an EnerSys® company

ALPHA OUTBACK ENERGY

Alpha® DM3.1 Transponder for XM3-HP™ Power Supply Status Monitoring Technical Manual

Effective: April 2024

Safety Notes

Review the drawings and illustrations contained in this document before proceeding. If there are any questions regarding the safe installation or operation of the system, contact Alpha Technologies Services, Inc. or the nearest Alpha® product sales representative. Save this document for future reference.

To reduce the risk of injury or death and to ensure the continued safe operation of this product, the following symbols have been placed throughout this manual. Where these symbols appear, use extra care and attention.

WARNING! GENERAL HAZARD

GENERAL HAZARD WARNING provides safety information to PREVENT INJURY OR DEATH to the technician or user.

WARNING! ELECTRICAL HAZARD

ELECTRICAL HAZARD WARNING provides electrical safety information to PREVENT INJURY OR DEATH to the technician or user.

WARNING! FUMES HAZARD

FUMES HAZARD WARNING provides fumes safety information to PREVENT INJURY OR DEATH to the technician or user.

WARNING! FIRE HAZARD

FIRE HAZARD WARNING provides flammability safety information to PREVENT INJURY OR DEATH to the technician or user.

There may be multiple warnings associated with the call out. Example:

WARNING! ELECTRICAL & FIRE HAZARD

This WARNING provides safety information for both Electrical AND Fire Hazards

CAUTION!

CAUTION provides safety information intended to PREVENT DAMAGE to material or equipment.

NOTICE:

NOTICE provides additional information to help complete a specific task or procedure.

ATTENTION:

ATTENTION provides specific regulatory/code requirements that may affect the placement of equipment and /or installation procedures.

Alpha® DM31 Transponder for XM3-HP™ Power Supply Status Monitoring

Technical Manual

017-891-B14-001, Rev. A

Effective Date: April 2024

Disclaimer

Images contained in this manual are for illustrative purposes only. These images may not match your installation.

Operator is cautioned to review the drawings and illustrations contained in this manual before proceeding. If there are questions regarding the safe operation of this powering system, please contact Alpha Technologies Services, Inc. or your nearest Alpha® product sales representative.

Alpha shall not be held liable for any damage or injury involving its enclosures, power supplies, generators, batteries or other hardware if used or operated in any manner or subject to any condition not consistent with its intended purpose or is installed or operated in an unapproved manner or improperly maintained.

Worldwide Corporate Offices

Headquarter Germany
Hansastrasse 8
D-91126 Schwabach
Tel: +49 9122 79889 0
Fax: +49 9122 79889 21
Mail: info@alpha-outback-energy.com

Eastern Europe
ee@alpha-outback-energy.com

Middle East
me@alpha-outback-energy.com

France and Benelux
fbnl@alpha-outback-energy.com

Spain
spain@alpha-outback-energy.com

Africa
africa@alpha-outback-energy.com

For more information please visit **www.alpha-outback-energy.com**

Table of Contents

Table of Contents

Figures

Tables

1.0 Introduction

The Alpha® DM31 transponder is an embedded DOCSIS® 3.1 transponder that allows monitoring of Alpha® XM3-HP™ series power supplies through existing cable network infrastructure. Advanced networking services provide quick reporting and access to critical powering information.

The DM31 transponder utilizes Simple Network Management Protocol (SNMP) and Management Information Bases (MIBs) to provide status monitoring and diagnostics. A web interface enables authorized personnel direct access to advanced diagnostics using a common web browser. No custom software is required.

This manual should be used in conjunction with the Alpha® XM3-HP™ Power Supply Technical Manual *(p/n 017-882-B0-001)*.

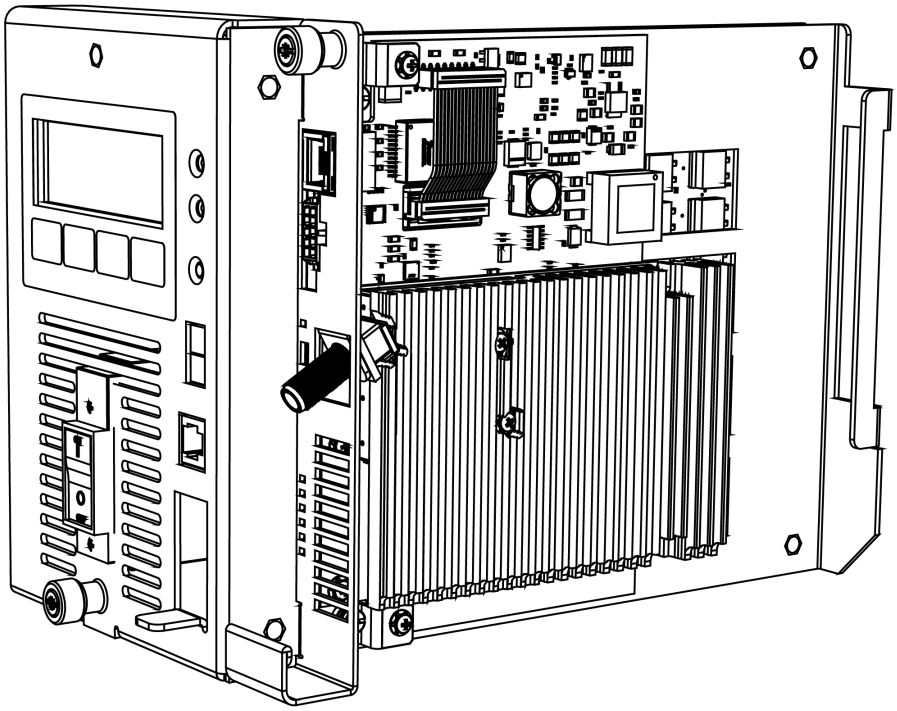
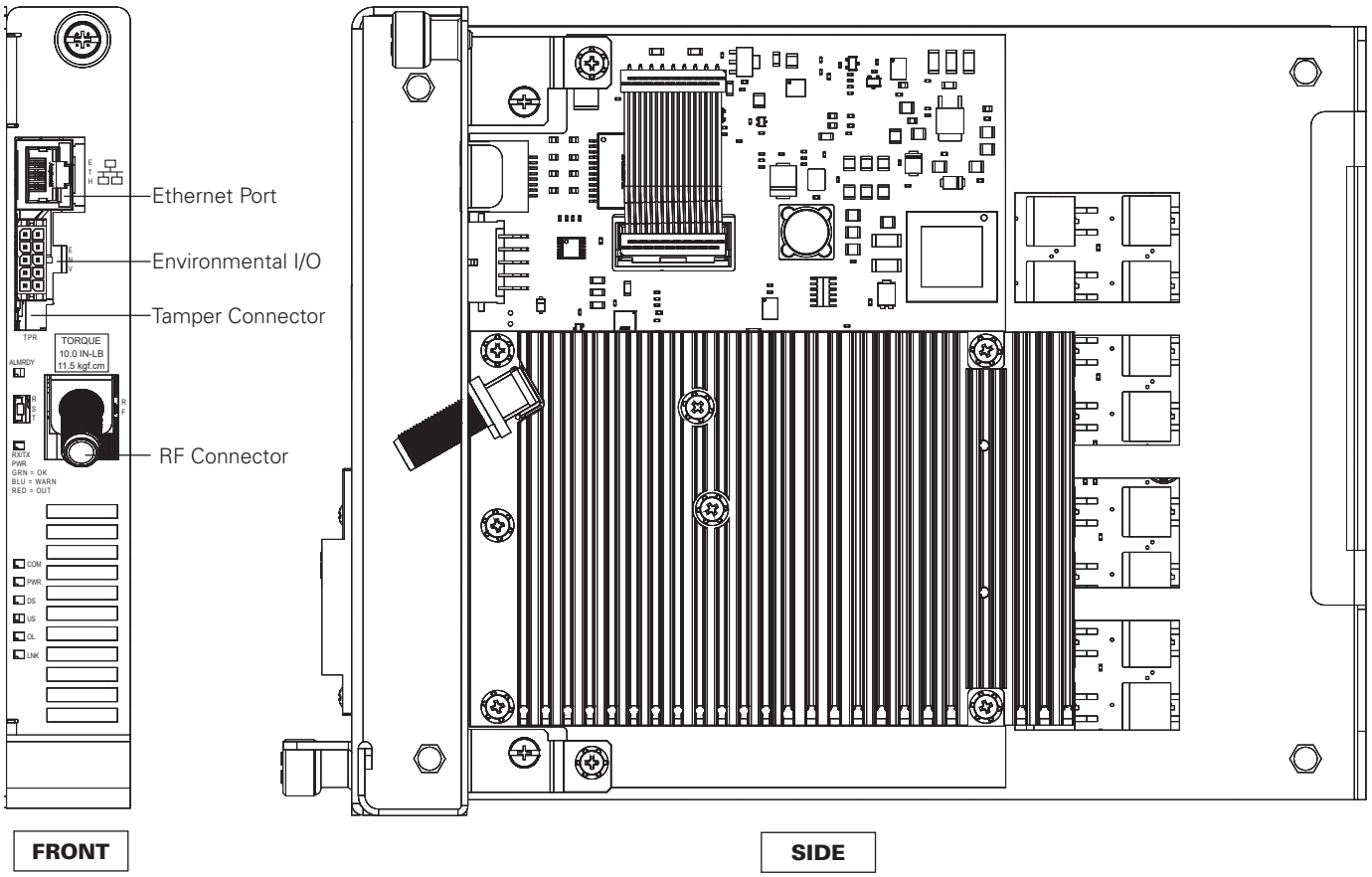


Fig. 1-1, Alpha® DM31 Transponder Attached to XM3-HP™ Power Supply Inverter

Primary Features

- DOCSIS® 3.0 and 3.1 compliant and certified cable modem for power supply status monitoring
- Supports SCTE® power supply standards
- Local 10/100/1000 Mbps auto-negotiating standard Ethernet interface provides technician on-site access to extensive power supply diagnostics (and also permits the connecting of external CPE devices)
- Embedded web server for direct diagnostics
- Supports SNMPv1, v2c, v3
- Extensive power supply diagnostic MIBs
- Supports RF spectrum full band capture
- Environmentally hardened DOCSIS cable modem and transponder
- Angled RF connector reduces cable bend radius strain
- Diagnostic LEDs
- North American or Euro DOCSIS available



LED Indicators			
ALM/RDY	DM31 ready, major/minor alarm	**DS**	Downstream RF carrier detection/lock
Rx/Tx PWR	RF power level	**US**	Upstream RF carrier detection/lock
COM	XM3-HP communications	**OL**	Registration lock
PWR	DM31 power	**LNK**	Ethernet link

Fig. 1-2, DM31 Transponder Components

1.1 Models and Diplexer Ranges

The DM31 transponder is available in three models, each supporting different RF diplexer ranges. Each model includes two software controlled upstream and downstream frequency ranges.

Modem diplexer ranges are shown in the table below:

Model (p/n)	Diplexer Range 1		Diplexer Range 2	
	Upstream Range	Downstream Range	Upstream Range	Downstream Range
DM31-H2	5 - 42 MHz	108 - 1002 MHz	5 - 85 MHz	108 - 1002 MHz
DM31-H3	5 - 45 MHz	258 - 1218 MHz	5 - 204 MHz	258 - 1218 MHz
DM31-H4E (Euro)	5 - 85 MHz	108 - 1218 MHz	5 - 204 MHz	258 - 1218 MHz

Table 1-1, Modem Diplexer Ranges

The diplexer can be controlled via the standard DOCSIS® 3.1 MDD TLV messages, and config file TLV settings. In addition, SNMP MIB object atiMgmtCfgDocsisRfSplit = 1.3.6.1.4.1.926.1.3.3.1.3 allows a real time switch of the diplexer for the current boot cycle. A reboot of the modem will default the diplexer to the behavior specified by DOCSIS®. MIB settings to configure the diplexer are shown in the table below:

OID Values to Set RF Splits			
Component	Description	Default	Values
atiMgmtCfgDocsisRfSplit 1.3.6.1.4.1.926.1.3.3.1.3	Selects which RF diplex split to use. Setting this value takes effect immediately, but normal DOCSIS behavior can subsequently change the setting.	unknown(0)	unknown(0) us5to85ds108to1218(1) us5to204ds258to1218(2) us5to42ds108to1002(3) us5to85ds108to1002(4) us5to42ds108to1218(5) us5to45ds258to1218(6)
atiMgmtCfgDocsisRfSplitSupport 1.3.6.1.4.1.926.1.3.3.1.4	Indicates which choices are supported for atiMgmtCfgDocsisFrequencyPlan on this device.		The value reported is the sum of each of the following values: 1 - us5to85ds108to1218(1) is a valid option 2 - us5to204ds258to1218(2) is a valid option 4 - us5to42ds108to1002(3) is a valid option 8 - us5to85ds108to1002(4) is a valid option 16 - us5to42ds108to1218(5) is a valid option 32 - us5to45ds258to1218(6) is a valid option

Table 1-2, OID Values to Set RF Splits

2.0 Overview

2.1 System Diagram

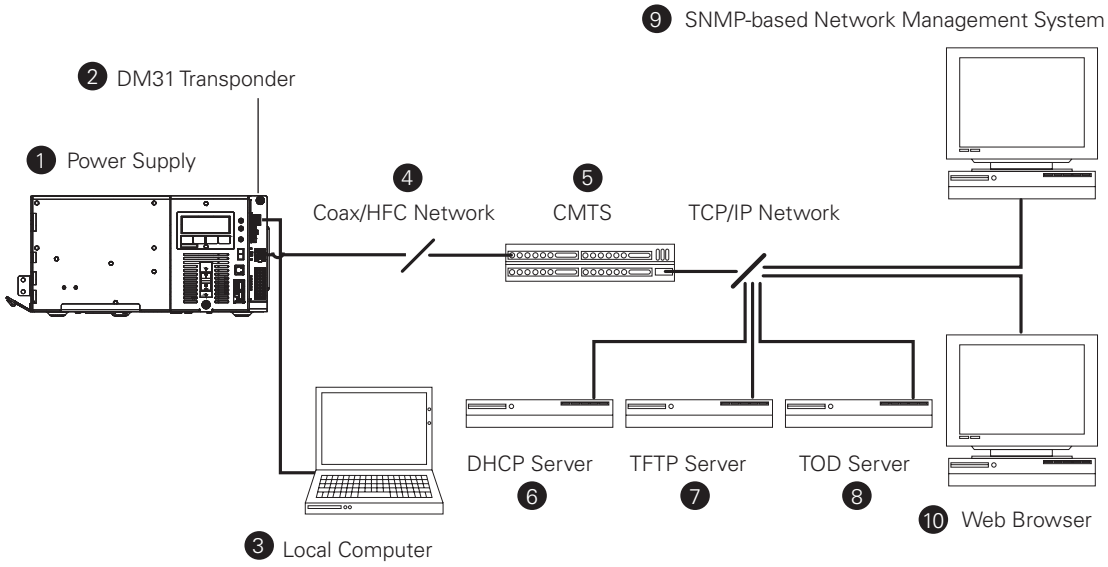


Fig. 2-1, Representative System Arrangement

1. The intelligent broadband UPS monitors and maintains all status information about the power supply operation. This data is accessible directly via the power supply's Smart Display (see the power supply's technical manual for details). The power supply communicates its data to the transponder.
2. The DM31 transponder contains both SCTE-HMS Management Information Base (MIBs) and the proprietary Alpha® MIB tables. The SCTE-HMS MIBs are industry standard MIB tables that report power supply and battery data (see **Section 6.0 Data Management**). The Alpha MIBs contain all the data of the SCTE-HMS MIBs plus additional power supply settings and values as well as the transponder's configuration values.
3. Power supply and transponder parameters can be monitored and set locally using a laptop and a standard Ethernet cable.
4. The transponder transmits data via its cable modem directly over the coax or hybrid fiber coax (HFC) network.
5. The Cable Modem Termination System (CMTS) is the bridge between the cable network and the TCP/IP network. The transponder's cable modem communicates over the HFC network to the CMTS.
6. The Dynamic Host Control Protocol (DHCP) server needs to be provisioned with the transponder's cable modem CM MAC address and the MAC address needs to be assigned a DOCSIS® configuration file.
7. The DOCSIS configuration file and firmware files should be available in the root directory of the Trivial File Transfer Protocol (TFTP) server.
8. The Time of Day (TOD) server provides the cable modem with the current date and time. Note that the Password Of The Day feature requires the TOD server to be working properly.
9. A Network Management System (NMS) or MIB browser allows remote monitoring, control, and configuration of the transponder, power supply and connected device parameters. Alarms and traps can be set and monitored.
10. The power supply data may be accessed remotely through the transponder's web page by placing its IP address into a standard web browser.

2.2 Network Connectivity

The DM31 transponder's cable modem must be provisioned in the cable system to allow it to be recognized by the CMTS as a valid device, to be assigned an IP address from the DHCP server with the correct options to locate the TFTP and TOD servers and to communicate with the SNMP management server (trap receiver).

In the default DM31 transponder configuration, data from both the cable modem and power supply are accessed and managed through the modem's IP address on the secure private modem network. Consequently, the Network Management System (NMS) that monitors the power supplies must have access to the same private modem network.

CMTS and system vendors use different security methods to insure network integrity, but common considerations are:

- Network MAC filtering may have to be modified to allow the cable modem OUI of 00:90:EA for Alpha® transponders.
- DHCP access must be provided, as with any DOCSIS modem. DHCP for IPv4 uses UDP port 67 outbound and UDP port 68 inbound. DHCPv6 for IPv6 uses UDP port 547 outbound and UDP port 546 inbound.
- TOD (Time Of Day) must be provided, as with any DOCSIS modem. TOD uses UDP port 37 outbound.
- TFTP access must be provided, as with any DOCSIS® modem. TFTP uses UDP port 69 outbound.
- If using TR-069 provisioning, access to the ACS must be provided, and configured through the cable modem configuration file or the DHCP offer. TR-069 uses TCP port 7547 inbound.
- For SNMP access, UDP ports 161 inbound for queries, and UDP port 162 outbound for notifications must not be blocked.
- For HTTP access, TCP port 80 inbound must not be blocked.
- For HTTPS access, TCP port 443 inbound must not be blocked.

When the DM31 transponder is configured for dual IP (see **Section 6.6 Dual IP Modee**), the power supply is accessed and managed through a separate IP address in the Customer Premises Equipment (CPE) network. In that setup, the NMS must have access to the CPE network, and SNMP, HTTP and HTTPS access all occur in that space.

2.3 System Configuration and Installation

NOTICE:

Before installation, read all of **Section 2.0 Overview**.

DM31 transponder installation and setup is comprised of three basic steps:

1. Configuring the Network: Provisioning the DHCP server with the transponder's MAC address and assigning it a DOCSIS® configuration file.
2. Setting Options: The DM31 transponder is designed for out-of-the-box, "plug and play" operation, but non-default settings such as SNMP trap destination addresses may be required for the Network Management System (NMS). SNMP trap addresses can be set automatically via the DOCSIS configuration file per RFC 4639 (IPv4), or through SNMPv3 notification settings (IPv6), while proprietary options may be set through type-11 TLV entries.
3. Field installation of the DM31 transponder into the power supply, connecting the tamper and environmental control (as applicable) and verifying operation.

These steps can be performed independently of one another. However, configuring the network prior to field installation will allow the installation to be verified while personnel are still on-site. Performing field installation before network configuration and before the installation can be verified, might result in additional field service calls to correct mistakes.

Carefully read the following section in order to understand the dependencies within the system before performing system configuration or hardware installation.

2.4 DM31 Transponder Start Up and Reboot Sequence

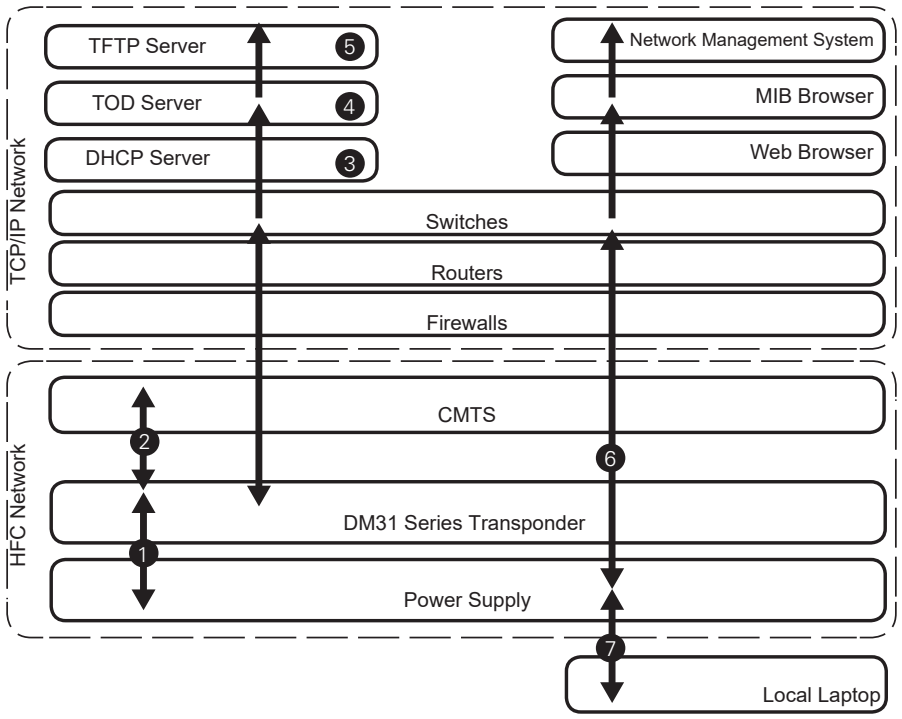


Fig. 2-2, DM31 Transponder Start-up and Reboot Sequence

The above diagram indicates the order of operations as the transponder comes online. There are certain conditions that must exist for each step to occur, resulting in successful data monitoring and management. The numbers below correspond to the numbered arrows above.

- Blue Rx/Tx Power LED indicates Rx/Tx Power at a warning level. Make the necessary RF level adjustments.
- Red Rx/Tx Power LED indicates Rx/Tx Power at an alert level. Make the necessary RF level adjustments.

LEDs and Indications								
Ref #	**Communications State**	**ALM / RDY**	**Rx / Tx Power**	**Communications (COM)**	**Downstream (DS)**	**Upstream (US)**	**ONLINE (OL)**	**Link (LNK)**
1	Transponder initializing / searching for downstream DOCSIS® channel	Flashing (Green)	OFF	OFF	Flashing	OFF	OFF	OFF
2	Downstream channel acquired, service group determination and ranging initialization	Flashing (Green)	OFF	OFF	ON	Flashing	OFF	OFF
3 - 5	Registration - coming online	Flashing (Green)	ON (Green = OK)	OFF and ON	ON	ON	Flashing	OFF
6	DM31 transponder fully functional	Flashing (Green)	ON (Green)	Bursts when communicating to the power supply	ON	ON	ON	OFF
7	Laptop connected (Local)	Flashing (Green)	ON (Green)	Bursts	ON	ON	ON	ON/Bursts

Table 2-1, LEDs and Indications

3.0 Network Configuration

3.1 Provisioning the DHCP Server with the MAC Addresses

On the DHCP server, assign the cable modem's CM MAC address with a DOCSIS® configuration file to set modem communication options. See **Section 3.3 DOCSIS® Configuration File** for instructions on how to create a DOCSIS configuration file.

The CM MAC address is located on the shielding on the side of the unit (see the figure below). Record this information prior to installation of the DM31 transponder.

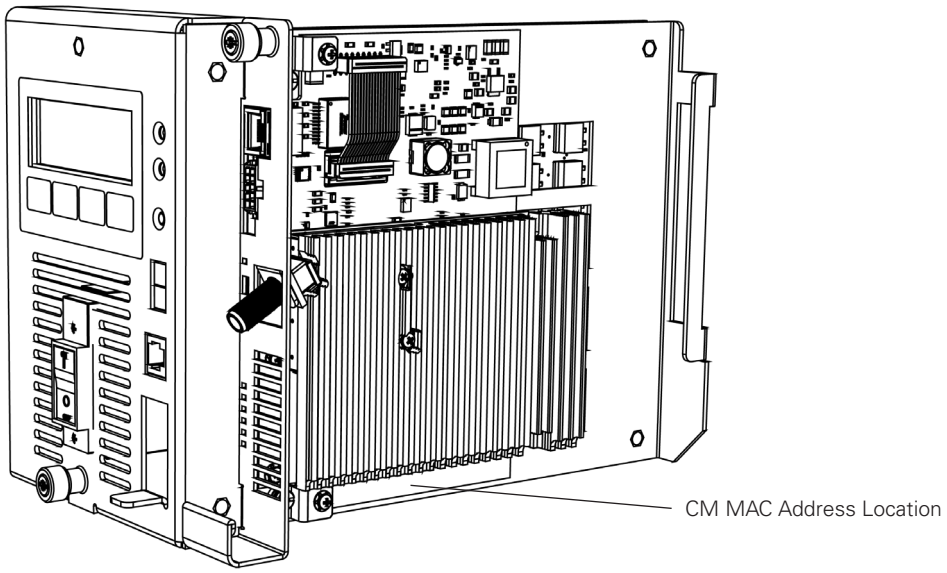


Fig. 3-1, Location of MAC Address Label

3.2 Establishing IP Connectivity

The DM31 transponder supports the CableLabs® DOCSIS® 3.0 and DOCSIS® 3.1 IPv6 implementation. The main benefit of IPv6 is its expanded addressing capability, increasing the address space from 32 to 128 bits, providing virtually unlimited numbers of networks and systems. The DM31 transponder determines the IP provisioning mode via the CableLabs SNMP MIB parameter docsIf3CmMdCfgIpProvMode (SNMP OID: 1.3.6.1.4.1.4491.2.1.20.1.31.1.1). The DM31 transponder supports the following configurable IP provisioning mode override policies:

- Honor MDD: The cable modem of the DM31 transponder will acquire an IPv6 or IPv4 address as directed by the MAC Domain Descriptor (MDD) message for provisioning and operation.
- IPv4 only: The cable modem of the DM31 transponder will acquire a single IPv4 address for the CM management stack, overriding the TLVs in the MDD message.
- IPv6 only: The cable modem of the DM31 transponder will acquire a single IPv6 address for the CM management stack, overriding the TLVs in the MDD message.

