

# Microsemi Outdoor PDS-104G PoE Switch

## PowerView Pro

### User Guide



**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.

### Table of Contents

<b>1</b>	<b>ABOUT THIS GUIDE .....</b>	<b>5</b>
1.1	OBJECTIVES .....	5
1.2	AUDIENCE.....	5
1.3	ORGANIZATION.....	6
1.4	CONVENTIONS.....	6
1.5	RELATED DOCUMENTATION.....	6
1.6	ABBREVIATIONS.....	6
<b>2</b>	<b>INTRODUCING THE POWER VIEW PRO (IPV4, IPV6).....</b>	<b>8</b>
2.1	FEATURES .....	8
2.2	SYSTEM NETWORK MANAGEMENT CAPABILITIES .....	9
2.3	ETHERNET SWITCH NETWORK CAPABILITIES.....	9
2.4	POE CAPABILITIES .....	9
2.5	CONFIGURATION OPTIONS.....	9
2.6	SECURITY AND USER AUTHENTICATION .....	9
2.6.1	Web HTTP/HTTPS, Telnet/SSH – Username & Password .....	10
2.6.2	SNMP Security.....	10
2.7	DEFAULT UNIT IP, USERNAME AND PASSWORD.....	10
<b>3</b>	<b>WEB INTERFACE .....</b>	<b>11</b>
3.1	SECURED SSL/TLS WEB INTERFACE – HANDLING CERTIFICATES.....	11
3.2	MAIN WEB PAGE .....	11
3.2.1	Main Web Page - Port Status .....	12
3.2.2	Main Web Page - Unit Status.....	13
3.2.3	Main Web Page – Ports Status/Reset.....	13
3.3	CONFIGURATION WEB PAGE .....	14
3.3.1	First-Time Configuration.....	14
3.3.2	Security Configuration.....	14
3.3.3	Network Configuration .....	15
	Configure unit IPv4, IPv6 and host name parameters.....	15
3.3.4	Network Services Configuration (IPv4/IPv6) .....	16
3.3.5	SNMP Configuration.....	17
3.3.6	PoE Configuration.....	18
3.4	ADVANCED WEB PAGE .....	19
3.4.1	Advanced Web Page – Automatic Weekly Schedule PoE Port Activation .....	19
3.4.2	Advanced Web Page – Automatic Weekly Schedule PoE Port Reset.....	20
3.4.3	Advanced Web Page – Reset Unit Options.....	21
3.5	INFORMATION WEB PAGE .....	22
3.5.1	Information Web Page – IP Address in-use .....	22
3.5.2	Information Web Page – Product Information .....	23
3.5.3	Information Web Page – SFP Module Information .....	24
<b>4</b>	<b>TELNET/SSH SERIAL INTERFACE.....</b>	<b>25</b>
4.1	TELNET/SSH – MAIN MENU .....	25
4.2	TELNET/SSH – VIEW MENU .....	26
4.2.1	Telnet/SSH– View PoE Ports Status .....	26
4.2.2	Telnet/SSH – View Network Parameters.....	27
4.2.3	Telnet/SSH – View Unit Information .....	28
4.3	TELNET/SSH – CONFIGURATION AND MAINTENANCE MENU .....	29
<b>5</b>	<b>SNMP MONITORING AND CONFIGURATION .....</b>	<b>31</b>
5.1	ENABLING SNMP .....	31



---

5.2	SNMP MIBs .....	32
5.3	RFC3621 PoE MIB .....	33
5.4	PRIVATE MIB.....	34
<b>6</b>	<b>SYSLOG MESSAGE REPORT .....</b>	<b>35</b>
6.1	SYSLOG MESSAGE TYPES.....	35
<b>7</b>	<b>UPLOAD/DOWNLOAD UNIT CONFIGURATION OVER TFTP .....</b>	<b>37</b>
7.1	UPLOAD UNIT CONFIGURATION TO TFTP SERVER.....	37
7.2	DOWNLOAD UNIT CONFIGURATION FROM TFTP SERVER.....	38
<b>8</b>	<b>SOFTWARE UPDATE.....</b>	<b>39</b>
8.1	NETWORK MANAGER SOFTWARE UPDATE.....	39
8.1.1	<i>Network Manager Software Update Recovery</i> .....	41
8.2	POE UNIT FIRMWARE SOFTWARE UPDATE.....	41
<b>9</b>	<b>RECOVERING FROM UNKNOWN USERNAME, PASSWORD.....</b>	<b>44</b>
9.1	SUMMARIZED USERNAME, PASSWORD RECOVERY PROCEDURE (FOR EXPERTS) .....	44
9.2	DETAILED STEP-BY-STEP USERNAME, PASSWORD RECOVERY PROCEDURE.....	44
<b>10</b>	<b>TROUBLESHOOTING.....</b>	<b>47</b>

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

- Device list:
  - PDS-104GO/AC/M – The PDS-104GO/AC/M is an outdoor PoE switch that enables connecting four powered devices to the network. The switch will deliver PoE power per device up to 60W (for ports 1,2 and up to 30W for ports 3,4. In addition, it enables remote monitoring and controlling of the status of the devices. The major benefit of the PDS-104GO 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 60 Watts and 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 update
- **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
<b>bold</b>	Keywords and commands
<i>italics</i>	<i>Represents a Web interface item</i>
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
- Technical Note 132: Using RFC3621 PoE MIB with Microsemi Unit.
- RFC3621 SNMP MIB, and private MIB
- Creating Certificate for PDS-104G Secured Web Server

### 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
SSL	Secure Sockets Layer
TLS	Transport Layer Security
MIB	Management Information Base
PD	Powered Device
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol

---

SysLog	System Log
SFP	Fiber interface, small form-factor plug

## 2 Introducing the Power View Pro (IPv4, IPv6)

Microsemi'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 Microsemi products via Web (HTTP/HTTPS) / 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 device.
  - **HTTPS - SSL/TLS:** Secured Web-based friendly configuration interface for managing remote Outdoor Power over Ethernet device.
  - **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
    - Various infrastructure and Network MIB's as IP-MIB, TCP-MIB, UDP-MIB, etc.
  - **Telnet:** Remote terminal over IP Network
  - **SSH:** Remote encrypted terminal over Ethernet Network
- **SysLog Server:** Unit sends various 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.
- Automatic PoE Ports reset 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, Telnet/SSH.

- **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/SSH** – used to view unit PoE and 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

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

## 2.4 PoE Capabilities

The following PoE options are available:

- **Two 4Pair PoE Ports** - Delivers up to 60 watts per port.
- **Two 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 PoE Port Reset** – Automatic PoE Ports reset based on time of day.
- **Weekly Schedule PoE Port Activation** – Automatic activation/deactivation of PoE ports based on time of day (Ethernet data flow for disabled PoE port remains enabled, however no PoE power is being applied).
- **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 (HTTP/HTTPS)
- **SNMPv1/2c/3:** Via an SNMP management application on a remote computer
- **Telnet/SSH:** Via a Telnet/SSH client on a remote computer. Please note that by default the unit is shipped with Telnet enabled and SSH disabled.

### 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 HTTPS/HTTPS, Telnet/SSH, SNMPv2 and SNMPv3 offer different security strength



### 2.6.1 Web HTTP/HTTPS, Telnet/SSH – Username & Password

Web HTTPS/HTTPS, Telnet and SSH 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 sniffing device.
- **SNMP v3:** Resolves SNMPv1/v2 security issues by adding authentication and encryption to layer on top of 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 the 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 Secured SSL/TLS Web interface – handling certificates

Please refer to document ***PDS-104G Web Certificate Management*** for instructions on how to create, sign, and upload self-signed or CA signed certificates to the unit.

#### 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.

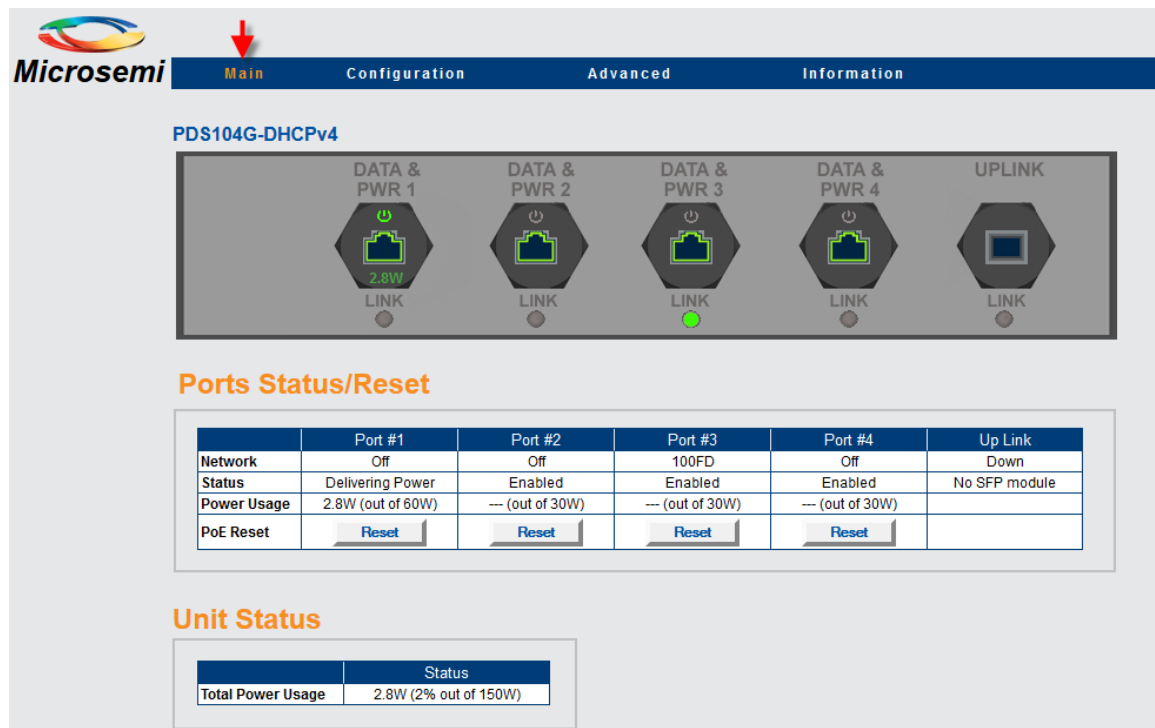


Figure 3-1: Main Web Page













#### NOTE:

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 various possible port states are:

