Power over Ethernet

Outdoor Power View Pro

User Guide

Version 1.0
Catalog Number PDS_NMS_UG

Acknowledgements

All other products or trademarks are property of their respective owners.

The product described by this manual is a licensed product of Microsemi.

Abbreviations and Terminology

Abbreviations are spelled out in full when first used or are listed in Table 1-1. Only industry-standard terms are used throughout this manual.

Note: Covered under U.S patent S/N 6,473,608. Other patents are pending.

Table of Contents

List of Figures

List of Tables

1 About This Guide

The following sections define the manual objectives, concepts used, conventions used and associated documentation.

1.1 Objectives

This user guide introduces PowerDsine's **IPv4/IPv6** capable Outdoor Power View Pro Web, SNMP and Telnet management features used for managing PowerDsine's Power over Ethernet (PoE) product line of IPv4/IPv6 capable PoE devices, including:

- Device list:
  - PDS-102GO/AC/M – The PDS-102GO/AC/M is an outdoor PoE switch that enables connecting two powered devices to the network. The switch will deliver PoE power up to 30W per device. In addition, it enables remote monitoring and controlling of the status of the devices. The major benefit of the PDS-102GO/AC/M outdoor unit is that it extends the maximum reach of the network switch by an additional 100 meters (to a total of 200 meters between the switch and the powered devices), while providing up to 2 x 30 watts to its network-powered PoE devices.

1.2 Audience

This guide is intended for network administrators, supervisors and installation technicians who have a background in:

- Basic concepts and terminology of networking
- Network topology
- Protocols
- Microsoft Windows environment

1.3 Organization

This guide is divided into the following sections:

- **Section 1**: Defines the concepts used, conventions used and associated documentation
- **Section 2**: Outdoor Power View Pro features and capabilities
- **Section 3**: Complete system installation procedure
- **Section 4**: Outdoor PowerView Pro Web interface detailed description
- **Section 5**: SNMP monitoring and configuration
- **Section 6**: Syslog message report
- **Section 7**: Upload/download unit configuration over TFTP
- **Section 8**: Software upgrade
- **Section 9**: Recovering from unknown username, password
- **Section 10**: Troubleshooting

1.4 Conventions

The various conventions used in defining commands and examples are given in the following table.

CONVENTION	DEFINITION
bold	Keywords and commands
italics	*Represents a Web interface item*
screen	Displayed Information
Courier text	Information to be entered
Notes	Helpful information

1.5 Related Documentation

For additional information, refer to the following documentation:

- Product user installation guide (included on the CD)
- Technical Note 132: Using RFC3621 PoE MIB with PowerDsine Midspan (included on the CD).
- RFC3621 SNMP MIB, and private MIB (included on the CD)
- IEEE Standard 802.3af, DTE Power via MDI

NOTE:

Power View Pro refers to the various management interfaces provided by the unit for remote management, including Web, SNMP, and Telnet.

1.6 Abbreviations

Table 1-1: List of Abbreviations

IPv4	32-bit long IP address
IPv6	128-bit long IP address
DHCPv4	Dynamic IPv4 Host Configuration Protocol
DHCPv6	Dynamic IPv6 Host Configuration Protocol
PoE	Power over Ethernet
NTP	Network Time Protocol
DES	Data Encryption Standard
MD5	Message Digest algorithm
SHA	Message Digest algorithm
MDI	Media Dependent Interface
MIB	Management Information Base
PD	Powered Device
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
SysLog	System Log

2 Introducing the Power View Pro (IPv4, IPv6)

PowerDsine's Power View Pro refers to the various management interfaces provided by the unit for remote management, including Web, SNMP, and Telnet. Management can be done over IPv4, IPv6 or both network protocols. The system provides direct online power supervision, configuration, monitoring, and diagnostics of PowerDsine products via Web / SNMPv2c / SNMPv3 / Telnet/ SSH.

2.1 Features

The manager provides a number of unique features along with multiple access options:

- **Supported network IP protocols:**
  - IPv4 – IP address is made out of 32 bits (static / DHCPv4).
  - IPv6 – IP address is made out of 128 bits (static / DHCPv6).
- **Access Options:**
  - **HTTP**: Web-based friendly configuration interface for managing remote Outdoor Power over Ethernet devices.
  - **SNMP**:
    - SNMPv2c for non-secured SNMP management
    - SNMPv3 for secured plus encrypted management
    - RFC1213 MIB-II Network statistics
    - RFC3621 Power over Ethernet (PoE) SNMP MIBs
    - Private MIB extension for RFC3621 PoE MIB
  - **Telnet**: Remote terminal over IP Network
- **SysLog Server**: Sends log events to remote SysLog Servers.
- Easy software update during run time without affecting active PoE ports.
- Configuration and real-time monitoring using graphical representations of the remote device
- System status display.
- Automatic activation / deactivation of PoE ports based on a weekly schedule configuration.

2.2 System Network Management Capabilities

The unit can be accessed from any computer using any Web browser, SNMPv2c/SNMPv3 management station or Telnet.

- **Web Interface** – used to view unit PoE and network status, unit configuration and view unit production information.
- **SNMP v2/v3** – Monitor unit over the network (MIB-II RFC1213), monitor / configure unit PoE capabilities (RFC3621).
- **Telnet** – used to view unit PoE & network status, unit configuration and production information**.** Software update, enable/disable PoE functionality, ping remote network devices for connectivity tests.
- **SNMP Traps** – used to report various PoE events such as PoE PD insertion / removal.
- **SysLog** – used to report PoE events, invalid remote user access, initial DHCPv4/v6 address, etc.

2.3 Ethernet Switch Network Capabilities

- 10M/100M/1000Mbit Half-Duplex / Full-Duplex Ethernet speed
- 8K internal MAC address lookup engine
- Auto MDIX
- Jumbo frames

2.4 POE Capabilities

The following Power over Ethernet (PoE) options are available:

- **IEEE 802.3at** – Delivers up to 30 watts per port.
- **PoE Enable/Disable** – Enable/disable PoE ports power output (Ethernet data is always enabled).
- **Weekly Schedule** – Automatic activation/deactivation of PoE ports based on time of day.
- **Remote device reset** – Turning temporary device power off and back on resets attached PD device.

2.5 Configuration Options

- **Web-based**: Via a Web browser
- **SNMPv1/2c/3**: Via an SNMP management application on a remote computer
- **Telnet**: Via a Telnet application on a remote computer

NOTE:

The unit default IPv4 address is 192.168.0.50. Make sure that a computer network card is configured to the same IPv4 network (for example 192.168.0.40).

NOTE:

For security reasons, when the unit is shipped the SNMP is disabled. Prior to enabling SNMP, modify SNMP community strings and only then enable it.

2.6 Security and User Authentication

Web/Telnet, SNMPv2 and SNMPv3 offer different security strength

2.6.1 Web/Telnet Security

Web interface and Telnet share the same username and password.

2.6.2 SNMP Security

- **SNMP v1/v2**: Community string is utilized for Get/Set/Trap authentication. SNMPv1/v2 is considered as unsecured protocol since the community string password can be easily intercepted by any network sniffer device.
- **SNMP v3**: Resolves SNMPv1/v2 security issues by adding authentication and encryption to SNMP packets.

2.7 Default unit IP, username and password

- The unit is shipped with the following factory default usernames and passwords:

NOTE:

Default IP address:

IP = *192.168.0.50*
Mask = *255.255.255.0*

Web/Telnet:

Username = ***"****admin****"***
password = ***"****password****"***

SNMP v2:

GET community string ="*public***"**
SET community string = "*private***"**

SNMP v3:

user name ="*admin***"**
authentication password (MD5) = "*password***"**
privacy password (DES)= "*password***"**

Username, password recovery:

For username and password recovery, whenever unit username or password were changed and are unavailable to the user, please refer to Section 9***, Recovering from Unknown Username, Password***.

3 Web Interface

Unit default IPv4 address is **192.168.0.50**. For first-time configuration, please configure your computer/laptop Ethernet network interface to the following IPv4 parameters:

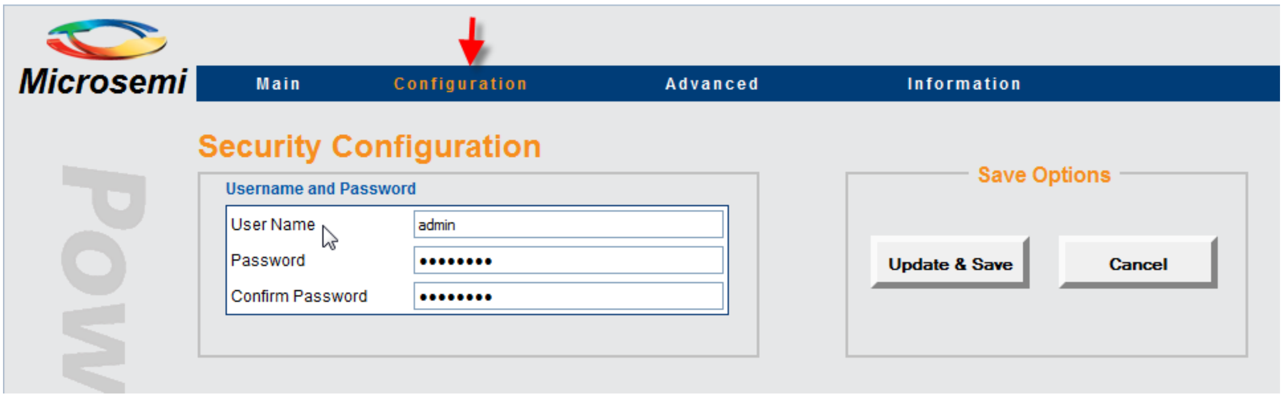
- **IPv4:** 192.168.0.40
- **IPv4 Mask:** **255.255.255.0**

3.1 First-Time Configuration

Connect your PC/laptop Ethernet network interface (should be configured to IP 192.168.0.40) to anyone of the unit Ethernet ports. Open your Web browser and type 192.168.0.50 in the top address field.

Default web username is ***admin***, and default password is ***password*.**

Selecting the Configuration option on the menu will reveal the unit configuration Web page. Please change the unit remote access username and password to other then ***admin/password***, unit IPv4/IPv6 address, and if required enable SNMP only after changing the default GET/SET community strings to other than ***public/private***.



Security Configuration

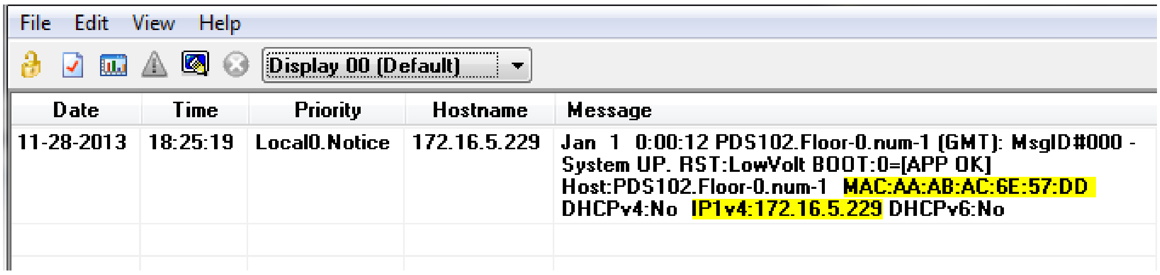
Username and Password

User Name: admin
Password: ••••••••
Confirm Password: ••••••••

Save Options

Figure 3-1: Configuration Web Page Option

To ease unit location over the network, the unit sends IPv4 SysLog broadcast message advertising its IP address upon power up and the first time an IPv4/IPv6 is obtained from the DHCPV4/DHCPv6 Server (see Figure 3-2).

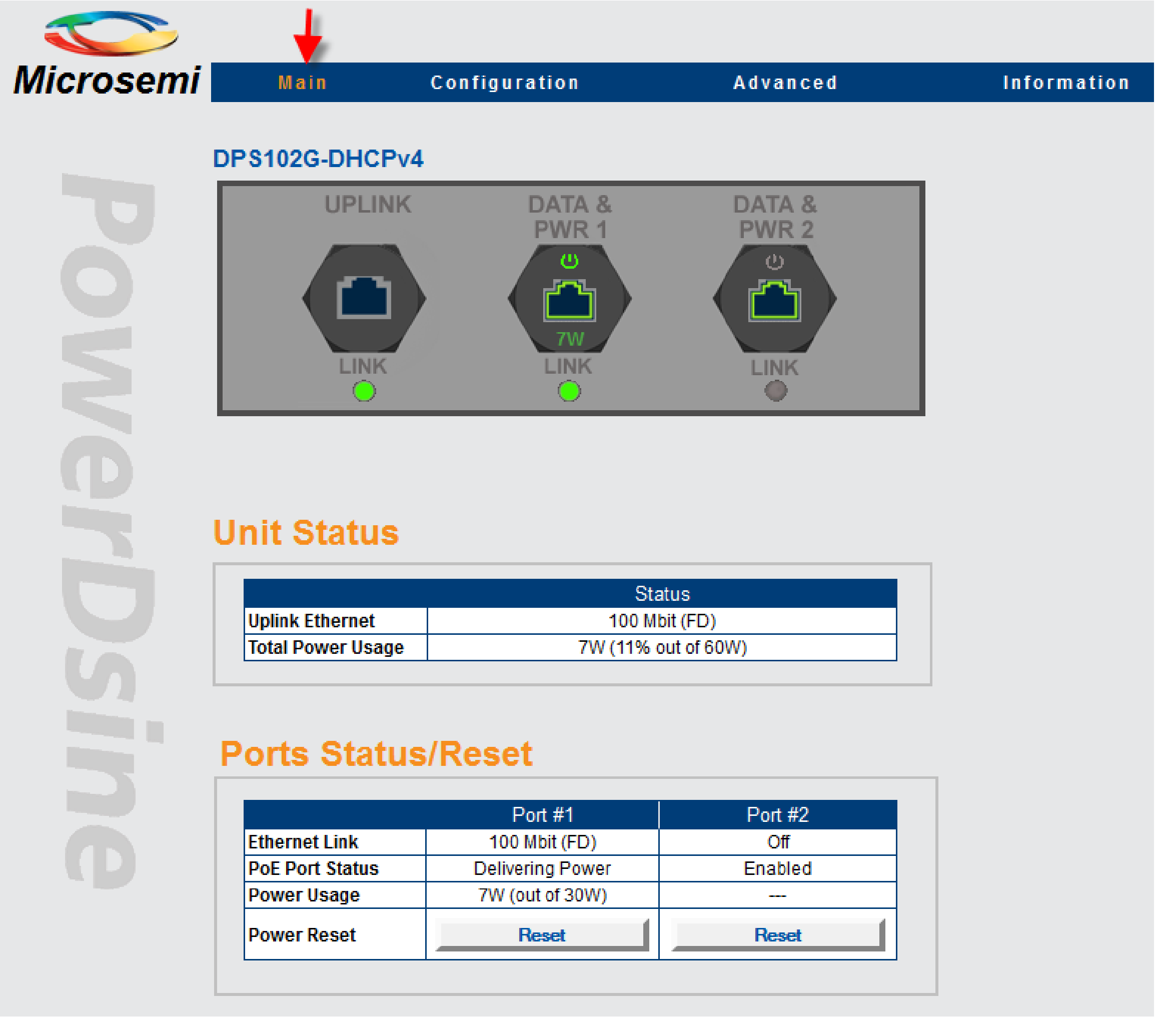


Date	Time	Priority	Hostname	Message
11-28-2013	18:25:19	Local0.Notice	172.16.5.229	Jan 1 0:00:12 PDS102.Floor-0.num-1 (GMT): MsgID#000 - System UP. RST:LowVolt BOOT:0=[APP OK] Host:PDS102.Floor-0.num-1 MAC:AA:AB:AC:6E:57:DD DHCPv4:No IPv4:172.16.5.229 DHCPv6:No

Figure 3-2: Powerup SysLog Report – Unit IP, MAC Address, Hostname, and More

3.2 Main Web Page

The main Web page is used to monitor unit status, PoE ports status such as Ethernet Link connection speed, PoE power consumption, and total unit PoE power consumption. The Web page is updated automatically every few seconds.