3.3 DOCSIS® Configuration File

A cable modem's DOCSIS configuration file is a type-length-value (TLV) file that contains important operational parameters as defined by the DOCSIS standards. It provides certain settings for the cable modem. In addition to standard entries, settings in the DOCSIS configuration file should include the modem's community strings, and if an upgrade is necessary, firmware upgrade parameters. Place the configuration file in the TFTP root directory.

The transponder's cable modem interface can support both IPv4 and IPv6 addressing schemes. The required DOCSIS configuration file operational parameters will differ depending on company policies, cable modem firmware versions and IP addressing schemes. The following DOCSIS configuration file details listed in this manual are general guidelines. Please consult the published DOCSIS specification resources (CableLabs®) for additional DOCSIS configuration file details and guidelines.

To build a DOCSIS configuration file, use a DOCSIS TLV editor program.

See the example configuration files in **Section 3.3.5 Sample DOCSIS® Configuration File Entries - docsDevNmAccess Method (Deprecated)** and **Section 3.3.6 Sample DOCSIS® Configuration File Entries - Coexistence Method**.

For automatically updating modem firmware with the DOCSIS configuration file, see **Section 5.1 Upgrading DM31 Transponder Modem Firmware**.

NOTICE:

For SNMPv1 and v2c, the modem community strings should be set in the DOCSIS configuration file.

3.3.1 Setting Modem Community Strings - docsDevNmAccess Method (Deprecated; IPv4 Only)

Set the modem community strings with the DOCSIS configuration file by including the following SNMP parameters.

Modem Community String Parameters docsDevNmAccess Method			
MIB Parameter	**Object ID**	**Description**	**Value**
docsDevNmAccessIp	1.3.6.1.2.1.69.1.2.1.2.x	The IP address (or subnet) of the NMS	e.g. 10.20.30.0
docsDevNmAccessIpMask	1.3.6.1.2.1.69.1.2.1.3.x	The IP subnet mask of the NMS	e.g. 255.255.255.0
docsDevNmAccessCommunity	1.3.6.1.2.1.69.1.2.1.4.x	The community string matched to this IP address net mask entry	alphanumeric string
docsDevNmAccessControl	1.3.6.1.2.1.69.1.2.1.5.x	The level of access granted	none(1) read(2) readWrite(3) roWithTraps(4) rwWithTraps(5) trapsOnly(6)
docsDevNmAccessInterfaces	1.3.6.1.2.1.69.1.2.1.6.x	Specifies the set of interfaces from which requests from this NMS will be accepted	0x40 : Cable interface (typical) 0x80 : Ethernet interface 0xC0 or 0x00 : Both interfaces
docsDevNmAccessStatus	1.3.6.1.2.1.69.1.2.1.7.x	Controls and reflects the status of rows in this table	createAndGo(4)

Note: x denotes the index of the SNMP entry

Table 3-1, Modem Community String Parameters - docsDevNmAccess Method

3.3.2 Setting Modem Community Strings - Coexistence Method

Set the modem community strings with the DOCSIS® configuration file for an IPv4 or IPv6 network by including the following SNMP parameters:

Modem Community String Parameters Coexistence Method			
TLV Type	**TLV Parameter**	**Description**	**Value**
53	SNMPv1v2c Coexistence Configuration	This object specifies the SNMPv1v2c Coexistence Access Control configuration of the CM. This TLV creates entries in SNMPv3 tables as specified in [DOCSIS OSSIv3.0]	Composite
53.1	SNMPv1v2c Community Name	This sub-TLV specifies the Community Name (community string) used in SNMP requests to the CM.	Text (e.g. AlphaRead)
53.2	SNMPv1v2c Transport Address Access	This sub-TLV specifies the Transport Address and Transport Address Mask pair used by the CM to grant access to the SNMP entity querying the CM.	Variable
53.2.1	SNMPv1v2c Transport Address	Specifies the Transport Address to use in conjunction with the Transport Address Mask used by the CM to grant access to the SNMP entity querying the CM. Length is 6 bytes for IPv4 and 18 bytes for IPv6. Two additional bytes are added to the IP address length for the port number.	Transport Address (e.g. 0.0.0.0/0 or 0:0:0:0:0:0:0:0/0)
53.2.2	SNMPv1v2c Transport Address Mask	Specifies the Transport Address Mask to use in conjunction with the Transport Address used by the CM to grant access to the SNMP entity querying the CM. Length is 6 bytes for IPv4 and 18 bytes for IPv6. Two additional bytes are added to the IP address length for the port number.	Transport Address (e.g. 0.0.0.0/0 or 0:0:0:0:0:0:0:0/0)
53.3	SNMPv1v2c Access View Type	Specifies the type of access to grant to the community name of this TLV. If not specified, default read-only is used.	1 = Read Only 2 = Read / Write
53.4	SNMPv1v2c Access View Name	Specifies the name of the view that provides the access indicated in sub-TLV SNMPv1v2c Access View Type.	String (e.g. docsisManagerView)

Table 3-2, Modem Community String Parameters - Coexistence Method

3.3.3 Setting SNMP Trap Destination Addresses - docsDevNmAccess Method (Deprecated; IPv4 Only)

Set the SNMP trap destination addresses via the DOCSIS® configuration file by including the following SNMP parameters. (A single entry can set both a trap destination and a community string for access.)

Trap Destination Addresses IPv4 Method			
MIB Parameter	**Object ID**	**Description**	**Value**
docsDevNmAccessIP	1.3.6.1.2.1.69.1.2.1.2.x	IP address of trap destination, e.g. NMS server	e.g. 10.20.30.40
docsDevNmAccessIpMask	1.3.6.1.2.1.69.1.2.1.3.x	Must be set to 255.255.255.255 per RFC 4639	255.255.255.255
docsDevNmAccessCommunity	1.3.6.1.2.1.69.1.2.1.4.x	Community string used by NMS to query transponder	alphanumeric string
docsDevNmAccessControl	1.3.6.1.2.1.69.1.2.1.5.x	Level of SNMP access to DM3.0 Series transponder from IP address specified in docsDevNmAccessIpMask	none(1) read(2) readWrite(3) roWithTraps(4) rwWithTraps(5) trapsOnly(6)
docsDevNmAccessInterfaces	1.3.6.1.2.1.69.1.2.1.6.x	Specifies the set of interfaces from which requests from this NMS will be accepted	0x40 : Cable interface (typical) 0x80 : Ethernet interface 0xC0 or 0x00 : Both interfaces
docsDevNmAccessStatus	1.3.6.1.2.1.69.1.2.1.7.x	Controls and reflects the status of rows in this table	createAndGo(4)

Note: x denotes the index of the SNMP entry

Table 3-3, Trap Destination Addresses - docsDevNmAccess Method

3.3.4 Setting SNMP Trap Destination Addresses - Coexistence Method

Set the SNMP trap destination addresses via the DOCSIS® configuration file by including the following SNMP parameters:

Trap Destination Addresses IPv4 Method			
TLV Type	**TLV Parameter**	**Description**	**Value**
38	SNMPv3 Notification Receiver	This config file element specifies an NMS that will receive notifications from the modem when it is in Coexistence mode. Up to 10 of these elements may be included in the configuration file.	Composite
38.1	SNMPv3 Notification Receiver IP Address	This sub-TLV specifies the IP address of the notification receiver. Length is 4 bytes for IPv4 and 16 bytes for IPv6.	0:0:0:0:0:0:0:0 (e.g.fc00:168:1:0:0:0:0:32) 0.0.0.0 (e.g. 10.11.0.1)
38.2	SNMPv3 Notification Receiver UDP Port Number	This sub-TLV specifies the UDP port number of the notification receiver. If this sub-TLV is not present, the default value of 162 should be used.	UDP port number (e.g. 162)
38.3	SNMPv3 Notification Receiver Trap Type	This sub-TLV specifies the type of trap to send.	The trap type may take values: 1 = SNMP v1 trap in an SNMP v1 packet 2 = SNMP v2c trap in an SNMP v2c packet 3 = SNMP inform in an SNMP v2c packet 4 = SNMP v2c trap in an SNMP v3 packet 5 = SNMP inform in an SNMP v3 packet
38.4	SNMPv3 Notification Receiver Timeout	This sub-TLV specifies the timeout value to use when sending an Inform message to the notification receiver.	Time in milliseconds (e.g. 15000)
38.5	SNMPv3 Notification Receiver Retries	This sub-TLV specifies the number of times to retry sending an Inform message if an acknowledgement is not received.	Number of retries (e.g. 3)
38.6	SNMPv3 Notification Receiver Filtering Parameters	Object Identifier of the snmpTrapOID value that identifies the notifications to be sent to the notification receiver. This notification and all below it will be sent.	Filter OID (e.g. 1.3.6)

Table 3-4, Trap Destination Addresses - docsDevNmAccess Method

NOTICE:

As an alternative to the docsDevNmAccessTable or SNMPv3 trap parameters, SNMP trap destination addresses may be set through the Alpha® proprietary MIB atiMgmtSnmpTrapTable (OID: 1.3.6.1.4.1.926.1.3.1.1) using a SNMP MIB browser or as an entry in the proprietary configuration file 'atidoc31.cfg' in **Section 3.3.7 Proprietary Configuration File 'atidoc31.cfg'**.

3.3.5 Sample DOCSIS® Configuration File Entries - docsDevNmAccess Method (Deprecated)

1
```
SNMP MIB Object (11) [Len=21]:docsDevNmAccessStatus.1/4
SNMP MIB Object (11) [Len=21]:docsDevNmAccessIp.1/10.56.21.0
SNMP MIB Object (11) [Len=21]:docsDevNmAccessIpMask.1/255.255.255.0
SNMP MIB Object (11) [Len=25]:docsDevNmAccessCommunity.1/"RW STRING"
SNMP MIB Object (11) [Len=25]:docsDevNmAccessInterfaces.1/"@"
SNMP MIB Object (11) [Len=21]:docsDevNmAccessControl.1/3
```

2
```
SNMP MIB Object (11) [Len=21]:docsDevNmAccessStatus.2/4
SNMP MIB Object (11) [Len=21]:docsDevNmAccessIp.2/10.20.30.40
SNMP MIB Object (11) [Len=21]:docsDevNmAccessIpMask.2/255.255.255.255
SNMP MIB Object (11) [Len=25]:docsDevNmAccessCommunity.2/"RW Trap string"
SNMP MIB Object (11) [Len=25]:docsDevNmAccessInterfaces.2/"@"
SNMP MIB Object (11) [Len=21]:docsDevNmAccessControl.2/5
```

3
```
Software Upgrade Filename(9) [Len=24]:"ModemFirmwareFile.bin"
SNMP MIB Object (11) [Len=20]:docsDevSwAdminStatus.0/2
```

4
```
Software Upgrade TFTP Server (21) [Len=4]:10.56.48.15
```

5
```
Manufacturer Code Verification Certificate (32) [Len=254]: 30 82 03 1A 30 82...
Manufacturer Code Verification Certificate (32) [Len=254]: 04 0A 13 11 41 4D...
Manufacturer Code Verification Certificate (32) [Len=254]: 04 0C 30 0A 06 01...
Manufacturer Code Verification Certificate (32) [Len=36]: 11 A3 41 A6 A7 D9....
```

Legend

1. Sets Read-Write community string. Set the IP address, netmask and community string to fit your system.
2. Sets the IP address of where the SNMP traps will be sent. This is typically set to match the IP address of the Network Managements System Server.
3. Sets firmware download parameters.
4. Specifies the IP address of the TFTP server used for upgrading firmware.
5. Sets Code Verification Certificate (CVC) for firmware upgrade security per the DOCSIS specification.

3.3.6 Sample DOCSIS® Configuration File Entries - Coexistence Method

❶
SNMPv1v2c Coexistence Configuration
SNMPv1v2c Community Name:ReadWrite
SNMPv1v2c Transport Address Access
SNMPv1v2c Transport Address:0.0.0.0/0
SNMPv1v2c Transport Address Mask:0.0.0.0/0
SNMPv1v2c Transport Address Access
SNMPv1v2c Transport Address:0:0:0:0:0:0:0:0/0
SNMPv1v2c Transport Address Mask:0:0:0:0:0:0:0:0/0
SNMPv1v2c Access View Type:read-write
SNMPv1v2c Access View Name:docsisManagerView

❷
Docsis V3 Notification Receiver
UDP Port number of trap receiver:162
Type of trap:SNMP v1 trap in an SNMP v1 packet
Timeout for sending inform:15000
Number of retries:3
Filtering Parameters:1.3.6
IPv6 Address of trap receiver:fc00:168:1:0:0:0:0:32
Docsis V3 Notification Receiver
IP Address of trap receiver:192.168.1.51
UDP Port number of trap receiver:162
Type of trap:SNMP v1 trap in an SNMP v1 packet
Timeout for sending inform:15000
Number of retries:3
Filtering Parameters:1.3.6

❸ Software Upgrade Filename:ModemFirmwareFile.bin

❹ Software Upgrade IPv6 TFTP Server:fc00:168:1:0:0:0:0:51

❺
Manufacturer Code Verification Certificate:3082031B30820…
Manufacturer Code Verification Certificate:040A1312414C5…
Manufacturer Code Verification Certificate:FF040C300A060…
Manufacturer Code Verification Certificate:257939C848CE0…

Legend

❶ Sets Read-Write community string. Set the IP address, netmask and community string to fit your system.

❷ Sets the IP address of where the SNMP traps will be sent. This is typically set to match the IP address of the Network Managements System Server.

❸ Sets firmware download parameters.

❹ Specifies the IP address of the TFTP server used for upgrading firmware.

❺ Sets Code Verification Certificate (CVC) for firmware upgrade security per the DOCSIS specification.

NOTICE:

DOCSIS configuration files vary from system to system. Take into consideration your company's policies, and test the file on a local system prior to wide scale deployment.

3.3.7 Proprietary Configuration File 'atidoc31.cfg'

The DM31 transponder will attempt to download a TLV-formatted file 'atidoc31.cfg' from the modem's provisioning TFTP server at start up and every 24 hours thereafter. The atidoc31.cfg proprietary configuration file is optional and provides an alternative method to the modem's DOCSIS® configuration file for deploying Alpha® proprietary SNMP MIB parameters to field-installed DM31 communications modules. The atidoc31.cfg file can be particularly helpful in "Dual IP" configurations, where power supply configuration is managed by a different file than modem configuration.

NOTICE:

Other Alpha® transponders have used different filenames for this configuration file. The DM3.0 series transponders used file 'atidoc33.cfg'.

The atidoc31.cfg file should be used if either of the following conditions are true:

1. Non-default settings, such as SNMP trap destination addresses, need to be distributed to all DM31 communications modules.
2. The operator does not desire to place Alpha-specific parameters into the modem's DOCSIS configuration file.

NOTICE:

The recommended method for setting the SNMP trap address(es) is through the modem DOCSIS configuration file (see **Section 3.3 DOCSIS® Configuration File**). Alpha-proprietary parameters may also be set through the modem's DOCSIS configuration file, eliminating the need for the atidoc31.cfg proprietary configuration file.

To build the atidoc31.cfg file, enter the desired SNMP OIDs and values from the Alpha® MIB into a TLV file as TLV type-11 entries using a TLV editor (refer to sample entries below). The DM31 transponder proprietary configuration setup file must be named "atidoc31.cfg" and placed in the root directory of the TFTP server. DM31 transponder settings are updated according to values defined in this file at start up and after every 24 hours of operation.

Sample atidoc31.cfg entries:

- Network Access Control (3) [Len = 1]: 1
- SNMP MIB Object (11) [Len = 24]: atiMgmtSnmpTrapAddress.1 / 10.20.30.40
- SNMP MIB Object (11) [Len = 24]: atiMgmtSnmpTrapAddress.2 / 10.20.30.50
- SNMP MIB Object (11) [Len = 23]: atiMgmtSysTamperPolarity.0 / 1

3.3.8 Changing Default atidoc31.cfg Download Settings

By default the DM31 transponder will download the atidoc31.cfg file from the provisioning TFTP server every 24 hours. However, these settings may be adjusted per the tables below by placing the respective SNMP varbinds into the modem's DOCSIS configuration file.

Default atidoc.cfg Download Settings			
Parameter	**Type**	**Description**	**Value**
atiMgmtSysDownloadConfigName 1.3.6.1.4.1.926.1.3.2.1.9.0	Alphanumeric String	Name of proprietary configuration file	"atidoc31.cfg" (Default)
atiMgmtSysDownloadReCfgTime 1.3.6.1.4.1.926.1.3.2.1.13.0	Integer	Download interval for atidoc31.cfg (hours)	24 (Default)

Search Order	Parameter	Type	Description	Value
1	atiMgmtSysDownloadConfigAddress OID 1.3.6.1.4.1.926.1.3.2.1.10.0	IP Address	Overrides default location	0.0.0.0 (Default)
2	docsDevServerConfigTftpAddress 1.3.6.1.2.1.69.1.4.11.0	IP Address	Default location (no change necessary)	CM's TFTP Server Address
3	docsDevSwServerAddress 1.3.6.1.2.1.69.1.3.7.0	IP Address	Set via DOCSIS configuration file	Configurable
4	Software Upgrade Server	IP Address	Set via DOCSIS configuration file	Configurable

Table 3-5, Default atidoc31.cfg Download Settings

3.4 Setting Communication Options

Communications settings may be changed through the Alpha® MIB remotely using an SNMP MIB browser or automatically by placing the SNMP parameters into the DOCSIS® configuration file.

NOTICE:

Before setting options, verify UDP ports 37, 69, 161, 162 and TCP port 80 are not blocked. Refer to **Section 2.2 Network Connectivity** for communication port information.

ATI-MGMT-SNMP-MIB			
OIDs for SNMP Communications			
Component	**Description**	**Default**	**Values**
atiMgmtSnmpTrapOnNormal OID: 1.3.6.1.4.1.926.1.3.1.5.1.0	Send SNMP trap when alarmed condition returns to normal state.	Integer	1 = Disabled 2 = Enabled (Default)
atiMgmtSysSnmpTimeout OID: 1.3.6.1.4.1.926.1.3.1.5.3.0	Time DM31 transponder will wait before reset if SNMP traffic is not detected (minutes).	Integer	240 (Default) Note: If set to zero, watchdog will be disabled.

Table 3-6, OIDs for SNMP Communications

ATI-MGMT-SYS-HTTP-LOGINS-MIB			
OIDs for Usernames and Passwords for Web Interface Access (atiHttpLoginCredentials)			
Component	**Description**	**Default**	**Values**
atiHttpLoginCredUserName 1.3.6.1.4.1.926.1.3.2.2.4.5.11.1.0	The login username for 'basic user' access to the web interface. atiHttpLoginCredUserAccess determines the level of access for this login.	Alpha	Can be changed to a customized string.
atiHttpLoginCredUserPassword 1.3.6.1.4.1.926.1.3.2.2.4.5.11.2.0	The login password for 'basic user' access to the web interface.	AlphaGet	Can be changed to a customized string.
atiHttpLoginCredAdminName 1.3.6.1.4.1.926.1.3.2.2.4.5.11.3.0	The login username for 'administrator' access to the web interface. atiHttpLoginCredAdminAccess determines the level of access for this login.	Admin	Can be changed to a customized string.
atiHttpLoginCredAdminPassword 1.3.6.1.4.1.926.1.3.2.2.4.5.11.4.0	The login password for 'administrator' access to the web interface.	AlphaSet	Can be changed to a customized string.
atiHttpLoginCredNoneAccess 1.3.6.1.4.1.926.1.3.2.2.4.5.11.5.0	This setting determines the level of web page interaction available without logging in to the web page.	viewAll(2)	noAccess(0) view(1) viewAll(2) edit(3) editAll(4)
atiHttpLoginCredUserAccess 1.3.6.1.4.1.926.1.3.2.2.4.5.11.6.0	This setting determines the level of web page interaction available with the 'basic user' login.	edit(3)	noAccess(0) view(1) viewAll(2) edit(3) editAll(4)
atiHttpLoginCredAdminAccess 1.3.6.1.4.1.926.1.3.2.2.4.5.11.7.0	This setting determines the level of web page interaction available with the 'administrator' login.	editAll(4)	noAccess(0) view(1) viewAll(2) edit(3) editAll(4)
atiHttpLoginPasswordRules (1.3.6.1.4.1.926.1.3.2.2.4.5.14.0)	This optional object determines how the system handles passwords for web logins.		1 = Simple(1) 2 = potd(2)

Table 3-7, OIDs for Usernames and Passwords

NOTICE:

The DM31 transponder will inherit the cable modem community string settings provided by the DOCSIS configuration file.

OIDs for Login Configuration and Information (atiMgmtSysHttpWriteEnabled, atiMgmtSysHttpLogins, and atiHttpLoginSessionTable)			
Component	**Description**	**Default**	**Values**
atiMgmtSysHttpWriteEnabled 1.3.6.1.4.1.926.1.3.2.2.4.4	Controls which interface connection write access is allowed.	localAndCmAndCpe(7)	disabled(0) cmOnly(1) cpeOnly(2) cmAndCpe(3) localOnly(4) localAndCm(5) localAndCpe(6) localAndCmAndCpe(7)
atiHttpLoginLocalAccess 1.3.6.1.4.1.926.1.3.2.2.4.5.1.0	Controls whether the device will accept web interface logins from the local Ethernet port.	access(2)	noAccess(1) access(2)
atiHttpLoginRemoteAccess 1.3.6.1.4.1.926.1.3.2.2.4.5.2.0	Controls whether the device will accept web interface logins from the network.	access(2)	noAccess(1) access(2)
atiHttpLoginEditsLevel 1.3.6.1.4.1.926.1.3.2.2.4.5.3.0	This is a read-only object that indicates the highest level of edit capability currently held by any web login session. This object has an associated entry in the Discrete Property Table.		noEdits(1) someEdits(2) allEdits(3)
atiHttpLoginTimeout 1.3.6.1.4.1.926.1.3.2.2.4.5.6.0	This is the time, in minutes, that a web login session may be inactive (time between page loads) before the session automatically ends. A setting of 0 means that no timeout is applied to a login session.	10 Minutes	
atiHttpLoginSessionUser 1.3.6.1.4.1.926.1.3.2.2.4.5.12.1.2.x	The user name(s) of a current or recent login session.		
atiHttpLoginSessionLevel 1.3.6.1.4.1.926.1.3.2.2.4.5.12.1.3.x	The access level(s) assigned at login for a current or recent login session. Reading a value of loggedOut(0) indicates a session no longer active. Writing a value of loggedOut(0) to an active session forces a logout of that session.		loggedOut(0) view(1) viewAll(2) edit(3) editAll(4)
atiHttpLoginSessionAddress 1.3.6.1.4.1.926.1.3.2.2.4.5.12.1.4.x	The IP address(es) of a client for a current or recent login session.		
atiHttpLoginSessionStart 1.3.6.1.4.1.926.1.3.2.2.4.5.12.1.5.x	The time(s) when a current or recent session started. If the returned time does not include a time zone, it is expressed in terms of local time on the device.		
atiHttpLoginSessionEnd 1.3.6.1.4.1.926.1.3.2.2.4.5.12.1.6.x	For a recent login session, this is the time(s) when that session ended. This object is not returned for a session that is still active. If the returned time does not include a time zone, it is expressed in terms of local time on the device.		

Table 3-7, OIDs for Usernames and Passwords, continued

4.0 Web Interface

The DM31 transponder provides an embedded web server interface to allow operations personnel the ability to connect locally or remotely via TCP/IP over Ethernet with a laptop/computer to verify the status of common data points and to configure various operating parameters.

4.1 Local Web Server Access

The DM31 transponder's Ethernet port (comparable to the craft port on some transponder models) will typically be used as a local connection point allowing the user to connect directly to the DM31 transponder web server interface to verify/configure common communication parameters and view power supply status and battery values. The Ethernet port on the DM31 transponder is a fully functional standard Ethernet port, capable of providing all the functionality of any standard Ethernet connection.

To access the DM31 transponder web server locally utilizing a web browser, use the following procedure:

1. Connect a standard Ethernet cable (CAT5 or better) between the DM31 transponder Ethernet port (ETH) and a laptop or computer's network interface port.
2. Launch a web browser (Chrome™, Edge®, etc.).
3. Enter the transponder's local IP address (192.168.100.1), or the DHCP assigned IP address, into the web browser's address field.
4. The DM31 transponder's web server Overview page will appear (see below). **Note:** when the DM31 transponder first powers up, the web page is not available until several seconds after the DS LED begins to blink.