Image	Description	Comments
	<ul style="list-style-type: none"> <li>PoE port is enabled (green line around the RJ45 connector)</li> <li>No PoE power is provided (upper power indicator is off)</li> <li>No Ethernet link (lower link indicator image is gray)</li> </ul>	
	<ul style="list-style-type: none"> <li>PoE port is enabled (green line around the RJ45 connector)</li> <li>No PoE power is provided (upper power indicator is off)</li> <li>Ethernet link is on (low link indicator image is green)</li> </ul>	
	<ul style="list-style-type: none"> <li>PoE port is enabled (green line around the RJ45 connector)</li> <li>PoE power is provided (upper power indicator is on).</li> <li>No Ethernet link (lower link indicator image is gray)</li> </ul>	
	<ul style="list-style-type: none"> <li>PoE port is enabled (green line around the RJ45 connector)</li> <li>PoE power is provided (upper power indicator is on).</li> <li>Ethernet link is on (low link indicator image is green)</li> </ul>	
	<ul style="list-style-type: none"> <li>PoE port is disabled (RJ45 connector marked by two red lines)</li> <li>No Ethernet link (lower link indicator image is gray)</li> </ul> <p>Note – PoE port can be disabled only by Telnet/SSH/SNMP</p>	Ethernet port is enabled even when PoE is disabled (applicable to non-PoE device)
	<ul style="list-style-type: none"> <li>PoE port was enabled by Automatic Weekly Schedule Port Activation functionality (green clock arrows, plus green line around the RJ45 connector)</li> <li>PoE power is provided (upper power indicator is on).</li> <li>Ethernet link is on (low link indicator image is green)</li> </ul>	
	<ul style="list-style-type: none"> <li>PoE port was disabled by <b>Automatic Weekly Schedule Port Activation</b> functionality (yellow clock arrows, plus two red cross lines)</li> <li>No Ethernet link (lower link indicator image is gray)</li> </ul>	Ethernet port is enabled even when PoE is disabled (applicable to non-PoE device)
	<ul style="list-style-type: none"> <li>Up-Link has no SFP module inserted.</li> </ul>	
	<ul style="list-style-type: none"> <li>SFP module is inserted into the Up-Link port</li> <li>No Ethernet link (lower link indicator image is gray)</li> </ul>	
	<ul style="list-style-type: none"> <li>SFP module is inserted into the Up-Link port</li> <li>Fiber Ethernet link is on (lower link indicator image is green)</li> </ul>	

**Figure 3-2: Port Status**

### 3.2.2 Main Web Page - Unit Status

Unit Status	
	Status
Total Power Usage	1.4W (1% out of 150W)

**Figure 3-3: Unit Status**

Unit status reports the aggregated power consumed by all PoE ports and the percentage of the consumed power relative to unit internal Power Supply power capabilities.

### 3.2.3 Main Web Page – Ports Status/Reset

Ports Status/Reset					
	Port #1	Port #2	Port #3	Port #4	Up Link
Network	Off	Off	100FD	Off	Down
Status	Enabled	Enabled	Enabled	Delivering Power	No SFP module
Power Usage	--- (out of 60W)	--- (out of 30W)	--- (out of 30W)	1.4W (out of 30W)	
PoE Reset	<input type="button" value="Reset"/>	<input type="button" value="Reset"/>	<input type="button" value="Reset"/>	<input type="button" value="Reset"/>	

**Figure 3-4: Ports Status/Reset**

- **Network** - reports for each port Ethernet link speed (10/100/1000MB) and if the Network connection is up or down
- **Status** – reports for each port the PoE port status as enabled, disabled, delivering-power, etc.
- **Power Usage** - reports for each port its actual power consumption and the maximum power it can deliver.
- **PoE Reset** - Pressing the Power Reset button turns off the PoE port power for a few seconds and then restores the PoE power back.



#### NOTE:

PoE port which was disabled by Telnet/SSH/SNMP will become enabled whenever **PoE Reset** button is pressed.

### 3.3 Configuration Web Page

This section describes the following topics:

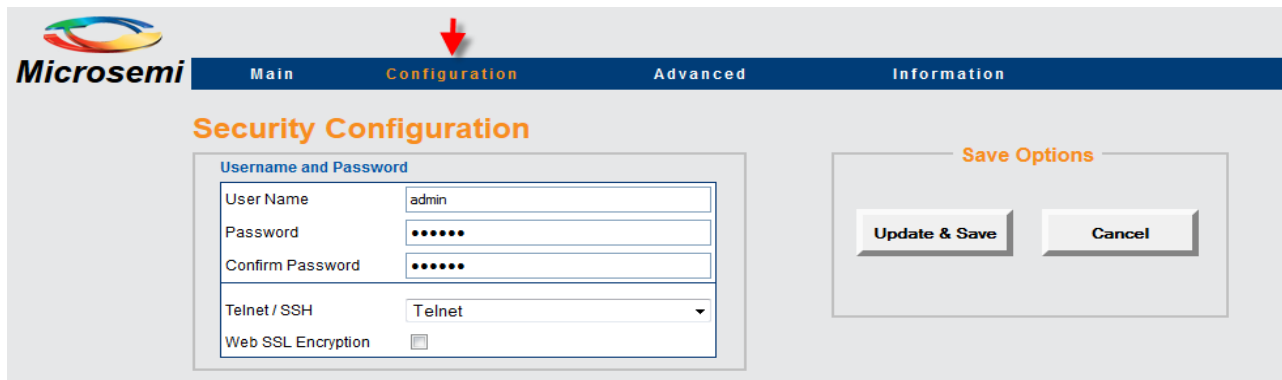
- Unit 1<sup>st</sup> time configuration
- Locating the unit over the local LAN Network whenever unit IP address is unknown
- Configuration Web Page.

#### 3.3.1 First-Time Configuration

Connect your PC/laptop Ethernet network interface (should be configured to IP 192.168.0.40) to any of the unit Ethernet/Fiber 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 than **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**.



**Figure 3-5: Configuration Web Page Option**



#### NOTE:

Unit web interface supports both SSL and TLS web encryption

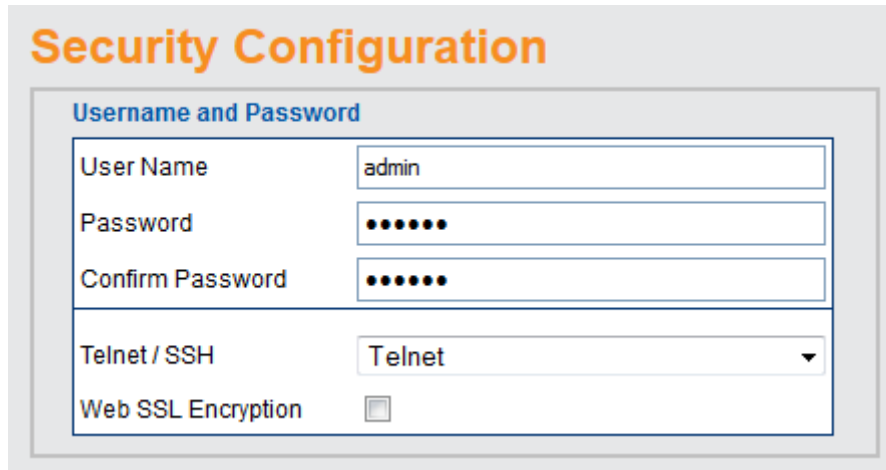
To ease locating the unit over the network, the unit sends an IPv4 SysLog broadcast message advertising its IP address upon power up and the first time an IPv4/IPv6 is obtained from the DHCPv4/DHCPv6 Server (see Figure 3-6).

Hostname	Message
192.168.0.50	Nov 30 00:00:24 My-Device MsgID#000 - System UP. RST:Power-On BOOT:0=[APP OK] Host:My-Device MAC:00:05:5a:03:4b:1c DHCPv4:No IPv4:192.168.0.50/24 DHCPv6:No IP1v6:2345::205:5AFF:FE03:4B1C/64 IP2v6:FE80::205:5AFF:FE03:4B1C/64

**Figure 3-6: Power up SysLog Report – Unit IP, MAC Address, Hostname, and More**

#### 3.3.2 Security Configuration

Configure unit user name and password for remote Web or Telnet/SSH access.



The image shows a web interface titled "Security Configuration". It contains a section titled "Username and Password" with the following fields:

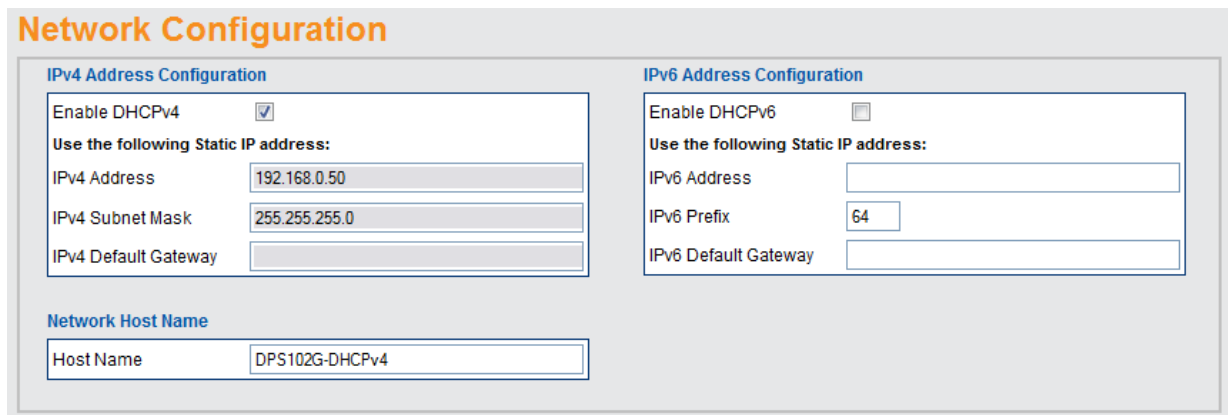
- User Name: admin
- Password: (masked with dots)
- Confirm Password: (masked with dots)
- Telnet / SSH: A dropdown menu with "Telnet" selected.
- Web SSL Encryption: An unchecked checkbox.

**Figure 3-7: Security Configuration**

User Name	Unit user name for remote Web/Telnet/SSH access
Password	Unit password for remote Web/Telnet/SSH access
Telnet/SSH	Enable remote login via Telnet or SSH
Web Encryption	Force all web pages to become encrypted over SSL/TLS

### 3.3.3 Network Configuration

Configure unit IPv4, IPv6 and host name parameters.



The image shows a web interface titled "Network Configuration". It contains two main sections:

- 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: (empty)
- IPv6 Address Configuration:**
  - Enable DHCPv6: ☐
  - Use the following Static IP address:
    - IPv6 Address: (empty)
    - IPv6 Prefix: 64
    - IPv6 Default Gateway: (empty)

Below these sections is a **Network Host Name** section with a field for Host Name containing "DPS102G-DHCPv4".

**Figure 3-8: Network Configuration**

#### 3.3.3.1 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

#### 3.3.3.2 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

### 3.3.3.3 Network Hostname/FQDN

Host name field is used by both 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.

### 3.3.4 Network Services Configuration (IPv4/IPv6)

#### Network Services (IPv4/IPv6)

**Domain Name Servers (DNS)**

DNS #1

192.168.0.30

DNS #2

**Network Time Protocol Server (NTP)**

NTP Server

192.168.0.30

**SysLog Servers**

SysLog Server #1

192.168.0.100

SysLog Server #2

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

GMT Offset: +/-Hour  

+2

GMT Offset: +Minutes  

0

Local Time(OK)  

14:20:21

**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 <b>Automatic Weekly Schedule PoE Port Activation</b> and <b>Automatic Weekly Schedule Port Reset</b> features.
Time Zone Offset	Local time shift from GMT time in hours and minutes.



