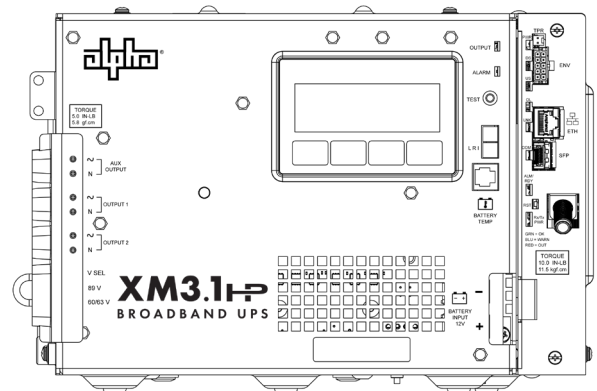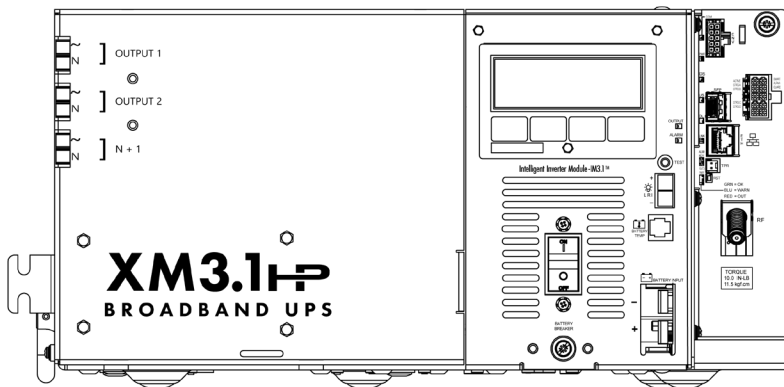**alpha®**

an EnerSys® company

XM3.1-HP™ Series Intelligent Broadband UPS Optical Status Monitoring User Guide

Effective: August 2024

Safety Notes

Review the content 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.

✓ NOTICE:

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

⚠ WARNING! GENERAL HAZARD

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

Sicherheitshinweise

Überprüfen Sie die in diesem Dokument enthaltenen Zeichnungen und Abbildungen, bevor Sie fortfahren. Wenn Sie Fragen zur sicheren Installation oder zum sicheren Betrieb des Systems haben, wenden Sie sich an Alpha Technologies Services, Inc. oder an die nächstgelegene Vertretung von Alpha®. Behalten Sie dieses Dokument zur späteren Verwendung.

Um die Verletzungs- oder Todesgefahr zu verringern und den sicheren Betrieb dieses Produkts zu gewährleisten, wurden die folgenden Symbole in diesem Handbuch durchgehend angebracht. Wo diese Symbole erscheinen, ist besondere Vorsicht und Aufmerksamkeit geboten.

✓ HINWEIS:

HINWEIS bietet zusätzliche Informationen, die bei der Erledigung einer bestimmten Aufgabe oder eines bestimmten Verfahrens helfen.

⚠ WARNUNG! ALLGEMEINE GEFAHR

ALLGEMEINE GEFAHR liefert dem Personal Sicherheitshinweise zur VERHÜTUNG VON VERLETZUNGEN ODER TOD.

Remarques sur la sécurité

Passez en revue les dessins et les illustrations contenus dans le présent document avant de procéder. Pour toute question concernant l'installation ou le fonctionnement sécuritaire du système, veuillez communiquer avec Alpha Technologies Services, Inc., ou le représentant Alpha^MC le plus près. Veuillez conserver le présent document pour le consulter ultérieurement.

Afin de réduire le risque de blessure ou de mort, et pour assurer le fonctionnement continu et sécuritaire de ce produit, les symboles suivants ont été répartis dans l'ensemble du manuel. Lorsque ces symboles sont présents, veuillez faire preuve de plus de prudence et d'attention.

✓ AVIS :

« AVIS » fournit des renseignements supplémentaires pour aider à terminer une tâche ou une procédure particulière.

⚠ AVERTISSEMENT! DANGER GÉNÉRAL

L'AVERTISSEMENT DE DANGER GÉNÉRAL fournit des renseignements sur la sécurité afin de PRÉVENIR LES BLESSURES au technicien ou à l'utilisateur, voire LA MORT.

Notas de Seguridad

Revise los dibujos e ilustraciones que figuran en este documento antes de continuar. Si tiene alguna pregunta sobre la instalación o el funcionamiento seguro del sistema, póngase en contacto con Alpha Technologies Services, Inc. o con el representante más cercano de Alpha®. Guarde este documento para futuras referencias.

Para reducir el riesgo de lesiones o muerte y para garantizar el funcionamiento seguro y continuo de este producto, se han colocado los siguientes símbolos en este manual. Cuando aparezcan estos símbolos, tenga mucho cuidado y atención.

✓ AVISO:

AVISO proporciona información adicional para ayudar a completar una tarea o procedimiento específico.

⚠ ¡ADVERTENCIA! RIESGO GENERAL

ADVERTENCIA DE RIESGO GENERAL proporciona información de seguridad para PREVENIR LESIONES O LA MUERTE al técnico o usuario.

Notas de Segurança

Veja os desenhos e ilustrações contidos neste documento antes de continuar. Se surgir qualquer dúvida sobre como instalar ou operar com segurança o sistema, contate a Alpha Technologies Services, Inc. ou o representante mais próximo da Alpha®. Guarde este documento para futuras consultas.

Para reduzir o risco de lesões ou morte e assegurar a operação segura continuada deste produto, os seguintes símbolos acompanham as instruções deste manual. Ao encontrar estes símbolos, recomenda-se maior precaução e atenção.

✓ AVISO:

AVISO fornece informações adicionais para ajudar a realizar um procedimento ou tarefa específica.

⚠ ATENÇÃO! RISCO GERAL

ALERTA DE RISCO GERAL fornece informações elétricas de segurança para EVITAR LESÕES OU MORTE de técnicos e usuários.

XM3.1-HP™ Series Intelligent Broadband UPS Optical Status Monitoring

User Guide

017-950-C0-001, Rev. B

Effective Date: August 2024

Disclaimer

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

Contact Information

Sales information and customer service in USA (7AM to 5PM, Pacific Time):	+1 800-322-5742
Complete technical support in USA (7AM to 5PM, Pacific Time or 24/7 emergency support):	+1 800-863-3364
Sales information and technical support in Canada:	+1 888-462-7487
Website:	www.alpha.com

Table of Contents

Figures

Tables

1.0 Optical Plant

This user guide provides information for using optical fiber networks for remote status monitoring of the Alpha® XM3.1-HP™ series of broadband power supplies.

An XM3.1-HP power supply can use an optical network as its connection to a back-office status monitoring system. An industry-standard gigabit small form-factor pluggable (SFP) socket on the power supply communications module allows connection to a variety of optical network types and layouts.

The optical network is a single fiber link between the SFP in the XM3.1-HP power supply and a network switch in the back-office. As long as the XM3.1-HP power supply has an optical Ethernet connection to the servers and client computers in the back-office, the power supply doesn't dictate the specifics of how the network traffic passes from the back-office to the SFP.

✓ NOTICE

For additional SFP communications options, see **Section 8.0 Addendum**.
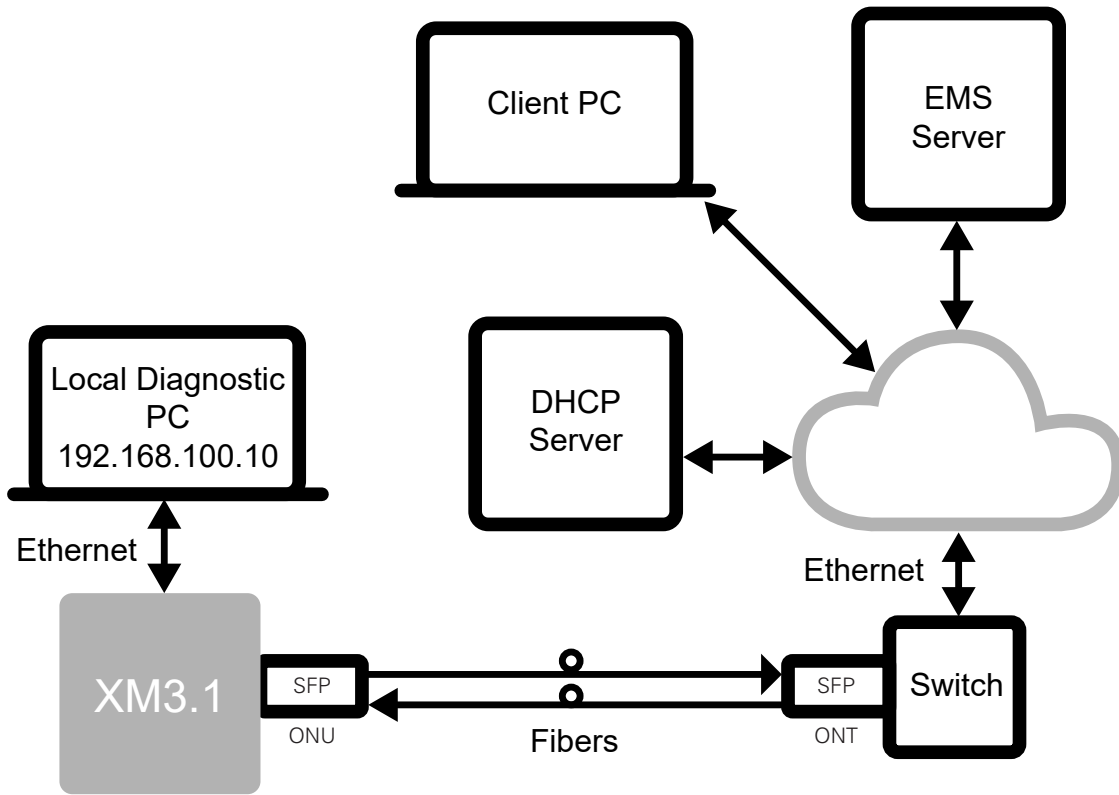
Fig. 1-1, Network Diagram Example

Typically, there is a network in the back-office, containing servers for the Element Management Systems (EMS) such as the Alpha® XD™ or Continuity™ platforms, Dynamic Host Configuration Protocol (DHCP) server, Trivial File Transfer Protocol (TFTP) server and time server. The power supply utilizes the optical link to join that network.

