Power over Ethernet BT PowerView Pro User Guide

Introduction to PowerView Pro (IPv4 and IPv6)

Microchip's PowerView Pro refers to a Web + SNMP interface that enables overall management capabilities for monitoring and controlling Microchip's Power over Ethernet (PoE) Midspans. Management can be carried out over IPv4, IPv6, or both network protocols. The system provides direct online power supervision, configuration, monitoring, and diagnostics of Microchip products through Web/SNMPv2c/SNMPv3/Telnet/SSH.

Note: The principle of operation is similar for all Midspan models described in this user guide.

Features

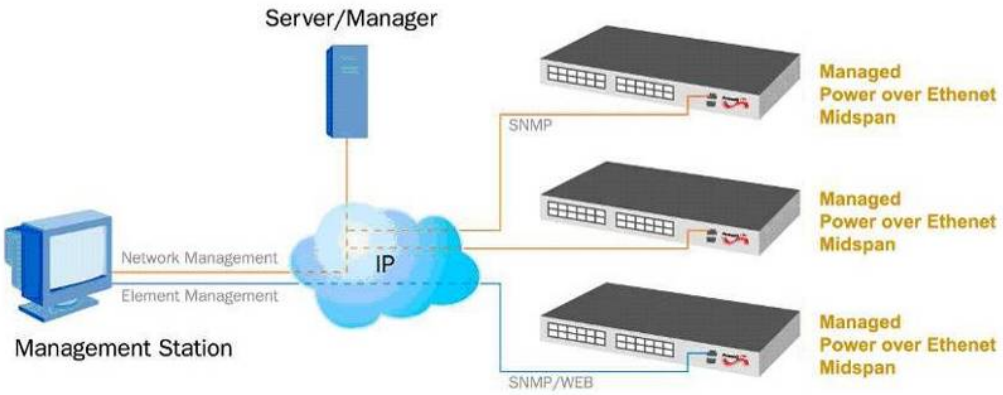
The Midspan management provides unique features with multiple access options:

- Supported network IP protocols:
  - IPv4—IP address is 32 bits (static/DHCPv4).
  - IPv6—IP address is 128 bits (static/DHCPv6).
- Access options:
  - HTTP: Web-based friendly configuration interface for managing remote PoE devices.
  - SSL: Secured web-based configuration.
  - SNMP: SNMPv2c and secured as well as encrypted SNMPv3 (legacy SNMPv1 is also supported).
    - RFC3621 PoE SNMP MIBs.
    - Private MIB extension for RFC3621 PoE MIB.
  - Telnet: Remote terminal over Ethernet network.
  - SSH: Remote encrypted terminal over Ethernet network.
- RADIUS: Authentication and accounting for web/Telnet/SSH remote web users.
- SysLog server: Sends log events to a remote SysLog server.
- Automatic Service Configuration by DHCP: Enables DHCP servers to automatically configure Midspan SNMP Manager's IP address, SysLog servers IP address, and Radius servers IP address.
- Access List Filtering: Controls which remote host or network can manage the Midspan device, and through which management interfaces, such as SNMP, Telnet, Web, and so on.
- Easy software update during runtime without affecting active PoE ports.
- Configuration and real-time monitoring using graphical representations of the remote device.
- System status display.
- Automatic activation or deactivation of PoE ports based on weekly schedule configuration.
- Automatic deactivation of low priority ports when UPS battery is low.
- Power backup by second Midspan or external power source.

System Capabilities

The manager interface can be accessed from any computer using any web browser, SNMPv2c/SNMPv3 management station, Telnet/SSH, RS232 terminal, or USB virtual COM. The PowerView Pro enables monitoring and controlling of PoE IP networks, as shown in the following figure.

Figure 1. Management Deployment



PoE Capabilities

The Midspan injects power over data-carrying Ethernet cabling, which reduces the need for AC outlets, local UPS, and AC/DC adapters near PDs. IEEE® 802.3bt standard delivers up to 90W (class 8) over four pairs.

Configuration Options

The serial communication configuration must set unit's initial IPv4 or IPv6 address (can also be set by a web browser), upload/download unit configuration, restore unit configuration to factory default (this can also be done from a web browser), or update software. Any other configuration must be carried out through the web browser.

- Web: Through a web browser
- SNMPv1/2c/3: Through a SNMP management application on a remote computer
- Telnet: Through a Telnet application on a remote computer
- SSH: Through a SSH client application on a remote computer
- Serial communication port through USB Virtual Communication Port driver: Install USB virtual com driver, and then use terminal emulation software such as PuTTY, Secure CRT, or any similar software.
  Notes:
  - The serial communication rate must be set to 38400 baud.
  - The Midspan default IPv4 address is 192.168.0.50. Make sure that your computer network card is configured to the same IPv4 network (for example, 192.168.0.40).
  - For security reasons, the unit is shipped with SNMP disabled. Before enabling SNMP, modify SNMP community strings and then enable it.
  - The Telnet/SSH and web configuration options are password protected.

Security and User Authentication

Different security profiles are available depending on the type of configuration that is used.

Web Security

The web interface has the following user access levels:

- Viewer: The user only has access to the web pages that report the status of Midspan's configuration summary and cannot change the Midspan configuration.
- Administrator: The Administrator has full access to all web pages and can modify Midspan's configuration.

Note: SSL (https) offers encryption and authentication protection in addition to Viewer and Administrator access levels.

SNMP Security

SNMP v1/v2: The community string is utilized for Get/Set/Trap authentication. SNMPv1/v2 is considered an unsecured protocol because the community string password can be easily intercepted by any network sniffer device.

SNMP v3: Resolves SNMPv1/v2 security issues by adding an authenticating and encryption level to SNMP packets.

Telnet/SSH Security

As Telnet/SSH provides access to various configuration parameters, software update, and data base upload or download, it is always password protected.

Notes:

- The Web interface has a dedicated password, while Telnet and SSH share the same passwords.
- The PowerView Pro is provided with the following factory defaults passwords:
  - **Web/Telnet/SSH**:
    View (usually user):
    user name = "user"
    password = "password"
  - **Configure (usually administrator)**:
    user name = "admin"
    password = "password"
  - **SNMP v3**:
    Guest (usually remote SNMP manager):
    user name = "public"
  - **View user (usually user)**:
    user name = "view"
    authentication password (MD5) = "password"
    privacy password (DES) = "password"
  - **Admin user (usually administrator)**:

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

Table of Contents

1. Preface

This user guide describes Microchip's IEEE 802.3bt compliant 60W/90W, 2.5 Gb–10 Gb IPv6-capable PowerView Pro Remote Web Manager, which is used for managing Microchip's PoE product line of IPv6-capable Midspan devices, including the following Gigabyte (Gb) IEEE 802.3bt PoE compliant Midspans:

- 1 Gb 60W/90W per port Midspan products:
  - PD-9506GC: 6-port 60W 1 Gb IEEE 802.3bt compliant Midspan.
  - PD-9512GC: 12-port 60W 1 Gb IEEE 802.3bt compliant Midspan.
  - PD-9524GC: 24-port 60W 1 Gb IEEE 802.3bt compliant Midspan.
  - PD-9606GC: 6-port 90W 1 Gb IEEE 802.3bt compliant Midspan.
  - PD-9612GC: 12-port 90W 1 Gb IEEE 802.3bt compliant Midspan.
  - PD-9624GC: 24-port 90W 1 Gb IEEE 802.3bt compliant Midspan.
- 2.5 Gb–10 Gb 60W Midspan products:
  - PD-9506-10GC: 6-port 60W 10 Gb IEEE 802.3bt compliant Midspan.
  - PD-9512-10GC: 12-port 60W 10 Gb IEEE 802.3bt compliant Midspan.
  - PD-9524-10GC: 24-port 60W 10 Gb IEEE 802.3bt compliant Midspan.

1.1 Audience

This user guide is intended for network administrators, supervisors, and installation technicians who have a background and knowledge of the following:

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

1.2 References

For more information, see the following documents available at Microchip Software Library.

- Product User Guide.
- Technical Note 132: Using RFC3621 PoE MIB with Microchip Midspans.
- Creating SSL Certificate for Midspan Secured Web Server User Guide.
- RFC3621 PoE SNMP MIB.
- Private SNMP MIB.
- IEEE 802.3af, DTE Power via MDI.

1.3 Terms and Acronyms

The following table lists the terms and acronyms used in this document.

Table 1-1. List of Terms and Acronyms

Terms/Acronym	Definition
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 5
MDI	Media Dependent Interface
MIB	Management Information Base
PD	Powered Device
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
TFTP	Trivial File Transfer Protocol
SysLog	System Log
SSH	Secure Shell
RADIUS	Remote Authentication Dial in User Service

2. Installation

The following sections describe the installation process of the PoE Midspan.

2.1 System Requirements

The following hardware/software items are required to configure and operate the PoE Midspan:

- Program the laptop/PC Ethernet network card to the following network parameters:
  - IPv4: 192.168.0.40
  - IPv4 Mask: 255.255.255.0
- Ethernet cable.
- Ethernet switch connected to the computer and Midspan management RJ45 port (cross cable connected directly between the computer and the Midspan can be used without using an Ethernet switch).
- Telnet application.
- USB type-B cable. For virtual com driver installation, see section 6.2.2 Checklist Prior to Performing Software Update.

Note: The Midspan is shipped with the default IP set to 192.168.0.50. Before connecting the Midspan to your network, verify that no other device has the same IP address.

2.2 Hardware Setup

Before configuring the units, set up your hardware as follows:

1. Connect an AC power cable to the PoE unit.
2. Verify that all LEDs are lit (self-test).
3. Configure the following units:
   - Midspan: Use a USB cable (verify that the virtual com port driver installation was already done).
   - Ethernet network: Connect a network cable to Midspan's RJ45 management port or directly to a laptop's Ethernet port. Make sure that the green main LED to the right of Midspan, below the RJ45 Management port is turned on. For more information, see section 7. Troubleshooting.

2.3 Configuration Procedure

The following sections describe installation of the unit through configuration options.

2.3.1 Connecting to Unit Using a Web Browser

Open the web browser and type **192.168.0.50** in the address field.

2.3.2 Connecting to Unit Using Window's Telnet

For Windows:

1. Click the Windows Start Menu Tiles icon and type **cmd** to open a black DOS window.
2. Type: **telnet 192.168.0.50**.
   Note: If Telnet is missing press Windows Tiles icon and type **add or remove programs**. Type **telnet** in the search window. An option **Turn Windows Features On/Off** appears. Then, add Telnet client.
3. Type the username (admin) and password (password).

Note: Use the Web browser to view the **System Configuration > Security** web page and ensure that Telnet is enabled.

2.3.3 Connecting to Unit Using Serial Port and a Hyper Terminal Application

Windows users must use the PuTTY application, which can be downloaded for free from the Internet.