Unit Status

	Status
Uplink Ethernet	100 Mbit (FD)
Total Power Usage	7W (11% out of 60W)

Ports Status/Reset

	Port #1	Port #2
Ethernet Link	100 Mbit (FD)	Off
PoE Port Status	Delivering Power	Enabled
Power Usage	7W (out of 30W)	---
Power Reset	Reset	Reset

Figure 3-3: Main Web Page

Ethernet Network link is always enabled, regardless of PoE configuration (enabled/disabled), supporting 10MB, 100MB, and 1000MB speeds.

3.2.1 Main Web Page - Port Status

Each port may deliver power, network connectivity, or both. The images in the table below describe the various possible port states:

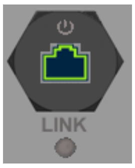
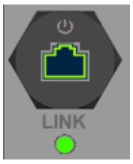
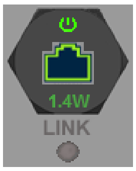
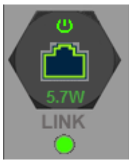
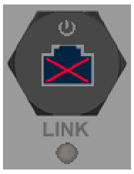
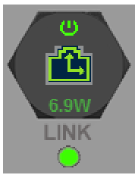
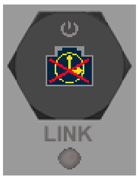
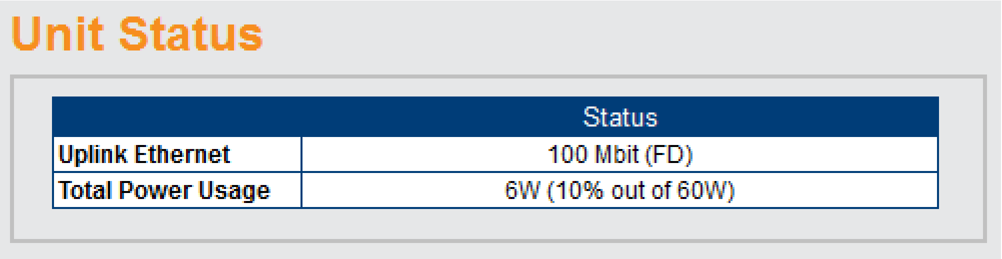
Image	Description	Comments
	• PoE port is enabled (green line around the RJ45 connector) • No PoE power is provided (upper power indicator is off) • No Ethernet link (lower link indicator image is gray)	
	• PoE port is enabled (green line around the RJ45 connector) • No PoE power is provided (upper power indicator is off) • Ethernet link is on (low link indicator image is green)	
	• PoE port is enabled (green line around the RJ45 connector) • PoE power is provided (upper power indicator is on). • No Ethernet link (lower link indicator image is gray)	
	• PoE port is enabled (green line around the RJ45 connector) • PoE power is provided (upper power indicator is on). • Ethernet link is on (low link indicator image is green)	
	• PoE port is disabled (RJ45 connector marked by two red lines) • No Ethernet link (lower link indicator image is gray) Note – PoE port can be disabled only by Telnet/SNMP	Ethernet port is enabled even when PoE is disabled (applicable to non-PoE device)
	• PoE port was enabled by Automatic Weekly Schedule Port Activation functionality (green clock arrows, plus green line around the RJ45 connector) • PoE power is provided (upper power indicator is on). • Ethernet link is on (low link indicator image is green)	
	• PoE port was disabled by ***Automatic Weekly Schedule Port Activation*** functionality (yellow clock arrows, plus two red cross lines) • No Ethernet link (lower link indicator image is gray)	Ethernet port is enabled even when PoE is disabled (applicable to non-PoE device)

Figure 3-4: Port Status

3.2.2 Main Web Page - Unit Status



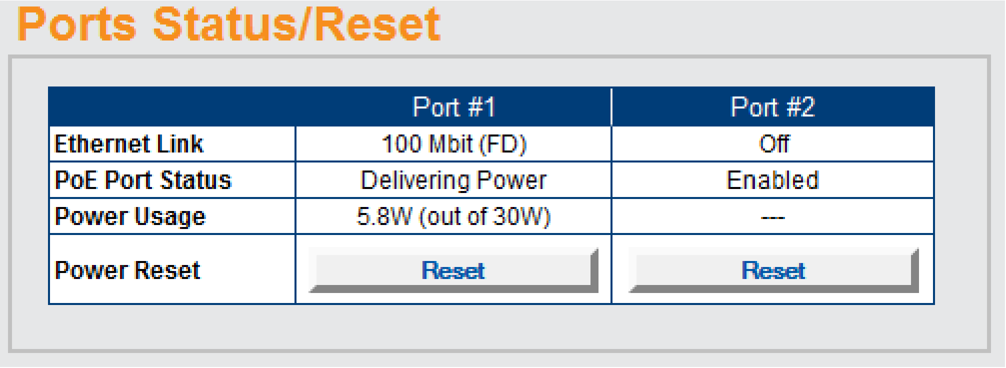
Unit Status

	Status
Uplink Ethernet	100 Mbit (FD)
Total Power Usage	6W (10% out of 60W)

Figure 3-5: Unit Status

Unit status reports uplink Ethernet speed (10/100/1000MB), and all ports total PoE power consumption.

3.2.3 Main Web Page – Ports Status/Reset



Ports Status/Reset

	Port #1	Port #2
Ethernet Link	100 Mbit (FD)	Off
PoE Port Status	Delivering Power	Enabled
Power Usage	5.8W (out of 30W)	---
Power Reset	Reset	Reset

Figure 3-6: Ports Status/Reset

- ***Port Status* – P**ort status reports for each port Ethernet link speed (10/100/1000MB) and type (Half Duplex, Full Duplex), PoE power consumption, and PoE port status.

- ***Power Reset* -** Pressing the Power Reset button turns off PoE port power for a few seconds, and immediately restores it back to enabled status.

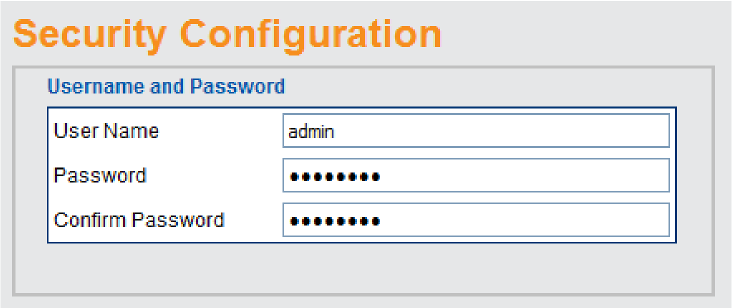
NOTE:

Pressing the Power Reset button will restore any PoE ports which were disabled by Telnet/SNMP back to enabled state.

3.3 Configuration Web Page

The configuration Web page allows configuring the following network parameters**:**

3.3.1 Security Configuration – Configure unit user name and password for remote Web or Telnet access.



Security Configuration

Username and Password

User Name: admin

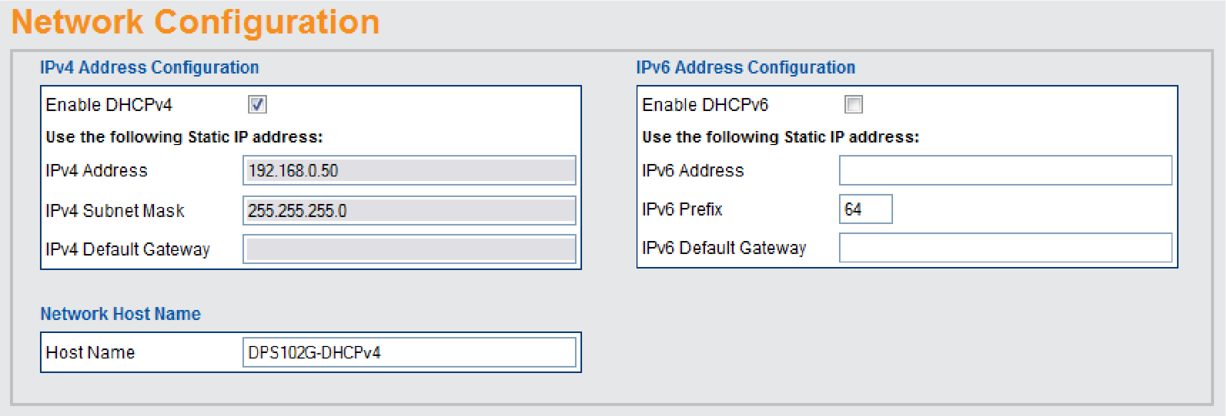
Password: ●●●●●●●●

Confirm Password: ●●●●●●●●

Figure 3-7: Security Configuration

User Name	Unit user name for remote Web/Telnet access
Password	Unit password for remote Web/Telnet access

3.3.2 Network Configuration – configure unit IPv4, IPv6 and host name parameters.



Network Configuration

IPv4 Address Configuration

Enable DHCPv4 ☑

Use the following Static IP address:

IPv4 Address: 192.168.0.50

IPv4 Subnet Mask: 255.255.255.0

IPv4 Default Gateway:

IPv6 Address Configuration

Enable DHCPv6 □

Use the following Static IP address:

IPv6 Address:

IPv6 Prefix: 64

IPv6 Default Gateway:

Network Host Name

Host Name: DPS102G-DHCPv4

Figure 3-8: Network Configuration

3.3.2.1 IPv4 Network Configuration

Enable DHCPv4	Obtain IPv4 address from DHCPv4 Server
IPv4 Address	Static IPv4 address whenever DHCPv4 is off
IPv4 Subnet Mask	Static IPv4 mask whenever DHCPv4 is off
IPv4 Default Gateway	Static IPv4 default gateway whenever DHCPv4 is off

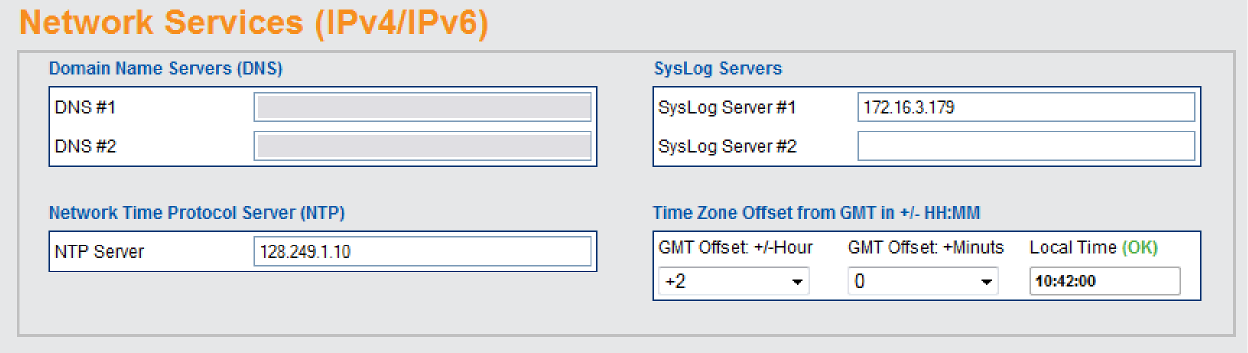
3.3.2.2 IPv6 Network Configuration

Enable DHCPv6	Obtain IPv6 address from DHCPv6 Server
IPv6 Address	Static IPv6 address whenever DHCPv4 is off
IPv6 Prefix	Static IPv6 mask whenever DHCPv4 is off
IPv6 Default Gateway	Static IPv6 default gateway whenever DHCPv4 is off

3.3.2.3 Network Hostname/FQDN

Host name field is used both by DHCPv4 and DHCPv6 to register the unit name in DHCPv4/v6 Server, allowing the IT manager to easily find which remote network device was given a specific IP address. Please note that IPv6 uses the FQDN terminology as host name.

3.3.3 Network Services Configuration (IPv4/IPv6)



Network Services (IPv4/IPv6)

Domain Name Servers (DNS)

DNS #1:

DNS #2:

SysLog Servers

SysLog Server #1: 172.16.3.179

SysLog Server #2:

Network Time Protocol Server (NTP)

NTP Server: 128.249.1.10

Time Zone Offset from GMT in +/- HH:MM

GMT Offset: +/-Hour: +2

GMT Offset: +Minuts: 0

Local Time (OK): 10:42:00

Figure 3-9: Network Services Configuration

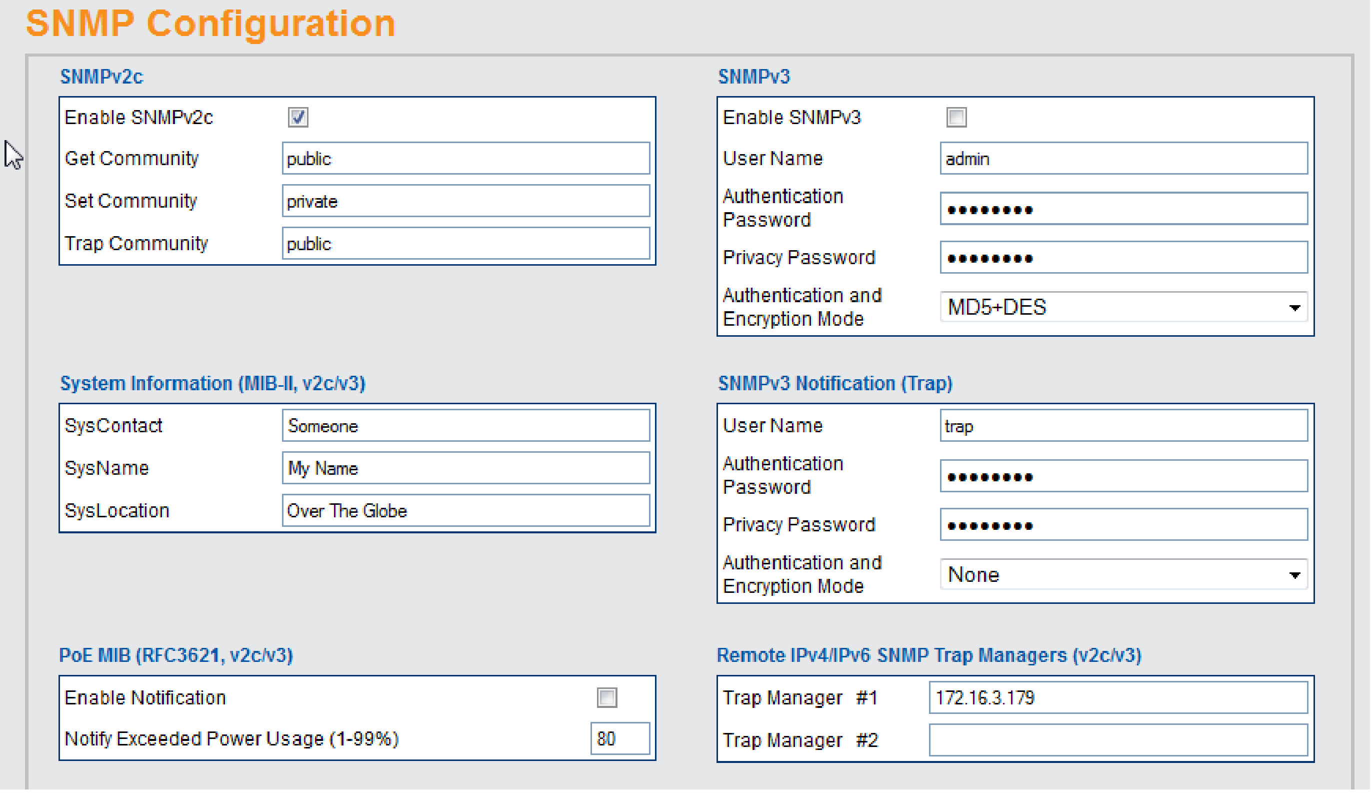
DNS Server #1 DNS Server #2	Domain Name Server IPv4/IPv6 address. Please note that DNS fields will become gray whenever DHCPv4 or DHCPv6 is enabled, expecting to get DNS IP address from DHCPv4/v6 Server.
SysLog Server #1 SysLog Server #2	Network System Log IPv4/IPv6 Servers address used to log various unit log message events, to be viewed later by the IT manager.
NTP Server	Network Time Protocol Server IPv4/IPv6 address required by ***Automatic Weekly Schedule PoE Port Activation*** feature.
Time Zone Offset	Local time shift from GMT time in hours and minutes.