The Ethernet port on the power supply allows a local technician access to that power supply. However, the power supply does not function as a router: a computer connected to the local Ethernet connection cannot connect to the optical network to function as a Customer-premises equipment (CPE) device.

1.1   Installation

⚠ **WARNING! GENERAL HAZARD**

Do not look into the open end of an SFP module when the fiber is not installed, and do not look into the end of a fiber optic drop cable connector. The built-in laser may cause serious eye damage.

Install a small form-factor pluggable (SFP) optical module into the SFP socket on the Cable Modem Module (CMM) of the XM3.1-HP™ power supply, making sure the module latches into place (see **Fig. 1-2** and **Fig. 1-3**). Insert the associated fiber(s) into the opening on the protruding end of the module. (An EPON SFP module uses a single fiber connection; most point-to-point SFP modules use a dual fiber connection.) Avoid excessive bends and tight turns in optical fibers as these add optical attenuation. Note that the electrical interface is limited to 10/100/1,000 Mbps data rates, and RF (DOCSIS®) support is not available when the SFP module is installed.

SFP Module Recommendations:

- SFP form factor modules with communication standards to 1 Gbps.
- Utilize SFP optical modules rated for industrial operating temperatures.
- The SFP port supports the following SFP module power ratings:
  - EMM with blue or green colored PCBA supports SFP modules drawing up to 1.0W:
    - XM3.1-HP™ power supply: *p/n 704-00302-20-001* or *704-983-20-001*
    - XM3.1-HP™ power supply, 3 and 5 Amp models: *p/n 704-00304-20-001* or *704-00272-20-002*
  - EMM with red colored PCBA supports SFP modules drawing up to 3.3W:
    - XM3.1-HP power supply: *p/n 704-00302-20-002*
    - XM3.1-HP power supply, 3 and 5 Amp models: *p/n 704-00304-20-002*
- Areas with hotter climates may require enclosure fan kits and/or SFP extension cables to meet the SFP thermal ratings.
- An RJ45 copper SFP module should only be used for a short connection to another communications device within the same cabinet.
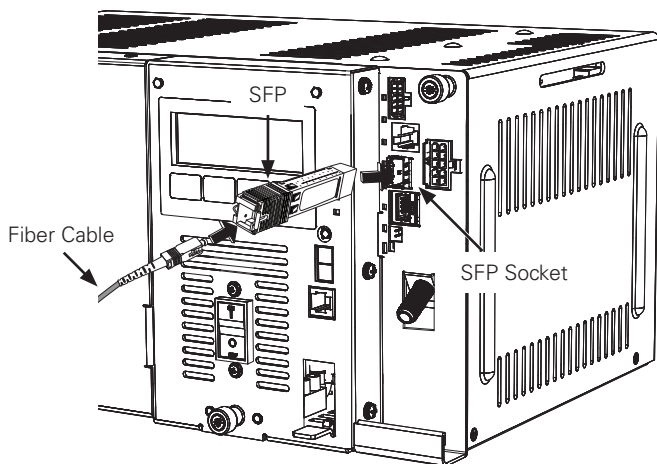
Fig. 1-2, Installing SFP in XM3.1-HP™ Power Supply
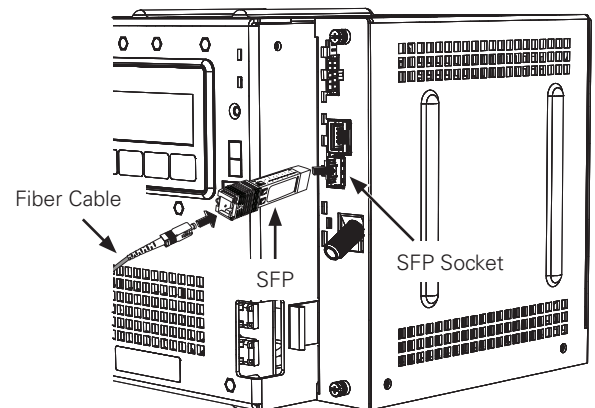
Fig. 1-3, Installing SFP in XM3.1-HP™ Power Supply (3 and 5 Amp models)

The status of the SFP link is indicated on the online (OL) LED as follows:

- **OFF:** No SFP module or there is no signal from the other end of the fiber.
- **FLASHING:** The CMM is registering with the network.
- **ON:** The optical link is ready for use.

1.0   Optical Plant, continued

Many SFP modules include Digital Diagnostics Monitoring (DDM) capabilities, which monitor key parameters of the module in real time. For any module that reports status warnings and alarms, whenever there is an optical link, the Rx/Tx PWR LEDs indicate the status of the receiver optical power as follows:

- **GREEN:** The receiver and transmit power levels are acceptable (or the SFP module doesn't report power status).
- **BLUE:** There is a WARNING for the receive power level.
- **RED:** There is an ALARM for the receive power level

When the Rx/Tx PWR LEDs indicate SFP receive power (and not DOCSIS RF power levels), the indicated LED briefly blinks off once per second. If there is an SFP module installed, but there is not an optical link, the Rx/Tx PWR LEDs briefly blink red once per second.

The particular ranges for warnings and alarms are specific to the SFP module. The Rx/Tx PWR LEDs only indicate the receiver optical power status, not the transmit optical power, because warnings or alarms for the transmit optical power represent a problem with the SFP module rather than with the optical link.

NOTICE:
For more detail on LED statuses and functions, see **Section 5.1 LEDs**.

2.0 Provisioning

An XM3.1-HP™ power supply with an SFP will go through a number of steps while coming online with the optical network. This section describes those steps.

2.1 Obtain an IP Address

The power supply requires an IP address to communicate over the optical link. By default, the power supply looks for both IPv4 and IPv6 addresses. It is not necessary to obtain both types of address, but provisioning cannot proceed until the power supply has at least one valid IP address.

2.1.1 IPv4 Address

By default, the power supply uses the DHCP protocol to request an IPv4 address, network scope, default gateway and other parameters through the optical link. The gateway from the DHCP offer is also used.

As an alternative to using DHCP, a fixed IP address, prefix length, and gateway can be configured for the optical link. This configuration can be performed locally, using address 192.168.100.1 through the Ethernet port, with either web page access or SNMP. The power supply can also be configured to not use any IPv4 address over the optical link.

SNMP settings for the IPv4 address are shown in **Table 2-1**. Use index .11 for the optical communications link.

OIDS FOR IPV4 ADDRESS CONFIGURATION			
COMPONENT	DESCRIPTION	DEFAULT	VALUES
atiMgmtSysCommsIpv4Mode 1.3.6.1.4.1.926.1.3.2.11.4.2.1.1	A setting for how the communications link obtains an IPv4 address.	dhcp(2)	disabled(1) dhcp(2) fixed(3)
atiMgmtSysCommsIpv4FixedAddress 1.3.6.1.4.1.926.1.3.2.11.4.2.1.2	When atiMgmtSysCommsIpv4Mode is set to fixed(3), this value is the IP address used by this communications link.	0.0.0.0	Any valid IPv4 address
atiMgmtSysCommsIpv4FixedPrfxLen 1.3.6.1.4.1.926.1.3.2.11.4.2.1.3	When atiMgmtSysCommsIpv4Mode is set to fixed(3), this value is the CIDR IPv4 prefix length used by this communications link.	24	0 — 32
atiMgmtSysCommsIpv4FixedGateway 1.3.6.1.4.1.926.1.3.2.11.4.2.1.4	When atiMgmtSysCommsIpv4Mode is set to fixed(3), AND this value is a valid IP address (not 0.0.0.0), then the product includes a route rule for the specified gateway.	0.0.0.0	Any valid IPv4 address

Table 2-1, OIDs for IPv4 Address Configuration

These settings may also be changed from the "SFP" web page when logged in with administrative rights. The IP address and prefix length are represented in a single field. A Classless Inter-Domain Routing (CIDR) prefix length of "24" is equivalent to a netmask of 255.255.255.0.

Fig. 2-1, Web Page IPv4 Address Configuration

2.1.2   IPv6 Address

By default, the transponder attempts to auto-configure an IPv6 address, following the Stateless Address Auto-configuration (SLAAC) protocol, and also attempts to request an IPv6 address using DHCPv6. (These two mechanisms are not mutually exclusive.)

Alternatively, a fixed IPv6 address, prefix length, and gateway can be configured for the optical link. The power supply can also be configured to only use a link local address for IPv6. The power supply can also be configured to not use any IPv6 address over the optical link.

SNMP settings for the IPv6 address are shown in **Table 2-2**. Use index .11 for the optical communications link.

OIDS FOR IPV6 ADDRESS CONFIGURATION			
COMPONENT	DESCRIPTION	DEFAULT	VALUES
atiMgmtSysCommsIpv6Mode 1.3.6.1.4.1.926.1.3.2.11.4.3.1.1	A setting for how the communications link obtains an IPv6 address.	auto(2)	disabled(1) auto(2) fixed(3) linkLocalOnly(4)
atiMgmtSysCommsIpv6FixedAddress 1.3.6.1.4.1.926.1.3.2.11.4.3.1.2	When atiMgmtSysCommsIpv6Mode is set to fixed(3), this value is the IP address used by this communications link.	::	Any valid IPv6 address, as an octet string
atiMgmtSysCommsIpv6FixedPrfxLen 1.3.6.1.4.1.926.1.3.2.11.4.3.1.3	When atiMgmtSysCommsIpv6Mode is set to fixed(3), this value is the IPv6 prefix length used by this communications link.	64	0 — 128
atiMgmtSysCommsIpv6FixedGateway 1.3.6.1.4.1.926.1.3.2.11.4.3.1.4	When atiMgmtSysCommsIpv6Mode is set to fixed(3), AND this value is a valid IP address (not ::), then the product includes a route rule for the specified gateway.	::	Any valid IPv6 address, as an octet string

Table 2-2, OIDs for IPv6 Address Configuration

These settings may also be changed from the "SFP" web page when logged in with administrative rights. The IP address and prefix length are represented in a single field.

Fig. 2-2, Web Page IPv6 Address Configuration

2.1.3   MAC Address

If the DHCP/DHCPv6 server gives out specific offers based upon the MAC address of the requesting device, the technician will need to know the MAC address used for the power supply. The power supply uses a MAC address for the optical link that is one higher than the MAC address for the cable modem link. To do this, add one to the MAC address listed on the label of the power supply.