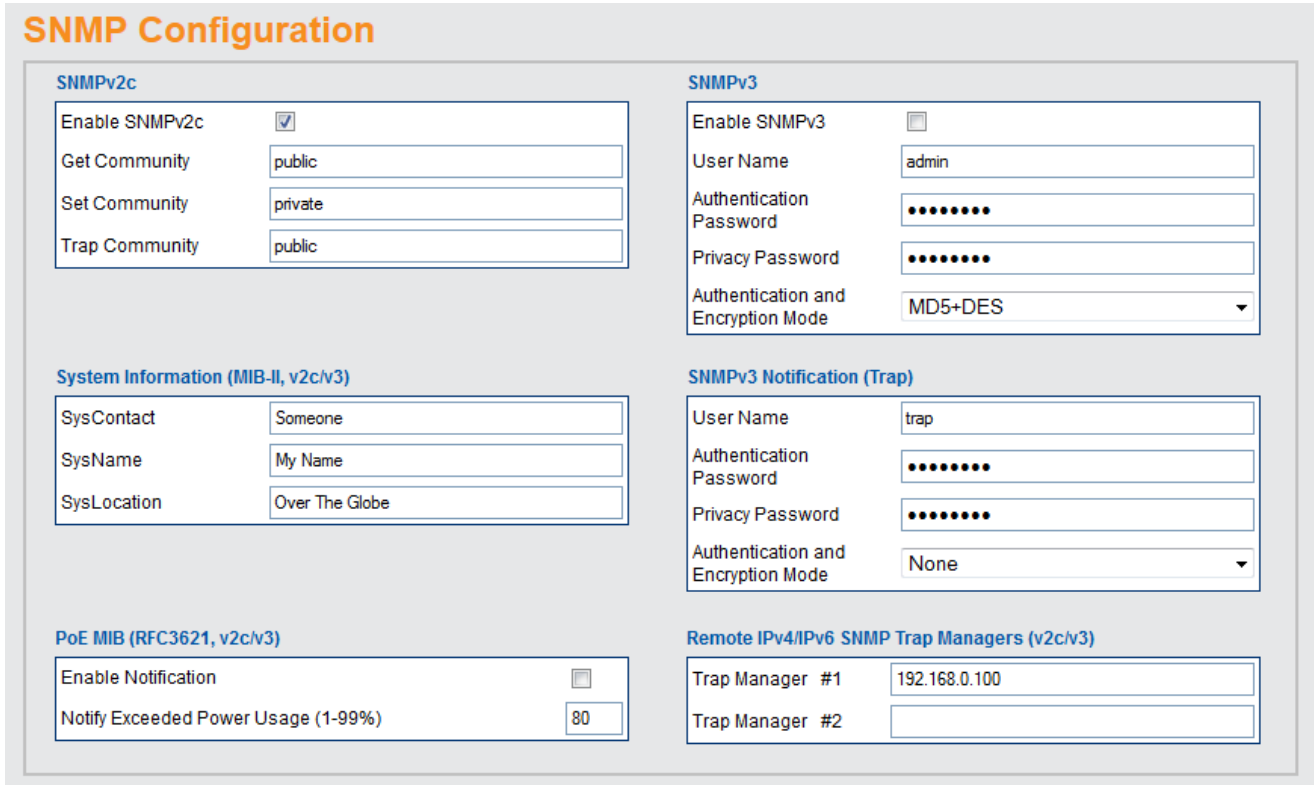
#### NOTE:

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).



### 3.3.5 SNMP Configuration

SNMP configuration refers to various configuration parameters applicable both for SNMPv2c, SNMPv3 or both. The blue title above each SNMP sub parameters group should guide the user if the parameters apply to SNMPv2c, SNMPv3 or both.



The screenshot shows the 'SNMP Configuration' web interface. It is divided into several sections:

- SNMPv2c:** Includes checkboxes for 'Enable SNMPv2c' (checked), and text boxes for 'Get Community' (public), 'Set Community' (private), and 'Trap Community' (public).
- SNMPv3:** Includes checkboxes for 'Enable SNMPv3' (unchecked), text boxes for 'User Name' (admin), 'Authentication Password' (masked), and 'Privacy Password' (masked), and a dropdown for 'Authentication and Encryption Mode' (MD5+DES).
- System Information (MIB-II, v2c/v3):** Includes text boxes for 'SysContact' (Someone), 'SysName' (My Name), and 'SysLocation' (Over The Globe).
- SNMPv3 Notification (Trap):** Includes text boxes for 'User Name' (trap), 'Authentication Password' (masked), and 'Privacy Password' (masked), and a dropdown for 'Authentication and Encryption Mode' (None).
- PoE MIB (RFC3621, v2c/v3):** Includes checkboxes for 'Enable Notification' (unchecked) and a text box for 'Notify Exceeded Power Usage (1-99%)' (80).
- Remote IPv4/IPv6 SNMP Trap Managers (v2c/v3):** Includes text boxes for 'Trap Manager #1' (192.168.0.100) and 'Trap Manager #2' (empty).

**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/AES.

SNMPv3 Authentication and Encryption Mode	<ul style="list-style-type: none"> <li>None – no authentication or encryption (no security - equivalent to SNMPv2).</li> <li>MD5 – MD5 authentication with no encryption (packet can't be changed, however it can easily be analyzed by network sniffers).</li> <li>SHA – SHA authentication with no encryption (similar to MD5, only using different authentication algorithm).</li> <li>MD5+DES – authentication is done by MD5, while encryption is done by DES.</li> <li>SHA+DES – authentication is done by SHA, while encryption is done by DES.</li> <li>MD5+AES – authentication is done by MD5, while encryption is done by AES.</li> <li>SHA + AES – authentication is done by SHA, while encryption is done by AES.</li> </ul>
SNMPv3 Notification (trap) Authentication and Encryption Mode	<ul style="list-style-type: none"> <li>None – no authentication or encryption (no security - equivalent to SNMPv2).</li> <li>MD5 – MD5 authentication with no encryption (packet can't be changed, however it can easily be analyzed by network sniffers).</li> <li>SHA – SHA authentication with no encryption (similar to MD5, only using different authentication algorithm).</li> <li>MD5+DES – authentication is done by MD5, while encryption is done by DES.</li> <li>SHA+DES – authentication is done by SHA, while encryption is done by DES.</li> <li>MD5+AES – authentication is done by MD5, while encryption is done by AES.</li> <li>SHA + AES – authentication is done by SHA, while encryption is done by AES.</li> </ul>
PoE MIB – Enable Notifications	Enable/Disable the following PoE trap reports <ul style="list-style-type: none"> <li>PoE power was provided / removed from PD device.</li> <li>Unit total power consumption exceeds xy% out of max unit power.</li> <li>Unit total power consumption was restored to less than xy% out of max unit power.</li> </ul>
PoE MIB - Notify Exceeded Power Usage (1-99%)	<ul style="list-style-type: none"> <li>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.</li> </ul>

### 3.3.6 PoE Configuration

The user has four PoE power schemes to select from. All four power schemes comply with unit maximum power capabilities.

PoE Configuration				
PoE Port Power				
PoE Power Options	Port #1	Port #2	Port #3	Port #4
In use Power Limit	60[W]	30[W]	30[W]	30[W]
<input checked="" type="radio"/> #1	60[W]	30[W]	30[W]	30[W]
<input type="radio"/> #2	60[W]	60[W]	30[W]	----
<input type="radio"/> #3	60[W]	60[W]	----	30[W]
<input type="radio"/> #4	60[W]	60[W]	15.4[W]	15.4[W]

**Figure 11: PoE Configuration**

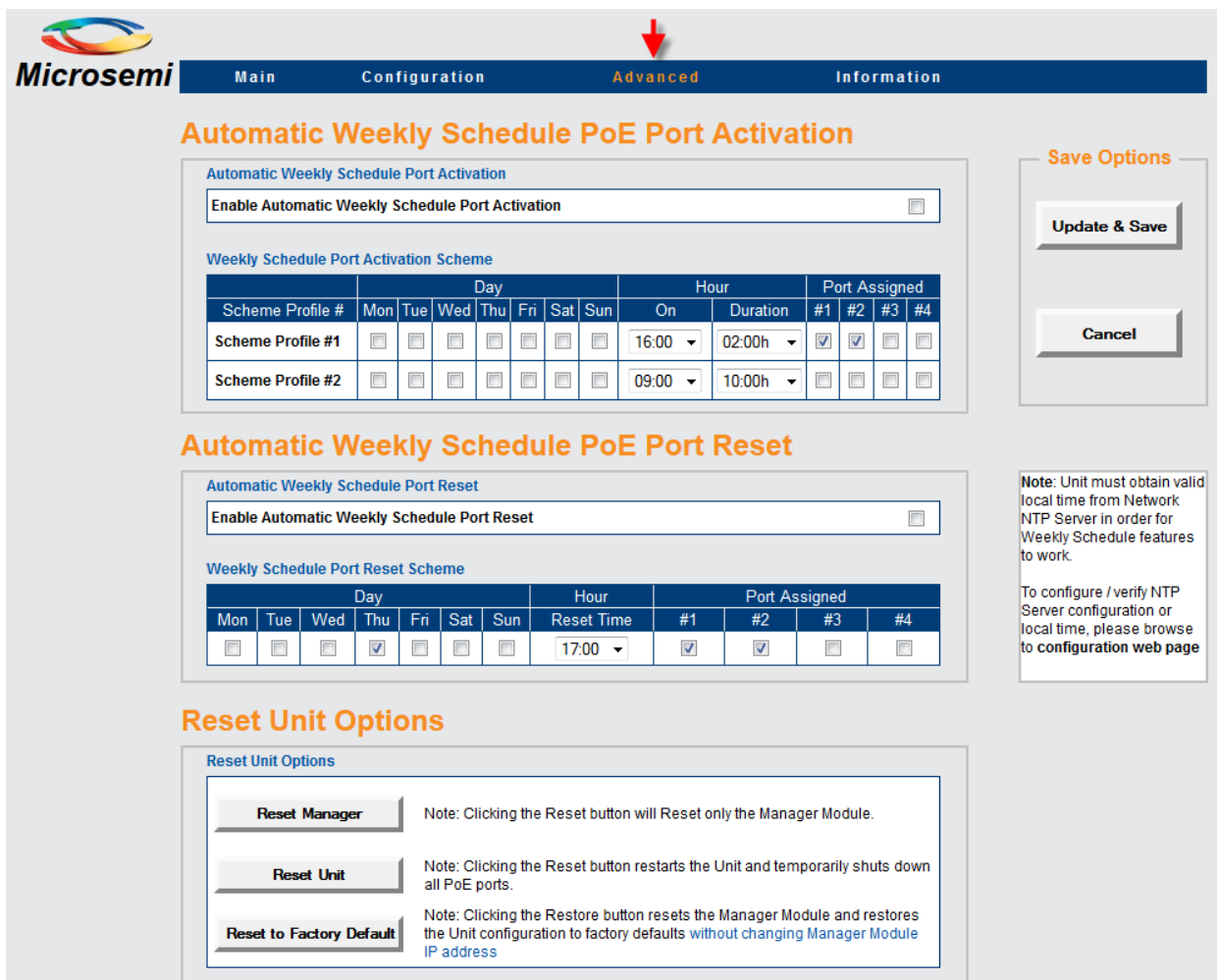
- 60W – deliver power over four pairs inside the Ethernet cable. Each pair delivers up to 30W.
- 30W – deliver power over two out of four pairs inside the Ethernet cable.
- 15.4W – deliver power over two out of four pairs inside the Ethernet cable.

- ---- – No PoE power (Ethernet port is enabled and functional but there are no PoE devices).