NOTE:

For valid NTP Server IP configuration, please make sure a green (OK) appears to the right of Local Time label (Web page reload refresh may be required).

3.3.4 SNMP Configuration

SNMP configuration applies to configuration parameters common both to SNMPv2 and SNMPv3 (as SNMP trap list), SNMPv2 only, SNMPv3, and partial RFC3621 PoE MIB.



SNMP Configuration

SNMPv2c

Enable SNMPv2c	☑
Get Community	public
Set Community	private
Trap Community	public

SNMPv3

Enable SNMPv3	□
User Name	admin
Authentication Password	••••••••
Privacy Password	••••••••
Authentication and Encryption Mode	MD5+DES

System Information (MIB-II, v2c/v3)

SysContact	Someone
SysName	My Name
SysLocation	Over The Globe

SNMPv3 Notification (Trap)

User Name	trap
Authentication Password	••••••••
Privacy Password	••••••••
Authentication and Encryption Mode	None

PoE MIB (RFC3621, v2c/v3)

Enable Notification	□
Notify Exceeded Power Usage (1-99%)	80

Remote IPv4/IPv6 SNMP Trap Managers (v2c/v3)

Trap Manager #1	172.16.3.179
Trap Manager #2	

Figure 3-10: SNMP Configuration

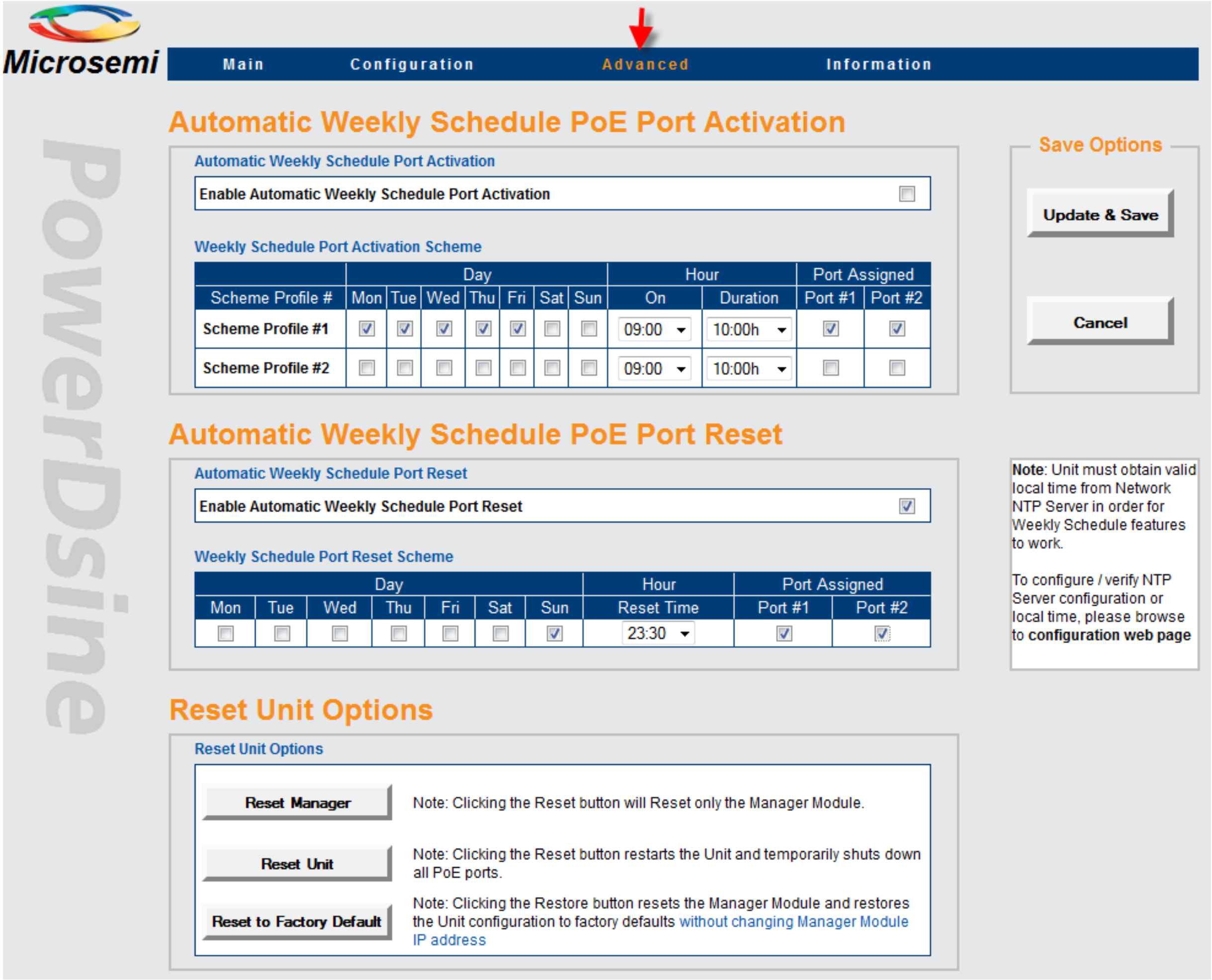
Enable SNMPv2	Enable/Disable SNMPv2 support.
SNMPv2 GET Community	SNMPv2 GET community string. For example – public.
SNMPv2 SET Community	SNMPv2 SET community string. For example – private.
SNMPv2 TRAP Community	SNMPv2 Trap community string. For example – public.
MIB-II SysContact	SNMP MIB-II system contact OiD string. For example – John.
MIB-II SysName	SNMP MIB-II system name. For example – My Unit.
MIB-II SysLocation	SNMP MIB-II system location. For example – University.
Trap Manager #1	First IPv4 / IPv6 / DNS name of remote SNMP Manager Server receiving unit trap reports such as Cold-Start, etc.
Trap Manager #2	Second IPv4 / IPv6 / DNS name of remote SNMP Manager Server receiving unit trap reports such as Cold-Start, etc.
Enable SNMPv3	Enable/Disable SNMPv3 support.
SNMPv3 User Name	SNMPv3 user name string.
SNMPv3 Authentication Password	SNMPv3 password to be used by MD5 / SHA.
SNMPv3 Privacy Password	SNMPv3 password to be used by DES.

SNMPv3 Authentication and Encryption Mode	• None – no authentication or encryption (no security - equivalent to SNMPv2). • MD5 – MD5 authentication with no encryption (packet can't be changed, however it can easily be analyzed by network sniffers). • SHA – SHA authentication with no encryption (similar to MD5, only using different authentication algorithm). • MD5+DES – authentication is done by MD5, while encryption is done by DES. • SHA+DES – authentication is done by SHA, while encryption is done by DES.
SNMPv3 Notification (trap) Authentication and Encryption Mode	• None – no authentication or encryption (no security - equivalent to SNMPv2). • MD5 – MD5 authentication with no encryption (packet can't be changed, however it can easily be analyzed by network sniffers). • SHA – SHA authentication with no encryption (similar to MD5, only using different authentication algorithm). • MD5+DES – authentication is done by MD5, while encryption is done by DES. • SHA+DES – authentication is done by SHA, while encryption is done by DES.
PoE MIB – Enable Notifications	Enable/Disable the following PoE trap reports • PoE power was provided / removed from PD device. • Unit total power consumption exceeds xy% out of max unit power. • Unit total power consumption was restored to less than xy% out of max unit power.
PoE MIB - Notify Exceeded Power Usage (1-99%)	• Report (if enabled) whenever unit total power consumption (xy%) percentage out of unit max power exceeds this percentage value. Also, report whenever unit total power drops below the same percentage.

3.4 Advanced Web Page

Advanced Web page offers the following features to be configured:

- Automatic Weekly Schedule PoE Port Activation
- Automatic Weekly Schedule PoE Port Reset
- Reset Unit Options
  - Reset Manager – Reset ***only the Network Manager*** without effecting PoE or network traffic through the various ports.
  - Reset Unit – Reset the internal Network Manager, internal PoE controller and internal Ethernet Switch.
  - Reset to Factory Default – Reset unit configuration to factory default ***excluding*** unit network configuration in order to enable remote unit access even after factory default button was pressed.



Automatic Weekly Schedule PoE Port Activation

Automatic Weekly Schedule Port Activation

Enable Automatic Weekly Schedule Port Activation ☐

Weekly Schedule Port Activation Scheme

	Day							Hour		Port Assigned	
Scheme Profile #	Mon	Tue	Wed	Thu	Fri	Sat	Sun	On	Duration	Port #1	Port #2
Scheme Profile #1	☑	☑	☑	☑	☑	☐	☐	09:00	10:00h	☑	☑
Scheme Profile #2	☐	☐	☐	☐	☐	☐	☐	09:00	10:00h	☐	☐

Save Options

Update & Save

Cancel

Automatic Weekly Schedule PoE Port Reset

Automatic Weekly Schedule Port Reset

Enable Automatic Weekly Schedule Port Reset ☑

Weekly Schedule Port Reset Scheme

Day							Hour	Port Assigned	
Mon	Tue	Wed	Thu	Fri	Sat	Sun	Reset Time	Port #1	Port #2
☐	☐	☐	☐	☐	☐	☑	23:30	☑	☑

Note: Unit must obtain valid local time from Network NTP Server in order for Weekly Schedule features to work.

To configure / verify NTP Server configuration or local time, please browse to **configuration web page**

Reset Unit Options

Reset Unit Options

Reset Manager — Note: Clicking the Reset button will Reset only the Manager Module.

Reset Unit — Note: Clicking the Reset button restarts the Unit and temporarily shuts down all PoE ports.

Reset to Factory Default — Note: Clicking the Restore button resets the Manager Module and restores the Unit configuration to factory defaults without changing Manager Module IP address

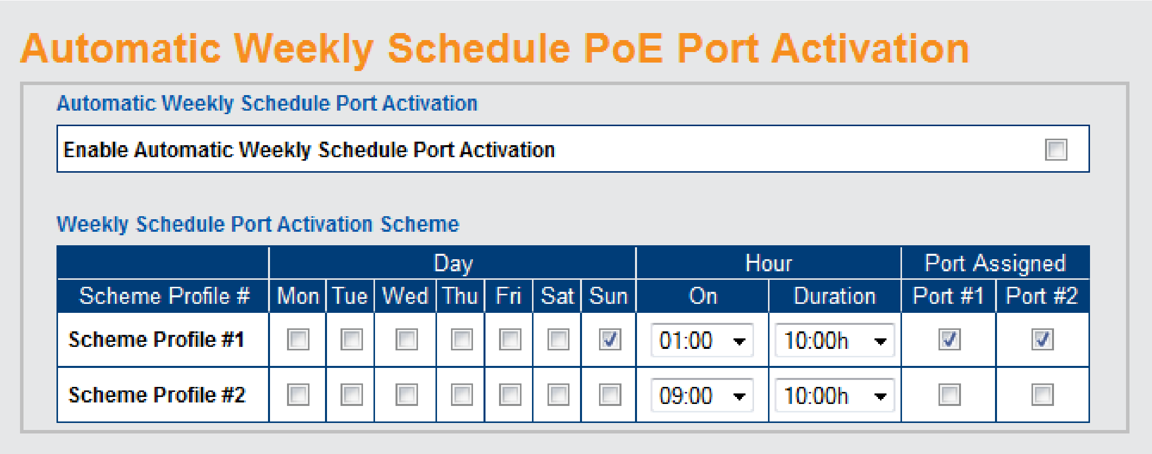
Figure 3-11: Advanced Web Page Configuration

3.4.1 Advanced Web Page – Automatic Weekly Schedule PoE Port Activation

Automatic Weekly Schedule PoE Port Activation offers automatic activation/deactivation of PoE devices on various days of the week for specific hours. It may be used to increase network security by turning off Wi-Fi Access Points during non-working hours or to save power during non-working hours by turning off PoE devices.

NOTE:

Automatic Weekly Schedule affects only PoE functionality, leaving Ethernet ports enabled, meaning that none PoE devices may still obtain network connectivity during the time PoE is disabled.



Automatic Weekly Schedule PoE Port Activation

Automatic Weekly Schedule Port Activation

Enable Automatic Weekly Schedule Port Activation □

Weekly Schedule Port Activation Scheme

	Day							Hour		Port Assigned	
Scheme Profile #	Mon	Tue	Wed	Thu	Fri	Sat	Sun	On	Duration	Port #1	Port #2
Scheme Profile #1	□	□	□	□	□	□	☑	01:00	10:00h	☑	☑
Scheme Profile #2	□	□	□	□	□	□	□	09:00	10:00h	□	□

Figure 3-12: Automatic Weekly Schedule PoE Port Activation

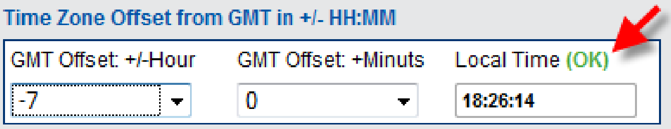
Automatic Weekly Schedule PoE Port Activation - main features:

- Two profile schemes to increase configuration flexibility by providing the option to activate different PoE ports on different days, hours, and time duration.
- 30-minute duration resolution, starting from 30 minutes up to 24 hours.
- One or more PoE ports can be assigned to each PoE activation scheme.

NOTE:

For Automatic Weekly Schedule PoE Port Activation to function properly, an NTP Server must be configured (see Configuration Web Page) providing correct GMT time.

Please make sure that a green "OK" appears to the right of the unit local time

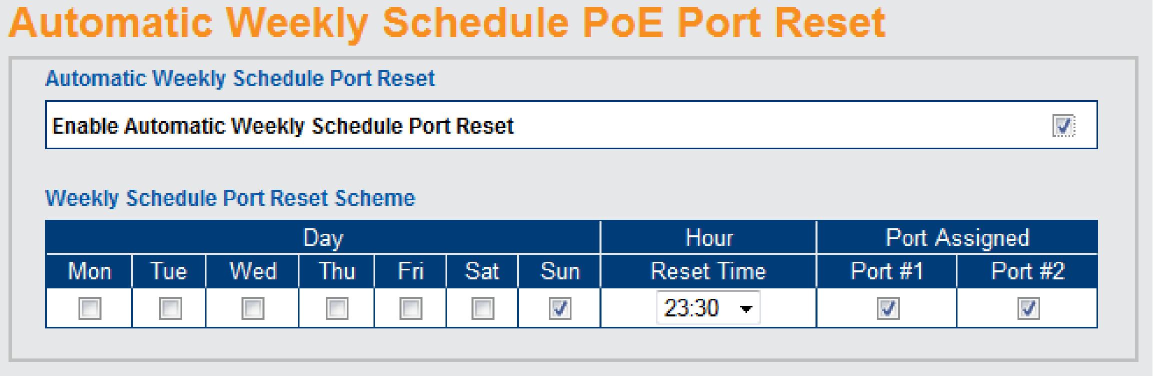


Time Zone Offset from GMT in +/- HH:MM

GMT Offset: +/-Hour	GMT Offset: +Minuts	Local Time (OK)
-7	0	18:26:14

3.4.2 Advanced Web Page – Automatic Weekly Schedule PoE Port Reset

Automatic Weekly Schedule PoE Port Reset provides auto PoE device initialization by turning off PoE power to PD device for a few seconds and restoring it back to on.



