Newtec

M6100

User Manual

M6100 Broadcast Satellite Modulator

R1.4

V1.4

Table of Contents

1 Copyright

Newtec Cy N.V.

Laarstraat 5

9100 Sint-Niklaas, Belgium

tel: +32 (0)3 780 65 00

fax: +32 (0)3 780 65 49

www.newtec.eu

sales@newtec.eu

2 EU Compliancy Statements

2.1 Radio and Telecommunications Terminal Equipment (R&TTE) Directive 1995/5/EC

We,

Declare that the following product:

- Product number: M6100
- Type identifier: NTC/2353

to which this declaration relates is in conformity with the essential requirements of European Union Directive 1999/5/EC Radio and Telecommunication Terminal Equipment Directive Essential Requirement 3.1(a), 3.1 (b), 3.2.

Done at St-Niklaas, on August 7, 2014

Serge Van Herck,

CEO

Newtec Cy N.V.

Laarstraat 5

B-9100 Sint-Niklaas

Belgium.

Tel: +32 (0)3 780 65 00

Fax: +32 (0)3 780 65 49

2.2 EMC Information

Relevant EMC information (to FCC rules)

This equipment has been tested and was found to comply with the limits for a class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and radiates radio frequency energy. If not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications.

Note that, if coaxial cables are connected to the ASI-type interfaces, these cables must be double shielded in order to keep the installation compliant with FCC rules.

Do not operate this equipment in a residential area, as it is likely to cause harmful interference. When this is the case, you will be required to correct the interference at your own expense.

2.3 Restriction of Hazardous Substances Directive (RoHS) (Directive 2011/65/EU)

The undersigned hereby confirms the following statement:

We hereby declare that this equipment is compliant to the RoHS Directive 2011/65/EU.

Done at St-Niklaas, on August 7, 2014

Serge Van Herck,

CEO

Newtec Cy N.V.

Laarstraat 5

B-9100 Sint-Niklaas

Belgium.

Tel: +32 (0)3 780 65 00

Fax: +32 (0)3 780 65 49

2.4 Registration, Evaluation and Authorization of Chemicals (REACH)

European Regulation N°1907/2006 "REACH" (Registration, Evaluation, and Authorization of Chemicals), came into force on June 1st, 2007. It aims at regulating the use of the chemical substances within the European Union.

We are committed to meeting our legal obligations under REACH, as a manufacturer of articles and as a downstream user of chemicals products.

In order to comply with the REACH regulation, Newtec Cy N.V. has put into place processes and procedures to ensure implementation and compliance with the regulation, especially the assessment of the presence of Substances of Very High Concern (SVHC's) and communication along the supply chain to both suppliers and customers.

All products manufactured by Newtec Cy N.V. fall under the category of Articles within the REACH Regulation and none of them present the notion of intentional release of SVHC's, therefore no obligation of registration applies.

Done at St-Niklaas, on August 7, 2014

Serge Van Herck,

CEO

Newtec Cy N.V.

Laarstraat 5

B-9100 Sint-Niklaas

Belgium.

Tel: +32 (0)3 780 65 00

Fax: +32 (0)3 780 65 49

2.5 WEEE – Waste Electrical and Electronic Equipment Directive

The undersigned hereby confirms the following statement:

We hereby declare that this equipment is compliant to the WEEE Directive 2012/19/EU.

Done at St-Niklaas, on August 7, 2014

Serge Van Herck,

CEO

Newtec Cy N.V.

Laarstraat 5

B-9100 Sint-Niklaas

Belgium.

Tel: +32 (0)3 780 65 00

Fax: +32 (0)3 780 65 49

3 Safety Regulations

Please read this chapter before you install and use this equipment.

To ensure your safety, the equipment has been designed to comply with the following safety standards:

Safety of Information Technology Equipment.

- IEC 60950-1:2006/A11:2009/A1:2010/A12:2011
- EN 60950-1:2006/A11:2009/A1:2010/A12:2011
- UL 60950-1, Second Edition
- CSA C22.2 N°. 60950-1-07.Second Edition

Before you start to install and operate the device, please make sure you observe the following points:

- The equipment described in this manual is designed to be used by properly trained personnel only. Only qualified personnel who are aware of hazards involved may adjust, maintain and repair the exposed equipment.

No operator serviceable parts inside. Refer servicing to qualified personnel.
To prevent electrical shock, do not remove covers.

- To use the equipment correctly and safely, it is essential that both operating and servicing personnel follow generally accepted safety procedures in addition to the safety precautions specified in this manual. Warning and caution statements and/or symbols are marked on the equipment when necessary. Whenever it is likely that safety protection is impaired, immediately switch off the equipment and secure it against unintended operation. Inform the appropriate servicing authority about the problem. For example, safety is likely to be impaired if the equipment fails to perform the intended measurements or shows visible damage.
- The only way to shut down the device is to disconnect the power cable from the power connector. Therefore make sure that the power cable is accessible and not obstructed when the device is operational. For more information please refer to section: *Power Connector. on page 22*

Additional safety requirements for Finland, Norway and Sweden

Telecommunication connections and cable distribution system.

Special conditions apply to the use of this equipment in Finland, Sweden and Norway due to different earthing arrangements in these countries. Therefore it is essential that the installation is done by authorized personnel and according to the national requirements only.

This equipment is specified for use in a restricted access location only, where equipotential bonding has been applied and which has provision for a permanently connected protective earthing conductor.

A protective earthing conductor must be installed by a Service Person.

Additional safety requirements for Norway and Sweden

Equipment connected to the protective earthing of the building installation through the mains connection or through other equipment with a connection to protective earthing - and to a cable distribution system using coaxial cable, may in some circumstances create a fire hazard. Connection to a cable distribution system has therefore to be provided through a device providing electrical isolation below a certain frequency range (galvanic isolator, see EN 60728-11)."

NOTE: In Norway, due to regulation for installations of cable distribution systems, and in Sweden, a galvanic isolator shall provide electrical insulation below 5 MHz. The insulation shall withstand a dielectric strength of 1,5 kV r.m.s., 50 Hz or 60 Hz, for 1 min.

Translation to Norwegian:

Utstyr som er koplet til beskyttelsesjord via nettplugg og/eller via annet jordtilkoplet utstyr - og er tilkoplet et kabel-TV nett, kan forårsake brannfare. For å unngå dette skal det ved tilkopling av utstyret til kabel-TV nettet installeres en galvanisk isolator mellom utstyret og kabel-TV nettet.

Translation to Swedish:

"Utrustning som är kopplad till skyddsjord via jordat vägguttag och/eller via annan utrustning och samtidigt är kopplad till kabel-TV nät kan i vissa fall medföra risk för brand. För att undvika detta skall vid anslutning av utrustningen till kabel-TV nät galvanisk isolator finnas mellan utrustningen och kabel-TV nätet."

3.1 Environmental

Operating the equipment in an environment other than that stated in the specifications also invalidates the safety compliance.

Do not use the equipment in an environment in which the unit is exposed to:

- Unpressurized altitudes higher than 2000 meters;
- Extreme temperatures outside the stated operating range operating temperature range 0 to + 50°C;
- Excessive dust;
- Moist or humid atmosphere above 85% RH;
- Excessive vibration;
- Flammable gases;
- Corrosive or explosive atmospheres;
- Direct sunlight.

Use a slightly damp cloth to clean the casing of the equipment. Do not use any cleaning liquids containing alcohol, methylated spirit or ammonia, etc.

3.2 Rack Mounting Instructions

- Elevated Operating ambient - If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature (Tma) specified by the manufacturer. 50°C.
- Reduced Air Flow - installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromized.
- Mechanical Loading - Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Circuit Overloading - Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.
- Reliable earthing - Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

3.3 Earth Ground

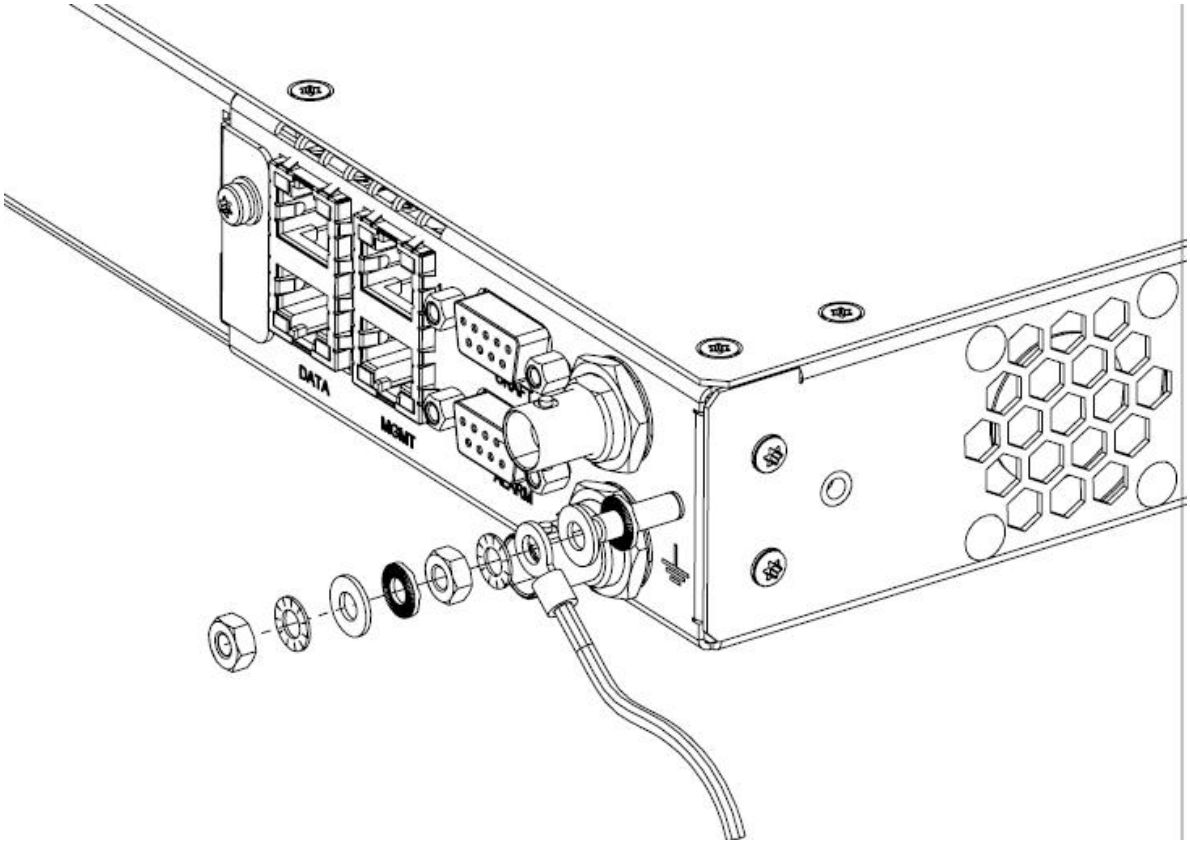
On the rear panel of the equipment an earth ground is available.

It is provided to:

- Ensure that all equipment chassis fixed within a rack are at the same technical earth potential. This is done by connecting a wire between the technical earth terminal and a suitable point on the rack.
- Eliminate the migration of stray charges when connecting between equipment.

In accordance to TNV-1 grounding requirements, the grounding thread of the device must be connected according to the local regulations.

The following figure shows the position and how to connect the earth ground.



4 Feedback

Newtec encourages your comments concerning this document. We are committed to providing documentation that meets your needs .

Please send any comments by contacting us at *documentation@newtec.eu*.

Please include document and any comment, error found or suggestion for improvement you have regarding this document.

5 About this Manual

This document is intended to help you to

- Understand the different possibilities of the M6100;
- Understand the basic features of the M6100;
- Find your way connecting and configuring the M6100.

5.1 Cautions and Symbols

The following symbols appear in this manual:

A caution message indicates a hazardous situation that, if not avoided, may result in minor or moderate injury. It may also refer to a procedure or practice that, if not correctly followed, could result in equipment damage or destruction.

A hint message indicates information for the proper operation of your equipment, including helpful hints, shortcuts or important reminders.

A reference message is used to direct to a location in a document with related document or a web-link.

5.2 Version History and Applicability

Document Version	Date	Subject	Comment
1.0	September 2013	M6100 Boadcast Satellite Modulator	• GUI update; • Support of S2-Extensions; • Switching between two M6100devices with different BISS SetupID is not possible; • BBF over IP; • DC-BUC Power on L-Band TX.
1.1	February 2014	M6100 Boadcast Satellite Modulator	• Remove BISS mode 0, 1 and E not applicable for this release. • Update MPE functionality description in section 11.7.
1.2	April 2014	M6100 Boadcast Satellite Modulator	• Update Physical Description Back Panel (section 7.2). • Update ASI Output, Signal Selection and Output Selection depending on the available ASI interfaces (four or six) on the back panel of the device (section 11.5).
1.3	April 2014	M6100 Boadcast Satellite Modulator	• Added a note that it is not advised to select low roll-off factors (20% and lower) in DVB-S and DVB-DSNG mode. (section 12.1.5)
1.4	August 2014	M6100 Boadcast Satellite Modulator	• Updated Traffic Classification, Shaping and Channels (section 11.7.4)

5.3 Related Documentation

- The M6100 Reference Manual describes the parameters available in the device;
- Device leaflet containing the specifications (We refer to *http://www.newtec.eu*);
- The System Integration Guide for M6100 describes how to integrate the device into a network management environment;

The user manual and more related documentation can be found on the CD-ROM that is delivered together with the device.

6 Introduction

6.1 Short Description

The Newtec M6100 Boadcast Satellite Modulator is the new generation DVB-S2, DVB-DSNG and DVB-S modulator specifically designed for broadcast direct-to-home, primary distribution to head ends and contribution of television and radio content. The modulator supports the S2 Extensions to achieve barrier-breaking efficiency.

The M6100 can be used in conjunction with set-top boxes; professional IRD's or professional satellite demodulators such as the MDM6100 and AZ910.

Delivering the Highest Uptime for Vital Links

Uptime and reliability are essential in the design of the modulator, taking a vital role in the satellite network. Input source redundancy, and the shortest redundancy switch-over times of modulators, operating both in 1+1 and N+1 topologies, are setting the standard in our industry.

Advanced capabilities such as a built-in MPEG Transport Stream analyzer, support of SMPTE 2022 FEC at the GbE inputs (for distributed IP head ends), and native support of Carrier ID according to the new DVB standard as well as in the transport stream NIT table. Special care was taken to cope with jittery transport stream over IP inputs. The six ASI ports allow for monitoring as well as operational ASI ports.

Get the Best Performance and Lower your Costs

The Broadcast Satellite Modulator performs among the best, offering unmatched bandwidth efficiency optimization options, thereby lowering overall Total Cost of Ownership. The fully automated operation of the field-proven Equalink® pre-distortion technology is now available for any satellite transmission application providing up to 10% bandwidth gains for single carrier per transponder constellations.

Clean Channel Technology™, in combination with S2 Extensions, improves satellite efficiency by up to 15%, thereby enabling much smaller carrier spacing.

Maximum symbol rates up to 72 Mbaud and modulations up to 64APSK (S2 extensions) combined with VCM (Variable Coding and Modulation) allow for maximum throughput in large contribution links. The availability of a DVB-S2 Mode Adaptation Input Interface (BaseBand Frames), combined with Newtec's AZ810 Stream Aggregator allows for the uplinking of up to 6 Transport Streams.

At the output of the Broadcast Satellite Modulator, the signal is available in IF or extended L-band (950 MHz-2150 MHz), providing a compact and cost effective solution. A switchable 10 MHz reference signal and optional 24V or 48V DC for an outdoor BUC is multiplexed on the L-band interface.

The Broadcast Satellite Modulator can be easily monitored and controlled via a comprehensive front panel menu, advanced web GUI, command line interface (CLI) as well as via SNMP protocol. This enables easy integration into any industry-standard EMS/NMS system.

Evolve Towards Tomorrow's Technology

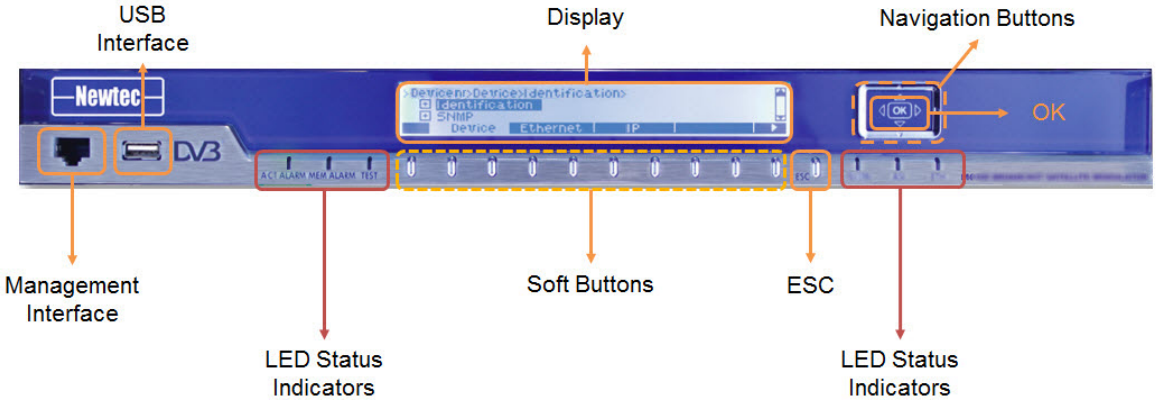
Built upon flexible and latest generation programmable technology, the Broadcast Satellite Modulator is a future-proof building block that lets any satellite network evolve to the next level of capabilities. A scalable, pay-as-you-grow, licensing and software upgrade mechanism facilitates the launch of new services, or last minute network design changes, without rebuilding the entire network infrastructure. Migration from ASI to GbE and IF to L-band or upgrade to S2 Extensions is facilitated by simple in-field installation of licence keys.

Additional capabilities such as DVB-S2 extensions and others are anticipated to become available on the platform as the standardization efforts materialize in the near future. The brand new DVB-CID carrier identifier is already available as a software option on the M6100.

7 Physical Description

7.1 Front Panel Description

The device can be configured, controlled and monitored using the front panel. The front panel consists out of the following parts.



For more information please refer to section: *How to Use the Front Panel. on page 53*

7.1.1 Display

The display consists of a 32 x 240 pixels LCD screen.

- The top rows indicates the tree menu pane;
- The bottom row indicates the root menu pane.

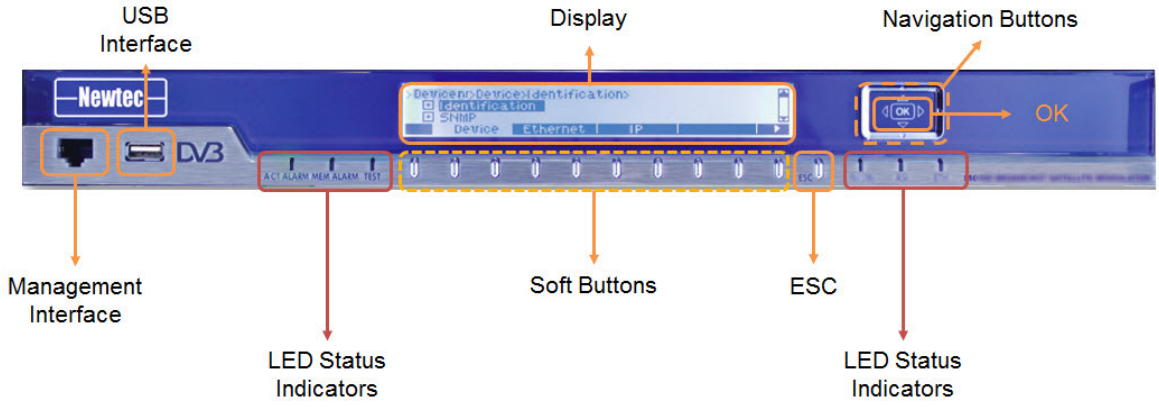
Menu Tree

The device management model is designed as a menu tree. The menu tree shows the organization of the parameters in the device. The tree is built up out of a root, branches, sub branches and leafs.

- Root: represents the complete device configuration;
- Branch/Sub branch: represents functional blocks that group leafs/parameters that are closely related to one another;
- Leafs: the leafs represent the parameters or commands that are used to perform a configuration.

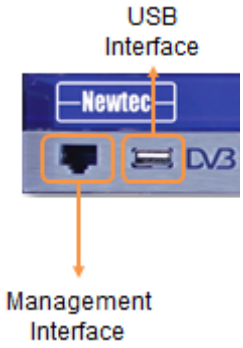
7.1.2 Soft Buttons and Navigation Buttons

Use the navigation button and soft buttons to navigate through the menu tree.



- The function of the soft buttons varies depending on the context. Their meaning is defined by the menu pane block setting atop of each button;
- Use the **navigation buttons** for navigating through the Tree menu pane;
- Use the **OK** button to confirm a selection;
- Use the **ESC** button to ignore a selection and to go up in the menu tree.

7.1.3 Front Panel Management Interface



The management interface allows the system administrators to manage the M6100 Boadcast Satellite Modulator and monitor its operation.

Note that this interface is disabled by default.

This connector has the same function as the management interface(s) on the back panel.

The management can also be done by using the GUI, CLI or SNMP. For more information please refer to section: *How to Manage the Device on page 30*

7.1.4 USB Interface

The USB interface is a flash drive connector that can be used to perform a license or software upgrade.

7.1.5 LED Status Indicators

The following table describes the LED indicators.

LED	LED Color	Description
ACT ALARM	Red	A general device or interface alarm is present on the device.
	Yellow	Alarms other than the general device alarm or interface alarm are present on the device.
	Green	There are no alarms present on the device.
MEM ALARM	Yellow	A memorized alarm is present on the device.
	Off	Indicates that all alarms are cleared, no memorized alarm is present on the device.
TEST	Green	Indicates that the internal PRBS generator is activated on the device.
	Off	The internal PRBS generator is not activated on the device.
Tx ON	Green	The device is transmitting.
	Off	The transmission is disabled.
ASI	Green	The incoming signal is valid.
	Red	Indicates an interface alarm.
	Off	The incoming signal is not valid.
ETH	Green	The incoming data signal is valid.
	Red	Indicates an Ethernet link failure on the MGMT and/or DATA interface(s).
	Off	The incoming data signal is valid.

7.2 Back Panel Description

The following figure shows the possible connections on the M6100. The back panel connections available depend on the specific hardware configuration of your device.

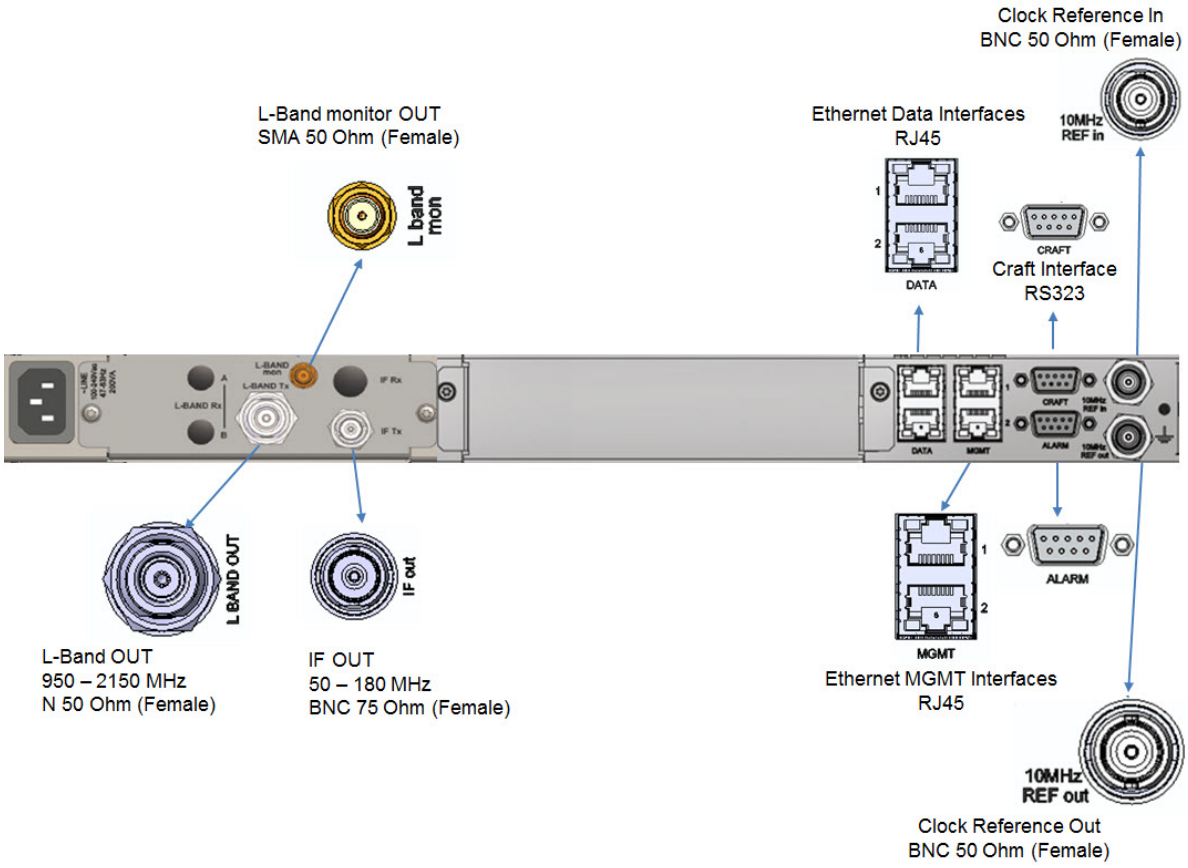
The maximum force that may be used to fix the SMA (L-Band monitor OUT) connector is restricted to 1.2Nm!

The maximum force for the other connectors is restricted to 1Nm!

When one of these limits is exceeded, the connectors can be damaged and the correct functioning of the connectors cannot be guaranteed.

Three major back panel configurations are available.

Default Hardware Configuration (Ordering number CH-01)

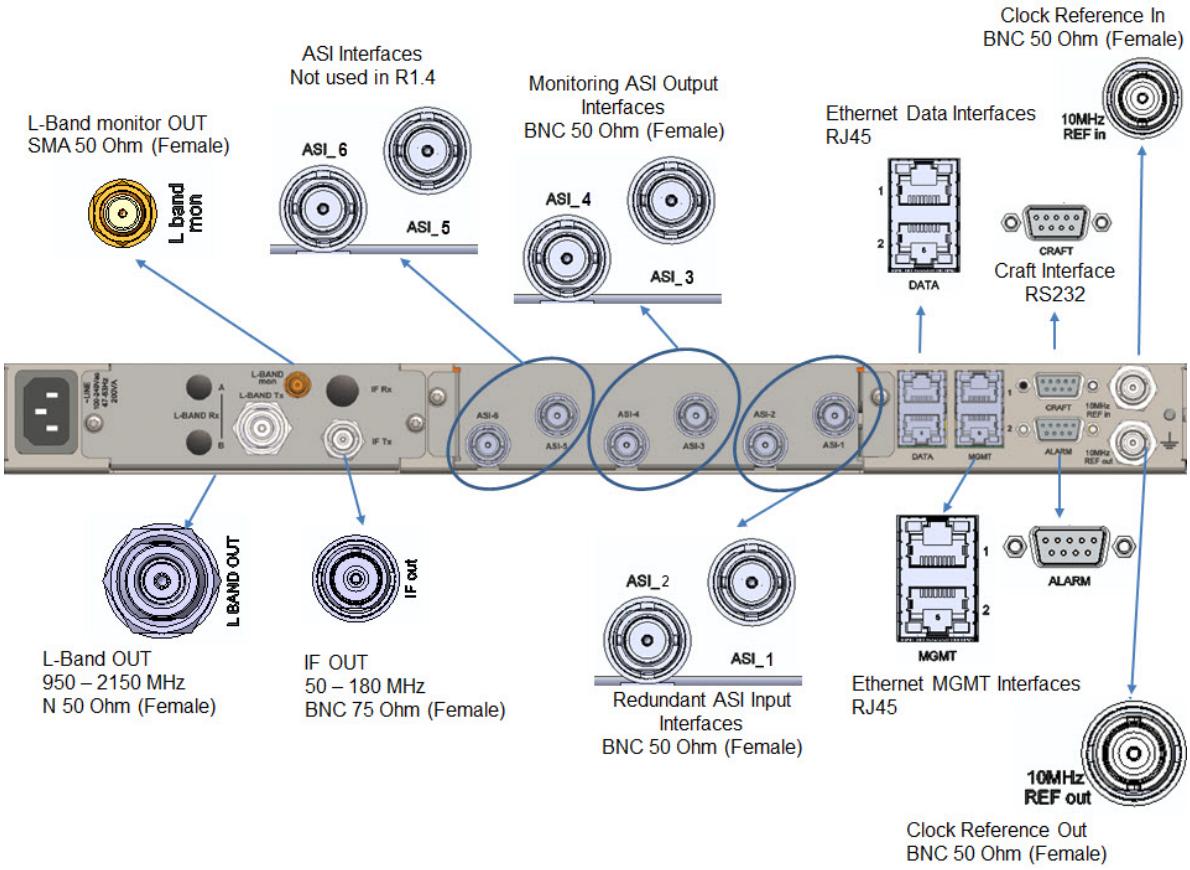


This configuration is used to perform TS over IP.

The license key VI-01 needs to be activated to enable TS over IP input interfaces.

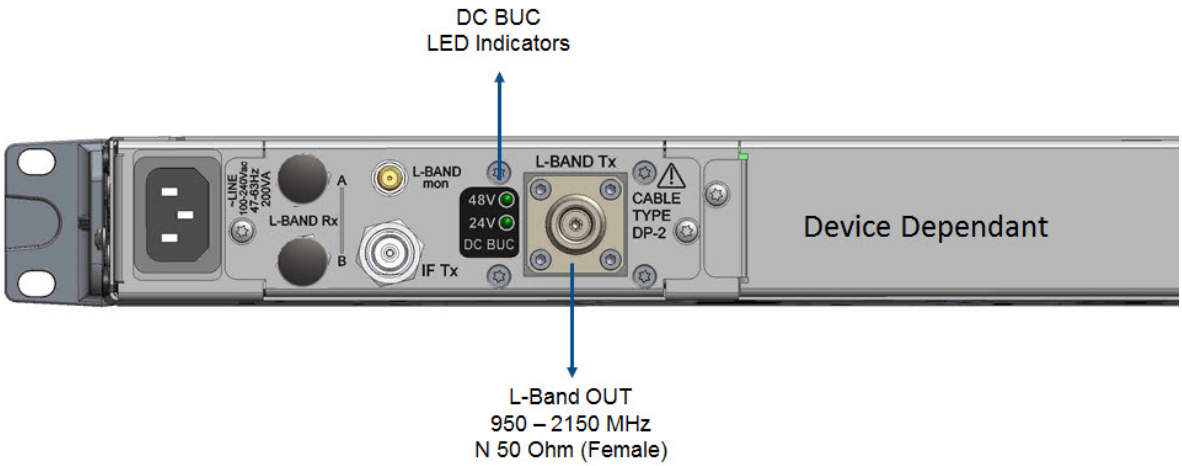
The 10MHz REF out is optional and is selected during ordering. (Ordering number is RO-01.)

Hardware configuration option with ASI inputs and outputs (Ordering number CH-01 and AS-02)



The 10MHz REF out is optional and is selected during ordering. (Ordering number is RO-01.)

Hardware configuration option with DC-BUC on L-Band TX (Ordering number OU-05 or OU-06)



7.2.1 Power Connector

This connector has a protective earthing incorporated.
Insert the mains plug only in a socket that has a protective earth contact.

Any interruption of the protective conductor inside or outside the device causes hazards or electrical shocks.

The only way to shut down the device is to disconnect the power cable from the power connector. Therefore, make sure that the power cable is accessible and not obstructed when the device is operational.

The power supply has the following specifications: 90-130 & 180-260 Vac, 105 VA, 47-63 Hz.

To have power redundancy, a dual power supply can be ordered (ordering nr. PS-01)

- It is advisable to connect the two mains plugs to two different power circuits, so the device remains operational if one of these circuits fails (for example: fuse blown).

The equipment with redundant power supply has more than one power supply cord. To reduce the risk of electric shock, disconnect two power supply cords before servicing.

7.2.2 Earth Ground

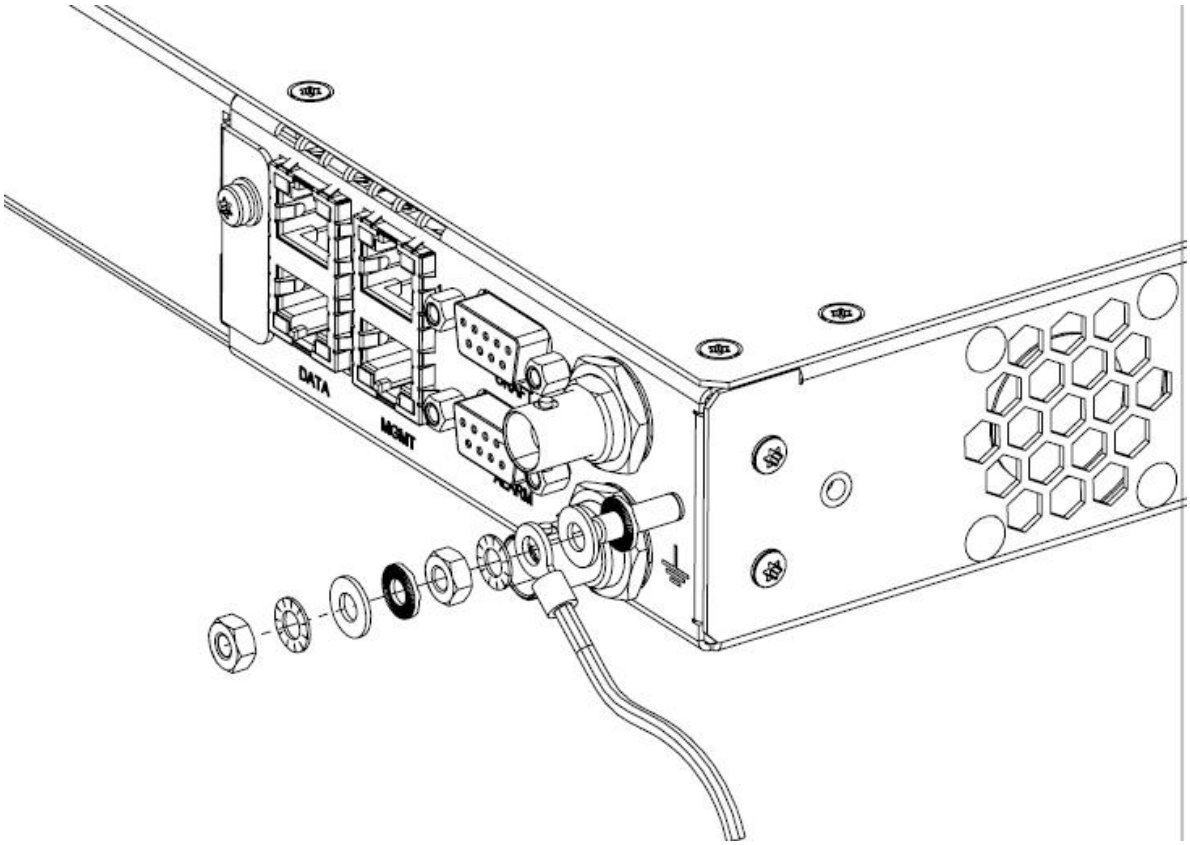
On the rear panel of the equipment an earth ground is available.

It is provided to:

- Ensure that all equipment chassis fixed within a rack are at the same technical earth potential. This is done by connecting a wire between the technical earth terminal and a suitable point on the rack.
- Eliminate the migration of stray charges when connecting between equipment.

In accordance to TNV-1 grounding requirements, the grounding thread of the device must be connected according to the local regulations.

The following figure shows the position and how to connect the earth ground.



7.2.3 Craft Interface

The **craft** interface is a SUBD 9 pin connector interface that can be used to manage the device using the command line interface (CLI). For more information please refer to section:
Command Line Interface (CLI) on page 59

It is used to control the device over RS232.

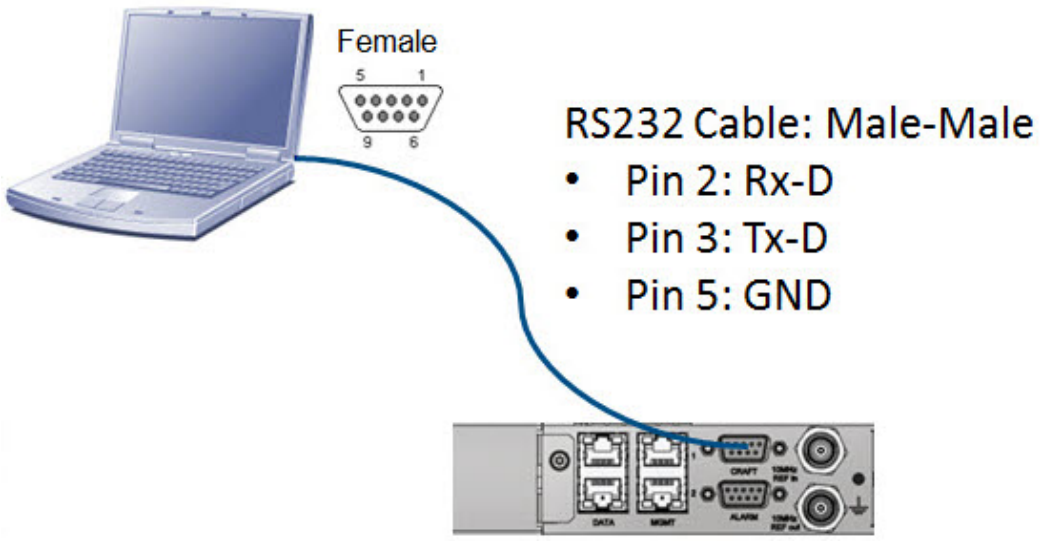
The line settings for the craft interface are:

- Speed 115200 baud;
- Eight data bits;
- No parity bit;
- One stop bit.

Use the following pin connections to create a crossover cable between the M6100 Boadcast Satellite Modulator and the managing device.

Pin	Name	Function
1		Not connected
2	Rx-D	Receive Data
3	Tx-D	Transmit Data
4		Not connected
5	GND	Shield ground
6		Not connected
7		Not connected
8		Not connected
9		Not connected

The following figure shows the craft interface connection.



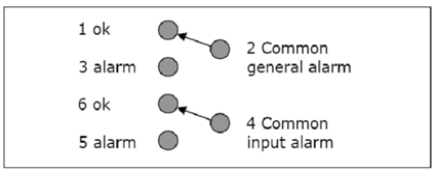
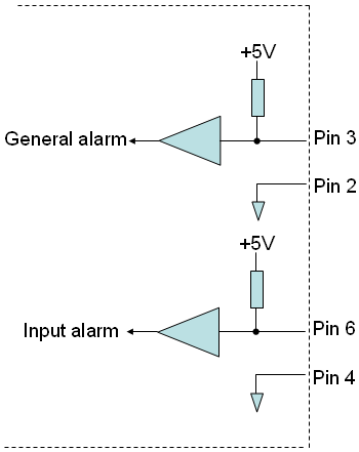
7.2.4 Alarm Interface

The alarm interface can be used to build up device redundancy switching systems.

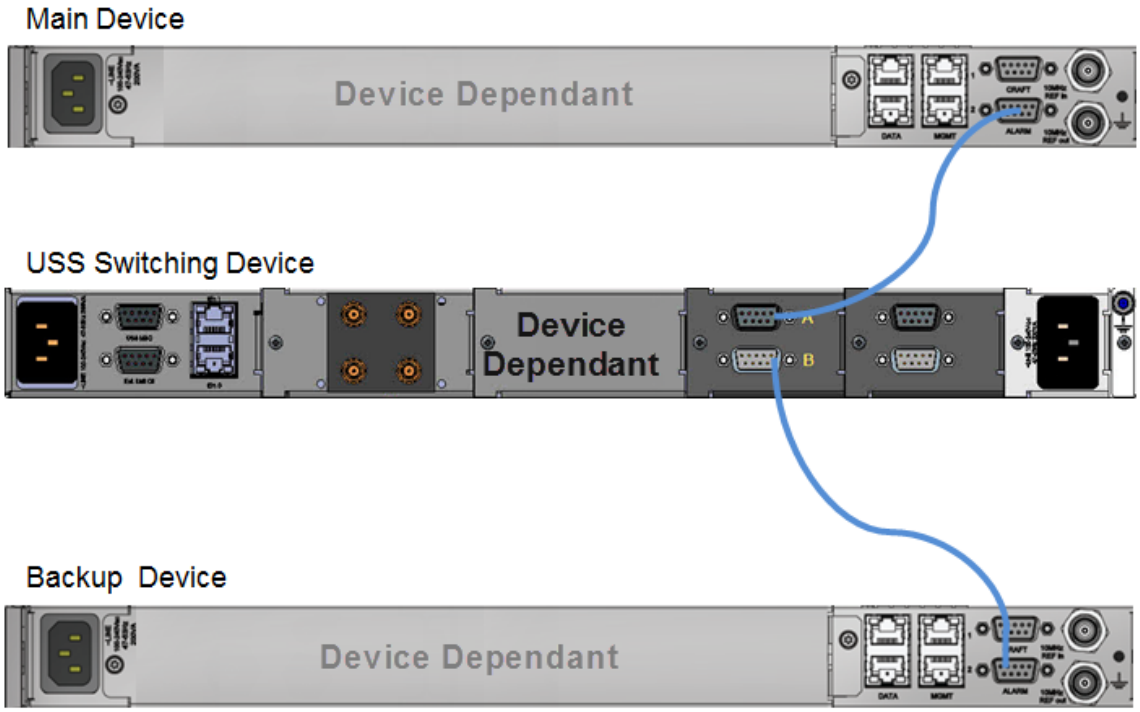
When using the AZ202 Universal Redundancy Switch it is not mandatory to use alarm contacts. The Universal Redundancy Switch can also gather the alarm status from the different pieces of equipment in the setup over the management interface. To enable device redundancy please refer to section: *Device Redundancy on page 107*

Connect the alarm interfaces.
The contacts are normally closed to insure that an alarm is generated when the alarm cables are removed.

Refer to the following figures for the pin layout:

Pin Layout	Technical Representation of the Pin Layout
	

The following figure shows how to connect the alarm cables in a 1+1 redundancy system.



8 Getting Started

Use this guide to configure the management IP Address of the device and save it as a boot configuration. Once this is done, it is possible to access the device using one of the following operational interfaces:

- GUI;
- CLI;
- SNMP.

Refer to the reference manual to check the factory default values of the device.

8.1 Set the Management IP Address

The factory default of the Mgmt IP Address is: 10.0.0.2/24 on Mgmt1 Ethernet interface.

» Insert the power cable to start the device;

» Wait until the welcome menu disappeared and the menu tree is displayed on the front panel;

» Select **Mgmt Itf** using the corresponding Soft Button;

» Navigate to **IP Address;**

» Press **OK** (to unfold the branch);

» Navigate to **Mgmt1;**

» Press **OK;**

» Press **OK** to select the IP Address/Prefix;

» Use the **Soft Buttons** to enter a new IP Address/Prefix;

» Press **OK** to confirm and save the setting;

» Connect an Ethernet cable between the Mgmt1 port on the back panel of the M6100 and the management PC. (The state indication on the front panel is changed from **off** to **on**).

Note that only device specific parameter settings are automatically saved.

All other parameters require an explicit save action!

To get an overview of the device specific parameters we refer to section *Configuration File on page 82*

Make sure that the management PC has access to this IP address or it belongs to this IP range.
If needed it is possible to configure the Mgmt Gateway.

To configure the Mgmt Gateway

» Navigate to **Mgmt Itf;**

» Navigate to **Gateway;**

» Enter the correct Gateway address;

» Click **OK.**

Now it is possible to access the device from a management PC.

8.2 Set Date and Time

It is advised to set the device date and time according to your time zone.

» Select **Device** from the corresponding soft button;

» Navigate to **Date and Time;**

» Press **OK** (to unfold the branch);

» Navigate to **Date or Time** and press **OK;**

» Use the navigation down button to display numerical values;

» Use the **Soft Buttons** to enter a new Date or Time;

» Press **OK** to confirm the setting.

8.3 Configure and Save

You can configure settings using the front panel, the graphical user interface (GUI) or the command line interface (CLI).

Please save to fix your configured settings.

To save settings via the front panel:

» Use the Soft Button Arrow and navigate to the right of the root menu pane and select **Actions;**

» Navigate to **Device Configuration Save** and press **OK;**

» Select the configuration file name and press **OK** to save the configuration.

9 How to Manage the Device

This section shows how the parameters in the device are ordered and managed according to your needs.
It also describes the different user profiles you can use to login and manage the device.

The device can be managed using one of the following physical interfaces:

- The front panel;
- The management Ethernet interfaces, used to work with a GUI (Graphical User Interface), CLI (Command Line Interface) or SNMP (Simple Network Management Protocol);
- The craft interface is used to work with the CLI.

9.1 Management Model / Menu Tree

The device management model is designed as a menu tree and a set of commands. The menu tree exposes the organization of the parameters in the device while the commands are used to execute actions other than simply setting or getting a parameter.

The menu tree is built up out of a root, branches, sub branches and leafs/parameters.

The menu trees of the GUI, front panel, CLI and SNMP are similar to one another.

Refer to the reference manual on the CD-ROM to get a full overview.

In some cases, there is a difference between the location of a parameter in the GUI and a location via the front panel.

The parameter location is displayed as follows:

M6100 >> Branch >> Zero or more Sub Branches >> Leafs

The previous line indicates the following:

» Navigate to **branch;**

» Navigate to **Sub Branch** (when a sub branch exists);

» Select a **leaf/parameter.**

For example:

M6100 >> Device Setup >> Mgmt Interface >> IP >> Mgmt1 IP Address/Prefix

The previous line indicates the following:

» Select **Mgmt Interface;**

» Navigate to **IP Address;**

» Insert a new value for **Mgmt1 IP Address/Prefix.**

The management Model / Menu Tree of the GUI, the frontpanel and the CLI can be consulted in the reference manual.

The reference manual provides an overview of all available parameters and if the parameters can be set or consulted by the operator or expert profile.

The complete reference manual can be found on the CD-ROM that is delivered together with the device.

The reference manual for the GUI can also be consulted from the tasks pane in the GUI, please refer to section:*GUI Pane Description. on page 42*

9.2 Management Ethernet Interfaces

Management interface 1 (Mgmt1) is activated by default; the other interfaces can be enabled on the following location in the device.

M6100 >> Device Setup >> Mgmt Interface

- Mgmt1 (This the top port on the back panel indicated as Mgmt1);
- Mgmt2 (This the bottom port on the back panel indicated as Mgmt2);
- Mgmt Frontpanel (This is the Ethernet port that is found on the front panel);

Do not disable the active management interface (interfaces) because this makes the device unreachable.
(The interface can be enabled again using the front panel buttons).

When link redundancy is used, Mgmt1 and Mgmt2 must be enabled and auto negotiation must be on. To enable link redundancy, refer to
Ethernet Link Redundancy. on page 34

Statistics

M6100 >> Device Setup >> Mgmt Interface >> Statistics

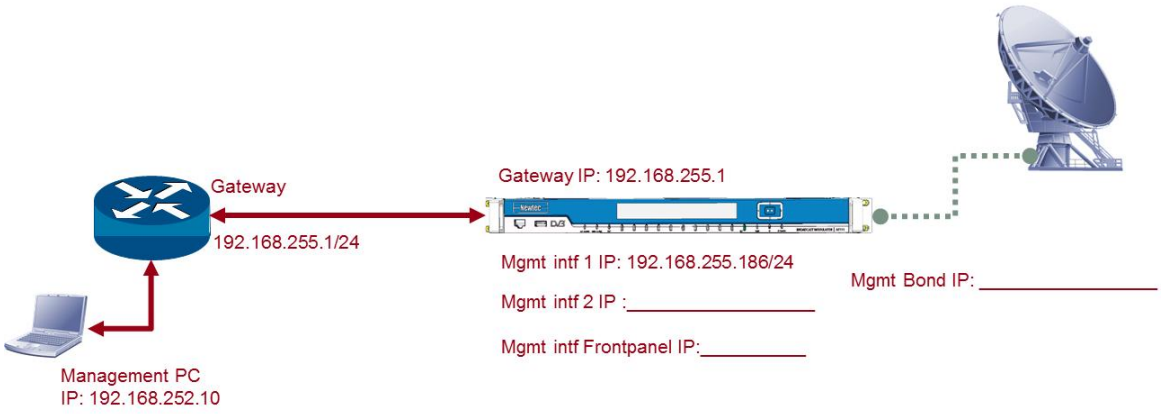
This provides an overview of the amount of traffic that is passing over the different management Ethernet ports.

The following statistics are displayed:

• Input Bytes; • Input Packets; • Input Dropped; • Input Errors;	• Output Bytes; • Output Packets; • Output Dropped; • Output Errors.

9.3 Management IP Connectivity

The following figure is an example of a setup:



Note: Before configuring the device make a proper design of the system setup.

To configure the management IP Addresses of the device go to the following location:

M6100 >> Device Setup >> Mgmt Interface >> IP Address

- Mgmt Gateway: This is the access point for the management port of the device.
- Mgmt interfaces: Configure at least one Mgmt interface to perform basic management using the GUI, CLI or SNMP.
  - Mgmt1, by default this IP address is: 10.0.0.2/24;
  - Mgmt2;
  - Mgmt Frontpanel;
  - Mgmt Bond.
    (This interface is used to perform link redundancy, effectively combining Mgmt1 and Mgmt2 into one new virtual interface).