Example: If the cable modem MAC address printed on the label is 00:90:EA:29:CE:F3, then the optical link is using MAC address 00:90:EA:29:CE:F4. If the cable modem MAC address printed on the label is 00:90:EA:29:CE:FF, then the optical link is using MAC address 00:90:EA:29:CF:00.

The optical link MAC address is also reported on the LCD (first entry in the "SFP - GENERAL" menu), and on the web user interface ("Overview" and "SFP" pages).

2.2   Obtain the Time of Day

Once the power supply has an IP address, it retrieves the current time from the network. (Without a proper time of day, the time stamps on log entries are not meaningful.)

A DHCP offer in IPv4 can tell the transponder how to retrieve the time. If the offer includes an "option time-servers" entry (DHCP option 4), each provided address is queried, in order, for the current time using the RFC 868 TCP/IP time protocol, stopping on the first success. If the offer includes an "option ntp-servers" entry (DHCP option 42), each provided address is queried, in order, for the current time using Simple Network Time Protocol (SNTP), stopping on the first success. Time servers provide UTC time, not local time. If the offer includes an "option time-offset" entry (DHCP option 2), that value is used as the adjustment from the time server to local time.

Similarly, the DHCPv6 offer can specify time server information. DHCPv6 includes a standard option for dhcp6.sntp-servers (DHCPv6 option 31); there is no standard DHCPv6 option for an RFC 868 TCP/IP time server or for a time zone offset, but both are specified within the CableLabs® vendor-specific option. If this is the configured setup for DOCSIS® IPv6, the same option response can be used for the optical link.

If the optical network isn't using DHCP/DHCPv6 or if fallback settings are required, a fixed time server address, protocol and time zone offset can be configured. See **Table 2-3** for time server settings.

The optical link provisioning tries a maximum of ten times to retrieve the time from the specified server(s). If the time has not been determined after ten attempts, the provisioning process continues despite not having a valid time set. To verify the system obtained a valid time, check atiMgmtSysCommsTimeStatus in SNMP or on the SFP web page.

OIDS FOR TIME SERVER CONFIGURATION			
COMPONENT	DESCRIPTION	DEFAULT	VALUES
atiMgmtSysCommsTimeServAddrType 1.3.6.1.4.1.926.1.3.2.11.1.4.1	This object and atiMgmtSysCommsTimeServerAddr specify a time server that can be used to establish the time of day at startup if no time server is otherwise known (from a DHCP offer).	unknown(0)	unknown(0) ipv4(1) ipv6(2)
atiMgmtSysCommsTimeServerAddr 1.3.6.1.4.1.926.1.3.2.11.1.4.2	This object and atiMgmtSysCommsTimeServAddrType specify a time server that can be used to establish the time of day at startup if no time server is otherwise known (from a DHCP offer).		Any valid IPv4 or IPv6 address, as an octet string
atiMgmtSysCommsTimeServerType 1.3.6.1.4.1.926.1.3.2.11.1.4.3	This object selects the type of time server indicated by atiMgmtSysCommsTimeServerAddr.	none(1)	none(1) ntp(2) time(3)
atiMgmtSysCommsTimeOffset 1.3.6.1.4.1.926.1.3.2.11.1.4.4	This object specifies the time zone adjustment, in seconds, to apply to Coordinated Universal Time (UTC) to yield the local time. Positive values are for time zones east of the prime meridian, and negative values are for time zones west of the prime meridian.	0	Offset value
atiMgmtSysCommsTimeStatus 1.3.6.1.4.1.926.1.3.2.11.1.4.5	This optional object indicates whether the system has obtained a real time clock setting from an external source.		notSet(1) set(2)
atiMgmtSysCommsTimeSrcAddrType 1.3.6.1.4.1.926.1.3.2.11.1.4.6	This optional object and atiMgmtSysCommsTimeSrcAddr specify the time server that provided an external real time clock setting. This object is only available when atiMgmtSysCommsTimeStatus shows set(2).		unknown(0) ipv4(1) ipv6(2
atiMgmtSysCommsTimeSrcAddr 1.3.6.1.4.1.926.1.3.2.11.1.4.7	This optional object and atiMgmtSysCommsTimeSrcAddrType specify the time server that provided an external real time clock setting. This object is only available when atiMgmtSysCommsTimeStatus shows set(2).		Any valid IPv4 or IPv6 address, as an octet string

Table 2-3, OIDs for Time Server Configuration

These settings may also be changed from the SFP web page when logged in with administrative rights.

Time Server Results	Set from 172.24.1.1
Fallback Time Protocol	None
Fallback Time Server	0.0.0.0

Fig. 2-3, Web Page Time Server Configuration

2.3   Obtain a Configuration File

After obtaining the time (or failing), the power supply loads a configuration file. This is an optional text file of arbitrary SNMP set operations to perform before coming fully online.

The IPv4 DHCP offer can tell the transponder where to get the configuration file. If the offer includes a "server-name" entry (BOOTP field) or an "option tftp-server-name" entry (DHCP option 66), the transponder tries those locations in that order. If the offer includes a "filename" entry (BOOTP field) or an "option bootfile-name" entry (DHCP option 67), the transponder tries those names in that order.

Similarly, the DHCPv6 offer can specify a configuration file within the CableLabs® vendor-specific option, which uses the same setup in the DHCP server as IPv6 DOCSIS.

If DHCP is not being used, or if fallback settings are required, a fixed server IP address and/or filename can be configured to be used after any DHCP fields. See **Table 2-4, Configuration File Status and Troubleshooting** for configuration file settings.

The power supply tries each combination of IP address (from DHCP and/or fixed address) and filename (from DHCP and/or fixed name), until one of these combinations retrieves and successfully processes a configuration file. If none of the combinations succeeds after three tries, provisioning continues.

2.3.1   Configuration File Syntax

The configuration file is a simple text file of SNMP object assignments. Each non-blank line should be an OID (Object Identifier), a type and a value to set. The # symbol indicates a comment. Only the part of a line prior to any # is processed. The "type" can be any of the following:

- Int - the value is a signed number: hexadecimal if preceded by "0x", octal if preceded by "0", and decimal otherwise.
- String - the value is any characters on the rest of the line past the space(s) following the "string" token, treated as a text string.
- Octet - the rest of the line is converted to a string of bytes, taking one- or two-digit hex byte values, separated by spaces
- IP - the value is a dotted IPv4 address
- OID - the value is a numeric SNMP OID

2.3.2   Example Configuration File

Here is an example configuration file, to set up a trap address using the SNMP target address table:

Designations: OID tree is Green, OID table is Blue, OID table reference is Orange, OID table function Red

```
# Sample config file for testing SNMPv2 setup

# snmpTargetAddrTDomain.Test1 = snmpUDPDomain
1.3.6.1.6.3.12.1.2.1.2.84.101.115.116.49 oid 1.3.6.1.6.1.1
# snmpTargetAddrTAddress.Test1 = 172.16.42.101:162 (AC.10.2A.65:00A2)
1.3.6.1.6.3.12.1.2.1.3.84.101.115.116.49 octet AC 10 2A 65 00 A2
# snmpTargetAddrParams.Test1 = Test
1.3.6.1.6.3.12.1.2.1.7.84.101.115.116.49 string Test
# snmpTargetAddrRowStatus.Test1 = active
1.3.6.1.6.3.12.1.2.1.9.84.101.115.116.49 int 1
# snmpTargetParamsMPModel.Test = SNMPv2c
1.3.6.1.6.3.12.1.3.1.2.84.101.115.116 int 1
# snmpTargetParamsSecurityModel.Test = SNMPv2c
1.3.6.1.6.3.12.1.3.1.3.84.101.115.116 int 2
# snmpTargetParamsSecurityName.Test = Test
1.3.6.1.6.3.12.1.3.1.4.84.101.115.116 string Test
# snmpTargetParamsSecurityLevel = noAuthNoPriv
1.3.6.1.6.3.12.1.3.1.5.84.101.115.116 int 1
# snmpTargetParamsRowStatus.Test = active
1.3.6.1.6.3.12.1.3.1.7.84.101.115.116 int 1
# snmpCommunityName.Test = TestTrap
1.3.6.1.6.3.18.1.1.1.2.84.101.115.116 string TestTrap
# snmpCommunitySecurityName = Test
1.3.6.1.6.3.18.1.1.1.3.84.101.115.116 string Test
# snmpCommunityStatus = active
1.3.6.1.6.3.18.1.1.1.8.84.101.115.116 int 1
```

Fig. 2-4, SNMPv2 Setup Configuration File Example

The sample follows a useful convention of a comment of what the setting is doing, followed by the setting itself. See SNMP-COMMUNITY-MIB for the particular settings used in this example.

The XM3.1 communication configuration file is in a text format; the characters and line feeds are OS agnostic, but file has to be in straight text UTF8 format

2.3.3   Configuration File Status and Debugging

The power supply reports the outcome of the configuration file processing in SNMP. Verify the count of entries (not counting blank lines or comment lines) that were processed successfully, and the count of entries that were not processed successfully.

Some entries may be tagged as invalid because SNMP also reports the first line number where an invalid entry was detected and the specific error message for that first invalid entry. (Line numbers do include blank lines and comment lines.) When creating a new configuration file, the power supply can be manually instructed to re-process the configuration file, which also updates the reported counts of successful and unsuccessful entries, the line number of the first unsuccessful entry and the error message associated with the first unsuccessful entry. See **Table 2-4**.