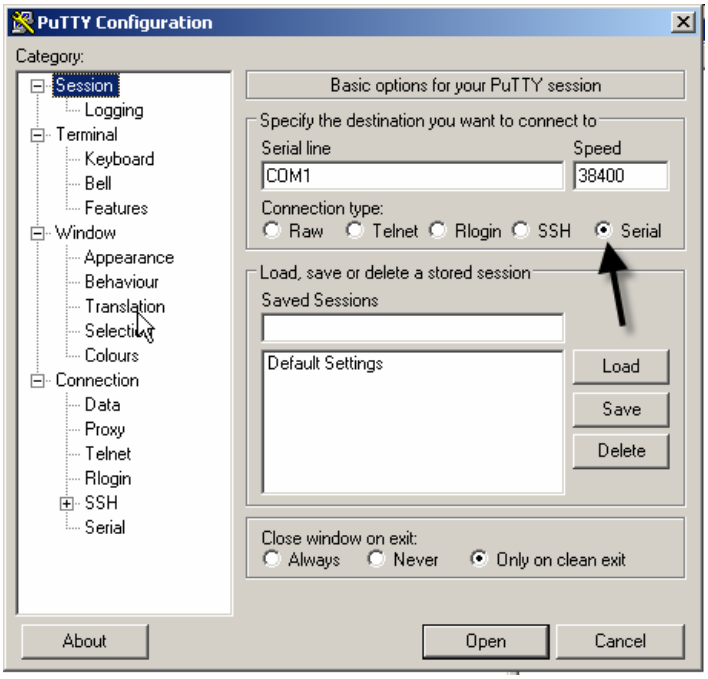
2.3.3.1 Windows PuTTY Freeware Serial Communication Configuration

Windows users must use the PuTTY freeware serial communication software.

1. Download the PuTTY freeware.

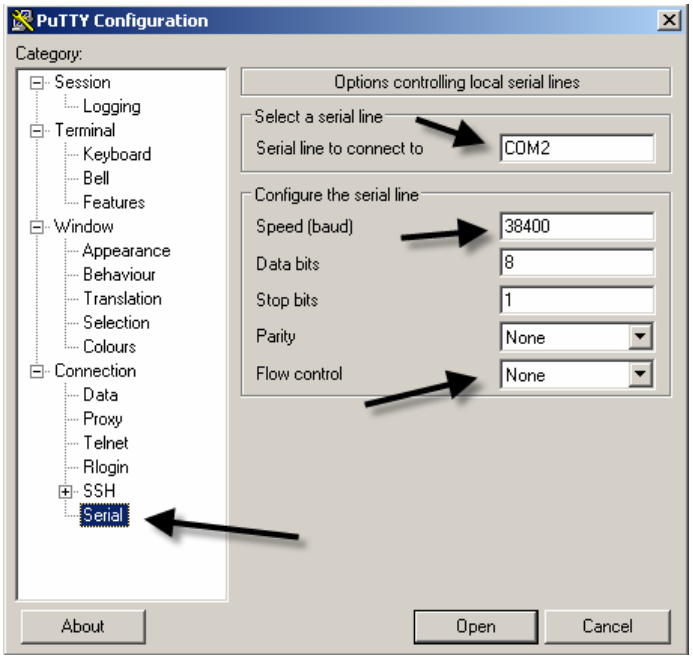
2. Run the PuttY freeware. The Putty Configuration window appears.

Figure 2-1. Putty Configuration Window



3. Under Connection type, select **Serial**. The following PuTTY Serial Configuration window appears.

Figure 2-2. PuTTY Serial Configuration Window Specifications



4. Select:

- Serial line to connect to: Required COM port
- Speed (baud): 38400
- Flow control: None

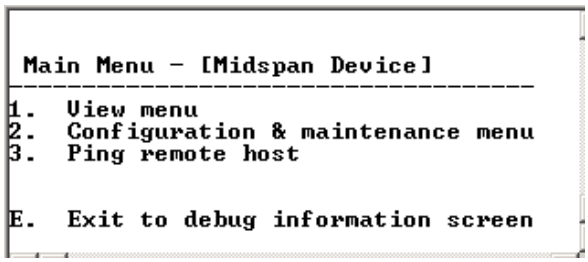
5. Click the Open tab.

2.3.4 Configuring System Through Serial Port

Note: There is no password protection while using the serial communication port. Password protection is only applicable for Telnet, SSH, or web access.

To configure the system through the USB serial interface, click the ESC or space key (if already in the main menu) for the main menu to appear.

Figure 2-3. Main Menu Screen



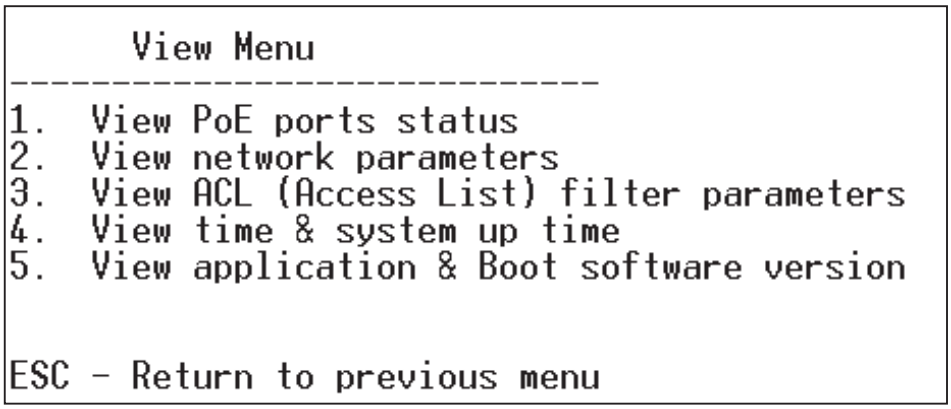
The following is the list of functions in the Main Menu:

- **View menu**: View PoE ports status, network configuration, ACL filter, software version, and release date.
- **Configuration and maintenance menu**: Enable or disable PoE ports, network configuration, upload or download configuration, update SSL certificate, software update, restore user name and password, or unit configuration to factory default and reset unit.
- **Ping remote host**: Determine if an IP system on a network is functional. Use this function to diagnose IPv4 and IPv6 networks connectivity.
- **Exit to debug the information screen**: Enable on-going debug information to be reported by the terminal.

2.3.5 Using the View Menu

In the Main Menu, select the View Menu option.

Figure 2-4. View Menu Screen



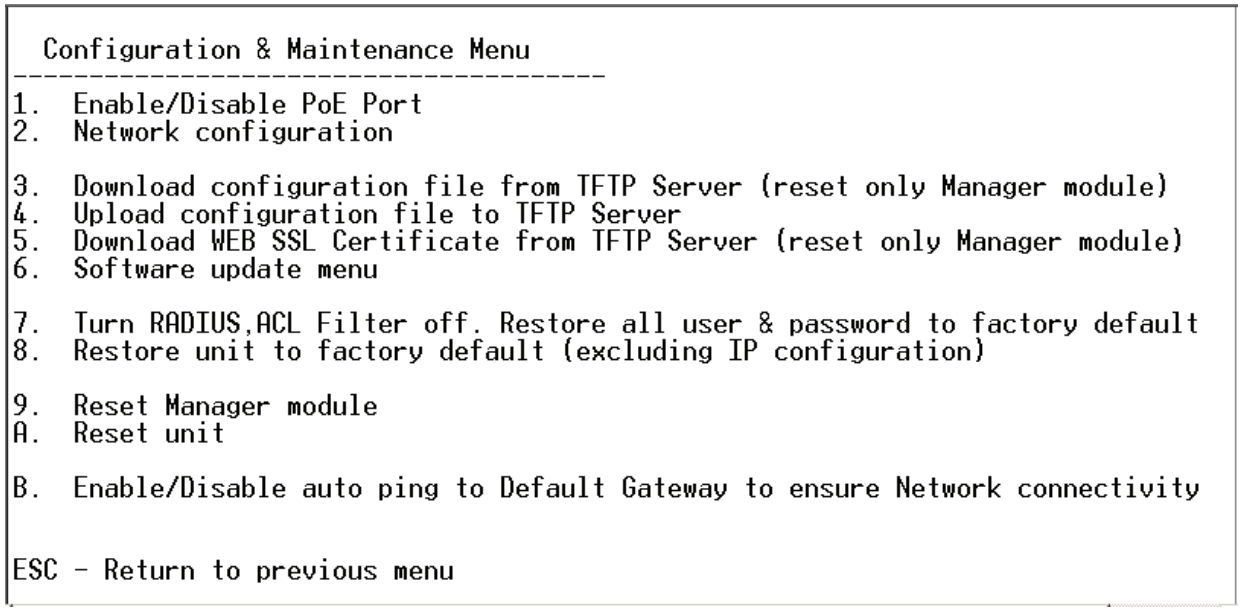
The View Menu contains the following functions:

- **View PoE ports status**: Shows if a PoE port is enabled or disabled, if the port provides power to a PD device, PD power consumption, and PD class.
- **View network parameters**: Displays the Midspan IPv4 address, subnet mask, and default gateway. The same for IPv6, plus DNS, SysLog servers, NTP server and unit MAC address.
  Note: While DHCP is in use, the DHCP server IP appears as well.
- **View ACL (Access List) filter parameters**: Shows access list filter configuration mode and statistics detailing how many network accesses were accepted or rejected by HTTP, HTTPS, SNMP, Telnet, and SSH filters.
- **View time and system up time**: Displays how many days, hours, minutes and seconds the unit has been operational.
- **View application and Boot software version**: Displays the application boot version number and creation date.

2.3.5.1 Using the Configuration and Maintenance Menu

In the Main Menu, select the Configuration and Maintenance menu.

Figure 2-5. Configuration and Maintenance Menu



The Configuration and Maintenance menu contains the following options:

- **Enable/Disable PoE Port**: Allows users to enable/disable a PoE port (same as from web/SNMP/Telnet/SSH).
- **Network configuration**:
  - Set IPv4 address (static/DHCPv4) and DNSv4
  - Set IPv6 address (static/DHCPv6) and DNSv6
  - Set Host name (used by DHCP4/DHCPv6)
- **Download Configuration File from TFTP Server**: Download a configuration file from a remote host using a TFTP application (host must run TFTP server application prior to using this option.
  Note: Upon successful downloading, only the manager module will reset itself without effecting active powered PD devices.
- **Upload Configuration File to TFTP Server**: The unit uploads its internal configuration file to the host, utilizing a TFTP application (host must run TFTP server application prior to using this option).
- **Download Web SSL Certificate from the TFTP Server**: Download a valid private key and certificate files for Web SSL by TFTP. The private key eliminates web browser security warnings whenever SSL is used.
  Note: For detailed procedure description and applicable utility files, see *Web SSL documentation*.

The software update menu enables you to update management module software or PoE firmware:

- **Turn RADIUS, ACL Filter OFF. Restore all user and password to factory default**: Turns RADIUS and ACL filter OFF, and restores Manager Module, and view/configure user name and password to default values (only the manager module resets itself without effecting active powered PD devices).
- **Restore the unit to factory default. Keep IP configuration unchanged**: Restores most of the unit's configuration parameters to factory default values.
  Note: To enable the remote user to access the Midspan after it was restored to factory default, various IP parameters (for example unit IP address) remain the same (only the manager module will reset itself without effecting active powered PD devices).
- **Reset Manager Module**: Only the Manager Module resets itself, without effecting active powered PD devices.
- **Reset unit**: Resets the entire unit, which causes all powered PD devices to be turned off for several seconds, and then re-powered.
- **Enable/Disable auto ping to Default Gateway to ensure network connectivity**: When enabled, it allows the Midspan network Management Module to verify proper network connectivity by pinging default gateway every 12 seconds (IPv4 DGW or IPv6 DGW). After ten consecutive ping failures, the network Management Module resets without effecting PoE ports.
  Note: The Manager Module does not reset if there are no DGWs.
- **ESC**: Return to previous menu.

2.3.5.2 Using the Ping Remote Host Menu

The Ping Remote Host Menu can test Midspan Network configuration and verify access to remote services, such as SysLog server, SNMP network management station, and so on.

Perform the following steps to ping a remote device:

1. In the Main menu, select the **Ping Remote Host Menu**.
2. Type the remote IPv4, IPv6 or remote host name (for using hostname, DNS must be configured).

3. Web Interface Description

The Web interface provides a user-friendly graphical interface for monitoring and configuring the Midspan unit.