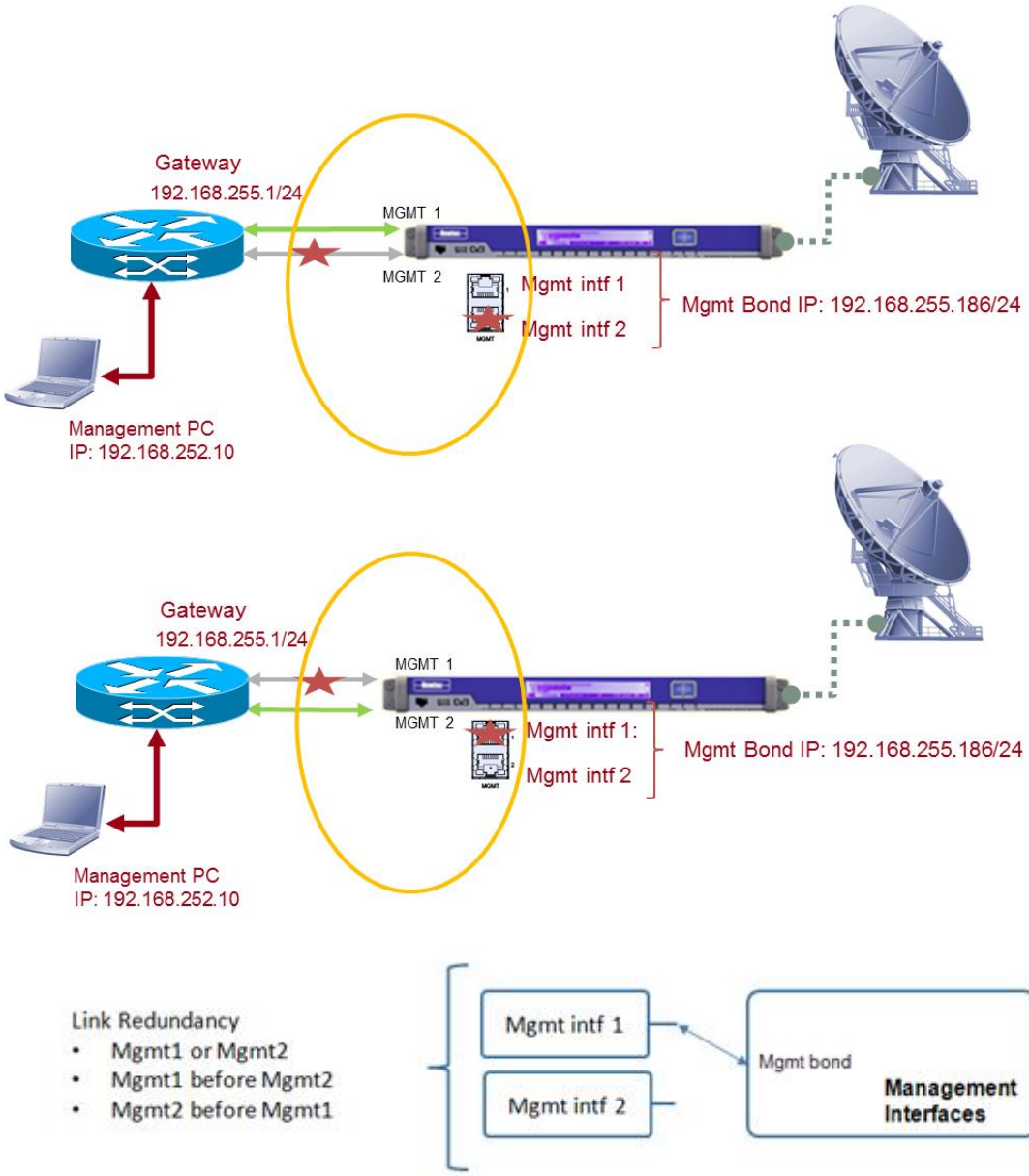
9.4 Ethernet Link Redundancy

It is possible to enable link redundancy (also known as bonding) on the management Ethernet interfaces.
Link redundancy is used to eliminate downtime as much as possible in the system setup. This increases the reliability of the system.

When link redundancy is enabled, two interfaces will behave as one virtual interface (interface bonding): only one of the two physical interfaces is active at a time.

When the link state of the active interface goes down (physically broken connection), the other interface takes over the operation.

Refer to the following figures: Note that the same principle is used for the data interfaces.



M6100 >> Device Setup >> Mgmt Interface >> IP Address >> Link Redundancy

When link redundancy is activated, the bond interface must be configured. This bond interface has an IP Address that is used as destination address by the source.

To have bonding working properly make sure to configure the switch/router in such a way that the spanning tree is not blocking the fast switchover between ports.

In a typical Cisco switch configured using rapid spanning tree this is achieved by setting the ports in PortFast mode.

9.5 How to Use the Graphical User Interface

The graphical user interface is a web application that gives remote access to the M6100. It allows the user to:

- Manage the device;
- Create or change configurations;
- Monitor the status of the M6100 through alarms.

The GUI is optimized for displays with a screen resolution of 1024 x 768 or higher.

9.5.1 Opening the GUI

Proceed as follows to open the GUI on a computer in the network:

» Open a web browser;

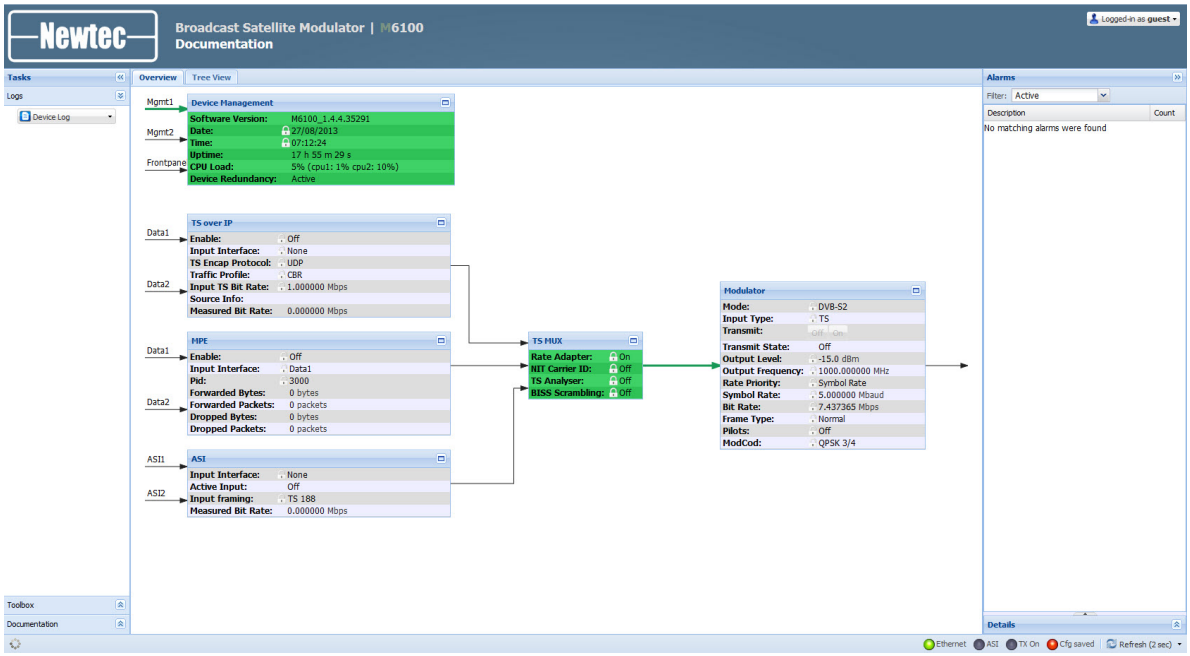
It is advised to use Firefox 10 or Google Chrome as standard browser, but the GUI can also run on other compatible browsers like Internet Explorer 9, Safari …

» Type the IP address of the device in the address bar of the browser. The default IP address is 10.0.0.2/24.

Make sure that the management PC has access to this IP Address or it belongs to this IP range. If needed it is possible to configure the Mgmt Gateway.

» Press **Enter**.

The following graphical user interface is displayed.


Newtec
Broadcast Satellite Modulator | M6100
Documentation
Logged-in as guest
Tasks
Logs
Device Log
Overview
Tree View
Mgmt1
Mgmt2
Frontpane
Device Management
Software Version: M6100_1.4.4.35291
Date: 27/08/2013
Time: 07:12:24
Uptime: 17 h 55 m 29 s
CPU Load: 5% (cpu1: 1% cpu2: 10%)
Device Redundancy: Active
Data1
Data2
TS over IP
Enable: Off
Input Interface: None
TS Encap Protocol: UDP
Traffic Profile: CBR
Input TS Bit Rate: 1.000000 Mbps
Source Info:
Measured Bit Rate: 0.000000 Mbps
MPE
Enable: Off
Input Interface: Data1
Pid: 3000
Forwarded Bytes: 0 bytes
Forwarded Packets: 0 packets
Dropped Bytes: 0 bytes
Dropped Packets: 0 packets
ASI1
ASI2
ASI
Input Interface: None
Active Input: Off
Input framing: TS 188
Measured Bit Rate: 0.000000 Mbps
TS MUX
Rate Adapter: On
NIT Carrier ID: Off
TS Analyser: Off
BISS Scrambling: Off
Modulator
Mode: DVB-S2
Input Type: TS
Transmit:
Transmit State: Off
Output Level: -15.0 dBm
Output Frequency: 1000.000000 MHz
Rate Priority: Symbol Rate
Symbol Rate: 5.000000 Mbaud
Bit Rate: 7.437365 Mbps
Frame Type: Normal
Pilots: Off
ModCod: QPSK 3/4
Alarms
Filter: Active
Description
Count
No matching alarms were found
Details
Toolbox
Documentation
Ethernet
ASI
TX On
Cfg saved
Refresh (2 sec)

9.5.2 User Profiles

The three possible user profiles are described in the following sections.

For security reasons it is recommended to change the default passwords of the user profiles. For more information please refer to section: *Change a Password. on page 41*

For detailed information on the access rights of the user profiles refer to the reference manual on the CD-ROM. .

9.5.2.1 Guest Profile

The user has read-only access to the typical configuration and monitoring options.

This is the default profile when logging in.

There is no password defined for this profile.

9.5.2.2 Operator Profile

Newtec recommends using this profile when configuring or maintaining a device.

The operator profile is developed in such a way that the user is not overloaded with all possible parameters.This is done to keep the configuration and maintenance of the device light and easy.

The user has read-write access to the typical configuration and monitoring options.

The default User Name and password for the operator profile is as follows:

- User Name: operator
- Password: operatoroperator

9.5.2.3 Expert Profile

This profile has read-write access to all configuration parameters.

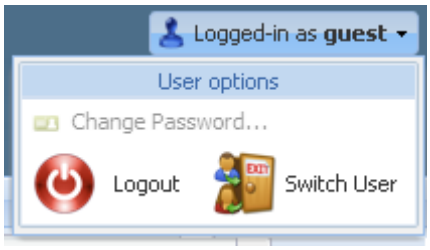
The expert profile can be used to configure specific features where the user needs more background of the different possibilities.

The default User Name and password for the expert profile is as follows:

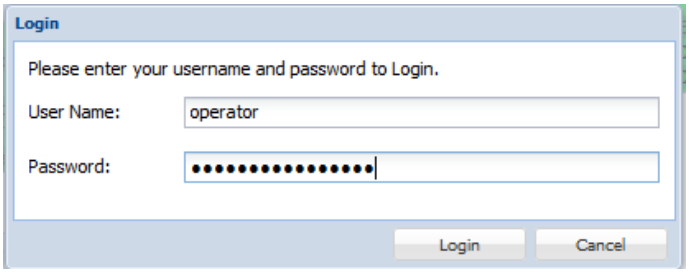
- User Name: expert
- Password: expertexpert

9.5.3 Switch User Profile

» Click **logged in as guest/operator/expert** (The User options window is displayed.)



» Click **Switch User** to change the user profile. (The Login window is displayed.)



The default User Name and password for the operator profile is as follows:

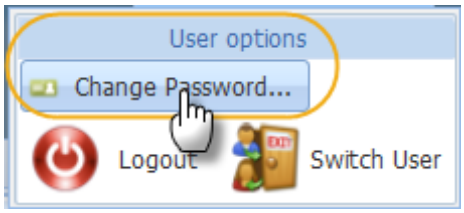
- **User Name**: operator
- **Password**: operatoroperator

The default User Name and password for the expert profile is as follows:

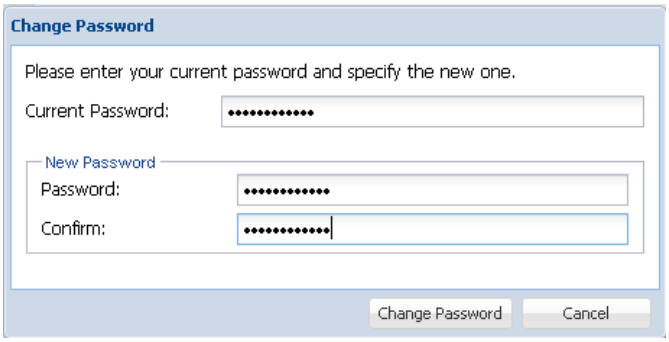
- **User Name**: expert
- **Password**: expertexpert

9.5.4 Change a Password

» In the users options window click **Change Password**



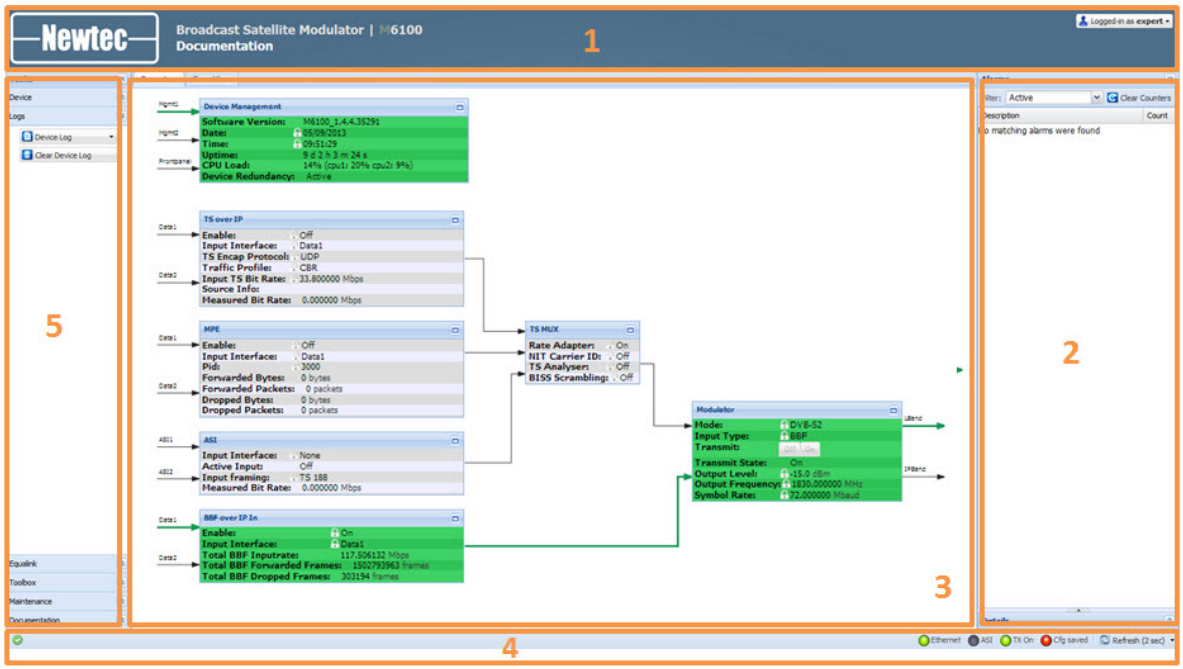
» Enter the Current Password and then the New Password. Also confirm the new password.



» Click **Change Password** to confirm the New Password.

9.5.5 GUI Pane Description

The following screen displays the general layout of the graphical user interface. The different panes are numbered clockwise and described in the pane description table.



The following table describes the sections numbered in the previous figure.

Pane No.	Pane name	Function
1	Banner	The top row of the banner displays the official device description and type. The top right row displays the current user profile. (To change the user profile, refer to *Switch User Profile on page 40*) The bottom left row of the banner is editable and can be used to assign a unique identifier to the device. Do this by clicking on the label. (In the previous figure, the label is marked: M6100). This name is also shown in the tab of the web browser and makes it easier to identify different devices.

Pane No.	Pane name	Function
2	Alarms list pane	The alarm list displays the alarms generated by the device. Alarms are sorted first by their activity and then by their severity (from critical alarms to warnings). • It is possible to filter Active, Memorized or All Alarms; • Clear the memorized alarms counter; • View details of the generated alarm. (State, History)
3	Function controls pane	This pane displays by default the **overview** tab. This overview tab provides: • An overview of the signal flow in the device; • Basic settings used to perform a configuration; • By clicking on the icon in the right upper corner of the functional block, a detailed overview with all parameters of the functional block opens in a new tab.
4	Status bar	The status bar informs on: • On-going interaction with the device via the status field on the left. • Refresh button, the status of the device gets refreshed; Click the arrow to configure the time interval of refreshing the status of the device.
5	Tasks pane	The tasks pane provides an overview of different tasks that are possible on following levels: • Device; – Configurations – Reset. • Logs; – Device Logging • Documentation. – Download the Reference Manual – Download the SNMP MIBs • Toolbox; – Diagnostics Report • Maintenance; – Software Upgrade – License Upgrade • Equalink™; – Automated Linear – Automated Non-Linear – Manual Import – Reset Predistortion

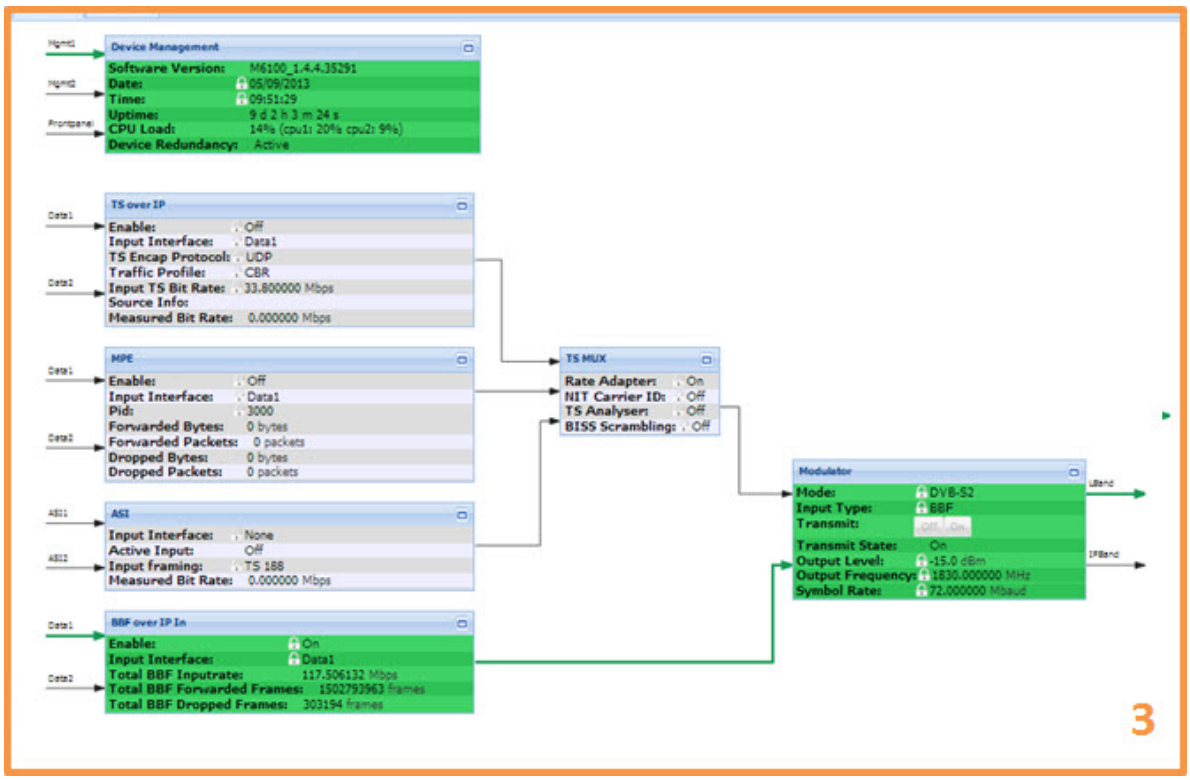
9.5.6 Overview Tab

The Overview tab contains a schematic representation of the data flow in the device.

The signal passes different functional blocks and each block contains a function name, basic settings and counters.

The blocks are connected with arrows that illustrate the data flow.

For more information on the colors used in the GUI please refer to section:
Colors Used in the GUI. on page 50

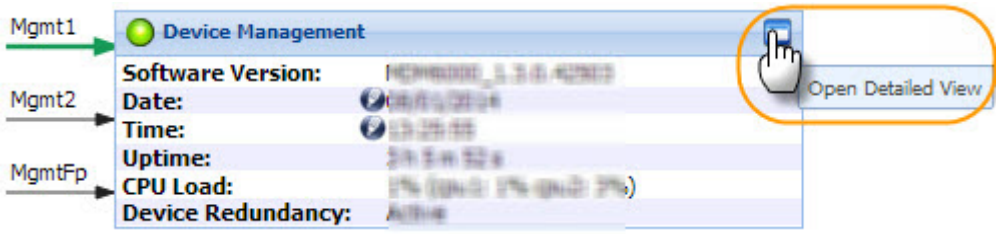


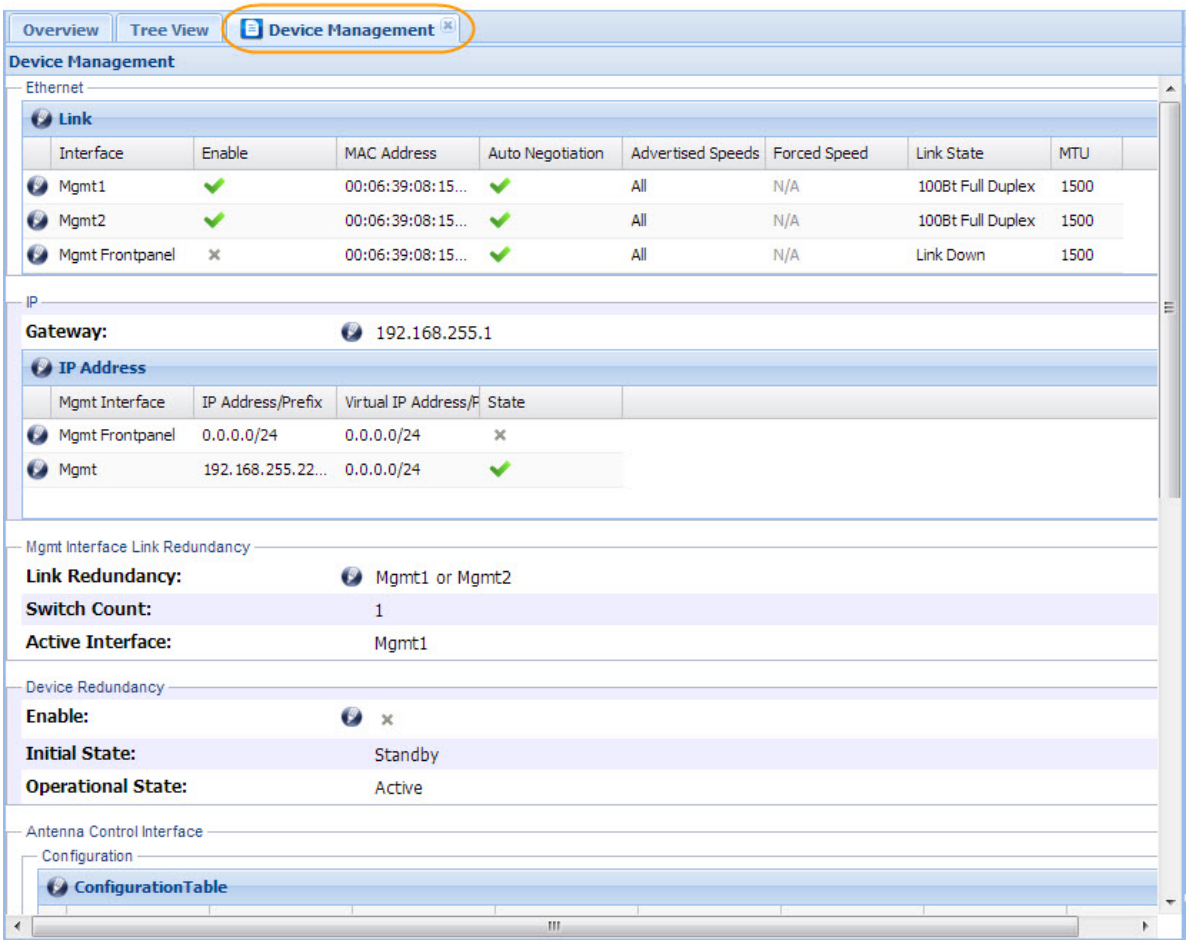
Functional Blocks	Description
Device Management	Functional block that allows to manage, configure and monitor the device management parameters. For Example: • Configure the management interfaces; • Manage the interface link redundancy; • Manage the device redundancy • Gather all device specific info such as, Serial number, Software version, ...
ASI	Functional block that allows to configure and monitor the ASI input interfaces.
MPE	Functional block that allows to configure and monitor the Multi protocol Encapsulation. This protocol makes it possible to transmit a typically limited amount of data along with the video transport stream.
BBF over IP In	Functional block that allows to configure and monitor the incoming traffic. (Typically received from an AZ810 Stream Aggregator).
TS MUX	Functional block that allows to configure and monitor the: • Rate Adapter; • NIT Carrier ID; • TS Analyser; • BISS Scrambling.
Modulator	Functional block that allows to configure and monitor the modulation of the traffic. For example: • Mode selection, DVB-S, DVB-S2 or S2-Extensions; • Transmit (on/off); • Output Frequency; • ….. Note that it is possible to control the Transmit (Off/On) from the overview tab.

9.5.7 Detailed View of a Functional Block

Click on the enlarge button in the top right corner of a functional block to view more parameters for the functional block.

Refer to the following figure:

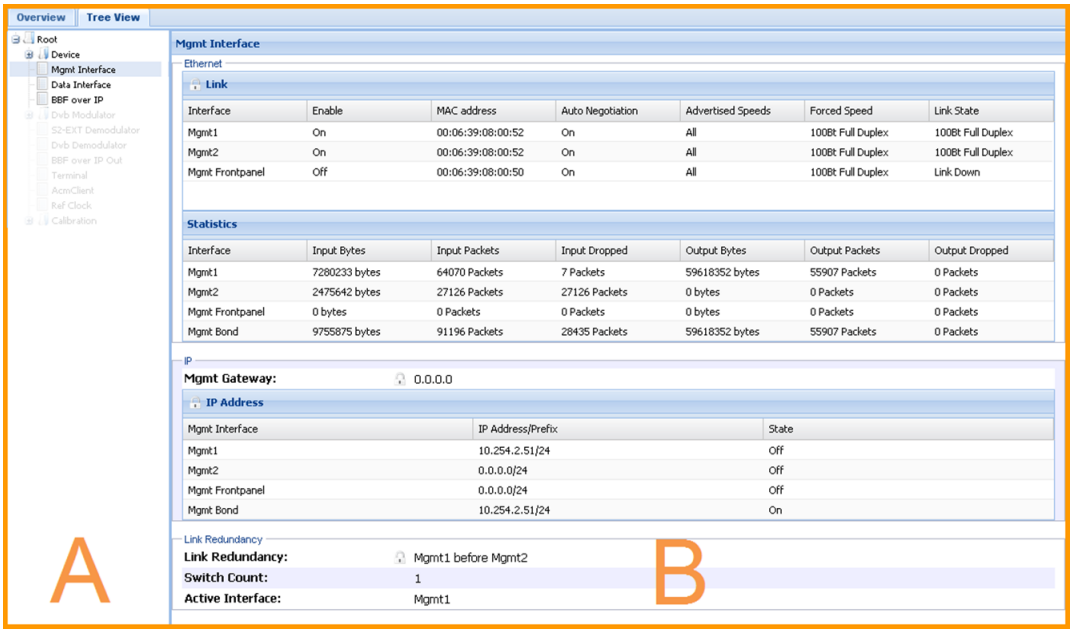




9.5.8 Tree View

The tree view shows all device parameters arranged in a tree structure consisting of branches, sub branches and leaves.

The following pane is displayed:



The tree view, divides the **function controls pane** in to two extra panes, they are called A and B in the previous figure:

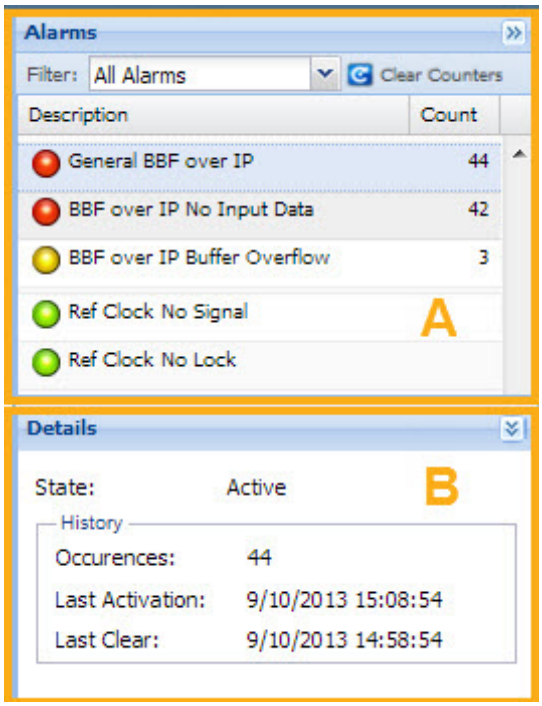
The following table describes the extra panes of the tree view.

Pane	Description
A	Displays the menu tree structure. Click on a branch or sub branch to navigate through the device. The menu tree structure uses the following icons: •  : This is a branch icon; it can contain sub branches or leaves/configuration parameters. •  : This is a sub branch icon; it contains leaves/configuration parameters.
B	Displays the sub branches or the details on the parameters (leafs) that exist under a selected branch.

9.5.9 Alarms Pane

The Alarms pane shows the alarms generated by the device.

Alarms are sorted first by their activity and then by their severity (from critical alarms to warnings.)



The alarm list pane contains the following information:

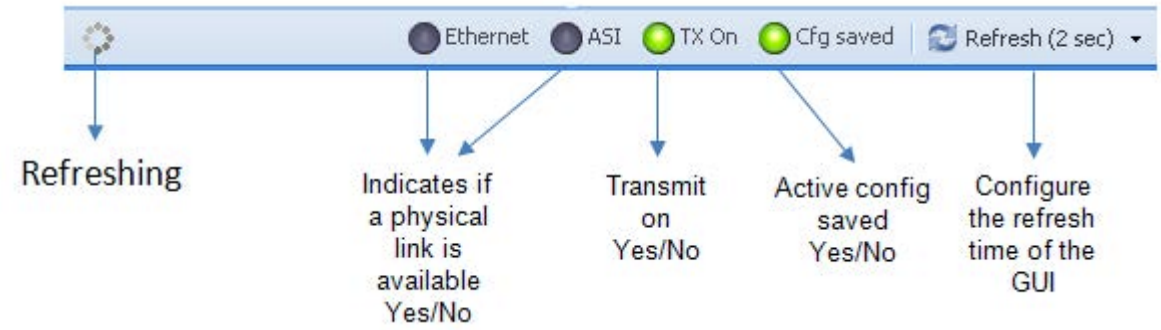
Pane	Description
A	This pane displays the alarms. It is possible to filter on the following alarm information: • Active • Active and Memorized • All Alarms (this displays the complete overview of all possible alarms)
B	This pane displays the details on the selected alarm. • How many times did the alarm occur since the last clear; • When was the last activation; • When the alarm was cleared for the last time.

» Click **Clear Counters** to clear the number of times an alarm was generated.
(Active alarms can be cleared but remain active, the last clear time is updated).

To perform alarm masking, refer to section: *Alarm Handling. on page 100*

9.5.10 Status Bar

The status bar informs on the following:



Cfg saved is red when the active configuration is modified but not saved.

To save the configuration, refer to section: *Save a Configuration on page 84*.

The following table describes the available LEDs.

LED	LED Color	Description
Ethernet (All interfaces are monitored)	Green	The incoming data signal is valid.
	Red	Indicates an interface alarm. Please check the alarm pane to get more details.
	Off	The incoming data signal is not valid.
ASI	Green	The incoming or outgoing data signal is valid.
	Red	The incoming / outgoing data is configured but there is no activity monitored during the last second.
	Off	The incoming signal is not valid.
Tx On	Green	The device is transmitting.
	Off	The transmission is disabled.
Cfg saved	Green	Indicates that the active configuration is saved.
	Red	Indicates that the active configuration is modified but not saved.
Refresh		Select the drop-down menu to define the GUI Refresh Time. When working over a slow/long-delay link (like a satellite link) slowing down this refresh time could be useful to improve the responsiveness of the GUI.

9.5.11 Colors Used in the GUI

In the schematic overview, colors are used per functional block to provide the status of the device. The traffic flow is also indicated between the functional blocks by arrows.

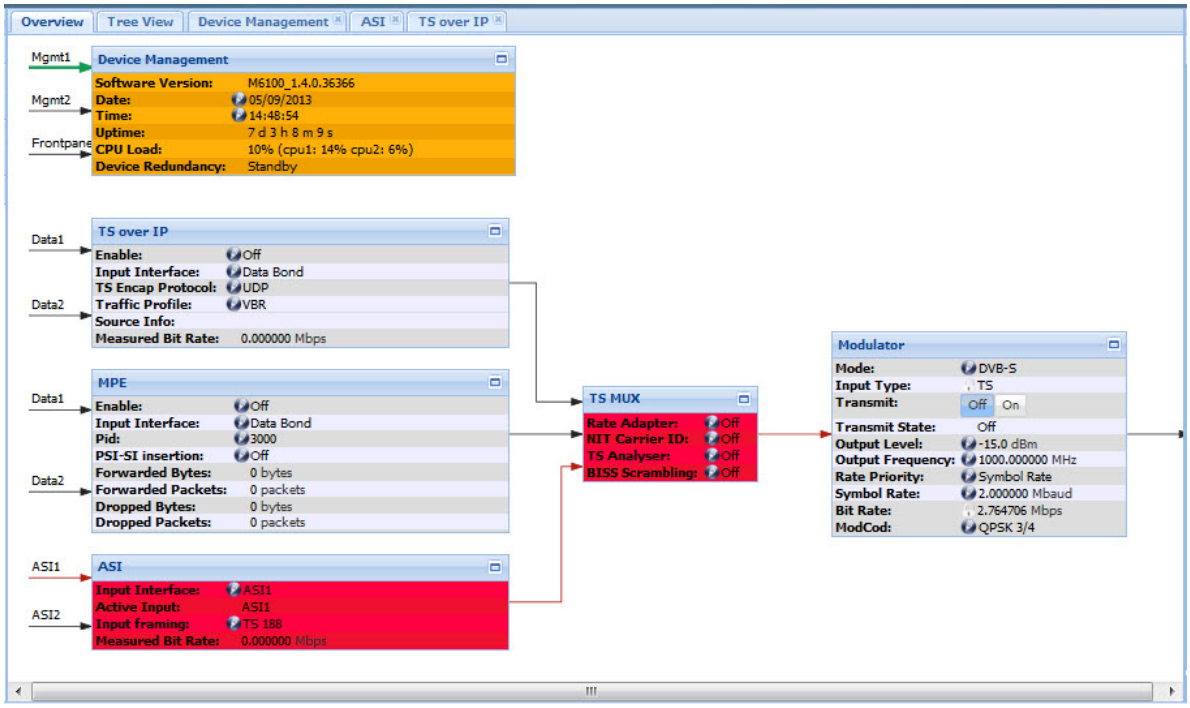
The following colors are used for the functional blocks.

- Green: The device is working as expected;
- Orange:
  - Device Management: Device redundancy is active and the device is in standby mode
    Note: orange is only used by this functional block.
- Grey: This functional block is not active in the current configuration.
- Red: An alarm is present on the functional block;

The following colors are used for the process flow arrows:

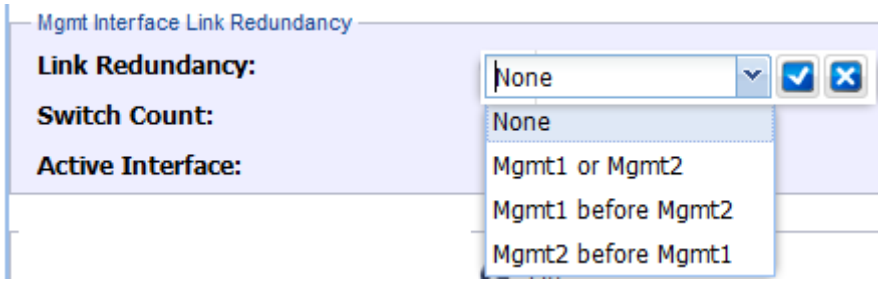
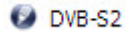
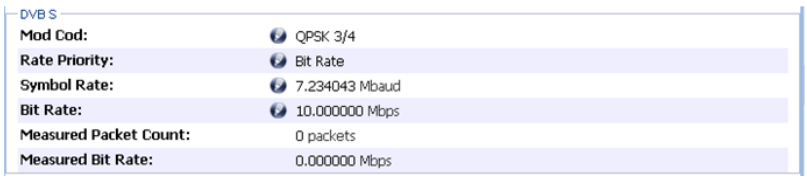
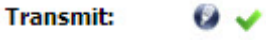
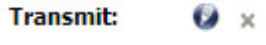
- Black: Inactive, no data is transported;
- Green: Data is available on this part in the process flow (incoming, outgoing or transfer of data within the device);
- Red: A problem exists on this part of the process flow.

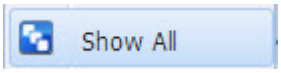
For example:



9.5.12 Parameters in the GUI

The GUI contains different types of parameter dialogue boxes to configure all parameters.

Dialogue box Type	Example
Drop-down-list-box	
Edit	 This pencil icon indicates that it is possible to edit the parameter
Lock	 The lock icon indicates that it is not possible to edit the parameter.
Data field	
Check box	• To apply a setting use the following icon  . • To cancel a setting use the following icon 
Table	
Functional group	
Enable/Disable button	
Enabled (indication)	
Disabled (indication)	
Reset button	

Show All	 Click this dialog box to open the functional block.
Open Detailed View	 Click this icon to open the detailed view, zooming in on the parameters of the specific block.
Delete	 Click this icon to delete a connection.

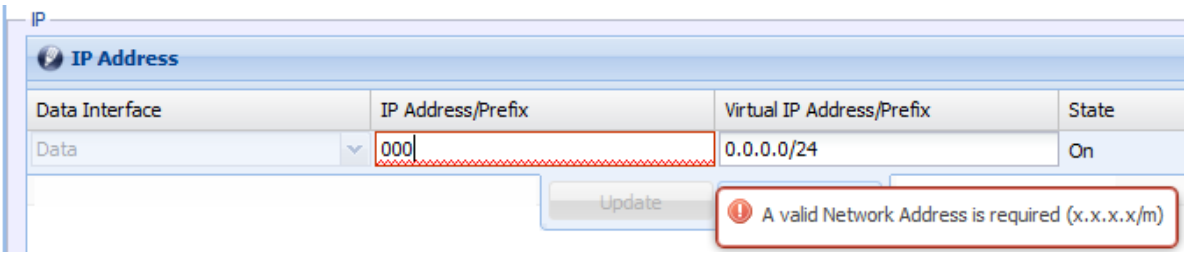
Hovering over a parameter shows more details about it.

9.5.13 Invalid Values

The GUI does not allow the input of invalid values. While typing a value this value is validated. The user interface has several features that help to insert valid parameters:

- When typing an invalid value for a parameter, the edges of the parameter field turn red and a tool tip displays the reason why the value is invalid;
- It is not possible to save values outside the defined ranges for the device.

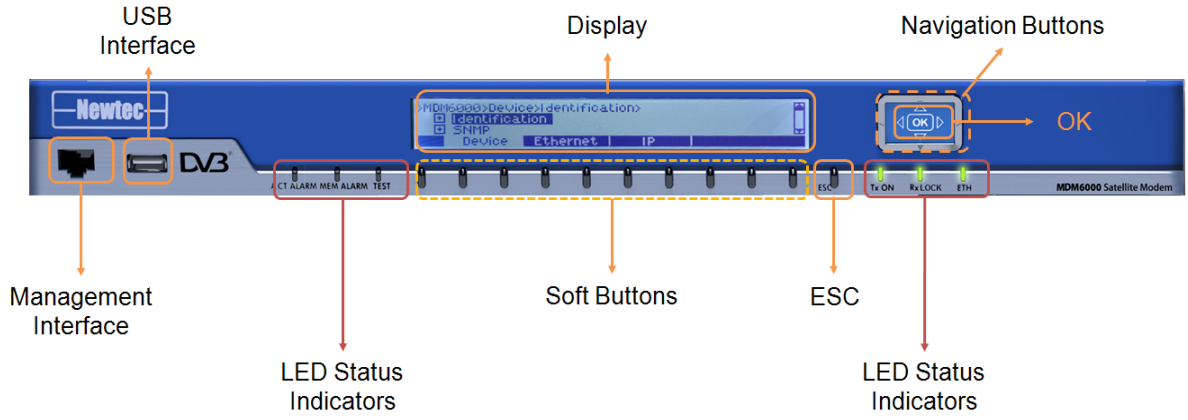
The following figure shows an example of the behavior of the GUI when you try to enter an invalid value.



9.6 How to Use the Front Panel

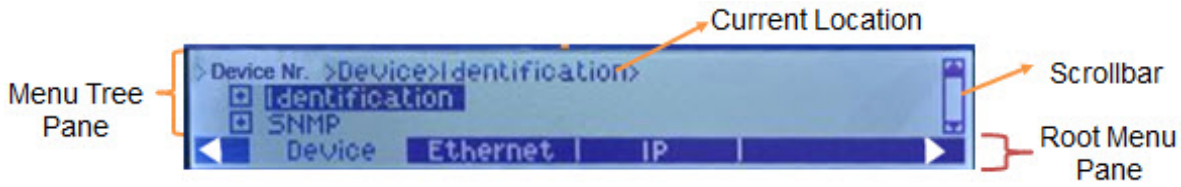
This section explains how the devices can be configured using the front panel.

The following figure shows the navigation buttons, indicators and connectors to the front panel.



9.6.1 Navigating Through the Display

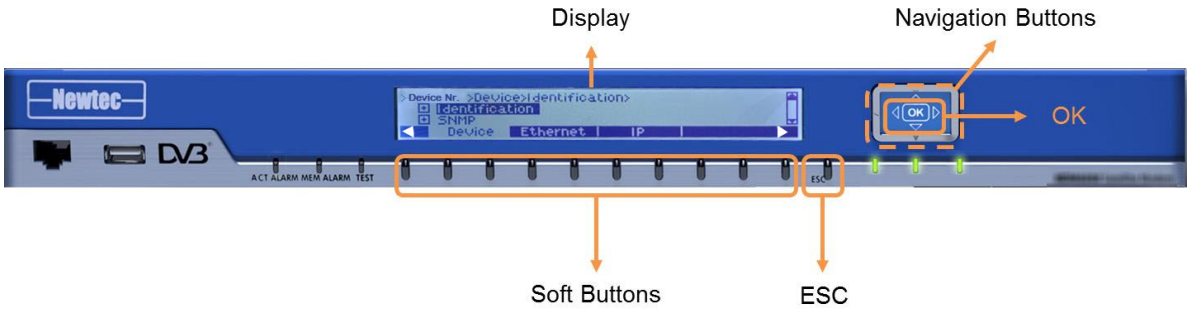
The display is divided horizontally into two regions in a matrix:



- Root Menu Pane: displays the branches of the device;
- Menu Tree Pane: displays the current location, the sub branches and/or parameters that exist under the selected branch or sub branch.

9.6.2 Front Panel Buttons Description

The following figure displays the different control buttons of the front panel.



The following table describes the buttons displayed in the previous figure.

Name/Symbol	Description
Arrow UP	Navigate to the upper item.
Arrow DOWN	Navigate to the lower item.
Arrow LEFT	Fold an expanded branch or a leaf sub item.
Arrow RIGHT	Unfold a collapsed branch.
OK	Depending on the position it has the following function: • Branch: Expand; • Leaf: Open a parameter; • Confirm a new value.
ESC	• Fold an expanded branch; • Discard a new value.
Soft Buttons	• Navigate through the root menu (arrows); • Select a main branch from the root menu.

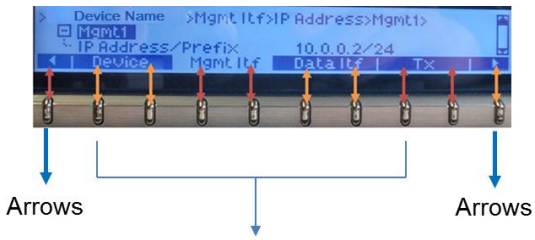
9.6.3 Root Menu Pane

This pane represents a list of the available branches.
It is presented at the bottom of the display in a horizontal way.

For example the following main menus:

- Device: This menu contains the device level parameters;
- Ethernet;
- IP;
- Modulator .

A branch is associated with one (or more) soft-button(s). This depends on the size and the position relative to the soft buttons.
When more than one branch is available the first and last soft button are used as arrows.
Refer to the following figure:



To select or navigate in the root menu it is possible to do one of the following:

» Press the soft button that is associated with the required menu;

» Use these arrows (soft buttons) to navigate to the required menu and press OK (on the navigation button).

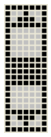
9.6.4 Tree Menu Pane

- The first row of the tree menu indicates the current location in the device.
  For example:

M6100 > Device> Identification

- A selectable item in the tree menu pane is visualized with a dark background.

The following table describes the icons that are used by the tree menu pane.

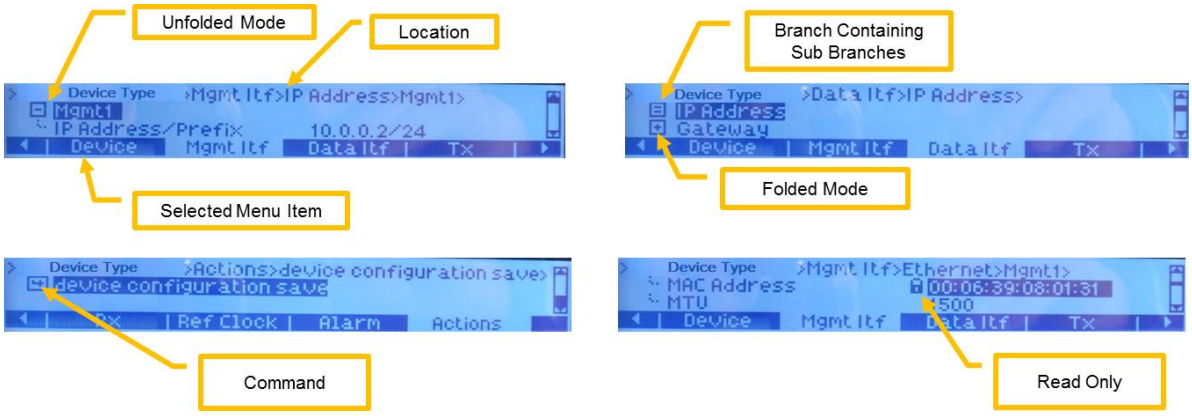
Icons	Description
	Indicates a branch that contains no sub branches. All parameters exist directly under this branch.
	Folded mode.
	Unfolded mode.
	Indicates an action. (for example: Save).
	Scroll bar Indicates that more than one line exists under this selection.
	Indicates a read only parameter.

In this pane, the parameters are listed vertically.

» Navigate through this pane by using the up/down arrow of the **navigation buttons**;

» Unfold a branch by using the right arrow or pressing **OK;**

» Fold a branch by using the left arrow or pressing **ESC**.



9.6.5 Example: Change the Access Level

Change the access level/user profile in the front panel.

Proceed as follows:

» Select **Device** using the corresponding **Soft button**

» Navigate to **Frontpanel** .

» Click **OK** (to unfold the branch)

» Navigate to **Access Level** .

» Click **OK**

» Navigate to the access level of your choice

– Read Only

– Operator

– Expert

» Click **OK**

or

» Select the .Number (**Soft button**) corresponding to the displayed access levels.

9.6.6 Example: Set the Output Frequency

» Select **Modulator** using the corresponding **Soft Button;**

» Navigate to **Output Frequency;**

» Click **OK;**

New value is displayed, indicating the current position by a blinking number.

» Insert the new value using the corresponding **Soft Buttons;**

» Click **OK;**

» The new value is displayed on the front panel.

9.6.7 Example: Check the Alarms

» Select **Alarms** using the corresponding **Soft Button;**
(use the soft button arrows to navigate through the root menu.)

» Navigate to **Active Alarms or Memorized Alarms;**

» Click **OK;**

» Navigate through the tree menu to see the active or Memorized alarms.

It is possible to clear the Memorized Alarms by pressing the **OK** button during three seconds.

9.7 Command Line Interface (CLI)

This sections describes how the device can be managed using the CLI.

The commands and how they can be applied are described in the following sections.