CONFIGURATION FILE STATUS AND TROUBLESHOOTING			
COMPONENT	DESCRIPTION	DEFAULT	VALUES
atiMgmtSysCfgFileName 1.3.6.1.4.1.926.1.3.2.11.1.3.1	This object provides the name of the most recently loaded configuration file.		File name
atiMgmtSysCfgFileSuccessful 1.3.6.1.4.1.926.1.3.2.11.1.3.2	This object provides the count of successfully loaded lines or entries from the most recently loaded configuration file.	0	Count
atiMgmtSysCfgFileSkipped 1.3.6.1.4.1.926.1.3.2.11.1.3.3	This object provides the count of lines or entries from the most recently loaded configuration file which represented unrecognized indexes of recognized OIDs. These items are skipped, but not considered to be errors.	0	Count
atiMgmtSysCfgFileUnsuccessful 1.3.6.1.4.1.926.1.3.2.11.1.3.4	This object provides the count of lines or entries from the most recently loaded configuration file which were NOT able to be processed.	0	Count
atiMgmtSysCfgFileErrorItem 1.3.6.1.4.1.926.1.3.2.11.1.3.5	This object provides the index of the first line in the most recently loaded configuration file which was not able to be processed.		Line number
atiMgmtSysCfgFileErrorMessage 1.3.6.1.4.1.926.1.3.2.11.1.3.6	This object provides a brief description of the specific problem with the first line or entry in the most recently loaded configuration file which was not able to be processed.		Error message
atiMgmtSysCfgFileReload 1.3.6.1.4.1.926.1.3.2.11.1.3.7	Setting this object to forceReload(1) causes the configuration file processing to be manually restarted.	normal(0)	normal(0) forceReload(1)
atiMgmtSysCfgFileServerAddrType 1.3.6.1.4.1.926.1.3.2.11.1.3.8	This object and atiMgmtSysCfgFileServerAddr specify a TFTP server that can be used to download a configuration file at startup if no TFTP server is otherwise known (from a DHCP offer).	unknown(0)	unknown(0) ipv4(1) ipv6(2)
atiMgmtSysCfgFileServerAddr 1.3.6.1.4.1.926.1.3.2.11.1.3.9	This object and atiMgmtSysCfgFileServerAddrType specify a TFTP server that can be used to download a configuration file at startup if no TFTP server is otherwise known (from a DHCP offer).		Any valid IPv4 or IPv6 address, as an octet string
atiMgmtSysCfgFileFilename 1.3.6.1.4.1.926.1.3.2.11.1.3.10	This object specifies the name of a configuration file to download at startup if no filename is otherwise known (from a DHCP offer).		File name

Table 2-4, Configuration File Status and Troubleshooting

These settings may also be changed from the SFP web page when logged in with administrative rights.

Configuration File	sfpcfg.txt
Configuration Results	Successful: 12; skipped: 0; unsuccessful: 0
Fallback Config Server	0.0.0.0
Fallback Config File	
	Reload Configuration File

Fig. 2-5, Web Page Configuration File Settings

2.4   Send an HMS Start Trap

Once the power supply has at least one SNMP trap server or IP address, and has the network time (or failed trying to obtain the time), and has processed a configuration file (or failed trying to obtain a configuration file), the final step in coming online is to issue an HMS cold-start or warm-start trap to the known server(s). This notification indicates to the server that the power supply is online.

The difference between the HMS cold-start trap and the HMS warm-start trap is whether the power supply has a different configuration than the last time it sent out an HMS start trap. The power supply computes a "check code" from the current configuration (including most non-volatile settings) and compares that value against the check code used when the last HMS start trap was issued. If the configuration is unchanged (same check code value) since the previous startup, the power supply issues an HMS warm-start trap. If the configuration (check code) has changed, the power supply issues an HMS cold-start trap.

This notifies the EMS server of the existence of the power supply. This only helps if the power supply already knows the IP address of the EMS server in order to send these traps. Refer to **Section 3.3 Notifications and Traps** for more detail. The server IP address could have previously been set up in non-volatile memory (see atiMgmtSnmpTrapTable in ATI-MGMT-SNMP-MIB) or it might be added to the SNMPv2 targets table using the configuration file, like the previous example (see snmpTargetAddrTable in SNMP-COMMUNITY-MIB).

3.0   Communicating with the Power Supply

There are several ways to interact with the power supply on an optical network. In a production setup, SNMP is the primary interface, but web page access is the most helpful for local technician access and initial testing.

3.1 HTTP / HTTPS

The power supply offers a set of web pages for easy troubleshooting. This is mostly used by a technician on site with the power supply, but also functions over the optical link.

For local access, connect to the local Ethernet port on the power supply and use address 192.168.100.1. (The connecting computer must be configured with a fixed IP address in the 192.168.100.0/24 subnet.) Over the optical link, use any IP address (IPv4 or IPv6) that the power supply has established.

The power supply web pages are also accessible remotely via a web browser on a network connected computer to the transponder's routable IP address.

Refer to the technical manual for the power supply model for more information on the web interface. The "SFP" page in the "Network" section deals with specific details of the optical link. (Note that this page may not be shown in the navigation tree on a power supply that doesn't have any SFP installed.)

Some of the settings for the power supply, including some details of the SFP page, may be configured through the web interface. Log in to the web pages in order to make changes. Refer to the technical manual for your power supply for details on login credentials and permissions.

3.2 Simple Network Management Protocol (SNMP)

The primary management interface is SNMP. A Continuity™ or Alpha® XD™ EMS server interacts with the power supply using the SNMP protocol over the optical link, in just the same way that these EMS systems interact with power supplies over a DOCSIS® link.

3.2.1   SNMP Access

SNMPv1 and SNMPv2 use a simple unsecured "community string" to filter out transactions that are not expected to be of interest. The power supply has two methods of choosing what community strings to accept. The simplest method involves two non-volatile settings for the community string to expect for "gets" (any read or MIB walk) and the community string to expect for "sets" (any alteration of an SNMP object). These are initially set to "AlphaGet" and "AlphaSet," respectively. If either of these settings are empty, there is no acceptable community string for the indicated operation.

A more specific method is to set up a list of acceptable IP addresses, the community string to accept for that range, and whether to permit both reads and writes, or just reads. This table is not persistent across a restart, and would need to be set up using a configuration file. If the table has any entries, then the global settings described in the previous paragraph are not used. The power supply checks all the entries to see that there both is an entry under which access should be allowed, and there is not an entry under which access should be forbidden. Use index .11 for the communications link followed by a row number for each rule.

COMMUNICATIONS ACCESS SETTINGS			
COMPONENT	DESCRIPTION	DEFAULT	VALUES
atiMgmtSysCommsAccessCmtyGet 1.3.6.1.4.1.926.1.3.2.11.2.1.1	This string defines an SNMP community string that may be used for 'get' operations from any client on any communications link, when there is not yet a read/write entry in atiMgmtSysCommsAccessTable. If this string is empty, there is no global community string for 'get' operations.	AlphaGet	Community string
atiMgmtSysCommsAccessCmtySet 1.3.6.1.4.1.926.1.3.2.11.2.1.2	This string defines an SNMP community string that may be used for 'set' operations from any client on any communications link, when there is not yet a read/write entry in atiMgmtSysCommsAccessTable. If this string is empty, there is no global community string for 'set' operations.	AlphaSet	Community string
atiMgmtSysCommsAccessTable 1.3.6.1.4.1.926.1.3.2.11.2.2	Table of dynamic access rules.		
atiMgmtSysCommsAccessAddressType 1.3.6.1.4.1.926.1.3.2.11.2.2.1.2	The type of address of the permitted client(s).	unknown(0)	unknown(0) ipv4(1) ipv6(2)
atiMgmtSysCommsAccessAddress 1.3.6.1.4.1.926.1.3.2.11.2.2.1.3	The address of the permitted client(s).		
atiMgmtSysCommsAccessPrefixLen 1.3.6.1.4.1.926.1.3.2.11.2.2.1.4	The number of bits of atiMgmtSysCommsAccessAddress that must match for the entry to apply to a particular client. A prefix length of 0 means that any address can match this entry. A prefix length equal to the number of bits in the address (32 for IPv4, 128 for IPv6) means that the address must match exactly. Any other prefix length means that a range of addresses may match.	0	0 — 128
atiMgmtSysCommsAccessCommunity 1.3.6.1.4.1.926.1.3.2.11.2.2.1.5	This object specifies the community string to be accepted for both 'get' and 'set' operations by a client matching this entry.		Community string
atiMgmtSysCommsAccessLevel 1.3.6.1.4.1.926.1.3.2.11.2.2.1.6	This object specifies the level of access granted to a client that matches the network address and community string values of this entry. An entry marked as noAccess prohibits any access, regardless of the community string, for a matching network address even if another entry grants access.	noAccess(1)	noAccess(1) read(2) readWrite(3)

Table 3-1, Communications Access Settings

3.0   Communicating with the Power Supply, continued

When setting up dynamic access rules in a configuration file, it is important to use the correct index value with each OID. Any object within atiMgmtSysCommsAccessTable takes two index values: the communications link to which it applies (always use "11" for the optical link) and a particular row number. For example, if three rules are set up, there should be three OIDs ending in .11.1, .11.2 and .11.3.

```
# Sample config file for setting up SNMP access rules

# Allow read access for anyone in 172.24.1.x...
# atiMgmtSysCommsAccessAddress.11.1 = 172.24.1.0
1.3.6.1.4.1.926.1.3.2.11.2.2.1.3.11.1 octet AC 18 01 00
# atiMgmtSysCommsAccessPrefixLen.11.1 = 24
1.3.6.1.4.1.926.1.3.2.11.2.2.1.4.11.1 int 24
# atiMgmtSysCommsAccessCommunity.11.1 = public
1.3.6.1.4.1.926.1.3.2.11.2.2.1.5.11.1 string public
# atiMgmtSysCommsAccessLevel.11.1 = read(2)
1.3.6.1.4.1.926.1.3.2.11.2.2.1.6.11.1 int 2


# Allow read/write access for only 172.24.1.42...
# atiMgmtSysCommsAccessAddress.11.2 = 172.24.1.42
1.3.6.1.4.1.926.1.3.2.11.2.2.1.3.11.2 octet AC 18 01 2A
# atiMgmtSysCommsAccessPrefixLen.11.2 = 32
1.3.6.1.4.1.926.1.3.2.11.2.2.1.4.11.2 int 32
# atiMgmtSysCommsAccessCommunity.11.2 = private
1.3.6.1.4.1.926.1.3.2.11.2.2.1.5.11.2 string private
# atiMgmtSysCommsAccessLevel.11.2 = readWrite(3)
1.3.6.1.4.1.926.1.3.2.11.2.2.1.6.11.2 int 3
```

Fig. 3-1, SNMP Access Rules Configuration File Example

3.2.2 Information Available Using SNMP

When an SNMP client (the EMS system, or a computer with a MIB browser) accesses the power supply, usually the information of interest is the power supply status. This information is reported primarily using the SCTE HMS power supply MIB objects (see SCTE-HMS-PS-MIB) and/or the Alpha-specific power supply MIB objects (see ATI-DEV-POWER-SUPPLIES-MIB and ATI-DEV-BATTERIES-MIB).

In most cases, the SNMP support for a power supply over the optical link is the same as the SNMP support for a power supply over a DOCSIS® link, except there is no DOCSIS information to report.