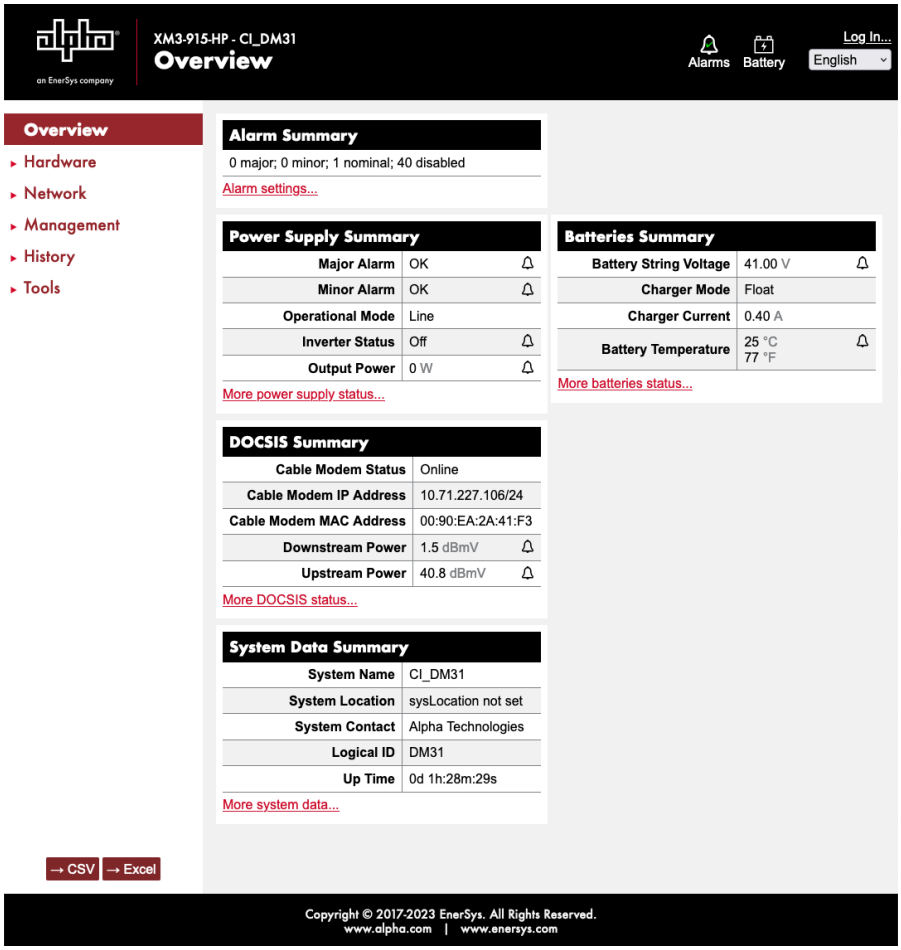


Fig. 4-1, Overview Web Page

NOTICE:

If you are unable to view the Overview page of the DM31 transponder using IP address 192.168.100.1, the network configuration on the computer that is being used to connect to the DM31 transponder may require a temporary static IP address (192.168.100.2) to be configured.

Use the following procedure to configure a static IP address on a laptop or computer with the Windows® operating system:

1. Go to the Network Connections screen. Depending upon your version of Windows®, you may be able to type "network connections" in the search box at the bottom of your screen, or by choosing "Change adapter options" from the Network & Internet page of Settings.
2. Right-click "Ethernet" (or whichever network device name represents your computer's local Ethernet network adapter). From the context menu, select "Properties." You will see a dialog box similar to **Fig. 4-2, Local Area Connection Properties Screen, Windows® 10**.
3. Click "Internet Protocol Version 4 (TCP/IPv4)" and then click the Properties button.
4. The "Internet Protocol Version 4 (TCP/IPv4) Properties" dialog box will open (**Fig. 4-3, Internet Protocol (TCP/IP) Properties Screen, Windows® 10**). (Record the existing IP address and Subnet mask in order to later return the computer to its original state.) Select "Use the following IP address". Enter the values shown: IP address 192.168.100.2 and Subnet mask 255.255.255.0.
5. Click the OK button. Try connecting to the DM31 transponder again using 192.168.100.1 in the web browser.

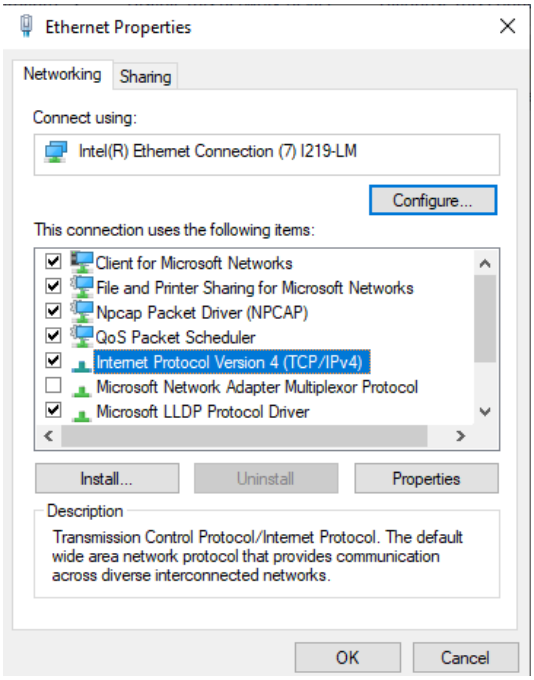


Fig. 4-2, Local Area Connection Properties Screen, Windows® 10

4.2 Remote Web Server Access

To remotely access the DM31 transponder web server utilizing a web browser, use the following procedure:

NOTICE:

For web server (HTTP) access, port 80 must not be blocked, and the computer must have access to the same network as the power supply IP address.

1. Connect the laptop or computer's network interface port to the company's Ethernet network.
2. Launch a web browser (Chrome™, Edge®, etc.).
3. Enter the DM31 transponder's DHCP designated IP address (e.g., 192.168.1.124) into the web browser's address field. Use square brackets when entering IPv6 IP addresses (e.g. [fc00:168:40::124]) into the web browser's address field.
4. The DM31 transponder's web server Overview page will appear (**Fig. 4-1, Overview Web Page**).

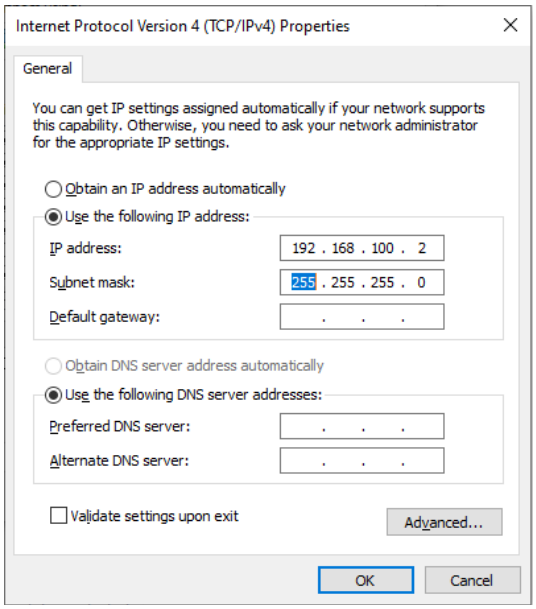


Fig. 4-3, Internet Protocol (TCP/IP) Properties Screen, Windows® 10

4.3 Navigating the Web Pages

Once the DM31 transponder web page has been successfully accessed, the operator is able to select various pages of information, enabling real-time data to be observed. The web pages share common features, highlighted below.

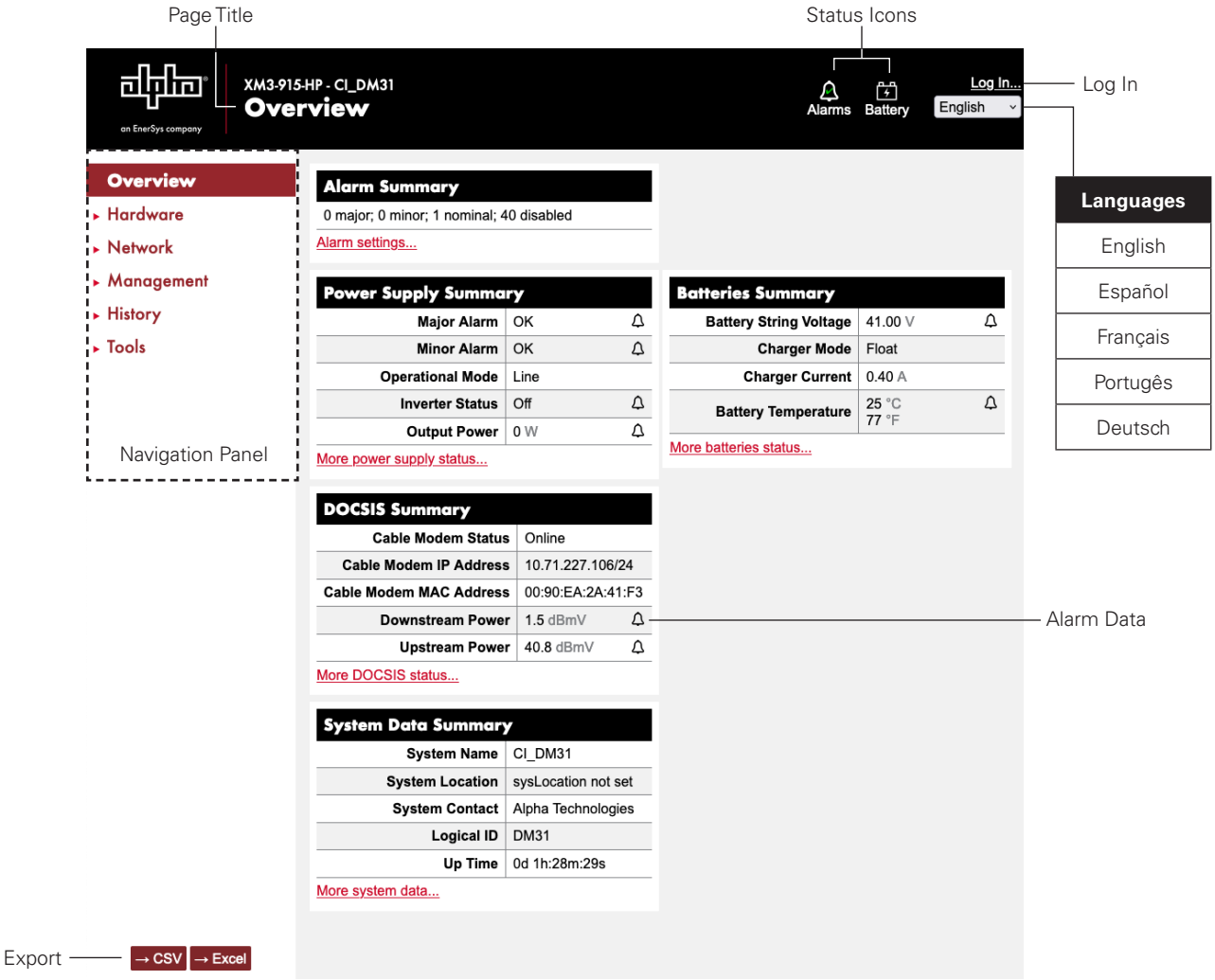


Fig. 4-4, Web Page Features

- **Page Title** displays which web page you are viewing, as selected from the navigation panel area.
- **Status Icons** show you, at a glance, if there are alarm conditions and the state of the battery system.
- **Log In** link allows you to access restricted features, with the correct credentials.
- **Languages** allows you to view the web pages in your choice of English, Spanish, Portuguese, French or German. By default, the web page uses the same language selected on the XM3-HP™ power supply front panel.
- **Navigation Panel** allows you to quickly switch to other pages. Click on a category (Network, Management, etc.) to select from the available pages in that category.
- **Alarm Data** is those values which can report alarms to the network management system (NMS). Click on the bell icon to view (and possibly edit) the alarm settings.
- **Export** the contents of the page to a text file (CSV format) or an Excel® spreadsheet.

The following list provides a summary of each of the web pages:

Overview: Provides a summary of information on alarms, the power supply, batteries, DOCSIS®, and system data.

Hardware

Power Supply: Displays power supply information as well as input, output and inverter information. Self-tests may also be performed from this page.

Batteries: Displays battery information and configuration, as well as the charger system status.

Environmental I/O: Status and configuration of tamper polarity and external devices connected to the ENV port.

Components: Displays information on major components of the power supply system (EMM, transformer, etc.) and temperature readings.

Network

DOCSIS: Provides real-time DOCSIS information such as upstream and downstream channels and network configuration.

RF Attenuation: Displays internal downstream power level adjustments. Log in to control the attenuation level.

Ethernet: Displays configuration information for the ETH port, and lists devices connected to it.

Advanced

Interfaces: Displays a summary of network interface status and addresses, and communications health monitoring controls.

Network Services: Manages which network service are permitted on the transponder.

Management

System Data: Configure and view the transponder's system status. The power supply system may be reset or restored to factory settings from this page, and system diagnostic information can be downloaded.

SNMP: Display SNMP (Simple Network Management Protocol) settings and trap destinations. Log in to change settings.

Alarms: View and configure all of the power supply system alarms.

Utility Power: View utility power status and past events.

History

Power Supply Events: View recorded power supply system events.

Power Supply Configuration: View recorded changes to the power supply's configurations.

Battery Events: View recorded battery events.

Modem Log: View recorded DOCSIS modem events.

Network System Log: Lists a record of login and logout events to the network.

Network Event Log: Lists a record of network related events such as provisioning.

Firewall Log: Lists recorded events pertaining to potential breaches in the firewall or changes to firewall settings.

Alarm Log: Displays recorded alarm events.

Tools

Spectrum: Display and analyze a detailed, full-band capture analysis of the DOCSIS® channels as seen by the transponder. This tool assists in identifying and troubleshooting common impairments throughout the range of DOCSIS channels.

Microreflections: Displays details about impairments on the DOCSIS network and the approximate distance(s) of the impairment(s). This tool requires the Adaptive Equalization function to be enabled on the CMTS.

Firmware Update: The power supply's firmware can be remotely updated by directly uploading the latest firmware, or update via TFTP. (Only visible when logged in with administrative privilege.) This should generally only be used as directed by Alpha® technical support.

4.3.1 Web Interface Security

The web page of the DM31 transponder provides tools for power supply and network diagnostics. Accessing some web interface features require additional security access.

Depending upon how your DM31 transponder is configured (see **Section 3.4 Setting Communication Options**), the initial web page may be set to one of five levels of access:

- **No Access** - the Overview page is the only information you can see without logging in
- **View** - you can see most information, but viewing some information or making changes requires a login
- **View All** - you can see all information, but making changes requires a login
- **Edit** - you can see all information, and make changes to common technician settings
- **Edit All** - you can see all information, and make changes to more advanced technician settings

With appropriate credentials, the operator can log in to the DM31 transponder web page to switch to one of the higher levels of access.

To log in, click the **Log In** link in the upper right corner of the web page. When prompted, enter the user name and password. Both are case-sensitive. If the credentials are accepted, the web page displays the additional information and/or capabilities.

The default credentials for the DM31 transponder are:

- **No log in** = provides View All access; everything is read-only.
- **User name:** Alpha / **Password:** AlphaGet = provides Edit access (see all information, make changes to common technician settings)
- **User name:** Admin / **Password:** AlphaSet = provides Edit All access (see all information, make changes to more advanced technician settings)

These credentials may be changed for a particular installation, and the DM31 transponder may be configured to use a Password of the Day system instead of a fixed password for a login.

4.4 Power Supply Page

The Hardware > Power Supply web page presents detailed information about the operation of the XM3-HP™ power supply.

In addition to the real-time status of the power supply, there are a number of configurable parameters that can be adjusted with the proper login. (Power supply parameters can also be adjusted through the Smart Display on the front of the power supply.)

4.4.1.1 Power Supply Self Tests

Remote Self Tests on power supplies may be started and stopped via the DM31 transponder web page. This requires a login with Edit permissions.

The Self Test section of the page shows the parameters for self tests, including the test interval and countdown for fully automatic self tests. A test interval of 0 indicates that the power supply does not perform automatic self tests.

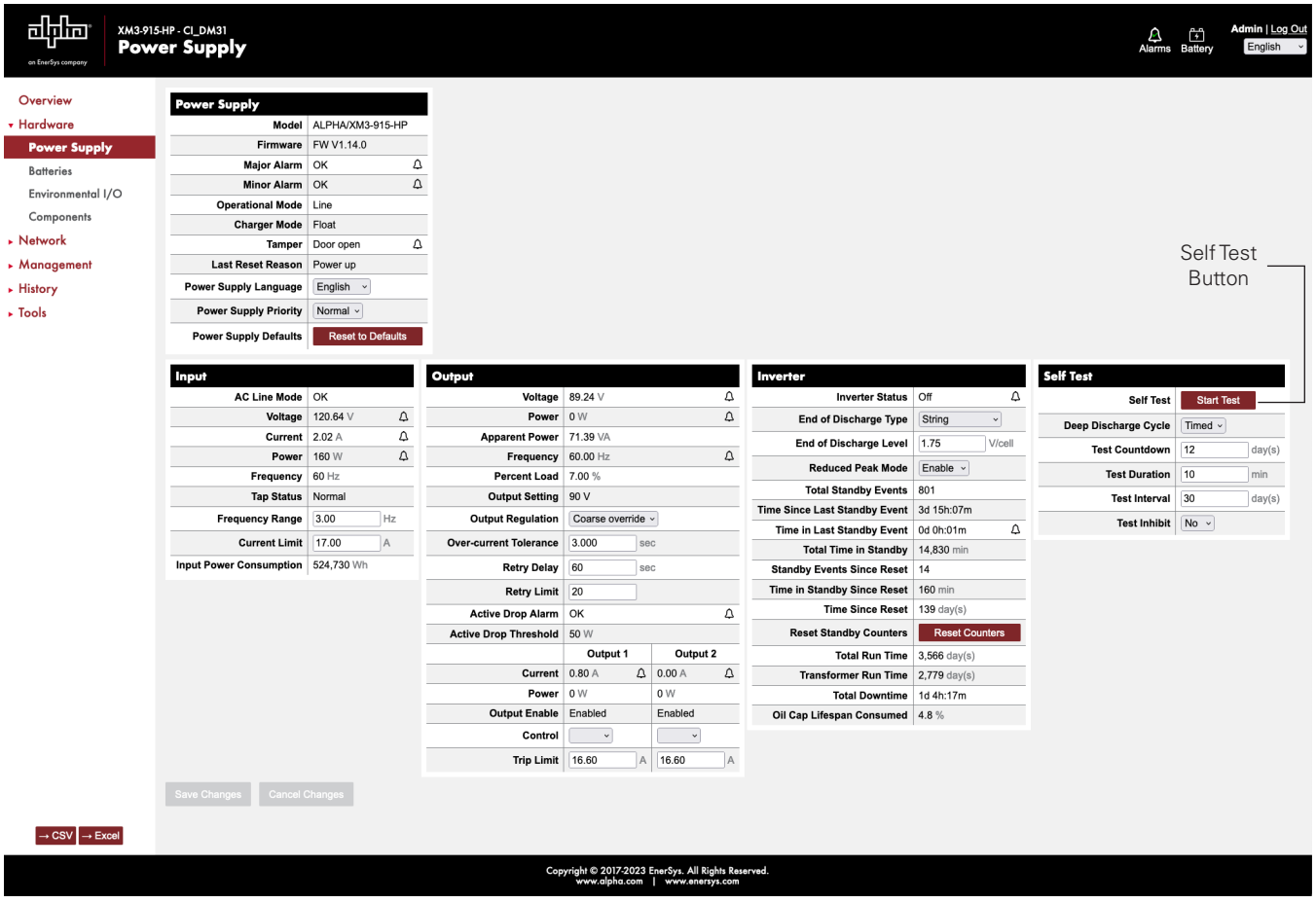


Fig. 4-5, Power Supply Web Page

To manually begin a power supply self test, click the Start Test button shown in Fig 4-5. If the power supply was running on AC line input, it will switch to running from batteries as if the utility power had failed. The web page will then display the time remaining on the test, which counts down as the test progresses. At the end of the test interval, the power supply switches back to utility power.

To interrupt a power supply self test, click the Stop Test button (displayed instead of Start Test while the test is running). The power supply switches back to utility power without completing the test interval.

4.4.1.2 Other Power Supply Controls

To reset an output that has shut off, open the pick list for the "Control" field in the Output section of the page and click on "Reset." Then, click the Save Changes button to apply this operation.

To reset the counters of standby events and time in standby since the last reset, click the Reset Counters button in the Inverter section of the page.

To reset the power supply's configurable parameters to the factory settings, click the Reset to Defaults button in the top section of the page. This function is only available when logged in with Edit All permission.

4.5 Batteries Page

The Hardware > Batteries web page presents configuration and status information for the power supply battery string(s).

The top section of the page, and the Battery Charging section, are the real-time status of the batteries. The Configuration section is primarily about what the power supply "knows" about the batteries in order to efficiently control their charging; select the appropriate type from the Battery Model list, where the battery model is listed, for the best results. The Conductance section is for recording conductance measurements on the batteries as well as the date of manufacture for each battery.

To configure the system for your battery, click the Battery Model drop down menu to view a selection of common battery models. If the installed battery model is not listed for your particular configuration, then select Other for the model type. Click the "Save Changes" button to save all edits.

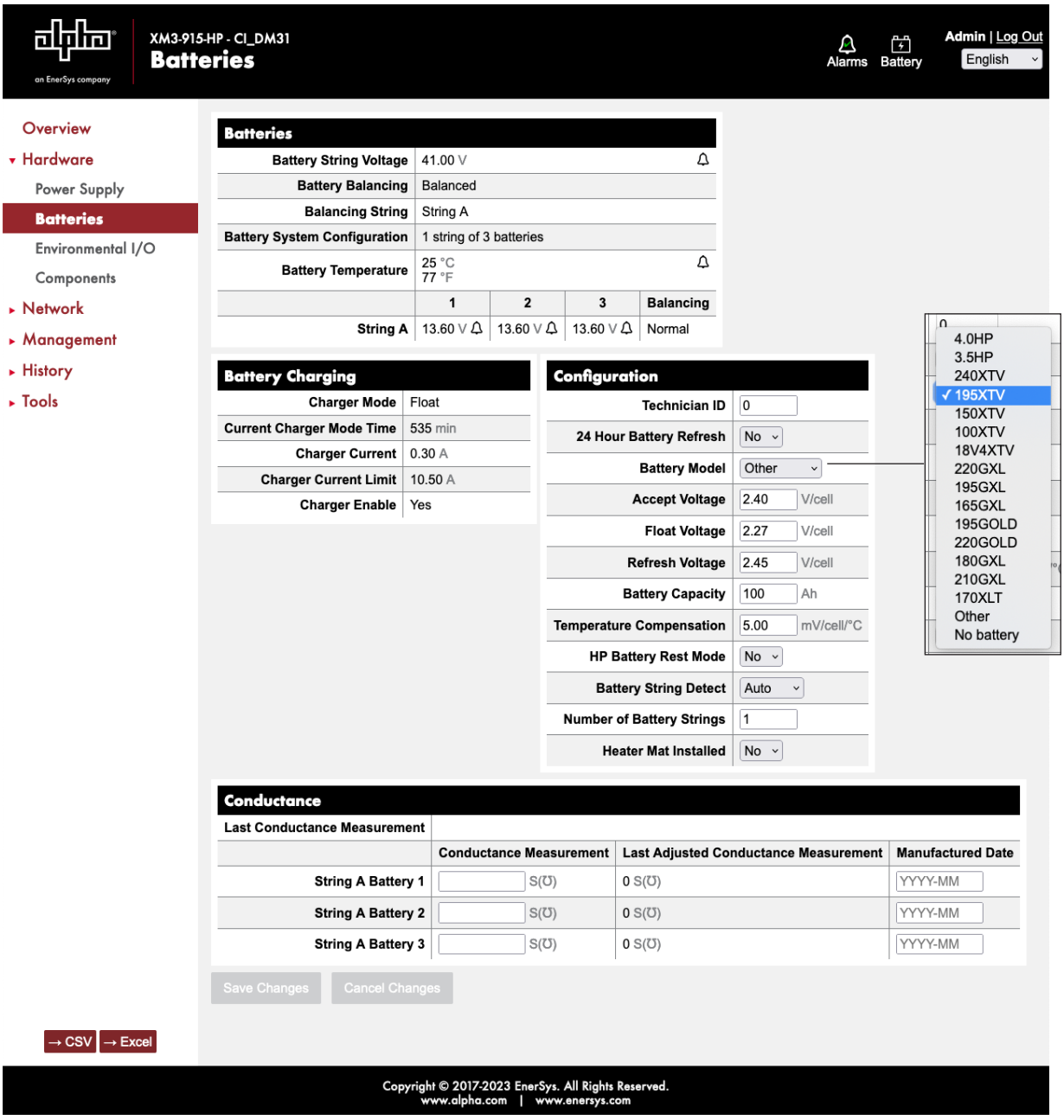


Fig. 4-6, Batteries Web Page

4.6 Firmware Update Page

The Tools > Firmware Update web page is only available when logged in with Edit All permission. This page displays the current major (DOCSIS®) firmware version, and provides several technician tools for updating the firmware of the DM31 transponder and/or XM3-HP™ power supply.