9.7.1 How to Access the CLI

Access the CLI via an Ethernet management interface or via the craft interface by using a RS232 serial cable.

Management Interface

To access the CLI via the management interface do the following:

» Configure the IP Address of the management interface using the front panel.

Make sure that the IP address of the M6100 Boadcast Satellite Modulator is in the same range as the IP Address of the managing device or that a default gateway is configured.

» Make an Ethernet connection between the managing device and the M6100.

Craft Interface

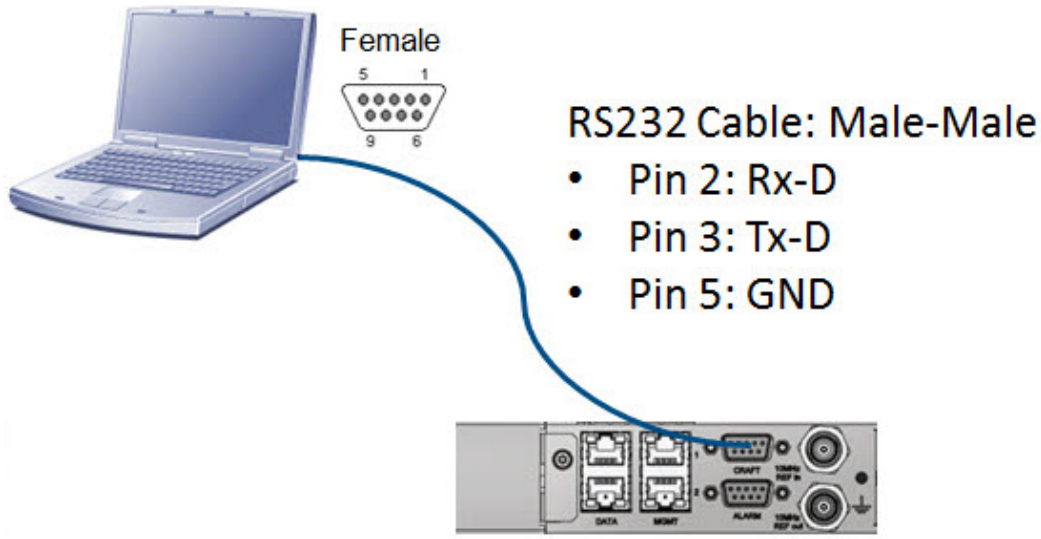
To access the CLI via the craft interface do the following:

» Configure the line settings of the serial port as follows:

- Speed 115200 baud;
- Eight data bits;
- No parity bit;
- One stop bit.

» Make an connection between the managing device and the M6100 Boadcast Satellite Modulator.

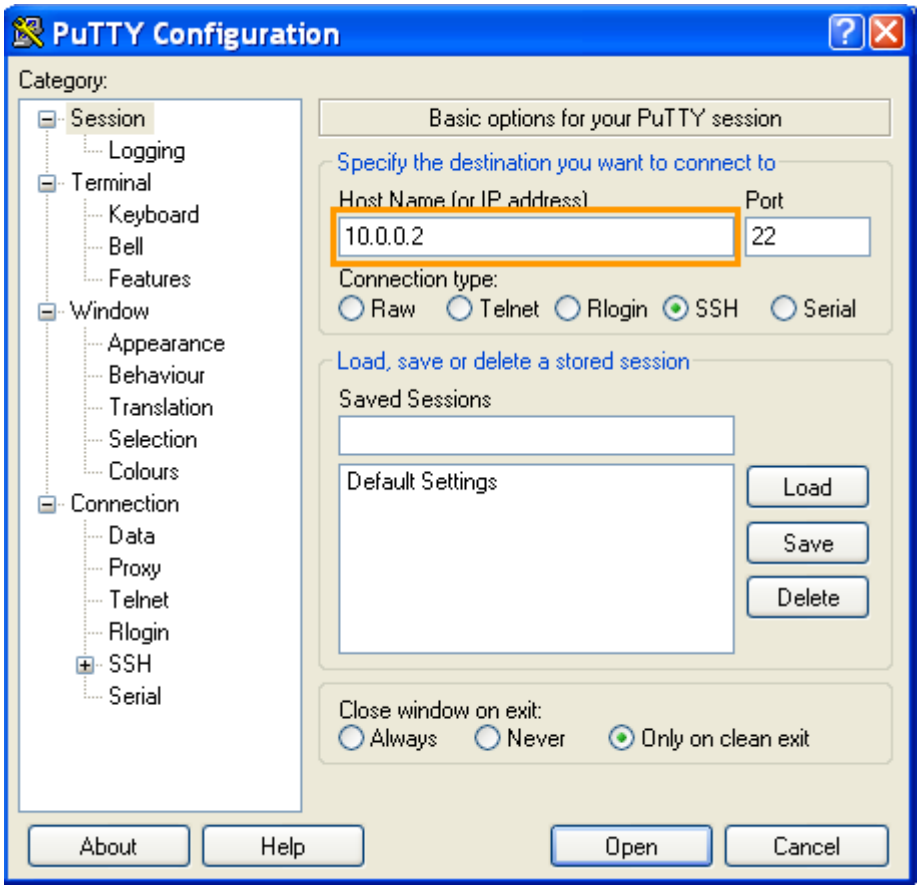
For more information please refer to section: *Craft Interface on page 24* .



9.7.2 Open the CLI using a Terminal Emulator

A terminal emulator is an application that can act as a client for the SSH (Secure Shell) computing protocol and as a serial console client. In this user manual PuTTY is used as terminal emulator. Go to the following website *http://www.putty.org/* to find the download page for PuTTY.

When opening PuTTY the following window is displayed.



» Insert the Management IP address of the device.
By default 10.0.0.2/24.

» Click **Open.** The Login Screen is displayed.

9.7.3 Log In as Expert

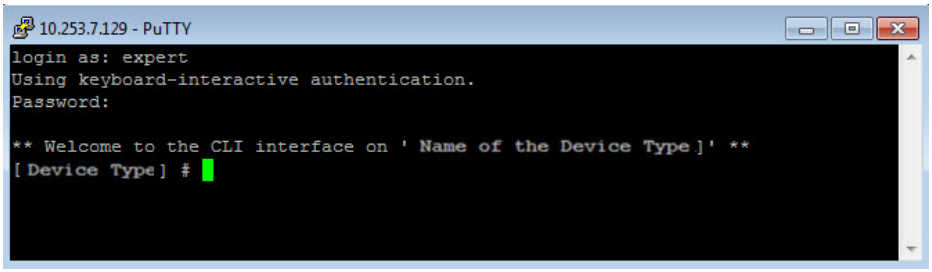
The CLI interface can only be accessed by the expert user.

» To login as expert type the following:

» login as: expert

» password: expertexpert

» The following window is displayed:



The device name is displayed between brackets.

9.7.4 Show, Help and Context Sensitive Help

These commands make it possible to request information on certain commands or parameters.

9.7.4.1 Show

The show command is used to display the different commands, branches or leaves that exist in a branch.

For Example:

[M6100] device# show

log/

diagnostics/

identification/

frontpanel/

snmp/

cli/

gui/

ftp/

datetime/

monitor/

configuration/

reset*

softwareupgrade*

license/

or

[M6100] modulator# show

```
transmitctrl/
 externalconvertor/
 dvbcid/
equalink/
dvbs2/
mode                    Dvbs2
transmit                on
outputfrequency         1550.000000 MHz
outputband              lBand
....                    ....
```

9.7.4.2 Help

The help command is used to provide information on a command or parameter.

Always type help at the end.

For example:

[M6100] device # **`reset help`**

```
reset the device

Mandatory parameters:

  * {enum}: Reset (default value = software) (possible enums are: hardware
software factory )
```

9.7.4.3 Context Sensitive Help "?"

This is used to provide possible completions.

When context sensitive help is used in a branch it displays all the possible commands, sub branches, parameters and possible values.

Context sensitive help provides all possible completions when typing a command.

The question mark (?) is not shown in the interface.

The (?) can be replaced by pressing two times the TAB key.

For example display possible parameters:

[M6100] modulator# **`o?`**

```
outputfrequency

outputband

occupiedbandwidth

outputlevel
```

For example display possible values:

[M6100] modulator# **`rolloff set ?`**

```
set RollOff

Mandatory parameters:

  * {enum}: Transmit filter roll-off factor. (default value = rolloff15) (possible
enums are: rolloff5 rolloff10 rolloff15 rolloff20 rolloff25 rolloff35 )
```

9.7.5 Navigate Through the Branches of the Device

Use the following commands to navigate through the different branches of the device.

In this manual the commands are presented as follows:

The input message is displayed as follows:

`Command input`

The return message is displayed as follows:

`Command output`

9.7.6 Go into a Branch

» Type in the branch name and press **Enter.**

For Example:

M6100] # **`modulator`**

[M6100] modulator#

9.7.7 Move Up one Level

» Type one of the following commands:
`exit`

or

» `..`

For Example:

M6100] modulator# **`exit`**
[*`M6100] #`*
or
[M6100] modulator#`..`
[*`M6100] #`*

9.7.8 Return to the Main Branch

» Type one of the following commands:**exitall**/[**CTRL-Z**] (key combination)

For Example:

[M6100] modulator dvbs2# exitall

[M6100]#

or

[polaris] modulator dvbs2# /

[M6100]#

or

[M6100] modulator dvbs2# [CTRL-Z]

[M6100]#

9.7.9 Supported Key Presses in the CLI

The CLI supports the following input characters:

Directly from the keyboard

- All printable characters;
- Arrows;
- Enter;
- Backspace;
- Delete;
- Tab: used to perform command completion;
- "?": used to get help on the current input context;
- Double Tab: this has the same function as the previous command "?".

Key Combinations

Key Combination	Description
CTRL+A	Go to beginning of the line.
CTRL+B	Move the cursor backwards.
CTRL+C	Flush the current line ignoring the contents and start a new line.
CTRL+D	Delete to the right.
CTRL+E	Move the cursor to the end of the line.
CTRL+F	Move the cursor forward.
CTRL+H	Delete to the left.
CTRL+K	Delete from the current cursor position to the end of line.
CTRL+P	Recall the previous line in history.
CTRL+M	Carriage return.
CTRL+N	Go to the next line in history.
CTRL+U	Delete from the current cursor position to the beginning of the line.
CTRL+S	Suspend asynchronous tracing, use this to pause the information stream.
CTRL+Q	Resume asynchronous tracing, use this to resume the information stream.
CTRL+Z	Return to the main branch.

9.7.10 Displayed Units

Some variables are by default scaled to a more readable unit.
For example:

- Symbol rate in Mbaud;
- Bit rate in Mbps;
- Frequencies in MHz.

When entering a new value (without specifying a scale) the default unit scaling is applied.

For example:

[M6100] modulator# **`set outputfrequency=1550`**

`OK`

[M6100] modulator# **`outputfrequency get`**

`1550 MHz`

9.7.11 Get and Set Parameter Values

Use these commands to read out and set parameter values.

It is not mandatory to navigate to the specific branch to execute a command. It is possible to request or set a value from the main branch.

When in a sub branch it is possible to get/set a value from another sub branch. Do this by entering a prefix "/" to indicate that the navigation starts from the main branch.

Get

» Type the location and the parameter name to readout the requested parameter value.

For example:

[M6100] # **device identification label get**

Modulator

or

It is also possible to navigate to the parameter location and make a request.

[M6100] # **mgmtintf**

[M6100] mgmtintf # **mgmtgateway get**

192.168.254.206

or

Request a parameter from another sub branch.

[M6100]# /**modulator mode get**

Dvbs2

Set

For example (change only one parameter):

[M6100] modulator# **outputlevel set -15dbm**

OK

For example (change multiple parameters):

[M6100] modulator# **set outputlevel=-25dbm outputfrequency=1550.000000 MHz**

OK

9.7.12 Dynamic Tables

The data model of the M6100 Boadcast Satellite Modulator uses a lot of tables. These tables are used to keep related information together.

The CLI allows to display these tables. Furthermore it is possible to access and change values of a parameter in a specific row and column, this makes the tables dynamic.

The command "showtable" displays the entire table including column headers.

The following figure shows the layout of a table in the CLI.

```
[CSE Modem R1.1 remote] mgmtinterface link# showtable
-----------------------------------------------------------------------------------------------------------------------------
| Interface   | Enable   | MacAddress          | AutoNegotiation   | AdvertisedSpeeds   | ForcedSpeed   | LinkState          | Mtu  |
-----------------------------------------------------------------------------------------------------------------------------
| mgmt1       | on       | 00:06:39:08:15:7a   | on                | all                | N/A           | 100BTFullDuplex    | 1500 |
| mgmt2       | off      | 00:06:39:08:15:79   | on                | all                | N/A           | linkDown           | 1500 |
| mgmtfp      | off      | 00:06:39:08:15:78   | on                | all                | N/A           | linkDown           | 1500 |
-----------------------------------------------------------------------------------------------------------------------------
```

Make sure that the resolution of the display is wide enough. When this is not the case the column indication becomes unclear.

9.7.12.1 Show Tables

Use the following command to show a table in the CLI.

"showtable"

For example:

M6100 Mgmt interface link#**`showtable`**

```
[CSE Modem R1.1 remote] mgmtinterface link# showtable
-----------------------------------------------------------------------------------------------------------------------------
| Interface   | Enable   | MacAddress          | AutoNegotiation   | AdvertisedSpeeds   | ForcedSpeed   | LinkState          | Mtu  |
-----------------------------------------------------------------------------------------------------------------------------
| mgmt1       | on       | 00:06:39:08:15:7a   | on                | all                | N/A           | 100BTFullDuplex    | 1500 |
| mgmt2       | off      | 00:06:39:08:15:79   | on                | all                | N/A           | linkDown           | 1500 |
| mgmtfp      | off      | 00:06:39:08:15:78   | on                | all                | N/A           | linkDown           | 1500 |
-----------------------------------------------------------------------------------------------------------------------------
```

9.7.12.2 Change Parameters in a Table

To access or change a specific row, type its row key and enter or specify the parameter you want to access or change.

For example:

M6100 datainterface link# **`showtable`**

```
[CSE Modem R1.1 remote] datainterface link# showtable
-----------------------------------------------------------------------------------------------------------------------
| Interface   | Enable   | MacAddress          | AutoNegotiation   | AdvertisedSpeeds   | ForcedSpeed   | LinkState          | Mtu  |
-----------------------------------------------------------------------------------------------------------------------
| data1       | on       | 00:06:39:08:15:77   | on                | all                | N/A           | 1000BTFullDuplex   | 1500 |
| data2       | off      | 00:06:39:08:15:7b   | on                | all                | N/A           | linkDown           | 1500 |
-----------------------------------------------------------------------------------------------------------------------
```

M6100 datainterface link# **data2 set enable=on**

OK

9.7.12.3 Add a New Row to a Table

In case of empty tables, the command showtable only shows the column headers.

This indicates the different parameters that can be defined for a row in this table.

To create a new row , use the command "new".

For example:

M6100 gsedecapsulation channels# **showtable**

```
-------------------------------------------------------------------------
| Name       | Enable   | Isi   | Label                | LabelFilter |
-------------------------------------------------------------------------
| Kinshasa   | off      | 1     | 00:00:00:00:00:00/0  | nofilter    |
| Paris      | on       | 1     | 00:00:00:00:00:00/0  | nofilter    |
-------------------------------------------------------------------------
```

M6100 gsedecapsulation channels# **new Senegal**

OK

M6100 gsedecapsulation channels# **showtable**

```
-------------------------------------------------------------------------
| Name       | Enable   | Isi   | Label                | LabelFilter |
-------------------------------------------------------------------------
| Kinshasa   | off      | 1     | 00:00:00:00:00:00/0  | nofilter    |
| Paris      | on       | 1     | 00:00:00:00:00:00/0  | nofilter    |
| senegal    | off      | 0     | 00:00:00:00:00:00/0  | nofilter    |
-------------------------------------------------------------------------
```

M6100 gsedecapsulation channels# **senegal set enable=on**

M6100 gsedecapsulation channels# **senegal set isi=3**

```
-------------------------------------------------------------------------
| Name       | Enable   | Isi   | Label                | LabelFilter |
-------------------------------------------------------------------------
| Kinshasa   | off      | 1     | 00:00:00:00:00:00/0  | nofilter    |
| Paris      | on       | 1     | 00:00:00:00:00:00/0  | nofilter    |
| senegal    | on       | 3     | 00:00:00:00:00:00/0  | nofilter    |
-------------------------------------------------------------------------
```

9.7.12.4 Delete a Row from a Table

Use the command "delete " to remove a row from the table.

For Example:

M6100 gsedecapsulation channels# **`delete senegal`**

`OK`

```
-------------------------------------------------------------------------
| Name       | Enable   | Isi   | Label                | LabelFilter |
-------------------------------------------------------------------------
| Kinshasa   | off      | 1     | 00:00:00:00:00:00/0  | nofilter    |
| Paris      | on       | 1     | 00:00:00:00:00:00/0  | nofilter    |
-------------------------------------------------------------------------
```

9.8 SNMP

SNMPv2c is used in the device. The MIBs as supported by the device can be downloaded from the GUI Device Tasks Pane.

M6100 >> Device Setup >> Access Control >> SNMP

SNMP (Simple Network Management Protocol) is used when the customer wants to control the device (or a complete system) through a NMS (Network Management System).

The following parameters must be set:

- Authentication (SNMP Communities);
  An SNMP community is a relationship between an SNMP managed device and a set of SNMP managers that defines authentication, access control, and proxy characteristics. The community must be set on the local device/managed device. The NMS must include the correct community string in its messages in order to get or set the different parameters of the device.
  Define the following communities:
  - Read Only Community: This string is always sent along with each SNMP Get action. The received string must be recognized by the managed device in order to allow or deny access to the device.
  - Read Write Community: This string must be sent along with each SNMP Set action. The string must be recognized by the device before a parameter can be set.
- Notification.
  - Set the destination IP Address where SNMP traps must be sent to. SNMP traps are messages indicating a specific state of the device.
  - Also a trap community must be configured for each trap destination.

The SNMP service is activated by default.

It is recommended to disable the SNMP service when the service is not used to manage the device. Do this to avoid unauthorized people accessing the device.

For more information on the use of the SNMP interface refer to the System Integration Guide on the CD-ROM that is delivered together with the device.

9.8.1 Consult or Download the SNMP MIBs (Management Information Base)

The SNMP MIBs can be downloaded using the GUI interface.

» Navigate to the **Tasks Pane** (GUI);

» Click **Documentation;**

» Click **SNMP MIBs**.

A mibs.zip file is downloaded and stored on the default folder of the management device.

The SNMP MIBs are also delivered on CD-ROM together with the device.

9.9 File Transfer Protocol (FTP)

This feature is used to download or upload files and is commonly used in combination with the CLI.

For example:

- Download files: (Diagnostics, Log files);
- Upload files: (Config files, software upgrades, license file, Equalink).

Enable or disable the FTP (File Transfer Protocol) server service and the FTP account on following location:

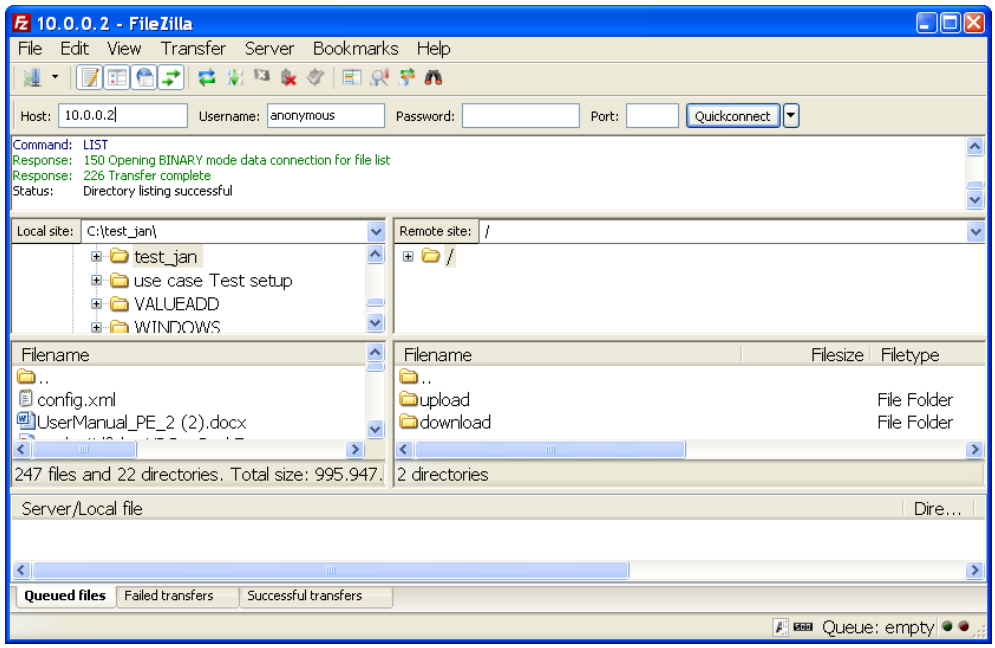
M6100 >> Device >> FTP

The FTP service (anonymous account) is activated by default.
For security reasons, it is advised to disable the anonymous ftp-account.

When this is done the FTP account can be consulted with the operator and expert user login and password.

Use an FTP client application to connect to the device.

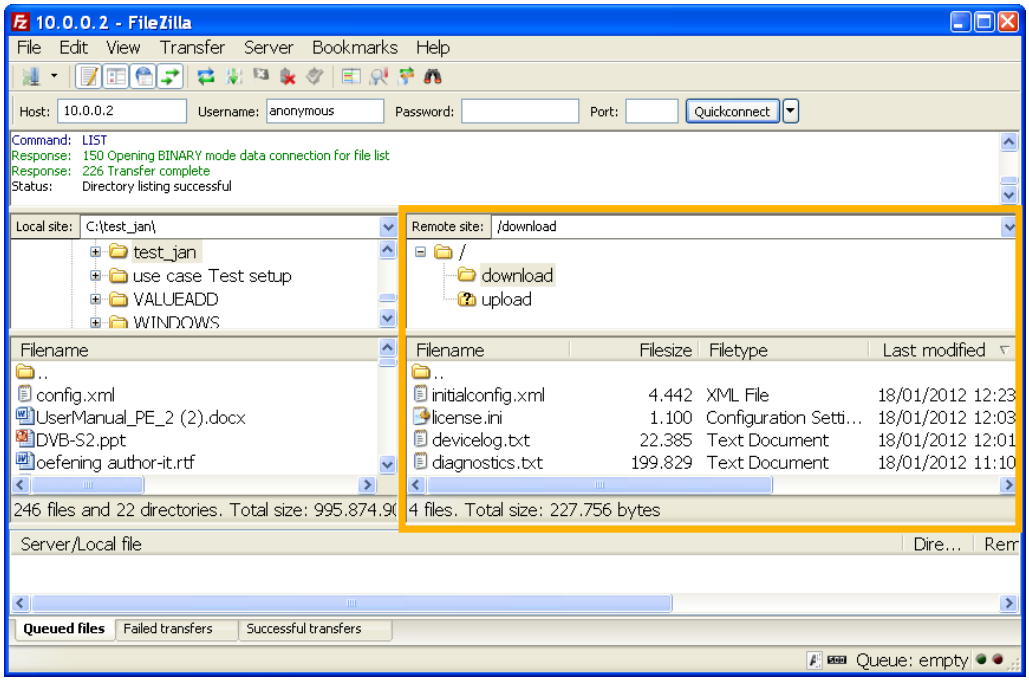
An example of such an application is FileZilla.



Downloaded or uploaded files can be consulted on the "Remote Site" in the download/upload folders.

For security reasons, updated files cannot be downloaded again.
(This to avoid that the device will be used as a file server.)

For example:


10.0.0.2 - FileZilla
File Edit View Transfer Server Bookmarks Help
Host: 10.0.0.2 Username: anonymous Password: Port: Quickconnect
Command: LIST
Response: 150 Opening BINARY mode data connection for file list
Response: 226 Transfer complete
Status: Directory listing successful
Local site: C:\test_jan\
test_jan
use case Test setup
VALUEADD
WINDOWS
Remote site: /download
/
download
upload
Filename
..
config.xml
UserManual_PE_2 (2).docx
DVB-S2.ppt
oefening author-it.rtf
246 files and 22 directories. Total size: 995.874.9
Filename Filesize Filetype Last modified
..
initialconfig.xml 4.442 XML File 18/01/2012 12:23
license.ini 1.100 Configuration Setti... 18/01/2012 12:03
devicelog.txt 22.385 Text Document 18/01/2012 12:01
diagnostics.txt 199.829 Text Document 18/01/2012 11:10
4 files. Total size: 227.756 bytes
Server/Local file
Dire...
Rem
Queued files
Failed transfers
Successful transfers
Queue: empty

10 General Device Settings and Actions

10.1 Access Control

Before implementing the device into a network it is recommended to consider which management channels need to be enabled.

It is recommended to disable unused services to prevent unauthorized access to the device. By default SNMP, CLI and FTP are enabled.

Login as expert user and navigate to the following locations to enable or disable these settings.

M6100 >> Device >> SNMP

M6100 >> Device >> CLI

M6100 >> Device >> FTP

M6100 >> Device >> Frontpanel

Once the frontpanel is put into read-only mode it can only be changed back to read-write mode via one of the other available interfaces.

For example via the CLI interface using the craft interface.
(This is useful when the management IP address has changed and the device is unreachable through IP connectivity).

10.2 License File

A license file contains the information about all the features/options that are enabled or disabled on the device.

A license file is device dependent.

When the license file is not valid, the device has limited functions.
The only possible actions are configuring the management interfaces and updating the license.

The following figure is an extract of a license file:

```
; M6100 : Broadcast Satellite Modulator
; with options :
;   All options enabled

[General]

; Generator info
generated_user = "buildsystem"
generated_time = "Thu Sep 22 00:00:00 UTC 2011"
generated_tool = "license_gen"

; Device info
device_name = "M6100"
device_serial = "30076719"
device_options = "All options enabled"

[Features]

configured_features = "asi, cleanchannelfilter, dvbs2, dvbs2s
```

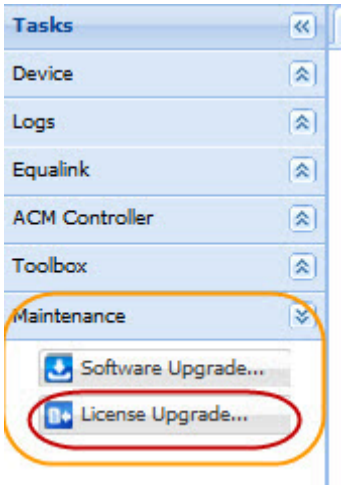
10.2.1 Import a License File

Importing a license file is done when a new functionality needs to be activated.

» Log in as **Expert** (Refer to section: *Switch User Profile on page 40*);

» Navigate to the **Tasks Pane**;

» Navigate to **Maintenance;**



» Select **License Upgrade;**

» Browse to the folder where the new license.ini file is stored;

» Select the licence.ini file and Click **Open;**

The following message is displayed:

Importing / upgrading a licence file reboots the device!

» Click **Upgrade;**

» After the upgrade, a message is displayed that the upgrade was performed successfully;

» Verify if the new functionality is active.

A license file is device dependent.

When the license file is not valid, the device has limited functions.
The only possible actions are configuring the management interfaces and updating the license.

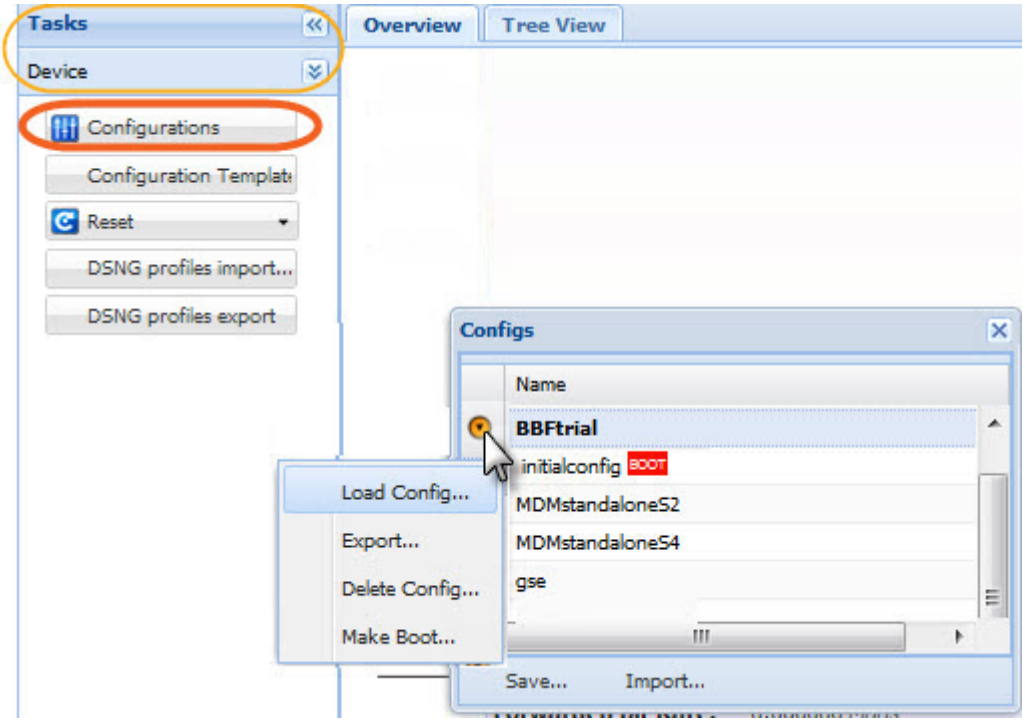
10.3 Configuration Settings

» Log in as **Operator or Expert** (Refer to section: *Switch User Profile on page 40*);

» Navigate to the **Tasks Pane** ;

» Click **Device;**

» Click **Configurations;**



From this menu it is possible to manage the configurations of the device.

Use the menu to perform the following tasks:

- Save the current configuration;
- Load a configuration;
- Import a configuration;
- Export a configuration;
- Delete a configuration;
- Make a configuration.bootable.

From the front panel it is possible to perform the following actions:

- Device Reset;
- Device Configuration Load;
- Device Configuration Save.

M6100>>Actions

10.3.1 Configuration File

There are two kinds of configuration sets stored on the device:

- Configuration files with device specific parameters;
- Configuration files with application specific parameters.

Device Specific Parameters

These parameters are used to set up device specific settings and they are excluded from the imported/exported configuration files. This is done to avoid losing connectivity with the device after loading a new configuration file or after a redundancy switch-over. The device specific parameters are:

- Mgmt Gateway IP Address;
- Mgmt Interface IP Addresses;
- Data Interface IP Addresses;
- Device Identification Label;
- Link Redundancy priority (None, Mgmt1 or Mgmt2, Mgmt1 before Mgmt2, …);
- Device Redundancy state (Enable, Initial State, Operational State).

The device specific parameters cannot be consulted or exported to an XML file.

Application Specific Parameters

These parameters are specific for the application settings.

All these settings are stored in an XML file. The following figure is an extract of such an XML file.

The XML or configuration file provides the possibility to import or export the device application specific parameters. This configuration file can be useful as a back-up file, to debug or configure the device offline.

It is possible to store up to 48 different configuration files. These files can be imported and exported

To view or download a configuration file, refer to section: *Export a Configuration. on page 86*

Configurations can be reused among devices where the same licenses are applicable.

10.3.2 Active Configuration

The active configuration is the configuration that is currently used on the device.

The active configuration is not necessarily a configuration that is saved on the device. When a configuration is completed, it is recommended to save this configuration onto the device.

Check the LED **Cfg saved** in the status bar to see if the active configuration is currently saved or not.

10.3.3 Saved Configuration

A saved configuration is a configuration that can be recalled at any time by an operator to modify the device behavior according to pre-defined settings.

For example: perform tests or prepare a migration of the device settings.

» Navigate to the **Tasks Pane** (GUI) to check the available configurations;

» Click **Device;**

» Click **Configurations**. (The available configurations are listed.).

The active configuration is indicated in bold.

The boot configuration is a loaded on the device during a reboot. (The boot configuration is recognized by a boot BOOT.-flag)

10.3.4 Save a Configuration

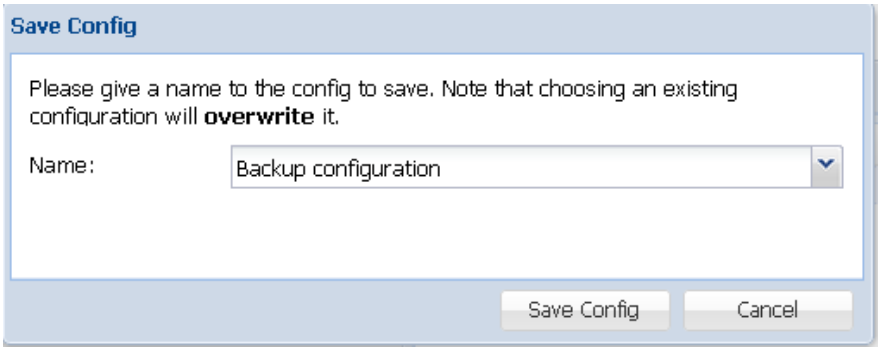
When parameters are changed, they are not directly saved into the active configuration.

» Navigate to the **Tasks Pane** to check the available configurations;

» Click **Device;**

» Click **Configurations;**

» Click **Save…**



» Enter a **Name** or select a configuration using the **drop down list**.

Use this menu to **Save** the current configuration.
Saving the current configuration makes it the default configuration.

This does not mean that it becomes the boot configuration.

By default, the selected configuration is overwritten upon saving. Enter a name to save the configuration under a new configuration file.

10.3.5 Import a Configuration

Import a configuration file that can be used as a new configuration.

» Navigate to the **Tasks Pane** to check the available configurations;

» Click **Device;**

» Click **Configurations;**

» Click **Import;**

» Browse to the correct folder and select the correct config.xml file.

Please note that after an import of a configuration, the configuration is not loaded automatically.
This requires an additional load step, refer to *Load a Configuration. on page 85*

The configuration file must comply with the available configuration options and activated licences on the device.

Note: If the BISS setupID of the device is not the same as the BISS setupID of the device having generated the configuration, the copy will result in corrupted BISS parameters. (Refer to section: *Basic Interoperable Scrambling System (BISS) on page 192*. If one of the setupIDs is zero, this will generate an error, unless the import/export is done on the same device (backup function).

10.3.6 Load a Configuration

Use this procedure to load a configuration file that is available in the configuration list.

The loaded configuration becomes the active configuration.

» Navigate to the **Tasks Pane** to check the available configurations;

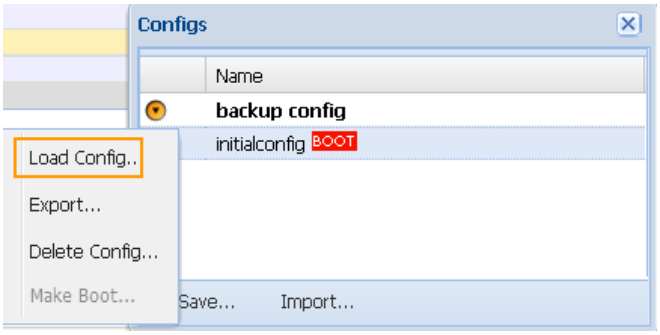
» Click **Device;**

» Click **Configurations;**

» Click the **Config Name** you want to load;

» Click the following icon ;

» Click **Load Config…**



10.3.7 Export a Configuration

Use this to export a configuration file.

Depending on the management interface GUI or CLI the following is done:

- GUI: the file is downloaded by the browser;
- CLI: the file is available on the FTP server.

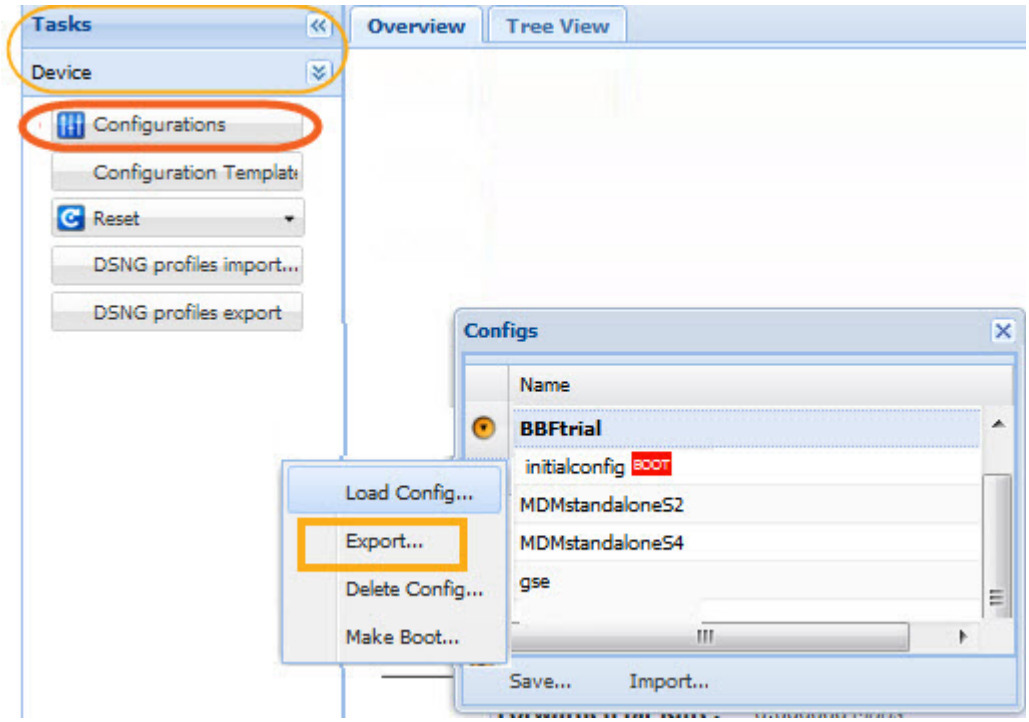
» Navigate to the **Tasks Pane**;

» Click **Device;**

» Click **Configurations;**

» Click the  in front of the **Config Name** you want Export;

» Click **Export** to export the XML file to a default folder (GUI) or to the FTP server (CLI).



The exported file can be:

- Used as a backup file;
- Edited offline and reused on another device In this case,
  - Make sure that the configured options and activated licences are the same on both devices.
- Forwarded for debugging purposes.

10.3.8 Delete a Configuration

Delete a configuration file from the device when it becomes obsolete.

» Navigate to the **Tasks Pane;**

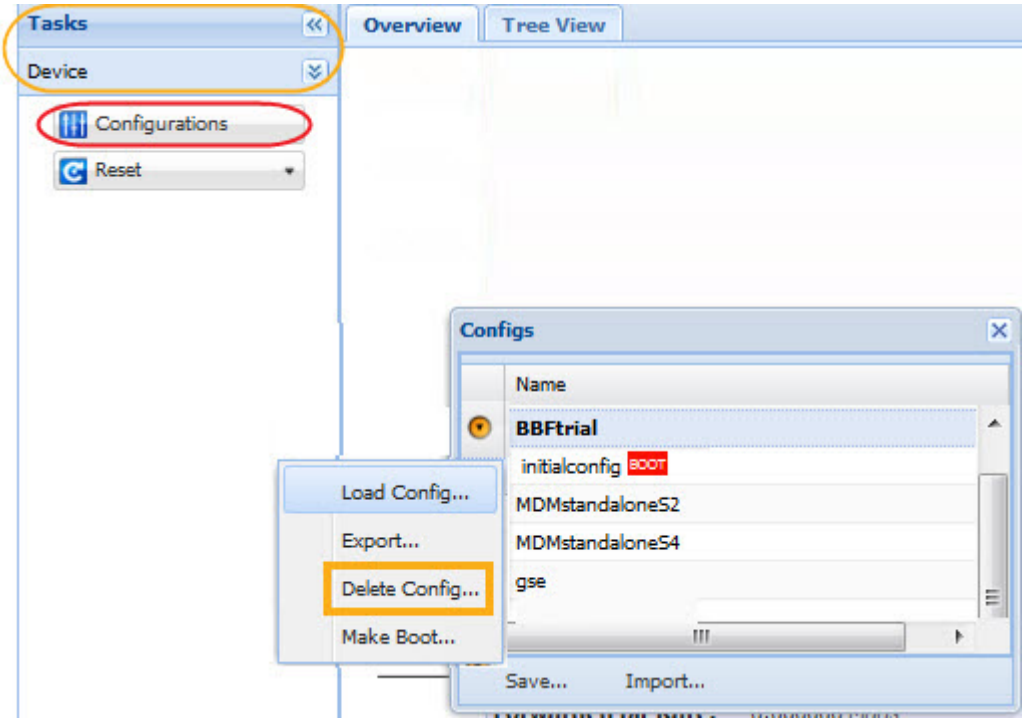
» Click **Device;**

» Click **Configurations;**

» Click the **Config Name** you want delete;

» Click the following icon  ;

» Click **Delete…**



Deleting a boot configuration causes a factory reset of this boot configuration!
All application specific parameters are reset to their default values.

Traffic can be impacted.

10.3.9 Make a Configuration File Bootable

» Navigate to the **Tasks Pane;**

» Click **Device;**

» Click **Configurations;**

» Click the following icon ;

» Click the **Config Name** you want make the boot configuration;

» Click **Make Boot** to make the selected configuration the boot configuration.

– The boot configuration is indicated as BOOT.

A boot configuration is used to set all parameters to their correct value at boot time. This implies that the management parameters (for example redundancy settings), Input / Output parameters are set according to the network requirements.

Once you have configured the device it is recommended to save the configuration and make the configuration bootable.

This is mandatory in order to keep the configuration after a power interruption.

Refer to section: *Save a Configuration on page 84*.

10.4 Software Upgrade

A software upgrade is needed in two cases:

- To provide bug fixes and/or software enhancements;
- To activate a new functionality in the device.

The upgrade procedure is explained on the next page.

This activation/upgrade can require a license update as well. Refer to section: *Licence File on page 79* .

Depending on the ordered Care Pack the customer will be informed when a new software release is available. For more information on the Care Pack please refer to section:
Care Packs.

10.4.1 Software Upgrade Procedure

Use the applicable software upgrade file (installer.bin).

Proceed as follows to perform a software upgrade:

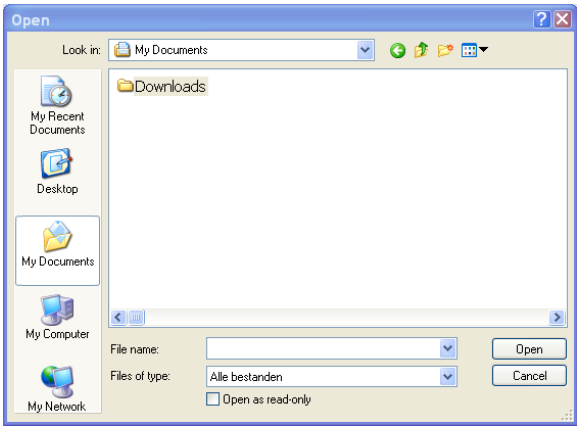
» Log in as **operator** or **expert;**

» Navigate to the Tasks Pane;

» Click **Maintenance**;

» Click **Software Upgrade....**

The following window opens:



» Browse to the folder where the "installer.bin file" is stored;

» Select the file and click **Open**.
The following message is displayed:

Software Upgrade:
This operation will reboot your device!
Are you sure, you want to upgrade the device firmware with the content of "installer.bin"?

» Click **Upgrade.**
Refresh the browser after about 40 seconds.

To perform a software upgrade using the CLI please refer to section: Software Upgrade (CLI).

10.5 Device Identification

M6100 >Device >> Identification

This menu provides an overview of the general device identification. Use this part to:

- Enter a logical device label for easy recognition of the device in a system setup;
- Look up the following:
  - Label;
  - Serial number;
  - Unique ID;
  - Product;
  - Type ID;
  - Device Description;
  - Type ID;
  - Hardware Revision;
  - Software ID;
  - Software Version;
  - Device options (displays the sales code and the code description)
    This displays the current options of the device.

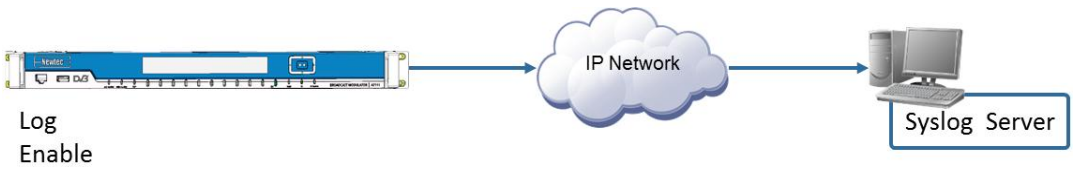
10.6 Logging

M6100 >Device Setup >> Logging

Enable or disable logging.

Logging can be performed on the following levels:

- Local device logging;
  Log files can be exported or cleared, refer to *Export or Clear Logging. on page 93*
- Remote logging using a remote syslog server (Syslog is a standardized mechanism for logging in computer systems.).



When remote logging is enabled and a remote IP address is inserted all logging information is forwarded to this address. The logging messages are packed in UDP (User Datagram Protocol) and sent to a specific UDP port (514 according to the syslog standard).

10.6.1 Syslog Filter

It is possible to assign up to nine different log levels to the following facilities.

Facility	Log Description
Alarms	An alarm is detected on the device.
Configuration	Configuration changes on the device.
System	System changes on the device.
Internal error	An internal error is detected on the device.
Authentication	User logged in.
Networking	Everything related to network interfaces.

Facility Overview of the Log File

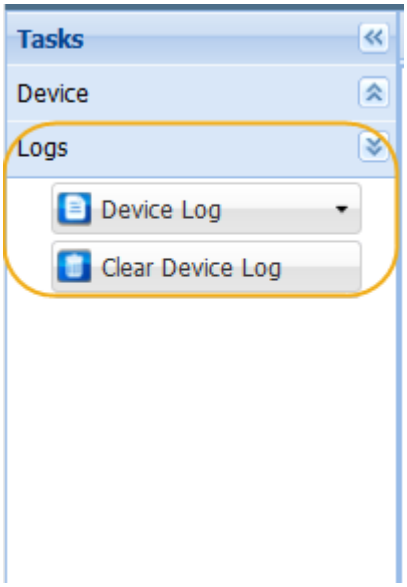
The default log level is hard coded. The lower the filter level, the more entries appear in the log file which may adversely impact the performance of the device.

Level	Description
Emergency	The system is unusable.
Alert	Action must be taken immediately.
Error	Critical conditions.
Warn	Normal but significant condition.
Notice	Notification messages.
Info	Informational messages.
Debug	Debug level messages.
Trace	Debug level messages.
Off	No logging is performed.

10.6.2 Export or Clear Logging

» Navigate to the **Tasks Pane;**

» Click **Logs;**



» Click **Device Log.**

Use this menu to **View** or **Download** the local board logging.

- When a view is requested, the log file is opened in a separate browser.
- When a download is requested, a text file is downloaded.

- When a **Clear Device Log** is requested, the logging information is removed. A new log file is started. This can be useful to perform debugging.

10.6.3 Interpretation of a Device Log File

A standard log file looks as follows:

[configuration-INFO][2012-12-16 10:27:53] writeValue /Root/SystemAlarm/Log/Source=GeneralInterface

[alarms-INFO][2012-12-16 10:27:54] alarm General Interface: OFF

Facility	Log Level	Time Stamp	Extra information about the action taken
[configuratio n	- INFO]	[2012-12-16 10:27:53]	writeValue /Root/SystemAlarm/Log/So urce=GeneralInterface
[alarms	-INFO]	[2012-12-16 10:27:54]	alarm General Interface: OFF

10.7 Diagnostics Report

Use this to get an overview of the complete configuration and get debugging information of the device. This report can be requested by the Customer Service department to perform debugging on the device. In most cases it is advised to let the Customer Service department analyze this report.

The document can be viewed using the GUI or downloaded as a text file.

Proceed as follows:

» Navigate to the **Tasks Pane;**

» Click **Toolbox;**

» Click **Diagnostic Report;**

» Select one of the following,

– **View**: opens the report in a separate browser window;

– **Download**: Downloads a diagnostics.txt file;

– **Download (Debug)**: This downloads an encrypted diagnostics report file and is only for use by our the Customer Service department.

The following figure is an extract of a diagnostics report:

```
************************************************************
*     DIAGNOSTICS REPORT date="2000-07-22 02:31:37"
************************************************************



************************************************************
*     Build info
************************************************************
<?xml version="1.0" standalone="yes"?>
<BuildInfo Buildtype="RMT" Release="  DevNr _1.0.0" Timestamp="20121003142250" Node="76382" />
OK


************************************************************
*     FPGA info
************************************************************
VersionRomWbdl: ntc6429, 1.2, 20-09-2012,17:49


```

```

************************************************************
*     Current volatile configuration
************************************************************
<?xml version="1.0" standalone="yes" ?>
<Configuration>
    <Root>
        <Device>
            <Identification Label=" Device Name and Number " />
            <FrontPanel Enable="on" AccessLevel="operator" />
            <Snmp Enable="on">
                <Authentication ReadOnlyCommunity="public" ReadWriteCommunity="private" />
                <Notifications>
                    <Destination Destination="1" IpAddress="0.0.0.0" Type="trapV2" Community="trapcom" />
                    <Destination Destination="2" IpAddress="0.0.0.0" Type="trapV2" Community="trapcom" />
                </Notifications>
            </Snmp>
            <Cli Enable="on" RemoteEnable="on" InactivityTimeout="600" />
            <Gui Enable="on" />
            <Ftp Enable="on" Anonymous="on" />
            <Log>
                <Local Enable="on" />
                <Remote Enable="off" IpAddress="0.0.0.0" UdpPort="514" />
```

10.8 Date and Time

M6100 >> Device Setup >> Date and Time

Navigate to this location to set or check the device date and time.