### 3.4 Advanced Web Page

Advanced Web page configuration offers the following features to be configured:

- Automatic Weekly Schedule PoE Port Activation (Ethernet port is always enabled)
- Automatic Weekly Schedule PoE Port Reset
- Reset Unit Options
  - Reset Manager – Reset **only the Network Manager** without affecting 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

Scheme Profile #	Day							Hour		Port Assigned			
	Mon	Tue	Wed	Thu	Fri	Sat	Sun	On	Duration	#1	#2	#3	#4
Scheme Profile #1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	16:00	02:00h	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Scheme Profile #2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	09:00	10:00h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**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	#1	#2	#3
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	17:00	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**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](#)

**Save Options**

Update & Save

Cancel

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

Figure 3-12: 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 no 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**

Scheme Profile #	Day							Hour		Port Assigned			
	Mon	Tue	Wed	Thu	Fri	Sat	Sun	On	Duration	#1	#2	#3	#4
Scheme Profile #1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	16:00	02:00h	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Scheme Profile #2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	09:00	10:00h	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 3-13: 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)

0 0 14:34:36

### 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 turning it back 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	#1	#2	#3	#4
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	23:30	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

**Figure 3-14: 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)

### 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 3-15: Reset Unit Options**

- **Reset Manager** – Reset only the internal network manager responsible for unit network management interfaces such as Web (HTTP/HTTPS), Telnet/SSH, 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.

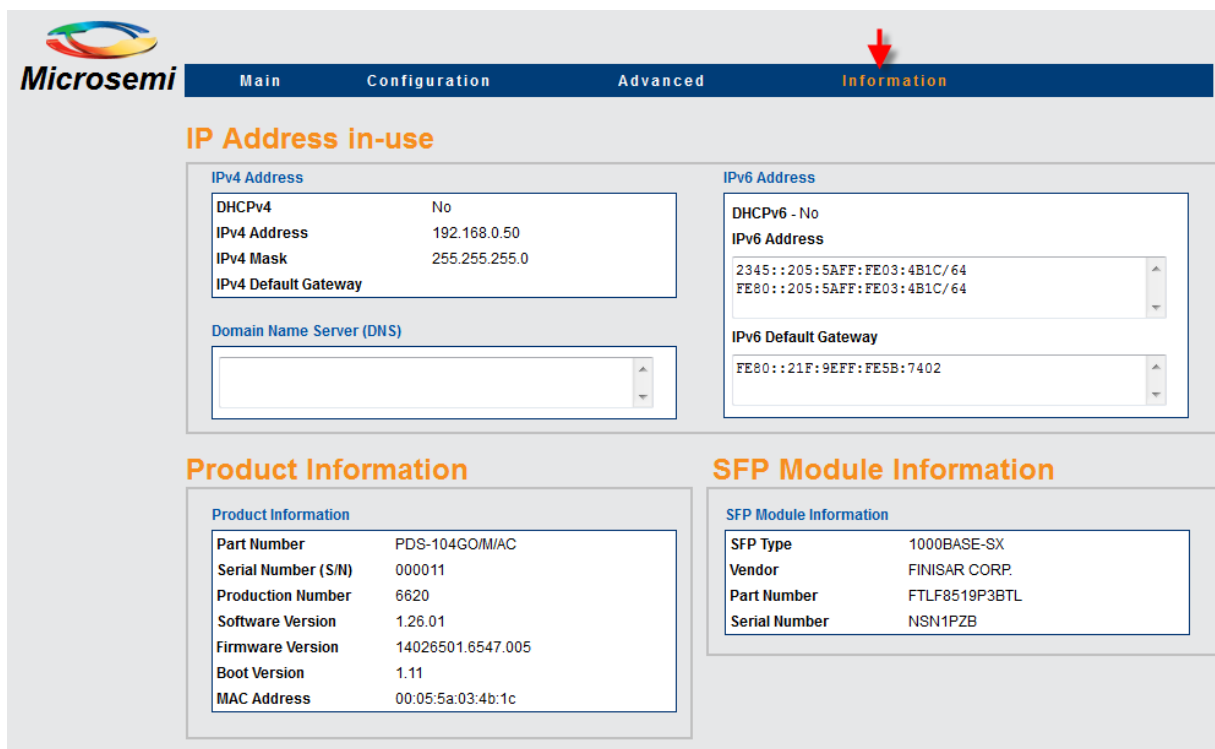
- **Reset Unit** – Reset the entire unit including the internal Network Manager, the PoE controller, and the internal Ethernet Switch.
- **Restore to Factory Default** – Restore unit configuration to factory default, *leaving IPv4/IPv6 network configuration unchanged* (as DHCP/Static IP, IP Address, 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 IP 255.255.255.255 to all SysLog servers 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, SFP module plus miscellaneous product information such as software version, PoE firmware version, etc.



**Microsemi** Main Configuration Advanced **Information**

#### IP Address in-use

**IPv4 Address**

DHCPv4	No
IPv4 Address	192.168.0.50
IPv4 Mask	255.255.255.0
IPv4 Default Gateway	

**IPv6 Address**

DHCPv6 - No	
IPv6 Address	2345::205:5AFF:FE03:4B1C/64 FE80::205:5AFF:FE03:4B1C/64
IPv6 Default Gateway	FE80::21F:9EFF:FE5B:7402

**Domain Name Server (DNS)**

--

#### Product Information

<b>Product Information</b>	
Part Number	PDS-104GO/M/AC
Serial Number (S/N)	000011
Production Number	6620
Software Version	1.26.01
Firmware Version	14026501.6547.005
Boot Version	1.11
MAC Address	00:05:5a:03:4b:1c

#### SFP Module Information

<b>SFP Module Information</b>	
SFP Type	1000BASE-SX
Vendor	FINISAR CORP.
Part Number	FTLF8519P3BTL
Serial Number	NSN1PZB

**Figure 3-16: 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	10.2.2.30
IPv4 Mask	255.255.255.0
IPv4 Default Gateway	10.2.2.10

**Domain Name Server (DNS)**

10.2.2.21  
10.2.2.20

**IPv6 Address**

DHCPv6 - No  
**IPv6 Address**  

1234::212:34FF:FE56:7894/64  
FE80::5678/64  
FE80::212:34FF:FE56:7894/64

**IPv6 Default Gateway**

FE80::21F:9EFF:FE5B:7402

**Figure 3-17: 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: <ul style="list-style-type: none"> <li>Local Link IPv6 address. For example: FE80::A8AB:ACFF:FE6E:57DD</li> <li>Stateless address auto configuration based on Router advertisement report message</li> <li>Static IPv6/DHCPv6 address.</li> </ul>
IPv6 Default Gateway	IPv6 address of the Default Gateway, or static IPv6 default gateway configuration.

#### 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-104GO/MAC
Serial Number (S/N)	000099
Production Number	6620
Software Version	1.15.01
Firmware Version	14026501.6547.005
Boot Version	1.06
MAC Address	00:12:34:56:78:94

**Figure 3-18: Product Information**

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

### 3.5.3 Information Web Page – SFP Module Information

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

### SFP Module Information

#### SFP Module Information

SFP Type	1000BASE-LX
Vendor	FINISAR CORP.
Part Number	FTLF1318P3BTL
Serial Number	PLP3VFF

**Figure 3-19: Product Information**

SFP Type	SFP module type (single-mode, multi-mode, etc.)
Vendor	SFP module vendor name
Part Number	SFP module part number
Serial Number	SFP module serial number



## 4 Telnet/SSH Serial Interface

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

**Telnet:** Provides unsecured unit serial interface over the Network.

**SSH:** Provides secured unit serial interface over the Network.

**NOTE:**

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

### 4.1 Telnet/SSH – Main Menu

```
Main Menu - [My-Device]
-----
1. View Menu
2. Configuration and maintenance menu
3. Ping remote host

E. Exit to debug information screen
```

**Figure 4-1: Telnet/SSH 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 easily identify the unit being accessed over Telnet/SSH (useful especially whenever the user has multiple units), the unit hostname string is shown to the right of the Main Menu title (My-Device in the example above)

## 4.2 Telnet/SSH – View Menu

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

```

View Menu
-----
1. View PoE ports status
2. View network parameters
3. View Unit information
ESC. Return to main menu
  
```

**Figure 4-2: Telnet/SSH View Menu**

### 4.2.1 Telnet/SSH– View PoE Ports Status

View PoE ports status provides Network plus PoE power consumption information for each one of the ports, plus overall power consumption and internal power supply voltage.

```

Port Status
-----
Up Link: DOWN

Port #1: No Power,      Link DOWN,
Port #2: Power=2.8[W],  Link DOWN,
Port #3: No Power,      Link UP,   Speed=10MBit
Port #4: No Power,      Link DOWN,

Total Power : 2.8[W](out of 152[W])
Power Supply: 54.1[V]

ESC - Return to previous menu
  
```

**Figure 4-3: Telnet/SSH View PoE Ports Status**

Network	Reports Ethernet link speed (10/100/1000) and HD/FD connection type
PoE	Power consumption by each PD device
Total Power	Total power consumption of all PDs from all active PoE ports plus maximum available power
Power Supply	Unit internal power supply voltage

### 4.2.2 Telnet/SSH – View Network Parameters

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

```

In Use IPv4 Network Parameters
-----
Use DHCPv4      : No
IP Address      : 192.168.0.50/24
Default Gateway:

In Use IPv6 Network Parameters
-----
Use DHCPv6: No
IP Address:
  2345::205:5AFF:FE03:4B1C/64
  FE80::205:5AFF:FE03:4B1C/64

Default Gateway:
  FE80::21F:9EFF:FE5B:7402

In use DNS network parameters
-----

More network parameters
-----
MAC Address: 00:05:5A:03:4B:1C

ESC - Return to previous menu
  
```

**Figure 4-4: Telnet/SSH View Network Parameters**

In-use IPv4 Network	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 IPv6 default gateway. Please note that IPv6 may report several IPv6 addresses which were obtained automatically in addition to a 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/SSH – 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-104GO/M/AC , Serial Number = 000011, Product Number = 6620
App Ver     = 1.26.01, Creation date & time= Nov 03 2015, 12:52:01
Boot Ver    = 1.11, Creation date & time= Oct 20 2015, 16:06:00
Firmware    = 14026501.6547.005

System Up time   : 1 Days,5 Hours,31 Min,53 Sec
System GMT time  : 05:31:53. Date=Wed,01/12/1999 (D/M/Y) - incorrect
System Local time: 05:31:53. Date=Wed,01/12/1999 (D/M/Y) - incorrect

ESC - Return to previous menu
  
```

**Figure 4-5: Telnet/SSH View Unit Information**

Part Number	Unit marketing part number (PDS-104GO/M/AC)
Serial Number	Unit six-digit serial number
Production Number	Unit production number (for internal use only)
App Ver	Network Manager software version
Boot Version	Network Manager Boot version
Firmware	PoE firmware version which is responsible for PoE functionality
System Up Time	The time passed since the unit was reset/powered up
System GMT time	Unit GMT time as it was obtained from NTP Server. Whenever unit is unable to obtain NTP time from NTP Server, the message "incorrect" will appear
System Local Time	Unit local time (GMT time plus time zone shift). Whenever unit is unable to obtain NTP time from NTP Server, the message "incorrect" will appear

### 4.3 Telnet/SSH – Configuration and Maintenance Menu

Telnet/SSH 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.