Automatic Weekly Schedule PoE Port Reset

Automatic Weekly Schedule Port Reset

Enable Automatic Weekly Schedule Port Reset	☑

Weekly Schedule Port Reset Scheme

Day							Hour	Port Assigned	
Mon	Tue	Wed	Thu	Fri	Sat	Sun	Reset Time	Port #1	Port #2
□	□	□	□	□	□	☑	23:30	☑	☑

Figure 3-13: Automatic Weekly Schedule PoE Port Reset

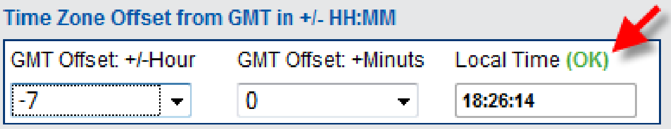
Automatic Weekly Schedule PoE Port Reset – main features:

- Flexibility on the days that PoE port reset should be done (multiple day combination).
- 30-minute duration resolution, starting from 30 minutes up to 24 hours.
- One or more PoE ports can be re-initialized.

NOTE:

For Automatic Weekly Schedule PoE Port Reset to function properly, an NTP Server must be configured (see Configuration Web Page) providing correct GMT time.

Please make sure that a green OK appears to the right of the unit local time

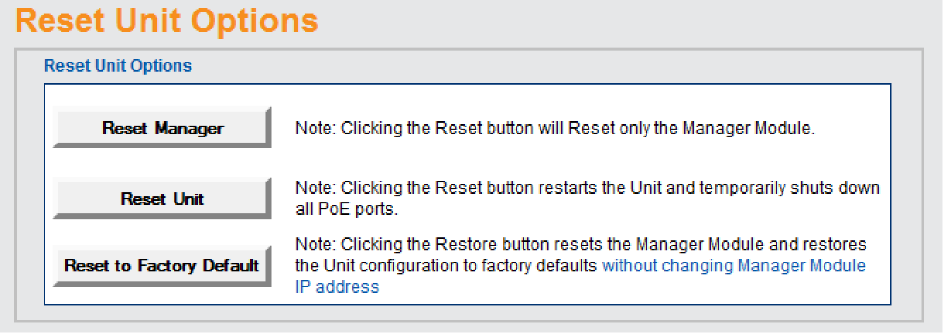


Time Zone Offset from GMT in +/- HH:MM

GMT Offset: +/-Hour	GMT Offset: +Minuts	Local Time (OK)
-7	0	18:26:14

3.4.3 Advanced Web Page – Reset Unit Options

The unit supports three different reset options (also available over Telnet)



Reset Unit Options

Reset Unit Options

Reset Manager	Note: Clicking the Reset button will Reset only the Manager Module.
Reset Unit	Note: Clicking the Reset button restarts the Unit and temporarily shuts down all PoE ports.
Reset to Factory Default	Note: Clicking the Restore button resets the Manager Module and restores the Unit configuration to factory defaults without changing Manager Module IP address

Figure 3-14: Reset Unit Options

- **Reset Manager** – Reset only the internal network manager responsible for unit network management interfaces such as Web, Telnet, SNMP, etc. Internal Ethernet switch will be also reset (network will be down for a few seconds) leaving PoE power unchanged (powered PD devices will continue normal operation as if no reset was done).

NOTE:

Network traffic to PD devices might be interrupted for several seconds, without affecting PoE power.

- **Reset Unit** – Reset the entire unit including the internal Network Manger, the PoE controller, and the internal Ethernet Switch.

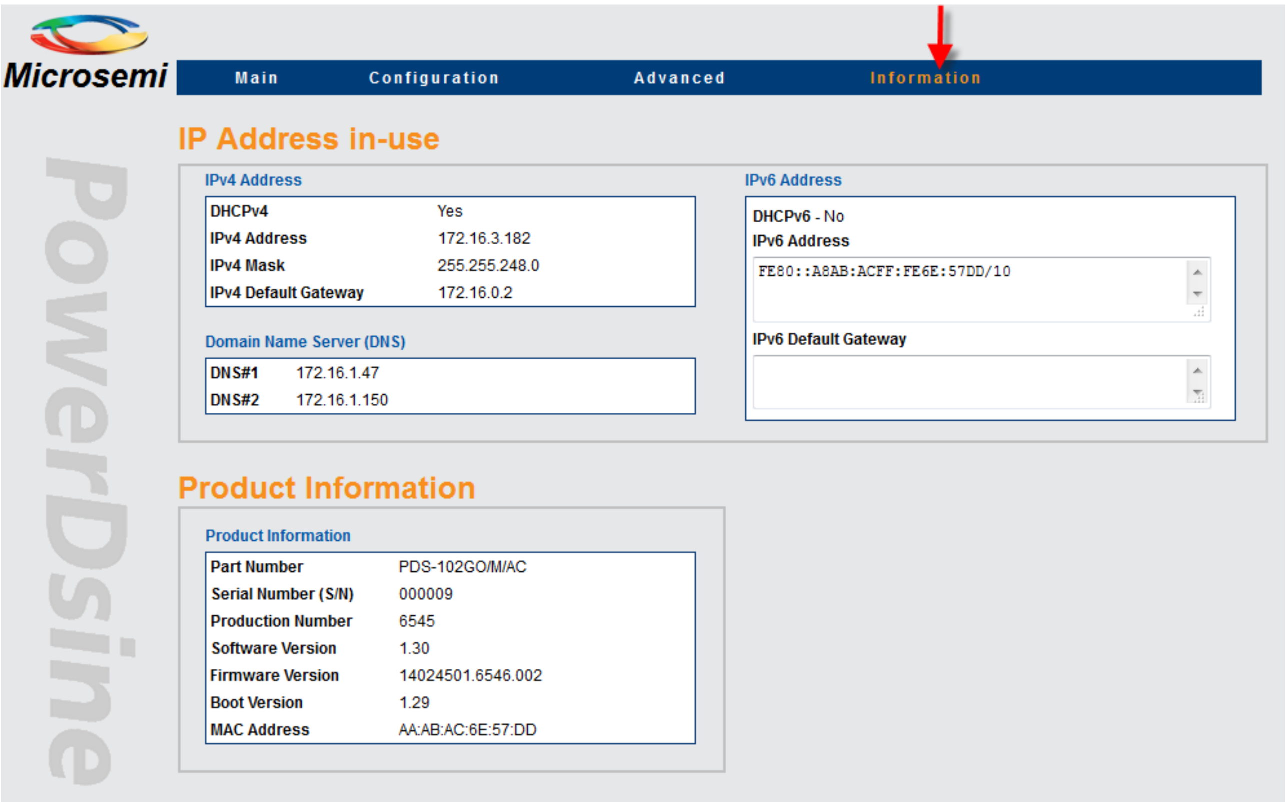
- **Restore to Factory Default** – Restore unit configuration to factory default***, leaving IPv4/IPv6 network configuration unchanged*** (as DHCP/Static IP, IP Address, etc.), maintaining the option to access the unit over the network as before.

NOTE:

To simplify finding the unit over the network, upon power up the unit will send SysLog broadcast messages (to any SysLog server on the Network) reporting its IP network configuration parameters, its MAC address, host name, etc.

3.5 Information Web Page

Information Web page provides information on current IPv4 and IPv6 addresses, plus miscellaneous product information such as software version, PoE firmware version, etc.



IP Address in-use

IPv4 Address

DHCPv4	Yes
IPv4 Address	172.16.3.182
IPv4 Mask	255.255.248.0
IPv4 Default Gateway	172.16.0.2

Domain Name Server (DNS)

DNS#1	172.16.1.47
DNS#2	172.16.1.150

IPv6 Address

DHCPv6 - No

IPv6 Address

FE80::A8AB:ACFF:FE6E:57DD/10

IPv6 Default Gateway

Product Information

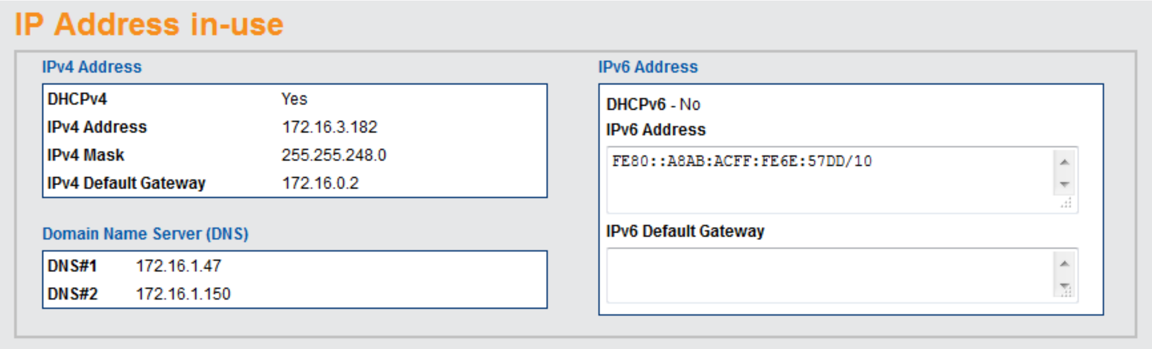
Product Information

Part Number	PDS-102GO/M/AC
Serial Number (S/N)	000009
Production Number	6545
Software Version	1.30
Firmware Version	14024501.6546.002
Boot Version	1.29
MAC Address	AA:AB:AC:6E:57:DD

Figure 3-15: Information Web Page

3.5.1 Information Web Page – IP Address in-use

The IP Address in-use reports in-use unit IPv4 address, in-use IPv6 address, and in-use DNS (Domain Name Servers)



IP Address in-use

IPv4 Address

DHCPv4	Yes
IPv4 Address	172.16.3.182
IPv4 Mask	255.255.248.0
IPv4 Default Gateway	172.16.0.2

Domain Name Server (DNS)

DNS#1	172.16.1.47
DNS#2	172.16.1.150

IPv6 Address

DHCPv6 - No

IPv6 Address

FE80::A8AB:ACFF:FE6E:57DD/10

IPv6 Default Gateway

Figure 3-16: IP Address In-Use

3.5.1.1 Information Web Page – In use IPv4 Address

DHCPv4	Yes/No – was the IP address obtained by DHCPv4, or is a static IP.
IPv4 Address	The actual in-use IPv4 address (for example 172.5.6.89).
IPv4 Mask	The actual in-use IPv4 address mask (for example (255.255.255.0).
IPv4 Default Gateway	The actual in-use IPv4 default gateway (for example 172.5.6.1).

3.5.1.2 Information Web Page – In-Use DNS

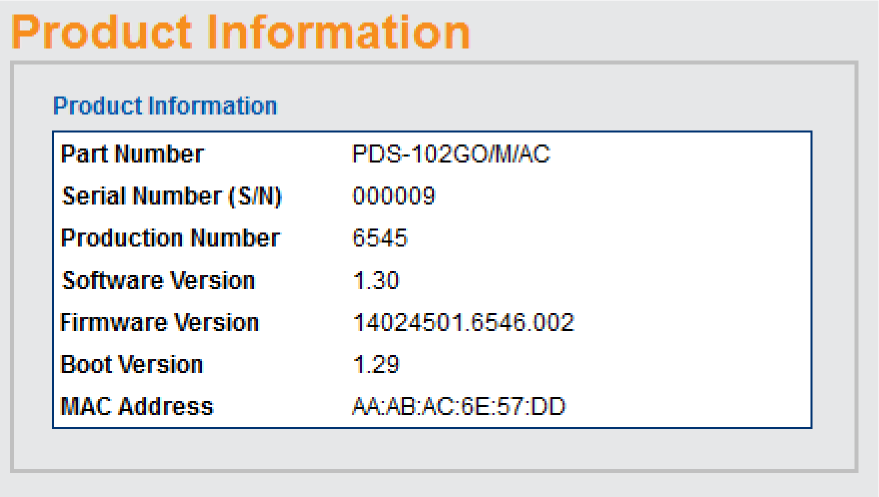
DNS #1	First in-use Domain Name Server (IPv4 / IPv6) responsible for converting URL names such as my-computer.com to IPv4/IPv6 addresses.
DNS #2	Alternate in-use second DNS to be used in case the first DNS is down.

3.5.1.3 Information Web Page – In-Use IPv6 Address

DHCPv6	Yes/No – was the IPv6 address obtained by DHCPv6, or is it a static IP.
IPv6 Address + Prefix	The actual in-use IPv6 address. While IPv4 has only a single address, IPv6 may have two or more IPv6 addresses: • Local Link IPv6 address. For example: FE80::A8AB:ACFF:FE6E:57DD • IPv6 address on same IPv6 Net as advertised by the IPv6 Router • Static / DHCPv6 address.
IPv6 Default Gateway	IPv6 address of the Default Gateway.

3.5.2 Information Web Page – Product Information

The product information section lists the unit MAC address, software version, PoE firmware, serial number, etc.



Product Information

Product Information

Part Number	PDS-102GO/M/AC
Serial Number (S/N)	000009
Production Number	6545
Software Version	1.30
Firmware Version	14024501.6546.002
Boot Version	1.29
MAC Address	AA:AB:AC:6E:57:DD

Figure 3-17: Product Information

Part Number	Unit marketing part number
Serial Number	Unit production serial number
Production Number	Unit internal production number (for internal use)
Software Version	Unit Network Manager software version
Firmware Version	Unit PoE firmware version (responsible for PoE functionality)
Boot Version	Unit Boot version
MAC Address	Unit MAC addresses. A unique 6-byte number used for Ethernet Network communication.

4 Telnet Interface

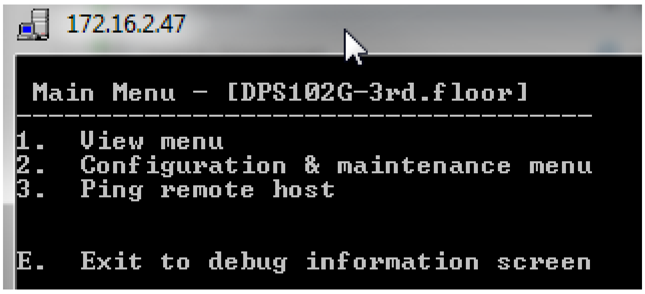
The Telnet interface was designed to be used mostly for various maintenance tasks such as software updates, and provides an easy and convenient interface for IT managers who are used to Telnet. To simplify Telnet usage, all Telnet menus are menu driven, eliminating the need to learn and remember complicated text commands.

NOTE:

- **Only one remote user can access Telnet at any given time. In case a second remote Telnet user will try to access the unit while the first Telnet user is still active, a short message will appear to the second Telnet user requesting the user to try and reconnect over Telnet a little later.**
- **Non-active Telnet session (no keystroke from remote user) will be terminated automatically after three minutes.**
- **Telnet is password protected, sharing the same username/password as for Web access.**

4.1 Telnet – Main Menu

To easily identify the unit being accessed by Telnet in case the user has multiple units, the unit hostname string is shown to the right of the Main Menu title.