NTP (Network Time Protocol)

M6100 >> Device Setup >> NTP

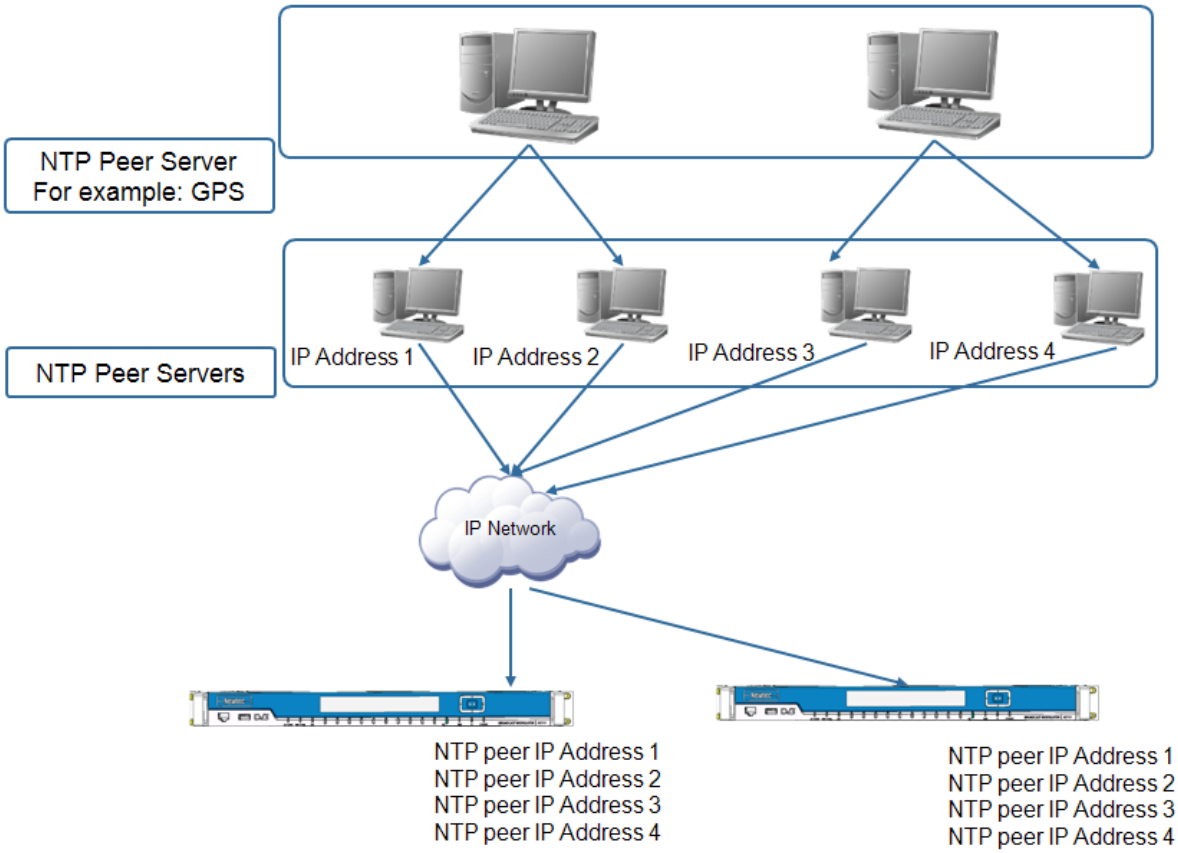
By default, NTP is disabled.

The NTP protocol is used to synchronize the clocks of different devices over a network. It is based on the principle of having all machines get as close as possible to the correct UTC time (Coordinated Universal Time).

Enter the different NTP peer IP Addresses to which must be synchronized.
The M6100 Boadcast Satellite Modulator acts as a client and periodically queries the server for a precise UTC time reference.

It is possible to enter up to four NTP peer IP addresses.

It is recommended to enter more than one NTP peer IP Address to increase the reliability of the network synchronization.



When the NTP peer addresses are inserted, time and date of the M6100 are updated with the received information as soon as the M6100 can connect to one of the NTP peer servers.

10.9 Device Monitoring

M6100 >> Device Setup >>Monitor

The following device level parameters are monitored.

- Temperature;
- Board Power supply;
- CPU (Central Processor Unit) load;
- Memory usage;
- Uptime.

10.10 Reset the Device

Resetting the device causes data loss on an active link!

When a user wants to perform a reset using the front panel or CLI, no caution message is displayed!

The device can be reset when needed.

» Navigate to the **Tasks Pane;**

» Click **Device;**

» Click **Reset.**

Different reset types are possible:

- **Hardware**: Resets the software and the hardware (=reboot);
- **Software**: Resets the software;
- **Configs**: Resets the application specific parameters.
  For connectivity reasons, the device specific parameters are **excluded** from this reset.For more information please refer to section: *Configuration File on page 82*
- **Factory**: Resets all parameters to their default values.
  This action is only possible via the CLI interface.

A factory reset removes all stored configurations.

All IP settings are reset to their default values, meaning that the device may become unreachable!

10.11 Alarm Handling

Alarm handling allows you to configure and manage the behavior of the different alarms in the device.
Meaning that it is possible to

- mask (hide) alarms;
- assign alarms to a general interface or general device alarm.

Navigate to the following location to perform alarm handling.

M6100 >> Device Setup >Alarm Handling

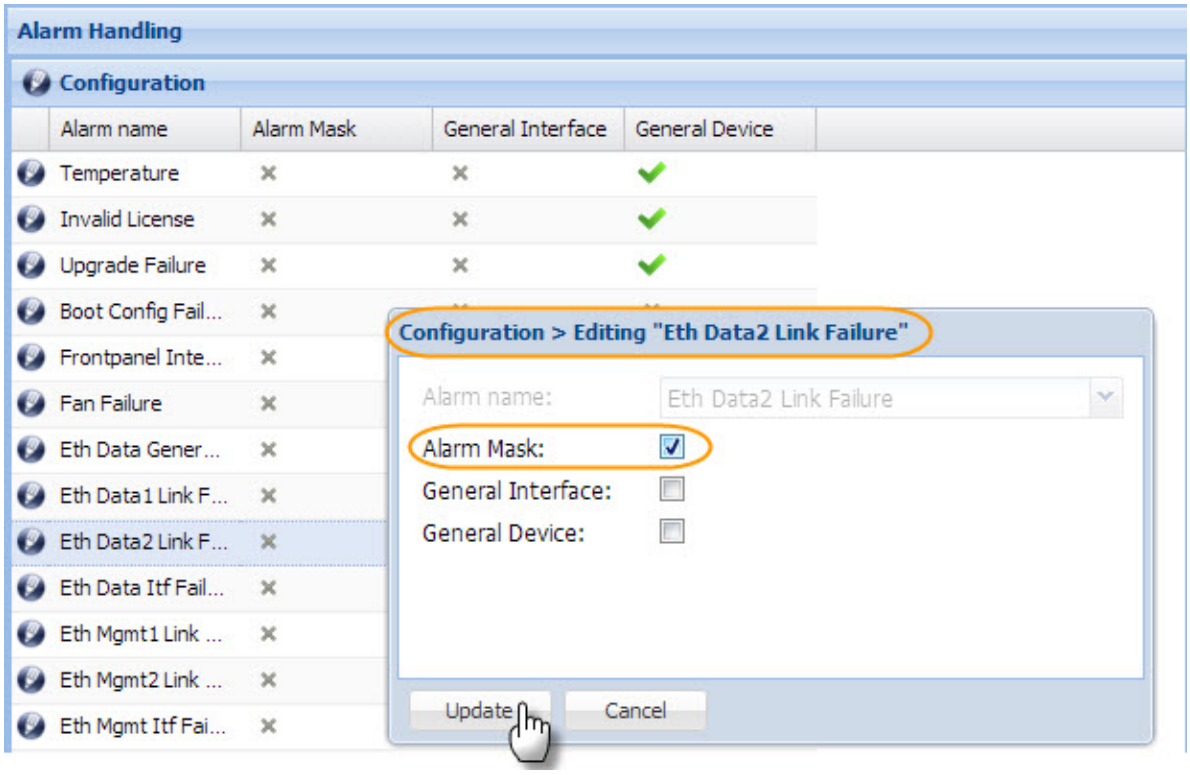
List of Alarms

For a comprehensive list of alarms, refer to *Appendix A - Alarm List on page 210*

This function is available via the GUI, CLI and SNMP but not through the front panel:

10.11.1 Alarm Masking

You can mask individually selected alarms. This means that you can hide alarms.



Be careful when configuring this, as a masked alarm is not recognized anymore by the M6100.

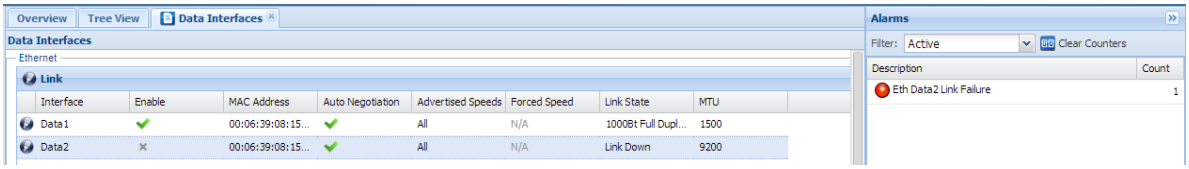
Alarm masking can also impact device redundancy, this because the alarm is not propagated into a general device or a general interface alarm.

For more information please refer to section: *Alarm Configuration. on page 103*

Example on the behavior of a masked alarm.

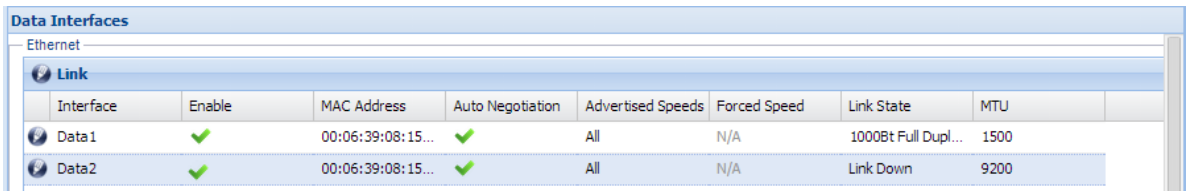
Eth Data2 Link Failure: Alarm Mask = Off

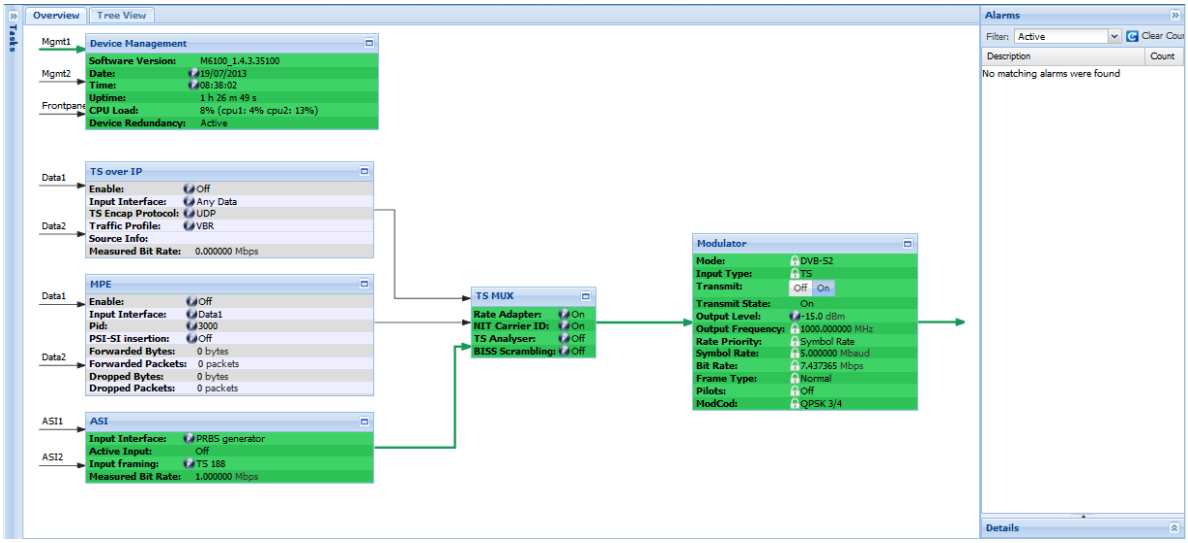
1. No active alarms are present (normal behavior of the M6100);
2. The Ethernet cable of Eth Data2 is removed;
3. The Eth Data2 Link Failure alarm is raised.
   - On the front panel the active alarm LED lights up according to the alarm that is present;
   - On the overview page of the GUI the Data2 arrow turns red;
   - The Alarm Pane shows the following:



Eth Data2 Link Failure: Alarm Mask = On

1. No active alarms are present;
2. The Ethernet cable of Eth Data2 is removed;
3. The "Eth Data2 Link Failure" alarm is masked so no alarms are triggered!





10.11.2 Alarm Configuration

The alarm configuration provides the flexibility to define per Alarm, whether or not the alarm is linked to a General Interface and/or General Device alarm.
This way the customer is able to define whether or not this specific alarm triggers a redundancy switch over as the redundancy system bases a switch over on one of these two alarms.

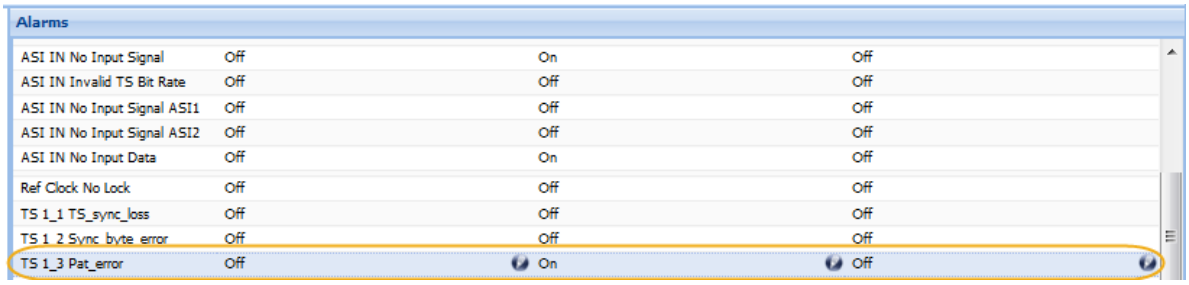
Be careful when changing the alarm configuration, as the general interface and general device alarms, are there to protect your device in critical situations.

For example, the "Temperature alarm", by default generates a general device alarm. The general device alarm switches off the main functional blocks of the M6100, to reduce the CPU load of the device.
In case the default setting is overruled and the general device alarm is not triggered, the device can become overheated.

The alarms are still recognized by the M6100 meaning that the alarm is displayed in the alarm pane and that the related functional block/arrow in the GUI changes color (turn red). On the front panel the active alarm LED lights up according to the alarm that is present.

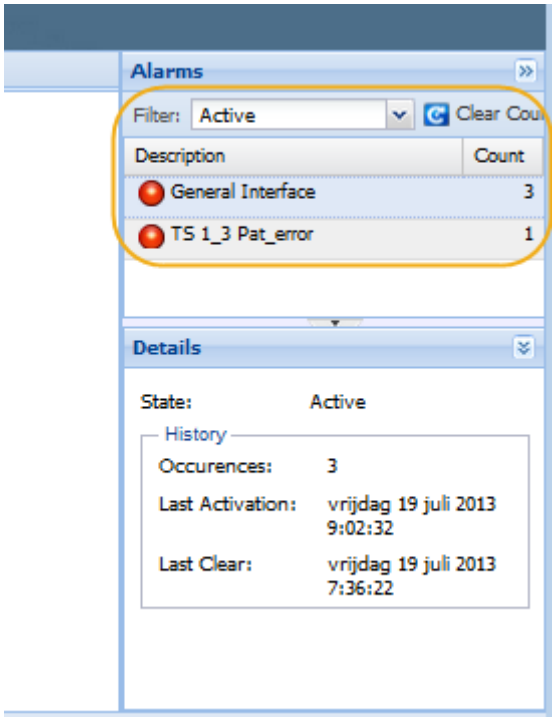
For example:

TS 1_3Pat Error Alarm must generate a General Interface alarm. (because this could be a reason that a switch to a redundant device is necessary).



When a PAT error is present, the general interface alarm is also triggered and displayed in the alarms pane.

The following figure shows the alarms pane.

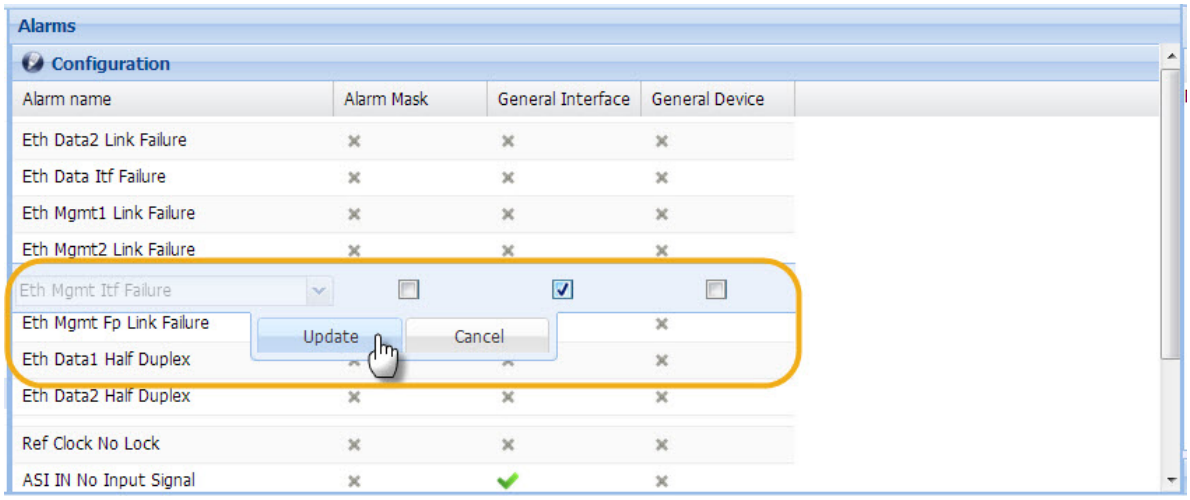


We want that the "Eth. Mgmt Itf Link Failure" alarm triggers a General Interface Alarm.

(The reason could be that this alarm must trigger a switchover to a redundant device).

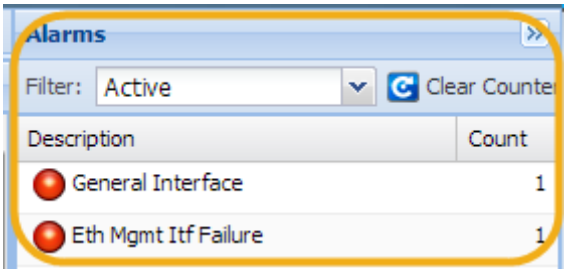
Note that a "Mgmt Itf Failure" by default does not trigger the alarm switches. To change this behavior you have to assign the "Mgmt Itf Failure" alarm to a General Interface or General Device alarm. (Whether to choose the General Interface or General Device alarm depends on the configuration of the USS (Universal Redundancy Switch).

The following figure shows the configuration of the "Eth Mgmt Itf Failure" alarm.



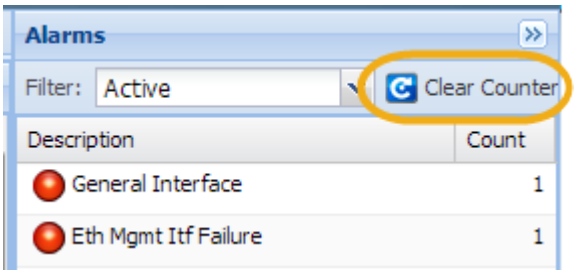
The next time when the Eth Mgmt Itf Failure alarm is present, a General Interface alarm is triggered.

The following figure shows the alarms pane.


Alarms
Filter:
Active
Clear Counte
Description
Count
General Interface
1
Eth Mgmt Itf Failure
1

10.11.3 Clear Alarm Counters

Alarm counters as presented in the *Alarms Pane on page 48* of the GUI and can be cleared all at once.



10.12 Reference Clock

M6100 >> Ref Clock

Configure the reference clock.
This reference signal for an outdoor BUC can be multiplexed on the L-band Tx interface.

A reference clock can be generated internally (default) or slave on an external source.

The internal reference clock is 10MHz.
The clock reference has the following specifications:

10MHz Ref	Specifications
Internal clock reference	Stability ± 2000 ppb over 0 to 70°C Ageing ± 1000 ppb/year
Very High Stability (optional)	Stability ±2x10e-9 over 0°C to 65°C Ageing: ± 0.5 ppb/day ± 500 ppb/10 year

When an external source is selected, the following frequencies can be inserted.

1MHz, 2MHz, 5MHz, 10MHz or 20MHz.

Select the external clock reference for synchronization with other devices to have a higher stability than the internal default stability.

10.13 Device Redundancy

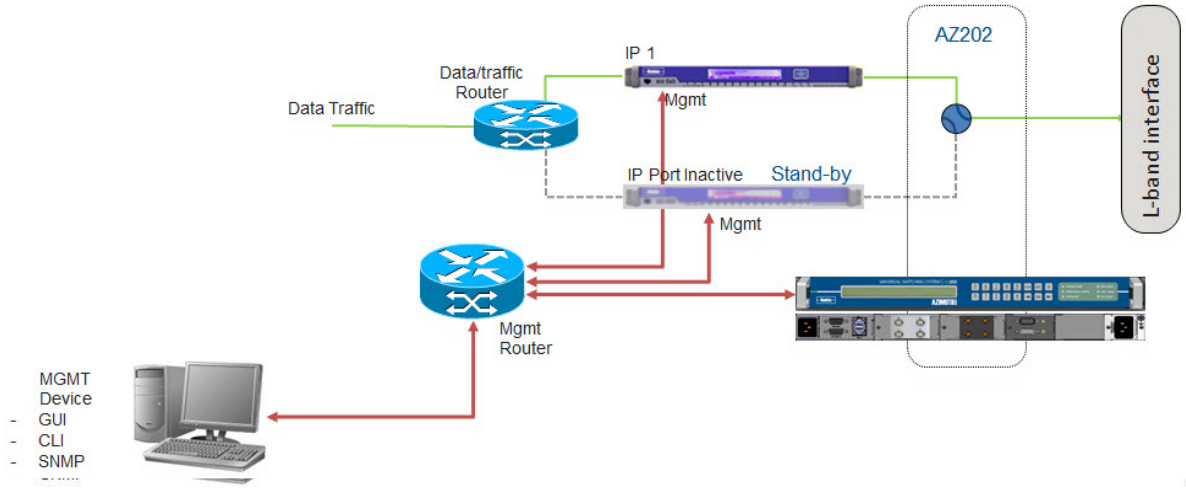
Redundancy is very important as a single failure of the M6100 affects many services at the same time.

Reliable operation of the M6100 in a satellite network is of key importance. The M6100 works seamlessly together with the Newtec AZ202/AZ212 redundancy switches to provide best-in-class system uptime.

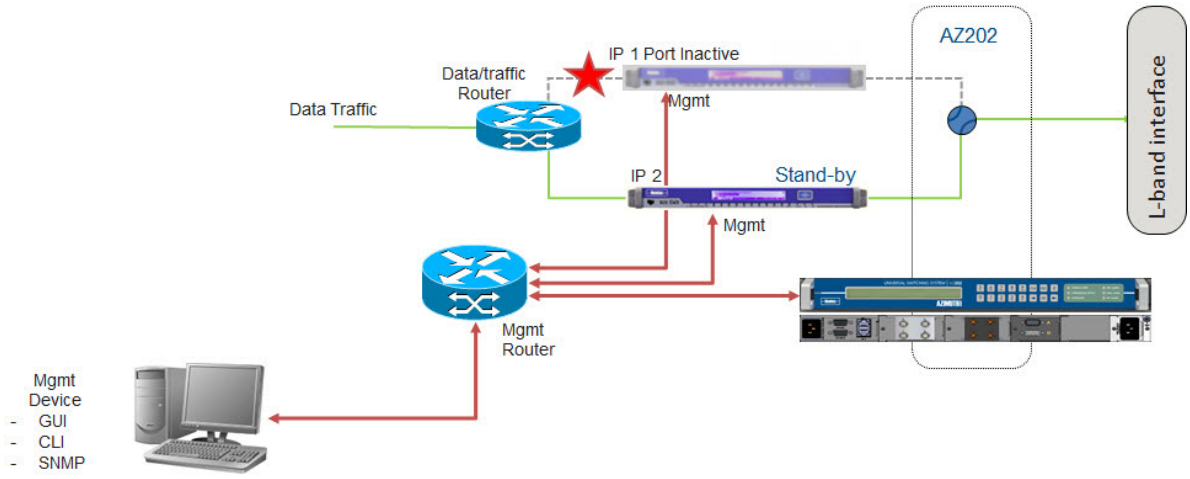
Refer to the user manual of the AZ202/AZ212 Universal Switching System.

The following figures shows a 1+1 protection scheme built up with the AZ202 switch, one in normal operation and one in redundant operation.

Normal Operation



Redundant Operation



To Enable or Disable device redundancy go to the following location:

M6100 >> Device >> Redundancy

By default, device redundancy is disabled.

Initial Redundancy State:

- Standby (default value): This means when the device starts up and redundancy is enabled, the initial state of the redundancy is standby. Typically:
  - The modulator output is disabled;
  - No IP Address on the data interface.
- Active.

11 Data Interfaces

11.1 Data Ethernet Interfaces

The data interfaces can be configured on the following location:

M6100 >> Data Interface >> Ethernet

- Data1 (This port is the top port on the back panel indicated as data1);
- Data2 (This port is the bottom port on the back panel indicated as data2);

When link redundancy is needed, Data1 and Data2 must be enabled and auto negation must be on. To enable link redundancy, refer to section:
Ethernet Link Redundancy. on page 112

Per interface, the following information is displayed.

• Default interface name; (read only) • Enabled (On/Off); • MAC address; • Auto Negotiation (On/Off);	• Advertised Speeds; • Forced Speed; • Link State. • MTU (Maximum Transmission Unit) Range: 68 - 9582

Statistics

M6100 >> Data Interface >> Statistics

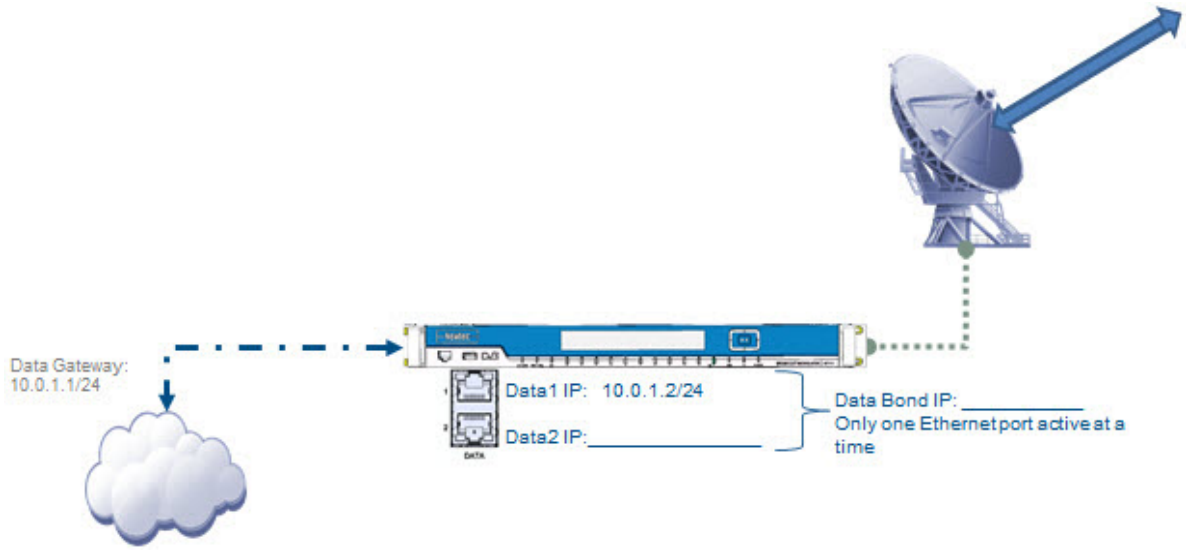
This provides an overview of the traffic that is passing over the different Ethernet ports.

The following statistics are displayed:

• Input Bytes; • Input Packets; • Input Dropped; • Input Errors;	• Output Bytes • Output Packets; • Output Dropped; • Output Errors.

11.2 Data IP Connectivity

The following figure is an example of a setup:



Use a network drawing to define the data input interfaces:

Make sure that the source device and the M6100 belong to the same IP range or the content is routed to the correct Data IP address.

M6100 >> Data Interface >> IP Address

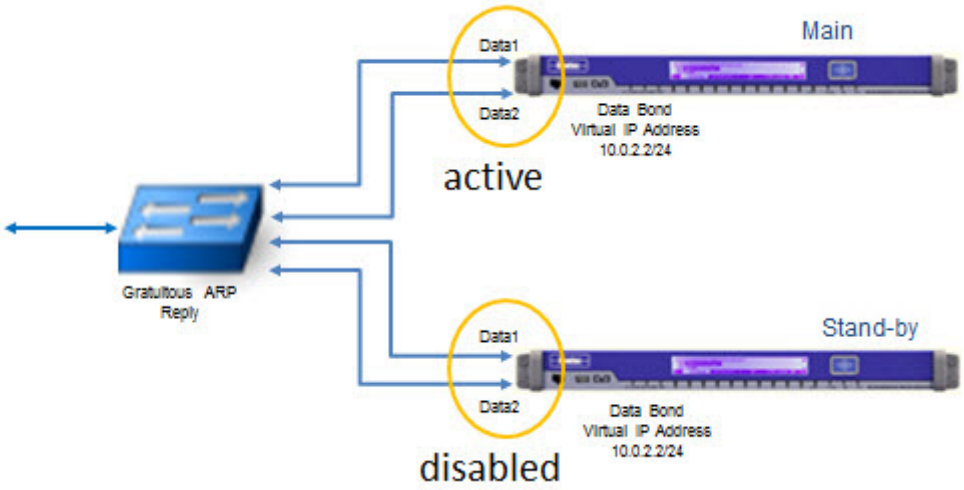
By default, the data IP addresses are 0.0.0.0/24:

- Data Gateway: This is the access point for the data port of the device;
- Data1 (Physical Ethernet interface);
- Data2 (Physical Ethernet interface);
- Data Bond (This IP address is used to perform link redundancy, effectively combining Data1 and Data2 into one new interface).

11.2.1 Virtual IP Address

Use virtual IP Addresses when working with device redundancy and a USS (Newtec's Universal Switching System).

The virtual IP Addresses are configured on the main device. These are automatically synchronized to the stand-by (spare) device. The moment the main device goes into alarm the Stand-by device inherits the IP address of the main modem. A gratuitous ARP (Address Resolution Protocol) Reply is sent to the Ethernet switch in order to update it's MAC table and reroute the traffic to the correct port.



M6100 >> Data Interface >> IP Address

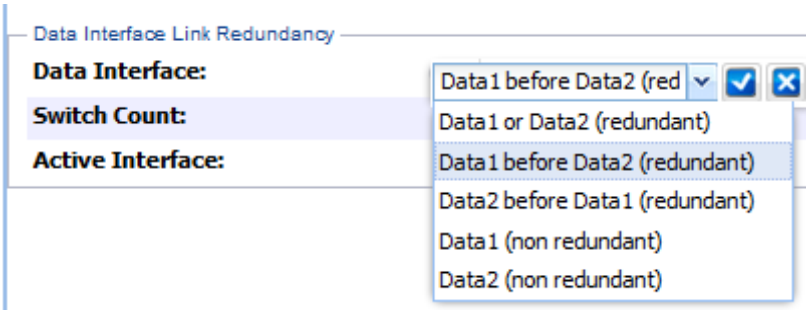
11.3 Data Ethernet Link Redundancy

It is possible to enable link redundancy (also known as bonding) on the management and data Ethernet interfaces. Link redundancy is used to eliminate downtime as much as possible in the system setup. This to increase the reliability of the system.

When Ethernet interface redundancy is enabled, two interfaces behave as one virtual interface (bond interface): only one of the two physical interfaces is active at a time. When the link state of the active interface goes down (physically broken connection), the other interface takes over the operation.

Refer to the following figure:

M6100 >> Data Interface >> Link Redundancy



Options	Descriptions
Data1 or Data2 (Data)	The bonding interface is active. There is no preference in priority between the two available interfaces.
Data1 before Data2 (Data)	The bonding interface is active. Interface Data1 has priority over interface Data2. This means that when Data1 is available, this will be the active interface.
Data2 before Data1 (Data)	The bonding interface is active. Interface Data2 has priority over interface Data1. This means that when Data2 is available, this will be the active interface.
Data1 (Non redundant)	The bonding interface is not active! Data1 is the active interface!
Data2 (Non redundant)	The bonding interface is not active! Data2 is the active interface!

To configure the bond interface, refer to section: *Data IP Connectivity on page 110*.

To have bonding working properly make sure to configure the switch/router in such a way that the spanning tree is not blocking the fast switchover between ports.

In a typical Cisco switch configured using rapid spanning tree this is achieved by setting the ports in PortFast mode.

11.4 ASI Input

Configure the ASI input interfaces on following location.

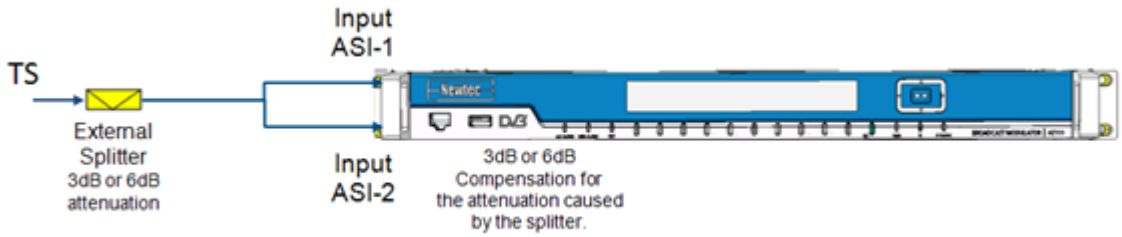
M6100 >> ASI Input >> Input Selection

The two ASI inputs make it possible to create a link redundant interface input.

Selection	Description
None	The ASI input is disabled and incoming traffic is discarded.
ASI1	Enables the ASI1 input, traffic is inserted on this interface.
ASI2	Enables the ASI2 input, traffic is inserted on this interface.
ASI or ASI2	When a valid ASI signal is detected, the active input remains selected. When no valid ASI signal is detected a switch is performed towards the other ASI interface. No switchback is performed when the problem on the original interface is resolved.
ASI1 before ASI2	When a valid ASI signal is detected on ASI1, this input remains selected. When no valid ASI signal is detected on ASI1, a switch is performed towards the ASI2 interface. A switchback is performed when the problem on the ASI1 input is resolved.
PRBS generator	Activate the internal PRBS (Pseudo Random Bit Sequence) generator. This option is selected to perform basic tests on the device or network. For more information please refer to section: *PRBS Generator. on page 174*

11.4.1 In-line Splitter

Use this parameter to compensate for an attenuation that is present due to the use of an external passive splitter. It is possible to compensate for 3dB or 6dB attenuation.



When a passive splitter is used and this compensation is not enabled, the incoming signal might be degraded too much so that a correct modulation cannot be guaranteed.

11.4.2 Input Framing

Configure the input framing type.

M6100> ASI Input > Input Framing

The incoming packets can be:

- TS188 (transport stream with 188-byte packets);
- TS204 (transport stream with 204-byte packets, 188 bytes with 16 bytes for error correction).

The 16 bytes for error correction (overhead) are removed before the actual modulation takes place.

When the incoming packets are not corresponding to the configured framing type, the following alarm is generated: ASI IN No Input Signal ASI1.

11.5 ASI Output

The ASI output can be used to perform monitoring on incoming signals.
The ASI output are loop through on BNC (F) - 75 ohms (coax).

The ASI output can be used to bring out one of the following input selections:

M6100>ASI Output >> Signal Selection

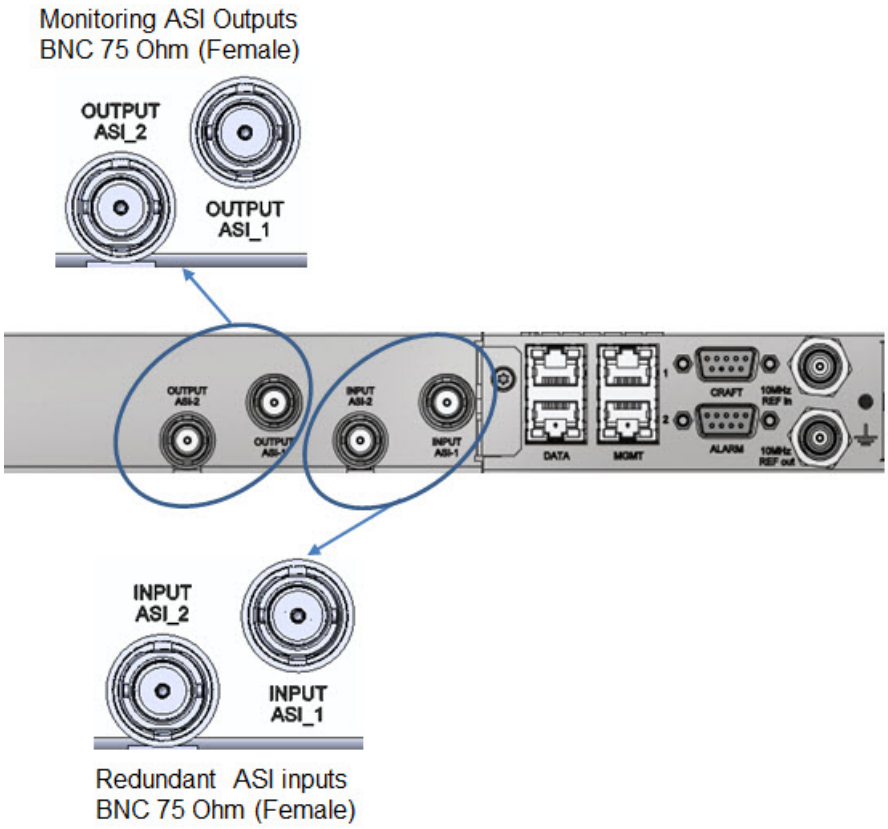
- Modulator Input, this is the signal output from the TS MUX block.
  This way the signal can be monitored when extra processing (such as rate adaptation) has been performed.
- Active ASI input;
- Inactive ASI input;
- PRBS generated signal, we also refer to section: *PRBS Generator on page 174*.

The output selection defines where the signal will be available.

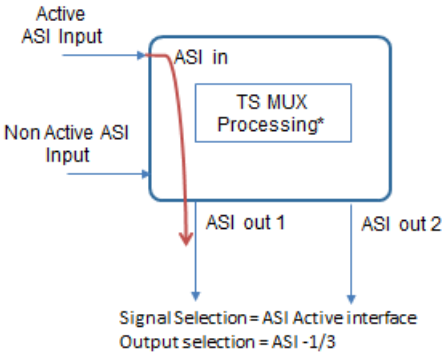
M6100>ASI Output >> Output Selection

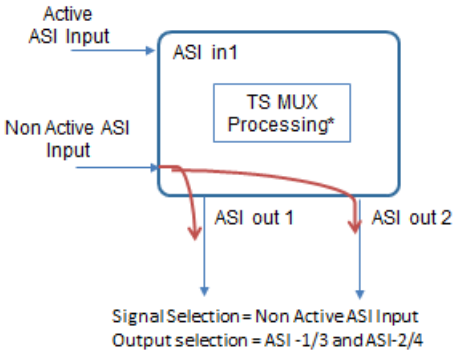
Depending on the hardware version of the device the back panel has four or six ASI interfaces available.
This is also reflected in the output selection parameters. The following sections shows the behavior in case of a back panel with four ASI and six ASI interfaces.

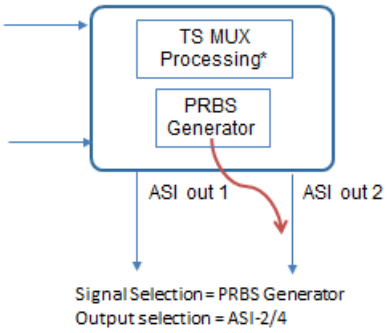
Four ASI interfaces available on the back panel (hardware before R1.4)

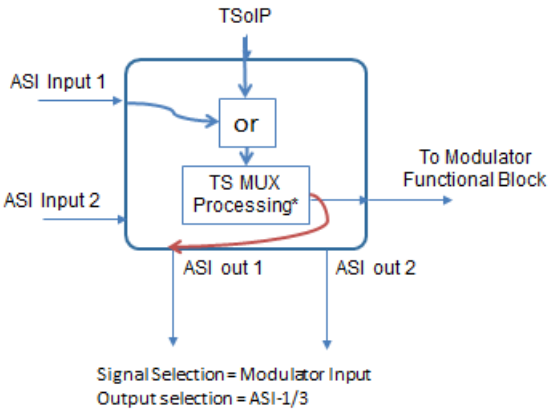


The following figures show different possibilities of output selection and to which output interface the signal is forwarded. (see next page)

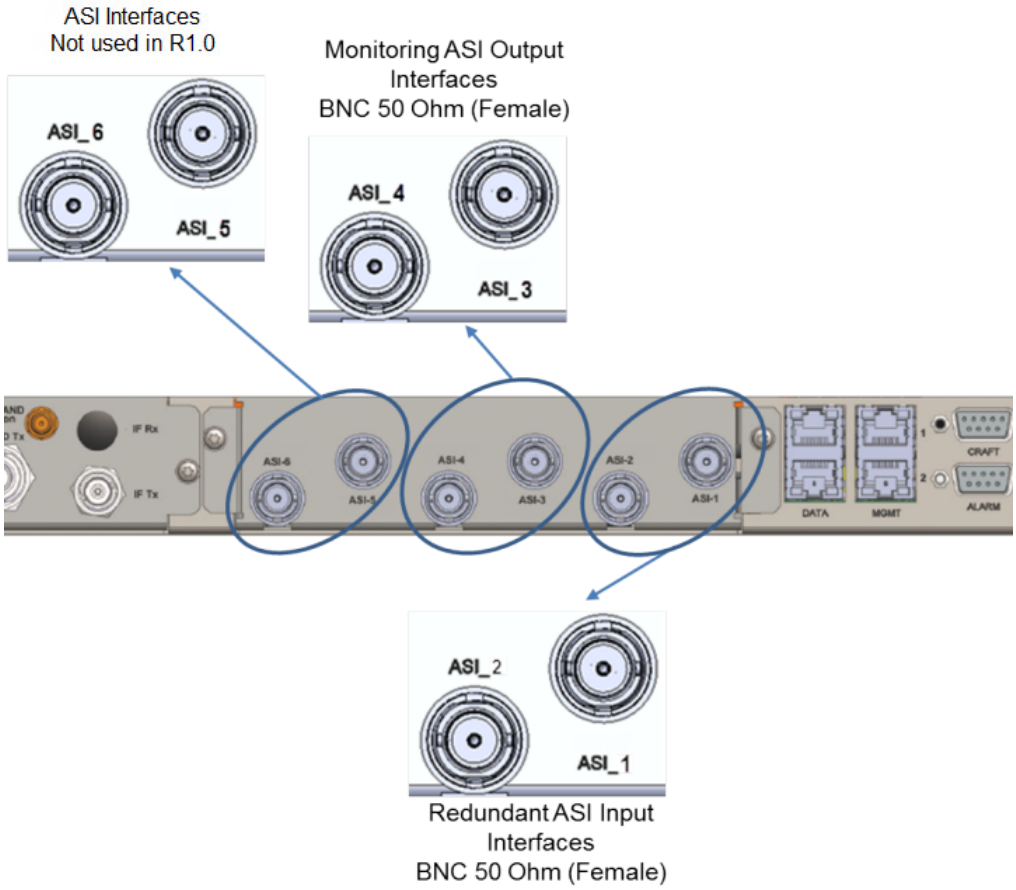

Active
ASI Input
ASI in
TS MUX
Processing*
Non Active ASI
Input
ASI out 1
ASI out 2
Signal Selection = ASI Active interface
Output selection = ASI -1/3


Active
ASI Input
ASI in1
TS MUX
Processing*
Non Active ASI
Input
ASI out 1
ASI out 2
Signal Selection = Non Active ASI Input
Output selection = ASI -1/3 and ASI-2/4

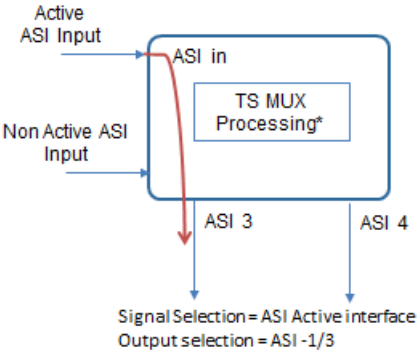

TS MUX
Processing*
PRBS
Generator
ASI out 1
ASI out 2
Signal Selection = PRBS Generator
Output selection = ASI-2/4

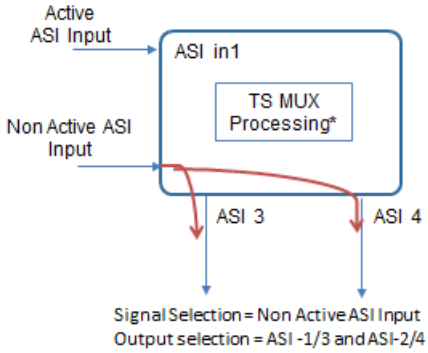

TSoIP
ASI Input 1
or
To Modulator
Functional Block
ASI Input 2
TS MUX
Processing*
ASI out 1
ASI out 2
Signal Selection = Modulator Input
Output selection = ASI-1/3

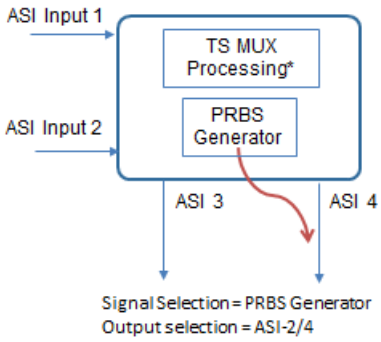
Six ASI interfaces available on the back panel (from R1.4 onwards)

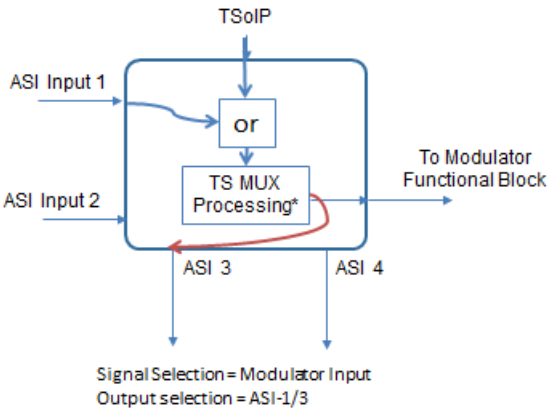


The following figures show different possibilities of output selection and to which output interface the signal is forwarded. (see next page)









PRBS can be activated from the following locations:

M6100 >> ASI Input

M6100 >> ASI Output

Also refer to section: *PRBS Generator on page 174*.

11.6 TS over IP

11.6.1 Why TS over IP

Transport stream over IP is a solution that is introduced to reduce costs and create more flexibility for teleports and network operators. Using Ethernet interfaces provides the flexibility of sending media files over the Internet towards the modulator.

11.6.2 IP Network Issues

Transporting time critical media files in TS over IP networks also implies the following main challenges:

- Timing (packet order);
- Packet loss;
- Traffic jitter;
- Latency.

These challenges are solved as much as possible by using a certain TS encapsulation protocol and setting the maximum traffic jitter and maximum buffer delay of the device.

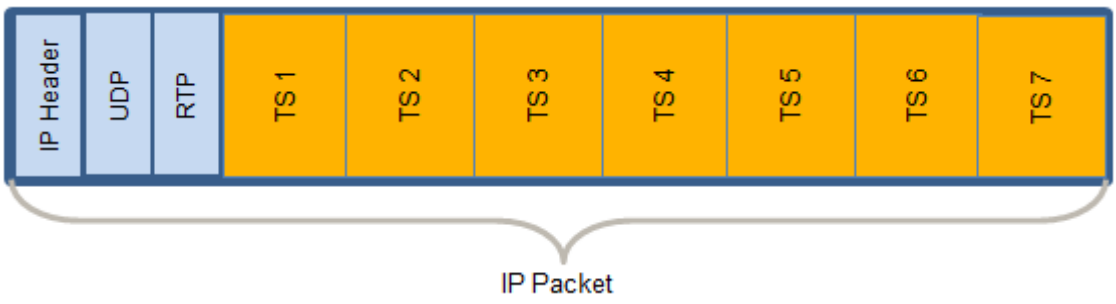
11.6.3 TS Encapsulation into an IP Packet

Before the transport streams are sent over an IP network they must be packed into an IP packet. The Maximum Transmission Unit (MTU) of an IP packet is set to 1500 bytes. This is done because most TS streams pass over an Ethernet network. The limitation of the IP packet is set to avoid IP fragmentation in the system setup.The MTU (1500) for the IP packet limits the number of TS packets (188 bytes) that can be packed into the IP packet.