```

Configuration and 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. Download WEB SSL Certificate from TFTP Server (reset only Web Server)
5. Software update menu
6. Restore unit to factory default (excluding IP configuration)
7. Reset only Network Manager
8. Reset unit
9. Enable/Disable auto ping to Default Gateway to ensure Network connectivity
ESC. Return to main menu
  
```

**Figure 4-6: Telnet/SSH 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).
Download WEB SSL Certificate from TFTP Server	Download from TFTP Server self-signed or CA signed certificates to the unit to allow secure web browsing to the unit with security confirmation by the Web Browser (green lock in the web browser URL area)
Software update menu	Performs software update the unit internal Network manager or update PoE firmware. Software update is done by downloading the relevant new files from TFTP Server (please refer to Section 8 for more details).  <b>Network Manager updates</b> - during the software update PoE functionality will remain active. However, network traffic may be interrupted for several seconds. <b>PoE Firmware update</b> – PoE functionality will not be available during the firmware update process (around 5-10 minutes)
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.



**Microsemi**

## PDS-104G PoE Switch

### Power Over Ethernet PowerView Pro User Guide

Reset only Network Manager	Reset only the internal Network Manager which is responsible for unit network management interfaces such as Web, Telnet/SSH, 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 Manager, 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.

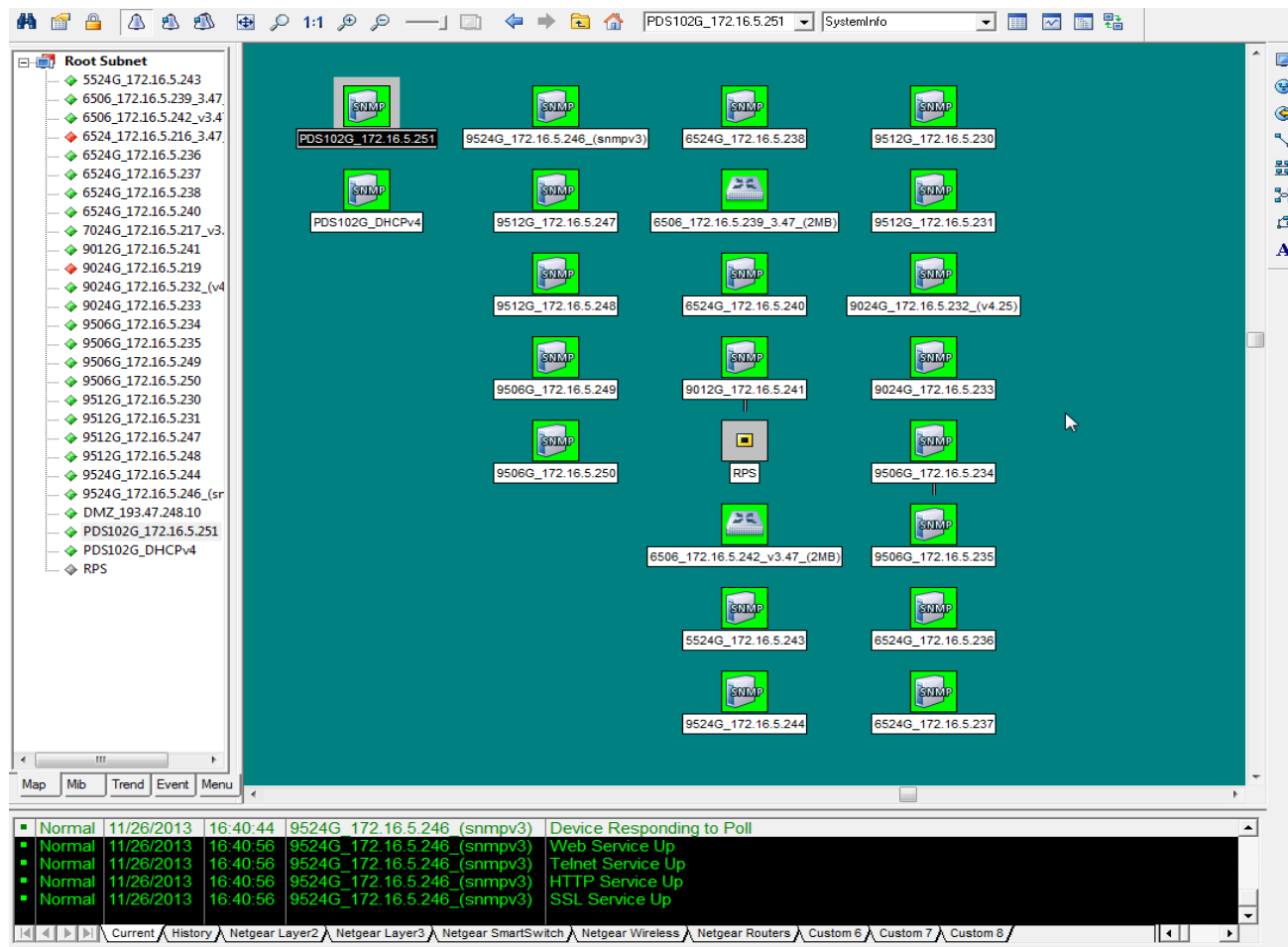


#### NOTE:

To simplify finding the unit over the network, upon power up the unit will send SysLog broadcast messages to IP 255.255.255.255 to all SysLog servers on the Network reporting its IP network configuration parameters, its MAC address, host name, etc

## 5 SNMP Monitoring and Configuration

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



**Figure 5-1: SNMPc Network Management Tool**



### NOTE:

Due to security concerns the unit is shipped with the **SNMPv2/v3 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, the unit will accept and reply to SNMPv1 packets however SNMP traps/notifications 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.

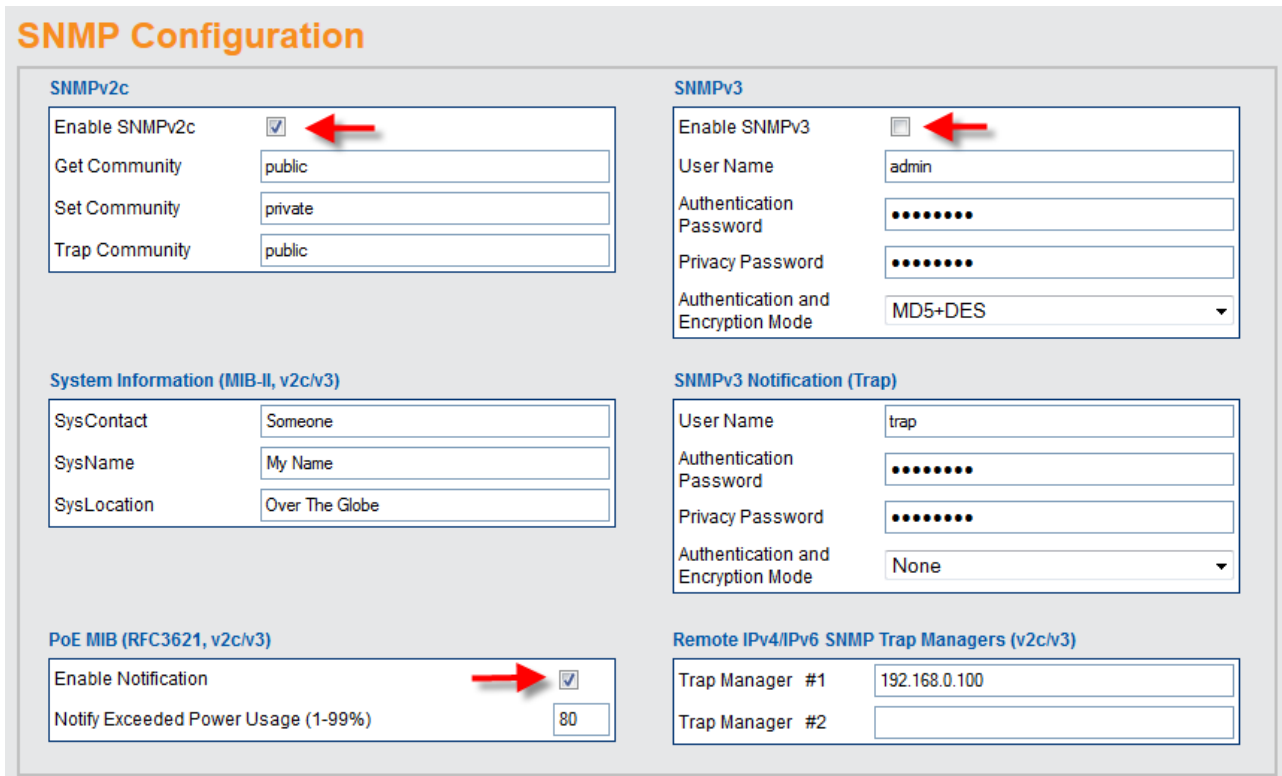


SNMP security parameter	Default value	Comments
Get Community	public	SNMPv2C
Set Community	private	SNMPv2C
Trap Community	public	SNMPv2C Trap
User Name	admin	SNMPv3
Authentication Password	password	SNMPv3
Privacy Password	password	SNMPv3
Authentication and Encryption Mode	MD5+DES	SNMPv3
User Name	trap	SNMPv3 Notification
Authentication Password	password	SNMPv3 Notification
Privacy Password	password	SNMPv3 Notification
Authentication and Encryption Mode	None	SNMPv3 Notification

Table 5-1 Default SNMP usernames and passwords

### 2. Traps:

- To enable traps set remote manager IP address in the **Remote IPv4/IPv6 SNMP Trap Managers** window. For SNMPv3 notifications/traps, make sure notification/trap username, authentication and privacy password and encryption methods match your SNMP manager Trap Manager.
- 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 ☒ (Red arrow)

Get Community: public

Set Community: private

Trap Community: public

**SNMPv3**

Enable SNMPv3 ☐ (Red arrow)

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

**PoE MIB (RFC3621, v2c/v3)**

Enable Notification ☒ (Red arrow)

Notify Exceeded Power Usage (1-99%): 80

**SNMPv3 Notification (Trap)**

User Name: trap

Authentication Password: .....

Privacy Password: .....

Authentication and Encryption Mode: None

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

Trap Manager #1: 192.168.0.100 (Red arrow)

Trap Manager #2:

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

## 5.2 SNMP MIBs

Several MIBs are supported by SNMP manager.





- **Network MIB's:** Various Network MIB's as RFC1213 MIB-II, etc. to be used for providing various Network statistics. Please note that those MIB's are not intended to be used for Network configuration over SNMP.
- **RFC3621:** Power Over Ethernet (PoE) MIB which provides various PoE management capabilities (see Figure 5-4)
- **Private MIB:** Enhance PoE functionality beyond RFC3621 PoE MIB.

Module identity	Root OID	Nodes
IP-MIB	1.3.6.1.2.1.4	301
NOTIFICATION-LOG-MIB	1.3.6.1.2.1.92	61
PDS-PRIVATE-MIB-V1_5	1.3.6.1.4.1.7428	27
POWER-ETHERNET-MIB	1.3.6.1.2.1.105	50
RFC1155-SMI	0	11
RFC1213-MIB	1.3.6.1.2.1	206