172.16.2.47

```
 Main Menu - [DPS102G-3rd.floor]
------------------------------------
1.  View menu
2.  Configuration & maintenance menu
3.  Ping remote host


E.  Exit to debug information screen
```

Figure 4-1: Telnet Main Menu

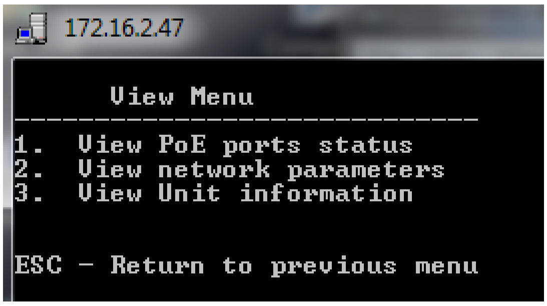
The Main Menu offers three options. All the View options are under the View menu. All the configuration and maintenance options (such as software updates, upload/download configurations) are under Configuration. The third option is Ping which should be used to resolve and test network connectivity issues.

NOTE:

To ease unit identification, the unit Hostname/FQDN string is also displayed in the main menu (PDS102G-3rd.floor in the example above).

4.2 Telnet – View Menu

Telnet View option provides information on PoE ports status, network in-use parameters, and unit information.



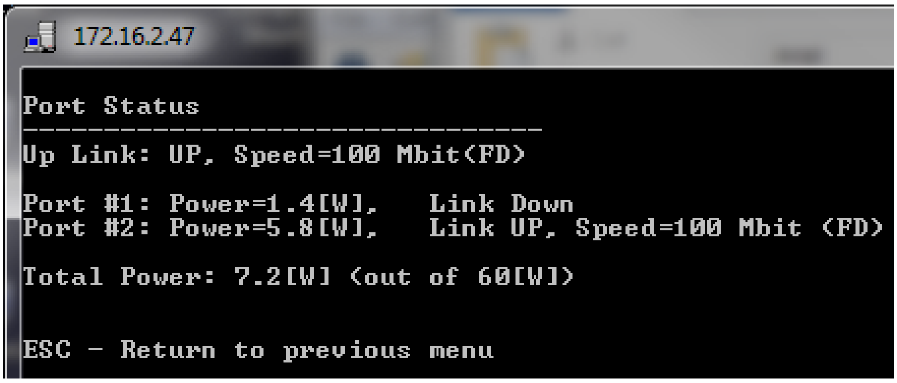
```
172.16.2.47

      View Menu
-----------------------------
1.   View PoE ports status
2.   View network parameters
3.   View Unit information


ESC - Return to previous menu
```

Figure 4-2: Telnet View Menu

4.2.1 Telnet – View PoE Ports Status

Telnet View PoE ports status provides network plus PoE power information about the various ports.

- **Network –** Reports Ethernet link speed (10/100/1000) and HD/FD connection type.
- **PoE –** Power consumption of each remote PD device.
- **Total Power –** Total power consumption of all PDs from all active PoE ports plus maximum available power.

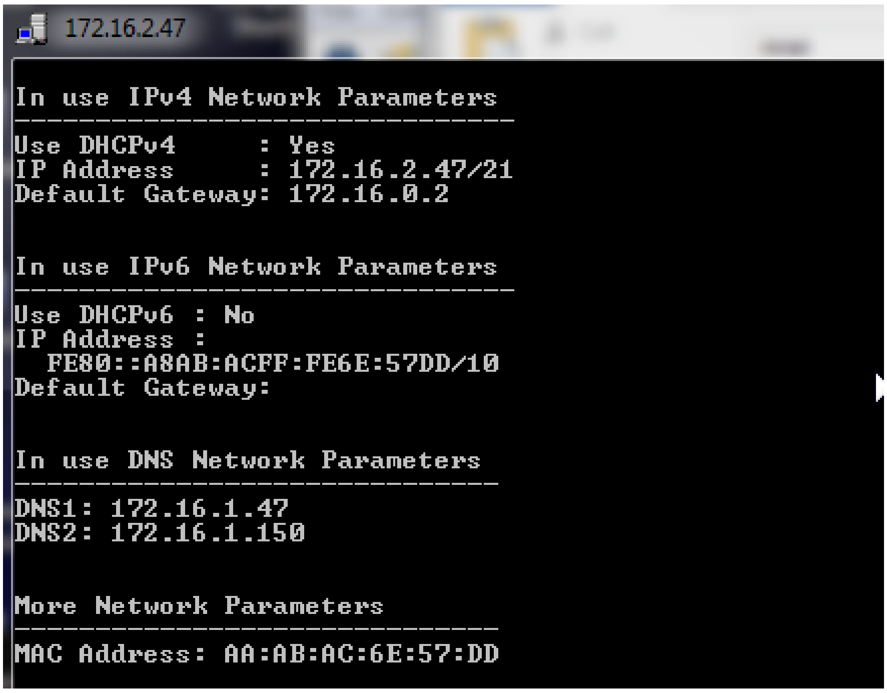


```
172.16.2.47

Port Status
--------------------------------
Up Link: UP, Speed=100 Mbit(FD)

Port #1: Power=1.4[W],   Link Down
Port #2: Power=5.8[W],   Link UP, Speed=100 Mbit (FD)

Total Power: 7.2[W] (out of 60[W])


ESC - Return to previous menu
```

Figure 4-3: Telnet View PoE Ports Status

4.2.2 Telnet – View Network Parameters

Telnet – View Network Parameters provides information on in-use IPv4, IPv4, Default Gateway and unit MAC Address.



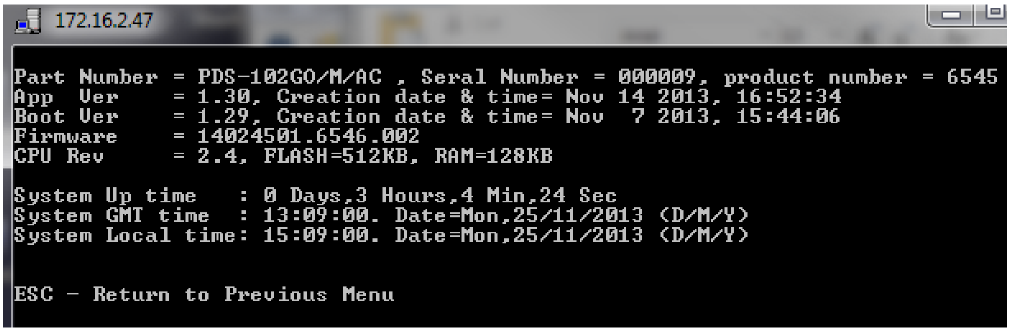
```
In use IPv4 Network Parameters
------------------------------
Use DHCPv4      : Yes
IP Address      : 172.16.2.47/21
Default Gateway: 172.16.0.2

In use IPv6 Network Parameters
------------------------------
Use DHCPv6 : No
IP Address :
  FE80::A8AB:ACFF:FE6E:57DD/10
Default Gateway:

In use DNS Network Parameters
-----------------------------
DNS1: 172.16.1.47
DNS2: 172.16.1.150

More Network Parameters
-----------------------------
MAC Address: AA:AB:AC:6E:57:DD
```

Figure 4-4: Telnet View Network Parameters

- **In-use IPv4 Network Parameters –** Reports if DHCPv4 is enabled or disabled, and the actual in-use IPv4 address, IPv4 mask and default gateway**.**
- **In-use IPv6 Network Parameters –** Reports if DHCPv6 is enabled or disabled, and the actual in-use IPv6 address, IPv6 prefix and default gateway**.** Please note that IPv6 may report several IPv6 addresses which were obtained automatically in addition to static/DHCPv6 IPv6 address.
- **In-use DNS Network Parameters –** Reports in-use IPv4/IPv6 Domain Name Server IPs which were configured statically or obtained by DHCPv4/DHCPv6.
- **More Network Parameters –** Reports the unit MAC address.

4.2.3 Telnet – View Unit Information

View Unit Information – provides a summary of unit production parameters such as software version, Boot version, product type, etc.



```
Part Number = PDS-102GO/M/AC , Seral Number = 000009, product number = 6545
App  Ver    = 1.30, Creation date & time= Nov 14 2013, 16:52:34
Boot Ver    = 1.29, Creation date & time= Nov  7 2013, 15:44:06
Firmware    = 14024501.6546.002
CPU  Rev    = 2.4, FLASH=512KB, RAM=128KB

System Up time    : 0 Days,3 Hours,4 Min,24 Sec
System GMT time   : 13:09:00. Date=Mon,25/11/2013 (D/M/Y)
System Local time: 15:09:00. Date=Mon,25/11/2013 (D/M/Y)


ESC - Return to Previous Menu
```

Figure 4-5: Telnet View Unit Information

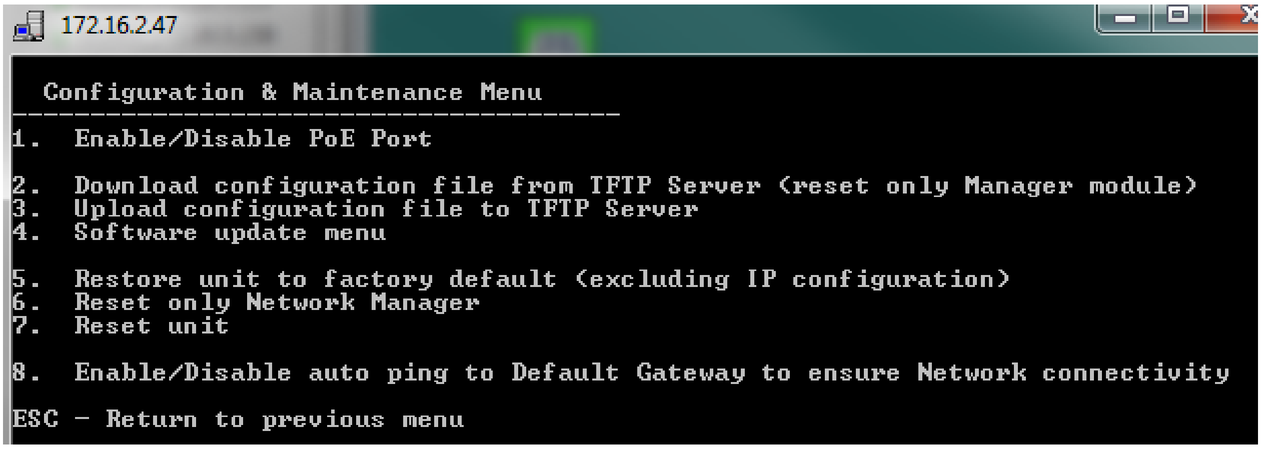
Part Number	Unit marketing part number
Serial Number	Unit production serial number
Production Number	Unit internal production number (for internal use only)
App Ver	Unit Network Manager software version
Boot Version	Unit Boot version
Firmware Version	Unit PoE firmware responsible for PoE functionality
CPU Rev, FLAH, RAM	For internal use only
System Up Time	The time passed since the unit was reset
System GMT time	Unit GMT time as it was obtained from NTP Server
System Local Time	Unit local time (GMT time plus time zone shift)

4.3 Telnet – Configuration and Maintenance Menu

Telnet Configuration and Maintenance Menu provides the option to enable/disable PoE ports (no effect on Ethernet Link), upload/download unit configuration and perform software updates, various unit reset options, and enable/disable auto ping to Default Gateway to ensure network connectivity.

NOTE:

Please refer to Sections 7 and 8 for a detailed description on how to upload/download the unit configuration or perform software updates.



```
172.16.2.47

 Configuration & Maintenance Menu
-----------------------------------------
1.  Enable/Disable PoE Port

2.  Download configuration file from TFTP Server (reset only Manager module)
3.  Upload configuration file to TFTP Server
4.  Software update menu

5.  Restore unit to factory default (excluding IP configuration)
6.  Reset only Network Manager
7.  Reset unit

8.  Enable/Disable auto ping to Default Gateway to ensure Network connectivity

ESC - Return to previous menu
```

Figure 4-6: Telnet Configuration and Maintenance Menu

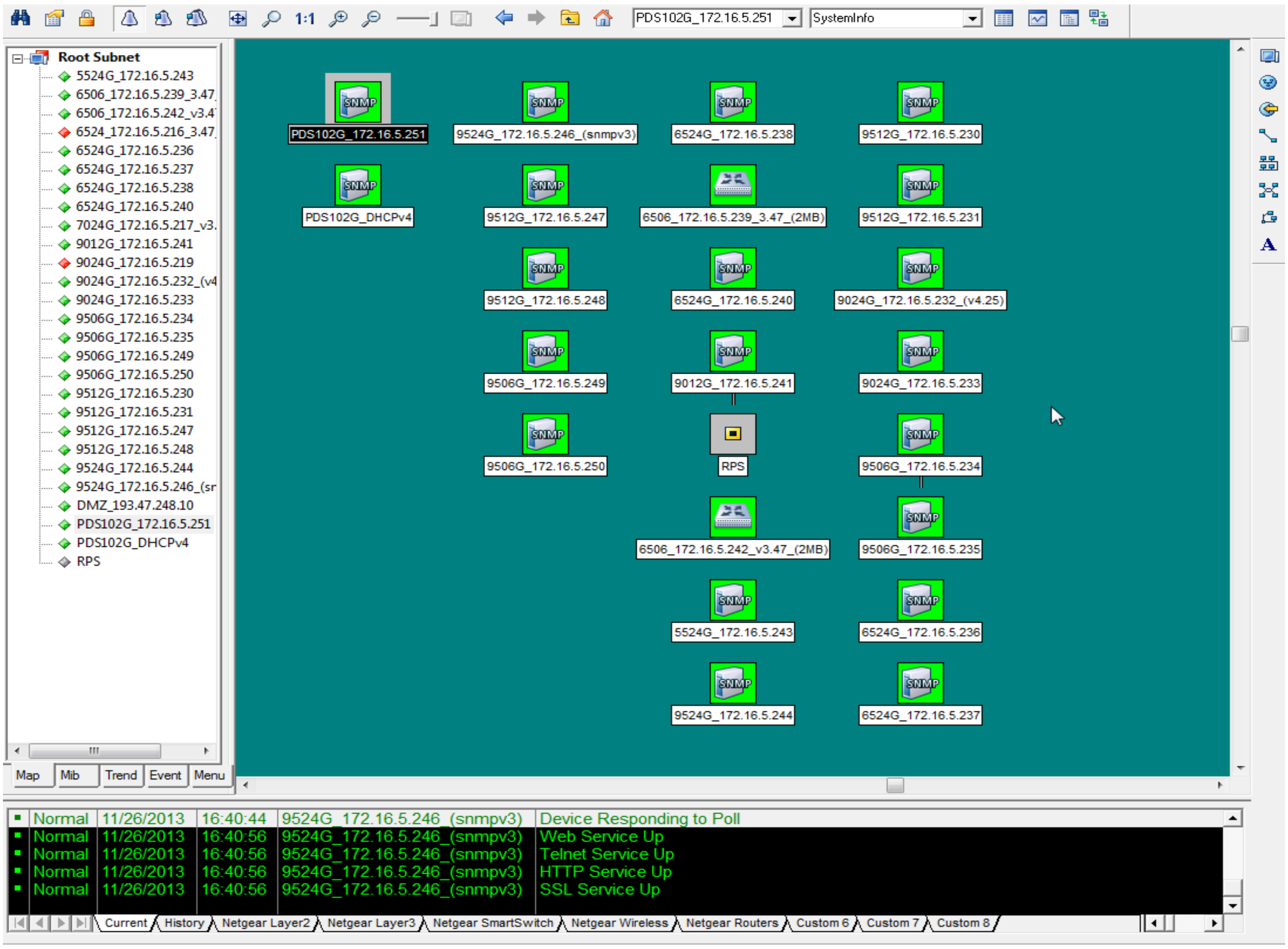
Enable/Disable PoE Port	Enable/disable PoE port (Ethernet link remains enabled even when no power is provided).
Download configuration file from TFTP Server	Download unit configuration file from TFTP Server to the unit over the network (please refer to Section 7 for more details). After successful configuration download the internal Network Manager will reset itself without affecting PoE functionality. However, network traffic may be interrupted for several seconds while the internal Ethernet Switch is reinitialized.
Upload configuration file to TFTP Server	Upload unit configuration file from unit to TFTP Server over the network (please refer to Section 7 for more details).
Software update menu	Performs software update by downloading new version from TFTP Server (please refer to Section 8 for more details). During the software update PoE functionality will remain active. However, network traffic may be interrupted for several seconds.
Restore unit to factory default (excluding IP configuration)	Restore unit configuration to factory default, leaving the IPv4/IPv6 network configuration unchanged (as DHCP/Static IP, IP Address, etc.). Leaving IP configuration unchanged maintains the option to access the unit over the network as before.
Reset only Network Manager	Reset only the internal Network Manager is responsible for unit network management interfaces such as Web, Telnet, SNMP, etc. Internal Ethernet switch will also be reset (the network will be down for a few seconds) leaving PoE power unchanged (powered PD devices will continue normal operation as if no reset was done).
Reset unit	Reset the entire unit including the internal Network Manger, the PoE controller, and the internal Ethernet Switch.
Enable/Disable auto ping to Default Gateway to ensure network connectivity	When enabled, the unit will verify proper network connectivity by pinging default gateway every 12 seconds (IPv4 DGW or IPv6 DGW). After 10 consecutive ping failures, Network Management Module will reset itself without affecting PoE ports.