3.1 Overview

The system provides the following features:

- View of PoE ports status, power consumption, and Midspan configuration.
- Modification of Midspan configurations, which are applicable for the entire Midspan unit.
- Modification of PoE ports configurations, such as enable or disable, priority, port description, and so on.

The Web Interface has two authorization levels (see section 3.3.8 System Configuration Security).

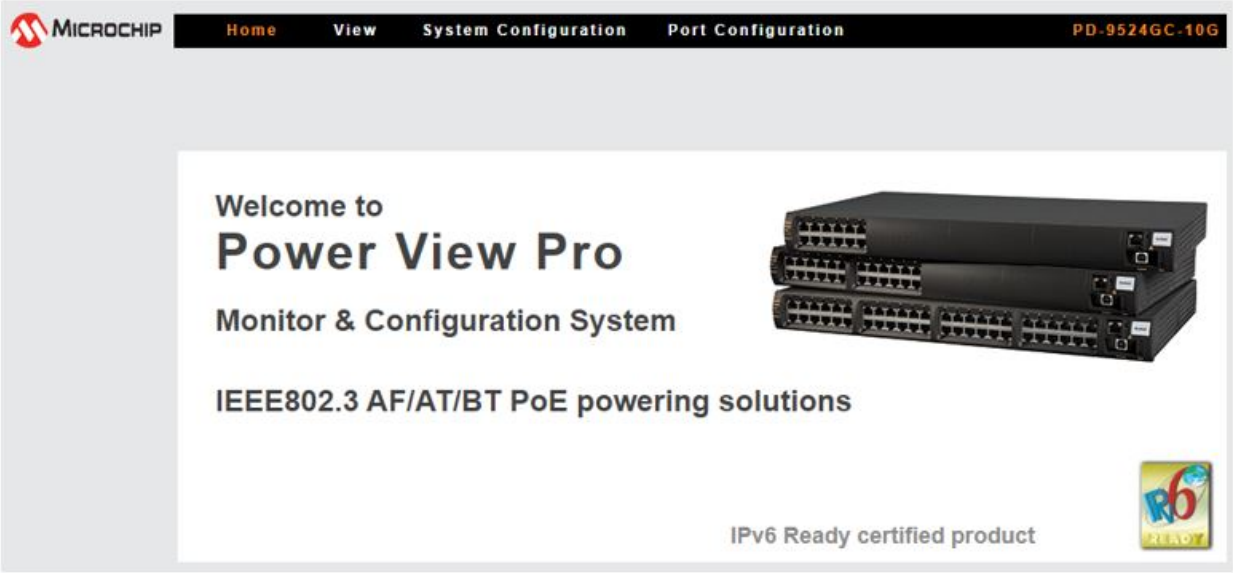
- User: Allows remote users to access only Web pages, which are located under the View menu.
- Administrator: Allows remote users full access to all Web pages.

3.2 Opening Screen

Browse to the Midspan IPv4 or IPv6 address. The main window (opening screen, Figure 3-1) appears. The opening screen comprises three main submenus and displays the product name to the right:

- **View menu**: View unit status, network configuration and product information.
- **System Configuration menu**: Configuring anything that is not PoE port specific (network, SNMP, security, RADIUS, UPS power management, access list filter, product parameters, and maintenance).
- **Port Configuration menu**: Enabling or disabling of ports, allocation of power, setting of priorities, and weekly based schedule automatic PoE ports activation or deactivation.
- **Product name**: Provides a brief description of the product, link for additional related products, and support email.

Figure 3-1. Power View Pro Main Window



3.3 View Menu

The View menu is used to view the following categories:

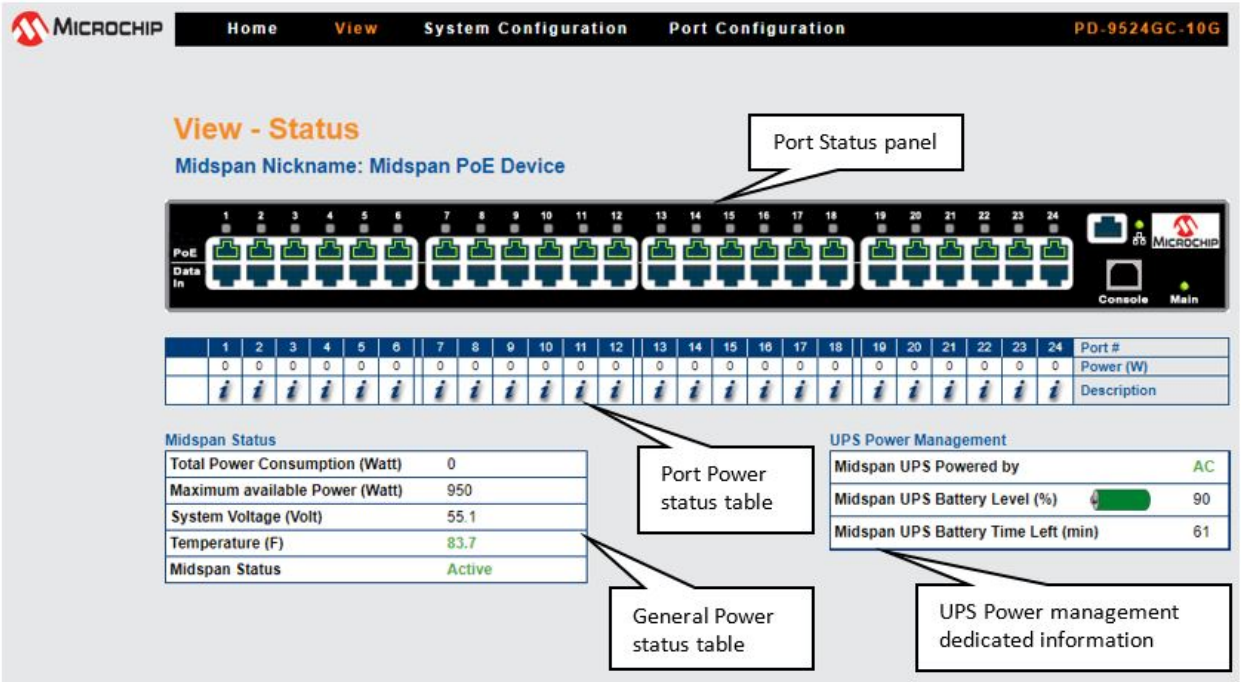
- Status
- Configuration summary
- Product information

3.3.1 View-Status Screen

The View-Status screen monitors the active PoE ports and power consumption for the entire unit or per port. It is made up of several elements:

- **Port status panel**: View which PoE ports are enabled, and the power consumption of each PD.
- **Port power status table**: Pressing the  or  icons opens a detailed port report window.
- **General power status table**: Reports internal power supply voltage, total power consumption, and so on.
- **UPS power management information**: Reports remote UPS battery level, and AC or battery power source. UPS power management information appears only when the UPS power management feature is enabled.
- **Power sources status**: Internal and external power sources status (powered by another Midspan).
- **External redundancy power source status**: Supports redundant power supplies.
- **PD power consumption (60W)**: PoE PD Power consumption reports up to 60W for IEEE 802.3bt devices or up to 65W, if Extended Power Mode is enabled.
- **PD power consumption (90W)**: PoE PD Power consumption reports up to 90W or up to 92.5W, if the Extended Power mode is enabled.
- **Temperature**: Midspans use internal temperature sensor to report Midspan internal temperature. The Midspan temperature can be obtained by View System Status web page and from Midspan SNMP Private MIB.

Figure 3-2. View-Status Screen



3.3.2 View-Status Screen Elements

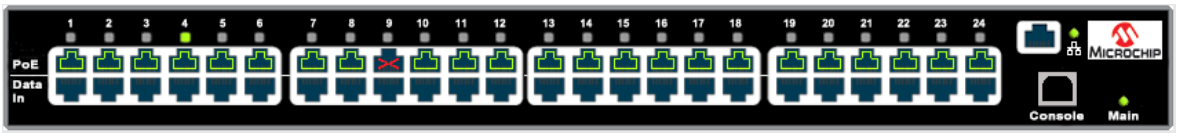
The following sections describe the View-Status screen elements.

3.3.2.1 Ports Status Panel

The display panel includes several visual indicators (see Figure 3-3).

- A green colored RJ45 port indicates that the PoE port is enabled and might provide power whenever a PD device is connected to this port.
- A green LED on top of the green colored RJ45 port indicates that the PoE port provides power to a PD.
- A red colored RJ45 port with an "X" symbol indicates a disabled PoE port (a port that cannot provide power).

Figure 3-3. Ports Status Panel



3.3.2.2 Midspan LED Indications

Two LEDs are located on the front panel. They are marked as “Main” (220/110VAC) and "Link" (Ethernet connection plus activity status), as listed in the following table.

Table 3-1. Main Status Indications

Indicator	Color	Main Power Status	Remarks
AC LED	Off	Internal power supply unit is unplugged or faulty.	Internal power supply voltage is too low. All ports are disconnected
	Green	Indicates that the AC power input active.	Internal power supply voltage is within limits
	Green blinking	Internal power supply voltage is out of range or Internal power supply is unplugged.	—
LINK LED	Green blinking	Indicates valid Ethernet link, and some data communication flow over the Ethernet network.	—
LINK LED	Green	Indicates valid Ethernet link (no communication data).	—

3.3.2.3 Midspan Status Table

The following figure shows the Midspan status table displaying the following parameters:

Figure 3-4. Midspan Status

Midspan Status

Total Power Consumption (Watt)	2.8
Maximum available Power (Watt)	950
System Voltage (Volt)	55.2
Temperature (F)	89.4
Midspan Status	Active

Table 3-2. Midspan Status Table Details

Parameter	Description
Total Power Consumption	Total power consumed by all PDs.
Maximum available Power	Maximum available power for all PDs.
System Voltage	Voltage level supplied to PDs.
Temperature	Internal temperature sensor reports the Midspan internal temperature.
Midspan Status	Reports the communication status between the internal management module and the PoE microcontroller responsible for all PoE functionality. The following options are available: • Active: Normal operation. • Midspan has no firmware. • Internal communication failure. • Midspan firmware update.

3.3.2.4 Detailed Port Information Report

Clicking the icon or the RJ45 jack image ( ) brings up a new pop-up Web page that provides detailed information on the specific port, as shown in the following figure.

Figure 3-5. Detailed Port Information

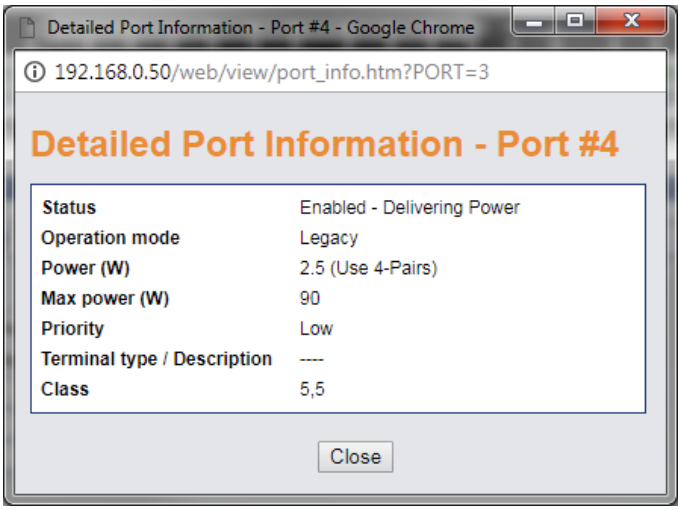


Table 3-3. Detailed Port Description Information

Parameter	Description
Status	Disabled: Port is disabled Enabled: Port is enabled Enabled—Delivering Power: Port is enabled and delivers power to PD device. Enabled—Failure to power a PoE Device: Port is enabled and the PoE PD device is connected, but no power is provided. Probable causes include: PoE device consumes too much power (overload) or the PoE PD device is invalid, and so on.
Operation mode	PSE port is configured to power IEEE 802.3bt compliant PD devices only, or Legacy devices which are not fully IEEE 802.3bt compliant.
Power (W)	Actual PD power consumption.
Max Power (W)	Maximum power allocated by the Midspan based on PD class signature.
Priority	Priority level set by the user.
Terminal Type/ Description	Textual port description as configured in the Port Configuration
Class	PD device class. PD class might be reported as a single digit ranging from 0–8 (each number applies to different PD max power) or as two digits, with each digit ranging from 0–8. For example, 4, 4 means that the unit total is expected to get 2xclass-4 power in [W].