There are three ways to update firmware in a DM31 transponder/XM3-HP power supply system:

- **Direct Firmware Update:** Uploading a peripheral firmware file to the XM3-HP power supply directly through the web page. This only works for XM3-HP power supply updates, not for the DOCSIS firmware update of the DM31 transponder.
- **TFTP Firmware Update:** This requires that the update file(s) be stored on a network TFTP server. Enter the IP address of the server and the file name on that server. From the Download Control selection, choose Reprogram to update the XM3-HP power supply firmware files, or System Reprogram to update the DM31 transponder DOCSIS firmware. (The System Reprogram function is quite similar to the DOCSIS firmware upgrades described in **Section 5.1 Upgrading DM31 Transponder Modem Firmware**.)
- **Bundle Firmware Update:** The DM31 transponder also contains a "bundle" of XM3-HP power supply firmware files. If any of these XM3-HP power supply components are running a different version of firmware than the bundle, these show in yellow. The "Apply Bundled Firmware" button instructs the DM31 transponder to apply all of the bundled updates that are needed to make the XM3-HP power supply match the bundle.

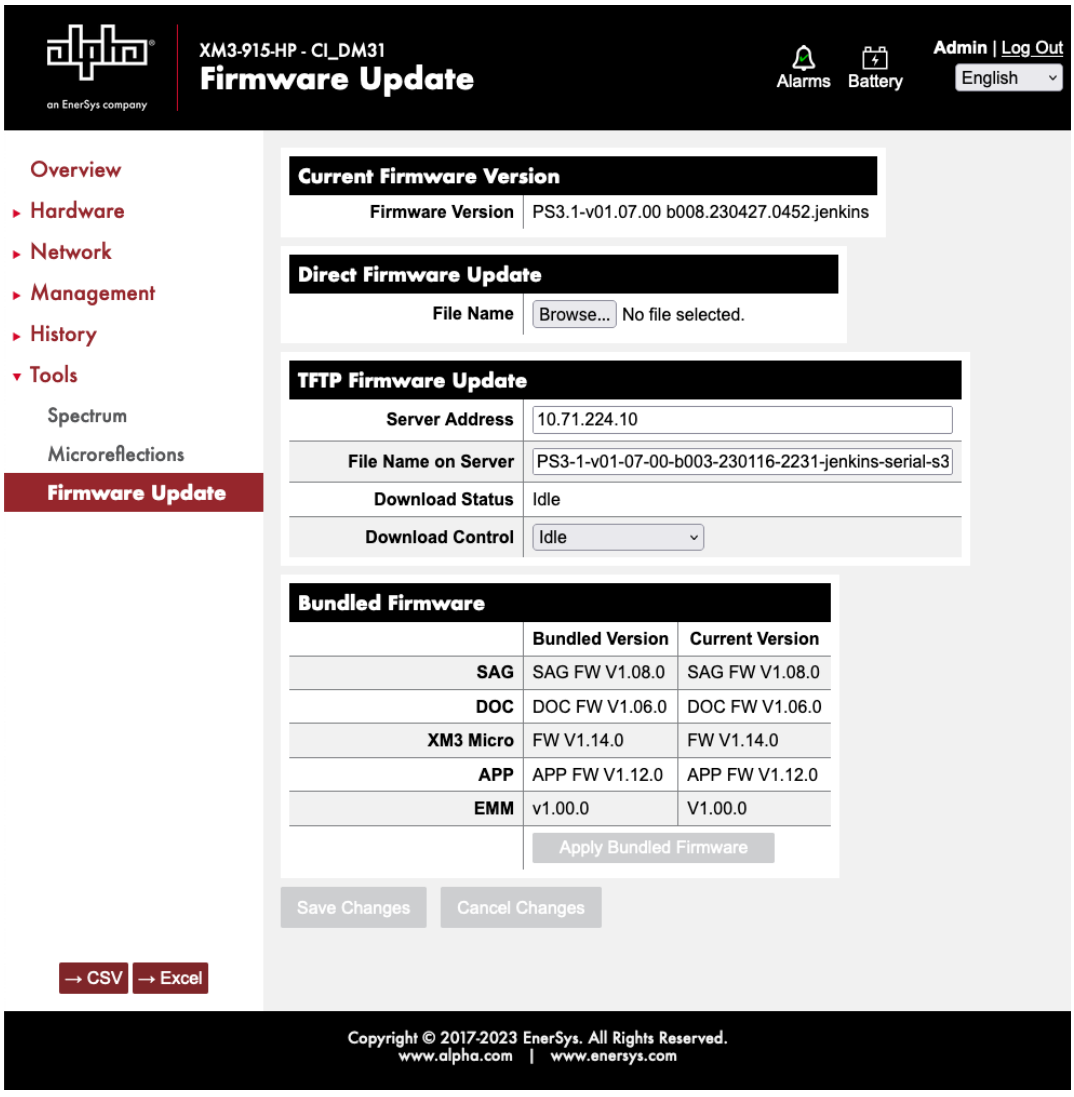


Fig. 4-7, Firmware Update Web Page

5.0 Upgrading Firmware

5.1 Upgrading DM31 Transponder Modem Firmware

The firmware is upgraded using standard DOCSIS® methods as defined in RFC4639. There are two ways to upgrade the modem's firmware: by directly setting the appropriate MIB parameters in the docsDevSoftware branch, or by including the appropriate SNMP parameters and values in the modem's DOCSIS configuration file, stored in the TFTP root directory. Both methods are explained below.

5.1.1 Identifying the Modem and Obtaining Firmware Files

The cable modem firmware in the DM31 transponder requires its own firmware and manufacturer's Code Verification Certificate (CVC file). Contact Alpha Technologies Services, Inc. to obtain the latest firmware and manufacturer's CVC files.

5.1.2 Modem Firmware Upgrade SNMP Parameters

Modem Firmware Upgrade SNMP Parameters		
Parameter	**Type**	**Value**
docsDevSwServer OID: 1.3.6.1.2.1.69.1.3.1.0	IP Address	The IP address of the TFTP server from which the firmware will be downloaded. This OID has been deprecated, refer to docsDevSwServerAddress (OID:1.3.6.1.2.1.69.1.3.7.0).
docDevSwFilename OID: 1.3.6.1.2.1.69.1.3.2.0	Octet String	Set to the filename of the firmware file. Example: ["firmwareImage.bin"]
docsDevSwAdminStatus OID: 1.3.6.1.2.1.69.1.3.3.0	Integer	1 = Initiate upgrade (manual method) 2 = Upgrade on next reboot (Config File Method) 3 = Ignore update
docsDevSwOperStatus OID: 1.3.6.1.2.1.69.1.3.4.0	Integer, Read Only	1 = TFTP download is in progress 2 = Last upgrade was performed at reboot 3 = Last upgrade was initiated by setting docsDevSwAdminStatus to "1" 4 = Firmware upgrade failed 5 = Other
docsDevSwCurrentVers OID: 1.3.6.1.2.1.69.1.3.5.0	Octet String, Read Only	The current version of firmware installed in the modem
docsDevSwServerAddressType 1.3.6.1.2.1.69.1.3.6.0	Integer, Read Only	The type of address (IPv4, IPv6) of server used for upgrades
docsDevSwServerAddress OID: 1.3.6.1.2.1.69.1.3.7.0	IP Address	The IP address of the server from which the firmware will be downloaded. A set of this object to an IPv4 address will result in also setting the value of docsDevSwServer to that address. If this object is set to an IPv6 address, docsDevSwServer is set to 0.0.0.0. If docsDevSwServer is set, this object is also set to that value.
docsDevSwServerTransportProtocol 1.3.6.1.2.1.69.1.3.8.0	Integer, Read Only	The Transport protocol to be used for software upgrades: 1 = TFTP 2 = HTTP

Table 5-1, Modem Firmware Upgrade SNMP Parameters

5.1.3 Upgrading Manually by Setting SNMP Parameters

1. Acquire the firmware and CVC files for your DM31 transponder from Alpha Technologies Services, Inc. Note that Alpha® provides two copies of the firmware, depending upon whether your configuration file uses DOCSIS® 3.1 code signing or earlier (DOCSIS® 3.0 and before) code signing. Select the appropriate file for your setup.
2. Import the CVC into the modem's DOCSIS configuration file (to create a configuration file, see **Section 3.3 DOCSIS® Configuration File**).
3. Set the following MIB parameters using an SNMP MIB browser. For additional information regarding the SNMP MIB parameters, refer to the table in **Section 5.1.2 Modem Firmware Upgrade SNMP Parameters**.

SNMP Parameters	
Parameter	**Value**
docsDevSwServerAddress OID:1.3.6.1.2.1.69.1.3.7.0	IP Address of theTFTP server (IPv4 or IPv6)
docsDevSwFilename OID:1.3.6.1.2.1.69.1.3.2.0	Firmware filename
docsDevSwAdminStatus OID: 1.3.6.1.2.1.69.1.3.3.0	1 (Initiate Upgrade)

Table 5-2, SNMP Parameters

The firmware upgrade will begin immediately. Monitor the upgrade status with the docsDevSwOperStatus MIB parameter, and verify the firmware version with the docsDevSwCurrentVers MIB parameter (refer to **Table 5-1, Modem Firmware Upgrade SNMP Parameters**). Once the firmware has been upgraded, the modem will automatically run the new version.

5.1.4 Upgrading via the DOCSIS Configuration File

1. Acquire the firmware and CVC files for your DM31 transponder from Alpha Technologies Services, Inc. Note that Alpha® provides two copies of the firmware, depending upon whether your configuration file uses DOCSIS® 3.1 code signing or earlier (DOCSIS® 3.0 and before) code signing. Select the appropriate file for your setup.
2. Import the CVC into the modem's DOCSIS configuration file (to create a configuration file, see **Section 3.3 DOCSIS® Configuration File**).

DM31 transponder firmware can be automatically upgraded using the DOCSIS configuration file by adding the following docsDevSoftware SNMP parameters and the manufacturer's Code Verification Certificate (CVC).

DOCSIS Configurations File Values	
Parameter	**Value**
docsDevSwServerAddress OID:1.3.6.1.2.1.69.1.3.7.0	IP Address of TFTP server
docsDevSwFilename OID:1.3.6.1.2.1.69.1.3.2.0	Firmware filename
docsDevSwAdminStatus OID: 1.3.6.1.2.1.69.1.3.3.0	2 (Upgrade on next reboot)
Manufacturer CVC TLV:32	The CVC file for the DM31 transponder (embed in the configuration file).

Table 5-3, DOCSIS Configurations File Values

The firmware will be upgraded on the next reset. Monitor the upgrade status with the docsDevSwOperStatus MIB parameter, and verify the firmware version with the docsDevSwCurrentVers MIB parameter (refer to Table 5-1, Modem Firmware Upgrade SNMP Parameters). Once the firmware has been upgraded, the modem will automatically run the new version.

5.2 Upgrading Power Supply Firmware

In addition to the DOCSIS® firmware updates described in the previous section, the DM31 transponder supports updating the firmware files for various components of the XM3-HP™ series power supply. Individual components can be manually updated from a file on a TFTP server or directly from a file on your computer. Additionally, the core modem firmware includes component firmware files "bundled" within it, and a simple SNMP operation can initiate the update.

5.2.1 Component Firmware Update Using TFTP

Component firmware files are identifiable with a ".afwu" file extension (for "Alpha FirmWare Update"). If the component file resides on a TFTP server, the DM31 transponder can be instructed to fetch and apply the update.

NOTICE:

Previous XM3-HP™ power supply transponders used a different file format for component updates. Only use the .afwu file type with the DM31 transponder.

- From SNMP, set atiMgmtSysDownloadTftpServerAddress to the address of the TFTP server, set atiMgmtSysDownloadFile to the name of the firmware file, and then set atiMgmtSysDownloadCtrl to reprogram(5) to initiate the transfer. (See **Table 5-4, Alpha Firmware Update Settings**.)
- If using the web page, log in with administrative rights, go to the Firmware Update page, fill in the "TFTP Firmware Update" section, including choosing "Reprogram" for Download Control, and click "Save Changes." (See **Fig. 4-7, Firmware Update Web Page**.)

If the transfer begins successfully, the download status (atiMgmtSysDownloadStatus in SNMP (also shown on the web page) will indicate downloading(10) while the file transfers from the TFTP server, then indicate programming(11) while the firmware update is in progress. When the operation is completed, the download status will then show a status of idle(1). If the transfer or the reprogramming DOES NOT succeed, the download status will report error(8) instead.

Alpha Firmware Update Settings			
Component	**Description**	**Default**	**Values**
atiMgmtSysDownloadTftpAddress 1.3.6.1.4.1.926.1.3.2.1.1	Address of download TFTP server Use atiMgmtSysDownloadTftpServerAddress instead to support both IPv4 and IPv6 servers.	0.0.0.0	Any valid IPv4 addresss
atiMgmtSysDownloadCtrl 1.3.6.1.4.1.926.1.3.2.1.2	Download Control	idle(3)	idle(3) abort(4) reprogram(5) systemReprogram(6)
atiMgmtSysDownloadStatus 1.3.6.1.4.1.926.1.3.2.1.3	Current Download Status	idle(3)	idle(1) error(8) downloading(10) programming(11)
atiMgmtSysDownloadFile 1.3.6.1.4.1.926.1.3.2.1.4	Download File Name		File name
atiMgmtSysDownloadTftpServerAddressType 1.3.6.1.4.1.926.1.3.2.1.15	Address mode of atiMgmtSysDownloadTftpServerAddress	unknown(0)	unknown(0) ipv4(1) ipv6(2)
atiMgmtSysDownloadTftpServerAddress 1.3.6.1.4.1.926.1.3.2.1.16	Address of download TFTP server		Any valid IPv4 or IPv6 address, as an octet string

Table 5-4, Alpha Firmware Update Settings

5.2.2 Component Firmware Update Using HTTP

If using the web page, there is an alternative method for updating component firmware directly from your computer.

1. Log in with administrative rights and go to the Firmware Update page (only visible when logged in).
2. In the "Direct Firmware Update" section at the top, click the "Browse" button to select the firmware file.
3. Click "Save Changes" to begin the transfer through a web browser. The page may take several seconds to respond, while sending the file, before indicating the update is occurring.

See **Fig. 4-7, Firmware Update Web Page**.

NOTICE:

This procedure does NOT work for the core modem firmware. Only the firmware file on your computer is needed, or a network location reachable from your computer (NOT necessarily reachable from the optical network).

5.2.3 Updating Components from Bundled Firmware

The core DM31 transponder firmware includes bundled versions of the latest component firmware files, as of the time when the core DOCSIS® firmware was released. This provides a simple way to sync up the firmware versions between the DM31 transponder and the XM3-HP™ power supply.

- From SNMP, set atiMgmtCfgFwBundleControl to updateNow(1) to initiate any needed updates. (See **Table 5-5, Bundled Firmware Settings**.)
- If using the web page, log in with administrative rights, go to the Firmware Update page, and click "Apply Bundled Firmware." (See **Fig. 4-7, Firmware Update Web Page**. If "Apply Bundled Firmware" is not enabled, no updates are required.)

Bundled Firmware Settings			
Component	**Description**	**Default**	**Values**
atiMgmtCfgFwBundleContent 1.3.6.1.4.1.926.1.3.3.4.2.1	Displays a string of the bundled components and versions that can be applied.		String of bundled components
atiMgmtCfgFwBundleUpdates 1.3.6.1.4.1.926.1.3.3.4.2.2	Determines whether bundled firmware is automatically applied when core (DOCSIS) firmware is updated. This setting is stored in non-volatile memory.	noAutoUpdate(1)	noAutoUpdate(1) autoUpdate(2)
atiMgmtCfgFwBundleControl 1.3.6.1.4.1.926.1.3.3.4.2.3	Controls manual application of the bundled firmware.	noAction(0)	noAction(0) updateNow(1)

Table 5-5, Bundled Firmware Settings

6.0 Data Management

6.1 SCTE-HMS MIBs

The DM31 transponder remotely reports power supply data and alarms using SNMP over the DOCSIS® communications standard. The DM31 transponder typically reports into a centralized Network Management System (NMS) through a standard collection of data access points referred to as the SCTE-HMS MIBs. The NMS polls the DM31 transponder for power supply data with the option of having the transponder send SNMP traps in the event that an alarm condition occurs.

The following MIB files are required for the NMS or SNMP Manager to collect data from the transponders. These files can be found on the Society of Cable Telecommunications Engineers® (SCTE®) website www.scte.org. There are dependencies between MIB files so they should be compiled in the order listed below:

SCTE-HMS MIB FIles	
Reference Number	**Description**
ANSI/SCTE 36 2002R2007 (formerly HMS 028)	SCTE-ROOT
ANSI/SCTE 37 2010 (formerly HMS 072)	SCTE-HMS-ROOTS
ANSI/SCTE 38-1 2009 (formerly HMS 026)	SCTE-HMS-PROPERTY-MIB
ANSI/SCTE 38-2 2005 (formerly HMS 023)	SCTE-HMS-ALARMS-MIB
ANSI/SCTE 38-3 2008 (formerly HMS 024)	SCTE-HMS-COMMON-MIB
ANSI/SCTE 38-4 2006 (formerly HMS 027)	SCTE-HMS-PS-MIB
ANSI/SCTE 38-7 2008 (formerly HMS 050)	SCTE-HMS-TIB-MIB

Table 6-1, SCTE-HMS MIB Files

6.2 SCTE-HMS MIB Alarms

6.2.1 SCTE-HMS Configurable Alarms

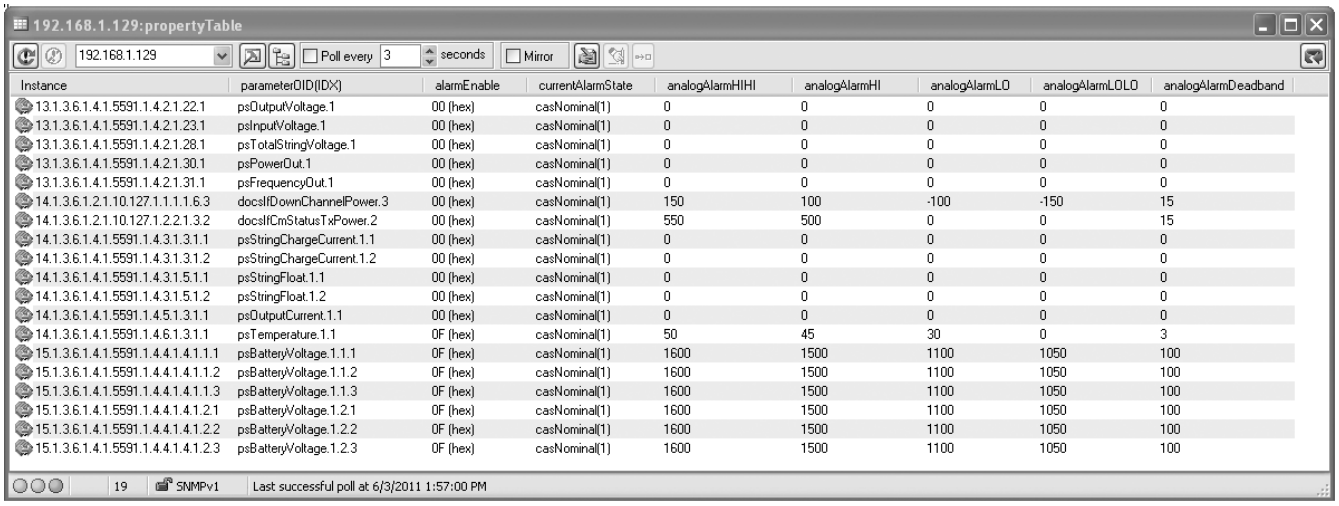
The HMS discrete and analog alarms provide the capability to monitor and alarm various power supply and environmental conditions and measurements. The alarms in the SCTE-HMS propertyTable and the discretePropertyTable can be defined and set to provide a customized monitoring system.

The following section provides an example and detailed information on how to set values and enable or disable alarms in the MIB tables. For ease of reference they are in this sequence:

- An example of how to set a temperature alarm.
- A table to help convert the desired reported alarm states to hexadecimal for setting the MIB.
- Commonly monitored parameters and recommended values.

Example:

The alarms for psTemperature are set so that the normal temperature range is from 30°C to 45°C. If the temperature rises above 45°C, a casHI alarm will be sent to the alarmTable. Anything over 50°C is considered a critical condition and will generate a casHIHI alarm. If the temperature falls below the normal level of 30°C, casLO will be generated and if it continues to drop below 0, a casLOLO will be generated. The temperature must rise above the LOLO limit plus the deadband value of 3°C before the casLOLO alarm will change to a casLO. The alarmEnable field is set to 0F Hex to monitor and alarm for all conditions.



Instance	parameterOID(IDX)	alarmEnable	currentAlarmState	analogAlarmHIHI	analogAlarmHI	analogAlarmLO	analogAlarmLOLO	analogAlarmDeadband
13.1.3.6.1.4.1.5591.1.4.2.1.22.1	psOutputVoltage.1	00 (hex)	casNominal(1)	0	0	0	0	0
13.1.3.6.1.4.1.5591.1.4.2.1.23.1	psInputVoltage.1	00 (hex)	casNominal(1)	0	0	0	0	0
13.1.3.6.1.4.1.5591.1.4.2.1.28.1	psTotalStringVoltage.1	00 (hex)	casNominal(1)	0	0	0	0	0
13.1.3.6.1.4.1.5591.1.4.2.1.30.1	psPowerOut.1	00 (hex)	casNominal(1)	0	0	0	0	0
13.1.3.6.1.4.1.5591.1.4.2.1.31.1	psFrequencyOut.1	00 (hex)	casNominal(1)	0	0	0	0	0
14.1.3.6.1.2.1.10.127.1.1.1.1.6.3	docsIfDownChannelPower.3	00 (hex)	casNominal(1)	150	100	-100	-150	15
14.1.3.6.1.2.1.10.127.1.2.2.1.3.2	docsIfCmStatusTxPower.2	00 (hex)	casNominal(1)	550	500	0	0	15
14.1.3.6.1.4.1.5591.1.4.3.1.3.1.1	psStringChargeCurrent.1.1	00 (hex)	casNominal(1)	0	0	0	0	0
14.1.3.6.1.4.1.5591.1.4.3.1.3.1.2	psStringChargeCurrent.1.2	00 (hex)	casNominal(1)	0	0	0	0	0
14.1.3.6.1.4.1.5591.1.4.3.1.5.1.1	psStringFloat.1.1	00 (hex)	casNominal(1)	0	0	0	0	0
14.1.3.6.1.4.1.5591.1.4.3.1.5.1.2	psStringFloat.1.2	00 (hex)	casNominal(1)	0	0	0	0	0
14.1.3.6.1.4.1.5591.1.4.5.1.3.1.1	psOutputCurrent.1.1	00 (hex)	casNominal(1)	0	0	0	0	0
14.1.3.6.1.4.1.5591.1.4.6.1.3.1.1	psTemperature.1.1	0F (hex)	casNominal(1)	50	45	30	0	3
15.1.3.6.1.4.1.5591.1.4.4.1.4.1.1.1	psBatteryVoltage.1.1.1	0F (hex)	casNominal(1)	1600	1500	1100	1050	100
15.1.3.6.1.4.1.5591.1.4.4.1.4.1.1.2	psBatteryVoltage.1.1.2	0F (hex)	casNominal(1)	1600	1500	1100	1050	100
15.1.3.6.1.4.1.5591.1.4.4.1.4.1.1.3	psBatteryVoltage.1.1.3	0F (hex)	casNominal(1)	1600	1500	1100	1050	100
15.1.3.6.1.4.1.5591.1.4.4.1.4.1.2.1	psBatteryVoltage.1.2.1	0F (hex)	casNominal(1)	1600	1500	1100	1050	100
15.1.3.6.1.4.1.5591.1.4.4.1.4.1.2.2	psBatteryVoltage.1.2.2	0F (hex)	casNominal(1)	1600	1500	1100	1050	100
15.1.3.6.1.4.1.5591.1.4.4.1.4.1.2.3	psBatteryVoltage.1.2.3	0F (hex)	casNominal(1)	1600	1500	1100	1050	100

Binary to Hex Conversions for Alarm Settings									
Unused				HiHi	Hi	Lo	LoLo	Hex	Enabled Alarms
Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0		
0	0	0	0	0	0	0	0	00	No Alarms
0	0	0	0	0	0	0	1	01	LoLo
0	0	0	0	0	0	1	0	02	Lo
0	0	0	0	0	0	1	1	03	Lo, LoLo
0	0	0	0	0	1	0	0	04	Hi
0	0	0	0	0	1	0	1	05	Hi, LoLo
0	0	0	0	0	1	1	0	06	Hi, Lo
0	0	0	0	0	1	1	1	07	Hi, Lo, LoLo
0	0	0	0	1	0	0	0	08	HiHi
0	0	0	0	1	0	0	1	09	HiHi, LoLo
0	0	0	0	1	0	1	0	0A	HiHi, Lo
0	0	0	0	1	0	1	1	0B	HiHI, Lo, LoLo
0	0	0	0	1	1	0	0	0C	HiHi, Hi
0	0	0	0	1	1	0	1	0D	HiHi, Hi, LoLo
0	0	0	0	1	1	1	0	0E	HiHi, Hi, Lo
0	0	0	0	1	1	1	1	0F	HiHi, Hi, Lo, LoLo

Table 6-2, Binary to Hex Conversions for Alarm Settings

The following table displays various analog alarms with common settings for the DM31 transponder.