The limitation is 1500/188 bytes= maximums seven TS packets.

The following picture shows the maximum amount of TS packets packed into one IP packet.

The device automatically detects the amount of TS packets that are encapsulated in an IP packet.

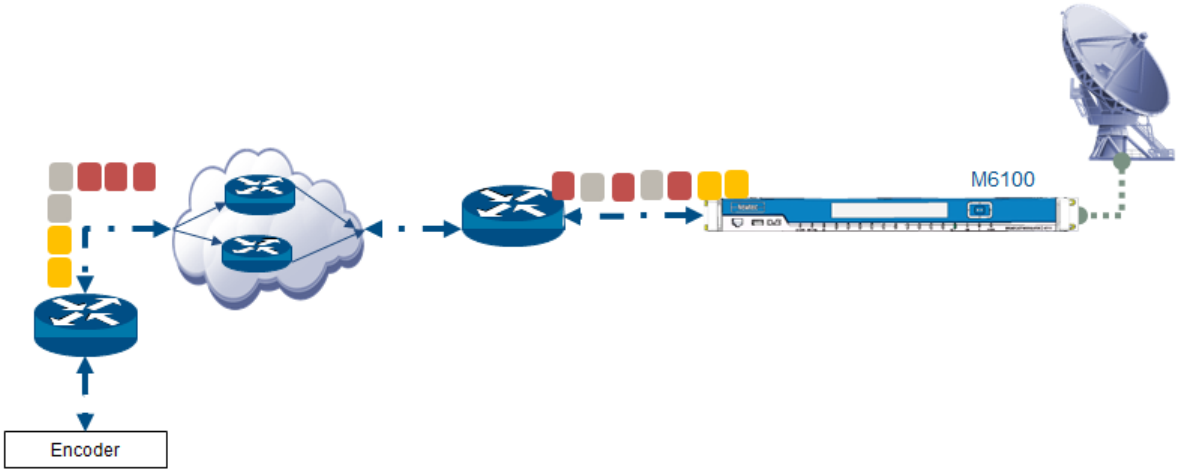


11.6.4 TS over IP Settings

The incoming traffic on the Ethernet interface of the modulator are IP packets with Transport Streams included. The IP information must be removed to recover the original transport stream. Do this by setting the parameters of the TsoIP so that it is in line with the encoder/video multiplexer settings:

- Encapsulation Protocol;
- IP Address Type;
- Traffic Profile.

The following figure shows the IP traffic flow through a network system setup.



11.6.5 TS over IP Input Interface

Configure the TsoIP input interface.

M6100> TS over IP >> Input Interface

The two data Ethernet inputs make it possible to create a redundant interface input. For more information pleaser refer to *Data Ethernet Link Redundancy. on page 112*

The following table describes the possible input selection options.

Selection	Description
None	No input selection, the functional block is not active.
Data 1	The data arriving on the Data 1 input interface is inserted into the device.
Data 2	The data arriving on the Data 2 input interface is inserted into the device.
Data Bond	The data arriving on the Data 1 or Data 2 input interface is inserted into the device. The bond interface is used to create the link redundancy. Only one link is active at a time.
Any Data	Data arriving on the Data 1 or Data 2 input interface is inserted into the device. The difference with data bond is that both links are active at the same time.

Source redundancy is always applied on TS over IP. Refer to section:
Source Redundancy. on page 132

This implies that all packets coming from one source are accepted. When using Any Data and the multicast traffic from the same source is present on Data1 and Data2, this data will be aggregated resulting in a corrupt Transport Stream.

11.6.6 TS Encapsulation Protocol

M6100> TS over IP >> TS Encap Protocol

To transport these time critical media files over IP networks it is possible one of the following protocols can be used.

- UDP (User Datagram Protocol);
- RTP (Real Time Protocol);
- RTP FEC (Real Time Protocol with Forward Error Correction).

The used protocol depends on the situation.

The following sections explain:

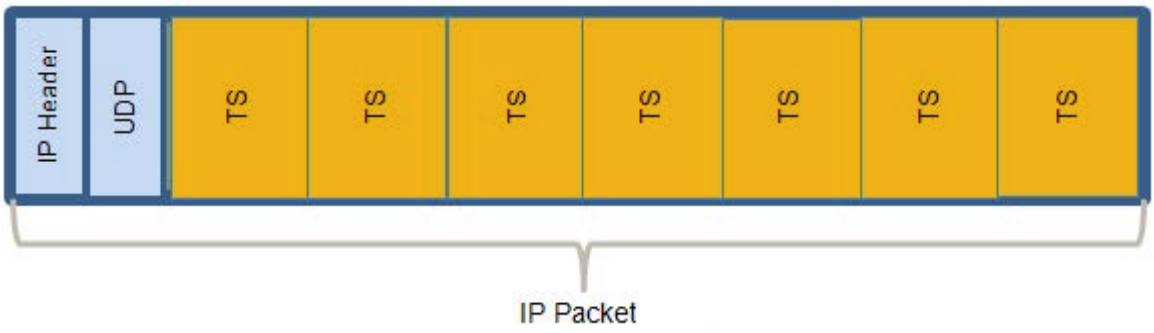
- The different protocols;
- When to use a certain protocol.

11.6.6.1 UDP

The User Datagram Protocol is used to send data (MPEG Transport Streams) from a source (encoder) to the modulator over an IP network. The protocol does not require to setup special transmission channels or data paths. UDP provides an unreliable service and it is possible that packets arrive out of order, are duplicated or are lost without notice. This means that UDP can only be used in simple IP networks where no jitter, packet loss or packet reordering is expected.

For example in a DSNG truck where two encoders are connected to two Modulators via a simple Ethernet switch. See the following figure:

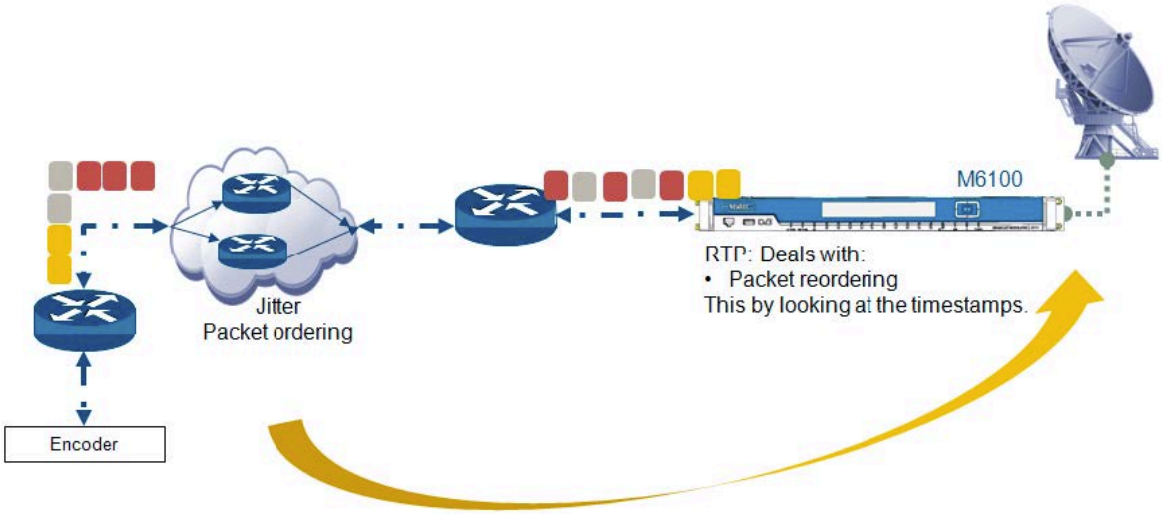
The TS packets are packed into IP packets with only a UDP header. This is displayed in the following figure:



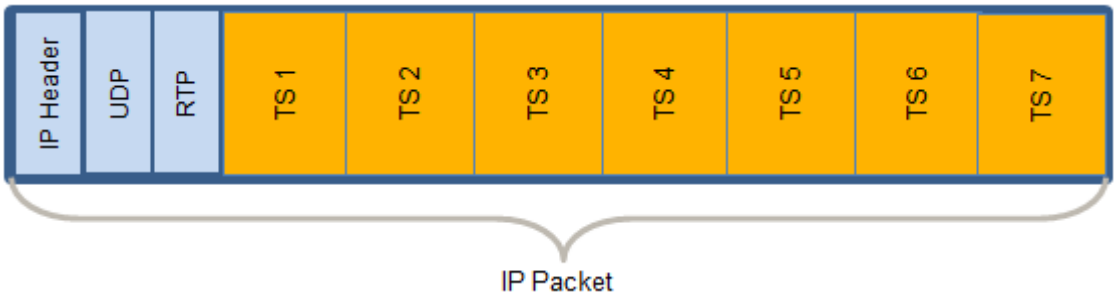
11.6.6.2 RTP

The Real-time Transport Protocol is used to send MPEG Transport Stream packets from a source (encoder) to the modulator over an IP network. This protocol is based on UDP but it uses extra header information such as sequence numbers and timestamps. This is inserted to deal with packets that arrive out of order and to store the payload information. The RTP protocol is used when networks become more complex.

The Real Time Protocol is defined in the standard RFC3550.



When sending TS over IP, the TS packets must be packed into IP packets. The packing of TS packets into one IP packet is restricted to a maximum of seven TS packets. This is displayed in the following figure.



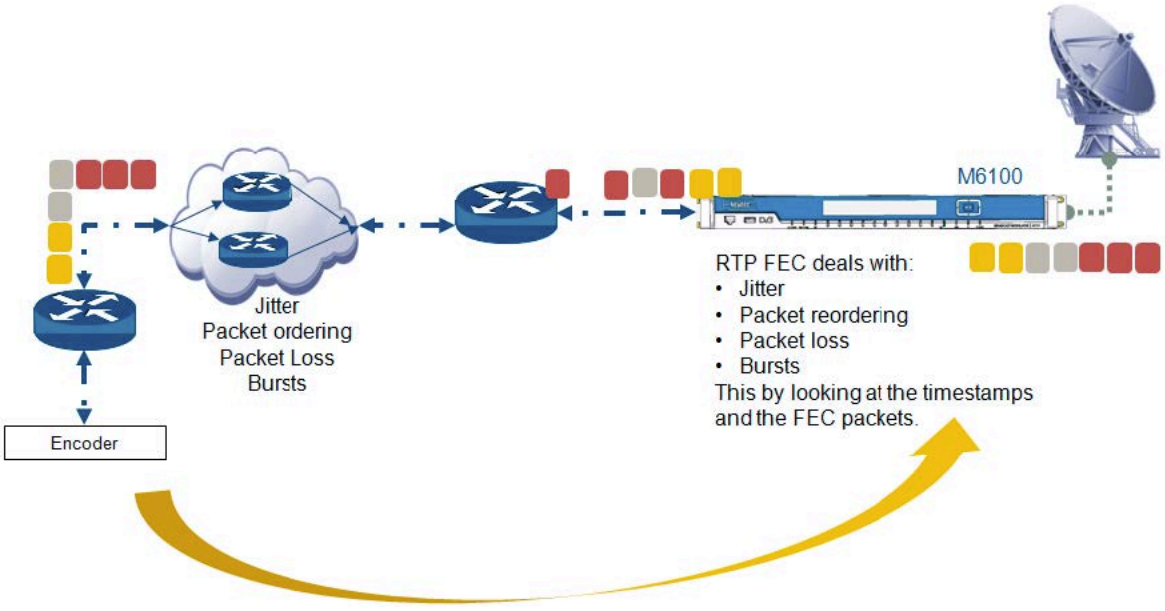
RTP is restricted in using consecutive packets that are used to generate the error correcting packets. This limits the burst correction efficiency. This is why RTP FEC is developed.

11.6.6.3 RTP FEC

This is the standard RTP protocol but it adds the possibility to insert non-consecutive packets. These non-consecutive packets are used to generate FEC (Forward Error Correction). This FEC information of a certain TS is inserted periodically in a parallel UDP port.

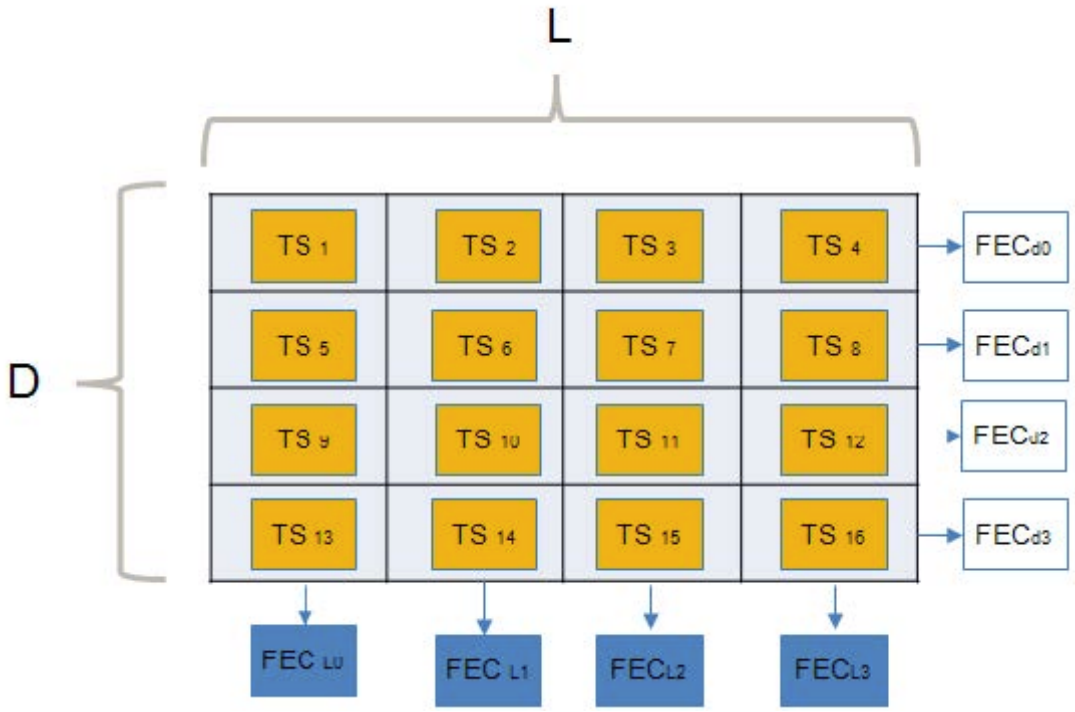
This mechanism is standardized by SMPTE.org in the standards SMPTE 2022 of which the M6100 Broadcast Satellite Modulator supports SMPTE 2022-1 and SMPTE 2022-2. These standards support only the protection of CBR (Constant Bit Rate) TS streams. The standards for VBR (Variable Bit Rate) TS streams are not supported.

• SMPTE-2022 used to be known by the name Pro-MPEG COP#3.



The insertion of SMPTE-2022 FEC packets is based on a two dimensional XOR (exclusive or) algorithm.
The size of the matrix (refer to the following figure) is defined by two parameters L and D.

- L = the period or space between the non-consecutive packets or the amount of columns in the matrix;
- D = defines the amount of rows in the matrix.



When the transport streams are aligned in the matrix the XOR function is applied to compute the FEC packets per column and row.

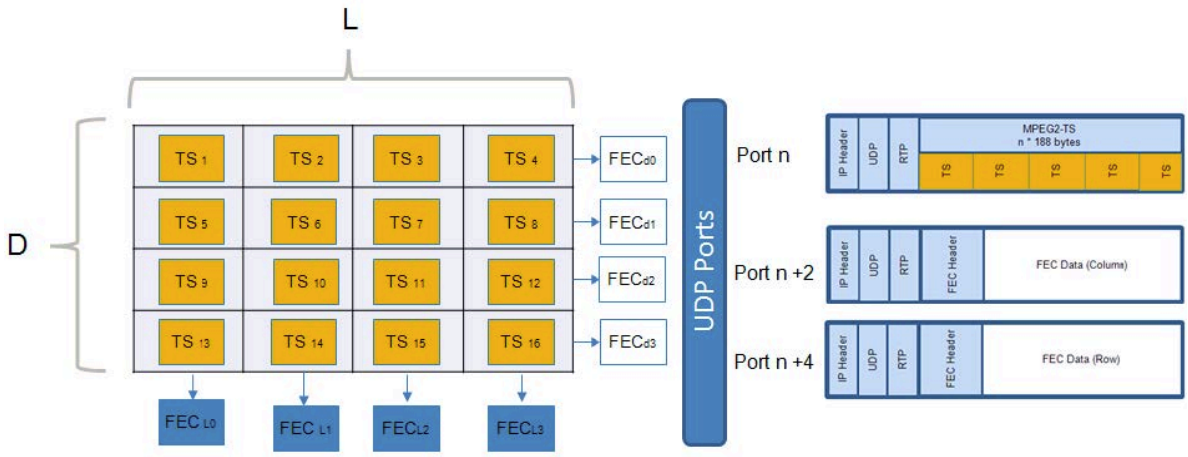
The FEC packets that are calculated in the columns deal with consecutive burst packet loss and this up to L packets. This FEC is used for correcting packet burst errors and random errors.

The FEC packets that are calculated in the rows deal with non-consecutive packet loss. It corrects single packet loss within a row of TS packets. This is used to correct random packet errors.

The combination of two dimensions (FEC streams) is used to realise a higher performance/correction capability then one single FEC stream.

The FEC streams must be transported separately on different UDP ports. The following matrix provides an overview of the transmission of the following:

- TS packets are transported on port n;
- The FEC column packets are transmitted on port n+2;
- The FEC row packets are transmitted on port n+4.



The M6100 Broadcast Satellite Modulator has all hardware on board to support L(column) and D (Row FEC) up to 20 where L*D<=100.

The M6100 Broadcast Satellite Modulator is able to detect the FEC packets automatically. These FEC packets are used to reconstruct the original transmitted transport stream.

The M6100 Broadcast Satellite Modulator corrects the errors but also removes the FEC overhead prior to transmission.

The error count and number of corrected errors are reported, the operator can use this information to monitor the link quality between video head-end and modulator.

These monitoring parameters can be located under.

M6100 Boadcast Satellite Modulator>TS over IP >> Monitor

Parameter	Description
RTP FEC Scheme	Displays the currently used RTP-FEC Scheme.
RTP In Count	Displays the number of received RTP packets.
RTP Column FEC In Count	Displays the number of received RTP column FEC packets.
RTP C Row FEC In Count	Displays the number of received RTP row FEC packets.

11.6.6.4 IP Address Type

Define whether unicast or multicast is used for TS over IP reception.

M6100>TS over IP >> Monitor

When unicast is used the device listens to the IP address of the input selection, being one of the following:

- Data 1;
- Data 2;
- Data Bond.

When multicast is used a specific multicast address must be defined.

This is the IP address where the different devices in the multicast group have to listen to.

IP Multicast uses a reserved range of IP addresses (from 224.0.0.0 to 239.255.255.255). The IGMP (Internet Group Management Protocol) is used as communication and coordination protocol between source and recipients.

With IGMPv3 a source address can be detected so that traffic from this source only is selected.

To configure an IP Address, refer to *Data IP Connectivity. on page 110*

IGMPv2 and IGMPv3 (standards) are supported by the M6100 Satellite Broadcast Modulator.

11.6.7 Traffic Profile

In the M6100 Broadcast Satellite Modulator the traffic profile must comply with the profile used in the encoder/video multiplexer. This is needed to ensure that the M6100 Broadcast Satellite Modulator recognizes the traffic.

11.6.7.1 VBR (Variable Bit Rate)

This is the property of a transport stream, where the packet rate is varying over time. It means that when the compressed data contains less information, less packets are sent. In other words, the number of packets in two time intervals of the same duration is variable.

- When the VBR profile is selected, it is not possible to slave the baud rate of the modulator onto the received TS rate.
- The jitter specifications are not applicable and traffic is taken in at best effort rate. This means when too much packets are received data is discarded.

11.6.7.2 CBR (Constant Bit Rate)

M6100> TS over IP >> Traffic Profile

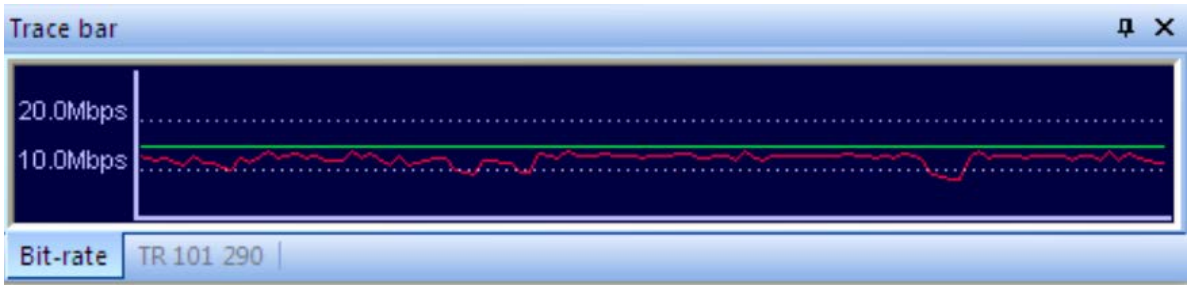
This is the property of a transport stream where the packet rate is constant over time, in other words there are always the same number of packets in two time intervals of the same duration. CBR streams are often used for transmission of multiplexes or programs over communications channels of fixed bandwidth.

Note that the CBR is on TS level and not on IP level. This means that on IP level jitter can be added but it does not impact the TS rate that stays constant.

In CBR mode, the baud rate of the modulator is slaved onto the received TS bit rate when the rate adapter is disabled.

It is important that the input rate is configured correctly

The following figure is an example of a constant bit rate:



The red line indicates the variable rate of the effective data, while the green line indicates the bit rate of the transport stream.

11.6.8 Maximum Traffic Jitter and Buffer Delay

M6100>TS over IP >> Max Buffer Delay

A typical IP network is introducing jitter on the arrival time of the IP packets which contain the encapsulated Transport Stream (TS). While, depending upon the network, jitter can be as low as 10 ms, the M6100 can compensate, for CBR streams, network jitter up to 500 ms.

Compensation is done by using a buffer. We refer to figure at the end of this section.

The buffer stores input data up to a certain level. This level is called the buffer delay. The buffer outputs Transport Stream data at a constant rate.

During start up the queue is filled until the configured buffer delay is reached. From this moment onwards, the traffic leaves the de-jitter buffer (First In First Out).

The rate is set by the *Input TS Bit Rate* (M6100 >> TS over IP >> Input TS Bit Rate) parameter. Any high frequency jitter is removed this way.

In case of VBR mode, the buffer is bypassed and there is no jitter removal at all.

For the correct functioning of the system, it is very important that the Input TS Bit Rate is configured correctly! Use the Transport Stream Analyser on-board the M6100 modulator.

Its measured PCR rate (M6100 >> TS Analyser >> Estimated TS Rate) is the most accurate indication for the TS input rate.

The buffer not only de-jitters the high-frequency jitter of the incoming data, it also takes care of any difference in rate between the reference clocks of the incoming TS and the modulator by the use of a (slow) control loop which targets to keep the buffer fill level constant at the same buffer delay .

The slow control loop guarantees an output clock variation lower than 10 ppm/hour in accordance with DVB standard requirements. For a 3 ppm difference in clock rate between the reference clocks of the TS and the modulator, a 20 ms buffer delay is sufficient. Coping with a difference of up to 30 ppm between the reference clocks of the TS and the modulator requires a 200 ms buffer delay. 30 ppm is the maximum allowed by DVB standard requirements. Buffer delay values are valid up to a 150 Mbps TS input rate.

Control parameters:

The user has two parameters for the configuration of the buffer.

Max Traffic Jitter: between 0 and 300 ms

The Buffer Delay equals Max Traffic Jitter + 200ms if not limited by the Max Buffer Delay value. In case the reference clocks of TS encoder and modulator are the same, the buffer will cope with up to 500 ms traffic jitter when Max Traffic Jitter is set at 300 ms.

Max Buffer Delay

If Max Buffer Delay is lower than Max Traffic Jitter + 200ms, then the Max Buffer Delay parameter value is used as the configured set point. This is useful when the reference clock differences are well known (e.g. could be zero if input TS and the modulator clock are on the same reference) to limit the buffer delay.

Monitoring parameters:

- Buffer Delay: the configured set point of the de-jitter buffer. It equals the Max Traffic Jitter + 200ms;
- Min Buffer Filling = The minimum measured value over a time interval;
- Max Buffer Filling = The maximum measured value over a time interval.

The "Minimum/Maximum Buffer Filling" monitoring parameters allow for checking the dimensioning of the buffer size. Minimum values close to zero or maximum values close to twice the " Buffer Delay" monitoring value mean the buffer is too small.

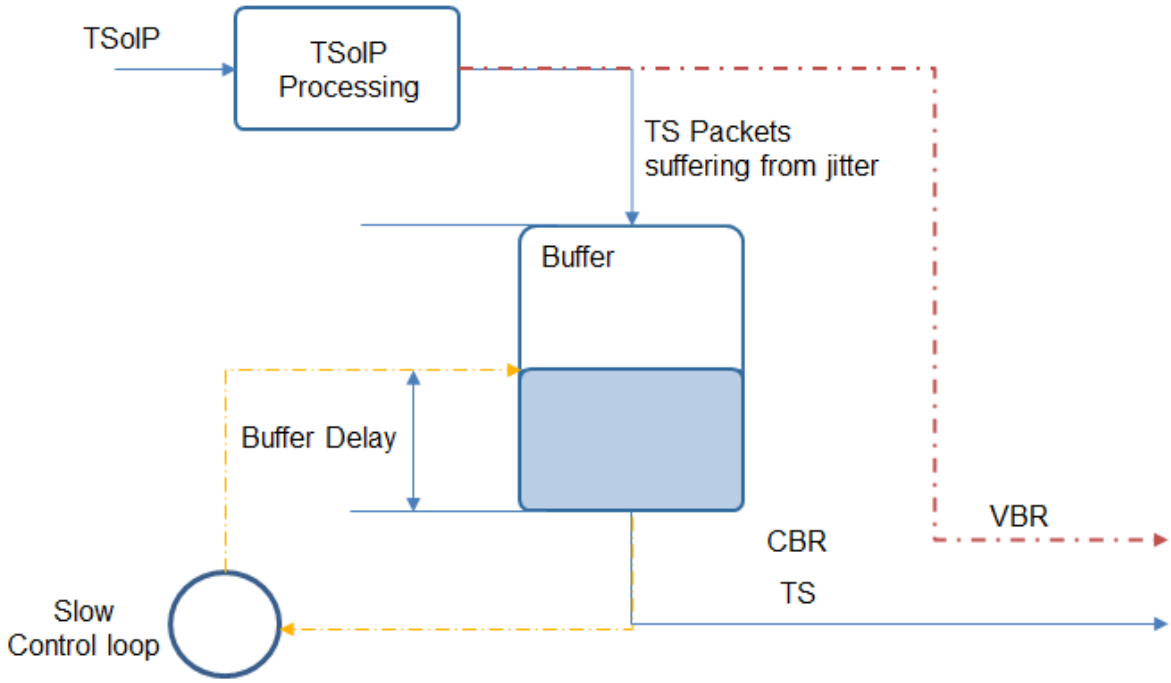
Example:

If it is known that Maximum Traffic Jitter = 20 ms and the difference between the reference clocks of the TS and the modulator could be up to 30 ppm, then set

- Max Traffic Jitter = 20 ms;
- Max Buffer Delay = 220 ms.

Monitoring parameters will give, once the slow control loop is in steady-state,

- Minimum buffer filling: 200 ms;
- Maximum buffer filling: 240 ms.



11.6.9 Input TS Bit Rate

M6100 TS over IP >> Input TS Bit Rate

Define the input TS bit rate when the CBR traffic profile is selected.

With the rate adapter enabled, the output rate will be adjusted to match the Modulator symbol rate.

To enable the rate adapter refer to *Rate Adaptation. on page 164*

When the inserted bit rate is too high/low the following alarm is generated: **TS over IP Invalid TS Bit Rate.**

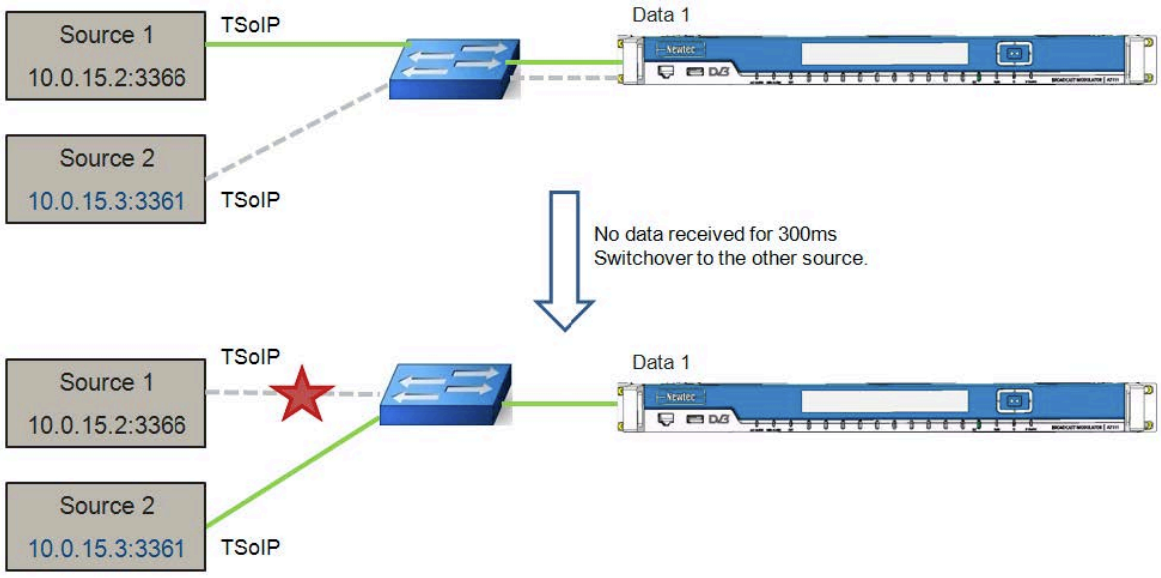
11.6.10 Source Redundancy

Source redundancy for TS over IP is a protection mechanism built into the modulator. This mechanism takes care of the fact that the modulator only listens to one source at a time.

In other words, the modulator takes in the first detected TS stream for further processing. The other stream (with the same UDP destination port) is ignored because the packets have a different source address.

When for 300ms no data is received from the “active” source, the modulator switches over to the TS stream delivered by the other source.

The source in this context is defined as an IP Address and a UDP port number.



M6100>TS over IP >> Monitor >> Source Info

This monitoring parameter provides the actual used input source IP Address and UDP port.

Source redundancy is only applicable for those remote devices sending to the same multicast address and same UDP port.Thus, source redundancy cannot be used for remote devices sending to a different multicast address or a different UDP port.

11.7 Multiprotocol Encapsulation

Multiprotocol Encapsulation is used to take in Ethernet data and insert it into a TS.

MPE is a data link layer protocol defined by DVB and published as: ETSI EN 301 192.

Note that ordering number VM-01 is required to activate this functionality.

Enable MPE on the following location:

M6100>MPE >> Enable MPE

Using MPE makes it possible to transmit data along with the video transport stream.

This data can contain for example: software image files for DTH set-top boxes,Multi Home Platform information or general low bit rate data for distribution in private networks.

The encapsulator replaces null-packets in the TS with useful payload of data packets. This optimizes the use of the available bandwidth by using opportunistic data insertion. The user just needs to define the bitrate of the carrier to something matching both streams at maximum load.

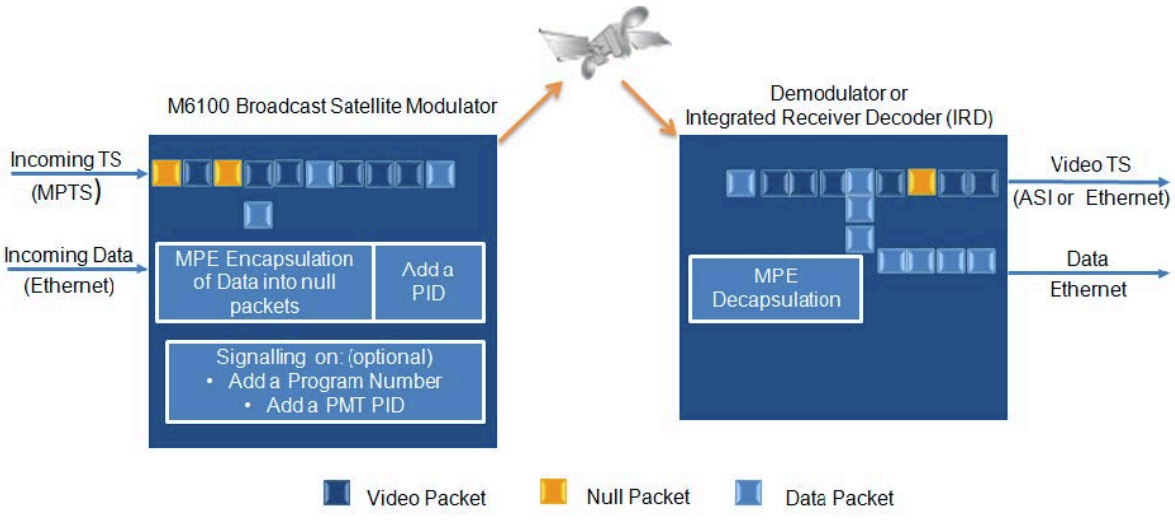
The TS will automatically be rate-adapted to the carrier rate and the MPE is inserted in it.

This feature works with any MPE capable receiver or IRD.

Input bit rates on the MPE input upto 20 Mbps are supported.

It is possible to insert signaling and perform shaping on this data.

Refer to the following figure:



11.7.1 MPE Input Selection

M6100>MPE >> Input Selection

Configure the MPE input interface.

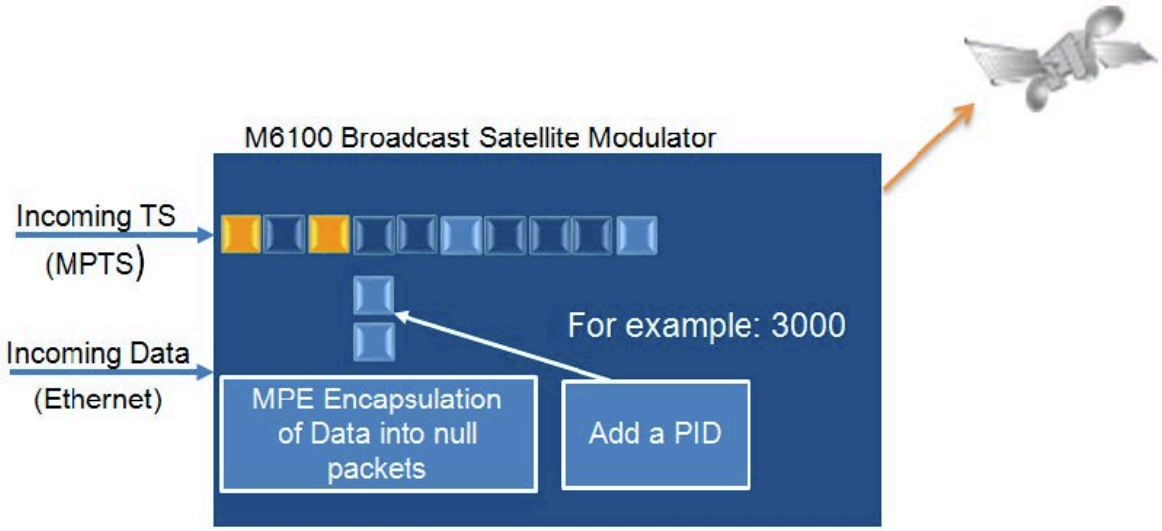
The two data Ethernet inputs make it possible to create a redundant interface input. Refer to section: *Data Ethernet Link Redundancy. on page 112*

Selection	Description
None	No input selection, the functional block is not active.
Data 1	The data arriving on the Data 1 input interface is inserted into the device.
Data 2	The data arriving on the Data 2 input interface is inserted into the device.
Data Bond	The data arriving on the Data 1 or Data 2 input interface is inserted into the device. The bond interface is used to create link redundancy.

11.7.2 Packet ID

M6100> MPE >> PID

When MPE is enabled, it is needed to add a packet Identifier to this stream. This makes it possible to filter the correct data on the receiving end.



11.7.3 Program-Specific Information (PSI-SI) Insertion

M6100>MPE >> PSI-SI Insertion

The program specific information is metadata about a program and is part of the MPEG TS.

The receiver uses the program-specific information to identify the properties of the stream.

This information is added to the PAT (Program Association Table) and to the PMT (Program Map Table).

The PAT lists all programs available in the transport stream. A program number can identify these listed programs. Each of the programs listed in the PAT has a PID for its PMT. The program map table contains detailed information about the programs added to the TS. For each program there is one PMT defined.

The following table is an example of a PAT containing MPE data.

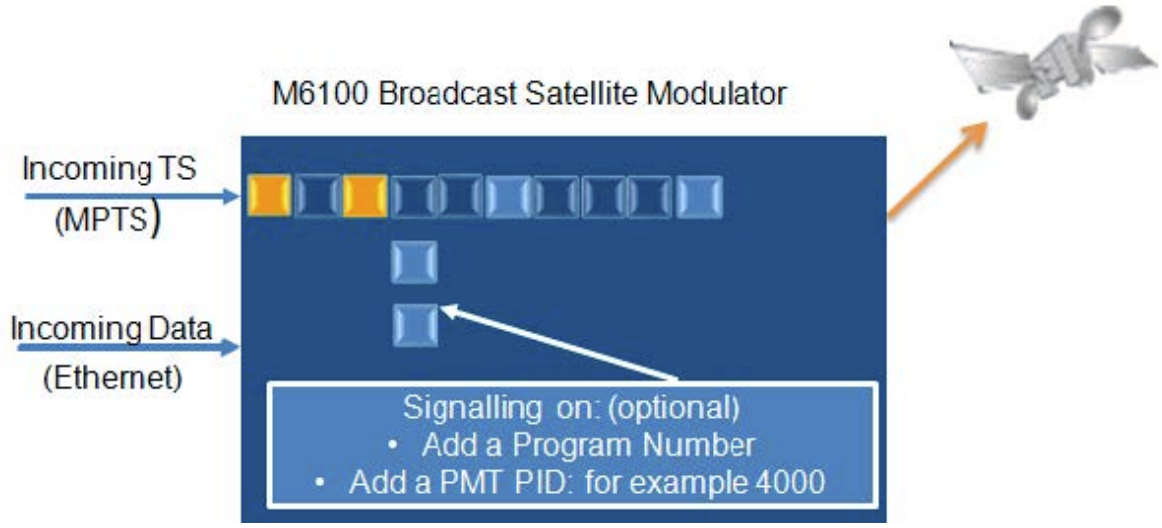
Program Number	PID	PMT	Content
1	1001	30	Video
	1002		Audio
	1005		Teletext
2	1501	31	Video
	1502		Audio
3	2001		Video
	2002		Audio 1
	2003		Audio 2
15	3000	4000	MPE

The following additional information can be added:

- Program Number;
- Program Map Table
  - PMT PID

When no signaling is present in the received TS, use the following settings to insert signaling when applicable.

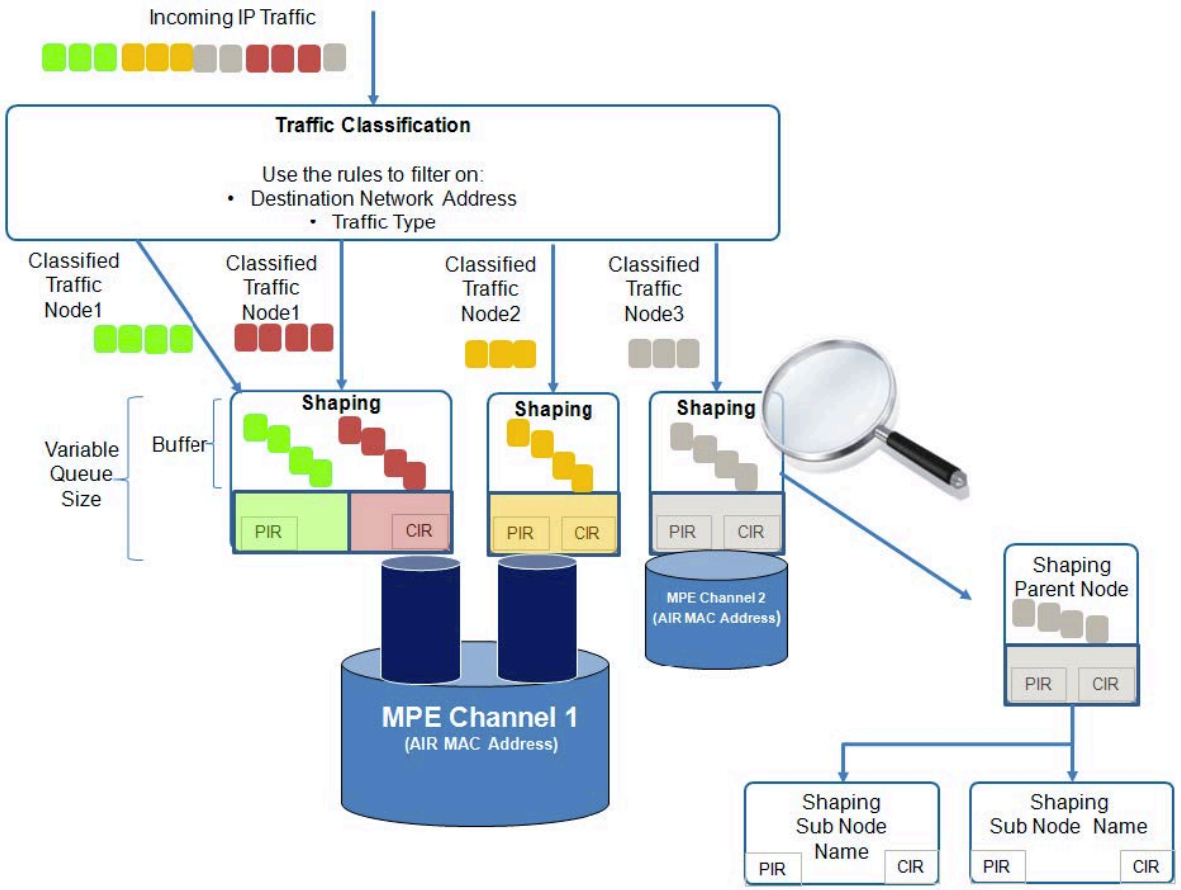
- PMT Repetition Rate: Program Map Table repetition rate in ms;
- PAT Repetition Rate: Program allocation table repetition rate in ms;
- SDT Repetition Rate: Service descriptor table repetition rate in ms;
- Transport Stream Id: Enter the transport stream identifier.



11.7.4 Traffic Classification, Shaping and Channels

M6100>MPE >> Traffic Classification

The purpose of this block is to classify, shape and send out the data to the correct output channel. The following figure represents the different steps that are performed:

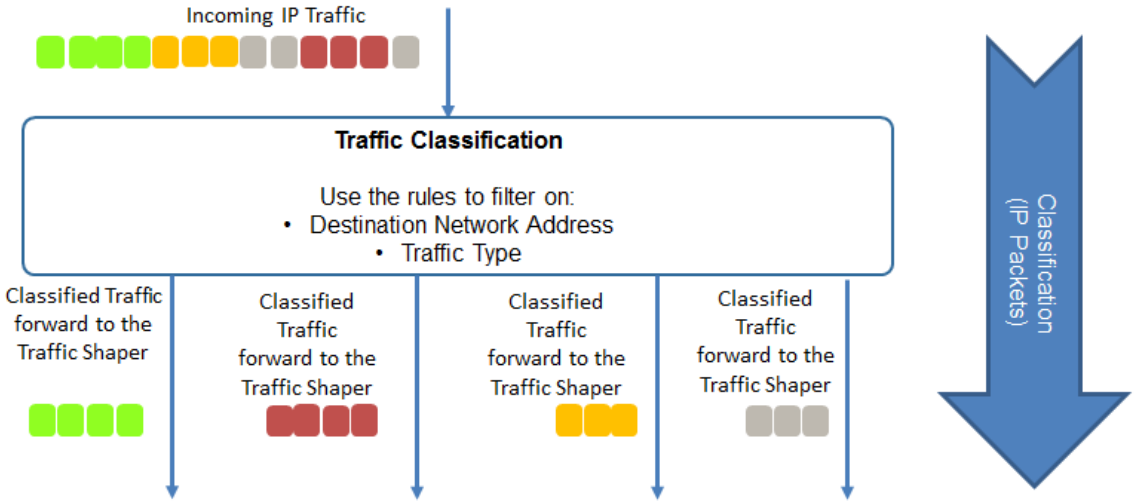


11.7.4.1 Traffic Classification

The purpose of traffic classification is to identify flows/streams of traffic that need a different treatment.
Traffic classification is based on the destination Network Address, via classification expressions or a combination of both.

Once the traffic is classified into a traffic node, this traffic is forwarded towards the traffic shaper.

The following figure illustrates how the incoming traffic is classified.



The traffic classification is listed under.

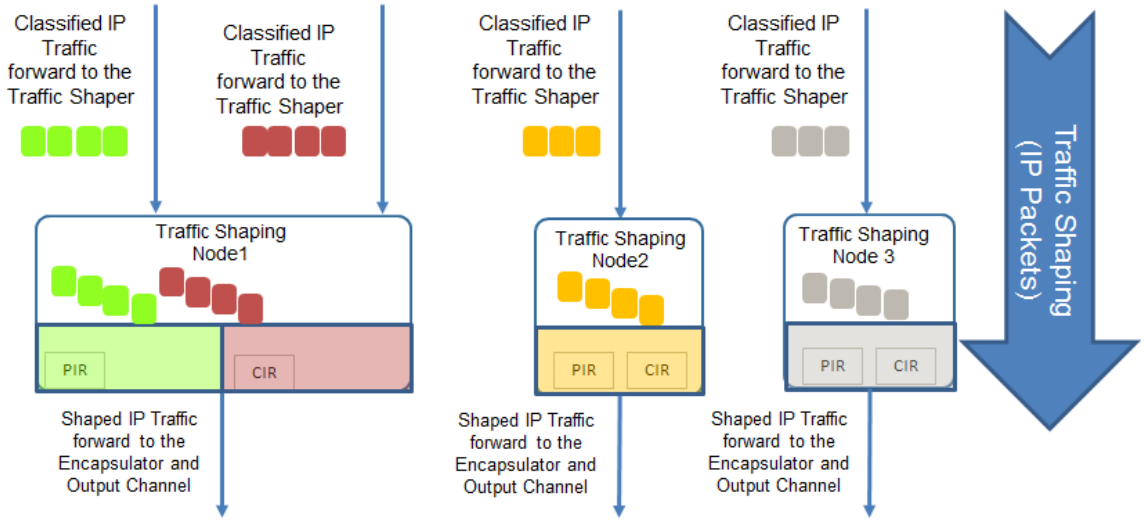
Traffic Classification

Index	Classification Name	Enable	Use Network Address	Network Address	Classification Expressio	Shaping Node Name
1	Rule1	On	No	0.0.0.0/24	not ip4 dst net 10.2...	Node1
2	Rule2	On	Yes	10.254.2.0/24		Node2
3	Rule3	Off	Yes	10.0.39.0/24		Node3
4	Rule4	Off	Yes	10.0.66.0/24		Node4

Parameter	Description
Classification Name	Enter a logical classification name/rule.
Enable	Activate the classification rule.
Classification Expression	It is possible to define an expression to classify/filter out specific traffic. This expression can be standalone or combined with the Network Address (see previous parameter). Note that the syntax of the expression is being checked while typing. Refer to appendix *Appendix C - Classification Expressions on page 221* to get an overview of the possible expressions.
Shaping Node Name	Enter the node name to which the classified traffic belongs. The Node Name must match with the Node Name defined in the Traffic Shaping Menu.
Matching Order	The matching order defines the order in which packets are processed by the classification rules. This is important for disambiguation when multiple classification rules match the same packet. The order ranges from 1 (match first) to 99 (match last).

11.7.4.2 Traffic Shaping

The following figure illustrates how the classified traffic is shaped by the traffic shaper.

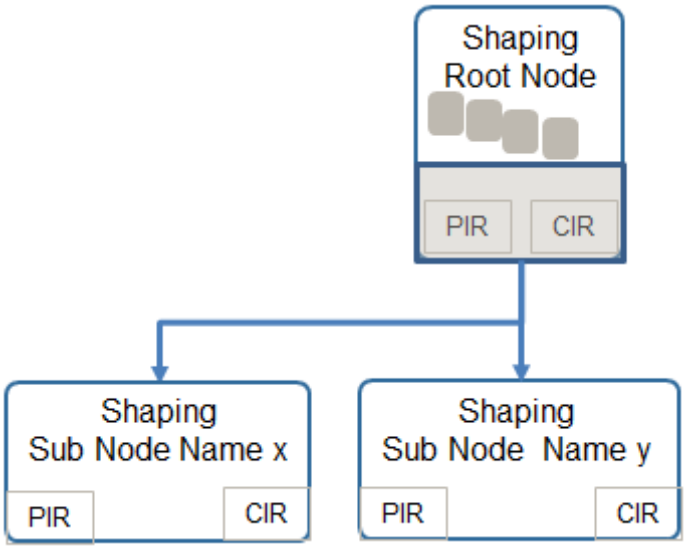


Per classified traffic node, traffic shaping can be performed.