3.3.2.5 Manual Override Key

Whenever the Weekly Schedule feature is activated, the IT manager can configure one of the Midspan PoE ports to act as a Manual Override Deactivation key. This enables easy temporary deactivation of the Weekly Schedule feature, whenever an authorized user arrives at work during unexpected hours. The IT manager selects the override port manually through the Web interface and then enables the override feature; an icon then appears on the selected port.

Note: The Deactivation key is an optional item and can be purchased separately from Microchip.

Upon unexpected user arrival to work, the user inserts the deactivation key into the previously assigned override port (usually routed through the patch panel near the doorway entrance).

Figure 3-6. Manual Override Deactivation Key

If the override key is inserted, all Weekly Schedule deactivated PoE ports remain active. Upon leaving work, the user removes the override key, which in-turn causes all Weekly Schedule assigned ports to turn off (Weekly Schedule time configuration dependent).

Note: In cases where the icon appears but the corresponding port LED does not illuminate, it means that the port had been assigned as a 'bypass' port, but the override key has not been inserted.

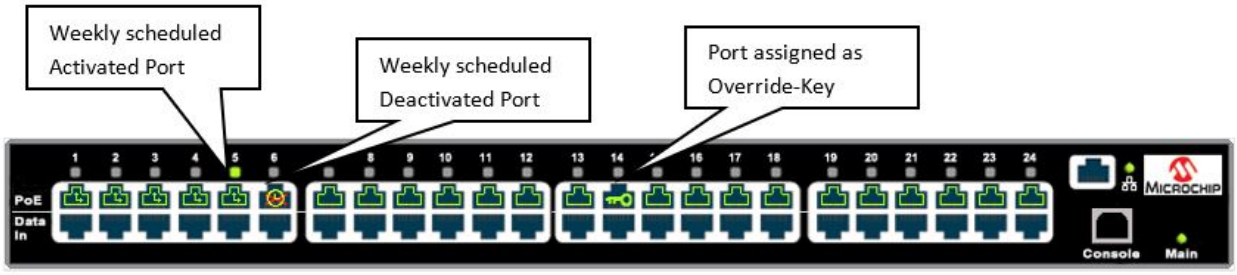
3.3.2.6 Weekly Scheduled Activated Port(s)

The Weekly Schedule feature enables (when checked) scheduling of automatic PoE ports activation or deactivation as set in the weekly schedule activation scheme.

When the icon appears on a port, it means that a specific port is temporary deactivated by the Weekly Schedule algorithm.

Note: The PoE port activation or deactivation hours depend on the user's Weekly Schedule configuration (see section 3.4.3.1 Weekly Schedule Ports Activation).

Figure 3-7. Weekly Activated/Deactivated Ports

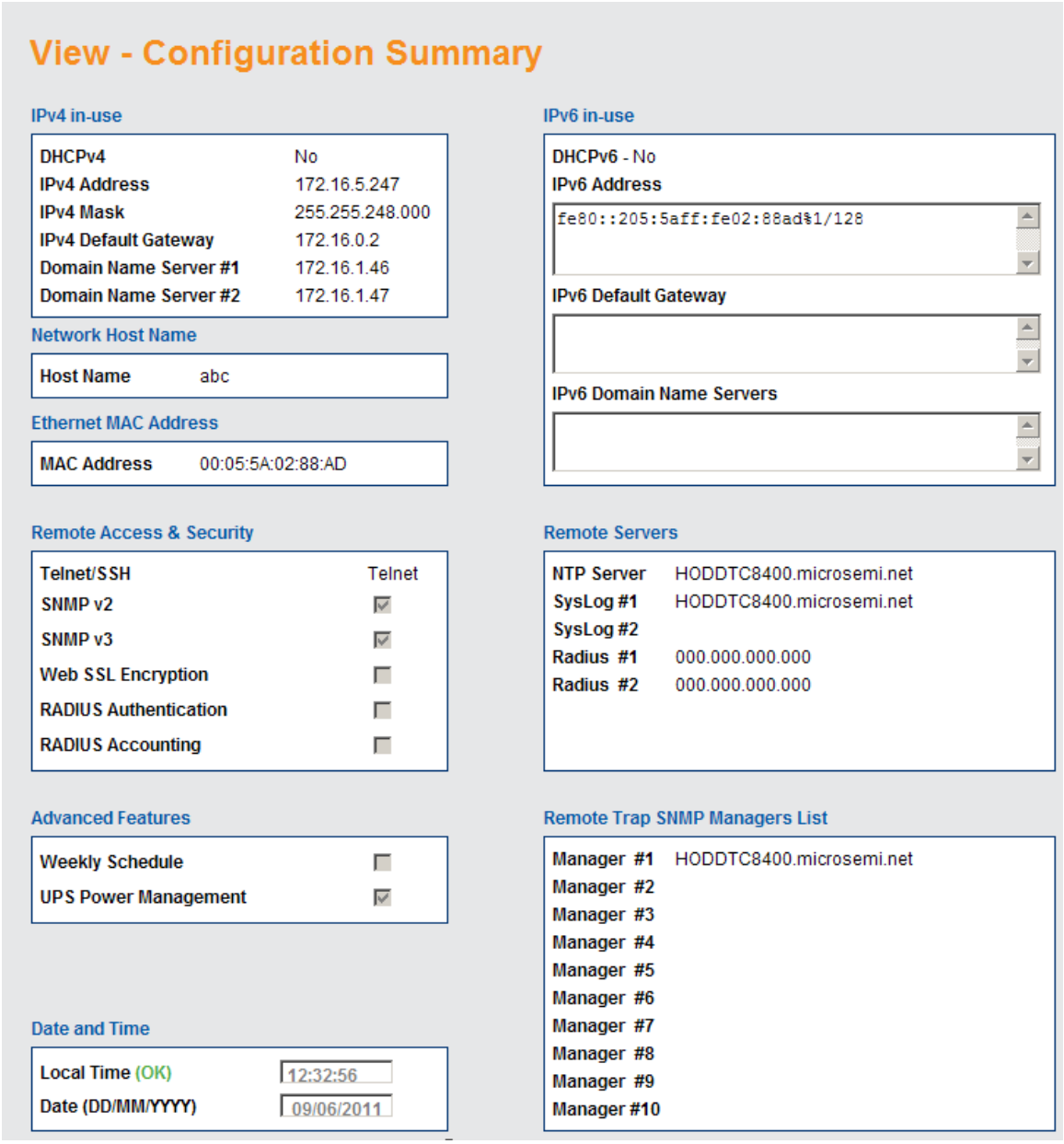


3.3.3 View-Configuration Summary

The View-Configuration Summary screen (Figure 3-8) displays the following parameters:

- **IPv4 in-use**: Currently in use IPv4 address/mask/gateway (may be acquired by DHCP or static configuration) and IPv4 Domain name servers.
- **IPv6 in-use**: Currently in use IPv6 address/prefix/gateway (may be acquired by DHCPv6 or static configuration) and IPv6 Domain name servers.
- **Network Host Name**: Midspan hostname used by IPv4/IPv6 to register Midspan hostname in DHCPv4/DHCPv6 Server.
  Note: Only A–Z, a–z, 0–9, minus, and dots are allowed. Hostname must start with a letter.
- **Ethernet MAC Address**: 6 byte (48 bit) unique Ethernet address.
- **Remote Servers**: IP address of remote Network Time Protocol (NTP) server, remote SysLog Servers, and remote Radius Servers.
- **Remote Trap SNMP Managers List**: List of assigned SNMP managers to receive Midspan SNMP Trap reports.
- **Date & Time**: Unit local time, as acquired from the NTP server (GMT time zone must be configured by the user).
- **Remote Access & Security**: A list of Midspan remote access and security options; SNMP v1/v2 and SNMPv3, Telnet/SSH, RADIUS, and SSL Web encryption
- **Advanced Features**: Indication of Automatic Weekly Schedule PoE ports activation, and UPS Power Management features activation.

Figure 3-8. View-Configuration Summary Screen



3.3.3.1 IPv4 in-use

The IPv4 in-use window displays the current IP address being used with the following parameters:

Figure 3-9. IPv4 in-use Window

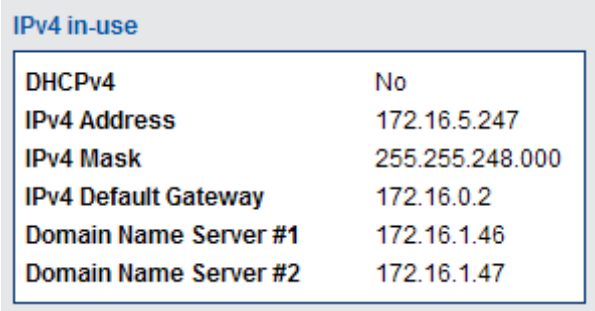


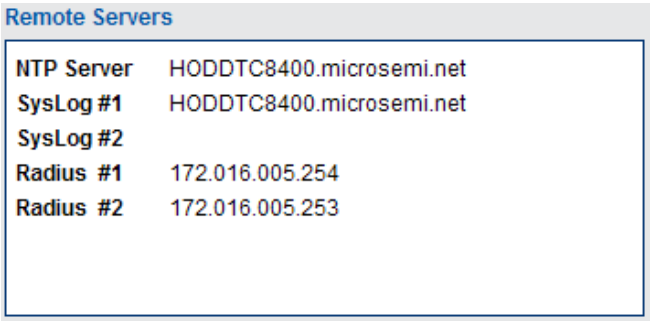
Table 3-4. IP in User Parameters

Parameter	Description
DHCPv4	Indicates if DHCPv4 or static IPv4 is in use.
IPv4 Address	IPv4 address of the Midspan in use.
IPv4 Mask	Determines the size of the IPv4 network.
IPv4 Default Gateway	IPv4 address of the local gateway, which enables communication with other IPv4 networks.
Domain Name Server 1 and 2	IPv4 address of DNS used for resolving remote host names.

3.3.3.2 Remote Servers

The Remote Servers window displays IPv4, IPv6, or remote hostname addresses of remote SysLog, RADIUS, and NTP servers.

Figure 3-10. Remote Servers Window



3.3.3.3 Date and Time

The Date and Time (GMT time zone) window displays the unit's local time as acquired from the NTP Time Protocol server by the user. It also sets the offset local time zone.

Figure 3-11. Date and Time Window

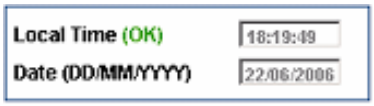


Table 3-5. IP in User Parameters

Parameter	Description
Local Time	Time (HH:MM:SS) as acquired from the NTP server, plus time zone offset.
Date	Date (DD/MM/YYYY) as acquired from the NTP server.