Analog Alarms and Common Settings								
Analog Alarms		**Description**	**Alarm Enable**	**LOLO**	**LO**	**HI**	**HIHI**	**Deadband**
psTotalStringVoltage	36V	Scaled representation of the full battery string in 1/100 Volts units	0x0F	3300	3500	4520	4570	50
Individual Battery Voltage		Battery Voltage of 12V Battery in 1/100 Volts units	0x0F	1050	1150	1530	1550	20
psInputVoltage	120V	Scaled representation of the input line voltage in 1/100 Volts units	0x0F	Varies by site. The XM3-HP™ power supply will switch to standby at nominal +15% / -30%				
	220V		0x0F					
psRMSCurrentIn		Scaled representation of the Power Supply's RMS curent in 1/100 A units	0x00	Set as desired per site				
psPowerIn		Representation of the Power Supply's input power in 1 W units	0x00	Set as desired per site				
psFrequencyOut		Representation of Power Supply's output frequency in 1/100 Hz units	0x00	Set as desired per site				
psOutputVoltage		Scaled representation of the Power Supply output voltage in 1/100 Volts units	0x0F	4300	4550	5050	5300	200
			0x0F	5650	6000	6600	7000	200
			0x0F	7800	8200	9150	9300	200
psPowerOut		Representation of Power Supply output power in 1W units	0x00	It is recommended that psOutputCurrent be used for output alarms.				
psStringChargeCurrent		Battery string charge current, scaled in 1/100 Amp units	0x0C	Disable	Disable	1200	1250	20
psStringDischargeCurrent		Scaled representation of battery string discharge current. This is an RMS value in 1/100 Amps	0x00	Set as desired per site				
psStringFloat		Battery string float charge current, scaled in 1/100 Amp units	0x0C	Disable	Disable	1200	1250	20
psOutputCurrent	15A	Scaled representation of Power Supply RMS currnt in 1/100 Amp units	0x0C	Disable	Disable	1650	1720	20
	18A		0x0C	Disable	Disable	1980	2060	20
psTemperature		-40 to +80 degrees C	0x0F	Varies by Site				
docsIfDownChannelPower		The CM's receive RF power scaled in 1/10 dBmV units	0x0F	-150	-10	10	150	15
docsIfCmStatusTxPower		The CM's transmit RF power scaled in 1/10 dBmV units	0x0C	0	0	500	550	15
atiBBsysViewTimeInStandby		Time in seconds that the Power Supply's inverter is currently running due to outage or self test	0x0C	0	0	Set as desired for notification of extended outage		10

Table 6-3, Example Settings for DM31 Transponder Analog Alarms

Example Settings for Discrete Alarms		
Discrete Alarms	**Description**	**Setting**
psInverterStatus (1)	Inverter Off	Disable
psInverterStatus (2)	Inverter Running Due to Loss of AC Line Voltage	discreteMinor
psInverterStatus (3)	Self Test Initiated Locally	Disable
psInverterStatus (4)	Self Test Initiated Remotely	Disable
psInverterStatus (5)	Last Self Test Failed	Disable
psMajorAlarm (1)	No Alarm	Disable
psMajorAlarm (2)	Alarm	discreteMajor
psMinorAlarm (1)	No Alarm	Disable
psMinorAlarm (2)	Alarm	discreteMinor
psTamper (1)	Closed	Disable
psTamper (2)	Open	discreteMajor
psInputVoltagePresence (1)	AC Line Voltage Lost	Disable
psInputVoltagePresence (2)	AC Line Voltage Present	Disable
Battery Standby Time Remaining (1)	Over 3 Hours Remaining	Disable
Battery Standby Time Remaining (2)	2 to 3 Hours Remaining	Disable
Battery Standby Time Remaining (3)	1 to 2 Hours Remaining	discreteMinor
Battery Standby Time Remaining (4)	Less than1 Hour Remaining	discreteMajor
Battery Standby Time Remaining (5)	Calculating	Disable
Battery Standby Time Remaining (6)	Not Available	Disable
tibControlMode (2)	Device is Under Local Control	Disable
tibControlMode (3)	Remote Device is Not Responding	discreteMajor
atiMgmtSysIoPinCtrl (1)	Contact Open	Disable
atiMgmtSysIoPinCtrl (2)	Contact Closed	Disable
atiMgmtSysIoPinIn4 (1)	Contact Open	Disable
atiMgmtSysIoPinIn4 (2)	Contact Closed	Disable
atiMgmtSysIoPinIn5 (1)	Contact Open	Disable
atiMgmtSysIoPinIn5 (2)	Contact Closed	Disable
atiMgmtSysIoPinIn6 (1)	Contact Open	Disable
atiMgmtSysIoPinIn6 (2)	Contact Closed	Disable

Table 6-4, Example Settings for Discrete Alarms

6.2.2 SNMP Traps

Use of SNMP traps allows the network manager to set conditions (alarms) under which the device autonomously reports to the headend the existence of the pre-configured event. The type of event determines the level of action to be taken.

1. Verify the IP address of the trap destination server(s) has been configured.
   - If the trap destination server requires configuration, refer to **Section 3.3.3 Setting SNMP Trap Destination Addresses - docsDevNmAccess Method (Deprecated; IPv4 Only)**, and **Section 3.3.4 Setting SNMP Trap Destination Addresses - Coexistence Method**, for instructions.

2. Alarms must be configured. SNMP alarm traps sent by the transponder are formatted according to the SCTE-HMS-ALARM-MIB specification with the following information included:
   - SNMP Trap community string:
   - commonTrapCommunityString, OID 1.3.6.1.4.1.5591.1.3.1.11.0
   - Default value is "public"

Example Alarm Trap:

The example below is a psTamper alarm trap indicating a discreteMinor alarm: Tamper is open. Data from the raw trap will appear as shown below. Refer to **Table 6-5, SNMP Alarm Trap Varbinds and Explanations**, for definitions of the varbinds.

Frame 441 (230 bytes on wire, 230 bytes captured)

Ethernet II, Src: 192.168.1.77 (00:90:EA:A0:01:4E), Dst: 3com_0d:1d:d4 (00:10:5a:0dL1d:d4)

Internet Protocol, Src Port: 62481 (62481), Dst Port: snmptrap (162)

Simple Network Management Protocol

Version: 1 (0)

Community: PUBLIC

PDU type: TRAP-V1 (4)

Enterprise: 1.3.6.1.4.1.5591.1 (SNMPv2-SMI::enterprises.5591.1)

Agent address: 0.0.0.0 (0.0.0.0)

Trap type: ENTERPRISE SPECIFIC (6)

Specific trap type: 1

Timestamp: 2358751

Object identifier 1: 1.3.6.1.4.1.5591.1.3.2.7.0 (SNMPv2-SMI::enterprises.5591.1.3.2.7.0)

Value: Hex-STRING: 00 90 EA A0 0B 82

Object identifier 2: 1.3.6.1.4.1.5591.1.3.1.1.0 (SNMPv2-SMI::enterprises.5591.1.3.2.1.0)

Value STRING: "123 Example Ave."

Object identifier 3: 1.3.6.1.4.1.5591.1.2.3.1.2.1 (SNMPv2-SMI::enterprises.5591.1.2.3.1.2.1)

Value: Hex-STRING: 00 00 00 76 07 10 06 0D 2B 06 01 04 01 AB 57 01 04 02 01 1B 01 02 01 02

Object identifier 4: 1.3.6.1.4.1.5591.1.4.2.1.27.1 (SNMPv2-SMI::enterprises.5591.1.3.2.1.0)

Value: INTEGER: 2

Object identifier 5: 1.3.6.1.4.1.5591.1.1.2.1.2 (SNMPv2-SMI::enterprises.5591.1.1.2.1.2)

Value: INTEGER: 7

When viewed through a third-party trap receiver, the translated varbinds and data values will be displayed in a format similar to the sample below:

Bindings (5)

Binding #1: commonPhysAddress.0 *** (octets) 00:90.EA.A0.01.4E (hex)

Binding #2: commonLogicalID.0 *** (octets) (123 Example Ave.)

Binding #3: alarmLogInformation.1 *** (octets) 00.00.00.76.07.10.06.0D.2B.06.01.04.01.AB.57.01.04.02.01.1B.01.02.01.02 (hex)

Binding #4: psTamper.1 *** (int32) open (2)

Binding #5: currentAlarmAlarmState *** (int32) caasDiscreteMinor(7)

SNMP Alarm Trap Varbinds and Explanations	
Varbind	**Explanation**
Binding #1 commonPhysAddress OID: 1.3.6.1.4.1.5591.1.3.2.7.0	MAC address of the Communications Module
Binding #2 commonLogicalID OID: 1.3.6.1.4.1.5591.1.3.1.1.0	Optional user-configurable parameter that is often used to provide a unique logical name, or even the physical address of where the Communications Module is installed.
Binding #3 alarmLogInformation OID: 1.3.6.1.4.1.5591.1.2.3.1.2.1	This varbind was designed by the SCTE-HMS committee with the intention of being used by sophisticated trap interpreters. The information is "coded" within the octet strings: Octet 1-4: POSIX Time of alarm occurrence (most significant byte first) Octet 5: Alarm Type (See description below) Octet 6: Contents of commonNeStatus immediately after alarm occurred Octet 7-m: Alarm Object Identifier (BER encoded) Octet n-z: Alarm value (BER encoded) Most trap interpreters cannot decode this message, which is why varbinds 4 and 5 were added that provide the same information in a more usable format.
Binding #4 Alarmed Parameter OID/Value OID: 1.3.6.1.4.1.5591.1.4.2.1.27.1	This field provides the varbind of the parameter that is alarming along with the value of that parameter. This is the same information encoded in varbind #3 Octets 7 through Z. In the example above the value would be: OID: 1.3.6.1.4.1.5591.1.4.2.1.27.1.0 (psTamper) Value: 2 (Open)
Binding #5 Alarm Location/Type OID: 1.3.6.1.4.1.5591.1.1.2.1.2	This is the information from varbind #3 Octet 5 above. The alarm location will always be the SCTE-HMS currentAlarmAlarmState and the type will be determined based on how the alarm was configured in the SCTE-HMS PropertyIdent MIB tables. OID 1.3.6.1.4.1.5591.1.1.2.1.2.0 (currentAlarmAlarmState) Type: 1-7 based on SCTE definitions: 1 NOMINAL 2 HIHI 3 HI 4 LO 5 LOLO 6 Discrete Major 7 Discrete Minor The Type will be determined by how the alarm is configured in the SCTE-HMS PropertyIdent MIB, whether it is a Discrete or Analog alarm and the level of alarm defined for that state.

Table 6-5, SNMP Alarm Trap Varbinds and Explanations

Trap on Normal

The DM31 transponder has the capability of sending a "return to normal" trap once an alarmed condition returns to a normal state. This feature is enabled by default, but can be disabled by setting the TRAP ON NORMAL parameter in the the MIB point atiMgmtSnmpTrapOnNormal to a value of "2". The contents of this trap message will be identical to the SNMP Alarm traps, but the value of the Alarm Type defined in the 5th varbind will be "1" (NOMINAL).

SCTE-HMS Warm-Start Trap

In addition to the SNMP alarm traps, the DM31 transponder will also send an SCTE-HMS warm-start trap when it is initialized. Some SNMP monitoring software requires this trap for auto-identification of the transponder. The format of this trap will be similar to the alarm trap, but the only information sent will be:

- commonTrapCommunityString, OID 1.3.6.1.4.1.5591.1.3.1.11.0
- commonPhyAddress, OID, 1.3.6.1.4.1.5591.1.3.2.7
- commonLogicalID, OID 1.3.6.1.4.1.5591.1.3.1.1.0

SCTE-HMS Cold-Start Trap

An SNMP-HMS cold-start trap will be generated by the DM31 transponder anytime it initializes with a new firmware version. In addition, a cold-start trap is sent whenever the configuration has changed. If any parameter in the HMS PROPERTY table has changed since the last reset, a cold-start trap will be sent upon the next reset.

6.2.3 SNMP Timeout Watchdog

If no SNMP communications has been detected within the time window set in the MIB atiMgmtSysSnmpTimeout (1.3.6.1.4.1.926.1.3.1.5.3), the modem will reboot. The default value for the DM31 transponder is 240 minutes (four hours). Set to 0 for "timeout disabled."

6.2.4 General Power Supply Alarms

The power supply detects a wide array of alarms, and displays the type of active alarm in the Smart Display screen and the severity of alarm (e.g., Major/Minor) by means of the inverter module LEDs.

General power supply alarms are passed directly from the power supply to the transponder without specific definition and are classified in the HMS MIB table as psMinorAlarm and psMajorAlarm. There are a number of problems that can generate these alarms and the exact nature of the situation is not specified. Minor and Major alarms are defined by the SCTE standards committee as follows:

psMajor

"Service has been dropped or a service interruption is imminent" indicates that an immediate truck roll is appropriate. Several psMajor alarms are latching, meaning that the alarm won't clear until the problem is fixed and after a successful completion of a Self Test. A Self Test is the preferred method of verifying the resolution of the alarm condition as cycling the power has the potential of masking the problem and not indicating the actual state of the system.

psMinor

"A non-service affecting condition has occurred and should be monitored."

The following table lists psMajor and psMinor alarm definitions for Alpha® power supplies.

Power Alarms: Classifications, Causes and Corrections				
Active Alarm	**Alarm Type**	**Probable Cause of Alarm**	**Corrective Action**	**Standby Disabled**
Self Test FAIL	Major	Output voltage failed, batteries less than 1.85V/C, or main AC interruption during Self Test.	1. Check Batteries 2. Check Inverter	NO
LINE ISOLATION	Major	Line isolation has failed and Inverter operations are suspended.	1. Replace Power Supply as soon as possible	YES
OUTPUT FAILURE	Major	The AC output has failed due to a bad Inverter or transformer.	1. Apply load >1.5A 2. Output Overloaded 3. Check Inverter	NO
OUTPUT OVERLOAD	Major	The output is overloaded or shorted.	1. Output Short Circuit 2. Check Output Current	NO
OUTPUT 1 TRIPPED	Major	Output 1 PIM hardware protection mode is engaged and overloaded.	1. Over Current 2. Check Settings	NO
OUTPUT 2 TRIPPED	Major	Output 2 PIM hardware protection mode is engaged and overloaded.	1. Over Current 2. Check Settings	NO
CHARGER FAILURE	Major	Charger has failed to shut down; possible battery over temperature condition exists.	1. Re-seat Inverter 2. Perform Self Test	NO
INVERTER TEMP	Major	Inverter heat sink has exceeded set temperature. (Stand-by operations suspended until temperature drops to a safe level.)	1. Check Inverter 2. Check PDB 3. Check Enclosure Ventilation	NO
CONFIG ERROR	Major	The Power Supply is improperly configured and operation is suspended until error is corrected.	1. Wrong Input Voltage or Frequency	NO
INVERTER ALARM / INVERTER FAILED	Major	No output detected with good batteries for 30 seconds OR inverter is disconnected from PDB.	1. Re-seat Inverter 2. Replace Inverter	YES
INPUT FAILURE	Minor	Utility AC input has failed.	1. Utility Failure 2. Check Input Breaker 3. Input Connections	NO
INPUT OVER CURR / INPUT CURRENT LIMIT	Minor	AC Input current exceeds threshold setting.	1. Reduce Output Load 2. Check Input Current Limit Setting	NO
SURGE MOV FAIL	Minor	The MOV board surge protection has failed and needs to be replaced.	1. Replace MOV Board	NO
INVERTER ENABLE	Minor	System controller has disabled the Inverter.	1. Check Inverter	YES
CHARGER ENABLE	Minor	System controller has disabled the charger.	1. Check Charger	NO
INV EEPROM ERROR	Minor	There has been an error reading the EEPROM on the inverter board.	1. Replace Inverter	NO
HW COMPATIBILITY	Minor	There is a hardware incompatibility between the main micro board and the inverter board.	1. Check Micro Board 2. Check Inverter Brd	NO
PDB EEPROM ERROR	Minor	There has been an error reading the EEPROM on the PDB.	1. Replace Power Supply	NO

Table 6-6, Power Alarms: Classifications, Causes and Corrections

6.2.5 Battery Alarms

The power supply detects a wide array of battery alarms and displays the type of active alarm in the Smart Display screen and the severity of alarm (e.g., Major/Minor) by means of the Inverter Module LEDs.

Battery Alarms: Classifications, Causes and Corrections				
Active Alarm	**Alarm Type**	**Probable Cause of Alarm**	**Corrective Action**	**Standby Disabled**
NO BATTERIES	Major	Detected the absence of batteries (alarm inactive when battery capacity or number of battery strings is set to 0)	1. Check Batt Breaker 2. Check Connections 3. Check Battery Fuse	YES
LOW BATT VOLTS	Major	Battery voltages below 1.833V/cell	1. Check AC Input 2. Restore AC Input 3. Connect Generator	NO
HIGH BATT VOLTS	Major	Battery voltages above 4.5V over target charger voltage	1. Check Batteries 2. Replace Inverter	NO
BATTERY EOD	Major	Output batteries dropped below the low voltage shutdown level (low battery disconnect)	1. Restore AC Input 2. Connect Generator	YES
BATTERY FAIL	Major	Charge current > 5.0A for 7 days while in float mode	1. Check Batteries 2. Replace Batteries	NO
BATT TEMP PROBE	Minor	Precision Temperature Sensor (PTS) failed or is not installed.	1. Check Connection 2. Replace Sensor	NO
REFRESH / BATT REFRESH ALARM	Minor	Battery Temperature Exceeded 60°C	1. Check Charger Settings 2. Check Batteries 3. Check Battery Temperature	NO
SAG DELTA MEAN	Minor	The voltage of one or more batteries is either too high or low from mean	1. Check Batteries 2. Replace Batteries	NO
SAG RELAY STUCK	Minor	Relay has stuck or 36V or 0V wire is no longer connected	1. Check SAG Wires BAT 2. Check SAG Wires Unit 3. Replace SAG Wires	NO
STR X MISWIRED	Minor	Battery wires are not connected properly	1. Check SAG Wires BAT 2. Check SAG Wires Unit 3. Replace SAG Wires	NO
SAG NOT CALIBRAT	Minor	Calibration data is not or is no longer available	1. Replace SAG	NO
X BAL STAGE	Minor	Stage 0 and 1 are normal. Stage 2 shows that the batteries are not of similar capacity. Stage 3-5 trigger check battery alarm to show that there is a major capacity imbalance	1. Check Batteries 2. Replace Batteries	NO
SAG NO HARNESS	Minor	Battery wires are not connected properly	1. Check SAG Wires BAT 2. Check SAG Wires Unit 3. Replace SAG Wires	NO

Table 6-7, Battery Alarms: Classifications, Causes and Corrections

6.2.6 Determining the Causes of Alarms

Although the SCTE HMS MIBs don't define the reasons for a psMajor or psMinor alarm, the DM31 transponder provides this information in several ways.

- The Smart Display lists the power supply and battery alarm reasons, as described in the previous tables.
- On the web page, the Overview page and the Power Supply page each display the "Major Alarm" and "Minor Alarm" fields with the reason for any alarm, or "OK" if the alarm is not active.
- In SNMP, psdIsMajorAlarm (1.3.6.1.4.1.926.1.5.1.7.1.1.1.1.25966) reports the reason(s) for a psMajor alarm, and psdIsMinorAlarm (1.3.6.1.4.1.926.1.5.1.7.1.1.2.1.25966) reports the reason(s) for a psMinor alarm. (In these OIDs, 25966 is the language code for English; other entries present the errors in different languages if desired.)

6.3 Digital Step Attenuation

The modem hardware incorporates a Digital Step Attenuation (DSA) on the RF receiver to moderate downstream RF levels. The DSA can be setup to operate in one of several different modes:

Non-configurable Parameters	
Mode	**Description**
Manual	The attenuation value is manually configured in a MIB.
Automatic (default)	The modem will select and update the appropriate attenuation value during operation mode.
Preferred	The modem attempts to use an attenuation value that has been manually configured in a MIB. If the modem is unable to come online with that choice, the device switches to automatic attenuation mode.

Table 6-8, Configurable Parameters

DSA operation is controlled using the MIB objects in the file ATI-MGMT-SYS-ATTN-MIB.my.

6.4 Password of the Day

Contact Alpha® Technical Services to request a copy of the Password of the Day document for setting up a password of the day.

6.5 Secure Shell Protocol (SSH)

Contact Alpha® Technical Services to request a copy of the Configurable Options document for how to perform SSH session.

6.6 Dual IP Mode

6.6.1 Overview

The DM31 transponder can operate in either Single (default) or Dual IP mode. In Single IP mode, data from both the cable modem and power supply are accessed and managed through the modem's IP address on the secure private modem network. In Dual IP mode, the Communications Module acts like a CPE device to the cable modem and registers a second IP address on the public CPE network.

The following table lists some of the basic characteristics of the DM31 transponder Single IP and Dual IP configurations:

Single IP Mode vs. Dual IP Mode		
	Single IP	**Dual IP**
Network	All data from both the cable modem and power supply are accessed and managed through the modem's IP address on the secure private modem network.	The Communications Module acts like a CPE device to the cable modem and registers a second IP address on the public CPE network.
Data Access	The Network Management System requires access to the same private modem network.	Dual IP mode allows the power supply data to be accessed and managed from anywhere within the public (CPE) network.
Security	Communication with the Communications Module is limited to the private LAN network, and is very secure.	Since the Communications Module is a CPE on the public network, access may be less secure.
IP Addresses	Where the IP address pool is limited, there is no need to issue the Communications Module a CPE IP address. Only one (1) IP Address is required for the cable modem of the DM3.	The CPE requires its own IP address, which may be in short supply. A total of two (2) IP addresses are required, one for the cable modem and one for the Communications Module.
Data Management	Access to the Communications Module is limited to the private LAN network making data management less versatile, especially for field personnel.	The Communications Module is accessible on the public (CPE) network. This makes data management more versatile for field personnel.

Table 6-9, Single IP Mode vs. Dual IP Mode

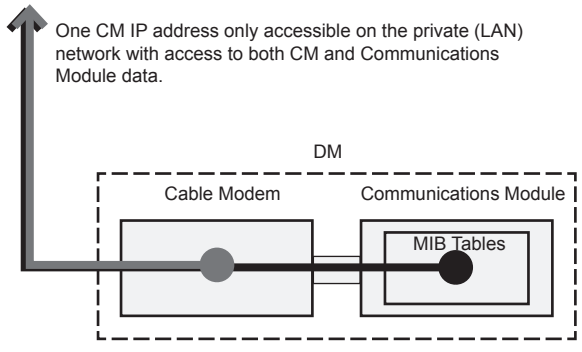


Fig. 6-1, Simplified Block Diagram Single IP Mode

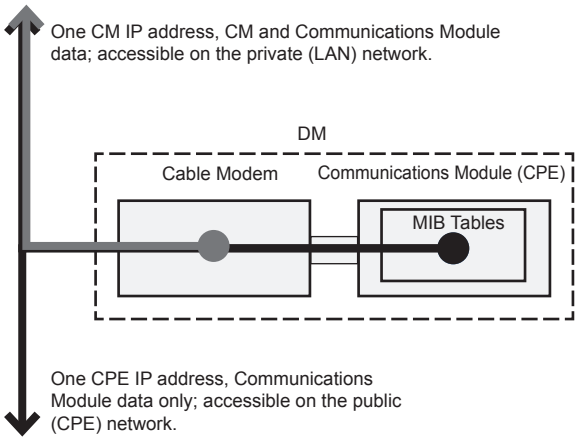


Fig. 6-2, Simplified Block Diagram Dual IP Mode

6.6.2 Web Comparison, Single IP Mode/Dual IP Mode

When accessing the web pages from either the local Ethernet port, or from the cable modem IP address, the full set of web pages (summarized in **Section 4.3 Navigating the Web Pages**) are available.

The choice of whether the transponder is configured for Dual IP can be seen on the DOCSIS web page, Configuration section (see **Fig. 6-3, DOCSIS Web Page, Single/Dual IP Mode**).