Traffic shaping makes it possible to restrict the maximum given PIR (Peak Information Rate) in a flexible way. Next to the PIR a CIR (Committed Information Rate) is used for the distribution of the total available rate.

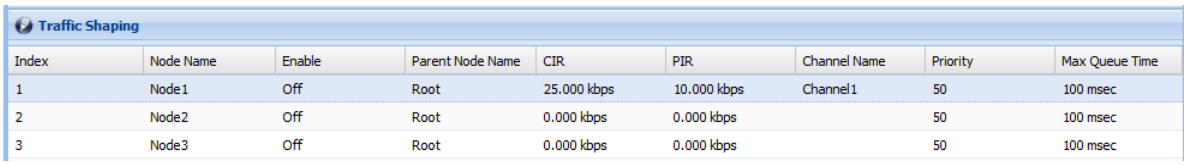
The traffic shaping software also allows the distribution of the available rate among services in order to e.g. higher prioritize time critical VoIP traffic and to throttle certain downloads.

As shown in the next figure, a Parent Node can contain more sub nodes. These sub nodes inherit the settings of the previous node and are then again divided in a PIR and CIR.



This is used to ensure that the available data rate is distributed in the most appropriate manner among the users of the satellite network. The traffic shaper provides adaptive traffic shaping, which makes it easy for shaping the traffic of networks where the throughput of the link is varying over time.

Once the shaping is performed, the traffic encapsulated into transport streams and forwarded to the correct output channel.



Traffic Shaping

Index	Node Name	Enable	Parent Node Name	CIR	PIR	Channel Name	Priority	Max Queue Time
1	Node1	Off	Root	25.000 kbps	10.000 kbps	Channel1	50	100 msec
2	Node2	Off	Root	0.000 kbps	0.000 kbps		50	100 msec
3	Node3	Off	Root	0.000 kbps	0.000 kbps		50	100 msec

Parameter	Description
Node Name	Enter the shaping node name.
Enable	This must be enabled (On), otherwise the node is not recognized and the data cannot be encapsulated.
Parent Node Name	The Root node is the top node of the shaping tree. The Root node represents the overall available bandwidth. The parent node name of the first shaping node must always be Root! Other nodes can have another parent node (when this node is defined in the device!)
CIR	Enter the Committed Information Rate for this Shaping Node.
PIR	Enter the Peak Information Rate for this Shaping Node.
Channel Name	Enter the corresponding channel name where the traffic must be sent to. One channel can have several nodes and shaping rules. Note: The channel names must match with a channel name configured under channels, refer to the previous section *Channels on page 144*.
Priority	Enter a priority for this shaping Node. Use this setting to prioritize the shaped traffic (for example: voice= 5, video=10) (The lower the value that is entered, the higher the priority.)
Max Queue time	Define a queue time per shaping node. This is a buffer based on the FIFO (First In First Out) principle. The buffer provides the possibility to store an amount of data in a shaping node. When the queue time is exceeded, data will be dropped.

11.7.4.3 Channels

Channels are logical pipes that are used to transport shaped traffic.
A channel can be used to transport a certain service towards a terminal or a group of terminals.
A terminal (receiving device) can receive multiple channels (for example: different services).

It is possible to combine traffic coming from several traffic shaping nodes and insert them into one channel.

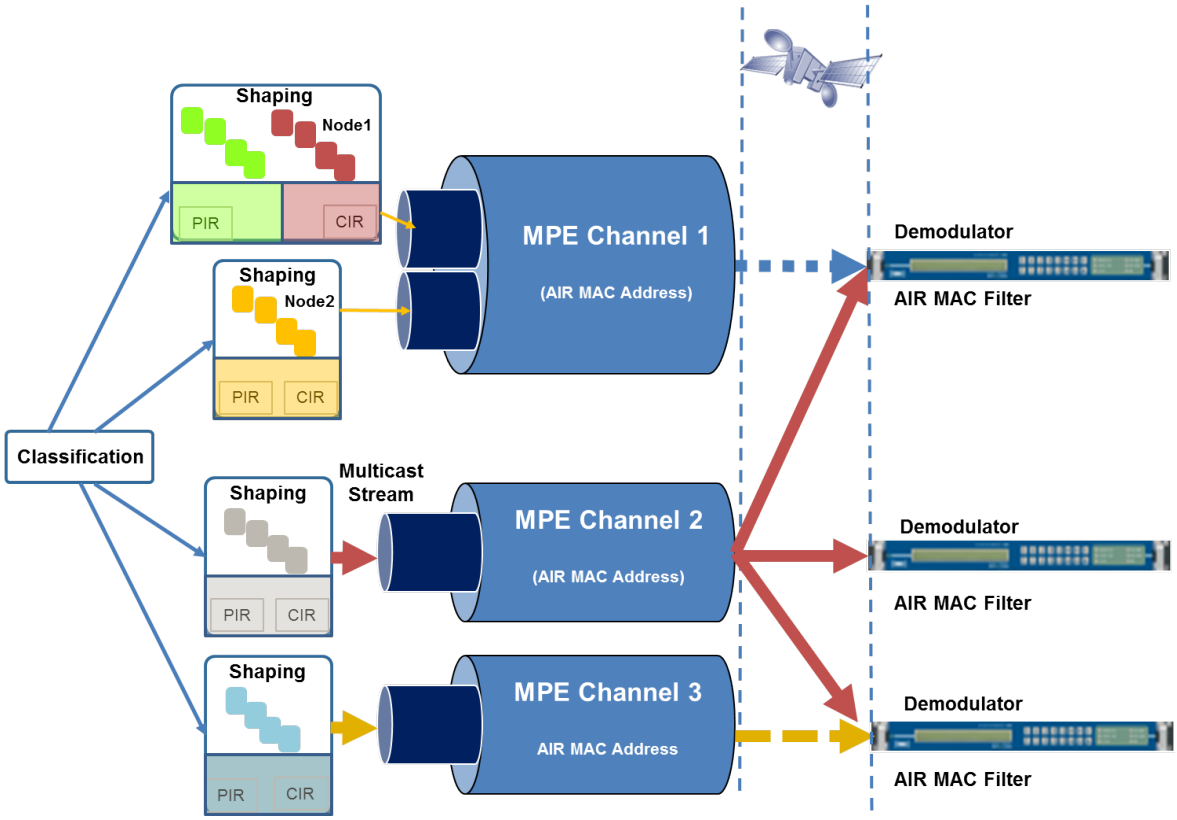
(Combining traffic from different shaping nodes is done by assigning the same Channel Name per shaping node.)

On the receiving end it is possible to filter on the different channels/AIR MAC Addresses.

Channels

Index	Channel Name	Enable	Mac Address
1	Channel1	On	00:00:00:00:00:00
2	Channel2	Off	00:00:00:00:00:00

The following figure shows the complete data flow through the encapsulator.
The figure also visualizes that it is possible to fill one channel with data coming from different shaping nodes. Furthermore it is indicated that the configuration flow is the opposite of the configuration flow.



Parameter	Description
Channel Name	Enter a logical channel name, for example the service that is transported over this channel (For example: VoIP Traffic,)
Enable	This must be Enabled **(On)** otherwise the channel is not recognized and the data cannot be encapsulated.
MAC Address	This is the AIR MAC address.

11.8 BBF over IP In

This block takes care of Baseband Frames (BBFs) received on the data Ethernet port(s) of the modem.

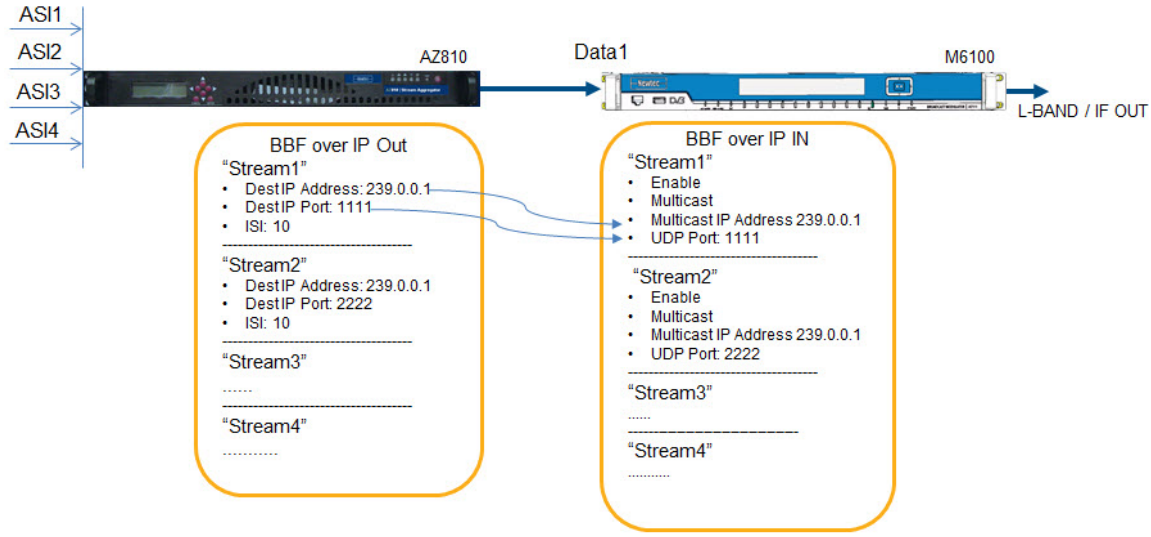
It is used when an external encapsulator (like AZ810) is used.

Navigate to the following location:

M6100 >> BBF over IP

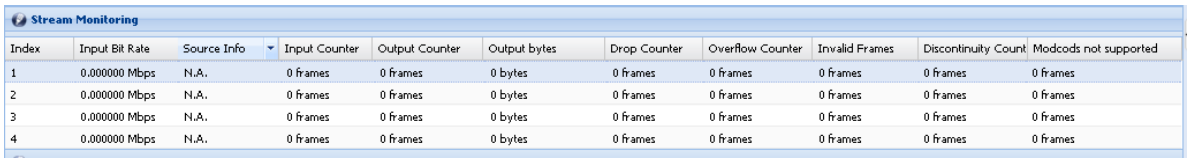
- **Enable:** reception of BBFs on this data input interface;
- **Input Selection**: Select on what physical interface to take in the data.
  - Data1;
  - Data2;
  - Data Bond (this is the bond interface, both physical interfaces and link redundancy must be activated).
- Reset monitoring counters.

The following figure shows an example of a setup between the AZ810 and the M6100.



BBF Stream Configuration	Description
Name	Enter a logical name.
Enable	Enable the specified BBF endpoint.
IP Address Type	Unicast: Multicast:
Multicast IP Address	Define to what multicast group the device belongs.
UDP Port	Define on what UDP port the BBFs are received. This is needed when the device belongs to a multicast group.
BBF Type	Define the BBF type that is send by the source (AZ810) towards this functional block. Note: This option is inserted for future development when other BBF-Types might become available.
Source Redundancy	Enable in case of source redundancy. The source ID is filtered and displayed in the monitoring info (Source Info). When for 300ms no input is detected due to a failure of the source, the redundant source is selected. Note: Source redundancy is only applicable for those remote devices sending to the same multicast address and same port. Thus source redundancy cannot be used for remote devices sending to a different multicast address or a different port.

Stream Monitoring



Monitoring Parameter	Description
Input Bit Rate	The incoming bit rate in Mbps measured per stream.
Source Info	This monitoring parameter provides the actual used input source IP Address and UDP port.
Input Counter	Displays the amount of incoming BBFs.
Output Counter	Displays the amount of outgoing BBFs.
Output Bytes	Displays the number of BBF bytes properly transmitted in a stream.
Drop Counter	Displays the amount of BBFs dropped because the received modulation type is not active on the source.
Invalid Frames	Displays the amount of Invalid frames.
Overflow Counter	Number of BBFs that are dropped for a specific BBF stream because the input data buffer is full.
Discontinuity Count	When the sequence numbers are not continuous for a certain BBF stream this counter will be incremented.
MODCODs not supported	Displays the amount of BBFs that are dropped because the received MODCOD is not licensed for a specified BBF stream.

12 Features Descriptions

12.1 Modulator

The modulator functional block is used to perform the actual modulation of the TS.

M6100> Modulator

The main parameters are:

- Mode DVB-S/DVB-S2/S2-Extensions;
- Transmit On/Off;
- Output Level;
- Output Frequency;
- Frame Type;
- Pilots;
- ModCod;
- Rate Priority;
- Symbol Rate;
- Bit Rate.

12.1.1 Modulation Mode

Select the modulation mode DVB-S, DVB-S2, S2-Extensions.

M6100> Modulator >> Mode

- DVB-S;
- DVB-S2;
- S2-Extensions.

12.1.2 Input Type

Select the type of input packets or frames.

- TS (Transport Stream);
- BBF (Baseband Frames).

12.1.3 Transmit

M6100 >> Modulator >> Transmit

This is the modulator output transmission.

Enable transmit when the complete configuration is done according to the system requirements.

A warning is displayed when it is not allowed to change a parameter when transmit is enabled.
This will be the case with parameters that influence the transmitted signal and its spectrum.

Transmit State Reason

The parameter displays why the transmission is on or off. This parameter is valuable when the transmission is off due to an alarm. It reflects the alarm state's that are configured under transmit control.

12.1.4 Output Frequency and Output Band

M6100 >> Modulator >> Output Frequency

Set the output frequency of the modulator. The output frequency must be in-line with the device capabilities (L-band or IF band) and the system requirements.

Output Frequency

- L-band: 950MHz to 2150MHz;
- IF-band: 50MHz to 180MHz.

The device performs a check whether the inserted frequency is within the allowed frequency range.

12.1.5 Roll Off Factor and Occupied Bandwidth

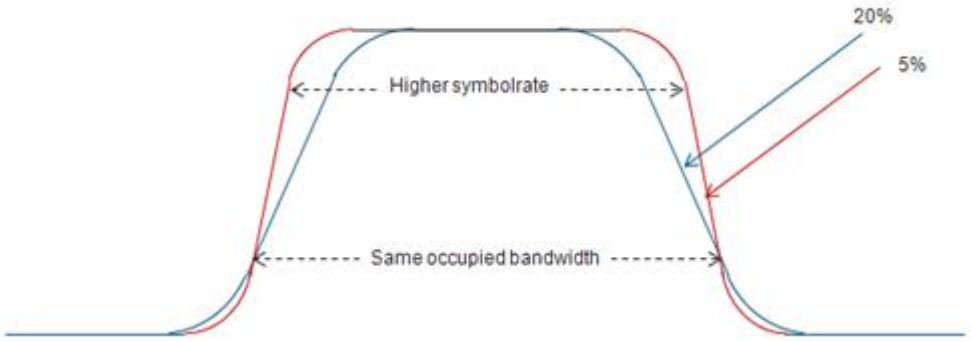
M6100 >> >> Roll-Off

Select the appropriate roll off factor.

The possibilities are:

- 35%;
- 25%;
- 20%;
- 15% (Clean Channel Technology™);
- 10% (Clean Channel Technology™);
- 5% (Clean Channel Technology™).

The following figure compares 20% roll-off with 5% roll-off.



By lowering the roll-off factor and accordingly increasing the symbol rate, the throughput can be increased while maintaining the same occupied (leased) bandwidth.

Clean Channel Technology™

Clean Channel Technology™ is a combination of improved roll-off factors for DVB-S2 and advanced filtering technologies to allow optimal carrier spacing. The combination can bring efficiency gains up to 15%.

Clean channel technology consists out of the following three effects.
A first effect in the Clean Channel Technology™ is applying a smaller Roll-Off (RO) percentage than currently used in the DVB-S2 standard. In the DVB-S2 standard the 20% and 25% Roll-Off factor percentages are common. Basically this means that these percentages need to be added to the desired bandwidth over satellite. Reducing these Roll-Off factors to 5%, 10% or 15% results in a direct gain in bandwidth. This is reflected in the following formula:

Multicarrier:

Occupied bandwidth = Symbol Rate*(1+Roll-Off factor).

Example for Occupied bandwidth 3MHz.

• DVB-S (35%)	2.2 Mbaud	• DVB-S2 (15%)	2.6 Mbaud
• DVB-S2 (25%)	2.4 Mbaud	• DVB-S2 (10%)	2.7 Mbaud
• DVB-S2 (20%)	2.5 Mbaud	• DVB-S2 (5%)	2.8 Mbaud

Single Carrier per Transponder:

Two limits are possible:

- Limit1:

Symbol Rate = Transponder Separation / (1+Roll-Off Factor)

The minimum roll-off factor that may be selected with this formula is 10%.

- Limit2:

Symbol Rate =User Bandwidth / (1+Roll-Off Factor)

For example:

A 36 MHz transponder with 40MHz Separation.

Roll-Off Factor (%)	Limit 1: Transponder Separation based	Limit 2: User Bandwidth based
35	29.6 Mbaud	26,7 Mbaud
25	32 Mbaud	28,8 Mbaud
20	33.3 Mbaud	30,0 Mbaud
15	34.8 Mbaud	31,1 Mbaud
10	36.4 Mbaud	32,7 Mbaud
5	36.4 Mbaud	34,3 Mbaud

12.1.6 Spectrum Polarity

M6100 >> Modulator >> Spectrum Polarity

Spectrum inversion can be enabled in case an inverting upconverter is used. As a general rule transmissions on satellite need to be non-inverted.

Most modern demodulators can detect and automatically adapt the spectrum inversion.

12.1.7 Output Level

M6100 >> Modulator >> Output Level

The output level must be set according to the network requirements.

For L-band the range is between -35/+7 dBm (± 2dB)

For IF-band the range is between -35/+10 dBm (± 2 dB);

The step size is 0.1dB.

12.1.8 Carrier Modulation

M6100 >> Modulator >> Carrier Modulation

This command controls the carrier modulation:

- On (Operational modulated carrier signal);
- Pure Carrier (unmodulated output signal);
- Test modulation (pulse);
- Test modulation (clock/4);
- Test modulation (clock/8);
- Test modulation (clock/16).

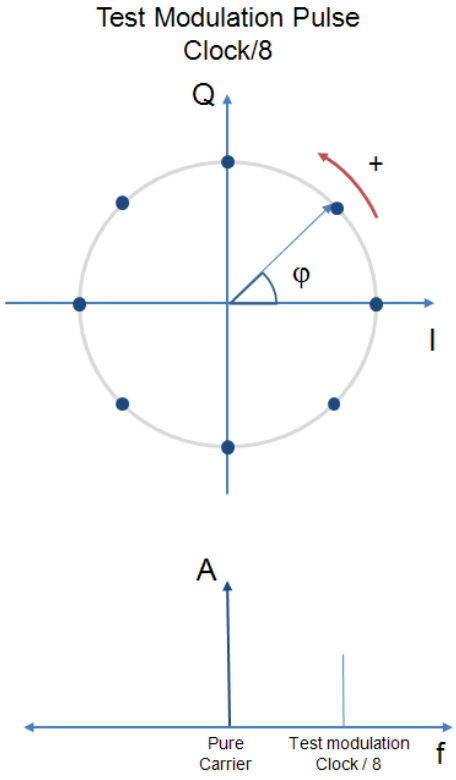
The pure carrier is used during line-up and to perform cross polarization tests with the satellite operator.

The test modulation settings are used for calibration and/or verification of the spectrum polarity.

In this case, a carrier is modulated by a rotating vector with a period of baudrate/n. This results in a single spectral line at:

+clock/n offset from the pure carrier.

The following figure shows the constellation diagram and the result on a frequency analyzer of a Test modulation clock/8.



12.1.9 Amplitude Slope Equaliser

M6100 >> Modulator >> Ampl Slope Equalizer

Configure the amplitude slope equalizer. An amplitude slope in the up-converter or in the high power amplifier can be compensated by using this equalizer. The equalizer has a maximum range of ± 2 dB/50 MHz.The compensation can be set in the range between -7 and +7.

The slope equalizer can also be used to compensate for cable slope.

12.1.10 Rate Priority

M6100> Modulator >> DVB-S >> Rate Priority

Define the rate priority:

- Symbol Rate;
- Bit Rate.

12.1.11 Symbol Rate

Define the symbol rate in Mbaud.

This parameter can only be set if the setting Rate Priority = Symbol Rate.

M6100> Modulator > DVB-S >> Symbol Rate

12.1.12 Bit Rate

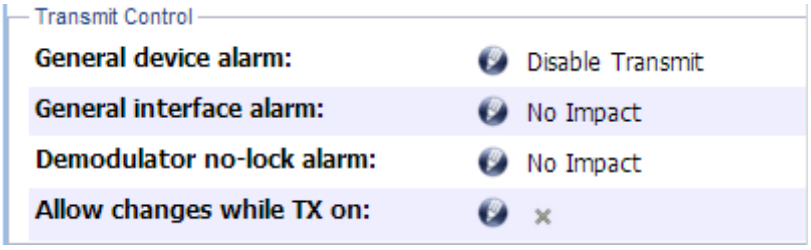
M6100> Modulator > DVB-S >> Bit Rate

Define the bit rate in bps (bits per second).

This parameter can only be set when the Rate Priority = Bit Rate.

12.1.13 Transmit Control

M6100 >> Modulator >> Transmit Ctrl

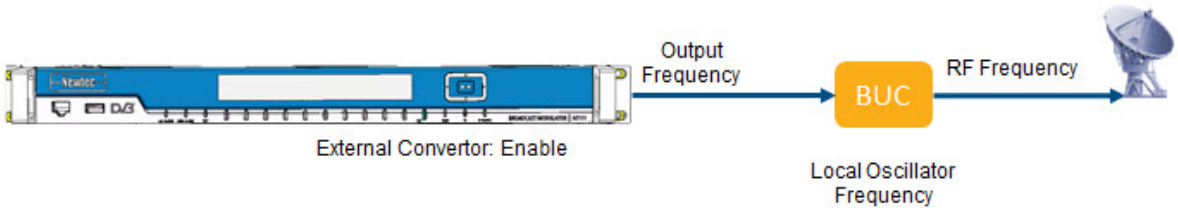


The transmission control parameters allows you to alter the default behavior of the transmitter.

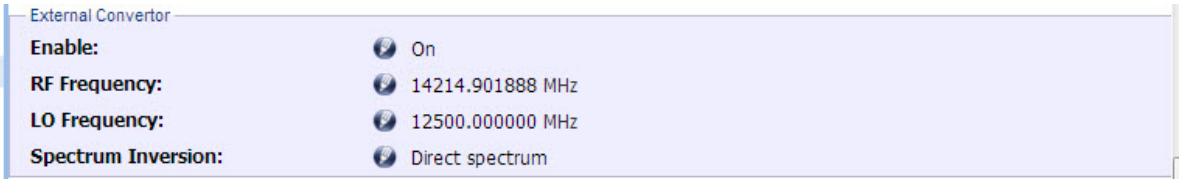
12.1.14 External Convertor

Navigate to enable the use of an external convertor (For example a Block Up Converter BUC).

M6100 >> Modulator >> External Convertor



» **Select Enable** On
When enabled it is possible to configure the transmit frequency (RF Frequency) in function of the LO Frequency of the BUC and the output frequency defined on the modulator.



Please check the specs of the external converter to determine LO (Local Oscillator) Frequency.

The following calculations are valid:

Direct Spectrum

RF Frequency = LO Frequency + Output Frequency

Inverted Spectrum

RF Frequency = LO Frequency - Output Frequency

12.1.15 DVB-S Specific Settings

12.1.15.1 Modulation and Coding

Define the ModCod that can be used.

12.1.16 DVB-S2 / S2 Extensions Specific Settings

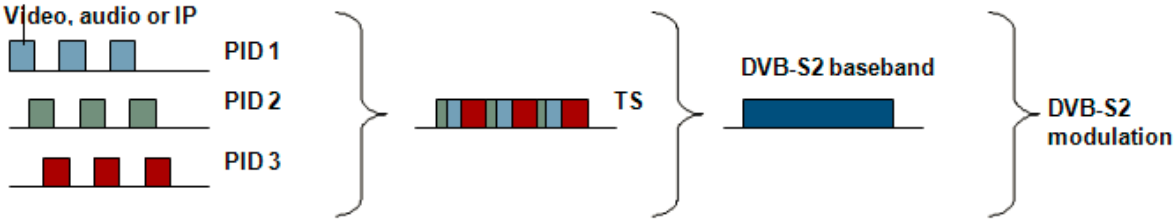
12.1.16.1 Frame Type

Select the Frame type

- Normal Frames (64800 bits);
- Short Frames (16200 bits).

This option is only available in the DVB-S2 standard.
DVB-S2 Extensions only supports normal frames.

DVB-S2 applies the error correction coding and the modulation to large frames of data called baseband frames. A DVB-S2 baseband frame is either 16200 bits (short frames) or 64800 bits (normal frames). The content of a frame can be a section of a transport stream, or any type of data, framed or unframed (Generic Stream).



Note that the DVB-S2 standard specifies how to encapsulate transport streams into Baseband frames, but not how to encapsulate IP data into baseband frames.

12.1.16.2 Modulation and Coding

Define the ModCod that can be used.

Newtec provides a tool (the DVB-S2 calculator) which calculates, in function of the chosen ModCod and other system parameters, the required Es/N0 for your application.

All available ModCods are listed in: *DVB-S2 on page 217* and *MODCOD Definitions S2-Extensions. on page 219*

Refer to (*http://www.newtec.eu/library/dvb-s2-calculator/*) to download the DVB-S2 calculator.

12.1.16.3 Pilots

M6100>Modulator >> Pilots

Define if it is needed to insert pilots or not.

This option is only available in the DVB-S2 standard.
In DVB-S2 Extensions Pilots are mandatory.

What are Pilots?

Pilots are unmodulated symbols grouped in blocks that are added on the physical layer framing level.

Why are Pilots used in DVB-S2?

- Use Pilots to increase the reliability of the receiver synchronization. (Increasing the performance and robustness of the demodulator.)
- Pilots reduce the influence of phase noise in the system;

Typically the LNB on the receiving side is the main source of phase noise.

Note: that pilots add about 2% of overhead.

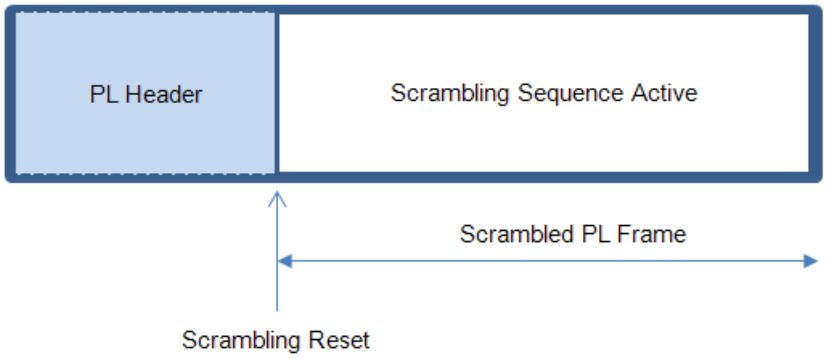
When are Pilots Used in DVB-S2?

In general it is advised to use pilots(especially in the following cases).

- When a noticeable amount of phase noise is present (for example LNBs with "bad" phase noise);
- At low data rates ;
- When distortion is present on the signal, for example due to non-linearity.

12.1.16.4 Physical Layer Scrambling

Physical layer scrambling is performed on each physical layer frame (excluding the Physical layer header) to perform energy dispersal of the modulated signal.



For more information on Physical Layer Scrambling, refer to the DVB-S2 standard: ETSI EN 302 307.

12.1.16.4.1 Dummy PL Scrambler Mode

M6100 >> Modulator >> Modulation >> Dummy PL scrambler mode

When bursty traffic (like IP) is transported, the physical layer can run out of data to transmit. In that case dummy physical layer frames are transmitted in order to keep the receiver locked.

There are two possible modes to perform scrambling of the dummy physical layer frames.

- DVB-S2 Standardized Reset (reinitialized):
  In this mode the randomization sequence is reinitialized at the end of each dummy physical layer frame header.
- Continuous:
  In this mode there is no re-initialization at the end of each **dummy** physical layer frame header. This is done to achieve more randomness in the dummy physical layer frames (carrier data) as desirable for bandwidth cancellation. The bandwidth canceller needs randomization in order to measure the time delay between the transmitted and the returned signal.

This Continuous mode is only valid for the dummy physical layer frames!

The Continuous mode is not DVB compliant.
As a consequence it is possible that some non-Newtec demodulators are not capable of working with this mode.

12.1.16.4.2 Physical Layer Scrambler Signature

M6100 >> Modulator >> PL Scrambler Signature

The following information about the Physical Scrambler Signature is taken from the DVB-S2 standard. Refer to the following document, ETSI EN 302 307.

In case of broadcasting services, the PL Scrambler Signature = 0 shall be used as default sequence, this to avoid manual receiver setting or synchronization delays.

The PL Scrambler Signature, assuming values in the range 0 to 262 141, indicates the spreading sequence number. The use of different PL Scrambling sequences allows a reduction of interference correlation between different services. For the same purpose, it is possible to reuse a shifted version of the same sequence in different satellite beams. Furthermore, the PL Scrambler Signature can be unequivocally associated to each satellite operator, satellite, or transponder, thus permitting identification of an interfering signal via the PL Scrambling "signature" detection. There is no explicit signaling method to convey the PL Scrambling signature value to the receiver.

12.1.16.4.3 Roll Off Signaling

M6100 >> Modulator >> Roll Off Signaling

- standard : (2 bits : "10") roll off signaling value is used for roll off = 20%;
- reserved : (2 bits: "11") roll-off signaling value is "reserved" (11) is used for roll off < 20%.

Some DVB-S2 receivers can use the received roll-off bits state '11' for selecting a 15% roll-off filter.

In this case, it is favorable to choose the setting "reserved".In all other cases, it is recommended to use the setting "standard" as this will guarantee compatibility with DVB-S2 receiving equipment.

12.1.16.5 Clock Output

M6100 >> Modulator >> Clock Output

Enables or disables the transmission of a 10MHz clock signal on the L-BAND output interface.

For the reference clock settings and characteristics, refer to *Reference Clock. on page 106*

12.1.16.6 Roll Off Signaling

M6100 >> Modulator >> Roll Off Signaling

- standard : (2 bits : "10") roll off signaling value is used for roll off = 20%;
- reserved : (2 bits: "11") roll-off signaling value is "reserved" (11) is used for roll off < 20%.

Some DVB-S2 receivers can use the received roll-off bits state '11' for selecting a 15% roll-off filter.

In this case, it is favorable to choose the setting "reserved".In all other cases, it is recommended to use the setting "standard" as this will guarantee compatibility with DVB-S2 receiving equipment.

12.2 Reference Clock

M6100 >> Ref Clock

Configure the reference clock.
This reference signal for an outdoor BUC can be multiplexed on the L-band Tx interface.

A reference clock can be generated internally (default) or slave on an external source.

The internal reference clock is 10MHz.
The clock reference has the following specifications:

10MHz Ref	Specifications
Internal clock reference	Stability ± 2000 ppb over 0 to 70°C Ageing ± 1000 ppb/year
Very High Stability (optional)	Stability ±2x10e-9 over 0°C to 65°C Ageing: ± 0.5 ppb/day ± 500 ppb/10 year

When an external source is selected, the following frequencies can be inserted.

1MHz, 2MHz, 5MHz, 10MHz or 20MHz.

Select the external clock reference for synchronization with other devices to have a higher stability than the internal default stability.

12.3 TS MUX

M6100 Boadcast Satellite Modulator> TS MUX

The multiplexer functional block incorporates the rate adapter and is responsible for the insertion of a carrier ID into the Network Information Table (NIT). For more information please refer to section:
NIT Carrier Identification. on page 166

12.3.1 Insert Signaling

M6100 Boadcast Satellite Modulator> TS MUX >> PSI-SI Insertion

Insert the Original Network Id (for SDT) as specified by the parameters Transport Stream Id and Network Id.

For more information please refer to section: *Program-Specific Information (PSI-SI) Insertion. on page 137*

12.4 Rate Adaptation

M6100 Boadcast Satellite Modulator> TS MUX >> Rate Adapter

In principle, a one to one relationship exists between the input bit rate and the symbol rate of the device. With rate adaptation this is no longer true. It is possible to set one variable independent of the other.

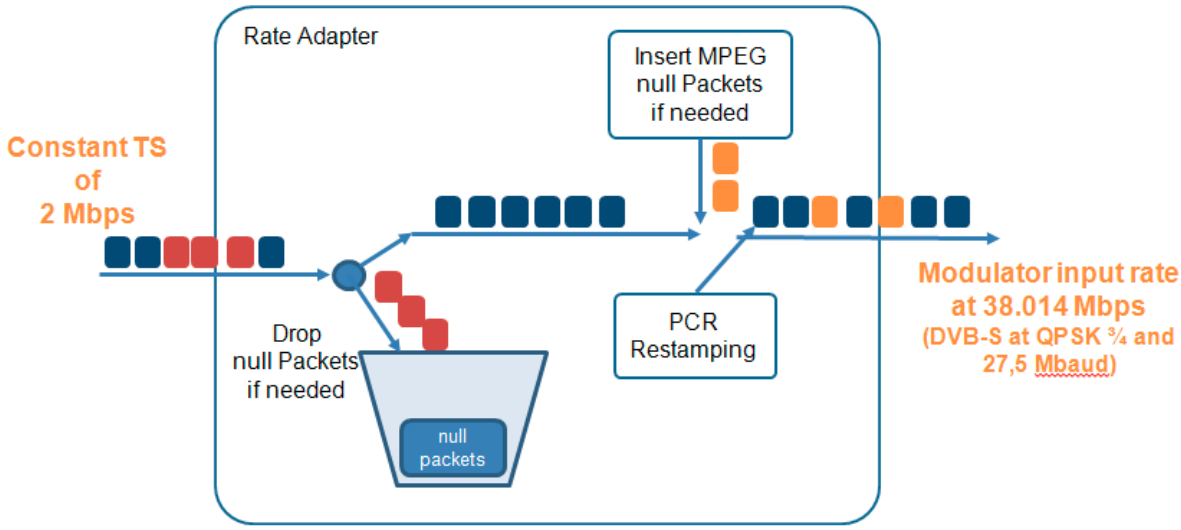
When activated, the on-board Rate Adapter will drop and insert MPEG null packets as required to obtain a fixed transmit symbol clock and uninterrupted service, even if the net input transport rate is variable.

The Rate Adapter re-calculates MPEG PCR (Program Clock Reference) time stamps as required by MPEG rules (PCR re-stamping if the PCR Restamping status is selected).

When the Rate Adapter is disabled, the device transmit clock is slaved to the interface (TS) clock rate.

- When rate adapter is disabled: the modulator symbol rate slaves on the input bit rate. In TS over IP this is only possible when the CBR traffic profile is selected;
- When the rate adapter is enabled the modulator symbol rate can differ from the input bit rate.

The following figure shows the rate adapter functionality.



12.5 NIT Carrier Identification

M6100 Boadcast Satellite Modulator> TS MUX >> NIT Carrier ID

The carrier identification is used to reduce RFI (Radio Frequency Interference). The NIT carrier ID allows the satellite operators to identify and contact the source of interference quickly. The carrier ID is implemented in the Network Information Table (NIT) of the TS, more specifically into the network descriptors set of the NIT. This information is readable by any MPEG analyzer system, which makes it easy to track the source of the carrier. The carrier ID contains the following information:

- Fixed identification of the source:
  - Modulator Manufacturer;
  - Serial number of the modulator;
  - MAC address of the modulator;
- User configurable data:
  - Descriptor Tag, this tag describes the carrier ID information in the NIT.
  - Carrier Identifier, insert a logical name for the carrier ID;
  - Telephone number;
  - Geo Coordinates;

When using both DVB-CID and NIT-CID, make sure that the Geo Coordinates entered are the same.

  - User Information.

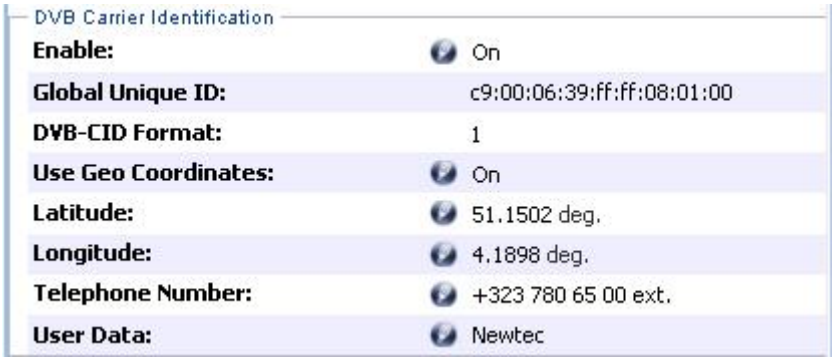
In case the incoming TS does not contain a NIT, a NIT will be generated except when no null packets are available in the TS to insert the NIT.

Make sure that enough null packets are available in the TS to insert the NIT.

The configurable carrier data is inserted into the NIT when this functionality is enabled. This means that the carrier ID of the incoming TS is replaced with the information entered in the M6100 Broadcast Satellite Modulator.

12.6 DVB Carrier Identification

M6100 >> Modulator >> DVB Carrier Identification



The DVB carrier identification standard is used to reduce RFI (Radio Frequency Interference). The DVB carrier identification allows the satellite operators to identify and contact the source of interference quickly.

The DVB carrier identification exists of a device unique parameter and device variable parameters.

12.6.1 Device Unique ID

- The **Global Unique ID** is a device unique identifier that is based on the MAC address of the modulator.

12.6.2 Device Variable Parameters

The device variable parameters can be adjusted by the operator.

The geo coordinates indicates the current position of the modulator.

When "**Use Geo Coordinates**" is turned **On**, the latitude and longitude information is added to carrier ID.

The telephone number makes it easier for satellite operators to contact you in case of emergency. It is possible to enter the extension number of the department or person that is responsible for the system configuration.

For example: +323 780 65 00 ext. xxxx. (With xxxx the correct extension number.)

Be aware that ext. is case sensitive.

The user data can be used to enter free text, it is possible to enter up to 24 characters.

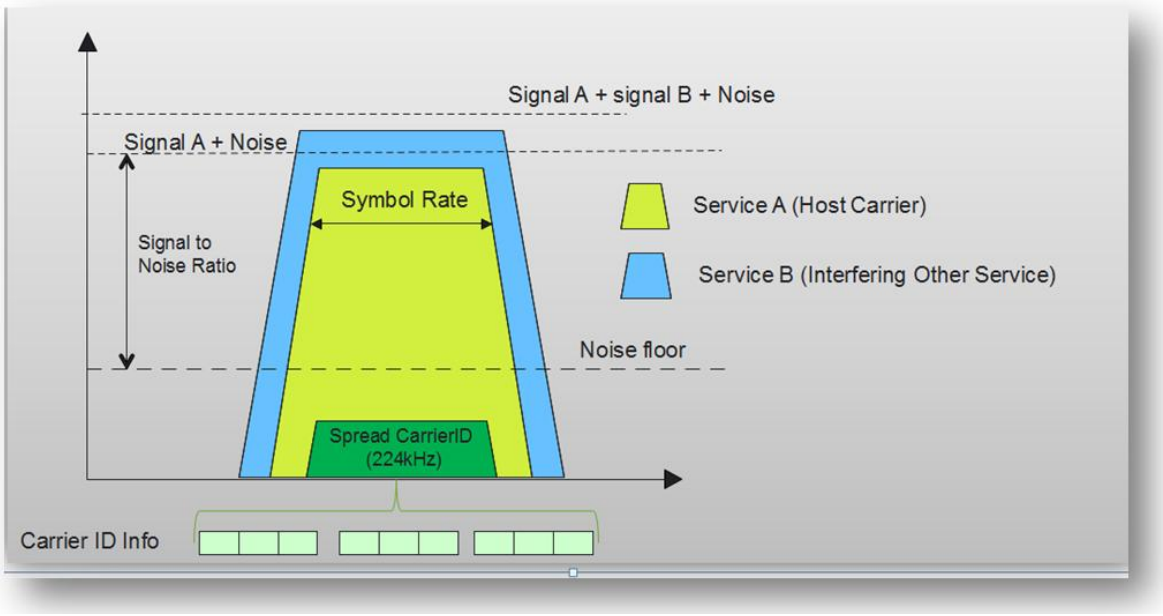
For example: Enter the name of the company that is responsible for the uplink.

DVB-CID Format: At this moment only one format exists and by default the parameter setting is 1.

12.6.3 How does it Work?

The DVB carrier identification is transmitted within the uplink RF carrier as a spread spectrum signal below the the carrier.

The DVB carrier identification information is independent of the payload of the carrier being identified.



12.6.4 What to do when Interference is Detected?

» Contact your satellite operator;

» The satellite operator has the right equipment to filter out the Carrier ID Information;

» Your satellite operator identifies who is responsible for the interference and takes contact with the other satellite operator to alert them of the interference.

12.7 TS Analyser

The transport stream analyser makes it possible to monitor the incoming transport stream. The purpose of this feature is to help determine if a problem seen at the output of a satellite receiver is due to a problem on the satellite link or to a problem in the head-end before the modulator. Consequently, it provides the possibility to identify the root cause of service outages that happened in the video head-end, or on the transmission path between the video mux and the satellite modulator. Because the analyser is built into the modulator, inserting it does not change the behavior of the signal or the topology of the network, making the troubleshooting easier. This leads to a shorter defect resolution time.

Go to the following location to view the parameters in this functional block.

M6100> TS Analyser

- The TS analyser can be enabled at any time.
- It is possible to reset the TS analyser and this to restart an analysis of the incoming transport stream.

When the user enables or resets the TS analyser the following alarms are reported:

• Pat_error;

• Sync_byte_error

• TS_sync_loss

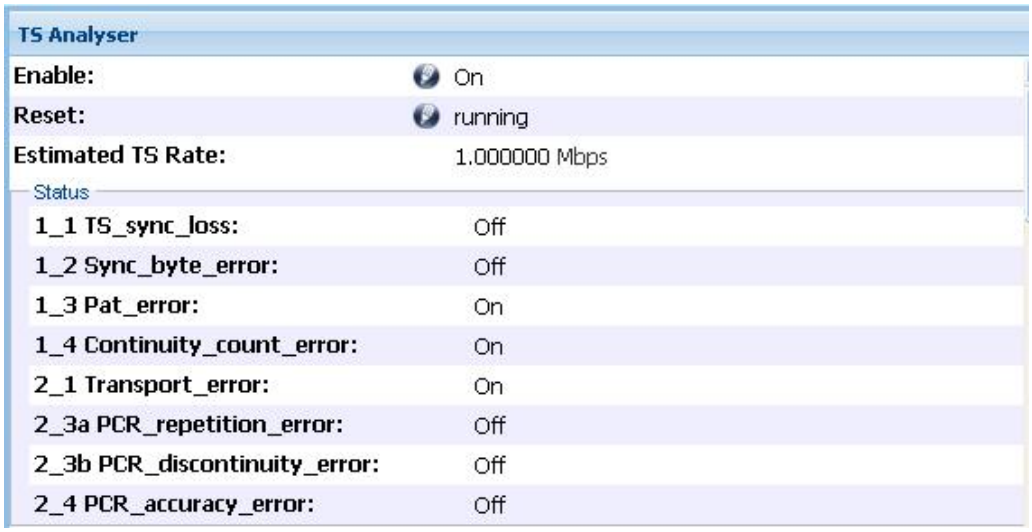
These alarms should disappear after five seconds. When these alarms do not disappear after five seconds it is needed to check the transport stream that is being analyzed.

Measurement of the transport stream bit rate, variations in the bit rate may indicate errors in the video processing head-end preceding the satellite modulator, in video source losses, still pictures, failing video encoder etc. This measurement is made on the incoming stream. The measured bit rate is accurate to the nearest entirely loaded packet. For example: for an incoming bit rate of 2250000bps or 149,6 TS packets/s. The actual measurement should be 149,6 packets/s but this value is rounded off to 149 packets/s. This translates into a measured bit rate = 149 x 188 x8= 224096bps. In case of TSoIP input, measurement is done after some jitter removal, but before the full rate smoothing performed just before the modulation stage. Jitter on the incoming signal may thus affect this measurement a bit.

While not being a full-fledged TS analyser, this feature provides most of the measurements needed for a good tracking of the origin of issues seen in a typical head-end.

12.7.1 TS Analyser Status Overview

The detection of the following MPEG errors status overview:



Note these Errors are defined in the following standard: TR101 290.
(The error explanations in this manual are kept short and intuitive.)

- All the errors trigger the corresponding alarm. These alarms are also displayed in the in the alarm pane of the GUI.
- The TS analyser errors are associated with an interface alarm and they can be used for redundancy purpose.

- Error 1.1: TS_sync_loss: absence of two or more SYNC bytes regularly spaced.
- Error 1.2: Sync_byte_error: the correct sync byte (0x47) does not appear after 188 or 204 bytes;
- Error 1.3 PAT_error: No valid PAT detected;
- Error 1.4 Continuity_count_error: This error is usually caused by a disordering of the packets, by the loss of a packet or by the duplication of a packet;
- Error 2.1 Transport_error: A Transport_error_indicator flag is set in the TS-Header of a packet;
- Error 2.3a PCR_repetition_error: Time interval between two consecutive PCR values is more than 40 ms;
- Error 2.3b PCR_discontinuity_indicator_error: The difference between two consecutive PCR values (PCRi+1 – PCRi) is outside the range of 0...100 ms without the discontinuity_ indicator set;
- Error 2.4 PCR_accuracy_error: PCR accuracy of a program is not within ±500 ns

The PCR_accuracy is measured using the MGF3 filter profile. Please refer to the TR101 290 standard for more information on this filter profile.

12.7.2 Error PID Table

This table summarizes the PIDs for which a PCR error was detected and displays the exact PID type. The table also indicates a continuity count error and a transport error.

Error PID Table

PID	Type	Continuity Count Error	Transport Error
8	Others	On	Off
14	Others	On	Off
18	EIT or ST CIT	On	Off
20	TDT or TOT or ST	Off	On
24	Others	On	On
28	Inband	On	Off
29	Measurement	On	Off
31	SIT	On	Off
46	Others or Ghost	Off	On
47	Others or Ghost	Off	On

12.7.3 PCR PID Table

This table lists all the PIDs that contain a PCR (Program Clock Reference) and the related measurements.

The PCR PID table is available in combination with the CBR traffic profile. With the VBR traffic profile, this table is not populated.

PCR PID Table

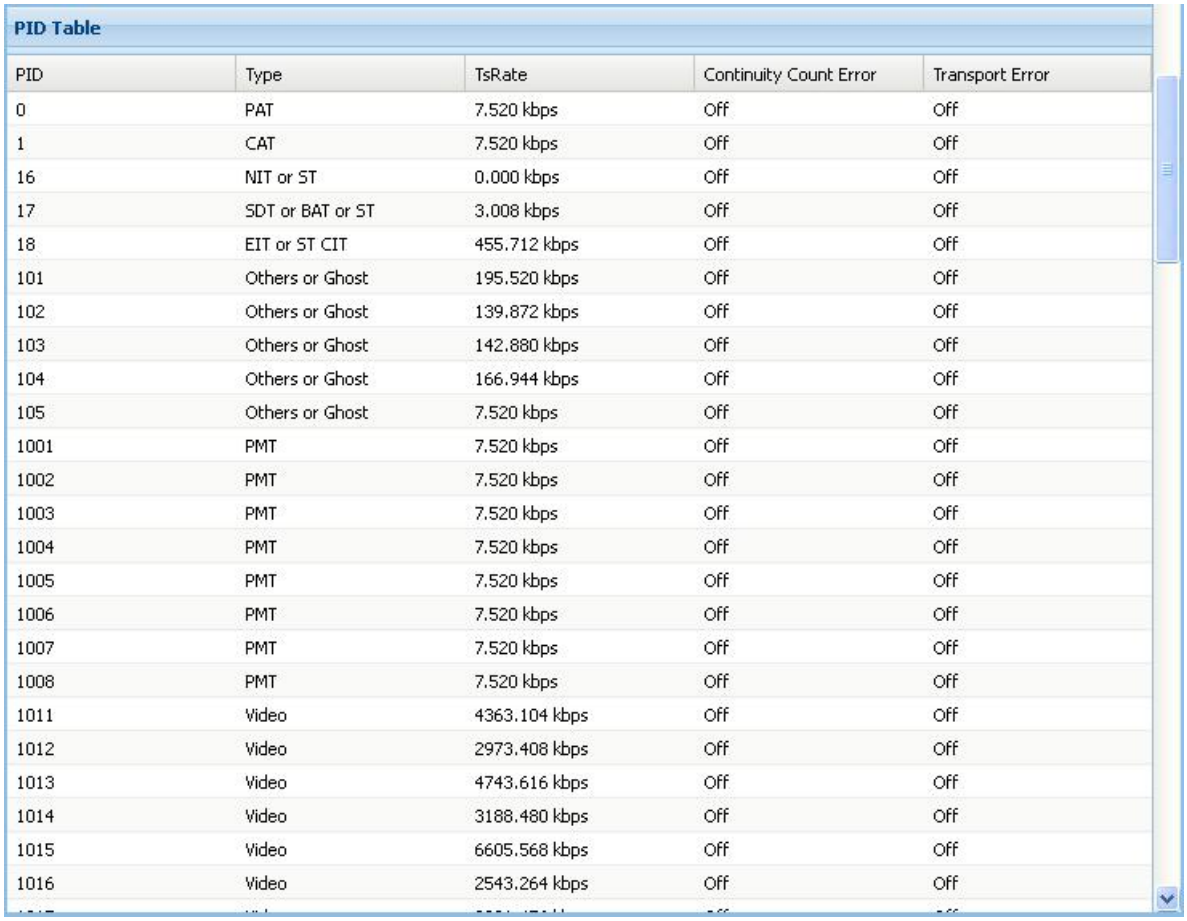
PID	PCR Interval	Repetition Err	Accuracy Errc	Min PCR_AC	Max PCR_AC	Min Peak PCR	Max Peak PCI	Rate Offset	PCR Rate
1011	25 ms	Off	Off	-72 ns	71 ns	-5640600 ...	1314578 ns	16 ppm	42.23771...
1012	37 ms	Off	Off	-122 ns	92 ns	-8340541 ...	1945393 ns	16 ppm	42.23770...
1013	24 ms	Off	Off	-129 ns	70 ns	-5642012 ...	1313488 ns	14 ppm	42.23761...
1014	36 ms	Off	Off	-83 ns	83 ns	-8369688 ...	1945251 ns	13 ppm	42.23759...
1015	25 ms	Off	Off	-86 ns	79 ns	-5642232 ...	1314030 ns	14 ppm	42.23761...
1016	37 ms	Off	Off	-83 ns	93 ns	-8351007 ...	1945278 ns	13 ppm	42.23760...
1017	24 ms	Off	Off	-124 ns	92 ns	-5625573 ...	1314039 ns	14 ppm	42.23763...
1018	37 ms	Off	Off	-103 ns	73 ns	-8349561 ...	1945077 ns	12 ppm	42.23753...
1311	14 ms	Off	Off	-132 ns	116 ns	-3264021 ...	1749257 ns	16 ppm	42.23769...
1312	14 ms	Off	Off	-161 ns	122 ns	-3262461 ...	1766360 ns	15 ppm	42.23769...
1313	14 ms	Off	Off	-168 ns	118 ns	-3339090 ...	1754216 ns	16 ppm	42.23769...
1314	14 ms	Off	Off	-187 ns	93 ns	-3327272 ...	1724478 ns	16 ppm	42.23769...
1315	14 ms	Off	Off	-159 ns	111 ns	-3308442 ...	1722299 ns	16 ppm	42.23769...
1316	14 ms	Off	Off	-128 ns	114 ns	-3626061 ...	1779367 ns	15 ppm	42.23768...