SNMP-FRAMEWORK-MIB	1.3.6.1.6.3.10	21
SNMP-MPD-MIB	1.3.6.1.6.3.11	18
SNMP-NOTIFICATION-MIB	1.3.6.1.6.3.13	40
SNMP-USER-BASED-SM-MIB	1.3.6.1.6.3.10.1.1.1	46
SNMPv2-MIB	1.3.6.1.2.1.1	78
SNMP-VIEW-BASED-ACM-MIB	1.3.6.1.6.3.16	44
TCP-MIB	1.3.6.1.2.1.6	57
UDP-MIB	1.3.6.1.2.1.7	37

**Figure 5-3: Unit supported SNMP MIB's**

### 5.3 RFC3621 PoE MIB

**NOTE:**

For a detailed PoE MIB description, please refer to Microsemi's Technical Note – 132, 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 5-4). 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 enables/disables PoE traps to be sent to remote SNMP managers.

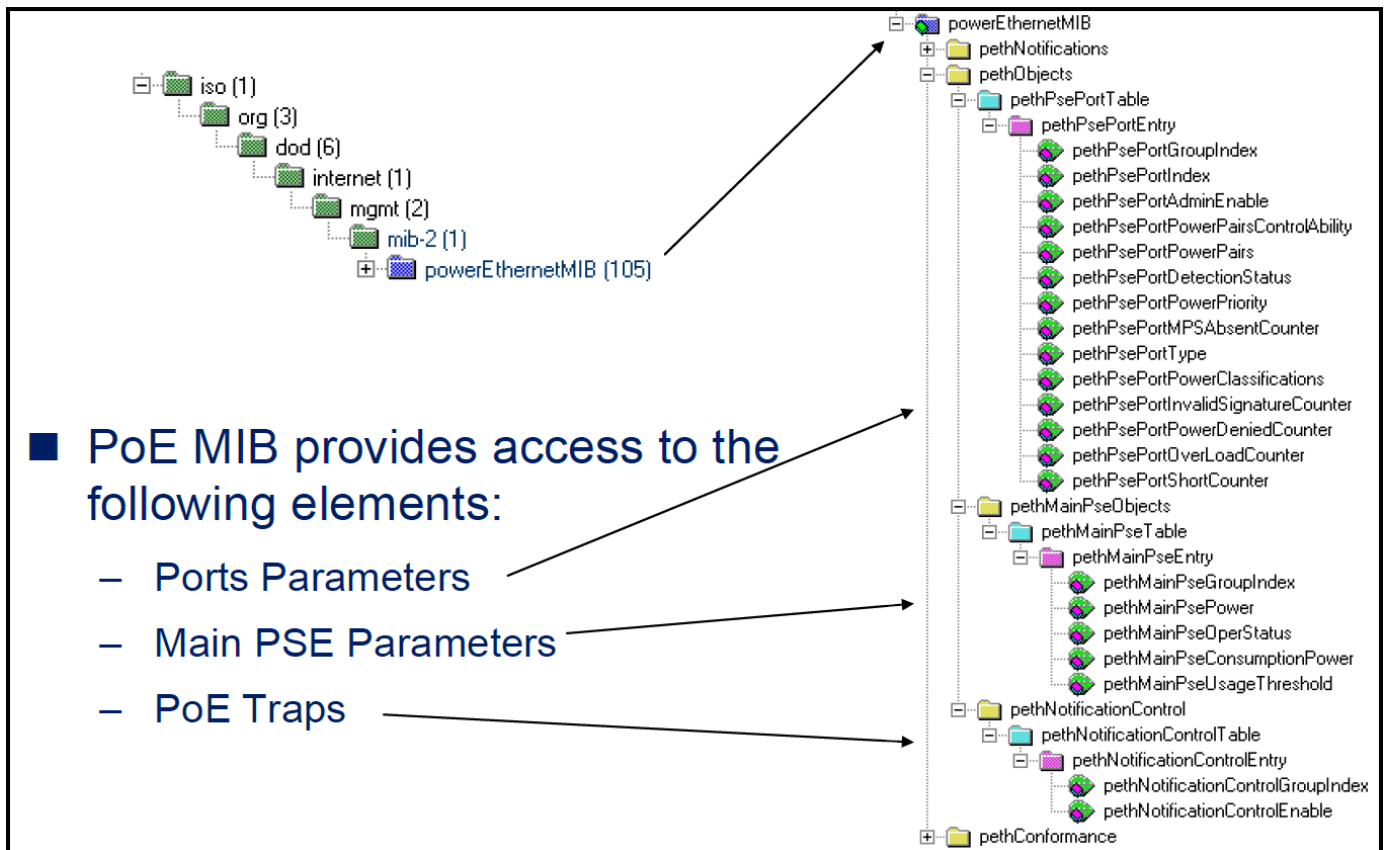


Figure 5-4: MIB Tree Structure

### 5.4 Private MIB

The following SNMP OIDs are supported by the SNMP private MIB

OiD Name	Type (R/W)	Description
poePortConsumptionPower	R	PoE port power consumption [Watt]
poePortMaxPower	R	PoE port maximum available power [Watt]
poePortType	R	PoE port type – Two Pair, 30 [Watt], Four Pair, 60 [Watt]
mainVoltage	R	Unit Power Supply voltage [Volt]

## 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 sent also as SysLog messages, simplifying the readability of such events to the remote user.
- Proprietary SysLog events such as potential security breach whenever remote user tries to access the unit over Web/Telnet/SSH 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:

**Table 2: SysLog Message Types**

Msg ID	Description	Information to be provided	Comments
0	<b>System UP</b> – Will be sent each time power is provided to the unit, or the internal Network Manager resets itself.	<ul style="list-style-type: none"> <li>• Reset cause</li> <li>• Boot status</li> <li>• Unit Hostname</li> <li>• Unit MAC Address</li> <li>• IPv4 Address (static/HDCPv4)</li> <li>• All IPv6 address (static/DHCPv6)</li> </ul>	Broadcast SysLog message send to IPv4 255.255.255.255
1	<b>PoE port status was changed</b> – 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 than 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
6	<b>Default configuration</b> – Unit was restored to default configuration.		SysLog Server IP is unchanged when restoring unit to factory default
7	<b>Unit configuration changed</b> – will be sent whenever unit configuration was changed.		
9	<b>PoE controller reset</b> – will be sent whenever PoE controller reset		



**Microsemi**

## PDS-104G PoE Switch

### Power Over Ethernet PowerView Pro User Guide

	occurred.		
10	<b>PoE controller has no firmware</b> – will be sent in case PoE controller firmware will be erased or become corrupted.		
11	<b>Invalid Telnet Telnet/SSH</b> - remote user tried to access the unit by Telnet Telnet/SSH with incorrect username/password.	Remote user IPv4/IPv6 address	
12	<b>DHCPv4</b> – Will be sent only upon the 1 <sup>st</sup> first time DHCPv4 address was obtained either by switching from static to DHCPv4 or on power-up.	<ul style="list-style-type: none"><li>• Unit Hostname</li><li>• Unit MAC Address</li></ul> DHCPv4 address	Broadcast SysLog message sent to IPv4 255.255.255.255
13	<b>DHCPv6</b> – Will be sent only when the first time DHCPv6 address was obtained either by switching from static to DHCPv6 or on power-up.	<ul style="list-style-type: none"><li>• Unit Hostname</li><li>• Unit MAC Address</li><li>• DHCPv6 address</li></ul>	Broadcast SysLog message sent to IPv4 255.255.255.255

:

## 7 Upload/Download Unit Configuration over TFTP

The unit supports uploading / downloading unit configuration. Below are some typical usage examples:

- Backup unit configuration for later use.
- Configure one unit, and later upload same configuration for additional units
- Modify unit configuration offline and later uploading it to one or more units.



### 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).

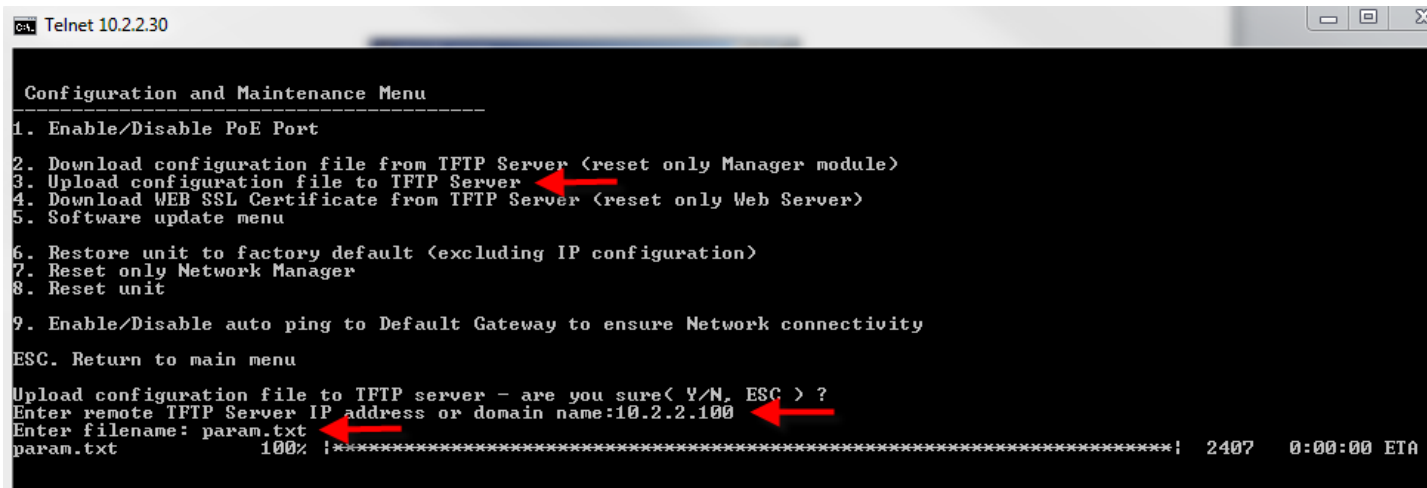
```
Download configuration operation start.....
Invalid DB checksum. DB File was rejected !!
```

2. For offline configuration changes please contact tech support at [poesupport@microsemi.com](mailto:poesupport@microsemi.com).

### 7.1 Upload Unit Configuration to TFTP Server

Use the following procedure to upload the unit configuration:

1. Activate and run IPv4 or IPv6 TFTP Server
2. Verify that the firewall on the computer running TFTP Server is off, or accepts incoming UDP traffic on port #69.
3. Set TFTP Server root files folder (for example d:\config\_files).
4. Enable TFTP Server to write incoming files to its local drive.
5. Open a Telnet/SSH session with the unit. Type username and password, and select the configuration menu.