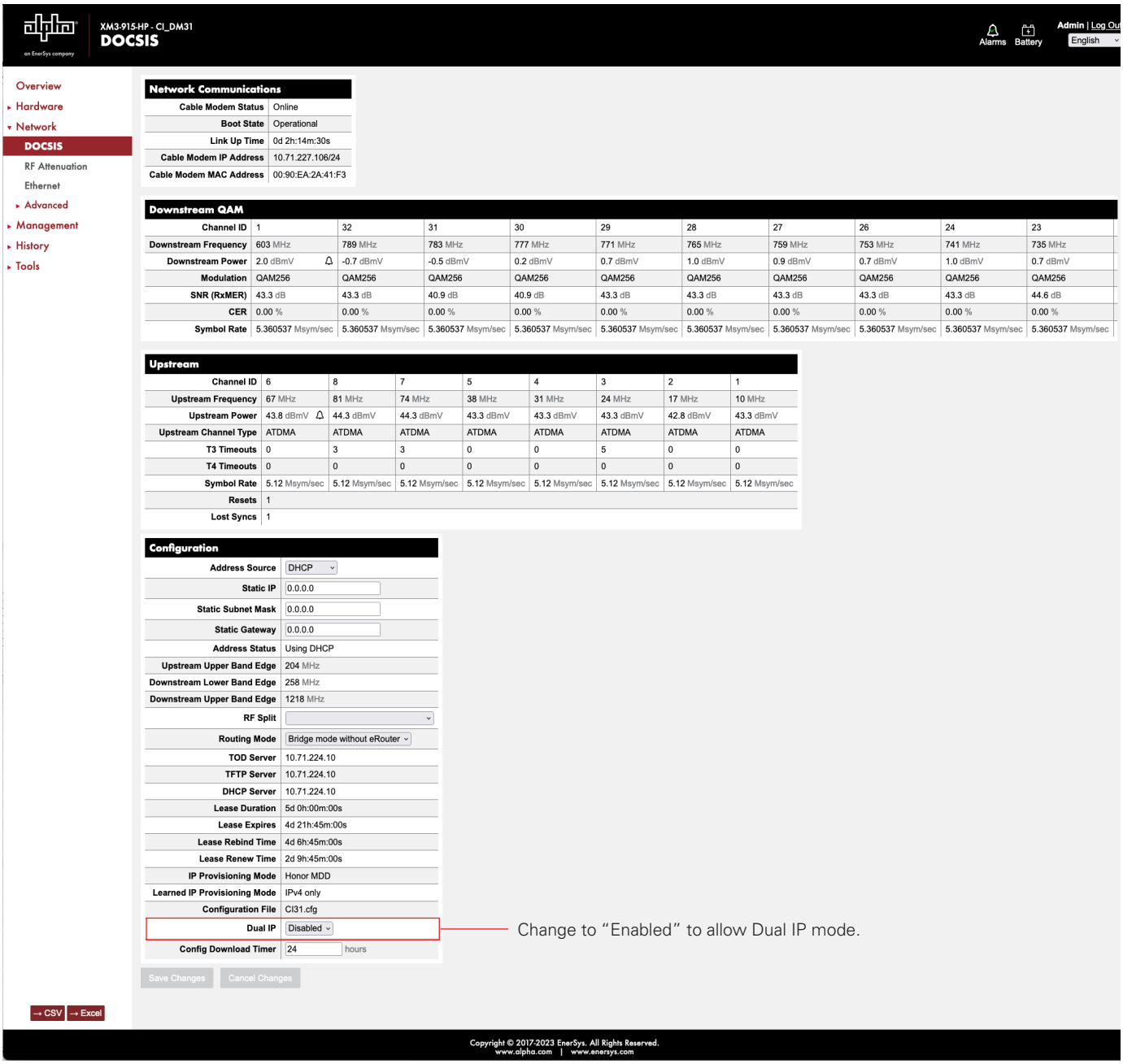


Fig. 6-3, DOCSIS Web Page, Single/Dual IP Mode

The CPE IP address assigned for the transponder in Dual IP mode is deliberately limited to only power supply functions, not network administration functions. For web access through the CPE IP address, several web pages are not available, including DOCSIS, RF Attenuation, Modem Log, Network System Log, Network Event Log, Firewall Log, Spectrum and Microreflections.

6.6.3 Configuring Dual IP Mode

To switch the DM31 transponder from Single to Dual IP mode, the atiMgmtSnmpSnmpCPEAccess parameter of the Alpha MIB will need to be enabled. The Dual IP enable setting can be set through the DOCSIS configuration file, the DM31 Setup File (atidoc31.cfg), the Provisioning Mode via the DOCSIS web page or remotely using SNMP by setting the following Alpha MIB:

Enabling Dual IP Mode			
MIB Parameter	**Object ID**	**Description**	**Value**
atiMgmtSnmpSnmpCPEAccess	1.3.6.1.4.1.926.1.3.1.3.6.0	Enables/Disables the CPE Interface	1=Disabled (Single IP) 2=Enabled (Dual IP)

Table 6-10, Enabling Dual IP Mode

NOTICE:

After configuring the Static settings the communications module must be reset in order for the settings to take effect.

The CPE Communications Module IP can be assigned its IP, Subnet Mask and Gateway Addresses either via DHCP (default) or manually, either through the web page or via the below SNMP settings:

CPE Communications Module IP Settings			
MIB Parameter	**Object ID**	**Description**	**Value**
atiMgmtSysMonitoringCpeStaticMode	1.3.6.1.4.1.926.1.3.2.2.5.2.1.0	Method by which the CPE acquires its IP address.	1=DHCP 2=Static
atiMgmtSysMonitoringCpeStaticAddress	1.3.6.1.4.1.926.1.3.2.2.5.2.2.0	When the IP address is static, this is the IP address to which the CPE will respond.	0.0.0.0 (default)
atiMgmtSysMonitoringCpeStaticMask	1.3.6.1.4.1.926.1.3.2.2.5.2.3.0	When the CPE IP address is static, this is the subnet mask.	0.0.0.0 (default)
atiMgmtSysMonitoringCpeStaticGateway	1.3.6.1.4.1.926.1.3.2.2.5.2.4.0	When the IP address is static, this is the IP address of the gateway.	0.0.0.0 (default)

Table 6-11, CPE Communications Module IP Settings

To change the CPE IP address allocation option from DHCP to Static via the web server, refer to the following:

1. Connect to DM31 transponder via web browser per the procedure in **Section 4.0 Web Interface**.
2. Log in with administrator rights.
3. On the DOCSIS page, in the Configuration section toward the bottom, enter the desired Static IP, Static Subnet Mask, and Static Gateway in the provided dtata fields.
4. Click the "Save Changes" button to update the DM31 transponder with the new values.
5. Confirm the new IP address for Dual IP is displayed in the Network Communications section at the top.

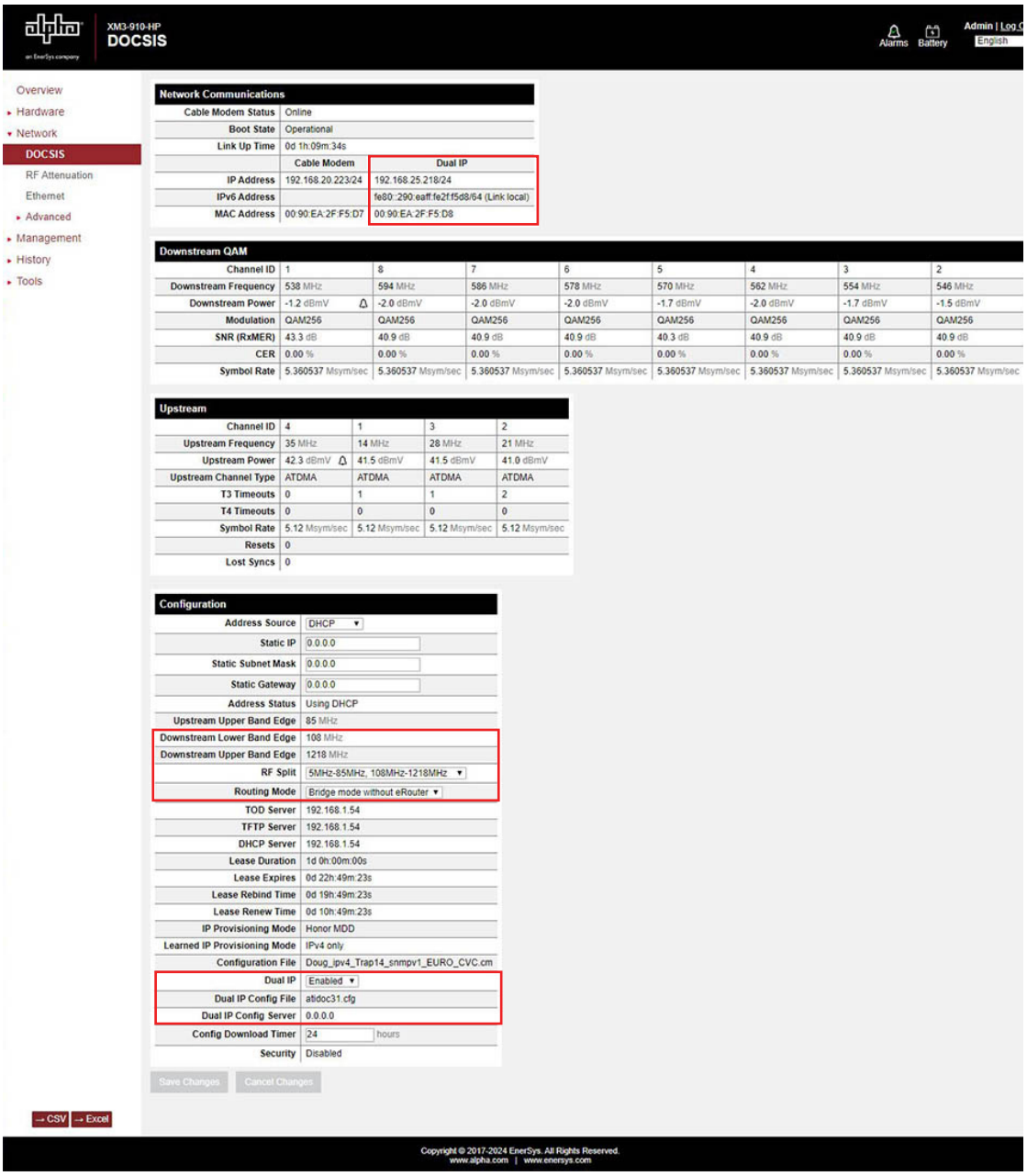


Fig. 6-5, Dual IP Configuration Settings for Web Server Communications Page

NOTICE:

Refer to **Section 3.3.7 Proprietary Configuration File 'atidoc31.cfg'** for details on using the atidoc31.cfg file to propagate custom settings to field-deployed DM31 Communications Modules.

atidoc31.cfg in Dual IP Mode

In Dual IP mode, the DM31 transponder will first attempt to download the proprietary configuration file atidoc31.cfg through the CPE's interface from a TFTP server on the CPE network. In many networks, the TFTP server is blocked or disabled, so the DM31 transponder also has provisions to download this file through the cable modem interface from the modem's provisioning server if necessary. The filename and TFTP server location may also be specified through special tags in the DHCP Offer, refer to the paragraph below "Specifying atidoc31.cfg Name and Location via DHCP Tags" for details. Similar to Single IP mode, any DM31 transponder proprietary SNMP MIB setting may be placed in the modem's DOCSIS configuration file which would eliminate the need for atidoc31.cfg.

Changing Default atidoc31.cfg Download Settings in Dual IP Mode

The following table explains the download options available for the atidoc31.cfg file in Dual IP mode. The 'Download Interface' indicates the network from which the DM31 transponder will attempt to download atidoc31.cfg, either the CPE network or the more secure cable modem management network.

Available Download Options				
Search Order	**Parameter**	**Comments**	**Value**	**Download Interface**
1	atiMgmtSysDownloadConfigAddress OID 1.3.6.1.4.1.926.1.3.2.1.10.0	Overrides Default Location	0.0.0.0 (Default)	CPE
2	DHCP Server IP	Server or Relay Agent Address from DHCP lease (No Change Necessary)	As Set	CPE
3	DHCP Option 54 Server IP	Server or Relay Agent Address from DHCP lease	As Set	CPE
4	DHCP Tags	User-defined	As Set	CPE
5	docsDevServerConfigTftpAddress 1.3.6.1.2.1.69.1.4.11.0	Automatically set in modem	CM's TFTP Server Address	CM
6	docsDevSwServerAddress 1.3.6.1.2.1.69.1.3.7.0	Set via DOCSIS configuration file	As Set	CM
7	Software Upgrade Server	Set via DOCSIS configuration file	As Set	CM

Table 6-12, Available Download Options

Specifying atidoc31.cfg name and location via DHCP Tags

In the User-defined area of the DHCP Tags, above option 192, the Communications Module will look for the following value:

Tag: [Insert Unique Tag Name, e.g. 'ati-tag']

Value: aticonfig

In the Tag value immediately following will be the value for the TFTP server to use:

Tag: [Insert Unique Tag Name, e.g. 'ati-ip']

Value: IP address of TFTP server (i.e. 192.168.1.51)

Immediately following will be the value for the config filename:

Tag: [Insert Unique Tag Name, e.g. 'ati-name']

Value: =atidoc31.cfg (an equal sign needs to be in front of the filename for the DHCP server to recognize this as a valid entry)

6.6.4 Dual IP SNMP Community Strings

The communications module community strings used for the CPE communications module in Dual IP mode can be configured by the operator. The default communications module read-only community string is AlphaGet. The default read-write community string is AlphaSet. These settings can be configured with the DOCSIS® configuration file, the DM31 Setup File (atidoc31.cfg) or remotely using SNMP by including the parameters below:

NOTICE:

These community strings are only applicable for CPE access in Dual IP mode. CM access in both Single IP and Dual IP modes use standard DOCSIS community strings set through the modem configuration file's docsDevNmAccessTable. See **Section 3.3.1 Setting Modem Community Strings - docsDevNmAccess Method (Deprecated; IPv4 Only)** and **Section 3.3.2 Setting Modem Community Strings - Coexistence Method**.

Community Strings			
MIB Parameter	**Object ID**	**Description**	**Value**
atiMgmtSnmpCommGet	1.3.6.1.4.1.926.1.3.1.4.1.0	Read Community String	AlphaGet (default)[desired value]
atiMgmtSnmpCommSet	1.3.6.1.4.1.926.1.3.1.4.2.0	Read-Write Community String	AlphaSet (default)[desired value]

Table 6-13, Community Strings

6.6.5 Security in Dual IP Mode

In Dual IP mode, additional SNMP security to the DM31 transponder proprietary MIBs is required since the Communications Module and power supply data is exposed on the CPE network, which may be more vulnerable to packet sniffing and community string deciphering than on the secure cable modem network.

There are two methods of providing SNMP Security in Dual IP mode: the Data Access Key (default), and the Secure Access List.

Method 1: Dual IP Security Using the Data Access Key

In Dual IP mode atiMgmtSnmpAlphaSetAccess is the only SNMP parameter within the Alpha® proprietary MIB with SNMP write access on the CPE network by default. When this parameter is set to the value of the parameter atiMgmtSnmpAlphaSetKey, the data access key, SNMP read/write access is granted to all parameters in the Alpha MIB tree with read/write attributes. When this access is granted, the value of atiMgmtSnmpCPESetEnabled is automatically changed to "2" (enabled). After the operator is finished setting the SNMP variables, SNMP write access can be disabled by setting the atiMgmtSnmpCPESetEnabled to "1" or by setting atiMgmtSnmpAlphaSetAccess to any value other than the data access key or by performing a reset to the DM31 transponder.

The data access key parameters can be changed from the default values through the DOCSIS configuration file, the DM31 Setup File (atidoc31.cfg) or remotely using SNMP by including the following Alpha MIB parameters:

Data Access Key Parameters			
MIB Parameter	**Object ID**	**Description**	**Value**
atiMgmtSnmpAlphaSetAccess	1.3.6.1.4.1.926.1.3.1.3.3.0	Set to Access Key	Set to match the value of atiMgmtSnmpAlphaSetKey
atiMgmtSnmpAlphaSetKey	1.3.6.1.4.1.926.1.3.1.3.4.0	Data Access Key (Dual IP)	CIBSET (default)
atiMgmtSnmpCPESetEnabled	1.3.6.1.4.1.926.1.3.1.3.5.0	Corresponds to whether or not the action taken on atiMgmtSnmpAlphaSetKey was successful. Once enabled, writing 1 to this variable will disable CPE sets.	1 = Disabled (False) 2 = Enabled (True)

Table 6-14, Data Access Key Parameters

Method 2: Dual IP Security Using the Secure Access List

The DM31 transponder provides an alternative method of providing additional SNMP security in Dual IP by limiting access to the Communications Module's CPE address. The Secure Access List method limits remote SNMP access to four IP addresses. Only the IP addresses listed in the SNMP Access Table are able to read or write to the Alpha MIB parameters from the public (CPE) network. This method overrides the default Data Access Key method.

The IP address entries in the SNMP Access Table can be set through the DOCSIS configuration file, the DM31 setup file (atidoc31.cfg) or remotely using SNMP by including the following Alpha MIB parameters:

Data Access Key Parameters			
MIB Parameter	**Object ID**	**Description**	**Value**
atiMgmtSnmpAccessTable	1.3.6.1.4.1.926.1.3.1.2	Table of SNMP Access Addresses	Object identifier
atiMgmtSnmpAccessAddress.1	1.3.6.1.4.1.926.1.3.1.2.1.2.1	SNMP access IP Address #1	0.0.0.0 (Default)
atiMgmtSnmpAccessAddress.2	1.3.6.1.4.1.926.1.3.1.2.1.2.2	SNMP access IP Address #2	0.0.0.0 (Default)
atiMgmtSnmpAccessAddress.3	1.3.6.1.4.1.926.1.3.1.2.1.2.3	SNMP access IP Address #3	0.0.0.0 (Default)
atiMgmtSnmpAccessAddress.4	1.3.6.1.4.1.926.1.3.1.2.1.2.4	SNMP access IP Address #4	0.0.0.0 (Default)

Table 6-15, Secure Access Table Parameters

7.0 Installation

WARNING! ELECTRICAL HAZARD

To reduce the risk of electric shock, completely remove the inverter module from the power supply prior to installation. For field installation, use a service power supply to avoid losing power to the load.

CAUTION!

The DM31 transponder is static sensitive. An ESD wrist strap should be worn when installing the transponder.

7.1 Installation / Replacement Procedure in XM3-HP™ Power Supplies

Removing the Inverter Module:

1. Turn off the battery breaker and remove the power supply cover.
2. Disconnect the battery input and temperature sensor cables from the inverter module, followed by the tamper and RF if a transponder is currently installed.
3. Loosen the thumbscrew on the XM3-HP™ power supply inverter module and the thumbscrew on the transponder (if applicable).
4. Grasp the handle on the bottom right side of the inverter module. Pull firmly to release the module from the inverter connector. Gently slide the module assembly straight out until the inverter module is accessible.

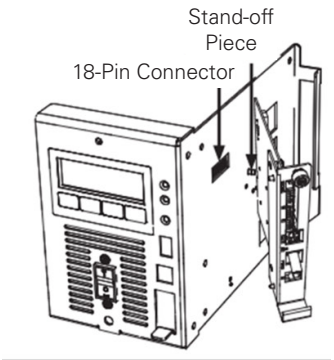
NOTICE:

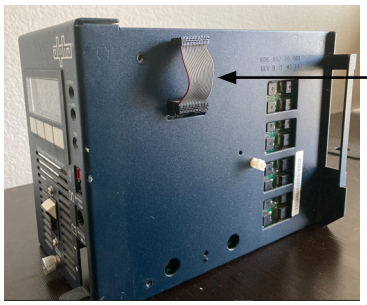
For XM3-HP™ power supplies in service, backup battery power will not be available during this procedure.

CAUTION!

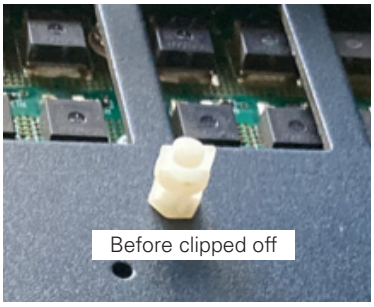
Service personnel must verify the inverter module battery breaker remains in the OFF position until instructed to return the unit to service.

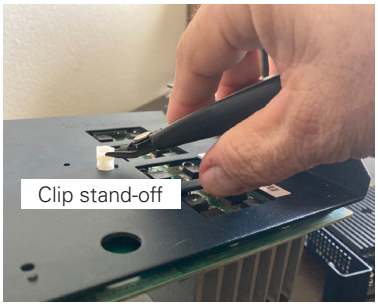
5. If applicable, remove the old transponder from the inverter module. Remove ribbon cable to make this easier.
6. The white stand-off on the side of the inverter module should be snipped off to avoid interference with the DM31 transponder assembly (**Fig. 7-1, Modifying Stand-off**). Use wire cutters to snip the stand-off.





To ease the installation process, remove the ribbon from the transponder.





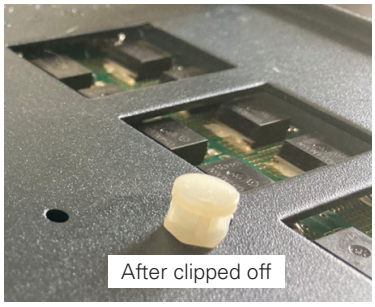


Fig. 7-1, Modifying Stand-off

7. Lower the transponder down so it's flush with the power supply and ensure the captive screws align with their designated holes (**Fig. 7-2, Inserting Captive Screws**). Ensure the PCBA slot is centered with the 18-pin connector.

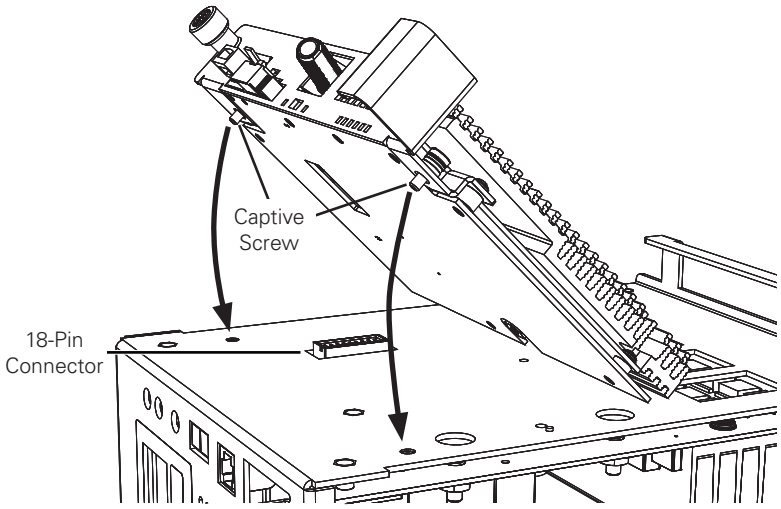


Fig. 7-2, Inserting Captive Screws

8. Fasten the transponder to the inverter module by tightening the two captive screws (**Fig. 7-3, Captive Screws**). It is recommended that the screws be tightened alternately, a few turns at a time, so the transponder aligns in parallel to the inverter module.

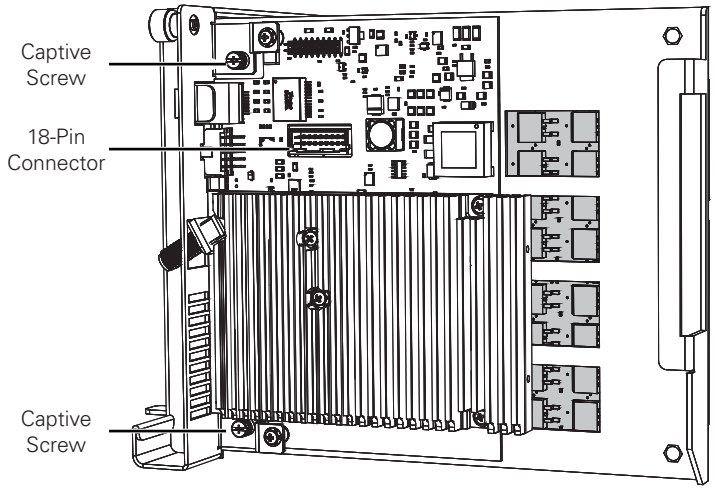


Fig. 7-3, Captive Screws

9. Install the 18-pin ribbon cable between the DM31 transponder and the inverter module (**Fig. 7-4, Ribbon Cable Installation**).
10. Reinstall the inverter module, tighten the two thumbscrews and reconnect the front panel connections (tamper, temperature sensor, battery harness, etc.).
11. Verify the recording of the cable modem MAC address (RF MAC) by navigating to the XM3-HP™ power supply Smart Display's **COMM** menu.

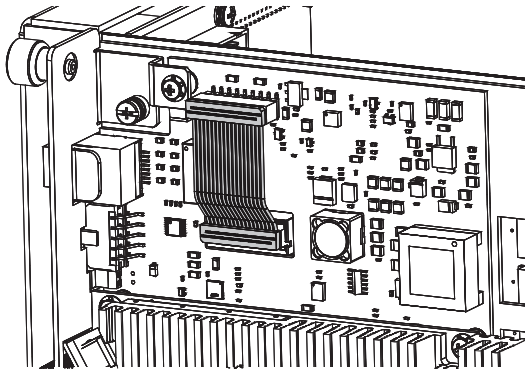


Fig. 7-4, Ribbon Cable Installation

CAUTION!

Before proceeding to the next step, the RF drop must have a properly installed grounded surge suppressor *(Alpha p/n 162-028-10 or equivalent)* in the enclosure. Failure to install an appropriate surge suppressor may void the warranty.

***NOTICE**:*

Alpha Technologies recommends tightening the RF cable connector and the cables attached to the grounded surge protector to a torque setting of 10 in-lb ± 1 in-lb.