Depending upon the capabilities of the SFP module, a variety of information can be reported over SNMP and the web page about that module and optical link. Note that only an SFP with Digital Diagnostics Monitoring (DDM) capabilities is able to report real-time status information about the optical link. See Section **Table 3-2, SFP Module Information**, and **Table 3-3, Alarmable SFP Status Information**. Use index .11 for the optical communications link.

SFP MODULE INFORMATION			
COMPONENT	DESCRIPTION	DEFAULT	VALUES
atiMgmtSysCommsOptInfoDescrip 1.3.6.1.4.1.926.1.3.2.11.3.1.1.1	This object provides a brief text description of the optical link hardware.		Text
atiMgmtSysCommsOptInfoVendor 1.3.6.1.4.1.926.1.3.2.11.3.1.1.2	This object provides the name of the vendor for the hardware element (SFP, etc.) supporting the optical link.		Vendor name
atiMgmtSysCommsOptInfoPartNum 1.3.6.1.4.1.926.1.3.2.11.3.1.1.3	This object provides the vendor part number for the hardware element (SFP, etc.) supporting the optical link.		Part number
atiMgmtSysCommsOptInfoRevision 1.3.6.1.4.1.926.1.3.2.11.3.1.1.4	This object provides the vendor revision ID for the hardware element (SFP, etc.) supporting the optical link.		Revision
atiMgmtSysCommsOptInfoSerialNum 1.3.6.1.4.1.926.1.3.2.11.3.1.1.5	This object provides the vendor serial number for the hardware element (SFP, etc.) supporting the optical link.		Serial number
atiMgmtSysCommsOptInfoOui 1.3.6.1.4.1.926.1.3.2.11.3.1.1.6	This object provides the Organizationally Unique Identifier (OUI) for the vendor of the hardware element (SFP, etc.) supporting the optical link.		Octet string, 3 bytes
atiMgmtSysCommsOptInfoMfgDate 1.3.6.1.4.1.926.1.3.2.11.3.1.1.7	This object provides the date of manufacture of the hardware element (SFP, etc.) supporting the optical link.		Year/month/day as octet string
atiMgmtSysCommsOptInfoWavelength 1.3.6.1.4.1.926.1.3.2.11.3.1.1.8	This object provides the laser wavelength for the hardware element (SFP, etc.) supporting the optical link.		Wavelength
atiMgmtSysCommsOptInfoDdm 1.3.6.1.4.1.926.1.3.2.11.3.1.1.9	This object indicates what level of support the SFP offers for digital diagnostics monitoring (per the SFF-8472 standard).		none(1) unsupported(2) internalCal(3) externalCal(4)
atiMgmtSysCommsOptExtState 1.3.6.1.4.1.926.1.3.2.11.3.3.1.1	This object represents the overall status of the optical communications link.		unknown(0) notInstalled(1) noLink(2) failure(3) portReady(4) provisioning(5) mgmtReady(6) disabled(7)
atiMgmtSysCommsOptExtRawModInfo 1.3.6.1.4.1.926.1.3.2.11.3.3.1.2	This object presents the serial ID data from the communications module (SFP, etc.), as defined by INF-8074i.		Octet string, 96 bytes
atiMgmtSysCommsOptExtModuleInst 1.3.6.1.4.1.926.1.3.2.11.3.3.1.3	This object indicates whether the communications module (SFP, etc.) is presently installed.		notInstalled(1) installed(2)
atiMgmtSysCommsOptCtrlTx 1.3.6.1.4.1.926.1.3.2.11.3.4.1.1	A setting for whether the transmitter is enabled or disabled for this link. A user may want to turn the transmitter off for a high-powered laser while changing fibers.	on(2)	off(1) on(2)
atiMgmtSysCommsOptCtrlHwRateSel 1.3.6.1.4.1.926.1.3.2.11.3.4.1.2	A setting for the rate selection signal for this link. This controls pin 7 of the SFP module. The specific result of either pin state is dependent upon the particular SFP module.	pinHigh(2)	pinLow(1) pinHigh(2)

Table 3-2, SFP Module Information

ALARMABLE SFP STATUS INFORMATION			
COMPONENT	DESCRIPTION	DEFAULT	VALUES
atiMgmtSysCommsOptStRxPwr 1.3.6.1.4.1.926.1.3.2.11.3.2.1.1	This object represents the optical power measured by the receiver, expressed in units of 1 microwatt.		Receive power
atiMgmtSysCommsOptStRxPwrAlm 1.3.6.1.4.1.926.1.3.2.11.3.2.1.2	This object represents the alarm state of the receiver optical power. The alarm state is determined on the basis of device-specific criteria, NOT by levels in the limit properties table.		noAlarm(1) alarmHi(2) warningHi(3) warningLo(4) alarmLo(5)
atiMgmtSysCommsOptStTxPwr 1.3.6.1.4.1.926.1.3.2.11.3.2.1.3	This object represents the output optical power measured at the transmitter, expressed in units of 1 microwatt.		Transmitter power
atiMgmtSysCommsOptStTxPwrAlm 1.3.6.1.4.1.926.1.3.2.11.3.2.1.4	This object represents the alarm state of the transmitter optical power. The alarm state is determined on the basis of device-specific criteria, NOT by levels in the limit properties table.		noAlarm(1) alarmHi(2) warningHi(3) warningLo(4) alarmLo(5)
atiMgmtSysCommsOptStTemp 1.3.6.1.4.1.926.1.3.2.11.3.2.1.5	This object represents the temperature of the optical hardware, expressed in units of 0.1°C.		Temperature
atiMgmtSysCommsOptStTempAlm 1.3.6.1.4.1.926.1.3.2.11.3.2.1.6	This object represents the alarm state of the optical hardware temperature. The alarm state is determined on the basis of device-specific criteria, NOT by levels in the limit properties table.		noAlarm(1) alarmHi(2) warningHi(3) warningLo(4) alarmLo(5)
atiMgmtSysCommsOptStSupply 1.3.6.1.4.1.926.1.3.2.11.3.2.1.7	This object represents the supply voltage for the optical hardware, expressed in units of 1 mVDC		Voltage
atiMgmtSysCommsOptStSupplyAlm 1.3.6.1.4.1.926.1.3.2.11.3.2.1.8	This object represents the alarm state of the optical hardware supply voltage. The alarm state is determined on the basis of device-specific criteria, NOT by levels in the limit properties table.		noAlarm(1) alarmHi(2) warningHi(3) warningLo(4) alarmLo(5)
atiMgmtSysCommsOptStTxBias 1.3.6.1.4.1.926.1.3.2.11.3.2.1.9	This object represents the transmitter bias current, expressed in units of 0.01 mA		Current
atiMgmtSysCommsOptStTxBiasAlm 1.3.6.1.4.1.926.1.3.2.11.3.2.1.10	This object represents the alarm state of the transmitter bias current. The alarm state is determined on the basis of device-specific criteria, NOT by levels in the limit properties table.		noAlarm(1) alarmHi(2) warningHi(3) warningLo(4) alarmLo(5)
atiMgmtSysCommsOptStTxFault 1.3.6.1.4.1.926.1.3.2.11.3.2.1.15	This object represents the state of the TX FAULT pin (2) on the SFP module.		noAlarm(1) alarm(2)

Table 3-3, Alarmable SFP Status Information

Fig. 3-2, Web Page SFP Module Status and Information

3.3   Notifications and Traps

In order to avoid the network overhead of constant polling of devices of interest, SNMP supports a system of notifications ("traps" in SNMPv1) to inform a server of events of interest. An EMS system (Continuity™, Alpha® XD™) uses this mechanism to stay up to date. This mechanism requires that the power supply knows which events should trigger notifications, and that the power supply knows what server(s) to notify.

3.3.1   Alarm Settings

The mechanism for specifying events of interest uses the SCTE HMS alarm properties system. (See SCTE-HMS-PROPERTY-MIB and SCTE-HMS-ALARMS-MIB.)

One type of alarm property deals with a numeric value that passes a threshold. These "analog alarms" depend upon setting any combination of four thresholds: major high, minor high, minor low and major low. Each threshold has its own enable for whether it is checked. An alarmable analog object can be in any of five states, depending upon its value: major high, minor high, nominal (no alarm condition), minor low and major low. A transition between states generates a notification. An object with no thresholds enabled is always in the nominal state, regardless of the value. See propertyTable in SCTE-HMS-PROPERTY-MIB.

Another type of alarm property deals with an enumerated object that has a specific value. These "discrete alarms" have a selection for each valid enumeration, to decide whether that value is a major alarm, minor alarm or no alarm. An alarmable discrete object can be in any of those three states. A transition between enumerations generates a notification, except a transition between a "no alarm" value and another "no alarm" value doesn't generate a notification. See discretePropertyTable in SCTE-HMS-PROPERTY-MIB.

While it is possible to configure alarm settings through the web page interface, in most cases this should be left to the EMS to configure through SNMP.

3.3.2   Notification Destinations

There are two ways to set up recipients for notifications and traps on a power supply; either or both may be used.

- The power supply maintains a non-volatile table of recipients for notifications. See atiMgmtSnmpTrapTable in ATI-MGMT-SNMP-MIB. These entries can also be set through the web page interface on the "SNMP" page.

- The power supply also supports the SNMPv2 target mechanism. These settings are not retained through a restart, and need to be set up using a configuration file (as described earlier in this document). See snmpTargetAddrTable in SNMP-COMMUNITY-MIB.

Both of these mechanisms are also supported in DOCSIS® systems. However, some MSOs still use the older docsDevNmAccessTable system for specifying notification targets, and that method is not available over the optical link.

3.4 Firmware Updates

✓ *NOTICE*

EnerSys always recommends the latest released firmware be used in our devices to provide the best function and most up to date security solutions.

The XM3.1-HP™ power supply support firmware updates in the field. There are several types of firmware updates to consider.

The first is core modem firmware, which supports both DOCSIS® and optical communications, the SNMP and web support. DOCSIS defines a standard way to perform modem firmware updates using SNMP or the cable modem configuration file. Over an optical link, the same update is performed using a different, Alpha-specific SNMP operation.

There are component firmware updates for the power supply hardware. Alpha® provides an SNMP operation for this, which is the same as previous generations of Alpha power supplies, which works the same for DOCSIS or for optical.

And lastly, the core modem firmware includes component firmware files "bundled" within it. If the power supply hardware components need to be updated with the firmware released as well as the modem firmware at the same time, a simple SNMP operation can initiate the update.