NOTE:

To simplify locating the unit over the Network, upon power up the unit will send SysLog broadcast messages (to any SysLog server on the network) reporting its IP network configuration parameters, its MAC address, host name, etc.

5 SNMP Monitoring and Configuration

Multiple units can be managed by using third-party standard network management tools such as HP Openview, IBM Tivoli, SNMPc, etc.



```
Normal  11/26/2013  16:40:44  9524G_172.16.5.246_(snmpv3)  Device Responding to Poll
Normal  11/26/2013  16:40:56  9524G_172.16.5.246_(snmpv3)  Web Service Up
Normal  11/26/2013  16:40:56  9524G_172.16.5.246_(snmpv3)  Telnet Service Up
Normal  11/26/2013  16:40:56  9524G_172.16.5.246_(snmpv3)  HTTP Service Up
Normal  11/26/2013  16:40:56  9524G_172.16.5.246_(snmpv3)  SSL Service Up
```

Figure 5-1: SNMPc Network Management Tool

NOTE:

Due to security concerns the unit is shipped with the SNMP disabled. Prior to enabling SNMP, please modify SNMP community strings and only then enable it.

5.1 Enabling SNMP

The Network Manager interface supports SNMPv1, SNMPv2c, and SNMPv3 (since SNMPv1 is obsolete, traps will be sent in SNMPv2, SNMPv3 or both).

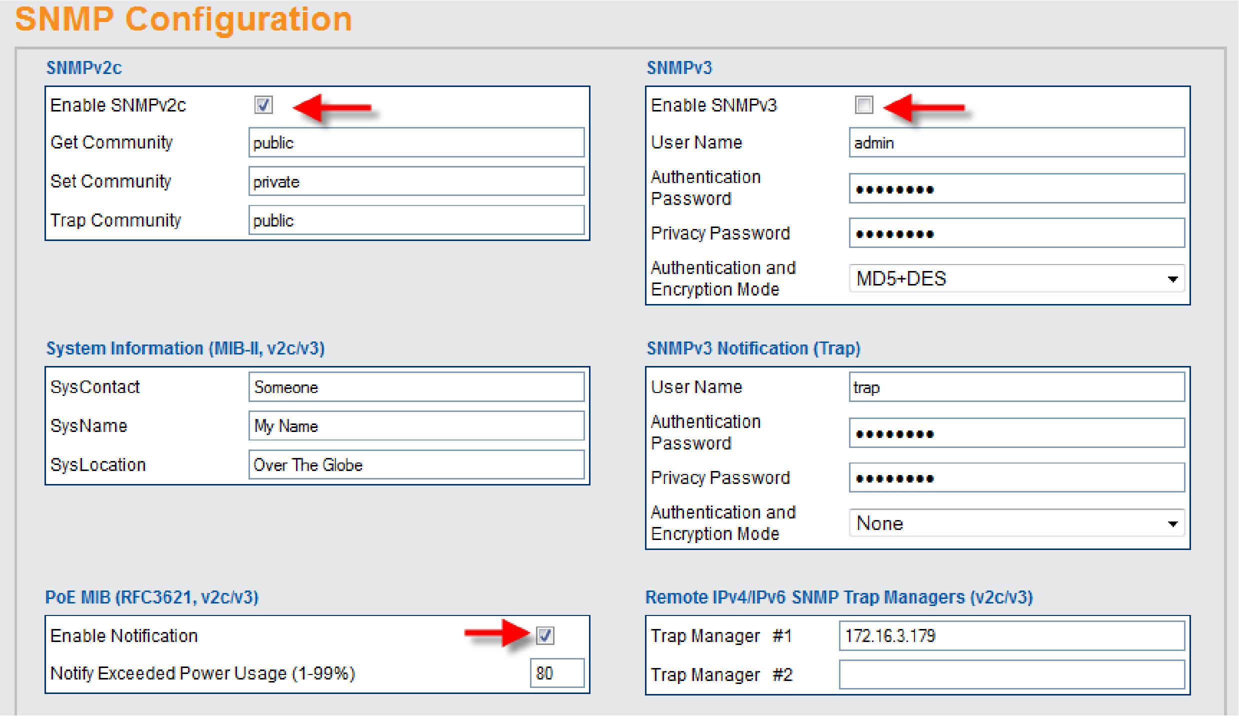
To use the SNMP:

1. Browse to the Configuration Web page and enable SNMPv2 or SNMPv3:

   - For SNMPv2c, make sure that community strings match your SNMP manager configuration.

- For SNMPv3, make sure username, authentication and privacy password and encryption methods match your SNMP manager configuration.

2. Traps:
   - To enable traps set remote manager IP address in the ***Remote IPv4/IPv6 SNMP Trap Managers*** window.
   - To enable PoE traps (PoE port status changed, unit consumes over xy% of total unit power, or unit now consumes less than xy% of total unit power), please enable PoE Notifications (see image below).



SNMP Configuration

SNMPv2c

Enable SNMPv2c	☑
Get Community	public
Set Community	private
Trap Community	public

SNMPv3

Enable SNMPv3	□
User Name	admin
Authentication Password	••••••••
Privacy Password	••••••••
Authentication and Encryption Mode	MD5+DES

System Information (MIB-II, v2c/v3)

SysContact	Someone
SysName	My Name
SysLocation	Over The Globe

SNMPv3 Notification (Trap)

User Name	trap
Authentication Password	••••••••
Privacy Password	••••••••
Authentication and Encryption Mode	None

PoE MIB (RFC3621, v2c/v3)

Enable Notification	☑
Notify Exceeded Power Usage (1-99%)	80

Remote IPv4/IPv6 SNMP Trap Managers (v2c/v3)

Trap Manager #1	172.16.3.179
Trap Manager #2	

Figure 5-2: Enable SNMPv2, SNMPv3 and PoE traps

5.2 SNMP MIBs

Several MIBs are supported by SNMP manager.

- **RFC1213**: MIB-II which provides general IPv4 network statistics, and information on the device being managed.
- **RFC3621**: Power Over Ethernet (PoE) MIB which provides various management capabilities (see Figure 5-3)
- **Private MIB**: Enhance PoE functionality beyond RFC3621 PoE MIB.

5.3 RFC3621 PoE MIB

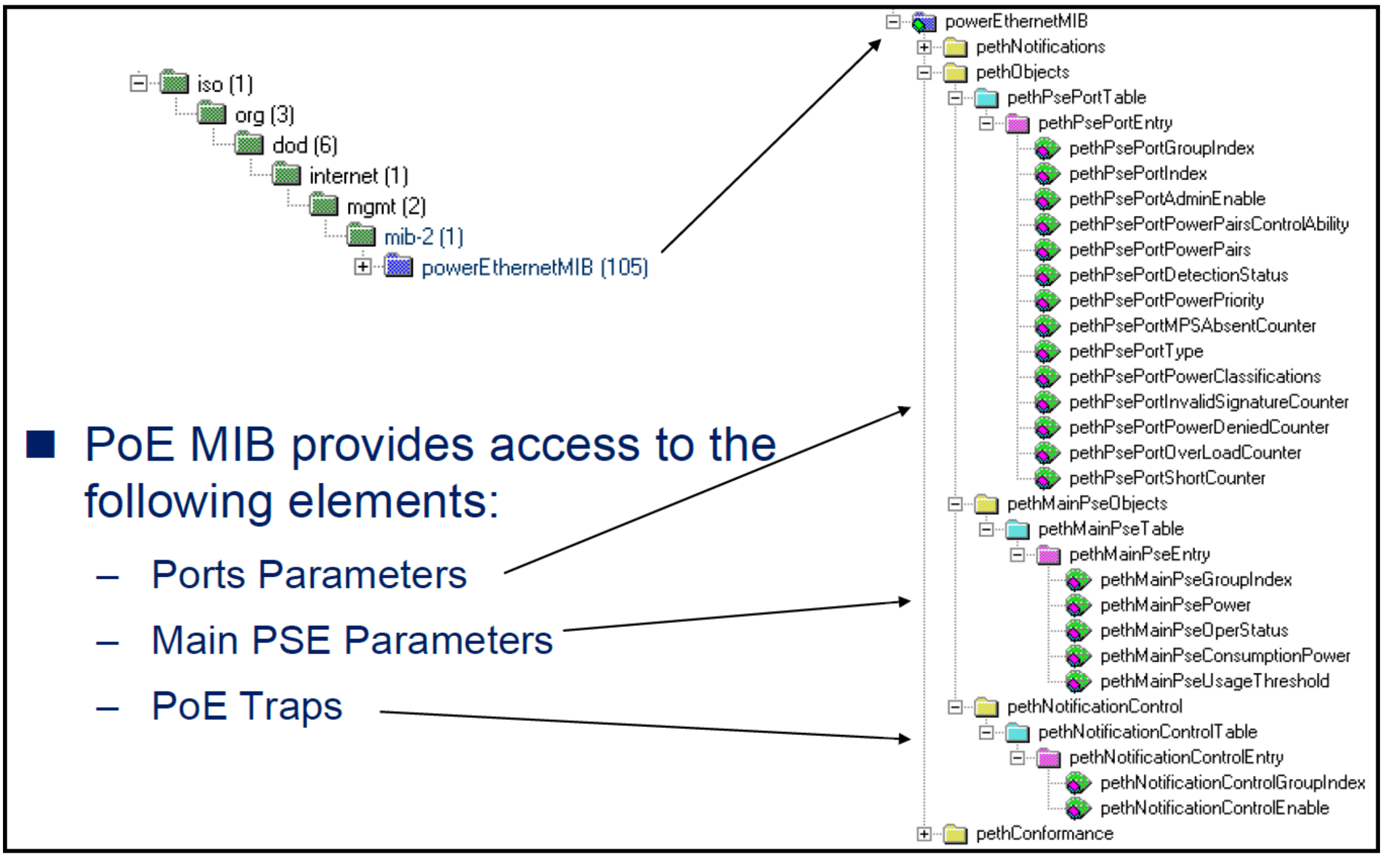
NOTE:

For a detailed PoE MIB description, please refer to Microsemi's Technical Note – 132 (can be found on the CD), which describes in detail PoE MIB functionality.

RFC3621 PoE MIB is located under 1.3.6.1.2.1.105 SNMP MIB tree. The MIB is divided into three sections (see Figure 5-3). The first section deals with PoE ports and provides functionality such as enable/disable, read port status, class, etc. Each OiD is accessed as a two-dimensional array table.

The second section deals with the power source that is responsible for providing power to a group of PoE ports. It enables reading total power consumption, power supply status, etc.

The third section enable/disables PoE traps to be sent to remote SNMP managers.



- PoE MIB provides access to the following elements:
  - Ports Parameters
  - Main PSE Parameters
  - PoE Traps

Figure 5-3: MIB Tree Structure

6 SysLog Message Report

The unit sends various internal event reports to an external IPv4/IPv6 host running a SysLog daemon application which logs those events for future use. For SysLog events to be sent, the user must configure SysLog server IP address by browsing to the unit configuration Web page.

The log events are divided into three categories:

- Broadcast IPv4 SysLog events to be intercepted by ***any*** SysLog server on the local LAN Network ***regardless of unit SysLog configuration,*** easing locating unit IP on the Network, and reporting major events such as unit recovery from power failure, etc.
- RFC3621 PoE traps to be send also as SysLog messages, simplifying the readability of such events to the remote user.
- Proprietary SysLog events as potential security breach whenever remote user tries to access the unit over Web/Telnet with incorrect username, potential failures, etc.

6.1 SysLog Message Types

The table below summarizes the various SysLog messages that may be sent by the SysLog Server:

Msg ID	Description	Information to be provided	Comments
0	**System UP** – Will be send each time power is provided to the unit, or the internal Network Manager resets itself.	• Reset cause • Boot status • Unit Hostname • Unit MAC Address • IPv4 Address (static/HDCPv4) • All IPv6 address (static/DHCPv6)	Broadcast SysLog message send to IPv4 255.255.255.255
1	**PoE port status was changed** – Will be sent whenever PoE port state is changed, such as when PD device is inserted/removed.	New PoE state as per one of the defined states in RFC3621 (searching, delivering power, fault, etc.).	RFC-3621 SNMP PoE MIB , trap equivalent SysLog report
2	PoE power usage exceeds xy% percent out of Power Supply maximum power.	Power usage percentage out of Power Supply maximum power.	RFC-3621 SNMP PoE MIB , trap equivalent SysLog report
3	PoE power usage became less then xy% percent out of Power Supply maximum power.	Power usage percentage out of Power Supply maximum power.	RFC-3621 SNMP PoE MIB , trap equivalent SysLog report
4	**Invalid Web GET** – remote user tried to access the unit over the Web interface with incorrect username/password.	Remote user IPv4/IPv6 address	
5	**Invalid Web POST** – remote user tried to post Web configuration form with incorrect username or password.	Remote user IPv4/IPv6 address	

6	**Default configuration** – Unit was restored to default configuration.		SysLog Server IP is unchanged when restoring unit to factory default,
7	**Unit configuration changed –** will be sent whenever unit configuration was changed.		
9	**PoE controller reset –** will be sent whenever PoE controller reset occurred.		
10	**PoE controller has no firmware –** will be sent in case PoE controller firmware will be erased or become corrupted.		
11	**Invalid Telnet** - remote user tried to access the unit by Telnet with incorrect username/password.	Remote user IPv4/IPv6 address	
12	**DHCPv4** – Will be sent only upon the 1stfirst time DHCPv4 address was obtained either by switching from static to DHCPv4 or on power-up.	• Unit Hostname • Unit MAC Address • DHCPv4 address	Broadcast SysLog message sent to IPv4 255.255.255.255
13	**DHCPv6** – Will be send only upon the 1stfirst time DHCPv6 address was obtained either by switching from static to DHCPv6 or on power-up.	• Unit Hostname • Unit MAC Address • DHCPv6 address	Broadcast SysLog message sent to IPv4 255.255.255.255

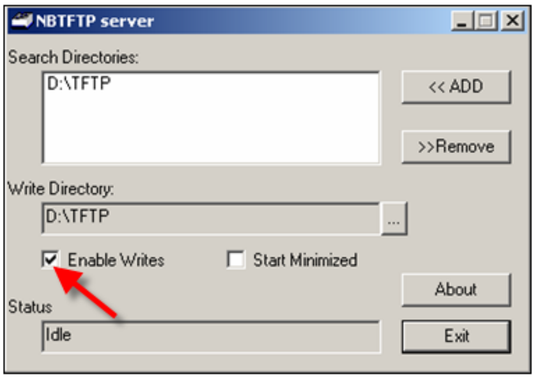
:

7 Upload/Download Unit Configuration over TFTP

7.1 Upload Unit Configuration

Use the following procedure to upload the unit configuration:

1. Activate and run IPv4 or IPv6 TFTP Server (the TFTP Server provided inside the CD supports only IPv4).
2. Verify that the firewall on the computer running TFTP Server is Off, or accepts incoming UDP traffic on port 69.