```

C:\> Telnet 10.2.2.30

Configuration and 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. Download WEB SSL Certificate from TFTP Server <reset only Web Server>
5. Software update menu
6. Restore unit to factory default <excluding IP configuration>
7. Reset only Network Manager
8. Reset unit
9. Enable/Disable auto ping to Default Gateway to ensure Network connectivity
ESC. Return to main menu

Upload configuration file to TFTP server - are you sure( Y/N, ESC ) ?
Enter remote TFTP Server IP address or domain name:10.2.2.100
Enter filename: param.txt
param.txt 100% !*****! 2407 0:00:00 ETA
  
```

**Figure 7-1: 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 from TFTP Server

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

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

```
Configuration and 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. Download WEB SSL Certificate from TFTP Server <reset only Web Server>
5. Software update menu
6. Restore unit to factory default <excluding IP configuration>
7. Reset only Network Manager
8. Reset unit
9. Enable/Disable auto ping to Default Gateway to ensure Network connectivity
ESC. Return to main menu

Download configuration file from TFTP server - are you sure( Y/N. ESC ) ?
Enter remote TFTP Server IP address or domain name:10.2.2.100
Enter filename: param.txt
param.txt 100% !*****! 2407 0:00:00 ETA
Downloading configuration operation start... [OK]
Downloaded file successfully. Manager will now reset.
During reset connection will be lost without affecting POE ports.
Please try to reconnect in one minute
Rebooting

Connection to host lost.
```

Figure 7-2: 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.

## 8 Software Update

The following section describes how to perform unit software update. Two software update options are available:

- **Network Manager Software Update** – Update the software responsible for unit management over the Network as Web, SNMP, Telnet/SSH, etc. Typically, such software update should have no or minimal effect on PoE functionality.
- **PoE Firmware Software Update** – Update the firmware responsible for the actual PoE functionality, having nothing with Network management of Network functionality capabilities.

**NOTE:**

Please note that PoE firmware is very rarely updated

Please contact tech support [poesupport@microsemi.com](mailto:poesupport@microsemi.com) prior trying to update PoE firmware

### 8.1 Network Manager Software Update

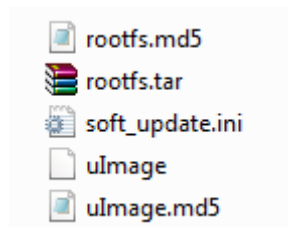
The Network Manager provides the graphical (Web), textual (Telnet/SSH), SNMP interface between the unit and the remote Network user, excluding PoE functionality which is performed by a dedicated Micro Controller, This allows updating the Network Manager module without affecting active PoE PD devices.

**NOTE:**

Please don't turn unit power off during the software update process. In case of Power loss during software update causing the unit to become unmanageable, please refer to following section describing how to recover from such an event.

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.
2. Verify that the firewall on the computer running TFTP Server is Off, or accepts incoming UDP traffic on port 69.
3. Copy the software update files (similar to the example below) to TFTP Server root folder (for example d:\temp).



4. Open a Telnet/SSH session with the unit. Type the username and password, and select the Configuration and Maintenance Menu.
5. Select Software update menu.

```

C:\ Telnet 10.2.2.30

Configuration and 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. Download WEB SSL Certificate from TFTP Server (reset only Web Server)
5. Software update menu
6. Restore unit to factory default (excluding IP configuration)
7. Reset only Network Manager
8. Reset unit
9. Enable/Disable auto ping to Default Gateway to ensure Network connectivity
ESC. Return to main menu
  
```

Figure 8-1: 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)
2. Update Unit PoE Firmware (reset unit)
ESC. Return to configuration menu
Enter TFTP server IP address: 10.2.2.100
Update unit software - are you sure( Y/N, ESC ) ?

soft_update.ini      100% |*****| 124  0:00:00 ETA
rootfs.md5           100% |*****| 33  0:00:00 ETA
rootfs.tar            100% |*****| 33480k 0:00:00 ETA
uImage.md5            100% |*****| 33  0:00:00 ETA
uImage               100% |*****| 1735k 0:00:00 ETA
PASS

The following Network parameters will be used for software update:
IPv4 Address: 10.2.2.30/24
IPv4 DGW: 10.2.2.10
IPv6 Address: 1234::212:34FF:FE56:7894/64
IPv6 DGW: FE80::21F:9EFF:FE5B:7402

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

/dev/mem opened.
Memory mapped at address 0x40006000.
Value at address 0x7F00000 (0x40006000): 0xAAAA
Written 0xFF00; readback 0xFF00
Rebooting
  
```

Figure 8-2: Selecting Update Unit Manager Module Software from the Software Update Menu

7. The files to be updated will be validated first and only then does the actual software update starts. The Telnet/SSH session will be lost during 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.



**NOTE:**

Software update takes up to 10 minutes so please be patient. During this time you will be able only to ping the unit. Upon successful software update, the unit will send SysLog IP broadcast 255.255.255.255 to all SysLog servers located on same LAN, reporting its in use IP, MAC Address, etc.



### 8.1.1 Network Manager Software Update Recovery

This section is applicable whenever unit power was lost during software update exactly whenever new software was being written to the unit internal FLASH, causing the unit to become unmanageable over the Network while PoE continues to work OK (unmanaged PoE Switch device).

The software update functionality is independent from the Network Manager software, meaning that even upon software update failure and corruption due to unexpected power loss, the unit will still be able to recover by itself by initiating by itself one of the two software update recovery procedures:

#### 8.1.1.1 Software update recovery procedure #1 - same remote TFTP Server:

Upon power being restored the Unit will re initiate by itself after around one minute software update from the same remote TFTP Server as it was instructed before power was lost. Upon successful self-initiated software update completion, the unit will become manageable again. The entire recovery process should take less than 10 minutes.

#### 8.1.1.2 Software update recovery procedure #2 - remote TFTP Server 192.168.0.50:

In case unit fail to re initiate software update from remote TFTP Server as it was instructed prior power loss (for example TFTP Server IP is no longer valid, or unit was disconnected from the Network and moved to local LAN Network), the unit will initiate by itself recovery procedure by trying to perform software update from TFTP Server IP address 192.168.0.40 while assigning to itself IP address 192.168.0.50 regardless to the IPv4 address it was configured before power loss. Upon successful software update recovery, the unit will re assign to itself the IPv4/v6 address it was configured prior software update procedure, and become manageable using same IP address as before.

## 8.2 PoE Unit firmware software Update

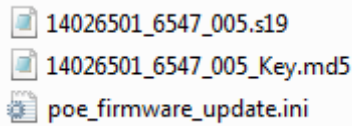
PoE firmware is responsible for the actual PoE functionality of delivering PoE power, making sure that PD device complies with PoE requirements, monitor PD power consumption, etc.

**NOTE:**

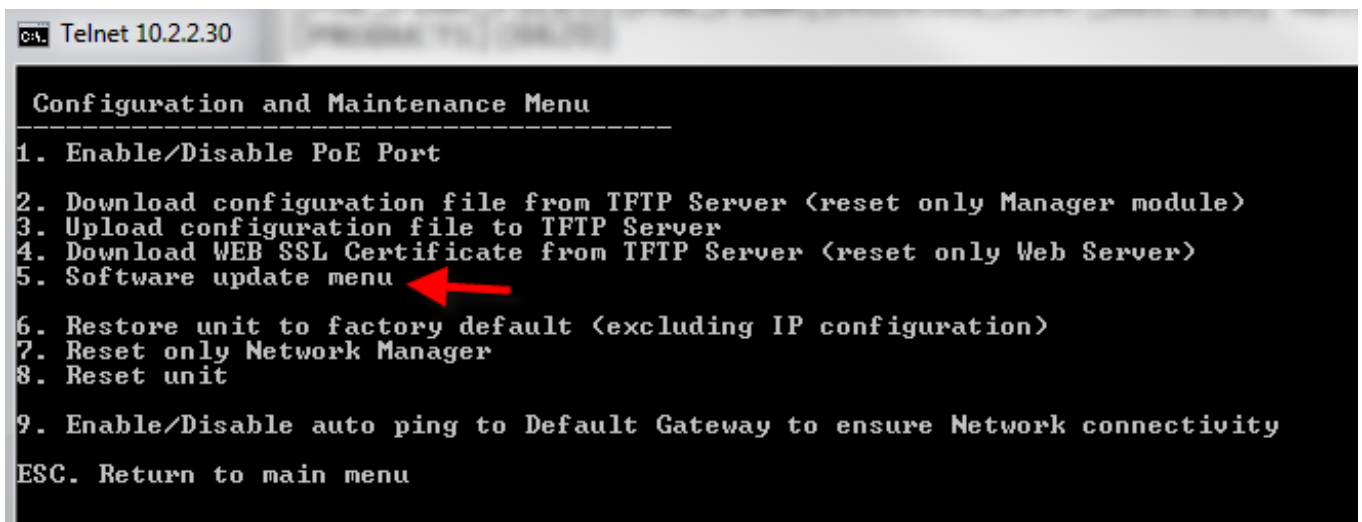
**PoE firmware rarely has to be updated. Please make sure you need to perform PoE firmware update rather than Network Manager software update.**

PoE Firmware update via TFTP is very similar to Upload/Download Unit Configuration.

1. Activate and run TFTP Server.
2. Verify that the firewall on the computer running TFTP Server is Off, or accepts incoming UDP traffic on port 69.
3. Copy the new PoE firmware files (as in the example below) to TFTP Server root folder (for example d:\temp).

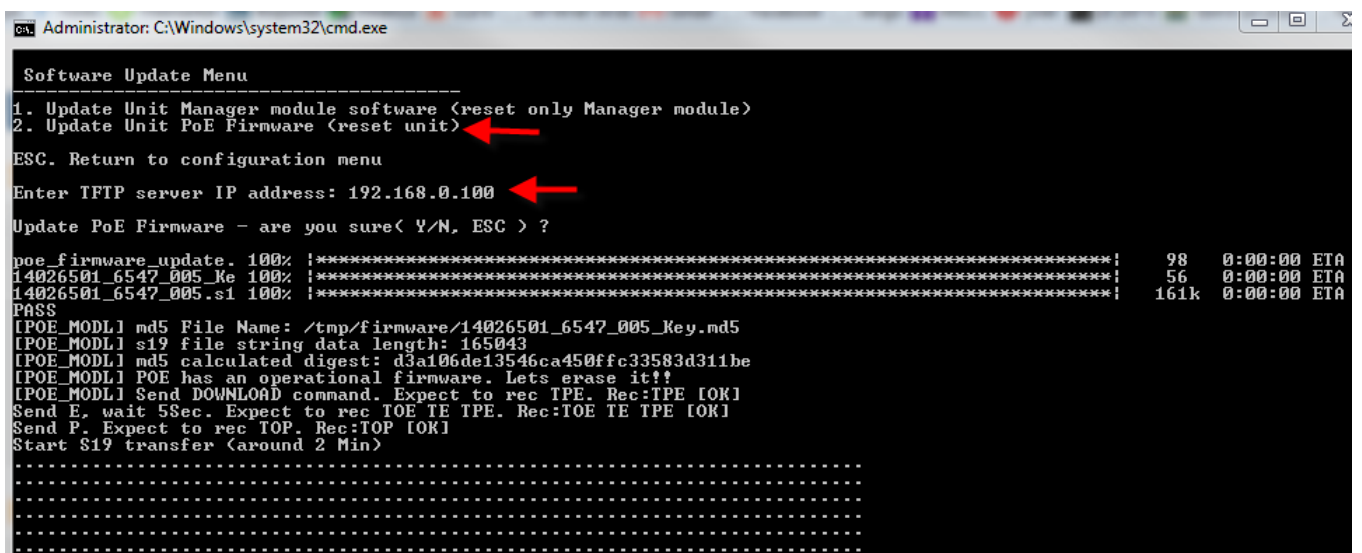


4. Open a Telnet/SSH session with the unit. Type the username and password, and select the Configuration and Maintenance Menu.
5. Select Software update menu.



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

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



**Figure 8-4: Selecting PoE Firmware Update from Software Update Menu**

7. The files to be updated will be validated first and only then does the actual software update start. The Telnet/SSH session will remain open during the entire PoE firmware update process. Upon completion



**Microsemi**

## **PDS-104G PoE Switch**

### **Power Over Ethernet PowerView Pro User Guide**

---

of the firmware update, the unit will reset itself, re power PD devices and 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/SSH due to unknown unit username or password.