3.4.1   Core Modem Firmware Update

To initiate a core modem firmware update, the firmware file must be stored on a TFTP server that is reachable from the optical network. Core modem firmware update files are identifiable by a ".img" file extension. Alpha® provides files for DOCSIS® 3.0 setups (filename ending in "-s30.img") and for DOCSIS 3.1 setups (filename ending in "-s31.img"); ONLY the DOCSIS 3.0 files ("-s30.img") can be used over an optical link.

The core modem firmware can be updated via the following methods:

- 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 systemReprogram(6) to initiate the transfer. (See **Table 3-4, Alpha Firmware Update Settings**.)
- If using the web page, log in with administrative rights, go to the Firmware Update page (only visible if logged in), fill in the "TFTP Firmware Update" section, including choosing "System reprogram" for Download Control, and click "Save Changes." (See **Fig. 3-3, Web Page TFTP Firmware Update**.)

If the transfer begins successfully, the download status (atiMgmtSysDownloadStatus in SNMP, also shown on the web page) will indicate downloading(10) during the lengthy update process. The system will restart, causing a network communications interruption for several minutes, and then show a status of idle(1). If the transfer 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 3-4, Alpha Firmware Update Settings

Fig. 3-3, Web Page TFTP Firmware Update

3.4.2   Component Firmware Update Using TFTP

There are two ways to perform a component firmware update. Component firmware files are identifiable with a "afwu" file extension (for "Alpha FirmWare Update"). The most common way is to install the file on a TFTP server, which is the same method for updating the core modem firmware.

- 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 3-4, Alpha Firmware Update Settings**.)

- If using the web page, log in with administrative rights, go to the Firmware Update, fill in the "TFTP Firmware Update" section, including choosing "Reprogram" for Download Control, and click "Save Changes." (See **Fig. 3-3, Web Page TFTP Firmware Update**.)

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.

3.4.3   Component Firmware Update Using HTTP

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

> **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).

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.

Fig. 3-4, Web Page Direct Firmware Update

3.4.4   Bundled Firmware

The core modem firmware files have the associated component firmware files bundled in, to provide a shortcut for bringing the components to the versions that were released at the same time as the core modem firmware. By default, these components are NOT automatically updated when the core modem firmware is updated. The power supply can be set to automatically apply the component firmware updates any time a core modem firmware update completes by setting atiMgmtCfgFwBundleUpdates to autoUpdate(2).

The firmware components bundled with the core modem firmware, and the version number for each, are reported in SNMP in atiMgmtCfgFwBundleContent. The version numbers in that report are the versions that could be installed, not necessarily the current versions for those components. The bundled firmware and current running version can be viewed on the Firmware Update web page by logging in to the web page with administrative rights.

The power supply can be instructed to apply the bundled updates. In SNMP, set atiMgmtCfgFwBundleControl to updateNow(1). From the Firmware Updates web page, click the "Apply Bundled Firmware" button. The power supply will apply any firmware updates where the versions are different. For any firmware where the reported version is the same as the bundled version, no update is performed.

BUNDLED FIRMWARE SETTINGS			
COMPONENT	DESCRIPTION	DEFAULT	VALUES
atiMgmtCfgFwUpdateStatus 1.3.6.1.4.1.926.1.3.3.4.1	This object indicates the status of the peripheral firmware update process.	idle(1)	idle(1) updating(2)
atiMgmtCfgFwBundleContent 1.3.6.1.4.1.926.1.3.3.4.2.1	This object displays information about the peripheral firmware that is bundled within the master firmware image.		Text
atiMgmtCfgFwBundleUpdates 1.3.6.1.4.1.926.1.3.3.4.2.2	This object indicates whether updating the master firmware image should also update all bundled peripheral firmware. Any future update of the master firmware image, while this object is set to autoUpdate(2), also triggers peripheral firmware updates as needed.	noAutoUpdate(1)	noAutoUpdate(1) autoUpdate(2)
atiMgmtCfgFwBundleControl 1.3.6.1.4.1.926.1.3.3.4.2.3	This object allows control of the bundled firmware.	noAction(0)	noAction(0) updateNow(1)

Table 3-5, Bundled Firmware Settings

Fig. 3-5, Web Page Bundled Firmware

4.0   SNMP Configuration for Vendor-specific DHCP Options

This section describes a method of conveying SNMP configuration information to an Alpha® optical transponder using vendor-specific DHCP options.

The initial release of the Alpha® XM3.1-HP™ power supplies supported a mechanism for provisioning the optical network interface that was, in some ways, similar to how a DOCSIS® cable modem is provisioned. The transponder would first obtain an IP address (ordinarily from a DHCP server). Standard options within the DHCP offer could direct the transponder to a TFTP server and filename with which to obtain a configuration file that could perform additional setup.

This new method is an alternative to the configuration file: a way for the DHCP offer itself to include some provisioning information for the transponder.

Note that the minimum core version of firmware that supports this function is version 01.05.00.b003.

4.1   Basic Concepts

A DHCP offer contains a variety of information fields beyond just an IP address. The standards for DHCP define various options that can be part of the DHCP offer, which the DHCP server can provide for all or selected requesting devices.

The information described in this specification is specific to Alpha optical transponders, making use of specific DHCP options reserved for vendor-specific use. For DHCP on IPv4, this information is provided using DHCP option 125 ("option vivso" in ISC DHCP server configuration). For DHCPv6 on IPv6, this information is provided using DHCPv6 option 17 ("option dhcp6.vendor-opts" in ISC DHCP server configuration). In either DHCP type, the DHCP offer includes a set of sub-options within the vendor-specific option to convey the pieces of information. Similarly, the DHCP request includes a set of sub-options within the vendor-specific option to convey identification information that the DHCP server may choose to use in deciding what offer to extend.

Each sub-option defined within this section of this document performs one of the following purposes:

- **Identification settings:** These allow the DHCP server to know basic information about the transponder before any other network connection has been established.
- **General SNMP settings:** These allow an arbitrary SNMP object to be set to a specified value.
- **SNMP access settings:** These allow an external SNMP client—typically a management system server—to perform SNMP operations with the transponder.
- **SNMP notification settings:** These configure the transponder to issue notifications or "traps" to a specific destination (typically a management system server).

This method of conveying provisioning information through the DHCP offer does not preclude use of the configuration file previously supported: the Alpha® optical transponder will still attempt to load the configuration file if information to do so is available in the DHCP offer. The DHCP information is processed before the configuration file information.

DHCP messages are relatively small, often only a few hundred bytes in size. Additionally, in IPv4, DHCP options have a 255 byte length limit. For these reasons, the DHCP options described in this specification should only be used for relatively simple configurations. A complex configuration should still prefer the TFTP configuration file technique already available.

If a transponder obtains both an IPv4 address using DHCP and an IPv6 address using DHCPv6, either of these DHCP offers could contain configuration data as described in this specification. For example, the DHCP offer could configure IPv4 access and/or notifications, and the DHCPv6 offer could configure IPv6 access and/or notifications. These sets of information are both processed; however, there is no guarantee as to which information will be received and processed first.

4.2   Alpha® DHCP Options

The SNMP provisioning information for Alpha® optical transponders is packaged in a DHCP message using an Alpha-specific identification:

For IPv4, the DHCP message needs to include the "vendor-identifying vendor-specific information option," option 125. This option needs to include the Alpha® enterprise number, which is 926, to distinguish the option from other vendor-specific options that might be used. The specific sub-options for the provisioning information are described in the next section.

For IPv6, the DHCPv6 message needs to include the "vendor-specific information option," option 17. This option needs to include the Alpha® enterprise number, which is 926, to distinguish the option from other vendor-specific options that

might be used. The specific sub-options for the provisioning information are described in the next section.

4.3   Sub-option Data

The SNMP provisioning information is packaged in a series of sub-options which, taken together, define the various settings. Each sub-option has a particular numeric identifier and format of associated data. The same sub-options have the same meaning in both DHCP (IPv4) and DHCPv6 (IPv6) messages.

4.3.1   Identification Data

When the optical transponder is soliciting DHCP offers, its messages include a set of sub-options to identify the product. This group of sub-options follows the precedent of some DOCSIS® devices.

Sub-option 4: Device Serial Number

This sub-option presents the serial number of the network device as a text string. This is equivalent to commonSerialNumber.

Sub-option 5: Hardware Version Number

This sub-option presents the version of the hardware as a text string. This is equivalent to the "HW_REV" field within sysDescr.

Sub-option 6: Software Version Number

This sub-option presents the version of the firmware as a text string. This is equivalent to the "SW_REV" field within sysDescr.

Sub-option 7: Bootloader Version Number

This sub-option presents the version of the bootloader as a text string. This is equivalent to the "BOOTR" field within sysDescr.

Sub-option 8: Vendor OUI

This sub-option presents the Organizationally Unique Identifier (OUI) as a text string of six hexadecimal characters. This is equivalent to the first three bytes of the transponder MAC address.

Sub-option 9: Model Number

This sub-option presents the model number of the network device as a text string. This is equivalent to the "MODEL" field within sysDescr.

Sub-option 10: Vendor Name

This sub-option presents the vendor name as a text string. This is equivalent to the "VENDOR" field within sysDescr.

4.3.2 General SNMP Settings

Any valid SNMP "set" operation can be encoded in the DHCP offer as a text string. (This functionality is comparable to TLV 11 in a DOCSIS® cable modem configuration file.)

Sub-option 20: SNMP Set

This sub-option contains one or more SNMP object settings. Each setting is expressed as a combination of the OID (SNMP object address), a type, and the value to be set, each separated by commas. For example:

> 1.3.6.1.4.1.5591.1.3.1.1.0,s,PS 123

This example sets the "commonLogicalID" object to the string "PS 123".

If more than one setting is to be performed, each additional setting is concatenated onto the string with a semicolon (";") as the separator between settings. For example:

> 1.3.6.1.4.1.5591.1.3.1.1.0,s,PS 123;1.3.6.1.4.1.5591.1.3.1.8.0,i,2

This example sets the "commonLogicalID" object to "PS 123" and sets the "commonAlarmDetectionControl" object to the integer value 2 (for "detectionEnabled").