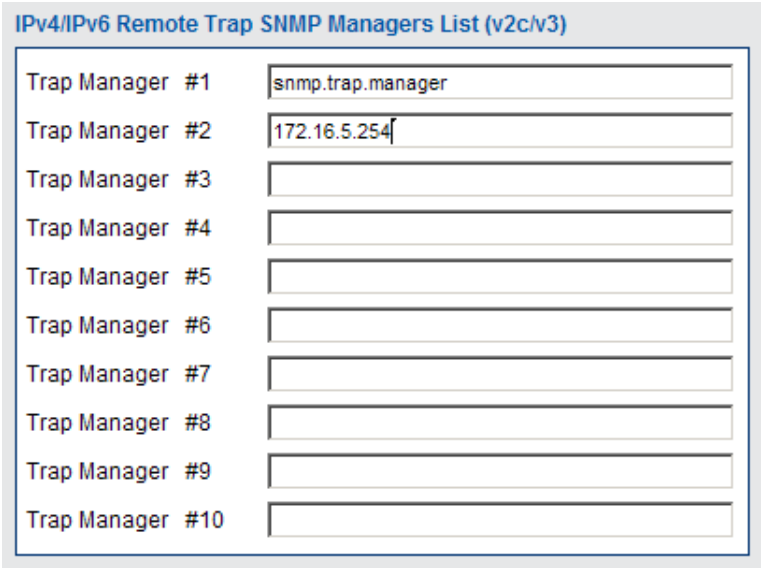
3.3.3.4 Remote Trap SNMP Managers List

This list displays all the user pre-configured SNMP managers (see 3.3.3.4 Remote Trap SNMP Managers List. All listed managers receive traps reported by the Midspan (to receive PoE traps, make sure that the PoE RFC3621 notification feature is enabled). Verify RFC3621 and Midspan private MIB are installed on the SNMP management station that monitors the Midspan device.

Notes:

1. When the appropriate time and date are acquired from the NTP server, an OK indication appears. Alongside the Time Zone Offset from GMT window in the System Configuration—Weekly Schedule Ports Activation menu (see section 3.4.3.1 Weekly Schedule Ports Activation). If the system fails to acquire the appropriate time and date, the 'FAIL' indication appears instead.
2. If the unit fails to acquire time from NTP Server, it displays the elapsed time starting from 1/1/2005.
3. If time and date are not acquired, Weekly Schedule functionality does not function.
4. If local time zone offset has been improperly set by the user (Weekly Schedule configuration web page), an incorrect time is shown.

Figure 3-12. Remote Trap SNMP Managers List



3.3.3.5 Remote Access and Security

The **Remote Access and Security** list summarizes if Midspan can be managed by SNMPv2, SNMPv3, Telnet or SSH, HTTP or HTTPS, and if RADIUS authentication and accounting is enabled.

Figure 3-13. Remote Access and Security Window

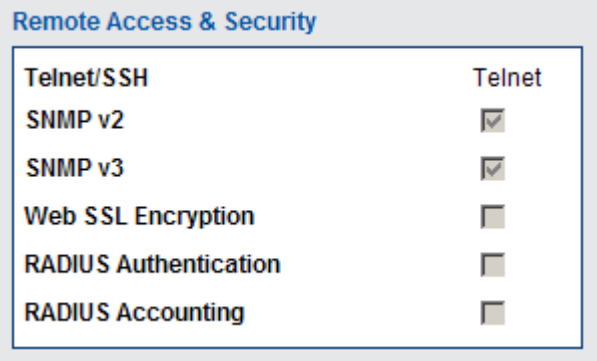


Table 3-6.

Parameter	Description
Telnet/SSH	Indicates if Midspan can be managed by Telnet, SSHv2 (secure and encrypted terminal) or by none of them.
SNMPv2	Indicates whether Midspan can be managed by SNMPv1/v2.
SNMPv3	Indicates whether Midspan can be managed by SNMPv3. It is not recommended to enable SNMPv2 while SNMPv3 is in use.
Web SSL	Indicates if Midspan Web pages are encrypted by SSL.
RADIUS Authentication	When checked, indicates that remote Telnet/SSH/Web users are authenticated by the RADIUS server rather than by the Midspan itself.
RADIUS Accounting	When checked, indicates that the Midspan sends an accounting report to the RADIUS server whenever remote users access Midspan by Telnet/SSH/Web.

3.3.3.6 Advanced Features

The Advanced Features window (Figure 3-14) displays which of the Weekly Schedule/UPS Power Management advanced features is activated.

The Weekly Schedule feature enables scheduling of automatic PoE ports activation or deactivation as set in the weekly schedule activation scheme.

The UPS Power Management feature extends the period, in which the Midspan might provide power to high priority PoE devices during a power failure. This is accomplished by monitoring the UPS battery level and automatically shutting down low priority PoE ports, when the UPS battery level drops to a low level.

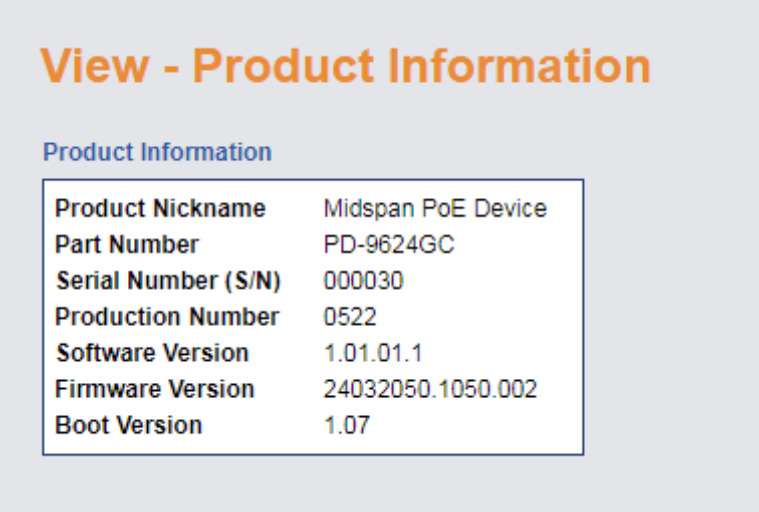
Figure 3-14. Advanced Features Window

Parameter	Description
Weekly Schedule	Indicates that the weekly schedule feature had been activated through the **System Configuration > Weekly Schedule Ports Activation** menu.
UPS Power Management	Indicates that the Midspan is configured to communicate with UPS SNMP agent to monitor its UPS battery level and automatically deactivate low priority PoE ports when UPS battery is low.

3.3.4 View-Product Information

The View-Product Information web page summarizes production-related parameters, such as product type, serial number, PoE firmware software version, and network management module software version, as shown in the following figure:

Figure 3-15. View-Product Information Screen



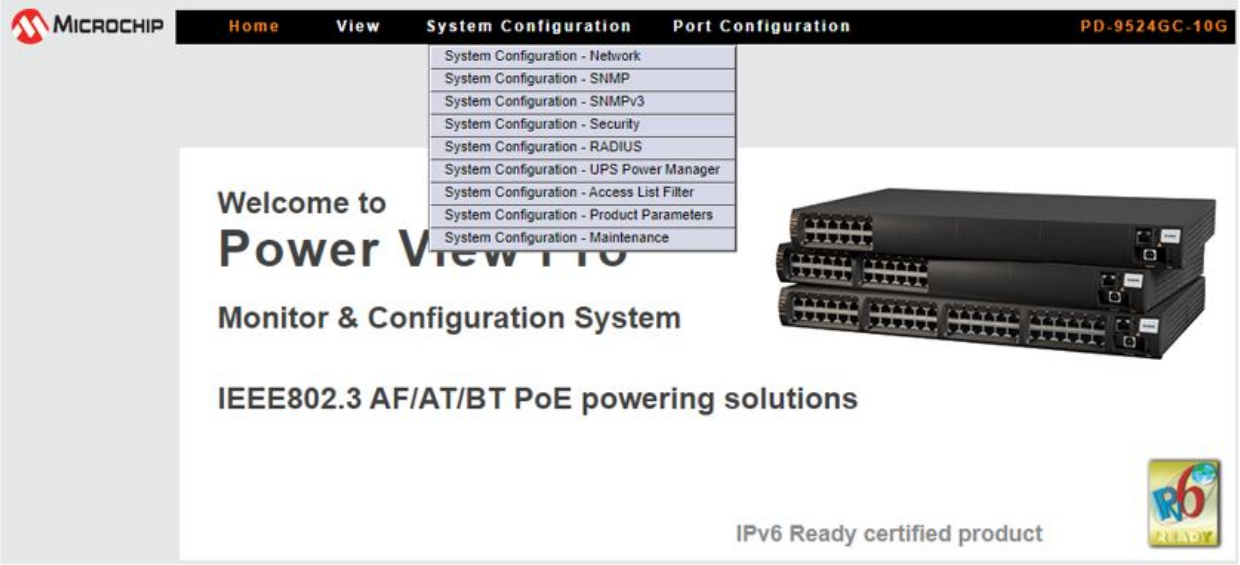
Parameter	Description
Product nickname	Unit nickname as configured by the network administrator to be displayed in the View-Status web page and in serial/Telnet/SSH menus.
Part number	Midspan part number.
Serial number	Midspan serial number.
Production number	Unique manufacturing product number per each Midspan type (all Midspans of the same type have the same production number).
Software version	PowerView Pro Network Manager module software version.
Firmware version	PoE Firmware version.
Boot version	Network Manager Module boot version.

3.3.5 System Configuration Screen

The System Configuration menu configures the following options (see Figure 3-16):

- Network configuration
- SNMP configuration
- SNMPv3 configuration
- Security configuration
- RADIUS configuration
- UPS Power Management configuration
- Access List Filter configuration
- Product parameters-configuration
- System configuration-maintenance

Figure 3-16. System Configuration Screen



3.3.5.1 System Configuration-Network

The System Configuration-Network menu (Figure 3-17) enables configuration of the following:

- Static/Dynamic IPv4 address
- Static/Dynamic IPv6 address
- NTP server (IPv4/IPv6)
- SysLog log (IPv4/IPv6) servers
- Automatic SNMP Trap list
- SysLog and Radius IP to be obtained by DHCP server, which simplifies management when many Midspan devices must be managed.

For a detailed description see section 3.3.5.2 Auto Services Configuration by DHCPv4.
Note: When enabling Automatic IP configuration for SNMP traps, SysLog, and DARIUS by DHCPv4 server, only IPv4 address type can be obtained automatically for SysLog, SNMP, and RADIUS.