The following values are provided:

Measurements	Description
PCR Interval	Measured interval time (in ms) between two consecutive PCR packets.
Repetition Error	PCR repetition error.
Accuracy Error	PCR Accuracy Error.
Min PCR_AC	Minimum value of PCR accuracy value (nanoseconds) over the last second.
Max PCR_AC	Maximum PCR_accuracy value detected over the last second.
Min Peak PCR_AC	Lowest PCR_accuracy value detected since last reset (with an initial wait time of a few second).
Max Peak PCR_AC	Highest PCR_accuracy value detected since last reset (with an initial wait time of a few second).
Rate Offset	Offset in ppm between the rate computed from the PCR values and the actual rate. The actual rate is the measured rate in case of ASI inputs, or the user-defined rate in case of TSoIP input.  Note: as the device clock has a precision of around 1 ppm, the rate offset is also an indication of the clock offset between the source device (encoder or multiplexor) and a true reference (with 1 ppm precision). The rate offset is thus also an indicative measurement of the PCR clock offset, while not being a formal measurement of this value as defined in the standard.
PCR Rate	Displays the current rate calculated from the PCR values in the corresponding PID.

12.7.4 PID Table

This table lists all the PIDs that are present in the stream.



PID Table

PID	Type	TsRate	Continuity Count Error	Transport Error
0	PAT	7.520 kbps	Off	Off
1	CAT	7.520 kbps	Off	Off
16	NIT or ST	0.000 kbps	Off	Off
17	SDT or BAT or ST	3.008 kbps	Off	Off
18	EIT or ST CIT	455.712 kbps	Off	Off
101	Others or Ghost	195.520 kbps	Off	Off
102	Others or Ghost	139.872 kbps	Off	Off
103	Others or Ghost	142.880 kbps	Off	Off
104	Others or Ghost	166.944 kbps	Off	Off
105	Others or Ghost	7.520 kbps	Off	Off
1001	PMT	7.520 kbps	Off	Off
1002	PMT	7.520 kbps	Off	Off
1003	PMT	7.520 kbps	Off	Off
1004	PMT	7.520 kbps	Off	Off
1005	PMT	7.520 kbps	Off	Off
1006	PMT	7.520 kbps	Off	Off
1007	PMT	7.520 kbps	Off	Off
1008	PMT	7.520 kbps	Off	Off
1011	Video	4363.104 kbps	Off	Off
1012	Video	2973.408 kbps	Off	Off
1013	Video	4743.616 kbps	Off	Off
1014	Video	3188.480 kbps	Off	Off
1015	Video	6605.568 kbps	Off	Off
1016	Video	2543.264 kbps	Off	Off

The following information is displayed in the table.

Information	Description
PID	Displays the PIDs that are present in the stream.
Type	The PID type that is detected.
TS Rate	Displays the transport rate.
Continuity Count Error	Indicates if a continuity count error is detected.
Transport Error	Indicates if a transport error is detected.

12.8 PRBS Generator

Option number AS-01 is required to use this feature!

The PRBS (Pseudo Random Bit Sequence) generator is used to perform basic tests on the device or to get an indication on the satellite link quality.

When using the PRBS generator check that the NIT Carrier ID and Rate Adapter are disabled. Note: The randomness of the signal is not guaranteed when these settings are enabled.

PRBS can be activated on the following locations:

M6100> ASI Input >> Signal Selection

M6100> ASI Output >> Signal Selection

A warning message is raised when the PRBS generator functionality is already used by another ASI interface. PRBS can only be active on one location in the device at a time.

Both locations display the following parameters:

M6100 Boadcast Satellite Modulator> ASI Input >> PRBS Generator

And

M6100 Boadcast Satellite Modulator> ASI Output >> PRBS Generator

Parameter	Description
TS Bit Rate	Enter a TS Bit Rate in bps that must be generated.
Type	Define what kind of test signal to use: • PRBS: Configures the test generator to generate transport stream packets containing PRBS data. The generated PRBS complies with HP3764 Compatible 2^23-1 PRBS sequence as specified in CCITT Rec. 0.151. • Counter: Configures the test generator to generate transport stream packets containing 8-bit counter values as data. This counter data cannot be analyzed by the test detector. It can only be used for manual verification by an external analyzer.
PID Handling	Configuration of the test generator to generate transport stream packets with a valid transport stream header. The configured PID (Packet Identifier) is inserted in the transport stream header and the continuity counter is incrementing. Possible settings: • Off: Transport stream packets are generated without a valid transport stream header. In this case, a 0x47 sync marker followed by 187 test bytes are generated.

	• On: The transport stream packets are generated with a PID value that is inserted in the first two bytes following the sync marker (byte 1 and byte 2) of each data packet. It is used for proper error detection when the rate of the generator is lower than the interface rate of the modulator board or when the test generator is configured to create a burst of transport packets (data packets combined with null packets).
PID Value	Configure the PRBS generator PID value.
Number Data Packets	Configure the number of data packets per burst that the test generator has to generate. The baseband source can generate alternating bursts of data packets and null packets. Once the burst is finished, it starts over repetitively. This is controlled by setting the number of data packets and null packets. This command controls the number of data packets per burst. The continuity counter is not reset when the next burst starts. A maximum of 255 data packets per burst is possible.
Number Null Packets	Configuration of the number of null packets per burst that have to be generated.

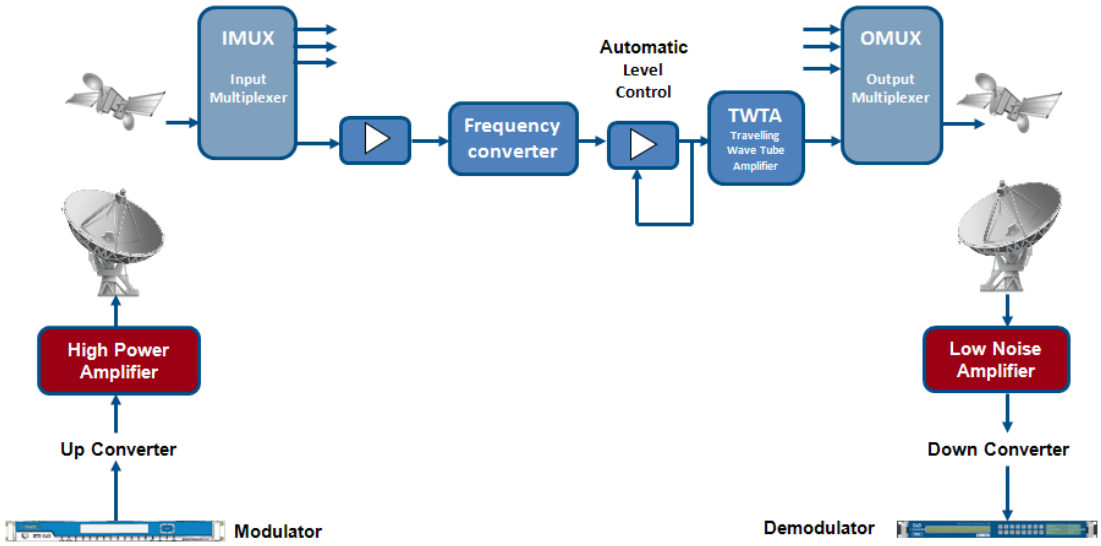
12.8.1 PRBS Monitor

These parameters can only be set on the following location:

M6100> ASI Input >> PRBS Monitor

Parameter	Description
Enable	Enable the PRBS Monitoring.
PID Handling	Enable/disable the detection of a PID inside data packets of the PRBS stream.
PID Value	Configure the PRBS monitor PID value. Define which PID value must be filtered out of the incoming data.

12.9 Equalink™



Equalink™ is introduced to optimize the satellite link performance by counteracting distortion effects in a satellite link.
The following distortions can be present:

Linear distortion

Linear distortions are typically compensated by the demodulator equalizer on most modern demodulators.

Older demodulators with less good equalizer specs can suffer from linear distortion. Therefor linear Equalink is only used to optimize a broadcast network with old demodulators..

- Imperfections of the amplitude response of the transponder;
- Degradation caused by the phase response of the IMUX/OMUX filters lead to imperfections in the group delay response.

Non Linear distortion

- AM/AM (output amplitude versus input amplitude);
- AM/PM (output phase versus input amplitude);
- Caused by the non-linearity in the amplifier of the satellite.

BER performance degradation due to transmission channel impairments is becoming increasingly important in DVB-S2 systems operating with higher order modulation formats (16APSK, 32APSK), in particular at higher symbol rates.

The Equalink™ concept effectively optimizes satellite link performance by counteracting these distortion effects.

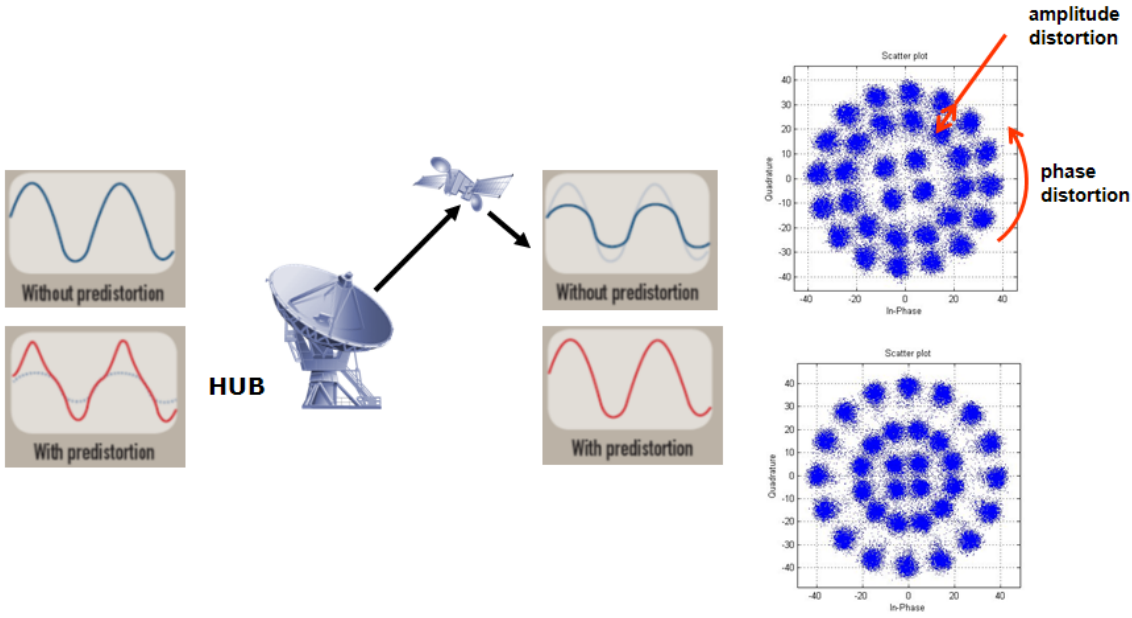
Link performance can be expressed in terms of Bit or Packet Error Rate (BER or PER) versus Energy-per-symbol to Noise density ratio (Es/No).

For a communication channel over a satellite link, the overall link performance can be severely degraded by channel impairments.
Examples of such impairments are:

- Adjacent Channel Interference and Co-Channel Interference;
- Inter-Modulation;
- Adjacent Satellite Interference;
- Phase noise;
- Signal distortion.

The Equalink™ concept effectively optimizes satellite link performance by counteracting these effects.

This is displayed in the following figure:



Newtec M6100, MDM6100, MDM6000 Modulators equipped with the Equalink™ feature contain both linear- and non-linear pre-distortion functions, which can be individually enabled/disabled.

12.9.1 Enable Equalink™

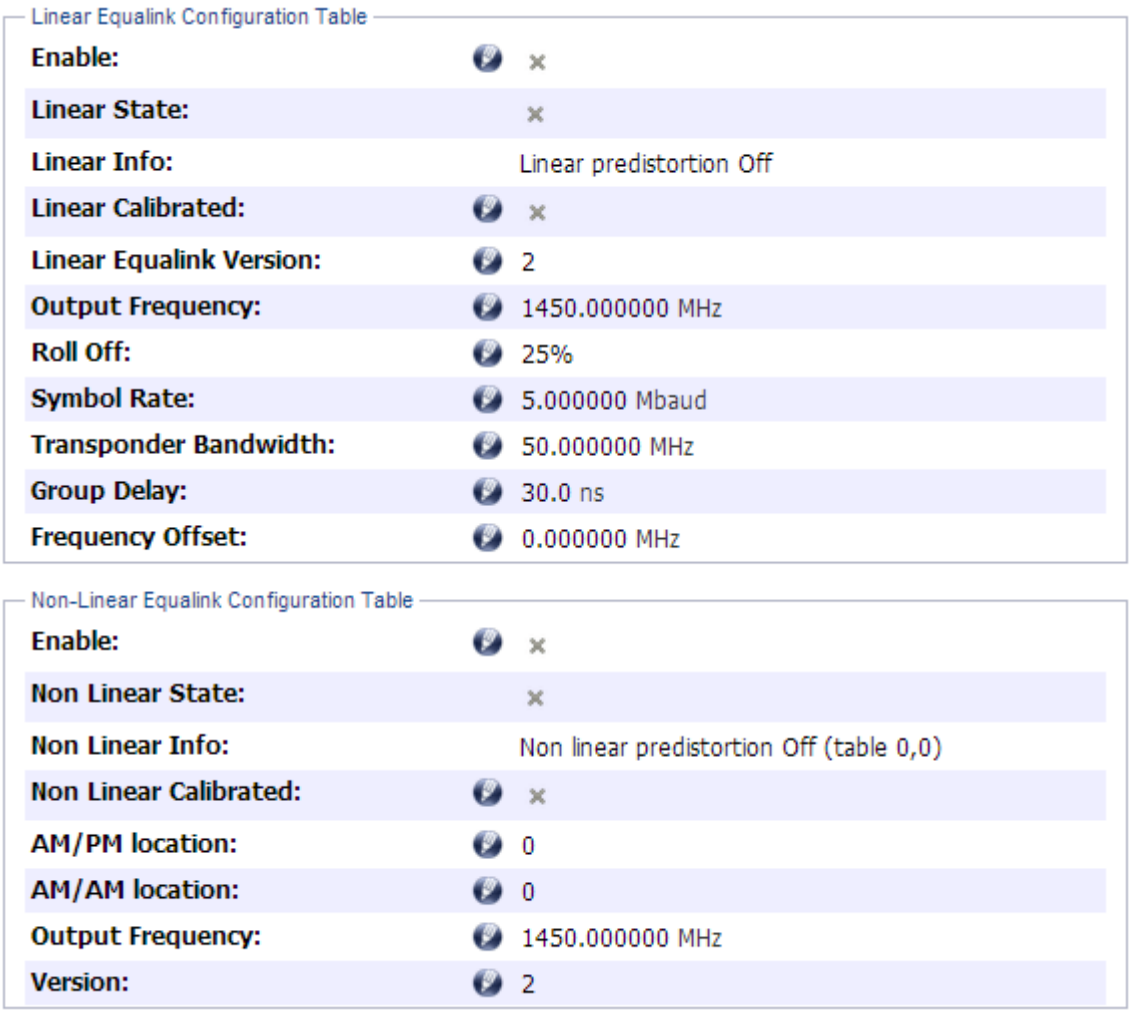
» Log in as expert.

Before enabling the Equalink feature, the calibration procedure must be run first. This calibration procedure calculates the Equalink parameters.

This can be done in two ways:

1. manually import an Equalink File (linear Equalink only);
2. use the automatic Equalink procedure (linear and non-linear).

The results of the Equalink calibration are shown in the GUI.



For correct Equalink usage, it is important that the modulator settings match the Equalink applicability parameters. If this is not the case, then restart the calibration procedure. As expert user it is possible to enter Equalink settings manually allowing to overrule the results from the calibration procedure and setting the (non)-linear calibration flag.

- Enable or disable the stored linear- and/or the non-linear predistortion.
- Read out the state of the predistortion.

The predistortion parameter can be enabled and the predistortion state can be off. This is the case when the operator needs to perform tests by sending a pure carrier. This test case automatically switches off the predistortion parameter.

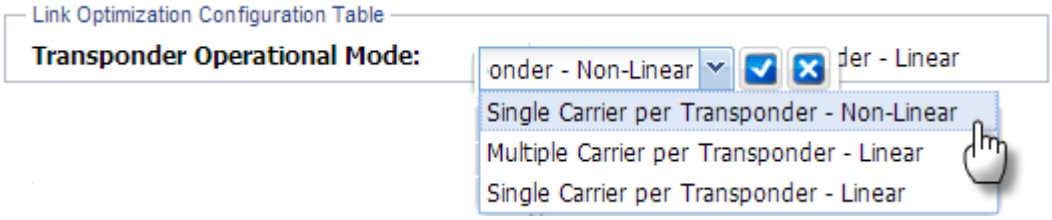
The Non-Linear Info: indicates if the non-linear predistortion is loaded or not.

Before enabling **linear Equalink**, check the following:

- Modulator Output frequency and Modulator symbol rate values must match with the corresponding Equalink applicability parameters. This should be the case if the calibration procedure was applied;
- Roll-off factor of the modulator = max 20% (so it must be 5%, 10%, 15% or 20%).
  Or if the applicable roll-off = 20%, the roll-off of the modulator should be ≤ 20%.

Before enabling **non-linear Equalink**, check the following:

- The 'transponder operational mode' parameter in the Link Optimization Table must be set to 'single carrier per transponder - Non-linear'



- Modulator output frequency value must match with the corresponding calculated Equalink applicability parameter;
- If Equalink version is ≥ 2, then the modulator symbol rate must be ≥ 22 Mbaud;

As the Equalink applicability parameters must match the corresponding modulator settings, it is advised not to change the modulator parameters when Equalink is enabled. Doing so will result in error messages, blocking you to change those modulator parameters.

12.9.2 Import Non-Linear Equalink™ File

In this menu it is possible to import the calculated predistortion file.

» Navigate to the **Tasks Pane**;

» Click **Equalink;**

» Click **Import…**.;

» Select the **Predistortion-type:**

• Non-linear.

» Click **Browse** and select the correct file;

» Click **Import**.

When a new non-linear Equalink™ file is imported, the previous file is overwritten.
This is independent of the device configuration.

12.9.3 Import the Linear Equalink™ File

In this menu it is possible to import the calculated predistortion file.

» Navigate to the **Tasks Pane** (GUI).

» Click **Equalink**.

» Click **Manual Import…**.

» Select the **Predistortion-type**:

• linear.

» Click **Browse** and select the correct file.

» Click **Import**.

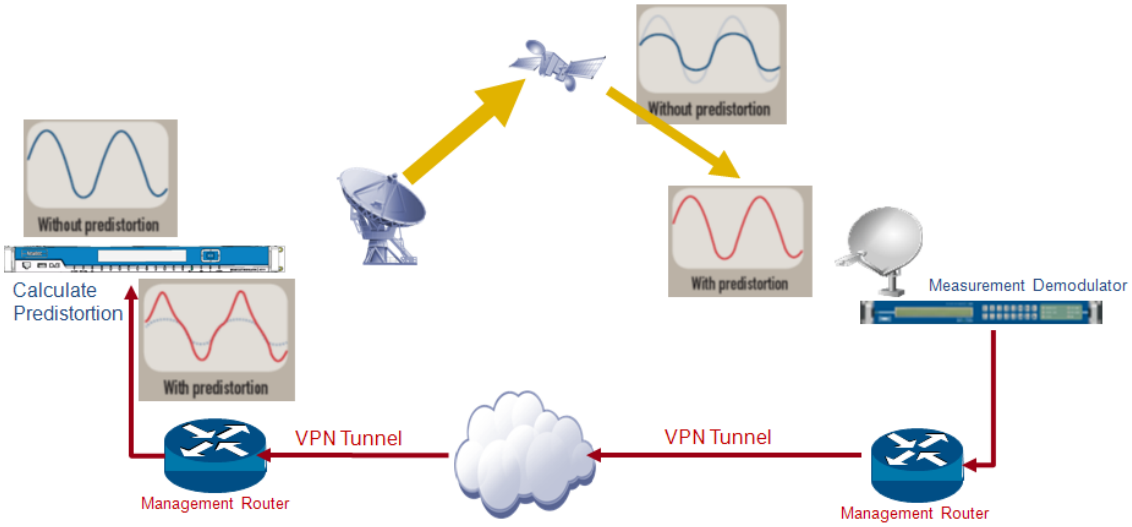
When a new linear equalink file is imported, the linear equalink settings are updated in the current configuration.

An explicit save is required!

12.9.4 Automated Linear Equalink™

M6100 >> Calibration >> Linear Equalink

This feature provides automated linear Equalink™.



The automated Equalink™ calibration is done by performing measurements between the M6100 and a Newtec demodulator or modem.
The demodulator is going to monitor the carrier to distortion ratio (C/D) of the satellite link during the automated Equalink™ calibration period.
The more monitoring iterations that are performed during the measurement the better the result of the calibration.

Note: The higher the amount of iterations, the longer the calibration period takes (typically one iteration takes 5 min).

The monitoring results are transferred towards the M6100 over an IP network (terrestrial link or satellite link) and used by the modulator to calculate the optimal predistortion result.

The calibration gain (in dB) displays the difference between the satellite link performance before and after committing the linear Equalink™.
Once the calibration gain is committed, the gain indicator is reset to zero. This implies that a new calibration can be started.

The fading margin (in dB) is used to monitor the fading during the automated Equalink™ calibration period. When the margin is exceeded the calibration is interrupted. The calibration must be restarted manually!

Consult the calibration log file to get a detailed overview of the automated Equalink™ calibration procedure.

12.9.5 Automated Linear Equalink™ using Internal test Traffic

Perform the **Internal Test Traffic** calibration procedure during uncritical hours!

This because the procedure is a **quasi**-non-service disruptive procedure.
The procedure causes about 15 small glitches (BBF error sequences).

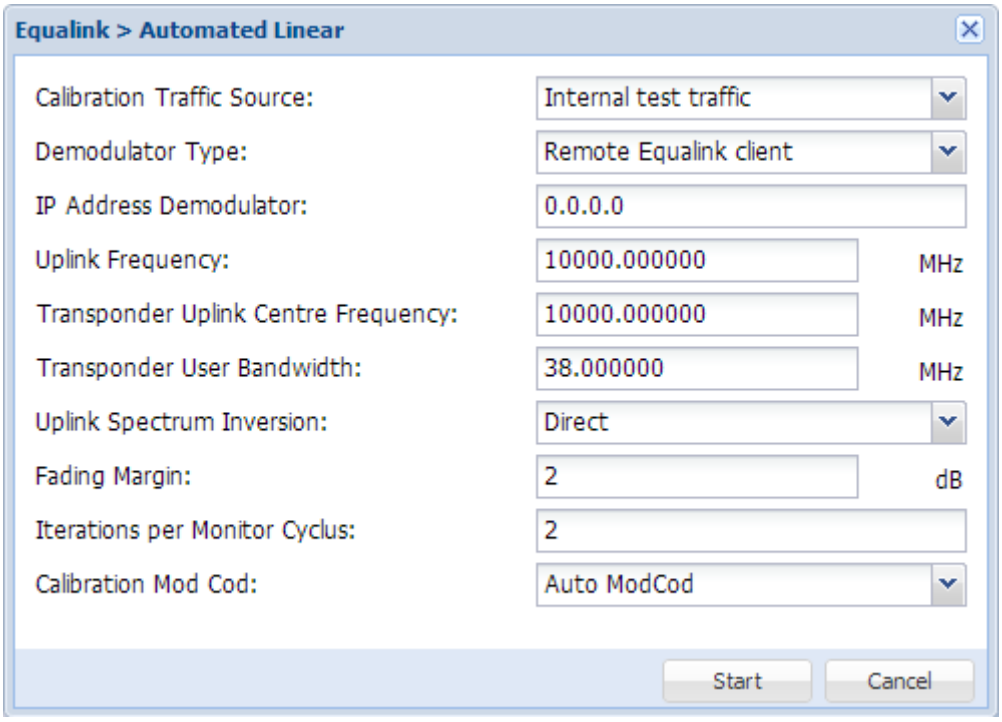
Use the following procedure to perform automated Linear Equalink™ measurements.

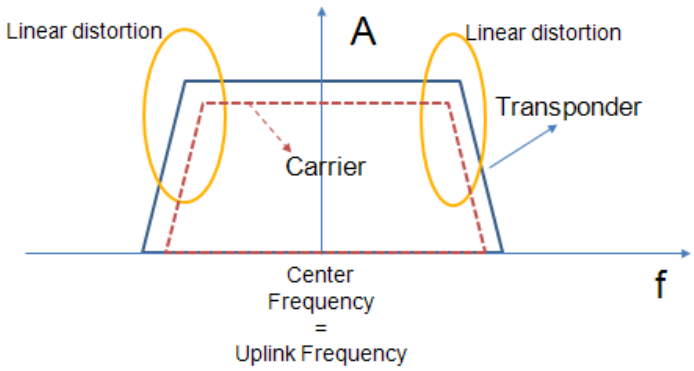
» Login as **expert user;**

» Navigate to the device **Tasks Pane** (GUI);

» Click **Equalink;**

» Click **Automated Linear**



Parameter	Description
Calibration Traffic Source	• **Internal test traffic** (When using this mode, the live traffic is interrupted and a PRBS is started to perform the calibration.)
Demodulator type	Indicate what type of demodulator is used to run the calibration procedure. • External demodulator: – RMCP Demodulator (select this type when working with equipment such as EL910. When this is selected, RMCP commands are used to communicate with this type of device.) – Remote Equalink Client, in this case the remote device is a M6 type demodulator. • Internal demodulator: – Local S2-EXT Demodulator, in this case you are calibrating with the wideband demodulator inside the modulating device. Note: When using this it is advised to add noise in the hub downlink.
IP Address Demodulator	Enter the MGMT IP address of the demodulator.
Uplink Frequency	Enter the uplink frequency.
Transponder Uplink Centre Frequency	Enter the same Uplink Frequency and Transponder Center Frequency to optimize the linear distortion for the full transponder. Refer to the following figure: 
Transponder User Bandwidth	Enter the corresponding bandwidth.
Iterations per Monitor Cycle	Enter the amount of iterations per monitoring cycle you want to perform. Two iterations provide a relative fast calibration.The higher the amount of iterations the longer the calibration period takes, (typically, one iteration takes 5 minutes). The number of iterations recommended is 3.

Parameter	Description
Fading Margin	Enter the maximum fading margin that is allowed during the calibration period.
Calibration ModCod	The calibration will run in DVB-S2 or DVB-S2X. • Auto ModCod: In this case the calibration uses different ModCods to perform the calibration. • Manual selection of the Equalink calibration ModCod.

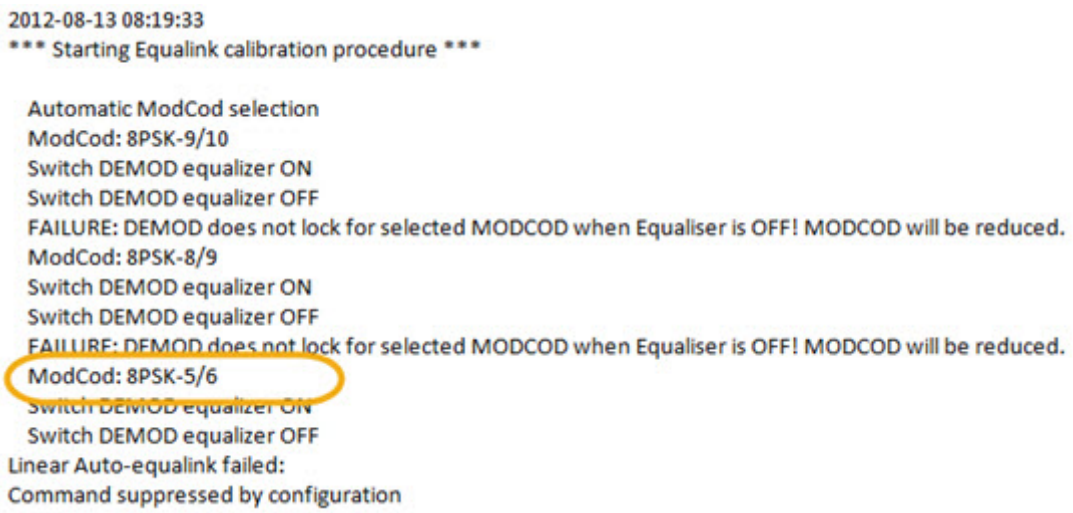
» By default the Calibration ModCod is set to Auto ModCod, in this case the application searches for the most optimal ModCod to perform the calibration;

It is possible that the calibration stops when running the procedure with Auto ModCod selected.

If this is the case, you have to select the Calibration ModCod manually.

Please check the log file and select the lowest ModCod value indicated in the log file.

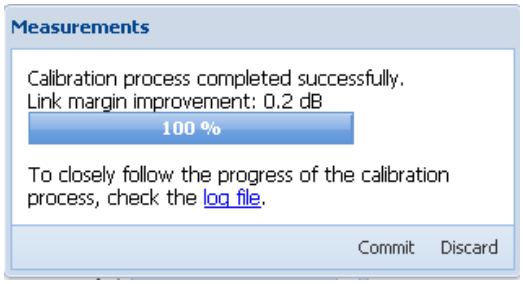
(please refer to the figure below)



» Click Start (to start the calculation);

» A progression bar is displayed;

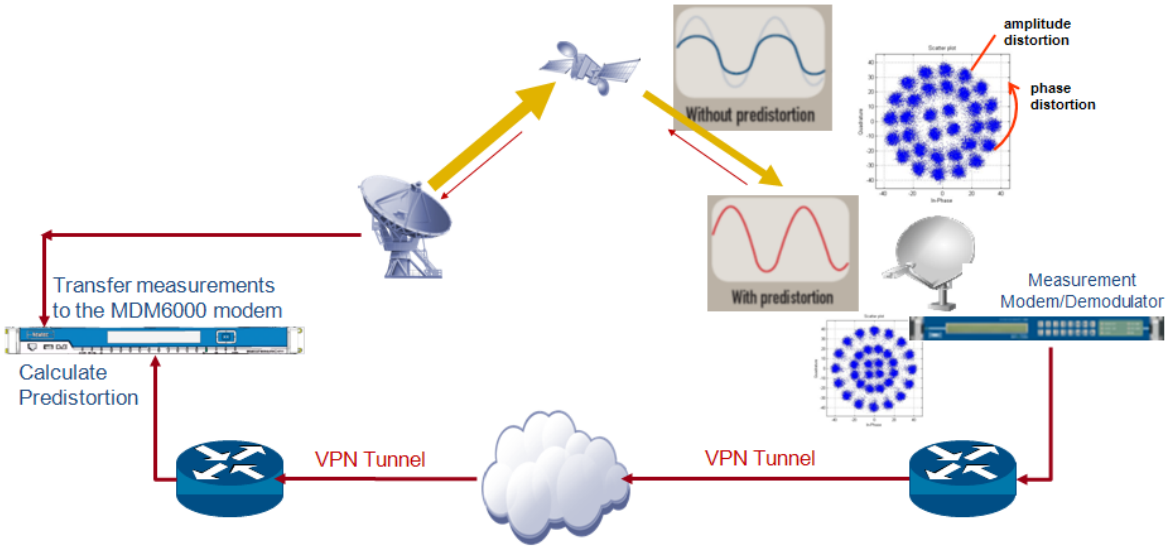
» When the measurements are performed, the link margin improvement is displayed;



» Click **Commit** to confirm the link margin improvement.

When a linear Equalink procedure is committed, the linear Equalink settings are updated in the current configuration. An explicit save is required!

12.9.6 Automated Non-Linear Equalink™ Procedure



Also refer to the Automated Non Linear Equalink™ procedure. This document describes the different calibration procedures depending on transponder settings (Fixed Gain Mode or Automatic Level Control).

The procedure can be found on the CD-ROM that is delivered together with the device.

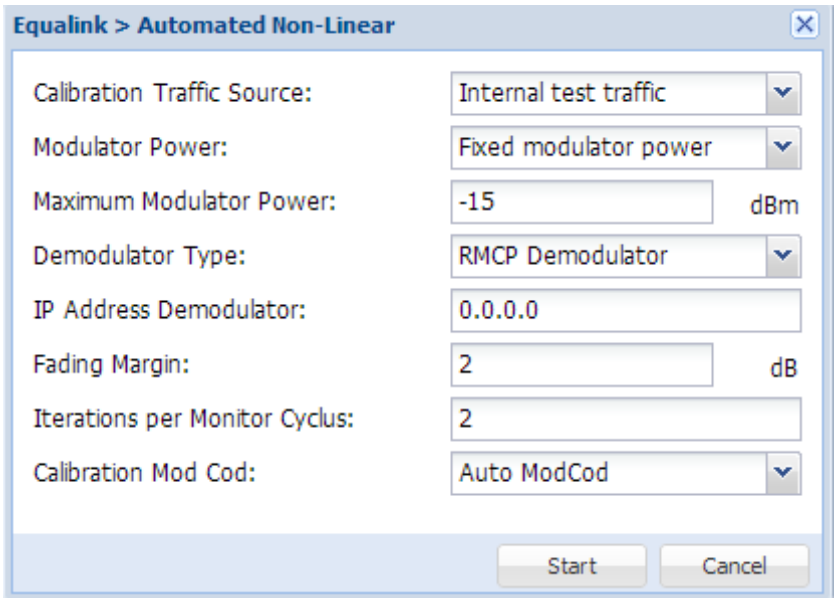
Use the following procedure to perform automated Non linear Equalink™ measurements.

» Login as **expert user;**

» Navigate to the **Tasks Pane** (GUI);

» Click **Equalink;**

» Click **Automated Non-Linear;**



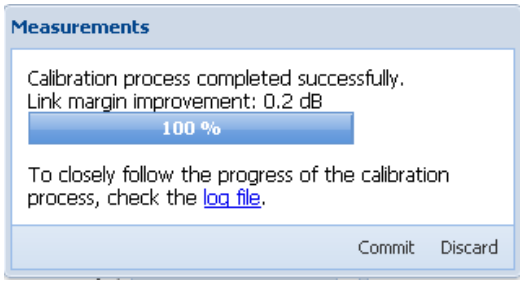
Parameter	Description
Calibration Traffic Source	• **Internal test traffic** (When using this mode, the live traffic is interrupted and a PRBS is started to perform the calibration.) • **Live Traffic** (When using this mode, the live traffic is not interrupted to perform the calibration.)
Modulator Power	• **Auto modulator power** The modulator systematically changes the output power to search for the optimal power. Note that output power will not exceed the Maximum Modulator Power. • **Fixed Modulator Power** The modulator power used is fixed and defined under modulator (output level).
Maximum Modulator Power	1. Enter the Maximum Modulator Power, the range is between -35dBm and 10dBm. The following parameters should be taken into account: – Highest level whereby measured C/D is >11dB and DEMOD is locked. (PRBS could be used to be certain that data is present in the carrier) – Highest level that is allowed by the uplink HPA. verify that spectral regrowth remains under -30dBc – Lowest OBO (Output Back Off) and Highest Downlink EIRP (Effective Isotropic Radiated Power) that is allowed by the Satellite Operator The Satellite operator will verify this during line up! 2. This value is not applicable incase the Fixed Modulator Power is used.
Demodulator type	• External demodulator: – RMCP Demodulator (select this type when working with equipment such as EL910. When this is selected, RMCP commands are used to communicate with this type of device.) – Remote Equalink Client, in this case the remote device is a M6 type demodulator. • Internal demodulator: – Local S2-EXT Demodulator, in this case you are calibrating with the wideband demodulator inside the modulating device. For more information refer to *Device Identification. on page 91* Note: When using this it is advised to add noise in

Parameter	Description
	the hub downlink.When using this it is advised to add noise in the hub downlink.
IP Address Demodulator	Enter the MGMT IP address of the external demodulator.
Fading Margin	Enter the maximum fading margin that is allowed during the calibration period.
Iterations per Monitor Cycle	Enter the amount of iterations per monitoring cycle you want to perform. Two iterations provide a relative fast calibration.The higher the amount of iterations the longer the calibration period takes, (typically, one iteration takes 5 minutes). The number of iterations recommended is 3.
Calibration ModCod	The calibration will run in DVB-S2 or DVB-S2X. • Auto ModCod: In this case the calibration uses different ModCods to perform the calibration. • Manual selection of the Equalink calibration ModCod.

» Click **Start;**

» A progression bar is displayed;

» When the measurements are performed, the link margin improvement is displayed:



» Click **Commit** to confirm the link margin improvement.

When a non-linear Equalink procedure is committed, the non-linear Equalink settings are up to date in the current configuration.

An explicit save is required to store the settings permanently!

12.10 DC BUC Power On L-Band Tx

The M6100 offers an optional DC power supply on the L-band Tx interface that can be used to power BUCs. This option combines the L-band transmit signal coming from the modulator with a DC power supply and an optional 10MHz reference signal. All these signals can be combined onto the L-band Tx Interface (N-connector).

The DC power supply (when enabled) provides a24V or 48V DC voltage with a maximum continuous current of 3.8A on the L-band Tx interface. Both possibilities are available when one of the following sales options, OU-05 or OU-06, is ordered.

12.10.1 Back Panel Description

The following figure shows the L-Band Tx connector when the BUC power for L-band Tx option is ordered.

The connector used is an N-connector 50 Ohm (Female).

Two LEDs indicate the state of the power supply.We refer to section
LED Behavior of the DC BUC Power for L-Band Tx on page 190

Switch off the power of the device before connecting the coax cable. This reduces the risk of personal injury from electric shock or damage to the device.

The maximum continuous current on this connector is 3.8A.
Use a coax cable (Cable Type DP-2!) as marked on the device.
This cable is tested for a maximum 60V DC and a maximum of 8A.

12.10.2 LED Behavior of the DC BUC Power for L-Band Tx

There are two LEDs that indicate the state of the DC BUC power for L-band TX.
The active LED corresponds to the selected voltage.

Both LEDs have the same behavior.

LED	State	Time	Behavior Description
48V or 24V	Off		This voltage is not applied on the L-Band Tx interface.
	Steady		This voltage is currently applied on the L-Band Tx interface.
	Blinking	1s	An overload alarm is present on the DC power supply. The circuit protection mechanism of the power supply is triggered and disables the output power. The protection mechanism monitors every 1s if the overload is removed and re-enables the DC supply if this is the case. The following situations can trigger the overload alarm: • The connected load is too high; • When a long cable is shorted at the outdoor equipment end.
		5s	A short circuit alarm is present on the DC supply. The circuit protection mechanism of the power supply is triggered and disables the output power.The protection mechanism monitors every 5s if the short circuit is removed and re-enables the DC supply. The following situations trigger the alarm: • The connected load is too high; • When a long cable is shorted at the outdoor equipment end. When a short circuit is present, due to a direct connection between the L-band Tx interface and the earthing, the LEDs on the back panel are off.

12.10.3 Set the DC BUC Power for L-Band Tx

M6100 > Modulator >> BUC Power on L Band TX

Parameter	Value	Description
Enable	On/Off	Enable or Disable the L-Band DC supply.
voltage	24V / 48V	Select the appropriate voltage for the equipment used in combination with the DC supply.On the back panel the corresponding LED is activated. Note: It is not possible to change this value when the DC supply is enabled.
Measured Output Voltage	Range 0V / 48V	Displays the actual voltage level on the L-band Tx interface.
Output Current	Range 0A / 8A	Displays the actual current being delivered by the DC supply: • When an overcurrent is detected the circuit protection mechanism is triggered and disables the DC supply. The protection mechanism monitors every 1s if the overload (overcurrent) is removed. The overload alarm is active. • When a short circuit is detected the circuit protection mechanism is triggered and disables the DC supply. The protection mechanism monitors every 5s if the short circuit is removed. The short circuit alarm is active.

12.11 Basic Interoperable Scrambling System (BISS)

12.11.1 Content Scrambling Modes

The BISS application on the M6100 protects the content of a MPTS (multi-program transport stream) during transmission.

BISS uses a Session Word as a scrambling key. The same key is used to scramble all programs.

The M6100 supports two different encryption modes with different scrambling behavior: standard mode or raw mode.

12.11.1.1 Standard Mode

The Standard Mode is fully DVB-compliant. In this mode, the payload of all packets is scrambled, except for the PSI/SI tables (PIDs<0x1F and PMT tables).

The scrambling starts when a valid PAT table is found and all existing PMT tables are identified.

When no PAT is detected within 1 second, the scrambling is however started in raw mode.

Each PMT table is updated with a proper CA descriptor (Conditional Access descriptor) if the descriptor is not yet available. The scrambler also inserts a CAT when no CAT is present in the transport stream.

In case of CRC error on the PAT or PMT, or if the incoming stream appears to be scrambled (CA descriptor in the incoming PMT), the scrambling is stopped to avoid making the signal unrecoverable. This behavior can be overruled with the “**Scrambling Suppression”** parameter.

Scrambling Suppression (for Standard Mode)

When operating in the **standard mode**, the scrambling by default stops in case of CRC errors on the PAT or a PMT or if a PMT already contains a CA descriptor. The reason is that the risk to scramble PMTs, or erase previous scrambling information would make the stream unrecoverable by an IRD.

It is possible to overrule this behavior, if the protection of the stream is more important than its decodability in case of errors. Do this by disabling the “**Scrambling Suppression**” parameter.

Keep this suppression enabled when the TS has high priority and getting the TS to the receiving end has more priority than scrambling the TS.

12.11.1.2 Raw Mode

In this mode the payload of all packets is scrambled except for the PID<0x1F. In this mode it is possible to overwrite the default 0x1F value in order to define the range of unscrambled PIDs (from 0x00 to a user-given value). Use the following parameters to define this range, **Min RAW Unscrambled PID and Max Raw Unscrambled PID.**

The scrambling starts immediately as this mode does not perform a check if a valid PAT is available in the TS.

Furthermore, this mode scrambles all PMTs (if any) and it does not insert a CAT in the transport stream.

This encryption mode guarantees SFN (Single Frequency Networks) integrity.

It can also be used to encrypt proprietary MPEG streams.

12.11.2 Key Management System

12.11.2.1 Odd/Even key

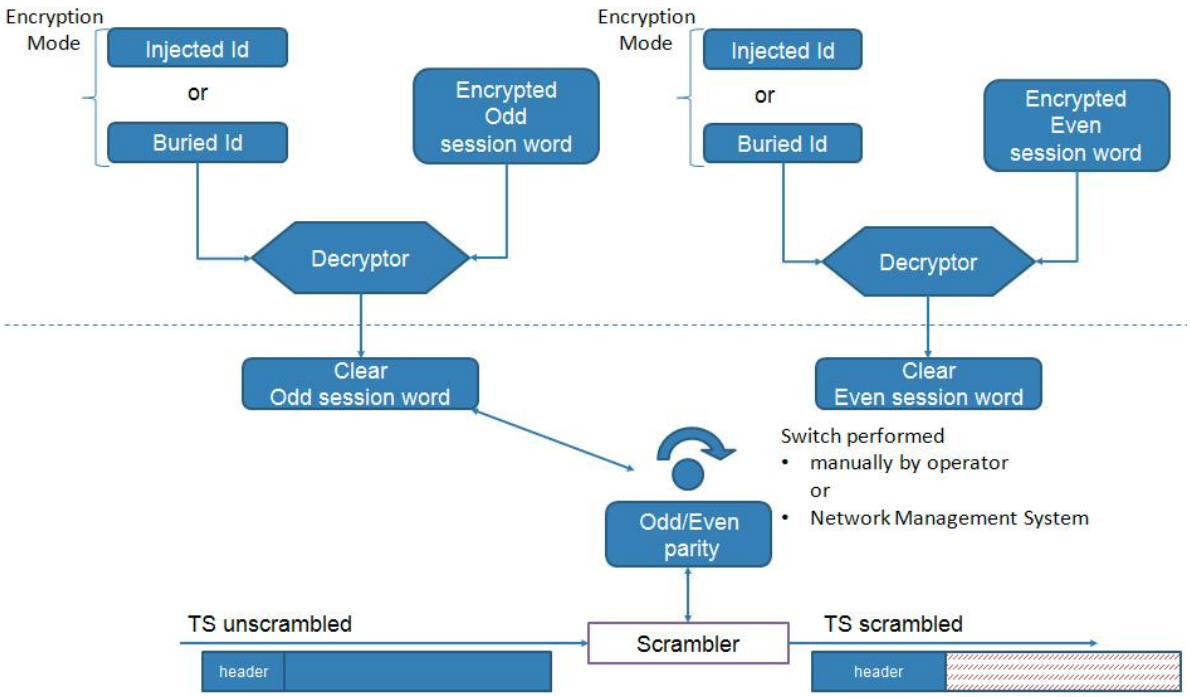
The BISS specification is based on the use of two scrambling keys: the odd key and the even key. One key is the active one, use to scramble the packets, while the other key is the future key to use. This allows to enter in devices the next key to use in advance and later activate at the chosen moment.

On the scrambling side (the modulator), the operator defines which key shall be used. On the descrambling side, the devices automatically detect which key to use.

Note that only the Even key should be used for BISS for interoperability with 3rd party receivers.

12.11.2.2 Key Management System Structure

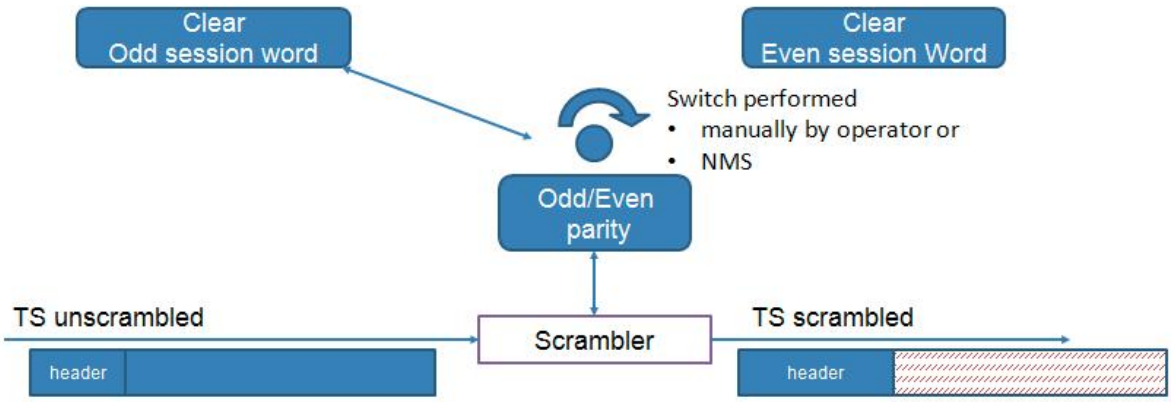
The following figure details the structure of the BISS Key management system that is implemented.



The key management structure can be split up into two parts, distribution of clear session words over a secure channel (bottom part) and distribution of Encrypted session words over a non-secure channel (top + bottom part). Both distribution methods are explained in the following sections.

12.11.2.3 Distribution of Clear Session Words over a Secure Channel

When the distribution of a session word can be performed over a secure channel (trusted manual operator, secured e-mail or any other trusted means), it is possible to enter the clear session word directly without extra protection.



Parameter	Description
Odd/Even Session word	This setting allows the user to set the odd or even clear session word. The entered clear session word is used by the scrambler as the real encryption key. The key parity defines if the odd or even key will be used by the scrambler. **Interface used** The clear session words are entered by the user through any interface (For example: Frontpanel, GUI, CLI, SNMP). It is not possible to read back the session words by any interface. **Hexadecimal** A session word exists out of 12 digits and is in hexadecimal format. When entering the session word, enter the most significant digit (nibble) first (reading from left to right). For example, 0xA13DBC42908F would be entered in the following sequence: A,1,3,D,B,C,4,2,9,0,8,F The clear session word must be distributed to all parties that are allowed to descramble the received data.
Key Parity	**Key Parity Selection on the Modulator** The user on the transmitting site selects whether to use the odd or the even session word. Note: When the Key Parity is set to odd, setting the even session word has no direct impact on the scrambled output and the other way around. The “new” session word becomes active when the key parity is switched on the scrambler.