Search Directories: D:\TFTP

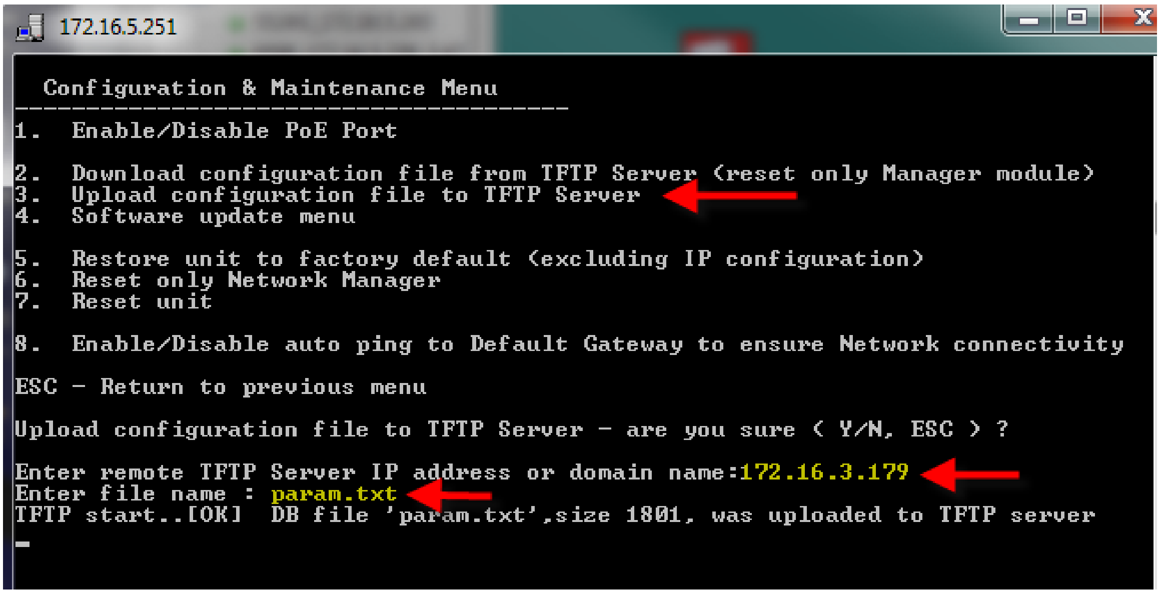
Write Directory: D:\TFTP

☑ Enable Writes ☐ Start Minimized

Status: Idle

Figure 7-1: NBTFTP Server

3. Set TFTP Server root files folder (for example d:\config_files).
4. Enable TFTP Server to write incoming files to its local drive (see Figure 7-1).
5. Open a Telnet session with the unit. Type username and password, and select the configuration menu.



```
 Configuration & Maintenance Menu
---------------------------------------
1.  Enable/Disable PoE Port

2.  Download configuration file from TFTP Server (reset only Manager module)
3.  Upload configuration file to TFTP Server
4.  Software update menu

5.  Restore unit to factory default (excluding IP configuration)
6.  Reset only Network Manager
7.  Reset unit

8.  Enable/Disable auto ping to Default Gateway to ensure Network connectivity

ESC - Return to previous menu

Upload configuration file to TFTP Server - are you sure ( Y/N, ESC ) ?

Enter remote TFTP Server IP address or domain name:172.16.3.179
Enter file name : param.txt
TFTP start..[OK]  DB file 'param.txt',size 1801, was uploaded to TFTP server
_
```

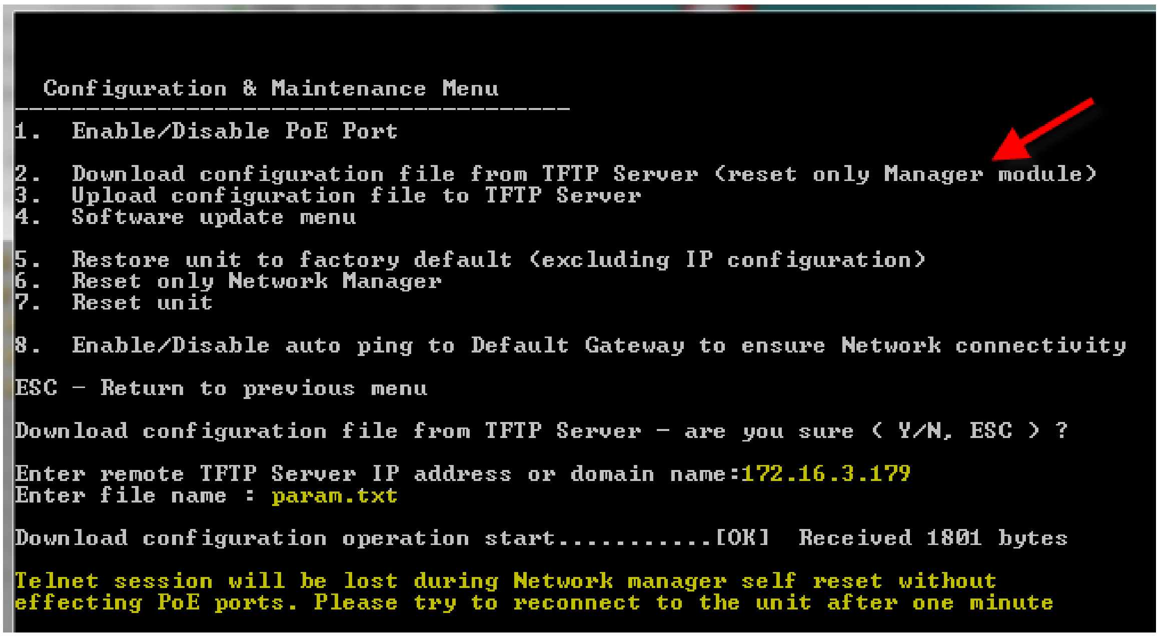
Figure 7-2: Upload Unit Configuration

6. Type the TFTP Server IPv4/IPv6 address, file name (for example param.txt), and press Enter to upload the unit configuration file to TFTP Server root folder.

7.2 Download Unit Configuration

Download unit configuration is very similar to upload unit configuration (see previous section):

1. Configure the TFTP Server as explained in Upload Unit Configuration.
2. Open a Telnet session with the unit (see Upload Unit Configuration), but this time select Download configuration file from TFTP Server.



```
  Configuration & Maintenance Menu
---------------------------------------
1.  Enable/Disable PoE Port

2.  Download configuration file from TFTP Server (reset only Manager module)
3.  Upload configuration file to TFTP Server
4.  Software update menu

5.  Restore unit to factory default (excluding IP configuration)
6.  Reset only Network Manager
7.  Reset unit

8.  Enable/Disable auto ping to Default Gateway to ensure Network connectivity

ESC - Return to previous menu

Download configuration file from TFTP Server - are you sure ( Y/N, ESC ) ?

Enter remote TFTP Server IP address or domain name:172.16.3.179
Enter file name : param.txt

Download configuration operation start...........[OK]  Received 1801 bytes

Telnet session will be lost during Network manager self reset without
effecting PoE ports. Please try to reconnect to the unit after one minute
```

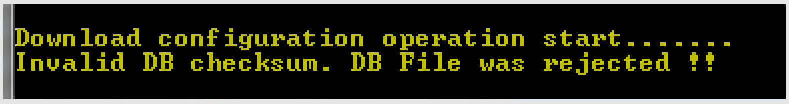
Figure 7-3: Download Unit Configuration

3. Type the TFTP Server IPv4/IPv6 address, file name (for example param.txt), and press Enter to download the unit configuration file from the TFTP Server root folder to the unit itself.

   Upon completion the unit will reset its internal Network Management module leaving PoE power unchanged. Network traffic involving the PoE devices may be interrupted for a few seconds during the time the Network Management Module re-initializes itself with the new configuration values.

NOTE:

1. **Although the configuration file is text-based, please don't try to change it manually. Such changes will be rejected (please see the message below).**



```
Download configuration operation start.......
Invalid DB checksum. DB File was rejected !!
```

2. **For offline configuration changes please contact tech support at customer.care_AMSG@microsemi.com.**

8 Software Upgrade

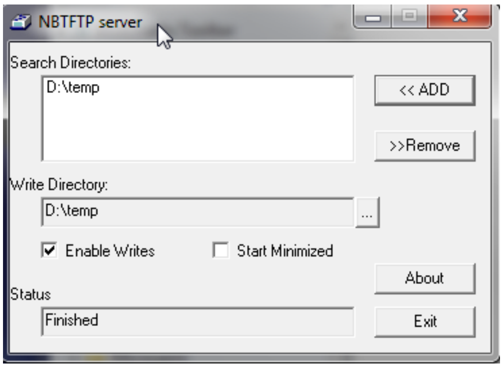
The following section describes how to perform unit software update.

8.1 Network Manager Software Update

The Network Manager provides the graphical (Web), textual (Telnet), SNMP interface between the unit and the remote Network user, excluding PoE functionality which is performed by a dedicated Micro Controller, This allows updating the Network Manager module without affecting active PoE PD devices.

Software update of the network manager interface is done over TFTP in a very similar way to Upload/Download Unit Configuration.

1. Activate and run TFTP Server (provided on the CD or any other TFTP Server).
2. Verify that the firewall on the computer running TFTP Server is Off, or accepts incoming UDP traffic on port 69.



NBTFTP server

Search Directories: D:\temp

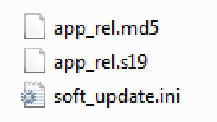
Write Directory: D:\temp

☑ Enable Writes   □ Start Minimized

Status: Finished

Figure 8-1: NBTFTP Server

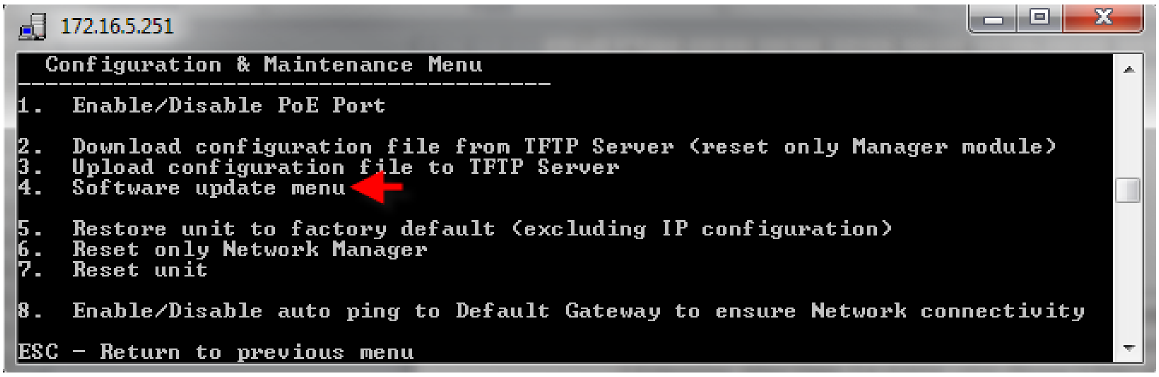
3. Copy the software update files (as in the example below) to TFTP Server root folder (for example d:\temp).



app_rel.md5
app_rel.s19
soft_update.ini

4. Open a Telnet session with the unit. Type the username and password, and select the Configuration and Maintenance Menu.

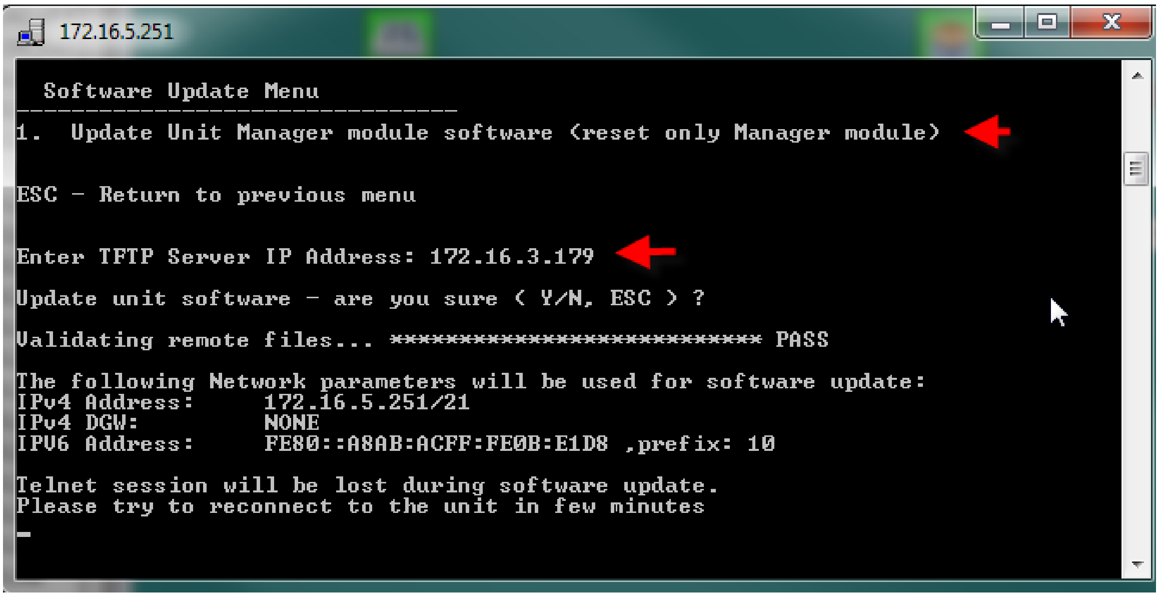
5. Select Software update menu.



```
  Configuration & Maintenance Menu
  ---------------------------------------
1.   Enable/Disable PoE Port

2.   Download configuration file from TFTP Server (reset only Manager module)
3.   Upload configuration file to TFTP Server
4.   Software update menu

5.   Restore unit to factory default (excluding IP configuration)
6.   Reset only Network Manager
7.   Reset unit

8.   Enable/Disable auto ping to Default Gateway to ensure Network connectivity

ESC - Return to previous menu
```

Figure 8-2: Selecting Software Update from the Configuration Menu

6. Select Update Unit Manager module software, and type the TFTP Server IP Address (see image below).



```
  Software Update Menu
  --------------------------------
1.  Update Unit Manager module software (reset only Manager module)


ESC - Return to previous menu


Enter TFTP Server IP Address: 172.16.3.179

Update unit software - are you sure ( Y/N, ESC ) ?

Validating remote files... ****************************** PASS

The following Network parameters will be used for software update:
IPv4 Address:      172.16.5.251/21
IPv4 DGW:          NONE
IPV6 Address:      FE80::A8AB:ACFF:FE0B:E1D8 ,prefix: 10

Telnet session will be lost during software update.
Please try to reconnect to the unit in few minutes
_
```

Figure 8-3: Selecting Software Update from the Configuration Menu

7. The files to be updated will be validated first and only then does the actual software update start. The Telnet session will be lost due to the software update process. However, PoE power will remain during the entire software update process. The same is true for network connectivity between the various switch Ethernet ports. Upon completion of the software update, the unit will send SysLog and SNMP Trap reports.