For each setting:

- The OID is a numeric dotted SNMP identifier. (Textual names like "commonLogicalID" are not recognized.)
- The type is one of the following characters:
  - i = signed integer (the value is a number, may begin with a minus sign for negative)
  - u = unsigned integer (the value is a number)
  - s = string (the value is a text string)
  - x = hex string (the value is a series of hexadecimal digit pairs, each pair representing one byte of string data; the digit pairs MAY be separated by spaces)
  - d = decimal string (the value is a series of numbers, each number representing one byte of string data; the numbers MUST be separated by spaces)
  - n = null object (the value is ignored)
  - o = object ID (the value is itself a numeric dotted SNMP identifier)
  - t = timeticks (the value is a number of ticks)
  - a = IPv4 address (the value is a dotted IP address)
  - b = bits (the value is a series of bit numbers; the numbers MUST be separated by spaces)
- The value is what you want to set; the type determines what that value should contain.

Each setting must contain all three parameters (OID, type, value).

4.3.3   SNMP Access Settings

Permission is granted for an outside computer to access SNMP on the transponder using a text string. (This functionality is comparable to TLV 53 in a DOCSIS cable modem configuration file.)

Sub-option 21: SNMP Access

This sub-option contains one or more access entries. Each entry is expressed as a combination of the network address(es) with prefix length, the community string, the access type, and the optional view name, each separated by commas. For example:

> 123.123.123.0/24,Cmty,W,

This example allows access for any IP address in the 123.123.123.x subnet, using community string "Cmty," with read/write access, using the default view name.

An entry may group more than one network address range into the same entry. You can add more address and prefix length values into the first parameter, separated by the plus sign ("+"). For example:

> 123.123.123.0/24+123.123.125.0/24,Cmty,W,

This example says that both 123.123.123.x and 123.123.125.x are allowed access with the "Cmty" community string.

If more than one access entry is requested, each additional entry is concatenated onto the string with a semicolon (";") as the separator between entries. For example:

> 123.123.123.0/24,Cmty,W,;fd00:1234:1234:1234::/64,V6Cmty,W,

This example allows access for any IP address in the 123.123.123.x subnet, using community string "Cmty," with read/write access, using the default view name, and allows access for any IP address in the fd00:1234:1234:1234:: subnet, using community string "V6Cmty," with read/write access, using the default view name.

For each entry:

- The network address is any valid IPv4 or IPv6 address followed by a slash and the prefix length. (The prefix length is a more compact representation than subnet masks, especially for IPv6. In IPv4, a prefix length of 24 is equivalent to a subnet mask of 255.255.255.0.) Multiple address and prefix length pairs can be specified in the same entry, separated by the plus sign.

- The community string is a text string for the expected community string in the access request. If this parameter is not provided (left blank), "public" is used as the default community string.

- The access type is a single character, "R" for read-only access or "W" for read/write access. If this parameter is not provided (left blank), read-only access is used as the default.

- The view name optionally specifies a particular SNMP view to use for the access. If provided, the view must either be a predefined view or separately established by a configuration setting; check with EnerSys® if you need to make this distinction. If this parameter is not provided (left blank), the default is full access to all SNMP objects. Using the default blank view name is recommended.

Only the first parameter (network address) is required; the other values can be skipped if the defaults are acceptable. Trailing commas may also be omitted, so the following examples mean the same thing:

> fd00:1234:1234:1234::/64,,,
>
> fd00:1234:1234:1234::/64

Both examples grant access to the fd00:1234:1234:1234:: subnet, using "public" as the community string, read-only access to all SNMP objects.

4.3.4   SNMP Notification Settings

Notifications or traps are sent to each target specified using a text string. (This functionality is comparable to TLV 38 in a DOCSIS® cable modem configuration file.)

Sub-option 22: SNMP Notification Target

This sub-option contains one or more notification destination entries. Each entry is expressed as a combination of the network address(es), the port number, the notification type, the timeout value, the retries count, the filter OID, and the security name, each separated by commas. For example:

> fd00:1234:1234:1234::123,8162,3,15000,5,1.3.6.1.4.1.5591.1,Secure

This example sends notifications to IP address fd00:1234:1234:1234::123 using UDP port 8162. These notifications are SNMP informs in SNMPv2 packets, with up to five retries with 15 second timeouts. Only notifications within the "scteHmsTree" area of SNMP should be sent to this recipient, and the SNMPv3 view name "Secure" is used.

An entry may group more than one network address into the same entry. You can add more addresses into the first parameter, separated by the plus sign ("+"). For example:

> fd00:1234:1234:1234::123+fd00:1234:1234:1234::abc,8162,3,15000,5,1.3.6.1.4.1.5591.1,Secure

This example is the same as before, except that both fd00:1234:1234:1234::123 and fd00:1234:1234:1234::abc are to receive the notifications.

If more than one notification destination entry is requested, each additional entry is concatenated onto the string with a semicolon (";") as the separator between entries. For example:

> fd00:1234:1234:1234::123,8162,3,15000,5,1.3.6.1.4.1.5591.1,Secure;123.123.123.123,9162,3,7500,3,
> 1.3.6.1.4.1.5591.1,Secure

This example sends notifications to IP address fd00:1234:1234:1234::123 using UDP port 8162. These notifications are SNMP informs in SNMPv2 packets, with up to five retries with 15 second timeouts. Only notifications within the "scteHmsTree" area of SNMP should be sent to this recipient, and the SNMPv3 view name "Secure" is used. This example also sends notifications to IP address 123.123.123.123 using UDP port 9162. These notifications are SNMP informs in SNMPv2 packets, with up to three retries with 7½ second timeouts. Only notifications within the "scteHmsTree" area of SNMP should be sent to this recipient, and the SNMPv3 view name "Secure" is used.

For each entry:

- The network address is any valid IPv4 or IPv6 address. Multiple addresses can be specified in the same entry, separated by the plus sign.
- The port number is the UDP destination port used for the notification. If this parameter is not provided (left blank), port 162 is used as the default.
- The notification type is one of five choices. If this parameter is not provided (left blank), 1 (SNMPv1 trap in an SNMPv1 packet) is used as the default for any IPv4 address, and 2 (SNMPv2c notification in an SNMPv2c packet) is used as the default for any IPv6 address. The choices are:
  - 1 = an SNMPv1 trap in an SNMPv1 packet
  - 2 = an SNMPv2c notification in an SNMPv2c packet
  - 3 = an SNMP inform in an SNMPv2c packet
  - 4 = an SNMPv2c notification in an SNMPv3 packet
  - 5 = an SNMP inform in an SNMPv3 packet
- The timeout value is the time, in milliseconds, before an inform times out for lack of response. This parameter is only meaningful for informs (notification type 3 or 5). If this parameter is not provided (left blank), 10000 (ten seconds) is used as the default.

- The retries count is how many times an inform times out before giving up sending them. This parameter is only meaningful for informs (notification type 3 or 5). If this parameter is not provided (left blank), 3 retries is used as the default.

- The filter OID is a numeric dotted SNMP identifier for the starting point in the SNMP tree for which notifications are included for this entry. That is, a notification whose identifier is this OID or any child of this OID is sent, and a notification whose identifier is not a descendant of this OID is not sent. If this parameter is not provided (left blank), any notification is sent to this target.

- The security name is a string used for the SNMPv3 packet security when the notification is sent. This parameter is only meaningful for SNMPv3 packets (notification type 4 or 5). If this parameter is not provided (left blank), "@config" is used as the default.

Only the first parameter (network address) is required; the other values can be skipped if the defaults are acceptable. Trailing commas may also be omitted, so the following examples mean the same thing:

> fd00:1234:1234:1234::123,,,,,,

> fd00:1234:1234:1234::123

Both examples send notifications to fd00:1234:1234:1234::123 on port 162, using SNMPv2c notifications in SNMPv2c packets, with no timeout or retry count, no filtering of the notifications and no security name.

4.3.5   Special Characters

Spaces

In sub-options 20, 21 and 22, spaces may be added for readability, before or after any parameter. These leading and trailing spaces are discarded, and do not affect the meaning of the content. (They do, however, add bytes to the DHCP packet, if that is a concern.) The following three examples have the same result:

> 1.3.6.1.4.1.5591.1.3.1.1.0,s,PS 123;1.3.6.1.4.1.5591.1.3.1.8.0,i,2

> 1.3.6.1.4.1.5591.1.3.1.1.0,s,PS 123;   1.3.6.1.4.1.5591.1.3.1.8.0,i,2

> 1.3.6.1.4.1.5591.1.3.1.1.0, s, PS 123;   1.3.6.1.4.1.5591.1.3.1.8.0, i, 2

In the third example, the space in "PS 123" is retained in the setting, even though the space before it was discarded.

Escapes

A parameter cannot contain a comma (these separate parameters) and it cannot contain a semicolon (these separate entries). This, for example, would be an invalid sub-option 20 entry:

> 1.3.6.1.4.1.5591.1.3.1.1.0,s,PS,15A

"PS,15A" was the intended setting, but a comma means a new parameter, so this entry would not be accepted by the DHCP options parser.

Any time a special character is needed within a parameter (a comma or semicolon, to avoid confusion with the DHCP option parsing, or any other character that could be a problem for the DHCP server setup in which these sub-option strings appear), it can be "escaped" using the same convention used in URLs: a percent sign followed by two hexadecimal digits representing the desired character code. If "PS,15A" was the intended setting, it can be expressed as "PS%2C15A" instead.

The essential escapes are:

- %2C = comma

- %3B = semicolon

- %25 = percent sign. (The percent sign has special meaning to identify an escape, so if a percent sign is needed in a parameter, it must be escaped.)

- %20 = space. (If you need a string to begin or end with a space, which would otherwise be discarded, that space must be escaped.)

4.4   References

RFC 2132: "DHCP Options and BOOTP Vendor Extensions".

RFC 3925: "Vendor-Identifying Vendor Options for Dynamic Host Configuration Protocol version 4 (DHCPv4)".

RFC 8415: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

5.0   XM3.1-HP™ Power Supply Details

Unless specifically configured otherwise, the XM3.1-HP™ power supply simultaneously attempts to come online with the DOCSIS® plant, and attempts to come online with the optical plant. Once the power supply comes online with either DOCSIS or optical, it stops attempting to use the other interface. To keep the power supply from trying both interfaces, disable either DOCSIS or optical (but not both) using atiMgmtSysCommsEnable in ATI-MGMT-SYS-COMMS-MIB (index .1 for DOCSIS, and index .11 for optical), or on the System Data web page.

For a technician on site with the XM3.1-HP power supply, there are a number of indicators available for the health and status of the optical link.

5.1   LEDs

5.1.1   Online LED

The online LED ("OL" on the front panel silk screen) has a dual meaning on XM3.1-HP power supply. This can be the DOCSIS online indicator, or it can be the SFP online indicator.

