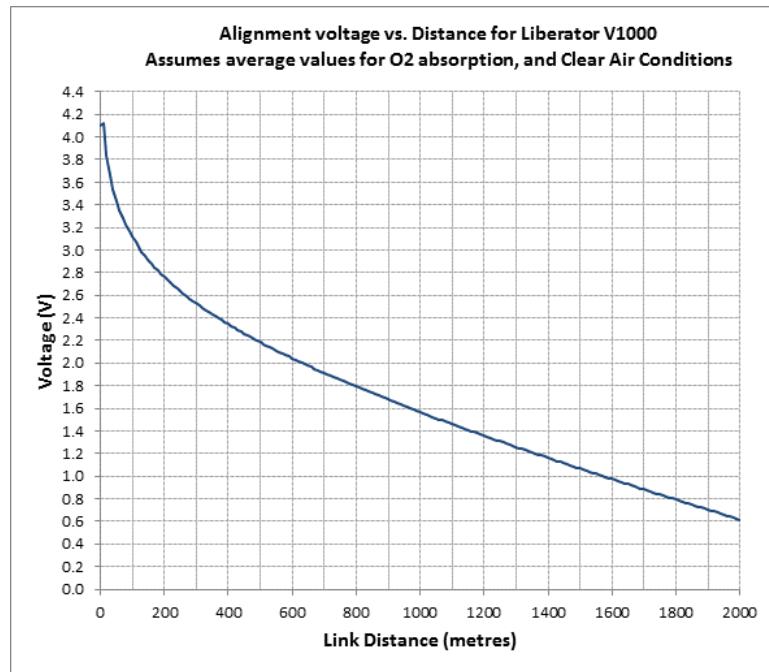


Figure 93 - Alignment Voltage vs. Distance for Liberator-V1000 in Clear Air Conditions

Note: Always use Liberator Predict Link Calculator for most accurate voltage based on geographic location.

[Return to Table of Contents](#)

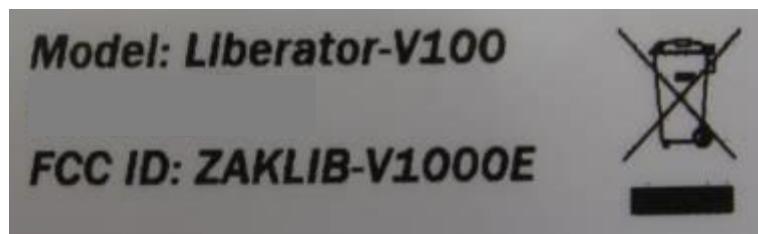
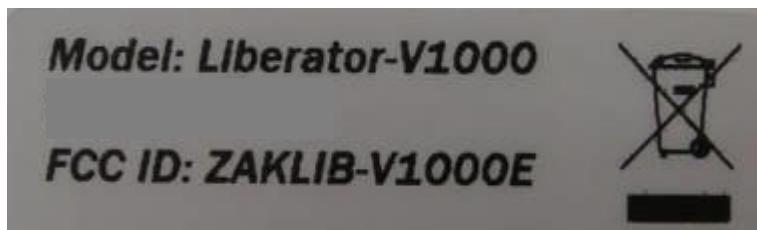
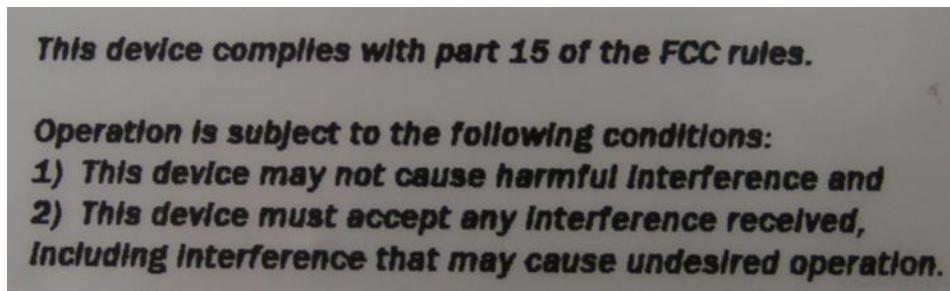
Appendix B – Regulatory Information

B 1. FCC Statement

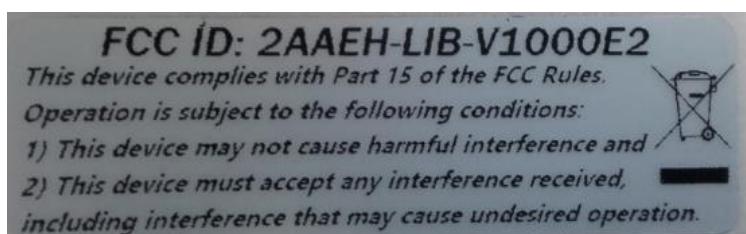
1.1. Regulatory Statements and Labels

The Liberator-V1000 Single-port (and Liberator-V100) have been certified as compliant with the FCC Rules under Part 15.255 and have been assigned the same FCC ID:ZAKLIB-V1000E as they use common hardware.

The following labels are affixed to the product in clearly visible locations to reflect this Certification.



The Liberator-V1000 Dual-port has been certified as compliant with the FCC Rules under Part 15.255 and has been assigned FCC ID: 2AAEH-LIB-V1000E2, and the label below is affixed to the Liberator-V1000 Dual-port radio terminal.



NOTE: The installer/user must not make any changes to the products operation without the express approval of Fastback Networks / Sub10 Systems Ltd., as unauthorised changes will invalidate the certification and may lead to action by the FCC.

Liberator-V1000 User Manual
Appendix B – Regulatory Information

1.2. Human Exposure to Non-Ionising Radiation in the USA

There are regulations defining limits for exposure of the general public to non-ionising radiation which is produced by radio transmitters. This is called "RF Exposure".

(a) Reference Documents

The documents applicable here are:

[1] US Code of Federal Regulations, in particular the policies, guidelines and requirements in Part 1 of Title 47 of the CFR. See (www.fcc.gov)

[2] Guidelines and recommendations for evaluating compliance contained in FCC Bulletin 65

[3] Safety Code 6 on the Health Canada Website www.hc-sc.gc.ca/

(b) Recommended separation distance

The radio terminal and antenna should always be mounted in such a way as to prevent human exposure to radio-frequencies, by ensuring that the following minimum safety distances are observed: Safety Distance = 1 metre on boresight. The antennas MUST be positioned to ensure that a minimum separation distance of 1 metre on antenna boresight is maintained between the installer or user and the antennas. The antennas MUST be positioned to ensure that no human being could be reasonably expected to come within 1 metre of the antenna during normal operation of the radio equipment.

B 2. Industry Canada Statement

The Liberator-V1000 is currently being processed for certification with Industry Canada.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

- (1) this device may not cause interference, and
- (2) this device must accept any interference, including interference that may cause undesired operation of the device

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante."

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

- (1) l'appareil ne doit pas produire de brouillage, et
- (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

[Return to Table of Contents](#)

Appendix C – Contact Information

Technical Assistance

Installers and users please visit the Fastback Networks Support website:

<http://support.fastbacknetworks.com/> ; Or contact - support@fastbacknetworks.com by email.

Sales & General Product Information

Customers please visit the Fastback Networks website:

<http://www.fastbacknetworks.com/> ; Or contact - info@fastbacknetworks.com by email.

Our Address:

Fastback Networks / Sub10 Systems Limited

Ash House

Canal Way

Kingsteignton

Newton Abbot

TQ12 3RZ

United Kingdom

Tel: +44 (0) 1626 818520

[Return to Table of Contents](#)