Setting Clear Session Words

Starting Point: The odd session word is used by the scrambler. This is indicated in the header of the transport stream packet.

- **Entering an even session word does not affect the scrambled output.**
- The even session word is stored in the device
- Switch Key Parity (to Even)
- The output is now scrambled with the even session word. The header of the transport stream packet indicates that the even session word is used. The descrambler of the receiver reads out the header information and decrypts with the correct key..

Entering new session words is limited by the BISS specification to 10 times within a 5 minute period and there must be a minimum of 10 seconds between two changes.

It is also possible to edit the active session word directly (the odd session word in the example here). It will then be directly used in the scrambling. The new session word has to be entered also on the descrambler side to allow proper descrambling. As a consequence, editing the active session word

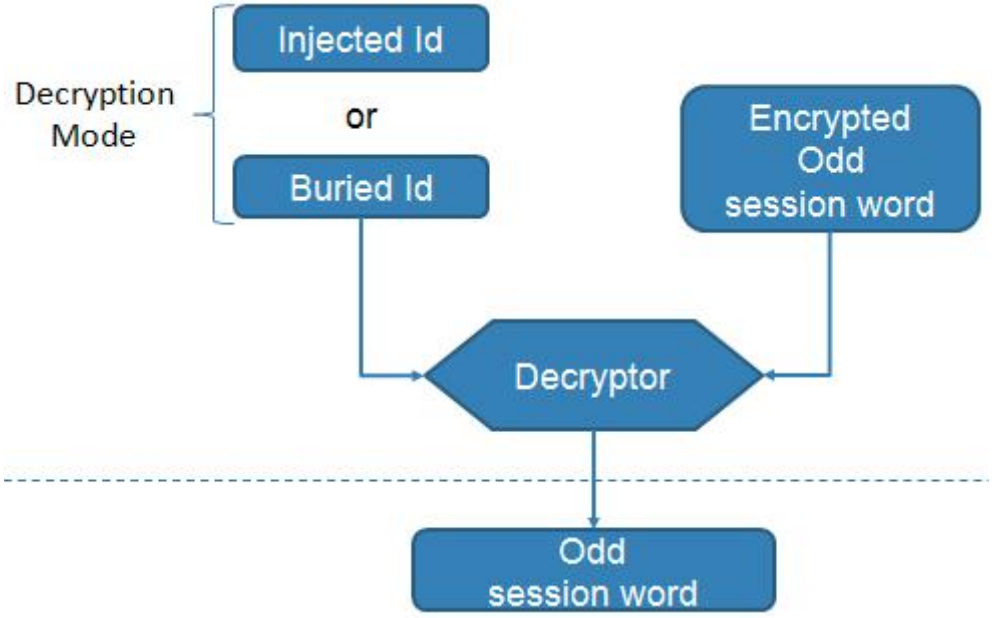
often creates a descrambling interruption on the receiver side. Changing the active session word on the scrambler side shall thus only be done if non-valuable content is being transmitted at that time. Otherwise, it is best to edit the inactive session word and then switch to it. The descrambler should automatically follow the changes, as described in the aforementioned procedure.

Changing the key parity on a scrambler will not interrupt the stream. It is thus a seamless operation, if the descrambler is properly configured on the receive side..

12.11.2.4 Distribution of Encrypted Session Words over a Non-Secure Channel

When the distribution of a session word cannot be performed over a secure channel it is advised to add extra protection to the clear session word.

Adding extra protection is done to avoid that non authorized parties have access to the clear session word and at the same time to the scrambled content.



The encryption key of the Session Word is called a device identifier. Two identifiers are defined in BISS:

- A group identifier (the Injected ID), common for several units. This identifier is secret and cannot be read by an operator. It is used when an organization has several devices part of the same network. The Injected ID is entered in all devices of the same network. The same Encrypted Session Word can then be used on all devices to protect a transmission. This Encrypted Session Word cannot be used on any other device that does not have this Injected ID.
- A buried identifier (the Buried ID), unique for each unit. This identifier can be read on the front panel. It is not fully secret. Its use is to protect a Session Word that has to be sent to that unit specifically. The operator will read the buried ID and communicate it to the Session Word owner, so that this person can send back the Encrypted Session Word. This Encrypted Session Word can only be used by that device.

Parameter	Description
Odd/Even Encrypted Session word	This setting allows the user to set the odd or even encrypted session word. An encrypted session word is computed by using the injected Id or buried Id and the clear session word. (To compute an Encrypted session word, we refer to section 8.10.2.5 on page 178) **Interface used** These encrypted session words can be entered by the user through any interface. (For example: Frontpanel, GUI, CLI, SNMP). It is not possible to read back the session words by any interface. **Hexadecimal** An encrypted session word exists out of 16 digits and is entered in hexadecimal format. For example, if the encrypted session word is 0xF76EE249BE01A286, enter it in the following sequence: • F,7,6,E,E,2,4,9,B,E,0,1,A,2,8 and 6.
Injected Id	The injected Id can be used to decrypt the encrypted session words. **Interface used** This Id can be entered by the user through any interface and is stored in the device. (For example: Frontpanel, GUI, CLI, SNMP). It is not possible to read back the injected Id by any interface. **Hexadecimal** The Injected Id exists out of 14 digits and is in hexadecimal format. **When to use an injected Id?** An injected Id can be entered (injected) on a single device or it can be entered on a group of devices.
Buried Id	The buried Id can be used to decrypt the encrypted session words. The buried Id is a fixed key that is unique per device. **Interface used** The buried Id is read only and can only be read by the expert user. It can be readout through any interface. (For example: Frontpanel, GUI, CLI, SNMP). **Hexadecimal** The buried Id exists out of 14 digits and is in hexadecimal format. **When to use a buried Id?** Use this Id to compute a device unique encrypted session word.
Encryption Mode	This parameter allows the user to select the way encrypted clear session words are decrypted. This can be done by using the buried Id or the injected Id. Setting this mode has no direct impact on the

Parameter	Description
	scrambled output. This because it is only used when entering a new encrypted session word.
Session Word Decryptor	The decrypter computes the clear session word from the injected or buried Id and the encrypted session word. The computed clear session word is used by the scrambler as the (real) clear session word.

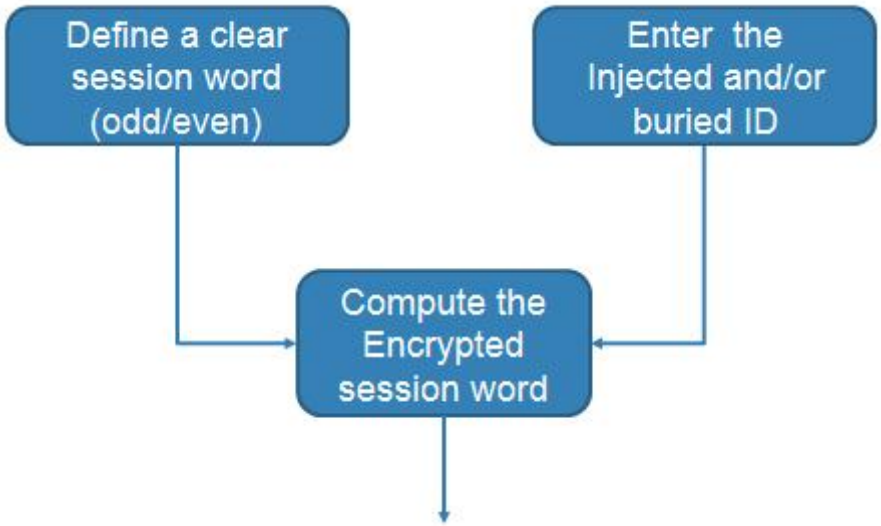
12.11.2.5 Compute Encrypted Session Words

Computing Encrypted Session Word before their distribution to devices shall be done off-line by an external tool.

The following figure shows how an encrypted session word is calculated.

Figure 94 – Compute an Encrypted Session Word

Newtec distributes:



Newtec distributes a simple web-based java script to compute encrypted session words for a specific device. Use the Newtec Service Desk tool to receive a copy:

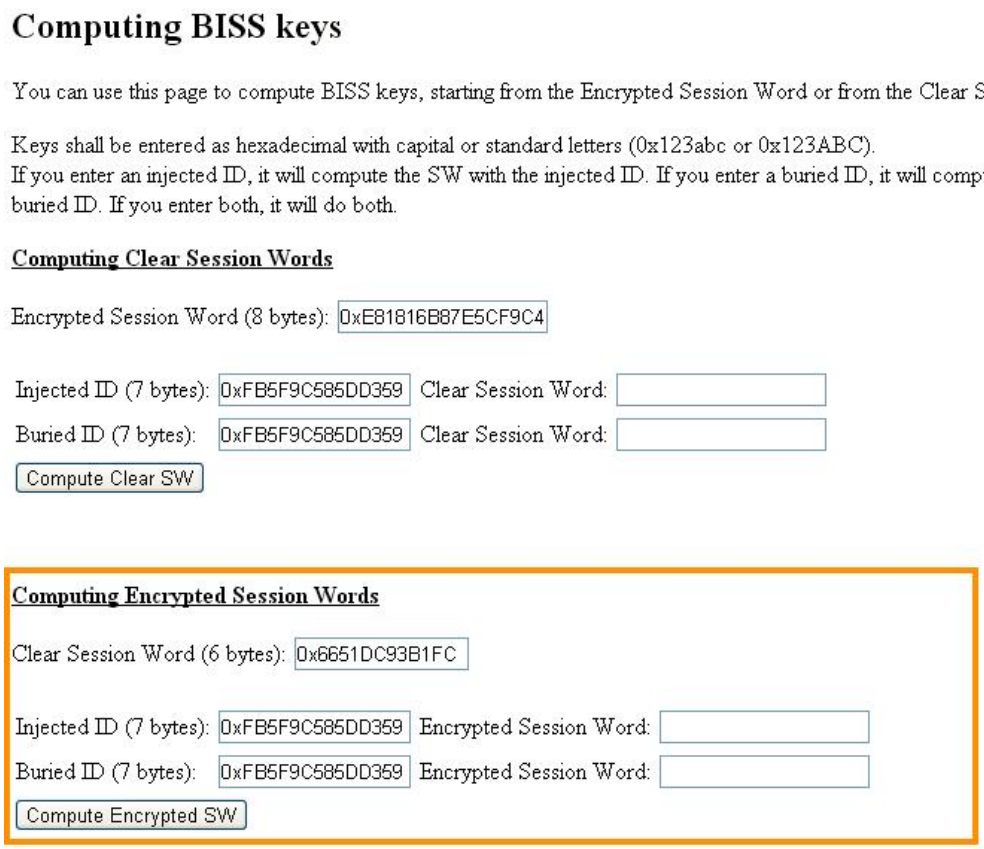
> Browse to **http://customersupport.newtec.eu .** > Fill in your Username and Password > Create a ticket

As response of your request you will receive the script from our support team.

In case you don't have a Username and Password yet for the Newtec Service Desk tool: request a login to **customersupport@newtec.eu.**

All session words or IDs used are in hexadecimal. For the algorithms, they are represented with the most significant byte (bit) first.

The following figure is an Excerpt of the web-based java script tool. .

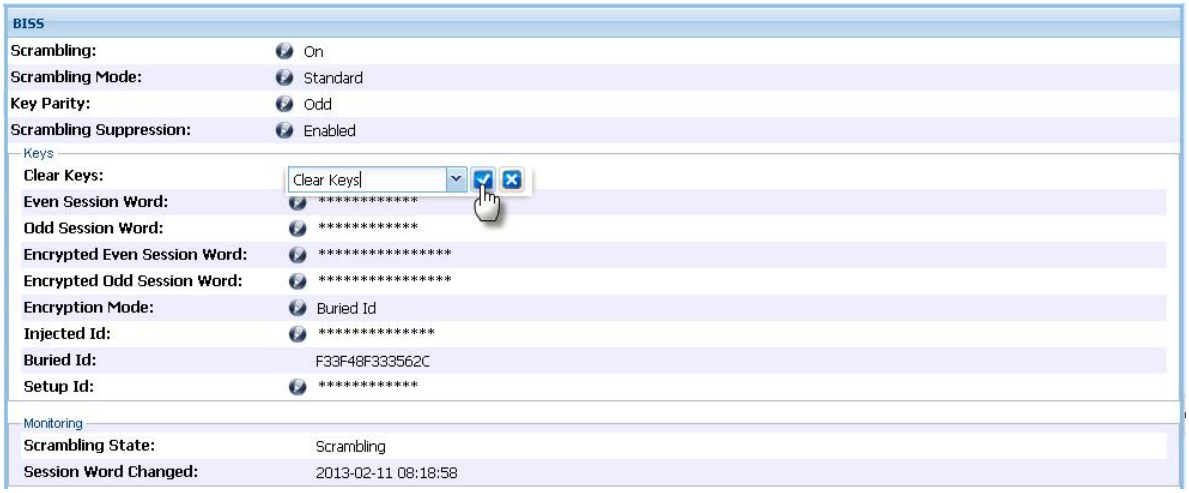


NOTE: To compute Clear Session Words from Encrypted Session Words, some bits are removed in the process. This means than when computing the reverse (from Clear Session Word to Encrypted Session Words, the system fills those added bits with a zero. So, if you decrypt an Encrypted Session Word, then re-encrypt it with the same ID, you may have a different result. The only way to be sure of the result is to decrypt again the Encrypted Session Word and check that the Clear Session Words are identical.

12.11.3 Deleting Keys

The command **Clear Keys** is implemented to reset the Injected Id and the Encrypted session words. The command writes the value 0 into these parameters.

For security reasons it is advised to enter new scrambling keys as soon as possible!



12.11.4 Seamless Key (Session Word) Change

The BISS key management system is designed to allow the change of a session word (odd/even) during a transmission without interrupting the stream. The scrambler adds information into the header to indicate whether the odd or even parity session word is used.

The demodulators/receivers can detect which key (odd or even key) is currently in use. When the modulator switches from one key to another, the demodulator/receiver automatically detects the change and switches to the other key in a synchronous way. This way, the demodulator always uses the proper session word to descramble the transport streams. No interruption or glitch appears at the output of the demodulator/receiver.

By changing the unused session word on the modulator, it is possible to switch again the key in the network.

12.11.5 Scrambling Monitoring Parameters

Here you get an overview of the current scrambling state and when the session word was last changed:

- **Scrambling State**: Continuously reads out whether the TS is scrambled or not. It is possible that scrambling is enabled but that due to PAT, PMT alarms and/or when a CA descriptor already exist, the scrambling is not allowed (in this case the parameter scrambling suppression is enabled). For more information on scrambling suppression refer to *Standard Mode. on page 192*
- **Session word Changed**: This parameter informs when the session word was changed for the last time. Each time a new session word is entered, the timestamp is written to this parameter. It helps the user to identify the user if the session word stored in the configuration is the right one or not.

12.11.6 Possible Alarms

Alarm	Description
BISS PAT Error	When the CRC of the PAT is not valid then this alarm is raised.
BISS PMT Error	BISS PMT Error
BISS CAT Error	When the CRC of the CAT is not valid then this alarm is raised.
BISS Program Already Scrambled	If a packet of a program to be scrambled is already scrambled (indicated by the scrambling bits), then this alarm is raised. The packet shall not be scrambled in that case, but scrambling continues for other packets.
BISS CA-Descriptor found on Input	If a PMT already contains a CA descriptor then this alarm is raised.
BISS Scrambling Error	This alarm is raised due to errors happening in the scrambling core (FPGA).

12.11.7 Operation of BISS

12.11.7.1 Setting a Key for Transmission

Starting point: the scrambler sends clear data to the descrambler. Both have their scrambling mode set to “Standard”, but scrambling is disabled.

Steps:

- The Session Word is entered in the descrambler (odd key);
- Enable scrambling on the descrambler;
- The Session Word is entered in the scrambler (odd key);
- Enable Scrambling on the scrambler (select ON).

12.11.7.2 Setting an Encrypted Session Word for Transmission

Starting Point: Scrambling is not enabled. Clear TS is send towards the receiver.

Steps:

If Injected ID is used:

  - Enter the Injected Id in the device, if it is not yet done (normally, the injected ID shall be defined earlier)

- Select the encryption mode of your choice:
  - Injected Id
  - Buried Id
- Enter the encrypted odd session word in the decryptor.
  - The odd session word is computed by the decryptor and available for use.

- Select the scrambling Mode (could be done at any step before):
  - Standard
  - Raw
- Enable Scrambling (select **ON**)
- The scrambler uses the odd session word.

12.11.7.3 Changing Keys Seamlessly

Starting Point: Scrambling is enabled and sends scrambled transport streams to the receiver. The odd session word is active.

Steps:

- Enter the encrypted even session word in the decrypt or;
- The even session word is computed by the decryptor and available for use;
- Set the key parity to even;
- The scrambler uses the even session word (this is indicated in the header of the TS packets, this to inform the receiver of the switchover).

12.11.7.4 Removing a Receiver from the Network

Starting point: the scrambler sends scrambled data to the descramblers. The odd key is active. All have their scrambling mode set to “Scramble/descramble” mode.

Steps:

1. Define a new Session Word;

2. The Session Word is entered in the descramblers (even key), except the one removed from the network;

3. The Session Word is entered in the scrambler (even key);

4. The scrambler is asked to switch to the even key.

12.11.7.5 Setting up a Secure BISS Network

Starting point: A scrambler and a set of descramblers in a secured facility (or in secured facilities).

Steps:

1. Define an Injected ID;

2. Insert the Injected ID in all devices by a trusted person/system;

3. Deploy the devices;

4. Sets the key for a transmission, sending Encrypted Session Words rather than Session Words.

12.11.7.6 Creating Groups of Receivers

Groups of receivers, mutually exclusive, are created by inserting different Injected IDs in those receivers and in the related sender. This way, another group of receivers cannot use Encrypted Session Words sent to a group of receivers.

12.11.8 Keys and Redundancy, Backup or Import

A solution based on BISS should combine security, but also guarantee operations. BISS Session Words cannot be copied from one device to another or exported, except in some cases:

• Redundancy;

• Export of a configuration for backup purposes;

• Import of a configuration pre-generated.

12.11.8.1 BISS and Redundancy

The BISS implementation allows copying a session word during a redundancy switch.

To ensure the security of the key, a Setup Identifier is used. A **Setup Identifier** is the equivalent of the Injected ID: it is used to encrypt session words when copied from one device to another, using the Newtec AZ202 switch.

The setup ID is typically the same for all devices in a redundancy bank. It is recommended that this setup ID is unique for each redundancy setup.

Setup IDs all have the same default value, so that redundancy always works for devices coming from factory.
In that case, the session word is not secured, as it can be copied to any other device during a switch. It is thus recommended to define the setup ID when deploying a redundant setup using BISS.

12.11.8.2 Backup a Configuration

It is possible to export and import device configurations. The Session Word is exported in an encrypted manner, as well as the Injected ID, so that they can be recovered after an import on the SAME device. If this configuration is imported on another device, the Injected ID will be ignored.

If this configuration is imported on a device with the same Setup ID, the Session Word will however be loaded.

The default value of the setupID is the same for all devices. By default, exporting and importing a configuration on another device will allow the copy of the BISS SW. To avoid that, define the setup ID to a secret value.

An alternative is to set the setup ID of the device to zero. This will allow backup of configuration, but will prevent the import of that configuration on any other device. The keys are then fully protected.

12.11.8.3 Import a Configuration

- It is possible to edit an exported configuration file and define a new Session Word or a new Injected ID in this file. When the changes are done, import the new configuration file into the device(s).

12.11.8.4 Erasing the setupID

To erase the setup ID, it is possible to enter a zero value. This will result in the fact that a unique setup ID is generated for that device. It will prevent copying any BISS key from that device to another device. Backup of configuration on the same device is still possible through import/export of configuration.

Trying to copy a config to or from a device with a setup ID equal to 0 will result in an error, unless it is the same device.

Should the device be used in a redundancy setup, a new setup ID has to be entered.Should users want to go back to the situation out of factory where BISS keys can be copied between devices, it is necessary to perform a config reset. Config reset can be done via the GUI when going to the TAB Device/Configurations. All config parameters are lost, but the device will behave again as out of factory.

12.12 Device Redundancy

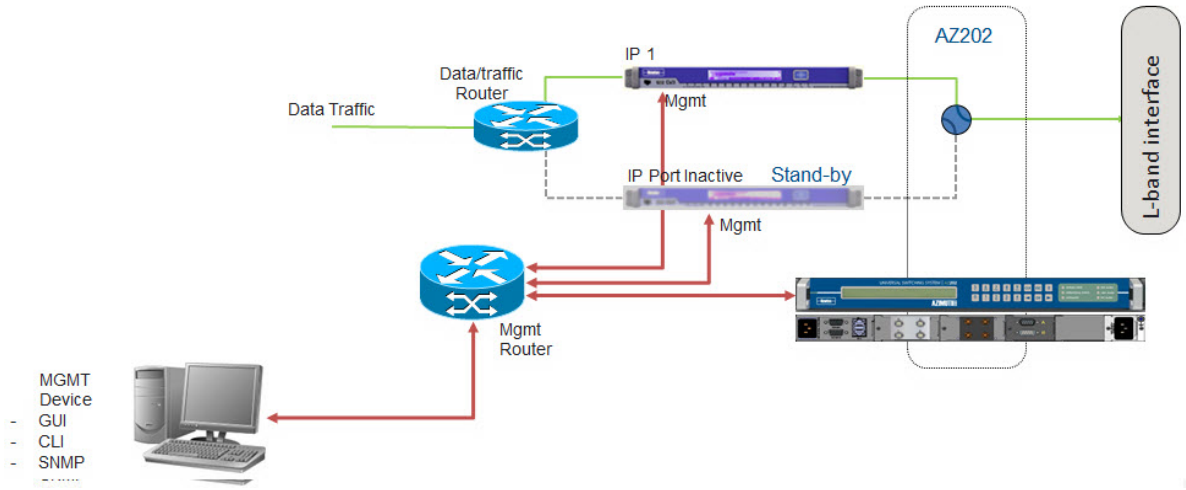
Redundancy is very important as a single failure of the M6100 affects many services at the same time.

Reliable operation of the M6100 in a satellite network is of key importance. The M6100 works seamlessly together with the Newtec AZ202/AZ212 redundancy switches to provide best-in-class system uptime.

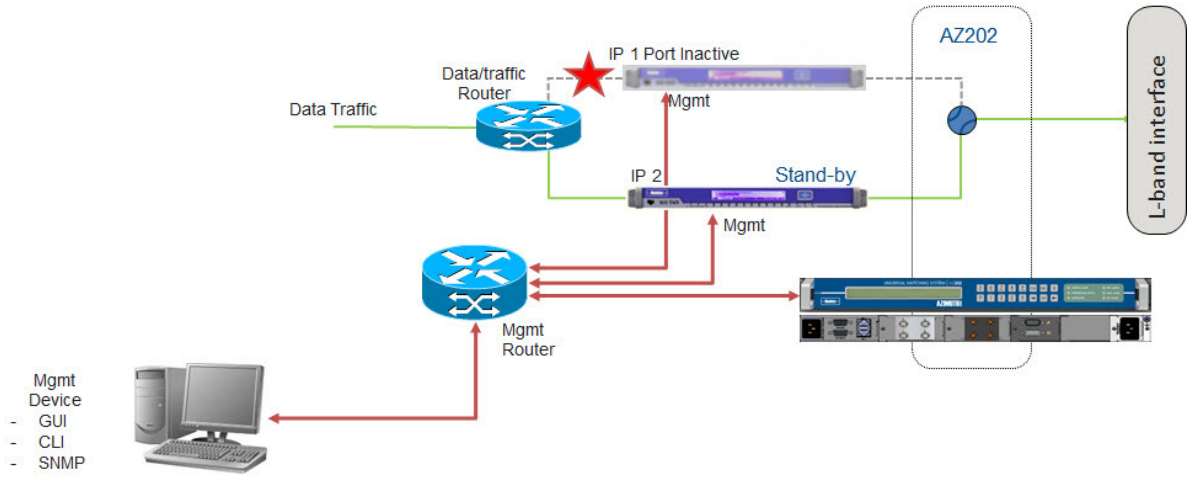
Refer to the user manual of the AZ202/AZ212 Universal Switching System.

The following figures shows a 1+1 protection scheme built up with the AZ202 switch, one in normal operation and one in redundant operation.

Normal Operation



Redundant Operation



To Enable or Disable device redundancy go to the following location:

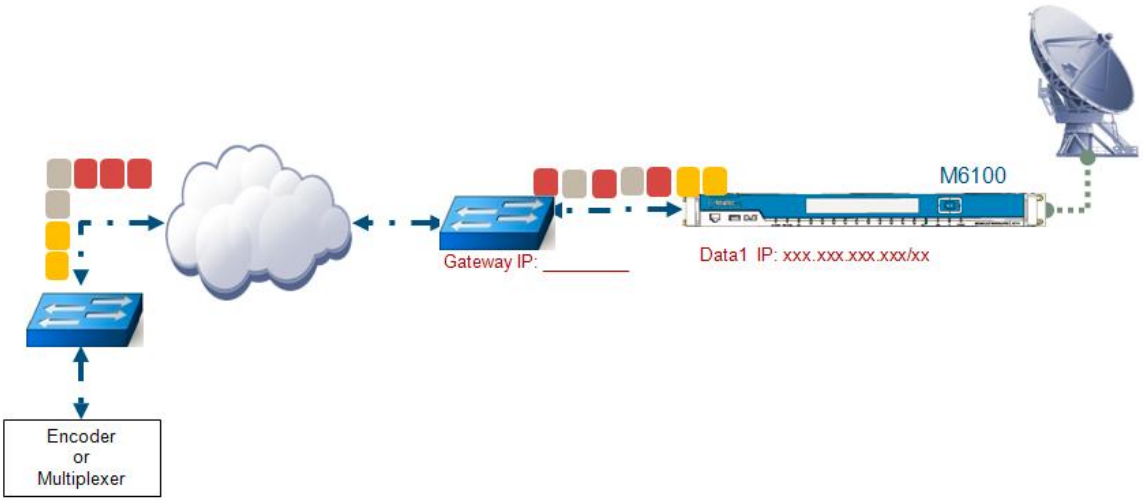
M6100 >> Device >> Redundancy

By default, device redundancy is disabled.

Initial Redundancy State:

- Standby (default value): This means when the device starts up and redundancy is enabled, the initial state of the redundancy is standby. Typically:
  - The modulator output is disabled;
  - No IP Address on the data interface.
- Active.

13 Use Case: TS over IP Constant Bit Rate



In this use case, the modulator is connected to a video encoding system that generates a TS over IP. To combat RFI we want to insert a Network ID into the TS. This TS is modulated in DVBS -2 QPSK and transmitted over satellite to set-top boxes in a DTH (Direct-To-Home) network.

The previous figure is an example of such a setup.

The main settings of the video encoding baseband system are:

• Traffic Profile = CBR;

• TS Encapsulation Protocol = UDP;

• TS Bit Rate = 13.5Mbps;

• RTP FEC;

• Destination IP Address.

In this use case, we presume that the management interface configuration is already done. The user is able to manage the device using the GUI.

13.1 Configure the Data Interfaces

- Log in as **Expert user**.
- **Enable** the Ethernet connectivity of the device.
- Configure the correct IP Addresses for the Data interface so that the M6100 is reachable for the encoder/multiplexer.

13.2 Configure the TS over IP Input

M6100> TS over IP

Set the parameters in this block according to the settings of the head-end encoder or multiplexer.

- Click on the **TS over IP functional block** (when in the GUI) and do the following:
- **Enable** this functional block (meaning that traffic must be taken in on TS over IP);
- Define the **Input selection**, (on what data interface the TS is taken in);
- The following parameters must be set according to the input of the head-end encoder/multiplexer;
- TS Ecapsulation Protocol = UDP;
- **IP Address Type** = Unicast:
- Configure the **UDP port** on which the TS over IP stream is received;
- Set the **Traffic Profile = CBR;**
- Define the **Input TS Bit Rate.**

When the inserted bit rate is too high/low the following alarm is generated:
TS over IP Invalid TS Bit Rate.

13.3 Configure the TS MUX

In this functional block, configure the NIT Carrier ID Information.

M6100> TS MUX >> NIT Carrier ID

- Enable **Carrier ID** and insert the appropriate carrier ID information.

This information is inserted into the NIT of the TS.

In case the incoming TS does not contain a NIT nor any null packets the NIT is not inserted automatically (because there is no room to store the NIT). Make sure that enough null packets are available in the TS to insert the NIT. (For example by enabling the rate adapter and setting the bit rate higher than the incoming CBR.).

13.4 Configure the Modulator

M6100>Modulator

» Modulation **Mode**: DVB-S2;

» **Output Frequency**: Set the output frequency according to the transmission plan. (L-band or IF-band, depending on the device capabilities);

» **Roll Off Factor;**

» **Occupied bandwidth**: a monitoring parameter that shows the occupied bandwidth [symbol rate x (1+α) with α: 0.20, 0.25 or 0.35];

» **Spectrum Inversion**: select between direct and inverted. Spectrum inversion can be applied in the modulator in case an external RF block up converter inverts the spectrum. In that case, the spectrum is not inverted on the satellite as specified by the satellite operator;

» **Output Level**: Set the output level according to the network requirements;

» **Clock Output**: Define if a 10MHz clock reference needs to be inserted, for example to synchronize the BUC;

» **Carrier Modulation**: When set to on, a modulated carrier is transmitted. (Use pure carrier to transmit an unmodulated (clean carrier or CW) carrier.);

» **Slope equalizer**: to compensate for cable slope.

Transmit Control

Define the impact of a General Device Alarm and a General Interface Alarm on the transmission of the signal.

DVB-S2 Settings

» **Frame Type**: Define normal or short frames;

» **ModCod**: QPSK select the used modulation and coding (FEC) according to the transmission plan;

» **Pilots**: Insert pilots to increase the reliability of the receiver synchronization;

» **Rate Priority**: Set the required priority;

» Enter the correct **Bit Rate** or **Symbol Rate**; Note: The symbol rate can be slaved on the input TS bit rate (CBR).

DVB-S2 Carrier Identification

» Enable: On (The Global Unique ID is transmitted along with the carrier.);

» Enable: Use Geo Coordinates and enter the corresponding coordinates;

» Enter a telephone number and additional user data. (All this information makes it easier for the satellite operator to contact you in case of interference.).

14 Appendix A - Alarm List

The alarm list provides an overview of the different alarms that can occur on the device.
The description of the alarm indicates where the alarm is situated and how the problem can be solved.

Most alarms are related to one of the functional blocks that exist in the device.
A few alarms can be an aggregation of different sub alarms.
This means that one of the sub alarms must exist before the overall alarm is displayed. When debugging this overall alarm it is necessary to check the sub alarms as this can exist out of more than one sub alarm.

14.1 Generic Alarms

Alarm	Description
Temperature	This alarm is raised when the monitored temperature exceeds 85 °C.
General Device	This alarm can be triggered by one of the following alarms: • Modulator DAC Failure; • Modulator No Calibration Data; • Invalid License; • Boot Config Failure; • Temperature; • Modulator Ref synthesizer failure alarm; • Modulator LO-1 synthesizer failure alarm; • Modulator LO-2 synthesizer failure alarm.
General Interface	This alarm is raised when an error is reported on an interface that is used in the data path. This alarm can be triggered by one of the following alarms: • Ethernet interface alarm. • Ref Clock No Signal; • S2 EXT Demodulator No Lock; • S2 EXT Demodulator Incompatible Baseband Frame; • DVB Demodulator No Lock.
Invalid License	This alarm is raised when the license file is not available or wrongly signed.
Boot Config Failure	This alarm is raised when an erroneous boot configuration was attempted to load and failed. Check the boot configuration file stored on the device.
Frontpanel Internal Failure	This alarm is raised when the front panel communication failed.

14.2 Ethernet Interface Alarms

Alarm	Description
Eth Data Link Failure	This alarm is raised when there is no signal on the corresponding Ethernet interface.
Eth Data Itf Failure	This alarm is raised when a failure is detected on the Ethernet interface.
Eth Mgmt Link Failure	This alarm is raised when there is no signal on the corresponding Ethernet interface.
Eth Mgmt Itf Failure	This alarm is raised when a failure is detected on the Ethernet interface.
Eth Mgmt Fp Link Failure	This alarm is raised when there is no signal on the corresponding Ethernet interface. (Front Panel)
Eth Data Half Duplex	This alarm is raised when an Ethernet interface is in half duplex mode as a result of a link negotiation. The alarm is not raised when the Ethernet interface was forced in half duplex mode by configuration on the device.

14.3 TS over IP Alarms

Alarm	Description
TS over IP General	This alarm is raised when there is a general TS over IP input alarm.
TS over IP No Input Data	This alarm is raised when no input data is received for the TS over IP functionality.
TS over IP Buffer Overflow	This alarm is raised when the input data buffer of TS over IP is full.
TS over IP Buffer Underflow	This alarm is raised when the input data buffer is below the minimum value.
TS over IP RTP No Sync	This alarm is raised when no valid RTP input data is received.
TS over IP Invalid TS Bit Rate	This alarm is raised when the measured input TS bit rate is higher/lower than the configured value. (only relevant for a CBR Traffic profile)

14.4 ASI Alarms

Alarm	Description
ASI IN General	This alarm is raised when there is a general ASI input alarm. • ASI IN No Input Signal; • ASI IN No Input Data; • ASI IN Buffer Overflow; • ASI IN Invalid TS Bit Rate.
ASI IN No Input Signal	This alarm is raised when no input signal is detected at the selected ASI input.
ASI IN Invalid TS Bit Rate	This alarm is raised when the measured input Transport-Stream (TS) bit rate is higher or lower than the expected value.
ASI IN No Input Signal ASI	This alarm is raised when no input signal is detected at the corresponding ASI input.
ASI IN No Input Data	This alarm is raised when no input data is detected at the selected ASI input.
ASI IN Buffer Overflow	This alarm is raised when the input data buffer is full.

14.5 Transport Stream Analyzer Alarms

Alarm	Description
TS 1_1 TS_sync_loss	Alarm indicating that the synchronization with the Transport-Stream (TS) has been lost. This condition occurs: When two or more consecutive corrupted SYNC bytes are received.
TS 1_2 Sync_byte_error	This alarm is raised when a single corrupted SYNC byte is detected. The alarm is cleared when the next correct SYNC byte appears.
TS 1_3 Pat_error	This alarm indicates that the 'Program Association Table' (PAT) cannot be detected properly in the stream. The PAT table id (0x00) should be detected in a PID 0x0000 at least every 0.5 s.
TS 1_4 Continuity_count_error	This alarm is raised when packets arrive out of sequence, get dropped or occur more than once.
TS 2_1 Transport_error	This alarm condition is detected when the 'Transport Error indicator'-bit in the TS-Header is set to '1' for a specific PID. The alarm condition is cleared when no Transport Error indication is detected for 5 s.
TS 2_3a PCR_repetition_error	This alarm is raised if the spacing between two consecutive PCR values is more than 40msec. The condition can occur When PCR packets get lost or when PCR packets are not present at a sufficient rate.

14.6 TS MUX Alarms

Alarms	Description
TS MUX Local PID on Input	This alarm is raised when a local generated packet is using a PID, which already is available on the input of the device. In case of error no data encapsulation will be supported.
TS MUX Signalling Processing Error	This alarm is raised when a local generated table is using a program number, which is already in use by the MPEG stream. In an error case no data encapsulation will be supported.

14.7 BISS Alarms

Alarms	Description
BISS PAT Error	This alarm is raised when the CRC of the PAT is not valid.
BISS PMT Error	This alarm is raised when the CRC of the PMT is not valid.
BISS CAT Error	This alarm is raised when the CRC of the CAT is not valid.
BISS Already Scrambled	This alarm is raised when a packet of a program is already scrambled
ISS CA Descriptor Found On Input	This alarm is raised when a CA descriptor is found on input.
BISS Scrambling Error	This alarm is raised when errors are happening in the scrambling core.
BISS SW Refused Error	This alarm is raised when the session words are changing too rapidly while scrambling is active.
BISS General	This alarm is raised when there is a general Biss error.

15 Appendix B - Overview of the Used Technologies

15.1 DVB-S2

Newtec M6100 delivers the best and most robust DVB-S2 performance in the market.

Refer to the DVB-S2 standard: ETSI EN 302 307.

The following table shows the Supported MODCODs and FEC:

QPSK 1/4	8PSK 3/5	16APSK 2/3	32APSK 3/4
QPSK 1/3	8PSK 2/3	16APSK 3/4	32APSK 4/5
QPSK 2/5	8PSK 3/4	16APSK 4/5	32APSK 5/6
QPSK 1/2	8PSK 5/6	16APSK 5/6	32APSK 8/9
QPSK 3/5	8PSK 8/9	16APSK 8/9	32APSK 9/10
QPSK 2/3	8PSK 9/10	16APSK 9/10	
QPSK 3/4			
QPSK 4/5			
QPSK 5/6			
QPSK 8/9			
QPSK 9/10			

15.2 S2 Extensions

Newtec also introduces a new modulation technology that outperforms the existing DVB-S2 standard. This new technology is called S2 Extensions and when combined with CCT it delivers gains up to 37% compared to standard DVB-S2 modulation.

The main features of the new technology are:

- Finer MODCOD granularity: there are 87 MODCODs (compared to the 28 MODCODs in DVB-S2);
- Better MODCOD performance: FEC codes and modulations have been redesigned in order to improve the performance of the existing DVB-S2 MODCODs;
- Optimization for linear and non-linear satellite links: Two sets of MODCODs are available:

– One set of ModCods is optimized for multi-carrier operation of the transponder (linear channel operation). In multi-carrier operation, the transponder can not be saturated and a given back-off is needed to avoid intermodulation between the individual carriers in the transponder.

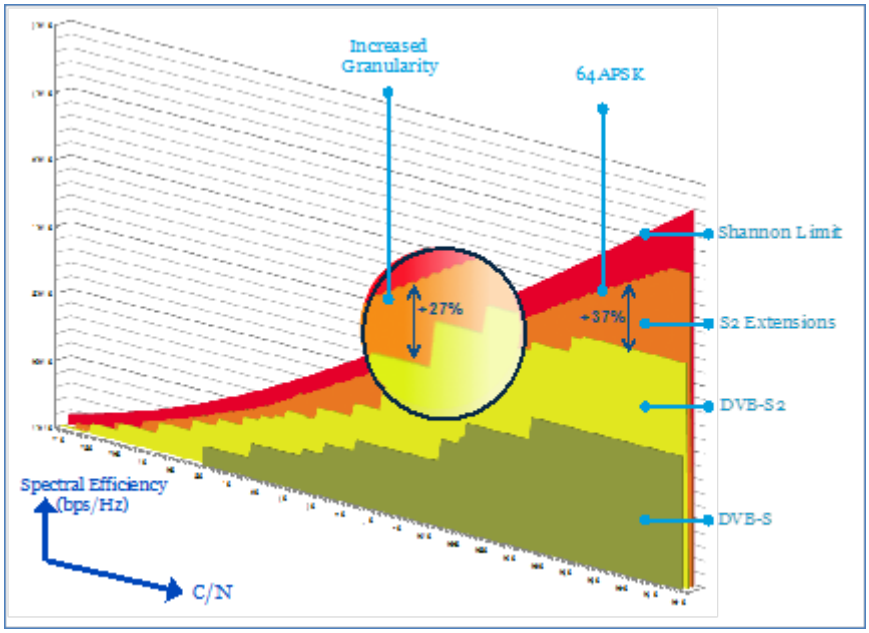
– The second set of ModCods is optimized for single carrier operation which allows to saturated the transponder (non-linear channel).

15.2.1 Performance of S2 Extensions

Newtec's implementation of the S2 Extensions increases the modulation and coding schemes and Forward Error Correction (FEC) choices (compared to DVB-S2), which then can provide the highest resolution for optimal modulation in all circumstances. The current DVB-S2 quantization steps are quite far apart. By adding granularity in the upcoming standard the service provider can further optimize the satellite link depending on the application. In combination with Adaptive Coding and Modulation (ACM), where the highest MODCOD is selected automatically, full efficiency can be gained. The amount of MODCODs has grown from 28 in DVB-S2 up to 87 in the S2 Extensions bringing efficiency as close to the theoretical Shannon limit as possible.

Adding higher modulation schemes such as 64APSK proves to be useful considering the professional applications that work with improved link budgets provided by more powerful satellites that become available. Newtec sees the 32APSK boundary being reached frequently with FlexACM during clear weather conditions. In these situations 64APSK is highly beneficial.

When combining the increased granularity (MODCODs and FECs) and 64 APSK (higher order modulation and coding) immediate efficiency gains up to 37% can be achieved compared to DVB-S2. The following figure shows the performance of S2 extensions compared to DVB-S and DVB-S2.



15.2.2 MODCOD Definitions S2 Extensions

S2 Extensions comprises 87 MODCODs, optimized for linear and non-linear channels. Although the MODCODs might use the same code/name as in DVB-S2, they are not interchangeable.

For linear channel applications, Newtec Cy N.V. has developed specific modulation schemes (constellation mappings).

The modulation schemes designed for linear channels are indicated with L.

For example: 16APSK-L 162/180

• QPSK 45/180 • QPSK 60/180 • QPSK 72/180 • QPSK 80/180 • QPSK 90/180 • QPSK 100/180 • QPSK 108/180 • QPSK 114/180 • QPSK 120/180 • QPSK 126/180 • QPSK 135/180 • QPSK 144/180 • QPSK 150/180 • QPSK 160/180 • QPSK 162/180	• 8PSK 80/180 • 8PSK 90/180 • 8PSK 100/180 • 8PSK 108/180 • 8PSK 114/180 • 8PSK 120/180 • 8PSK 126/180 • 8PSK 135/180 • 8PSK 144/180 • 8PSK 150/180
• 16APSK 80/180 • 16APSK 90/180 • 16APSK 100/180 • 16APSK 108/180 • 16APSK 114/180 • 16APSK 120/180 • 16APSK 126/180 • 16APSK 135/180 • 16APSK 144/180 • 16APSK 150/180 • 16APSK 160/180	• 32APSK 100/180 • 32APSK 108/180 • 32APSK 114/180 • 32APSK 120/180 • 32APSK 126/180 • 32APSK 135/180 • 32APSK 144/180 • 32APSK 150/180 • 32APSK 160/180 • 32APSK 162/180

• 16APSK 162/180	
• 64APSK 90/180 • 64APSK 100/180 • 64APSK 108/180 • 64APSK 114/180 • 64APSK 120/180 • 64APSK 126/180 • 64APSK 135/180 • 64APSK 144/180 • 64APSK 150/180 • 64APSK 160/180 • 64APSK 162/180	• 8PSK-L 80/180 • 8PSK-L 90/180 • 8PSK-L 100/180 • 8PSK-L 108/180 • 8PSK-L 114/180 • 8PSK-L 120/180
• 16APSK-L 80/180 • 16APSK-L 90/180 • 16APSK-L 100/180 • 16APSK-L 108/180 • 16APSK-L 114/180 • 16APSK-L 120/180 • 16APSK-L 126/180 • 16APSK-L 135/180 • 16APSK-L 144/180 • 16APSK-L 150/180 • 16APSK-L 160/180 • 16APSK-L 162/180	• 64APSK-L 90/180 • 64APSK-L 100/180 • 64APSK-L 108/180 • 64APSK-L 114/180 • 64APSK-L 120/180 • 64APSK-L 126/180 • 64APSK-L 135/180 • 64APSK-L 144/180 • 64APSK-L 150/180 • 64APSK-L 160/180 • 64APSK-L 162/180

When operating in saturated single-carrier per transponder mode, Newtec recommends to use the MODCODs QPSK, 8PSK, 16APSK, 32APSK and 64APSK.

When operating in a multi-carrier per transponder mode, the optimal MODCODs are QPSK, 8PSK-L, 16APSK-L, 32APSK and 64APSK-L.

16 Appendix C - Classification Expressions

Filter all incoming packets based on expressions that match any field of an incoming packet:

- IP addresses, TOS byte, protocol, etc.

Expressions can be ANDed (&&), ORed (||), negated (!), brackets can be used to group different expressions.

expression=expression and expression	expression=(expression)
expression=expression && expression	expression=protocol
expression=expression or expression	expression=field value
expression=expression || expression	expression=protocol field value
expression=not expression	expression=always expression=never
expression=!expression	
IPv4	**UDP**
ip4 tos <tos>	udp src port <port>
ip4 dscp <dscp>	udp src port <port>-<port>
ip4 protocol <protocol>	udp dst port <port>
ip4 src host <ip4address>	udp dst port <port>-<port>
ip4 src net <ip4address>-<ip4address>	udp rtp-detection <rtpdetect>
ip4 src net <ip4address> mask	udplite src port <port>
<ip4netmask>	udplite src port <port>-<port>
ip4 src net <ip4address>/<ip4bits>	udplite dst port <port>
ip4 dst host <ip4address>	udplite dst port <port>-<port>
ip4 dst net <ip4address>-<ip4address>	udplite rtp-detection <rtpdetect>
ip4 dst net <ip4address> mask	**TCP**
<ip4netmask>	tcp src port <port>
ip4 dst net <ip4address>/<ip4bits>	tcp src port <port>-<port>
ip4 unicast	tcp dst port <port>
ip4 multicast	tcp dst port <port>-<port>
ip4 broadcast	
ip4 ah	**ICMP4**
ip4 esp	icmp4 type <icmp4type>
IGMP	icmp4 code <icmp4code>
igmp type <igmptype>	
igmp host <ip4address>	
igmp net <ip4address>-<ip4address>	
igmp net <ip4address> mask	
<ip4netmask>	
igmp net <ip4address>/<ip4bits>	

17 Appendix D - Acronyms

Acronym	Definition
ACM	Adaptive Coding Modulation
APSK	Amplitude and Phase Shift Keying
ASI	Asynchronous Serial Interface
BCH	Chaudhuri and Hocquengham
BER	Bit Error Rate/Ratio
BISS	Basic Interoperable Scrambling System
BNC	Bayonet (Neill Concelman) Connector (for coaxial cable)
BUC	Block Up Converter
CBR	Constant Bit Rate
CCITT	Comite Consultatif International Télégraphique et Téléphonique (known today as the ITU-T)
CCM	Constant Coding and Modulation
CD	Compact Disc (digital audio recordings)
CD-ROM	Compact Disc Read Only Memory (in computer systems)
CEC	Canadian Electrical Code
CIR	Committed Information Rate
CLI	Command Line Interface
CPU	Central Processing Unit
CTRL	Control
DSNG	Digital Satellite News Gathering
DTH	Direct to Home
DVB-S	Digital Video Broadcasting-Satellite

EMC	ElectroMagnetic Compatibility
ETH	Ethernet
ETSI	European Telecommunication Standards Institute
FCC	Federal Communications Commission
FEC	Forward Error Correction (in data transmission systems)
FTP	File Transfer Protocol (computer networks & systems)
GND	Ground (connection in equipment or circuits)
GPS	Global Positioning System
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
ID	Identifier
IEC	International Electrotechnical Commission
IF	Intermediate Frequency
IP	Internet Protocol
IRD	Integrated Receiver Decoder
LCD	Liquid Crystal Display
LDPC	Low-density Parity-check code
LED	Light Emitting Diode
LNB	Low Noise Block Converter
MAC	Medium Access Control
MHP	Multimedia Home Platform
MIB	Management Information Base
ModCod	Modulation and Coding
MPE	Multiprotocol Encapsulation

MPEG	Motion Picture Experts Group
MPTS	Multiple Program Transport Stream
MTU	Maximum Transmission Unit
MUX	Multiplex communications transmissions
NEC	National Electrical Code
NIT	Network Information Table
NMS	Network Management System
NTP	Network Time Protocol
PAT	(MPEG2) Programme Association Table
PC	Personal Computer
PCR	Program Clock Reference
PER	Packet Error Rate
PID	Packet Identification
PIR	Peak Information Rate
PMT	(MPEG 2) Program Map Table
PRBS	Pseudo Random Binary Sequence
QPSK	Quadrature Phase Shift Keying
REACH	Evaluation and Authorization of Chemicals
RF	Radio Frequency
RFI	Radio Frequency Interference
RH	Restriction of Hazardous
RS	Reed Solomon
RTP	Real-time Transmission Protocol
SDT	Service Description Table

SFN	Single Frequency Network
SMA	SubMiniature version A
SMPTE	Society of Motion Picture & Television Engineers
SNMP	Simple Network Management Protocol
SPTS	Single Program Transport Stream
SSH	Secure Shell
SVHC	Substances of Very High Concern
TS	Transport Stream
UDP	User Datagram Protocol
UL	Underwriters Laboratory
UTC	Universal Coordinated Time (replaced GMT)
VA	Volt-Ampere
VBR	Variable Bit Rate
XML	Extensible Markup Language

Get More Out of Your Equipment

The understanding of your application in combination with our product leads to reliable and cost-efficient solutions.

Visit: *www.newtec.eu/applications* for our full application range.

Feedback on this document?

Please provide any comment, error found or suggestion for improvement, you may have about this document to

documentation@newtec.eu

Twitter.com/Newtec_Satcom

Linkedin.com/company/newtec

Youtube.com/NewtecSatcom

Slideshare.net/newtec_satcom

Visit our website: www.newtec.eu