12. Connect the RF drop as shown in **Fig. 7-5, RF Cable Installation**. The DOCSIS® specification for downstream power level is ±15 dBmV. However, for optimal performance, set the level as close to 0 dBmV as possible. RF attenuators may be required to obtain optimal downstream (receive) RF levels.
13. Connect any other front panel connections at this time (e.g. tamper switch, etc.) Refer to **Section 7.5 I/O Connections (Tamper Switch, Environmental I/O Connector)**.

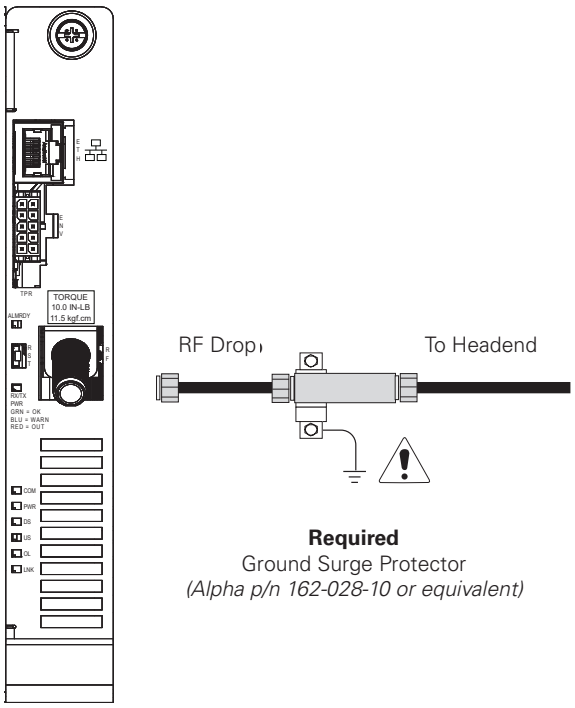


Fig. 7-5, RF Cable Installation

7.2 Initial Power-Up and Test / Return Unit to Service

1. Plug the power supply into the AC outlet.
2. Switch battery breaker ON.
3. The transponder LED indicators will all blink in unison upon initial power up. The RDY indicator will then begin blinking steadily indicating normal processor activity.
4. Once the transponder is online, verify the DS and OL indicators are on solid (refer to **Section 2.4 DM31 Transponder Start Up and Reboot Sequence**). This verifies the communications module has registered an IP address on the network.
5. Verify the RF indicator is solid green, indicating upstream and downstream power is within the default specified range and the Upstream RF Power is below the recommended +50 dBmV (**Table 7-1, RF Power Default Values**).
6. Verify no XM3-HP™ power supply alarms are active.

RF Power Default Values		
LED Color	**Rx Range (dBmV)**	**Tx Range (dBmV)**
Green	+10 to -10	0 to +50
Blue	+15 to +10 and -10 to -15	+50 to +55
Red	>+15 and <-15	>+55

Table 7-1, RF Power Default Values

7.3 Verify Communications

7.3.1 XM3-HP™ Power Supply Smart Display - COMM Menu

Verify the DM31 transponder communication parameters such as IP address, RF Power Levels and Signal/Noise Ratio on the **COMM - GENERAL** menu of the XM3-HP power supply Smart Display. Press **ENTR** to open the **COMM-GENERAL** menu enabling the operator to view values for communications parameters. Pressing the up or down arrow softkeys will show two lines of information for each submenu item (**Fig. 7-6, COMM - GENERAL Menu**).

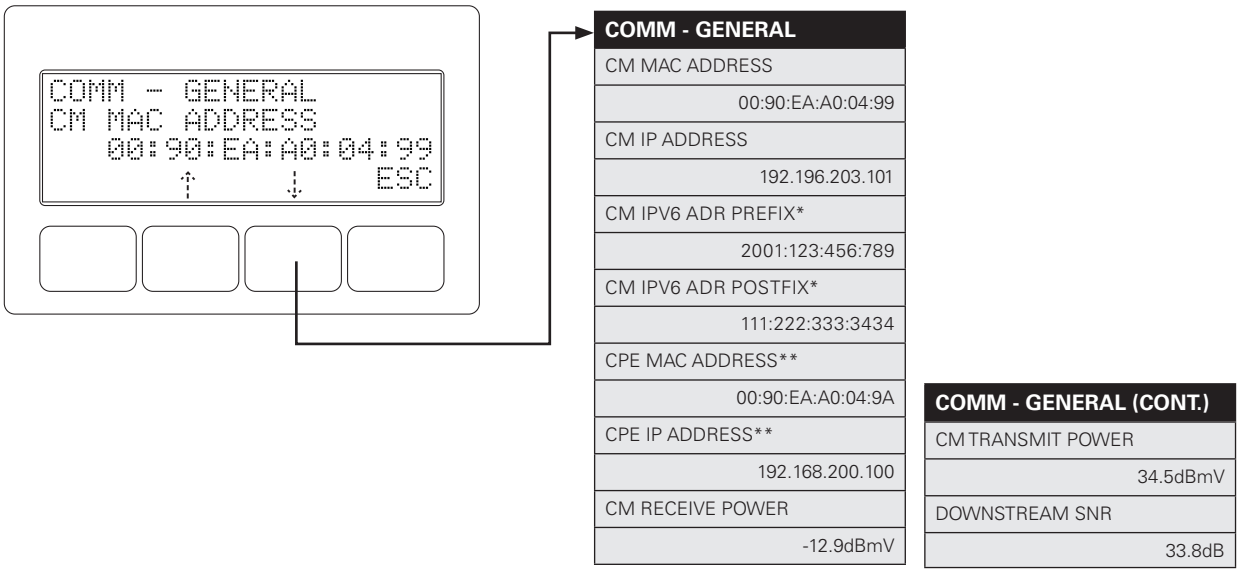
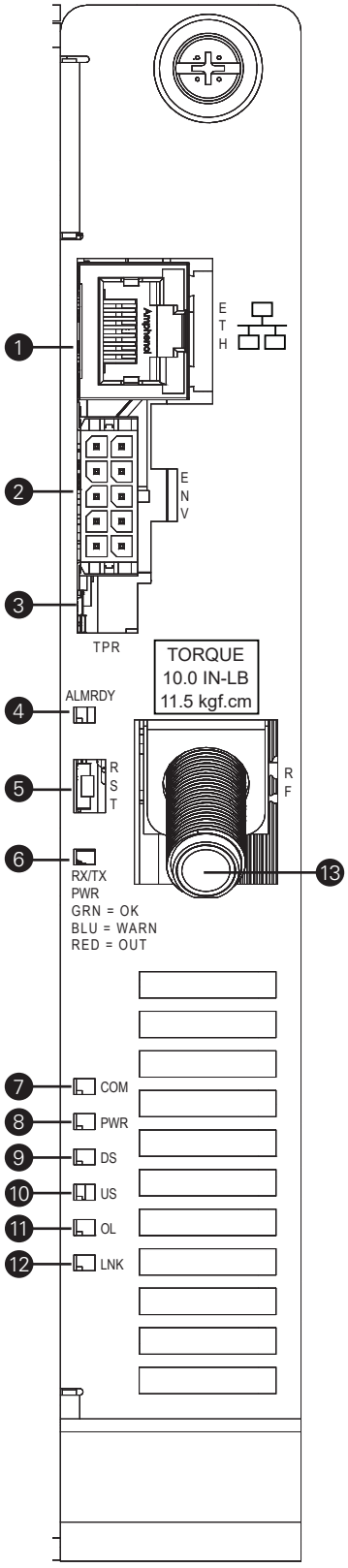


Fig. 7-6, COMM - GENERAL Menu

7.4 DM31 Transponder LEDs and Connections



DM31 Transponder LEDs and Connectors				
Item	**LED or Connector**	**Status**	**Behavior**	**Indication**
1	ETH: Ethernet connection			
2	ENV: Environmental control connector			
3	TPR: Tamper switch connector			
4	ALM / RDY: Alarm and Ready	N/A	OFF	No power or malfunctioning communications module
		GRN	ON	Reset of the DM31 transponder in process
			Steady blinking	Normal operation
		RED	Blinking more OFF than ON	Minor alarm
			Blinking more ON than OFF	Major alarm
5	RST: Reset button			
6	RF power level indicator	TRI	OFF	No RF detected
			BLUE	Rx / Tx power at a Warning Level as Set within the SCTE-HMS Property Table
			GREEN	Rx / Tx RF power level within tolerance
			RED	Rx / Tx power at an Alert Level as set within the SCTE-HMS Property Table
7	COM: XM3-HP™ power supply communications			Power supply communications
8	PWR: DM31 transponder power	GRN		Indicates power to unit
9	DS: Downstream RF carrier detection and lock	GRN	OFF	No power / Downstream carrier
			OFF / ON	Power on, downstream carrier frequency searching
			ON	Downstream carrier lock
10	US: Upstream ranging and registration lock	GRN	OFF	No power, upstream frequency undetermined
			OFF / ON	Power on, downstream locked, upstream frequency ranging, DHCP request in progress
			ON	CMTS registration completed
11	OL: CPE activity status (or Online status)	GRN	OFF	No Ethernet communications activity
			OFF / ON	Momentary flashes during CPE communications via the Ethernet craft port when connected to a CPE device OR flashes while performing early authentication, IP connectivity, BPI initialization.
			ON	Online and operational
12	LNK: CPE link status	GRN	OFF	No Ethernet link
			ON	Link on Ethernet craft port
13	RF Connection			

Fig. 7-7, DM31 Transponder LEDs and Connectors

7.5 I/O Connections (Tamper Switch, Environmental I/O Connector)

The Alpha® DM31 transponders are populated with a Tamper interface to report the status of the power supply enclosure door when equipped with the optional tamper switch. The DM31 transponders are also populated with the Environmental and I/O Controller interface (referred to in this section as I/O port) which can be used to monitor and control an array of contact relay devices such as battery heater mats, enclosure moisture sensors and emergency generators.

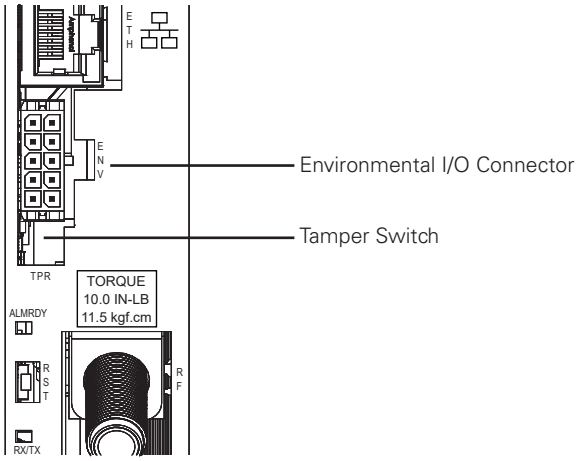


Fig. 7-9, Environmental (ENV) I/O and Tamper Switch Interface (TPR) Connection Locations

7.5.1 Tamper (TPR) Switch Interface

The tamper switch interface is designed to report and alarm the status of the power supply enclosure door. The circuit created by the tamper switch is a contact relay, so other contact relay devices can be designed to be monitored through this interface.

NOTICE:

In the OID column of the following table, 'X' denotes power supply device address (Default = 1).

Tamper (TPR) Switch Specifications				
Function	**Parameter**	**OID**	**Values**	**Description**
Tamper	psTamper	1.3.6.1.4.1.5591.1.4.2.1.27.1 See Note 1	1 = Closed 2 = Open	Status of enclosure door
Utility Sense	psTamper	1.3.6.1.4.1.5591.1.4.2.1.27.1	1 = No Voltage 2 = Voltage Present	Status of utility voltage
	tamperPolarity	1.3.6.1.4.1.926.1.3.2.6.1.0	1 = Report "Open" When Contact Open 2 = Report "Open" When Contact Closed	Controls polarity of "psTamper" reporting
Alarm / Trap	psTamper (Closed)	1.3.6.1.4.1.5591.1.1.3.1.3.13.1.3.6.1.4.1.5591.1.4.2.1.27.1.1	1 = Disable 2 = enableMajor 3 = enableMinor	Alarm enable for psTamper = Closed
Alarm / Trap	psTamper (Open)	1.3.6.1.4.1.5591.1.1.3.1.3.13.1.3.6.1.4.1.5591.1.4.2.1.27.1.2	1 = Disable 2 = enableMajor 3 = enableMinor	Alarm enable for psTamper = Open

Table 7-2, Tamper (TPR) Switch Specifications

7.5.2 I/O Port Interface

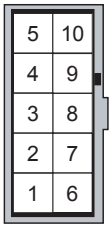
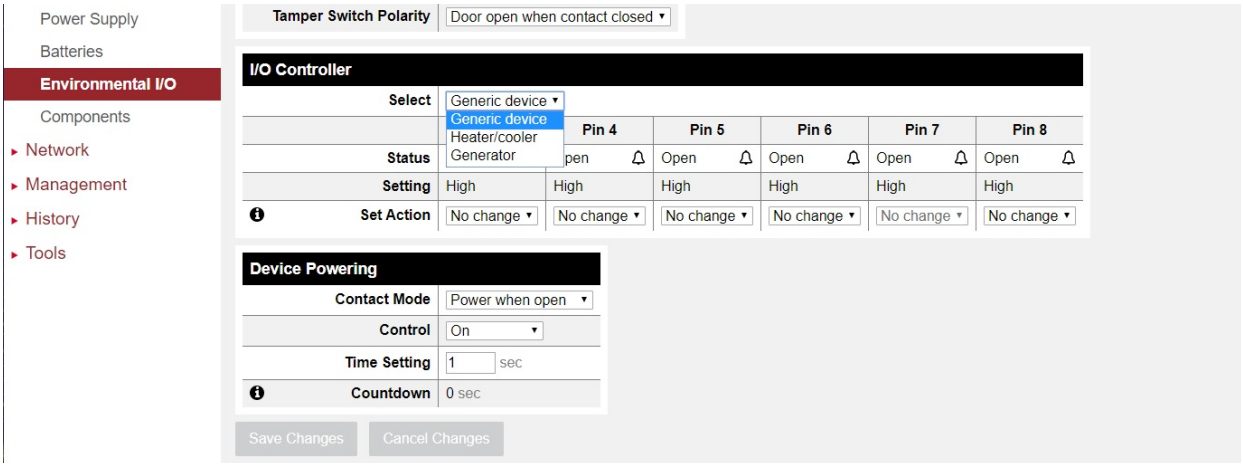
ENV Connector and Pin Descriptions		
ENV Connector	**Pin**	**Description**
 Back of ENV Connector	1	Logic Gnd
	2	5V +/- 0.5V voltage Shotky Protection – 15mA max. – Relay current drive
	3	Open/Close Control – 0V/15mA sink = Close, 3.3V/0mA = Open
	4	Open/Close Sense – Pin 4 relay contact short to pin 1 = Close, Pin 4 open = Open
	5	Open/Close Sense – Pin 5 relay contact short to pin 1 = Close, Pin 5 open = Open
	6	Open/Close Sense – Pin 6 relay contact short to pin 1 = Close, Pin 6 open = Open
	7	Open/Close Control – 0V/15mA sink = Close, 3.3V/0mA = Open
	8	Open/Close Sense – Pin 8 relay contact short to pin 1 = Close, Pin 8 open = Open
	9	Not Connected
	10	Not Connected

Table 7-3, ENV Connector and Pin Descriptions



Steps to configure DM31 transponder to monitor I/O device.

1. Set atiMgmtSysIoSelect appropriately (SNMP or Web) for device to monitor.

   OID 1.3.6.1.4.1.926.1.3.2.8.1.0

   1 = Generic

   The device can be selected through the Web page by navigating to 'Advanced Configuration', 'I/O – Environment' and selecting from the pull-down list
2. Configure alarms (Generic Only – See below section for details).
3. Monitor appropriate SNMP parameters (See each section below for details).

7.5.3 Configuring I/O Port Connections

The I/O port SNMP MIB includes support for some legacy devices. New installations should not implement device specific settings listed in **Table 7-4, I/O Port Specifications**. Contact Alpha customer support for questions about connecting legacy equipment to the I/O Port.

Alpha® has created logic for control and reporting of specific devices or combination of devices. The Alpha proprietary SNMP MIB atiMgmtSysIoSelect, 1.3.6.1.4.1.926.1.3.2.8.1.0 must be set appropriately before the device status will be correctly reported. The monitored device can also be set through the transponder's "Advanced Configuration - I/O" Web page pull-down. The status of the generic I/O Pins can still be monitored and alarmed via the SCTE-HMS discretePropertyTable even when specific devices have been selected.

I/O Port Specifications		
atiMgmtSysIoSelect (1.3.6.1.4.1.926.1.3.2.8.1.0)		
MIB Value	Device	Reported Parameter of MIB Branch
1	No Device (Generic)	I/O Pins Only

*MIBs within atiMgmtSysTempMgr branch will report and control will be allowed regardless of the value reported by atiMgmtSysIoSelect.

Table 7-4, I/O Port Specifications

7.5.4 I/O Port: Generic Device

The I/O connector on the transponder allows the headend to remotely monitor and control external contact relay devices. Each input pin can be configured through the SCTE-HMS discretePropertyTable for alarm and SNMP trap generation.

I/O Port: Generic Device Specifications				
Function	Parameter	OID	Values	Description
Input	atiMgmtSysIOPinIn4	1.3.6.1.4.1.926.1.3.2.8.21.0	1 = Contact Open	
Input	atiMgmtSysIOPinIn5	1.3.6.1.4.1.926.1.3.2.8.22.0	1 = Contact Open 2 = Contact Closed	Used to monitor moisture sensor
Input	atiMgmtSysIOPinIn6	1.3.6.1.4.1.926.1.3.2.8.23.0	1 = Contact Open 2 = Contact Closed	
Control	atiMgmtSysIOPinCtrl	1.3.6.1.4.1.926.1.3.2.8.20.0	1 = Contact Open 2 = Contact Closed	Open/Close a contact
Alarm / Trap	IOPinIn4(Open)	1.3.6.1.4.1.5591.1.1.3.1.3.13.1.3.6.1.4.1.926. 1.3.2.8.21.0.1	1 = disable 2 = enableMajor 3 = enableMinor	Alarm enable when Pin4 contact is Open
Alarm / Trap	IOPinIn4 (Closed)	1.3.6.1.4.1.5591.1.1.3.1.3.13.1.3.6.1.4.1.926. 1.3.2.8.21.0.2	1 = disable 2 = enableMajor 3 = enableMinor	Alarm enable when Pin4 contact is Closed
Alarm / Trap	IOPinIn5 (Open)	1.3.6.1.4.1.5591.1.1.3.1.3.13.1.3.6.1.4.1.926. 1.3.2.8.22.0.1	1 = disable 2 = enableMajor 3 = enableMinor	Alarm enable when Pin5 contact is Open
Alarm / Trap	IOPinIn5 (Closed)	1.3.6.1.4.1.5591.1.1.3.1.3.13.1.3.6.1.4.1.926. 1.3.2.8.22.0.2	1 = disable 2 = enableMajor 3 = enableMinor	Alarm enable when Pin5 contact is Closed
Alarm / Trap	IOPinIn6 (Open)	1.3.6.1.4.1.5591.1.1.3.1.3.13.1.3.6.1.4.1.926. 1.3.2.8.23.0.1	1 = disable 2 = enableMajor 3 = enableMinor	Alarm enable when Pin6 contact is Open
Alarm / Trap	IOPinIn6 (Closed)	1.3.6.1.4.1.5591.1.1.3.1.3.13.1.3.6.1.4.1.926. 1.3.2.8.23.0.2	1 = disable 2 = enableMajor 3 = enableMinor	Alarm enable when Pin6 contact is Closed
Alarm / Trap	IOPinCtrl (Open)	1.3.6.1.4.1.5591.1.1.3.1.3.13.1.3.6.1.4.1.926. 1.3.2.8.20.0.1	1 = disable 2 = enableMajor 3 = enableMinor	Alarm enable when control contact is Open
Alarm / Trap	IOPinCtrl (Closed)	1.3.6.1.4.1.5591.1.1.3.1.3.13.1.3.6.1.4.1.926. 1.3.2.8.20.0.2	1 = disable 2 = enableMajor 3 = enableMinor	Alarm enable when control contact is Closed

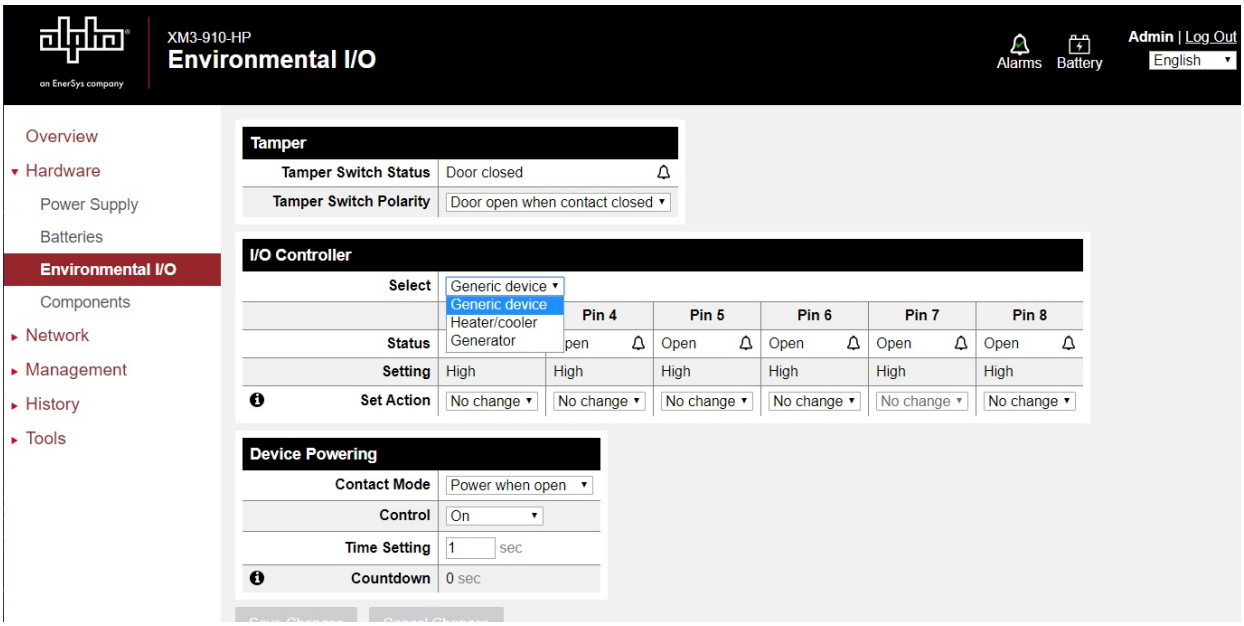
Table 7-5, I/O Port: Generic Device Specifications

7.5.5 Connecting a Generic I/O Device

For generic device configurations consult your Alpha representative.

7.5.6 Configuring and Monitoring a Generic I/O Device

Set the parameter atiMgmtSysIoSelect 1.3.6.1.4.1.926.1.3.2.8.1.0 to a value of "1" (Generic). Alternatively, navigate to 'Advanced Configuration', 'I/O – Environment' and select "Generic Device" from the pull-down list.



The status of the control and input pins can be monitored through the following OIDs.

Pin 3 (Control) 1.3.6.1.4.1.926.1.3.2.8.20	1 = Contact Open 2 = Contact Closed
Pin 4 (Input) 1.3.6.1.4.1.926.1.3.2.8.21	1 = Contact Open 2 = Contact Closed
Inpu Pin 5 (Input) 1.3.6.1.4.1.926.1.3.2.8.22 t	1 = Contact Open 2 = Contact Closed
Pin 6 (Input) 1.3.6.1.4.1.926.1.3.2.8.23	1 = Contact Open 2 = Contact Closed

Voltage to drive Pin 3 is managed through the following SNMP OID.

atiMgmtSystempCtrl 1.3.6.1.4.1.926.1.3.2.4.1	1 = Off 5 = On

The SCTE-HMS discretePropertyTable can be configured to generate SNMP traps based upon the desired contact state of any of the I/O input or control pins (see **Table 7-3, ENV Connector and Pin Descriptions**).

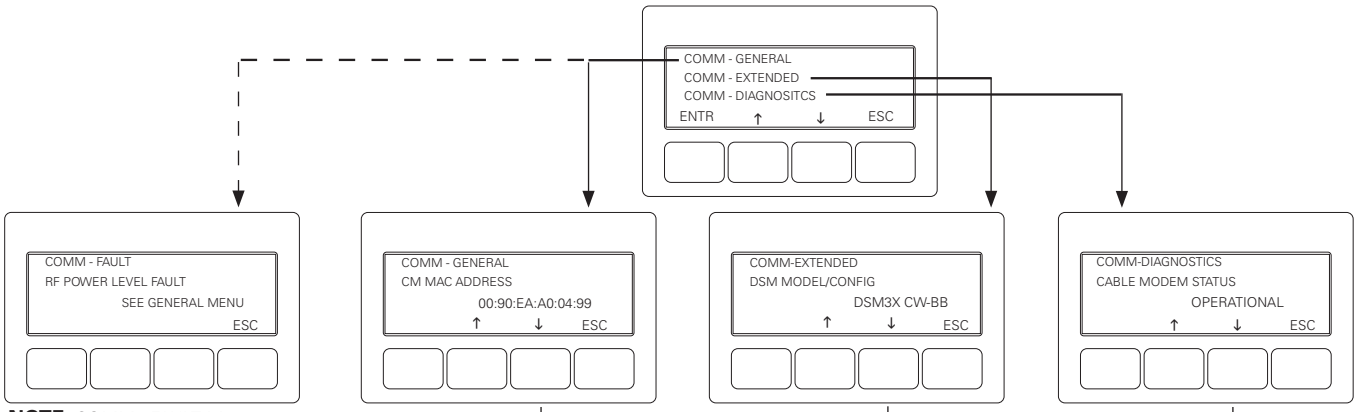
8.0 Start Up and Verification

8.1 Initial Start Up and Local Verification

To confirm successful hardware installation before leaving the installation site, verify network connectivity and correct hardware interconnection.