Figure 3-17. System Configuration-Network Screen

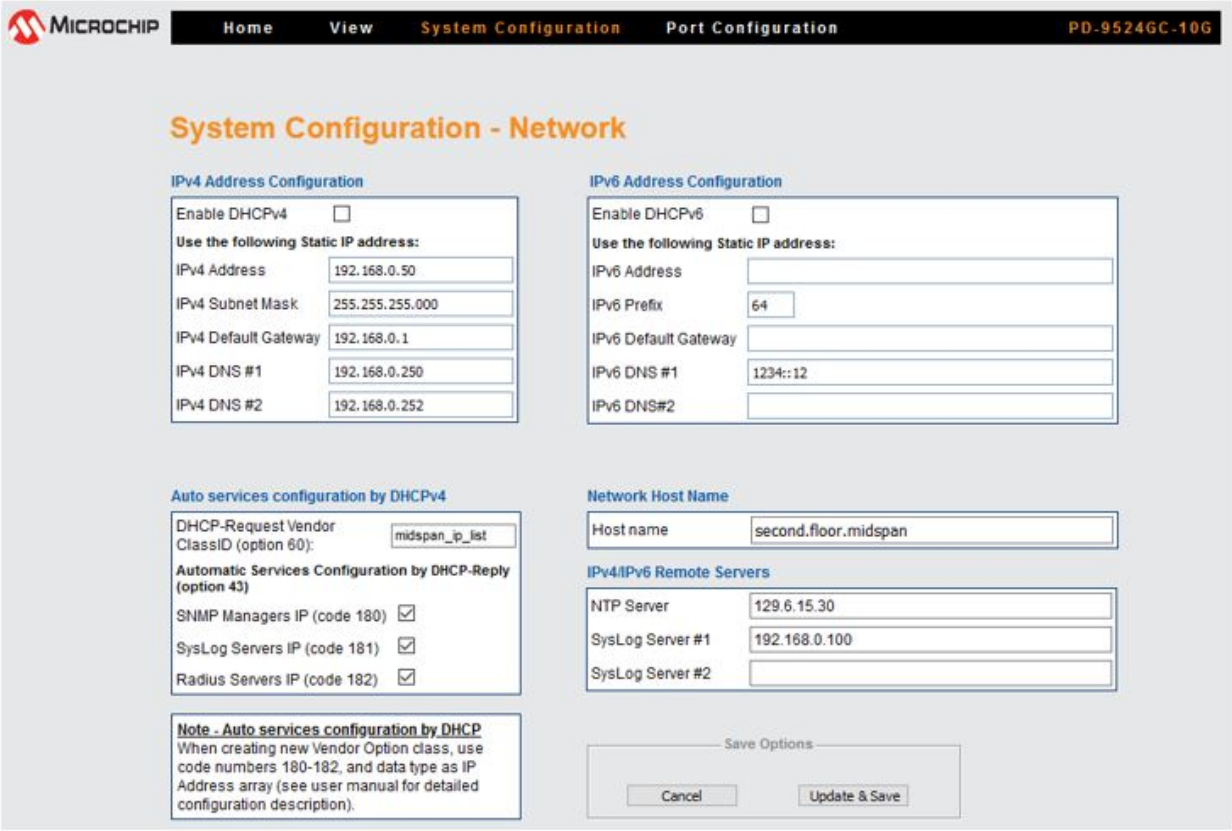
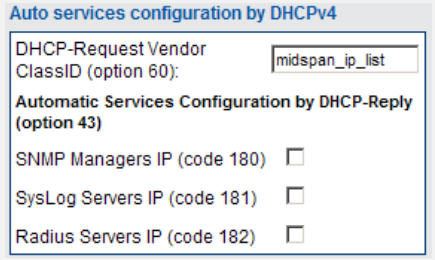
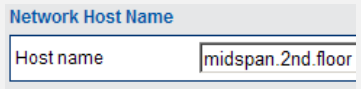
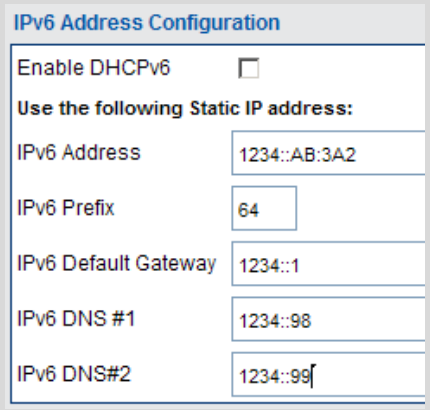
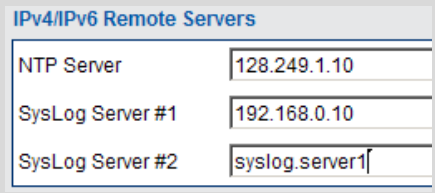
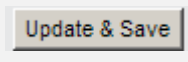
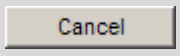


Table 3-7. System Configuration Network Screen Details

Parameter	Description
IPv4 Address Configuration Enable DHCPv4 Use the following Static IP address: IPv4 Address 172.16.5.247 IPv4 Subnet Mask 255.255.248.000 IPv4 Default Gateway 172.16.0.2 IPv4 DNS #1 172.16.1.46 IPv4 DNS #2 172.16.1.47	DHCPv4 En/Dis—When checked, it enables Midspan to obtain IPv4 address from a DHCPv4 server.
	IPv4 Address—Static IPv4 address to be used if DHCPv4 is disabled.
	IPv4 Subnet Mask—Static IPv4 subnet mask to be used if DHCPv4 is disabled.
	IPv4 Default Gateway—Static IPv4 default gateway to be used, if DHCPv4 is disabled.
	IPv4 DNS #1—Static IPv4. The first DNS IPv4 address to be used, if DHCPv4 is disabled.
	IPv4 DNS #2—Static IPv4. The second DNS IPv4 address to be used, if DHCPv4 is disabled.

.....continued

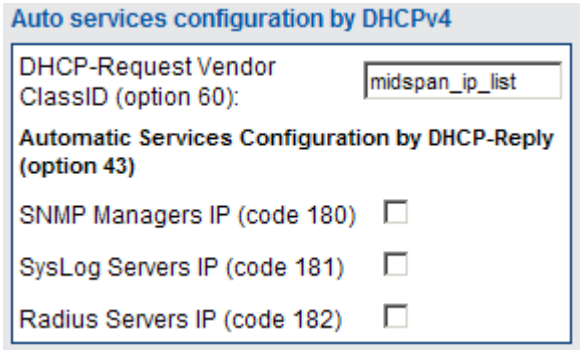
Parameter	Description
	Set Vendor Class ID string (DHCPv4 option #60) within DHCPv4 request message sent by Midspan to the DHCP server. Whenever DHCPv4 is active, enable or disable the DHCPv4 server to automatically configure SNMP Managers IP, SysLog Server IP, and RADIUS server IP.
	Midspan hostname to be included within DHCPv4 and DHCPv6 messages.
	**Notes:** • DHCPv6 functionality varies by M&O bits, which are advertised by IPv6 router over the network. • M = 1, O = 1: Obtain IPv6 address & DNS from DHCPv6 server. • M = 0, O = 1: Obtain only DNS from DHCPv6 server. • Use Automatic link-local IPv6 address. IPv6 Address—Static IPv6 address to be used if DHCPv6 is disabled. IPv6 Prefix—Static IPv6 prefix (subnet mask) to be used if DHCPv6 is disabled. IPv6 Default Gateway—Static IPv6 default gateway to be used, if DHCPv6 is disabled. IPv6 DNS #1—Static IPv6. The first DNS IPv6 address to be used, if DHCPv6 is disabled. IPv6 DNS #2—Static IPv6. The second DNS IPv6 address to be used, if DHCPv6 is disabled.
	**Note:** Local time GMT offset can be configured through the Weekly Schedule Port Activation web page. SysLog Server #1—IPv4/IPv6/hostname address of remote SysLog Server #1. SysLog Server #2—IPv4/IPv6/hostname address of remote SysLog Server #2.
	Updates new network parameters. All properties and remote server parameters become effective only after clicking this button.
	Cancels current operation and restores previous values if Update & Save buttons are not clicked.

3.3.5.2 Auto Services Configuration by DHCPv4

DHCPv4 server can be configured (see Figure 3-18) to automatically set the Midspan SNMP Manager list, SysLog servers, and RADIUS servers. Such a configuration simplifies multiple Midspans management. The configuration example shown in Figure 3-18 is based on a Windows 2008 server. The same configuration guidelines must be used when another DHCP server type is in use.

Configuring Midspan DHCP Vendor Class ID (DHCP option 60) on Midspan: Set Vendor Class ID string, which is sent from the Midspan to DHCP server in each DHCP-Discover and DHCP-Request message.

Figure 3-18. Auto Services Configuration by DHCP



Configuring DHCP Vendor Class ID on DHCP Server: Configure the same Vendor Class ID on the DHCP server. Whenever the DHCP Server detects a known Vendor Class ID string, it might be configured to provide various IP addresses, which are unique for each pre-configured Vendor Class ID string.

1. Right-click DHCP root and then choose **Define Vendor Class** (Figure 3-19).
2. Click **Add**.
3. Fill the **Display name** and Description fields.
4. Click on the ASCII section and type **midspan_IP_list** (Figure 3-20).
5. Click **OK** to close the window.

Figure 3-19. Defining Vendor Class

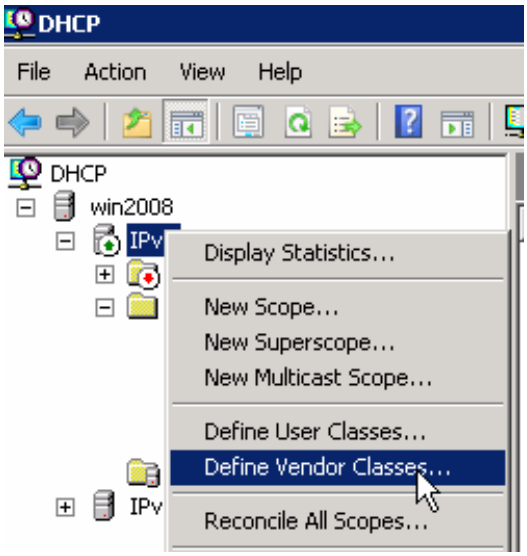
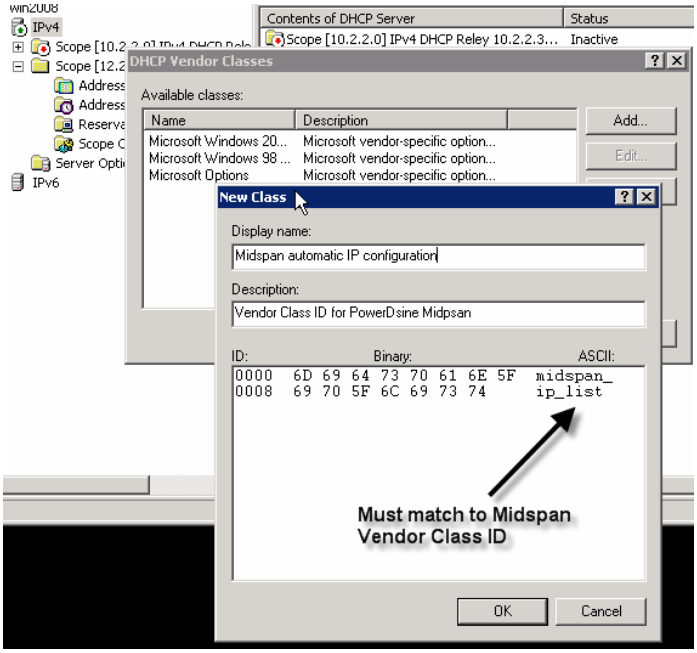


Figure 3-20. Set Vendor Class String



Perform the following steps to add predefined sub types:

1. Right-click DHCP root.
2. Select the **Set Predefined Options** (Figure 3-21).
3. Select the new option class: **Midspan automatic IP configuration** (Figure 3-22).
4. Click **OK**.
5. Click **Add**.