### NOTE:



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

For security concerns - username, password recovery can be performed only from Unit local LAN using unit IPv6 Link-Local address as FE80::9C39:DB8b:62DE:7CD4:

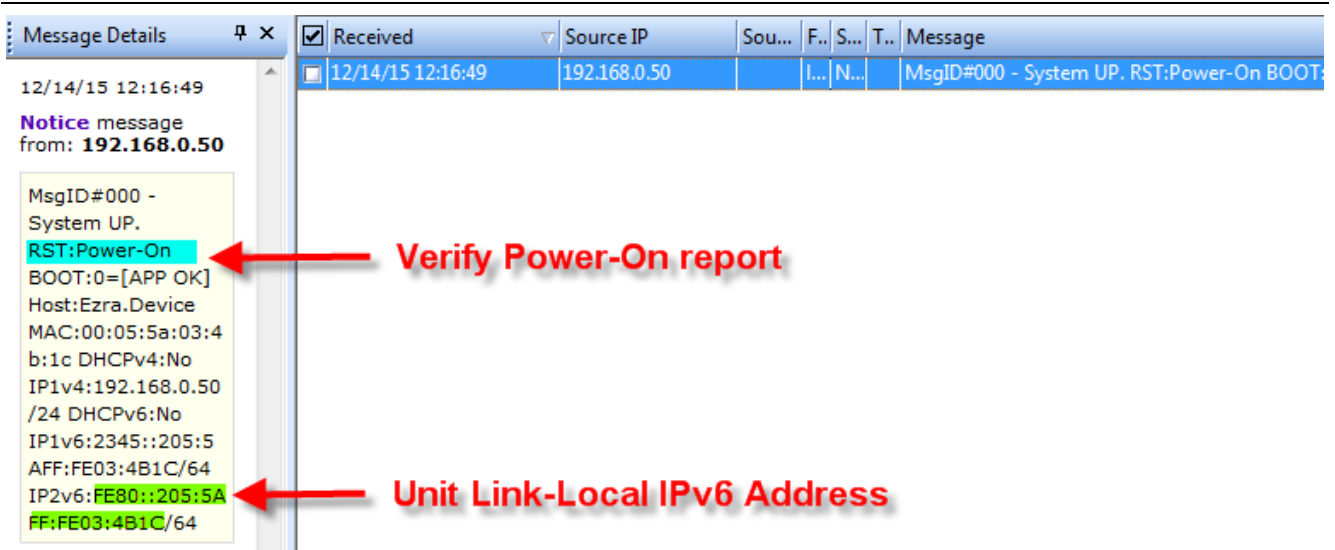
- IPv6 Link-Local is limited to local LAN since it is blocked by all routers, meaning that password recovery can be done only from the local LAN network, and not over the Internet or from remote IP Network.
- No need to configure laptop or unit IPv6 Link-Local address since it is generated automatically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

### 9.1 Summarized Username, Password Recovery Procedure (for Experts)

1. **Only one unit Ethernet link** may be up, leaving the other Ethernet ports disconnected.
2. **No PD device** is connected, meaning no power is provided by the unit to PD device.
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 30** seconds.
5. The entire procedure described below should be done in **less than 120** seconds since power was applied to the unit.
6. Connect to the unit Link-Local IPv6 address over **Telnet over TCP port 2525** (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 *complete factory default including all unit Network configuration* parameters, or cancel. Selecting the restore option will cause the unit to *restore completely to factory default parameters including all unit Network configuration* parameters.
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

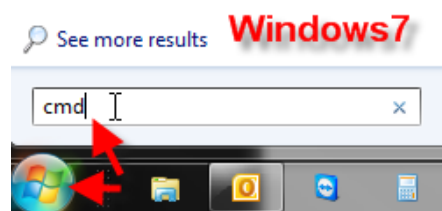
1. Please disconnect from the unit all except for one Ethernet cable (only one Ethernet port should be active).
2. Run IPv4 capable SysLog Server on your laptop/PC (make sure the firewall is turned off, or enable UDP port **514** to pass through).
3. Turn the unit off, wait 10 seconds, and turn it back 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).



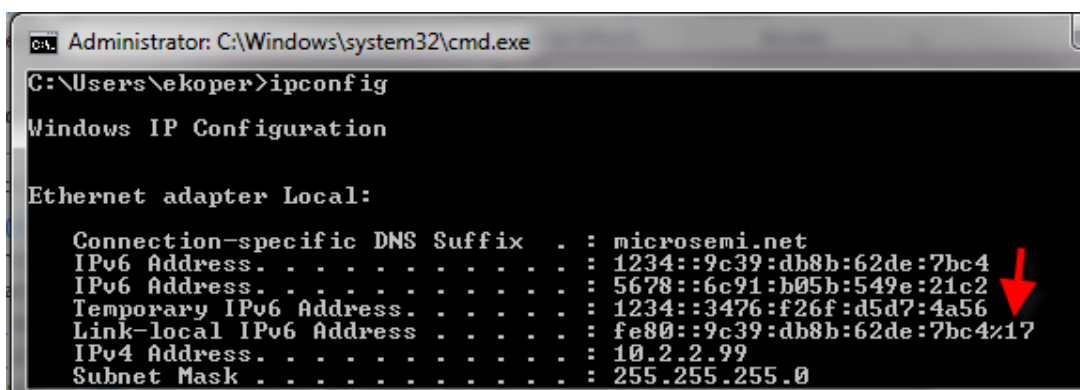
**Figure 9-1: Find Unit IPv6 Link-Local address from Power-Up SysLog Report**

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, type **cmd**.



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



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

6. Prepare Telnet/SSH 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 2525** but don't press Enter.

### NOTE:

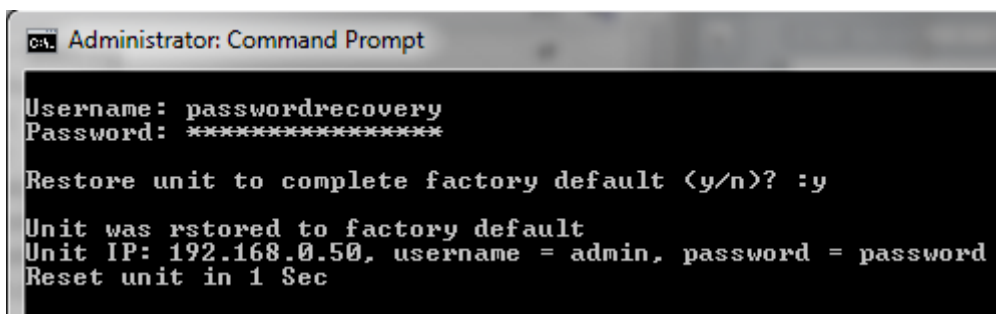


You may need to add Telnet client service to Windows7 or Windows8,10. Please refer to the following links for detailed instruction on how to add Telnet to Win7/Win8:

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 30 seconds before pressing Enter to start the **Telnet session on TCP port 2525**. Please note that the time window for password recovery is limited to 120 Sec since power up.
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 complete factory default configuration including unit Network configuration, causing the unit to restart with default IPv4 **192.168.0.50** and username as **admin**, and password as **password**.



```

Administrator: Command Prompt

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
  
```

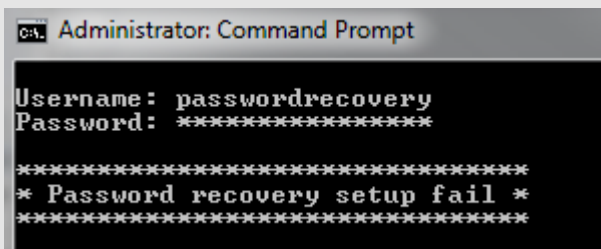
Figure 9-3: Password Recovery by Restoring the Unit to Factory Default

### NOTE:



**NOTE1** - The entire recovery process from unit power-on until the username and password was applied using Telnet TCP port 2525 must take less than 120 seconds.

**NOTE2** - Whenever one of the restrictions isn't met (for example password was typed after 120 seconds had passed) then the following message will be reported:



```

Administrator: Command Prompt

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

*****
* 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.	<ol style="list-style-type: none"> <li>1. Verify your PC/Laptop and Unit share the same IP Network.</li> <li>2. Launch SysLog Server, turn the unit off and back on, and wait for SysLog message to appear reporting IP Address.</li> </ol>
Unit can be pinged from a local host but when trying to use the Unit Ping utility, there is no reply.	<ol style="list-style-type: none"> <li>1. Try to turn off host firewall.</li> <li>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).</li> </ol>
Software update by TFTP cannot be performed.	<ol style="list-style-type: none"> <li>1. Use the Unit Ping utility to ping the host running the TFTP Server application.</li> <li>2. Turn off firewall, or enable UDP port 69.</li> <li>3. Verify that the appropriate update files package was copied to the TFTP Server root folder.</li> </ol>
Log on to unit via Telnet/SSH is okay but Telnet/SSH session is terminated after a while.	Telnet/SSH 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.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Turn Off firewall on SNMP manager station, or allow UDP port 162 to pass through it.</li> </ol>
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.	<ol style="list-style-type: none"> <li>1. Verify NTP Server IP address was configured properly.</li> <li>2. Verify the Time Zone Offset on the GMT window displays <b>OK</b>.</li> <li>3. Verify your company's firewall does not block outgoing/incoming NTP packets (UDP Port 123).</li> </ol>





# PDS-104G PoE Switch

## Power Over Ethernet PowerView Pro User Guide

**Microsemi**

The information contained in the document (unless it is publicly available on the Web without access restrictions) is PROPRIETARY AND CONFIDENTIAL information of Microsemi and cannot be copied, published, uploaded, posted, transmitted, distributed or disclosed or used without the express duly signed written consent of Microsemi. If the recipient of this document has entered into a disclosure agreement with Microsemi, then the terms of such Agreement will also apply. This document and the information contained herein may not be modified, by any person other than authorized personnel of Microsemi. No license under any patent, copyright, trade secret or other intellectual property right is granted to or conferred upon you by disclosure or delivery of the information, either expressly, by implication, inducement, estoppels or otherwise. Any license under such intellectual property rights must be approved by Microsemi in writing signed by an officer of Microsemi.

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. Any performance specifications believed to be reliable but are not verified and customer or user must conduct and complete all performance and other testing of this product as well as any user or customers final application. User or customer shall not rely on any data and performance specifications or parameters provided by Microsemi. It is the customer's and user's responsibility to independently determine suitability of any Microsemi product and to test and verify the same. The information contained herein is provided "AS IS, WHERE IS" and with all faults, and the entire risk associated with such information is entirely with the User. Microsemi specifically disclaims any liability of any kind including for consequential, incidental and punitive damages as well as lost profit. The product is subject to other terms and conditions which can be located on the web at <http://www.microsemi.com/company/terms-and-conditions>.

### Revision History

Revision Level / Date	Para. Affected	Description
1.0		Initial release

© 2016 Microsemi Corp.

All rights reserved.

For support contact: [PoEsupport@microsemi.com](mailto:PoEsupport@microsemi.com)

Visit our web site at: <http://www.microsemi.com/products/poe-systems/poe-systems>

Document Catalog Number: PDS-104GO/AC/M\_NMS\_User.Manual