When an SFP is plugged in, the online LED can indicate either of the following:

- Blinking - the SFP is detected, but not yet fully online for management
- On - the SFP is fully online for management (the provisioning steps outlined earlier in this document have completed)

If the online LED is off, the power supply doesn't detect the SFP (or the optical link was manually disabled).

When using the DOCSIS RF link, the online LED shows the DOCSIS online status instead.

5.1.2   Receive/Transmit Power LED

The receive/transmit power LED ("RX/TX PWR" on the front panel silk screen, three colors in the same spot) similarly has a dual meaning on XM3.1-HP power supply. When DOCSIS isn't being used, these show one of the following:

RX/TX POWER LED STATUS	
LED INDICATOR BEHAVIOR	STATUS
Off	The SFP is not installed
Mostly off, with a quick red flash	The SFP is installed, but there is no incoming link. (Usually this means the optical fiber is removed or bad, or the other end is powered off.)
Mostly green, with a quick flash off	The SFP has an incoming link, which reports as good (or the SFP doesn't have fault detection to tell us otherwise)
Mostly blue, with a quick flash off	The incoming link is in a warning optical receive level
Mostly red, with a quick flash off	The incoming link is in a critical optical receive level

Table 4-1, RX/TX Power LED Status

✓ **NOTICE:**

> Note that the quick flashes on the Rx/Tx LED always indicate an SFP power reading; a DOCSIS RF power reading indication does not have flashes.

The SFP must have fault detection capabilities (a specific subset of DDM functionality) in order for receiver warnings or critical levels to be indicated on the LED. If it is not known whether the installed SFP has this feature, check the SFP web page. If the "SFP Module Status" table includes a column labeled "Condition," then fault detection is supported for that SFP, and can be indicated in the color of the LED.

Although the LED is labeled for receive and transmit power, only the receive power status is indicated for an optical link. (The transmit power of an SFP is not an indication of the link health like it is in DOCSIS; it only indicates the functioning of the SFP module.)

5.2 LCD

When an SFP is installed in the power supply, the LCD display adds two new sub-menus to the COMM menu:

- **SFP – GENERAL:** contains the most-used information about the optical link: the MAC address and any IP addresses for the optical interface, and the receive and transmit power of the SFP (if the SFP is able to report these).
- **SFP – DIAGNOSTICS:** contains more details about the optical link (status, uptime and configuration file) and the SFP. (The actual details about the SFP depend upon what information the SFP is able to present.)

For optical link details beyond what the LCD menu presents, use the "SFP" web page on a computer connected to the local Ethernet port.

6.0   Comparison Between DOCSIS® and Optical Links

The following table compares the DOCSIS and optical link behaviors as a quick reference for someone already familiar with status monitoring in a DOCSIS plant.

DOCSIS AND OPTICAL LINK COMPARISONS		
	DOCSIS	OPTICAL LINK
PHYSICAL INTERFACE	RF (QAM/OFDM, ATDMA/OFDMA)	Gigabit SFP (single-mode/multi-mode, unidirectional/bidirectional, EPON ONU, etc.)
SUPPORTS IPV4	Yes	Yes
SUPPORTS IPV6	Since DOCSIS 2.0+IPv6	Yes
IP ADDRESS ASSIGNMENT	DHCP; DHCPv6	DHCP; SLAAC; DHCPv6; fixed address
NETWORK TIME	Required, RFC 868	Optional, (S)NTP or RFC 868
CONFIGURATION FILE	Required, DOCSIS TLV file	Optional, text file
SECURE CHANNEL	BPI+	No (expects secure optical plant)
ACCESS RIGHTS	SNMP VACM; docsDevNmAccessTable	SNMP VACM; Alpha access MIBs
NOTIFICATION RECIPIENTS	SNMP targets; Alpha trap dests; docsDevNmAcccessTable	SNMP targets; Alpha trap dests
ALARM SETUP	SCTE properties	SCTE properties

Table 5-1, DOCSIS® and Optical Link Comparisons

7.0   Additional References

For further information, refer to the technical manual for your particular power supply. For SNMP access, the following MIB files may be needed:

| MIB FILE	FUNCTION
ATI-DEV-BATTERIES-MIB	Alpha battery system device information. This overlaps functionality in SCTE-HMS-PS-MIB.
ATI-DEV-POWER-SUPPLEIS-MIB	Alpha power supply device information. This overlaps functionality in SCTE-HMS-PS-MIB.
ATI-MGMT-SNMP-MIB	Alpha SNMP configuration.
ATI-MGMT-SYS-COMMS-MIB	Alpha communications interface information. This includes entries for the optical interface.
ATI-MGMT-SYS-COMMS-OPTICAL-MIB	Alpha supplemental information specific to optical/SFP communications interfaces.
SCTE-HMS-ALARMS-MIB	SCTE general alarm reporting.
SCTE-HMS-PROPERTY-MIB	SCTE general alarm properties setup.
SCTE-HMS-PS-MIB	SCTE standard power supply functionality.
SNMP-COMMUNITY-MIB	SNMPv2 setup including notification targets.

Table 6-1, MIB Files

8.0   Addendum

## 8.1   SFP Communication Options

The SFP connector enables even more communications options:

- PON network
  - Fiber using 1G PON
  - SFP hosted fiber ONU 10G PON
  - Copper SFP to operator ONU 10G PON
- Point to point fiber connection using SFP
  - Single or dual dark fiber SFP
  - Single or dual OOB ITU fiber channels to SFP
  - Copper SFP Ethernet direct connection
- Other forms of connection
  - Cellular modem to copper SFP
  - Wi-Fi bridge to copper SFP
  - Satellite communication to copper SFP
  - DSL connection to copper SFP
  - Other wireless or wireline link
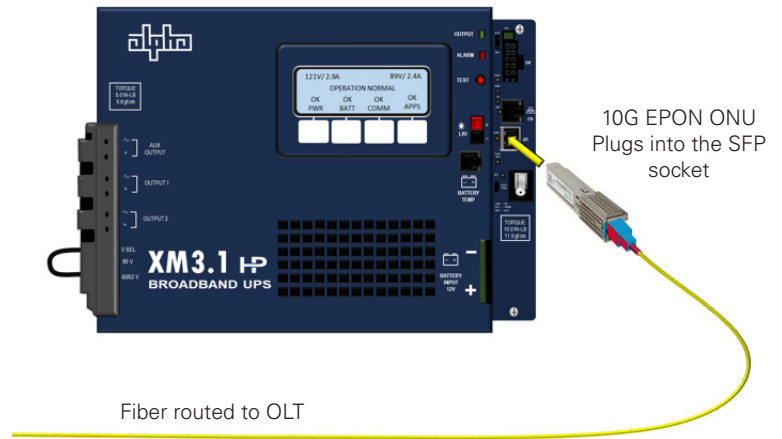
Fig. 8-1, XM3.1-HP™ (3 & 5 Amp) Power Supply w/ 10G EPON ONU
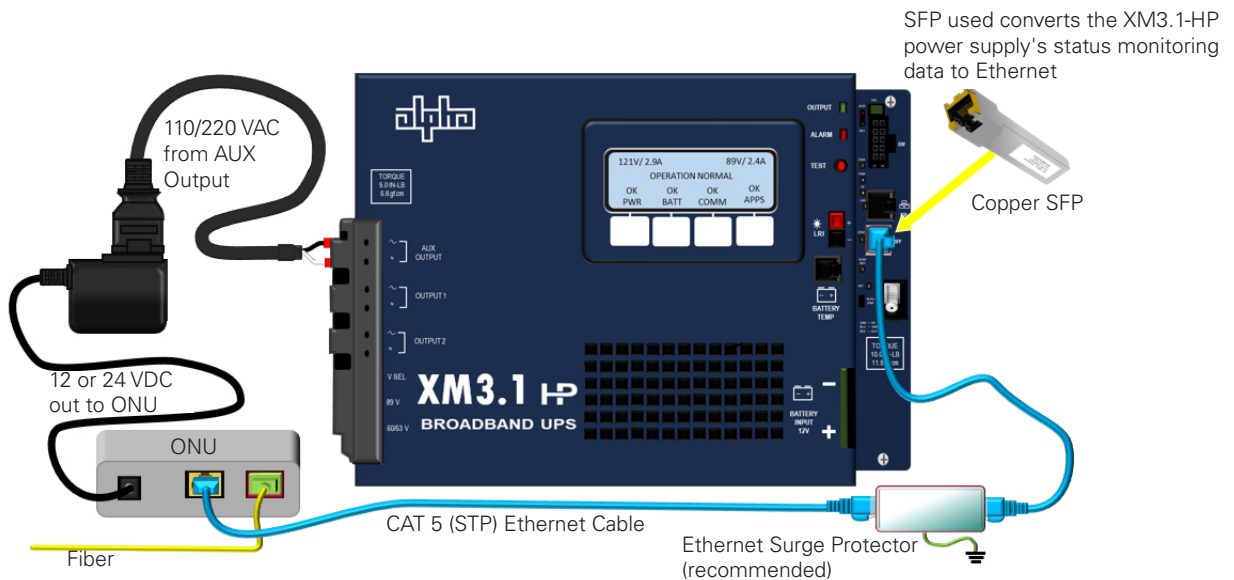
Fig. 8-2, XM3.1-HP™ (3 & 5 Amp) Power Supply w/ Copper SFP, External ONU or ONT

8.0   Addendum, continued

Each of these connections has nuances for operation, routing, information, features, and configuration.

The Routing configuration has to take the following into account:

- DHCP server access

- TFTP server access

- TOD/NTP server access

- SNMP monitoring server connection

    ◦ SNMP

    ◦ SNMP traps

- Potential client web page address

Operation – There may be core device operation expected using one form of communication method that may interfere when another form of connection is used. An example would be the DOCSIS® communications watchdog timers that would not be satisfied if the XM3.1-HP™ power supply is communicating through the SFP connection.

- DOCSIS watchdog timers

- Telemetry SNMP watchdog timers

- SFP interconnect

Features – Features from one connection may not be available when using another form of communications. An example would be the ability to use the ethernet craft port to backhaul another devices data when using the RF connector that is not available when using the SFP for connection.

- Ethernet port gateway backhaul

- E-Router

- Electronic diplexers

- Electronic attenuation

- RF displays

    ◦ Constellation

    ◦ Micro-reflections

    ◦ Spectrum analyzer

- SFP information

Page intentionally left blank.