Figure 3-21. Set Predefined Options

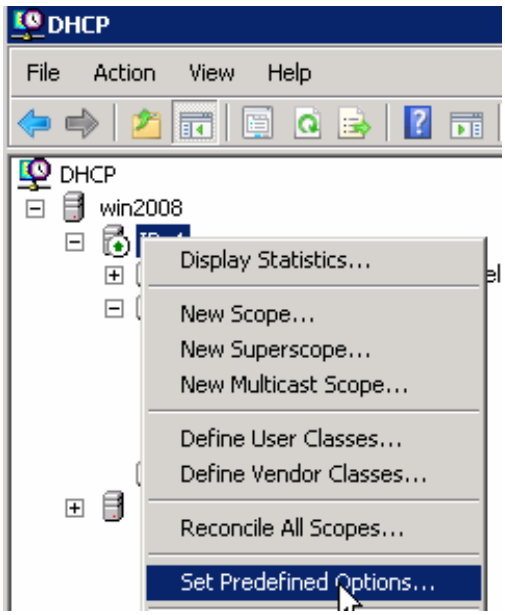
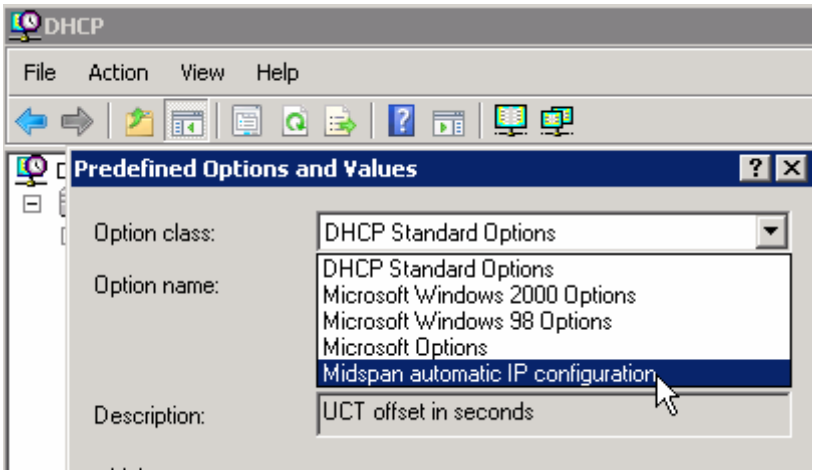


Figure 3-22. Adding Predefined Subtypes



In the Option Type window (Figure 3-23):

1. Fill the **Name** and **Description** fields.
2. Set **Data Type** to IP Address.
3. Check the array checkbox. The Code field must be the same as in the Midspan (Figure 3-24).
4. Click **OK**.

Figure 3-23. SNMP Manager Option Type

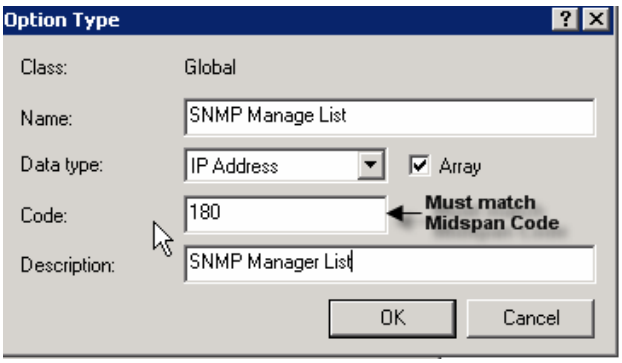
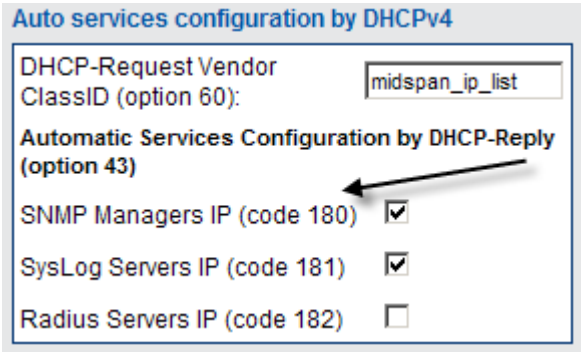


Figure 3-24. Midspan Option Code



- Code 180: SNMP Manager IP list.
- Code 181: SysLog IP list.
- Code 182: Radius IP list.

Repeat the same procedure to create the **SysLog Manager List** and **Radius Manager List Option Type**, as shown in Figure 3-25 and Figure 3-26.

Figure 3-25. SysLog Option Type

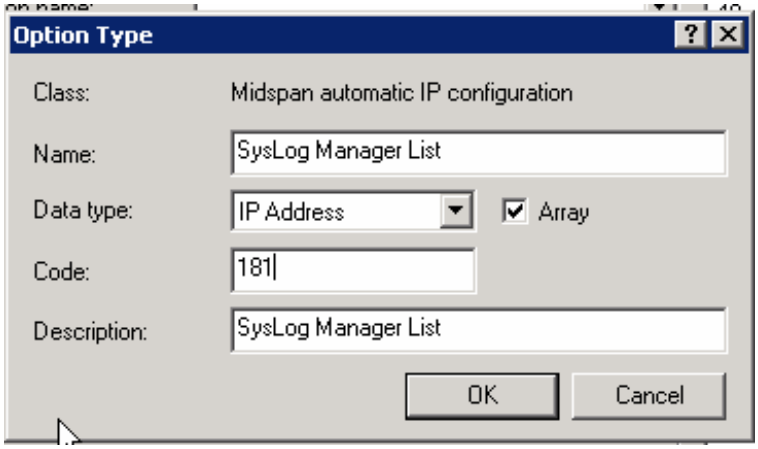
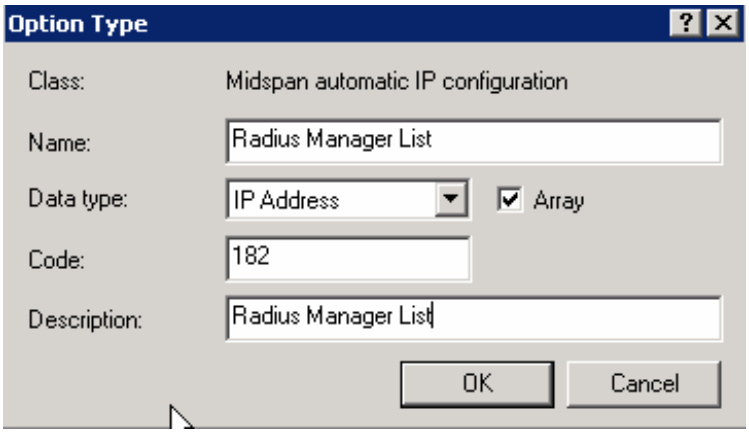


Figure 3-26. RADIUS Option Type



Setting Scope Options:

1. Select the appropriate **DHCP**.
2. Right-click **Scope Options**.
3. Select **Configure Options** (Figure 3-27).
4. Select the Advanced tab (Figure 3-28).
5. In the Vendor class, select the new defined vendor class: **Midspan automatic IP configuration**.

Figure 3-27. Scope Options Configurations

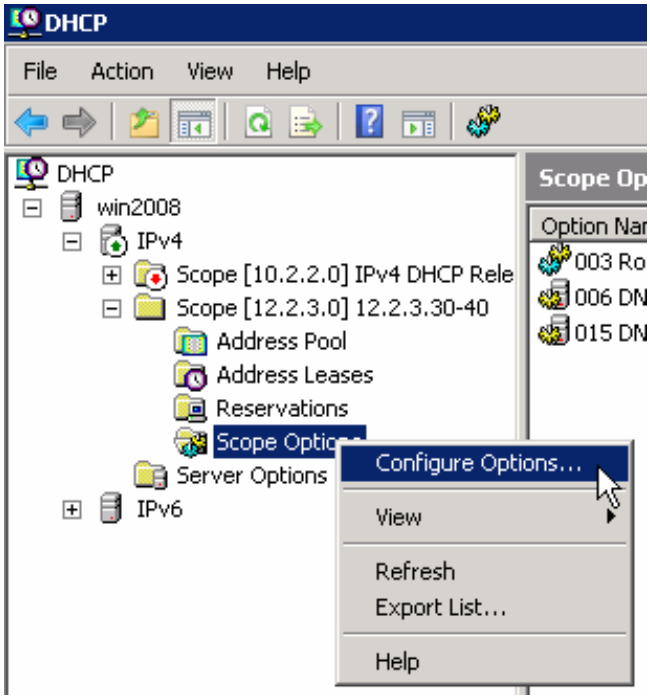
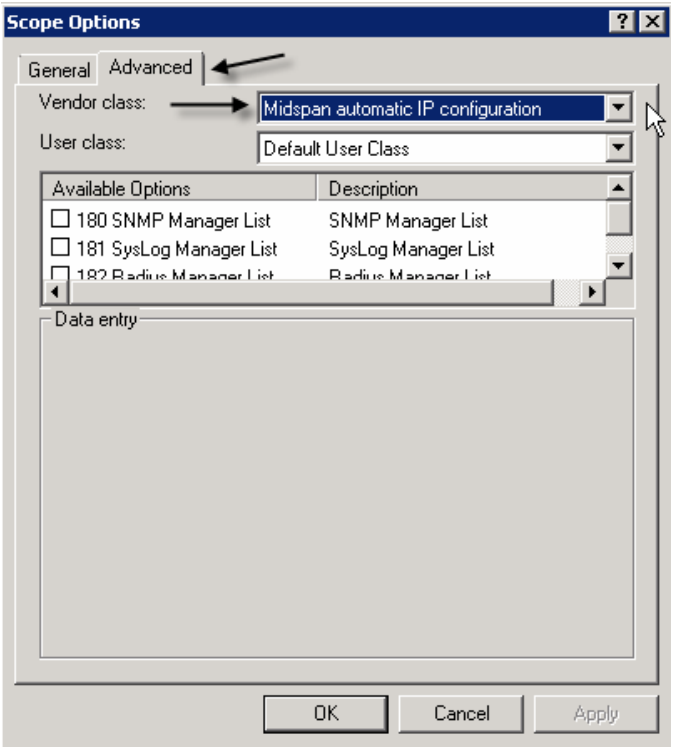


Figure 3-28. Midspan Scope Options



Check the sub vendor options that the DHCP server must advertise, so that the various IP addresses used by the Midspan are automatically configured. The new configured scope options are added to the Scope Options advertised by the DHCP server, as shown in Figure 3-30.

Figure 3-29. Configuring Scope Options

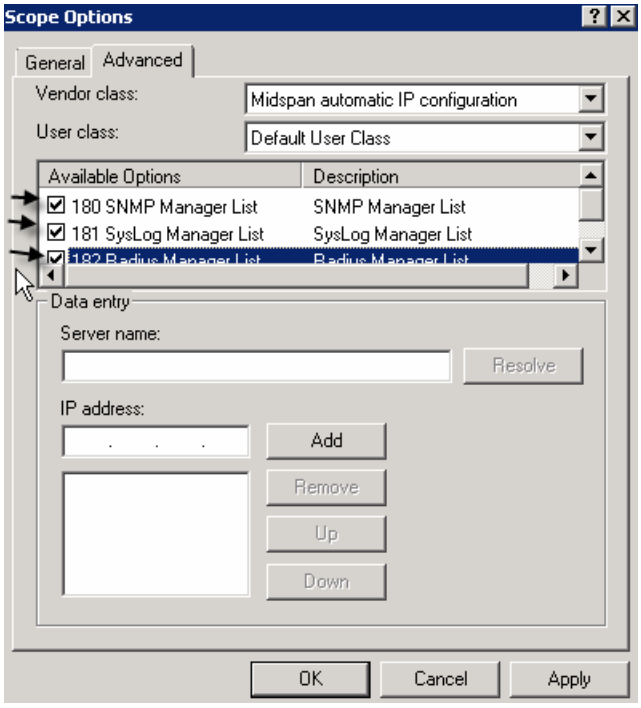
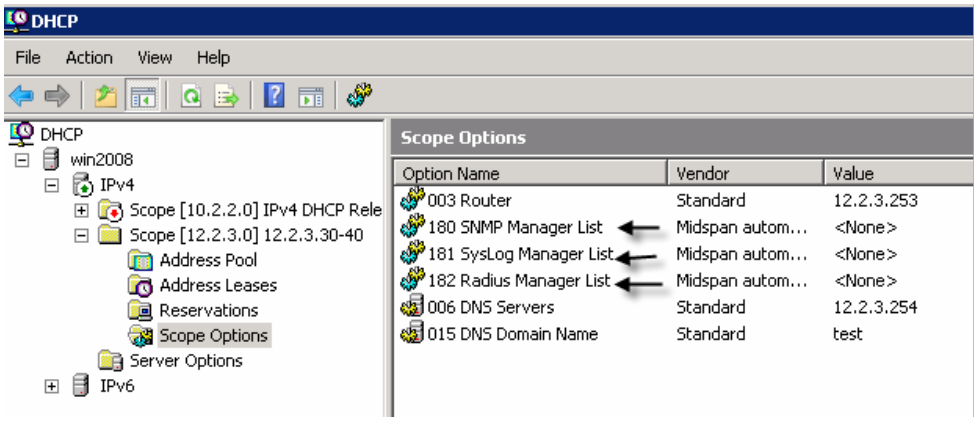


Figure 3-30. Advertised Scope Options



Setting SNMP Manager IP Address List:

1. Select SNMP Manager List.
2. Right-click and select **Properties** (Figure 3-31).
3. Type **SNMP Manager IP Address** (up to 10 SNMP Managers).
4. Click **Add**.
5. Repeat same process for the **SysLog IP list** (up to two addresses) and **Radius Servers IP list** (Figure 3-32).