The DS, US, and OL LEDs on the front of the DM31 transponder should be ON solid green. This indicates successful registration with the CMTS via the RF link. In addition, the RF LED should also be ON solid green indicating proper RF power levels and the ALM/RDY LED should be blinking green for normal operation.

With the DM31 transponder used in conjunction with the Alpha® power supply, network connectivity can be verified via the COMM menu on the Smart Display. The figure below provides a list of parameters available on the power supply Smart Display populated with sample values.



NOTE: COMM - FAULT Menu appears only if there is no RF connection or RF interruption occurs.

COMM - GENERAL
CM MAC ADDRESS
00:90:EA:A0:04:99
CM IP ADDRESS
192.196.203.101
CM IPV6 ADR PREFIX*
2001:123:456:789
CM IPV6 ADR POSTFIX*
111:222:333:3434
CPE MAC ADDRESS**
00:90:EA:A0:04:9A
CPE IP ADDRESS**
192.168.200.100
CM RECEIVE POWER
-12.9dBmV
CM TRANSMIT POWER
34.5dBmV
DOWNSTREAM SNR
33.8dB

* Menu item available if DM31 transponder is provisioned in IPv6 mode.

** Menu item available if DM31 transponder is provisioned in Dual-IP mode.

COMM - EXTENDED
MODEL/CONFIG
CMOA-45204F
FIRMWARE VERSION
PS3.1-v01.10.00 b001
SYSTEM NAME
ABC123 CABLE
SYSTEM CONTACT
JOHN DOE
SYSTEM LOCATION
123 BAKERVIEW
COMMON LOGICAL ID
12345-3767 ALPHAWAY
DOCSIS CONFIG FILE
ALPHA_DSM3.CM
SERIAL NUMBER
2101F6700469

* Menu item will populate for only Cableware configured units

COMM - DIAGNOSTICS
CABLE MODEM STATUS
OPERATIONAL
SYSTEM UPTIME
3 DAYS 05H:16M:59S
DOWNSTREAM FREQUENCY
300.000 MHZ
DOWN MODULATION TYPE
256 QAM × 32
UPSTREAM FREQUENCY
15.000 MHZ
UP MODULATION TYPE
ATDMA × 8
T3 TIMEOUTS
80360
T4 TIMEOUTS
51
CODEWORD ERROR RATIO
8.20%
MICROREFLECTIONS
-5 DBC
CM RESETS
10
CM LOST SYNCS
5
LAST SNMP QUERY
Date/Time

Fig. 8-1, XM3-HP™ Power Supply Smart Display Screens

8.0 Start Up and Verification, continued

Connect a computer's network port to the transponder's Ethernet port using a standard network cable. Launch an Internet browser and enter 192.168.100.1 into the address. The transponder will return the web page shown below. The DOCSIS Summary section confirms connectivity.

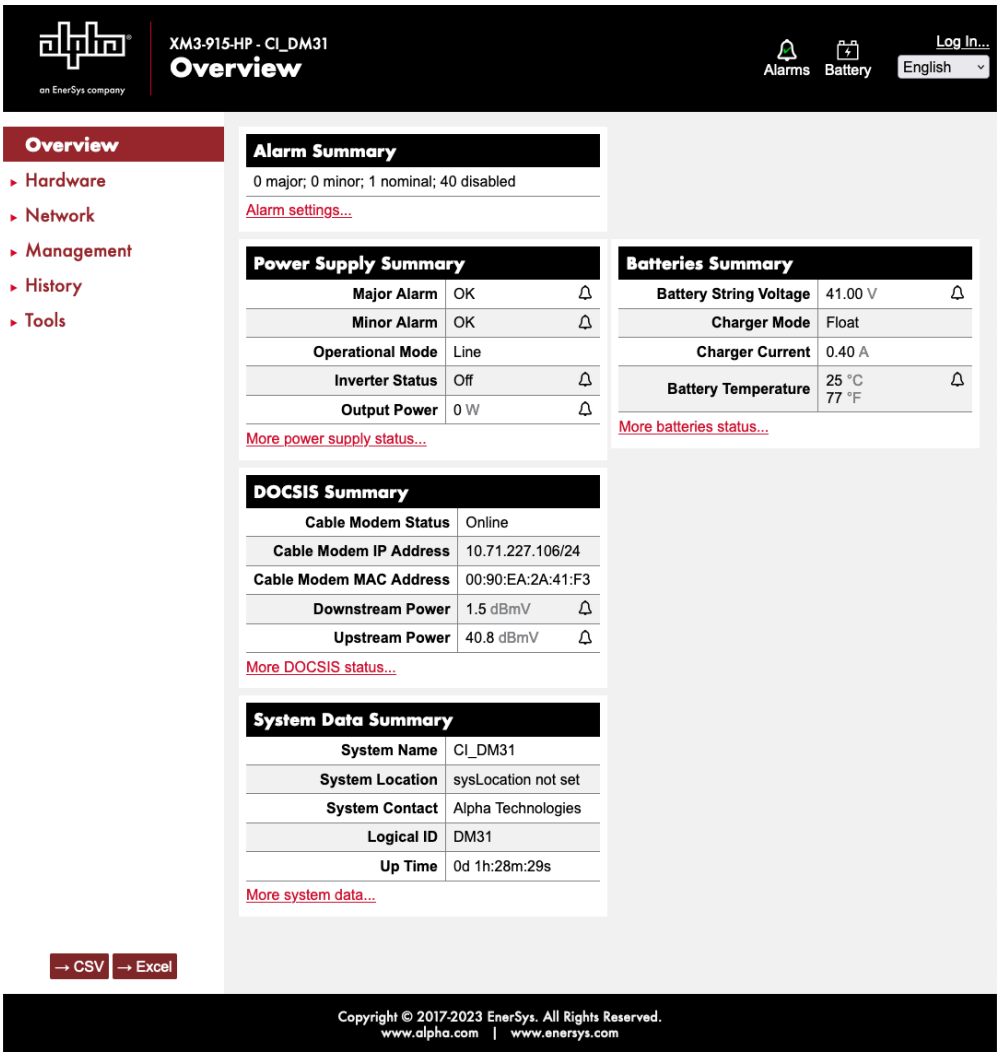


Fig. 8-2, Overview Web Page

8.2 Verifying Correct Battery Connections

From the Batteries web page, the following screen will be visible and the parameters shown will be available for viewing and verification. To test hardware interconnection using the Ethernet port, verify valid values for individual battery voltages.

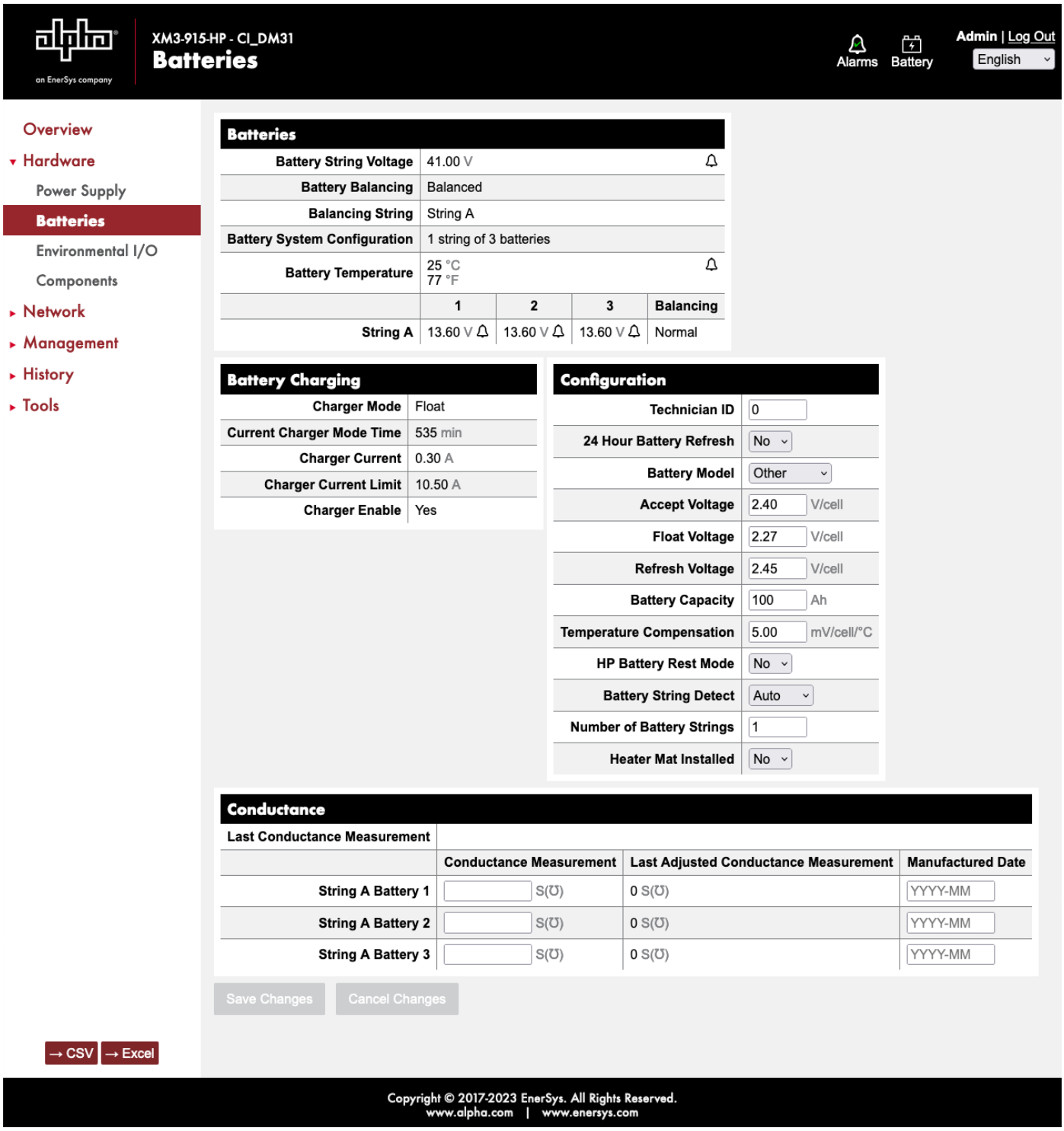


Fig. 8-3, Batteries Web Page

8.3 System Status Indicators and Reset Button

As viewed from the front of the unit, the DM31 transponder utilizes LEDs to indicate system status. During system start up, the LEDs will first blink momentarily then indicate the current status of a variety of parameters on the DM31 transponder. The LEDs indicate alarms, RF power level status, battery string connectivity and communications activity with the network. See **Section 7.4 DM31 Transponder LEDs and Connections** for LED locations and indications.

8.3.1 Detailed LED Descriptions

After power is applied or a reset occurs, all LEDs will flash in certain patterns indicating the cable modem chipset is starting or restarting. Once it is ready, it will begin the DOCSIS® requirement of searching for the downstream frequency lock and the LEDs will follow the detailed descriptions below.

ALM/RDY - Alarm/Ready

During normal operation, this LED blinks GREEN, indicating a heartbeat pulse from the processor. The frequency of flashing by this LED provides a visual alert for power supply discrete major and minor alarms, if configured in the property and discrete property tables of the SCTE-HMS MIB. The ALM LED (RED) is factory defaulted OFF. Refer to **Section 6.2.4 General Power Supply Alarms** for information on configuring the DM31 transponder for active monitoring and alarming. If an event triggers an HMS alarm, the ALM/RDY LED blinks RED according to the alarm type until the alarm has been resolved. For a minor alarm, the frequency of flashing (RED) will be more OFF than ON and for a major alarm the frequency of flashing will be (RED) more ON than OFF. If there are multiple active alarms, including one or more major alarms with one or more minor alarms, the major alarm will take precedence in terms of the indication.

Rx/Tx PWR - Receive/Transmit Power

The RF Power LED utilizes a tricolor LED to provide the installer a quick verification of the modem transmit (Tx) and receive (Rx) RF power levels. The RF PWR LED will illuminate green when both the cable modem Tx and cable modem Rx RF power levels are within the range as specified in the SCTE-HMS PropertyTable. The LED indicator illuminates blue when Rx and/or Tx levels are within the warning range as specified by the SCTE-HMS PropertyTable. The LED indicator illuminates red when Rx and/or Tx levels are outside the range as specified by the SCTE-HMS PropertyTable.

COM - Internal Communications

The COM LED flashes to indicate an exchange of information between the DM31 transponder and the Alpha® power supply.

PWR - DM31 Transponder Power

This LED is on when the DM31 transponder has power, even when just starting up.

DS - Downstream Communication

This LED indicates the state of the CM's attempt to gain a downstream signal. This process may take several seconds, depending on how long it takes the CM to locate a carrier signal and lock onto a channel. The LED flashes while searching for the downstream DOCSIS® channel and is on solid when the downstream channel is locked.

US - CM Registration

The upstream (US) LED indicates the state of the CM's attempt to establish an upstream (return path) connection. This process may take several seconds, depending upon how long it takes the CM and the CMTS to agree on a link. The LED flashes while establishing the upstream connection, and is on solid when that connection is ready.

OL - Network Communication Status

Once a downstream channel has been negotiated between the CM and CMTS, the modem attempts to register with the DHCP server and obtain the configuration file. This LED flashes while the process takes place. Once a ranging status of 'success' has been received, the LED will remain on solid. This is the best indication that the DM31 transponder is communicating with the CMTS in the headend.

LNK - CPE Activity

The Ethernet link LED remains ON when there is an active connection on the Ethernet port (e.g., a computer is connected for local diagnostics). This LED flashes while performing early authentication, IP connectivity, BPI initialization.

Refer to the following table for default ranges in the SCTE-HMS PropertyTable:

SCTE-HMS Property Table							
	Parameter	Alarm Enable	HiHi	Hi	Lo	LoLo	Deadband
Rx	docsIfDownChannelPower (OID:1.3.6.1.2.1.10.127.1.1.1.1.6)	00 (0F*)	150	100	-100	-150	15
Tx	docsIfCmStatusTxPower (OID:1.3.6.1.2.1.10.127.1.2.2.1.3)	00 (0C*)	550	500	00	00	15

Table 8-1, SCTE-HMS Property Table

By default, alarmEnable is set to 00 (disabled) to prevent unwanted SNMP traps but the LED behavior will function as if the alarmEnable were set to the values in the above table. If the alarmEnable bits are set to anything other than 00, the LEDs will then follow the behavior of the desired enable bit setting.

The above default values translate into the following RF power LED color ranges:

RF Power LED Color Ranges		
LED Color	Rx Range (dBmV)	Tx Range (dBmV)
Green	+10 to -10	0 to +50
Blue	+15 to +10 and -10 to -15	+50 to +55
Red	>+15 and <-15	>+55

Table 8-2, RF Power LED Color Ranges

The current RF level status for both the Rx and Tx are displayed in the DOCSIS Summary on the Overview web page (see below), providing verification of modem RF power levels.

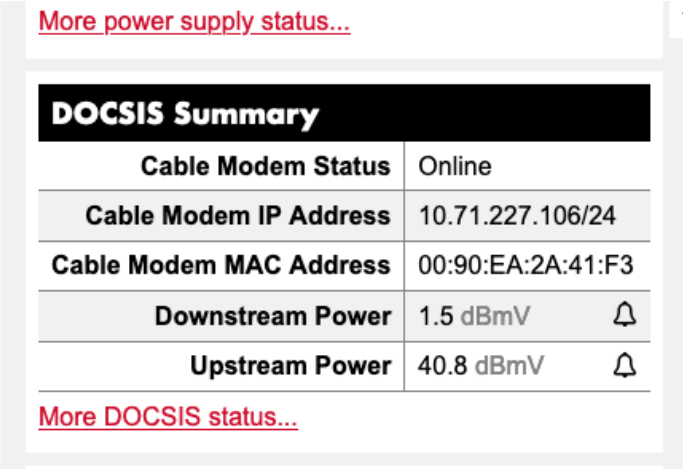


Fig. 8-4, DOCSIS Summary

Configuring the RF Power LED - Custom Settings

If desired, the RF Power Level ranges for the RF Power LED may be customized via SNMP by adjusting the HiHi, Hi, Lo, LoLo values for the docsIfDownChannelPower and docsIfCmStatusTxPower in the SCTE-HMS Property Table (OID:1.3.6.1.4.1.5591.1.1.1). Be careful not to exceed the RF Input Power and Output Power range specifications of the DM31 transponder.

Resetting the Transponder

Should the need arise to reset the transponder locally, such as in the case of adding additional power supplies, a generator, or carrying out maintenance activities, do the following:

Press and hold the reset button (RST) for approximately three (3) to four (4) seconds until the ALM/RDY LED stops blinking and turns solid (green). Release the button. The transponder will perform its power up sequence.

Note that holding down the reset button for 10 seconds will factory reset the power supply. (A factory reset clears all customer configuration choices before restarting.)

8.4 Verifying Communications via the Headend

Using SNMP, check connectivity by verifying power supply data by doing the following:

- With a MIB browser, check power supply data in the psIdent MIB branch (1.3.6.1.4.1.5591.1) of the SCTE-HMS tree.
- With network management software, verify the DM31 transponder has been identified and is reporting data correctly.

9.0 Specifications

General					
Power supply compatibility	Alpha® XM3-HP™ Broadband CableUPS, platform 14 (V.1.14.0) firmware or higher				
Hardware					
LAN Port (ETH)	1Gb/s Ethernet (RJ45)				
WAN Port (RF)	F-connector, 75 Ohms, DOCSIS® 3.0, 3.1 compliant, tested to 35 in-lb tightening torque using test method ANSI/SCTE 149 2019				
LEDs	**ALM/RDY** – DM31 transponder ready, major/minor alarm **RX/TX PWR** – RF power level **COM** – XM3-HP power supply communications **PWR** – DM31 transponder power		**DS** – Downstream RF carrier detection/lock **US** – Upstream RF carrier detection/lock **OL** – Registration lock **LNK** – Ethernet link		
Tamper (TPR)	Tamper switch input connection, compatible with normally open or normally closed magnetic enclosure door switch				
Environmental Interface (ENV)	General purpose monitoring and control signals				
Diplexer Options[1]	**Modem Model**	**Upstream Range 1**	**Downstream Range 1**	**Upstream Range 2**	**Downstream Range 2**
	DM31-H2	5 to 42 MHz	108 to 1002 MHz	5 to 85 MHz	108 to 1002 MHz[2]
	DM31-H3	5 to 45 MHz	258 to 1218 MHz	5 to 204 MHz	258 to 1218 MHz
	DM31-H4E (Euro)	5 to 85 MHz	108 to 1218 MHz	5 to 204 MHz	258 to 1218 MHz
XM3-HP Interface	DM31 transponder installs in XM3-HP communications module slot (RHS). Power and communications is via internal 18-pin ribbon cable. DM31 transponder maximum power draw is 15W.				
Reset / Watchdog	• Forced hardware reset interface control signal • Multi-level watchdog timers reset modem in the event of unforeseen lock-up. Eliminates truck rolls to reset unresponsive units.				

[1] Dual hardware diplexers per model. Range 1 and 2 are software selectable within each model. (Factory default: Range 1)
[2] A downstream upper limit frequency of 1218 MHz available with firmware upgrade.

Environmental	
Operating Temperature Range	-40 to 140°F (-40 to +60°C)
Storage Temperature Range	-40 to 185°F (-40 to +85°C)
Relative Humidity	0 to 95% non-condensing
Agency Compliance	
Regulatory / Standards (Verified with DM31 installed in application product)	**For safety standards and certification details, please reference the Alpha® XM3-HP™ Power Supply Technical Manual.** • **EN 50083 2:2006:** EMC requirements for CATV equipment • **EN 62040 2:2006:** Uninterruptable Power Systems (UPS) - Electromagnetic Compatibility (EMC) Requirements - Category C2 • **FCC Part 15** - Class A • **CISPR24/EN55024:** 10V/m radiated susceptibility • **IEEE® 587 - Category B3:** Surge, test method: 10 positive cycles/10 negative cycles, alternating • I**EEE® C62.41:** RF surge, 6,000V peak, combination wave., ten events, alternating positive and negative, using a 2 Ohm source impedance with "Outcome 1" per IEEE 62.45 • **IEC®/EN 61000-4-2:** Direct electrostatic contact discharge at 8kV at the RF connector shield without data loss • **RoHS® Compliant/Directive 2002/95/EC**

Table 9-1, Specifications

Advanced Diagnostics	
RF Network	• Full band capture data available through CableLabs® MIB and internal web server • Micro-reflection diagram available via internal web server
Power Supply Display	**Power supply display will show advanced network diagnostics including:** Upstream and downstream frequencies and RF levels, IPv4 or IPv6 address assigned by network DHCP server, MAC address, DOCSIS® timeout error codes and firmware versions
Utility Power Diagnostics	With XM3-HP™ power supply app card, utility performance status including outages, sags, surges and out-of-frequency events
Battery Diagnostics	With XM3-HP™ power supply app card, power supply diagnostics report when batteries should be serviced including battery string runtime remaining and battery life remaining
Event Logging	With XM3-HP™ power supply app card, logs include power supply events, power supply configurations and battery events
Features	
DOCSIS® 3.0 Bonded Channels	Up to 32 downstream Up to 8 upstream
DOCSIS® 3.1 OFDM Channels (receiver)	24 MHz to 192 MHz OFDM channels downstream Supports 2 OFDM channels and 24 SC-QAM channels SC Channel Modulation up to 4096 QAM
DOCSIS® 3.1 OFDMA Channels (transmitter)	96 MHz maximum OFDMA channel bandwidth upstream Supports 2 OFDMA channels ***NOTE: Dual 96MHz OFDMA operation requires 204 MHz upstream split***
Digital Step Attenuation (DSA)	Pre-diplexer, digital step attenuator (DSA) for RF receiver 0-31 dB attenuation range in 0.5 dB steps Software controlled
WAN Services Over DOCSIS®	• IPv4, IPv6, UDP, TCP, DHCP, TOD, TFTP, NAT, BPI, RIPv2, SNMPv1, SNMPv2c, SNMPv3, SSH, HTTP • TR-181 parameters over TR-069 and SNMP • Business Services over DOCSIS® (BSoD) supports L2VPN encrypted traffic • DNS address resolution WAN-LAN pass-through modes supported, see LAN DNS • Static IPv4, IPv6 configurable • Full spectrum capture (CableLabs® MIBs and HTML) • Full spectrum diagnostics (proprietary MIB) • Micro-reflections (HTML) • Constellation Diagrams (HTML)
Web Page	• Web interface accessible through WAN interface (Port 80 enabled via TLV) and local IP address LAN port • Write access password controlled, can be disabled using TLV in configuration file • Web interface displays operating parameters including: ◦ DOCSIS® parameters ◦ Ethernet diagnostics (e.g., RFC 2544, latency, jitter, frame loss) ◦ Full band capture statistics ◦ Micro-reflection statistics ◦ Constellation statistics ◦ Application specific parameters
Password of the Day (PotD) option	Operator provided date and seed. PotD encryption from 3DES / AES algorithm.
CableLabs® Compliance	DOCSIS® 3.1, Cable Modem, DOCSIS® 3.0 Cable Modem

Table 9-1, Specifications, continued

10.0 Glossary

10.1 Acronym Definitions

- ANSI: American National Standards Institute
- BER: Basic Encoding Rules [Bit Error Rate]
- CM: Cable Modem
- CMTS: Cable Modem Termination System
- CPE: Customer Premises Equipment
- DHCP: Dynamic Host Configuration Protocol
- DOCSIS: Data Over Cable Service Interface Specification
- EMS: Element Management System
- EVM: Error Vector Magnitude
- HMS: Hybrid Management Sublayer
- IT: Information Technology
- MAC: Media Access Control
- MER: Modulation Error Ratio
- MIB: Management Information Base
- NMS: Network Management System
- QoS: Quality of Service
- RTS: Remote Temperature Sensor
- SCTE: Society of Cable Telecommunications Engineers
- SI: Serial Interface
- SNMP: Simple Network Management Protocol
- SNTP: Simple Network Time Protocol
- TFTP: Trivial File Transfer Protocol
- TOD: Time of Day
- UDP: User Datagram Protocol
- VoIP: Voice over Internet Protocol

Worldwide Corporate Offices

Headquarter Germany

Hansastrasse 8
D-91126 Schwabach
Tel: +49 9122 79889 0

Mail: info@alpha-outback-energy.com

Eastern Europe
ee@alpha-outback-energy.com

Middle East
me@alpha-outback-energy.com

France and Benelux
fbnl@alpha-outback-energy.com

Spain
spain@alpha-outback-energy.com

Africa
africa@alpha-outback-energy.com

017-891-B14-001, Rev. A (04/2024)

For more information please visit **www.alpha-outback-energy.com**