9 Recovering from Unknown Username, Password

The procedure below describes how to recover from a scenario in which the user is unable to access the unit by Web or Telnet due to unknown unit username or password.

NOTE:

The recovery procedure can be performed only from the user LAN (not over the Internet). User should be able to turn the unit power off when needed. All PoE ports need to be disconnected, and the unit should have only a single active Ethernet link between user's local LAN and the unit.

For username, password recovery over the network, only user PC or laptop having IPv6 Link-Local address as FE80::9C39:DB8b:62DE:7CD4 can be used for the following reasons:

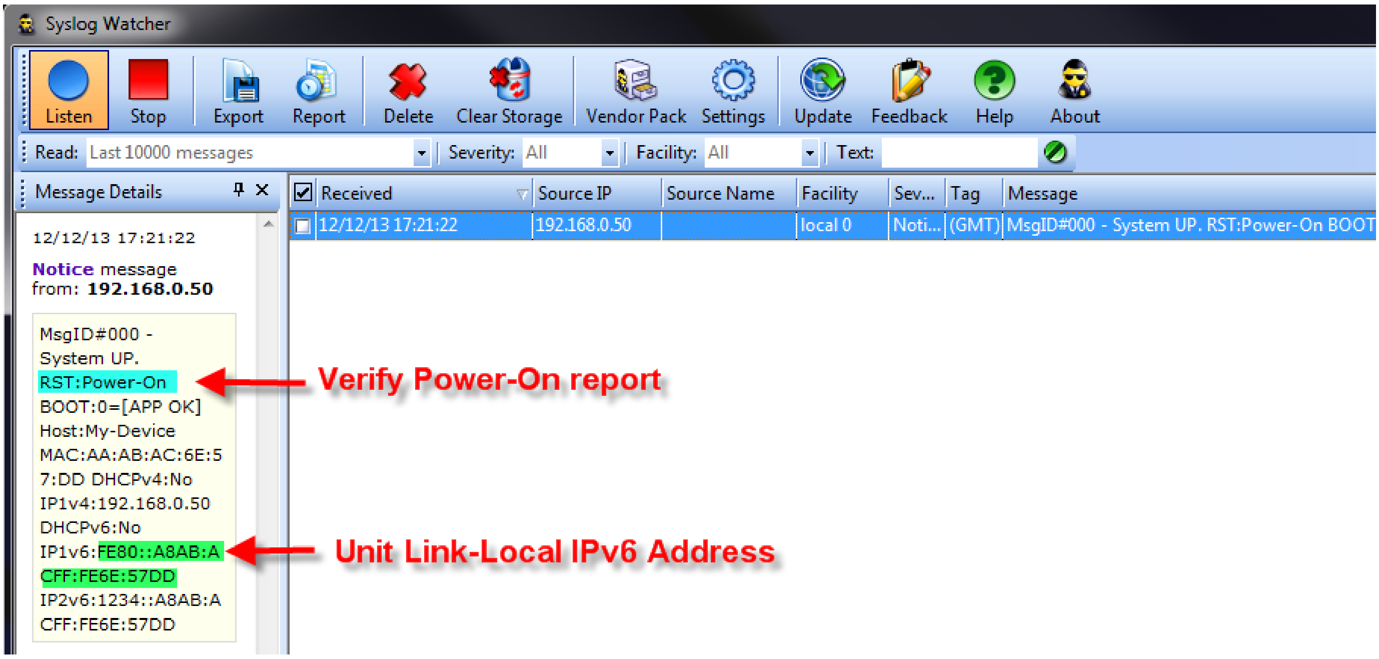
- IPv6 Link-Local is limited to local LAN since it is blocked by all routers, meaning that password recovery can be done only from the local LAN network, and not over the Internet.
- No need to configure laptop or unit IPv6 Link-Local address since it is generated automatically (MAC address-based).

9.1 Summarized Username, Password Recovery Procedure (for Experts)

1. Only one Ethernet link may be up, leaving the other Ethernet ports disconnected.
2. Make sure no PD device is connected, meaning no power is provided to any of the PD devices.
3. Turn unit power Off. Wait 10 seconds or so to make sure the unit is completely off.
4. Apply back power to the unit. And wait around 15 seconds.
5. The entire procedure described below should be done in less than **90** seconds since power was applied to the unit.
6. Connect to the unit Link-Local IPv6 address over Telnet (use the help of SysLog Server in order to find out unit IPv6 Link-Local address). Use ***passwordrecovery*** both as username and password. Trying to access the unit using any other known unit IPv4/IPv6 address will not lead to recovering the unit from unknown username, password.
7. Upon successful login, the user will be given the option to restore the unit to factory default, or cancel. Selecting the restore option will cause the unit to restore itself to factory default and reset itself.
8. After unit reset, the user can regain control over unit configuration by browsing to IPv4 address 192.168.0.50, using the default username ***admin***, and the default password ***password***.

9.2 Detailed Step-by-Step Username, Password Recovery Procedure

1. Please disconnect all except for one Ethernet cable from the unit (only one Ethernet port should be active).
2. Run IPv4 capable SysLog Server on your laptop/PC (make sure the firewall is turned off, or enable UDP port **514** to pass through).
3. Turn the unit off, wait 10 seconds, and turn it back on. A SysLog message similar to the one in Figure 9-1: Find Unit IPv6 Link-Local address from Power-Up SysLog Report below should appear after 15 seconds or so. Please identify unit IPv6 address (IPv6 Link-Local address always starts with FE80).



Received	Source IP	Source Name	Facility	Sev...	Tag	Message
□ 12/12/13 17:21:22	192.168.0.50		local 0	Noti...	(GMT)	MsgID#000 - System UP. RST:Power-On BOOT

12/12/13 17:21:22

Notice message
from: **192.168.0.50**

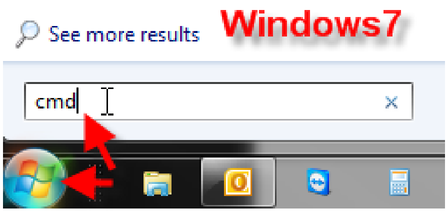
MsgID#000 -
System UP.
RST:Power-On
BOOT:0=[APP OK]
Host:My-Device
MAC:AA:AB:AC:6E:5
7:DD DHCPv4:No
IP1v4:192.168.0.50
DHCPv6:No
IP1v6:FE80::A8AB:A
CFF:FE6E:57DD
IP2v6:1234::A8AB:A
CFF:FE6E:57DD

Verify Power-On report

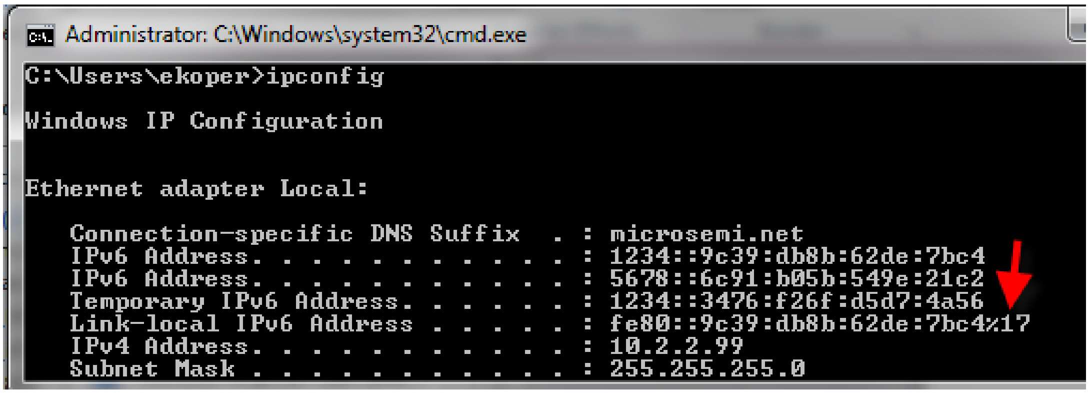
Unit Link-Local IPv6 Address

Figure 9-1: Find Unit IPv6 Link-Local address from Power-Up SysLog Report

4. Open a command window on your Windows7/Windows8 machine
   - For Windows 7 – Click Start and type ***cmd.***
   - For Windows 8 – Press the Windows key + R key, and type ***cmd.***



5. Type ***ipconfig*** to identify the virtual interface index of your IPv6 Link-Local address (%17) in the image below.



```
C:\Users\ekoper>ipconfig

Windows IP Configuration


Ethernet adapter Local:

   Connection-specific DNS Suffix  . : microsemi.net
   IPv6 Address. . . . . . . . . . . : 1234::9c39:db8b:62de:7bc4
   IPv6 Address. . . . . . . . . . . : 5678::6c91:b05b:549e:21c2
   Temporary IPv6 Address. . . . . . : 1234::3476:f26f:d5d7:4a56
   Link-local IPv6 Address . . . . . : fe80::9c39:db8b:62de:7bc4%17
   IPv4 Address. . . . . . . . . . . : 10.2.2.99
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
```

Figure 9-2: Find Unit IPv6 Link Local address from Power-Up SysLog Report

6. Prepare Telnet connection to be opened easily by typing:
Telnet *<unit IPv6 Local-Link Address as reported by SysLog Server><%virtual interface number>*
for example ***telnet FE80::A8AB:ACFF:FE6E:57DD%17*** but **don't** press Enter.

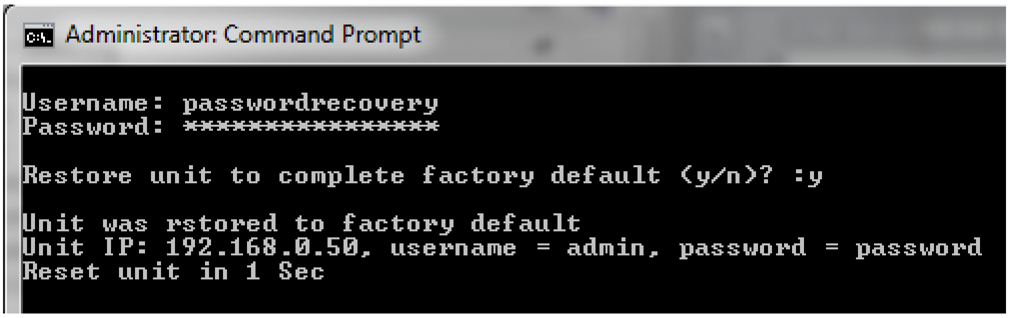
NOTE:

You may need to add Telnet client service to Windows7 and Windows8. Please refer to the following links for detailed instruction on how to add Telnet to Win7/Win8:

Win7: http://technet.microsoft.com/en-us/library/cc771275%28v=ws.10%29.aspx

Win8: http://www.sysprobs.com/install-and-enable-telnet-in-windows-8-use-as-telnet-client

7. Now that everything is ready, turn the unit off, wait 10 seconds, and turn it On. Wait for 15 seconds before pressing Enter to start the Telnet session.
8. Type ***passwordrecovery*** as username and ***passwordrecovery*** as password. A recovery option will be presented to the user. Press 'Y' to restore the unit to factory default configuration, causing the unit to restart with default IPv4 ***192.168.0.50*** and username as ***admin***, and password as ***password***.



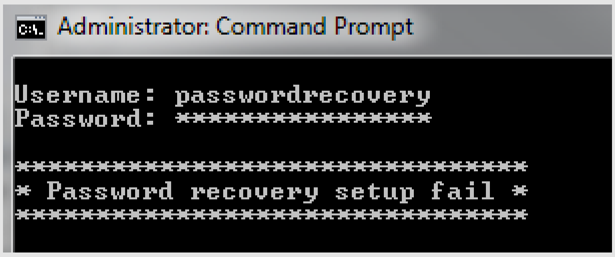
```
Username: passwordrecovery
Password: ****************

Restore unit to complete factory default (y/n)? :y

Unit was rstored to factory default
Unit IP: 192.168.0.50, username = admin, password = password
Reset unit in 1 Sec
```

Figure 9-3: Password Recovery by Restoring the Unit to Factory Default

NOTE:

NOTE1 - The entire recovery process from unit power-on until the username and password were applied must take less than 90 seconds.

NOTE2 - Whenever one of the restrictions isn't meet (for example password was typed after 90 seconds had passed) then the following message will be reported:



```
Username: passwordrecovery
Password: ****************

********************************
* Password recovery setup fail *
********************************
```

10 Troubleshooting

This paragraph provides a symptom and resolution sequence to assist in the troubleshooting of operating problems. If the steps given do not solve your problem, do not hesitate to call your local dealer for further assistance. Refer to Table 10-1.

Table 10-1: Troubleshooting Guide

Symptom	Corrective Steps
Fail to ping the unit IP Address.	1. Verify your PC/Laptop and Unit share the same IP Network. 2. Launch SysLog Server, turn the unit off and back on, and wait for SysLog message to appear reporting IP Address.
Unit can be pinged from a local host but when trying to use the Unit Ping utility, there is no reply.	1. Try to turn off host firewall. 2. If Ping is okay, access the advanced firewall options and enable the Ping option and TFTP (UDP port 69), SNMP Trap ports (UDP port 162).
Software update by TFTP cannot be performed.	1. Use the Unit Ping utility to ping the host running the TFTP Server application. 2. Turn off firewall, or enable UDP port 69. 3. Verify that the appropriate update files package was copied to the TFTP Server root folder.
Log on to unit via Telnet is okay but Telnet session is terminated after a while.	Telnet session is terminated in case no key is pressed and no activity takes place for more than three minutes.
No SNMP Trap events are received.	1. Use the Web browser to view unit configuration and verify the SNMP checkbox is selected. Also, verify the remote SNMP manager IP matches and Trap community string matches the Remote SNMP manager Trap configuration. 2. Turn Off firewall on SNMP manager station, or allow UDP port 162 to pass through it.
SysLog Server IP was set properly, but Log messages are not received.	Turn off host firewall, or allow UDP port 514 to pass through it.
Weekly schedule was properly configured but PoE ports do not turn on/off in accordance with the weekly schedule scheme.	1. Verify NTP Server IP address was configured properly. 2. Verify the Time Zone Offset on the GMT window displays OK. 3. Verify your company's firewall does not block outgoing/incoming NTP packets (UDP Port 123).

Microsemi reserves the right to change the configuration, functionality and performance of its products at anytime without any notice. This product has been subject to limited testing and should not be used in conjunction with life-support or other mission-critical equipment or applications. Microsemi assumes no liability whatsoever, and Microsemi disclaims any express or implied warranty, relating to sale and/or use of Microsemi products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. The product is subject to other terms and conditions which can be located on the web at http://www.microsemi.com/legal/tnc.asp.

Revision History

Revision Level / Date	Para. Affected	Description
0.1	Whole Document	Initial draft
1.0	Whole Document	Final draft, approved by NMS Eng, DE & PJM.

For support contact: customer.care_AMSG@microsemi.com

Visit our web site at: http://www.microsemi.com/powerdsine Catalog Number: PD_NMS_UG

Microsemi Corporate Headquarters
One Enterprise, Aliso Viejo CA 92656 USA
Within the USA: +1(949) 380-6100
Sales: +1 (949) 380-6136
Fax: +1 (949) 215-4996

Microsemi Corporation (NASDAQ: MSCC) offers a comprehensive portfolio of semiconductor solutions for: aerospace, defense and security; enterprise and communications; and industrial and alternative energy markets. Products include high-performance, high-reliability analog and RF devices, mixed signal and RF integrated circuits, customizable SoCs, FPGAs, and complete subsystems. Microsemi is headquartered in Aliso Viejo, Calif. Learn more at **www.microsemi.com**.