Figure 3-31. SNMP Scope Options

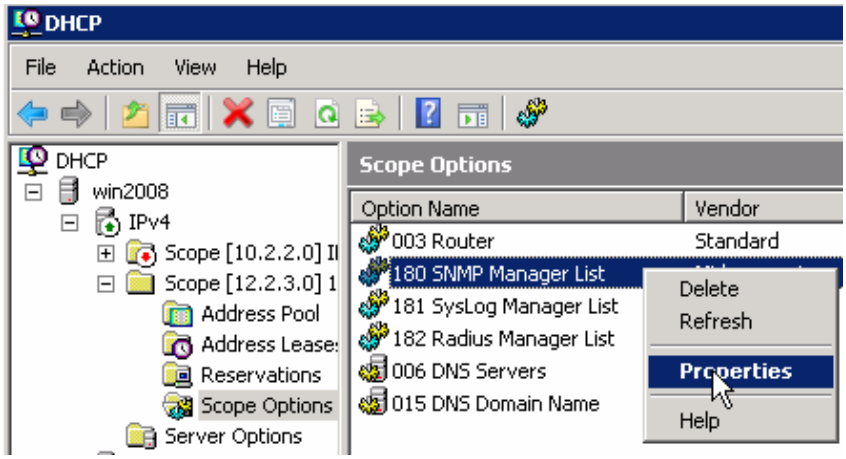
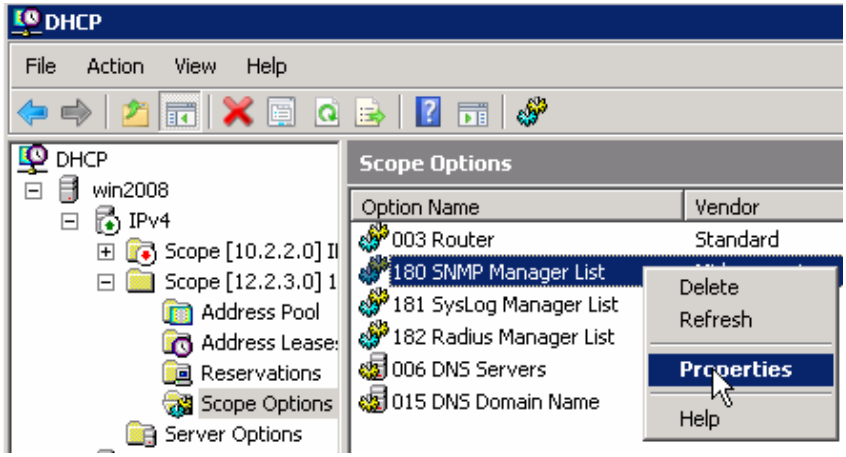
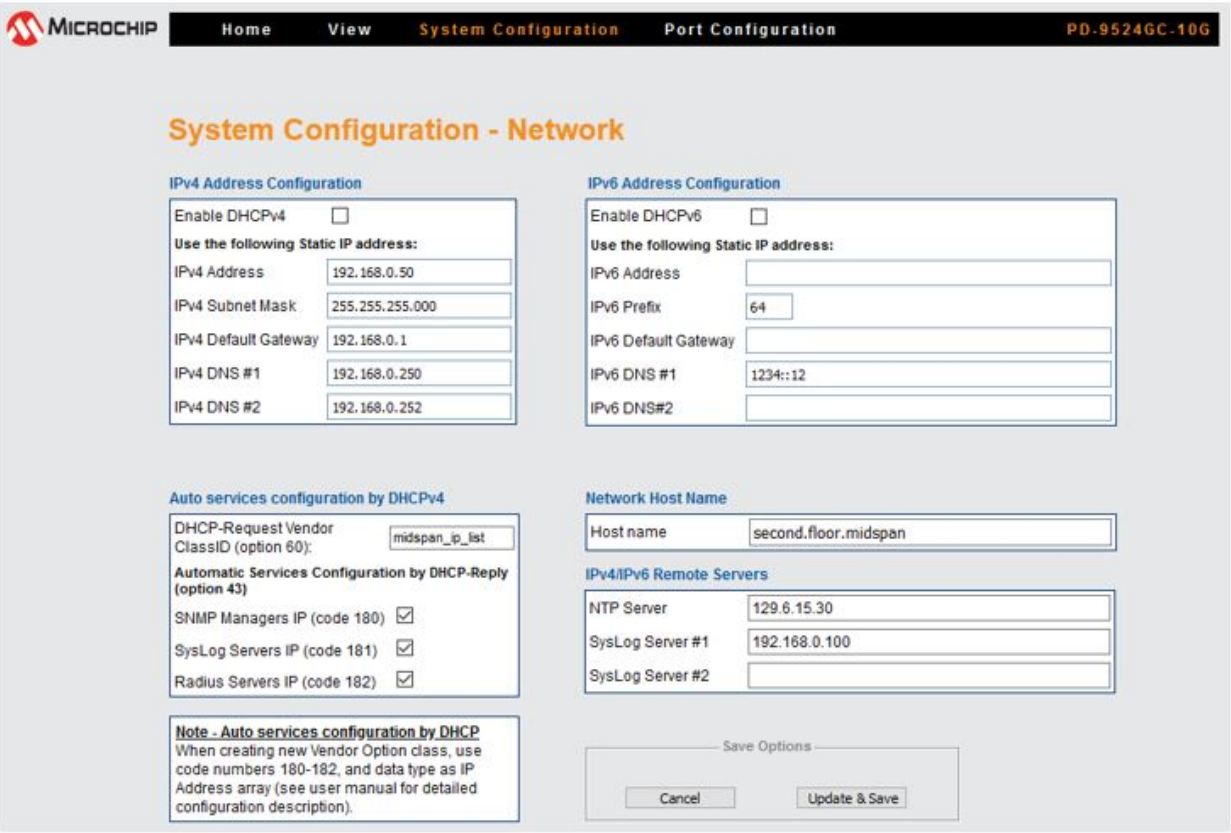


Figure 3-32. Setting SNMP Manager IP List



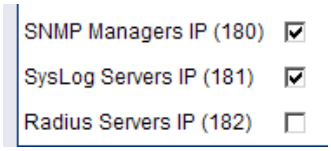
Setting Midspan Automatic Service Configuration: After configuring the DHCP server to advertise the SNMP Manager, SysLog servers, and RADIUS server lists, configure which Midspan network services must be configured dynamically, and which ones must use Midspan static configuration. SNMP Manager IP list and SysLog IP are updated dynamically by the DHCP server. The Radius servers IP list is not updated even if it advertised by the DHCP server. Check Obtain IP by DHCP checkbox and click the **Update & Save** option, as shown in Figure 3-33.

Figure 3-33. Midspan Automatic Service Configuration



Notes:

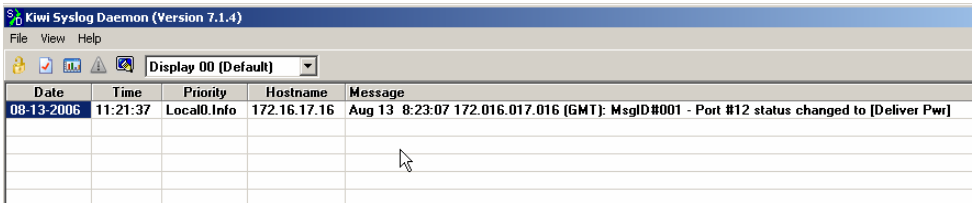
- All IP addresses obtained by the Auto Service Configuration by DHCP are saved even after the Midspan DHCPv4 option is disabled.
- Checking the SNMP, SysLog, or RADIUS has no effect, if DHCPv4 is disabled.



3.3.5.3 Log Server

The Midspan can send various internal event reports to an external IPv4/IPv6 host running SysLog daemon application (see Figure 3-34), which logs those events for future use. For an example of a similar IPv4 SysLog server application, visit kiwisyslog.com.

Figure 3-34. Syslog Server Log Events



SysLog messages are sent when the SysLog server's IP field is other than 0.0.0 or none empty string. The following events might be sent by the Midspan:

- System UP
- Port status has changed (PoE port was changed to another RFC3621 SNMP MIB port state).

- Midspan delivers power above xy% threshold.
- Midspan delivers power less then xy% threshold (after exceeded power message was sent).
- Remote user tries to access web view pages using an incorrect username or password.
- Remote user tries to access web configuration pages using incorrect username or password.
- Remote user tries to post web form using incorrect username or password.
- Unit is restored to factory default values.
- Unit configuration is changed.
- PoE controller reset is detected.
- Remote Telnet/SSH user fails to login (incorrect username or password).
- Remote Telnet/SSH/Web user is rejected by RADIUS Server (incorrect username or password).
- Remote Telnet/SSH/Web user is rejected, as there is no reply from primary and secondary RADIUS server.
- Remote Telnet/SSH/web user gets viewing access privilege from remote RADIUS server, while trying to access configuration section.
- Weekly schedule override key is inserted.
- Weekly schedule override key is removed.
- Remote UPS operates on battery.
- Remote UPS is switched back to AC.
- Maximum delivered power by Midspan is changed by remote SNMP manager or UPS dynamic power management algorithm.
- Internal power source failure. External power source is in use.
- Internal power source is restored.
- External power source failure.
- External power source is restored.
- Midspan is connected to incompatible Power-Backup source type. Turn off the unit and disconnect it.

Note: Each SysLog message contains a message date and time (GMT). The Midspan acquires date and time from the network NTP server.

3.3.5.4 NTP Server

When a valid NTP server IPv4/IPv6/NTP-server-hostname is configured, the Midspan acquires date and time (GMT) from the network NTP server. When no valid IP is set, or when Midspan fails to acquire time from the NTP server, initial Midspan time is set to 1/1/2005 as default.

3.3.6 System Configuration SNMP

The Unit's SNMP agent (v1/v2/v3) can be accessed either by IPv4 or IPv6. It enables a remote SNMP management station to monitor and configure the unit as per RFC3621 (enable/disable PoE ports, view total power consumption, and so on) and view MIB-II network statistics. The Private MIB extends PoE functionality beyond the RFC3621 PoE MIB. For example:

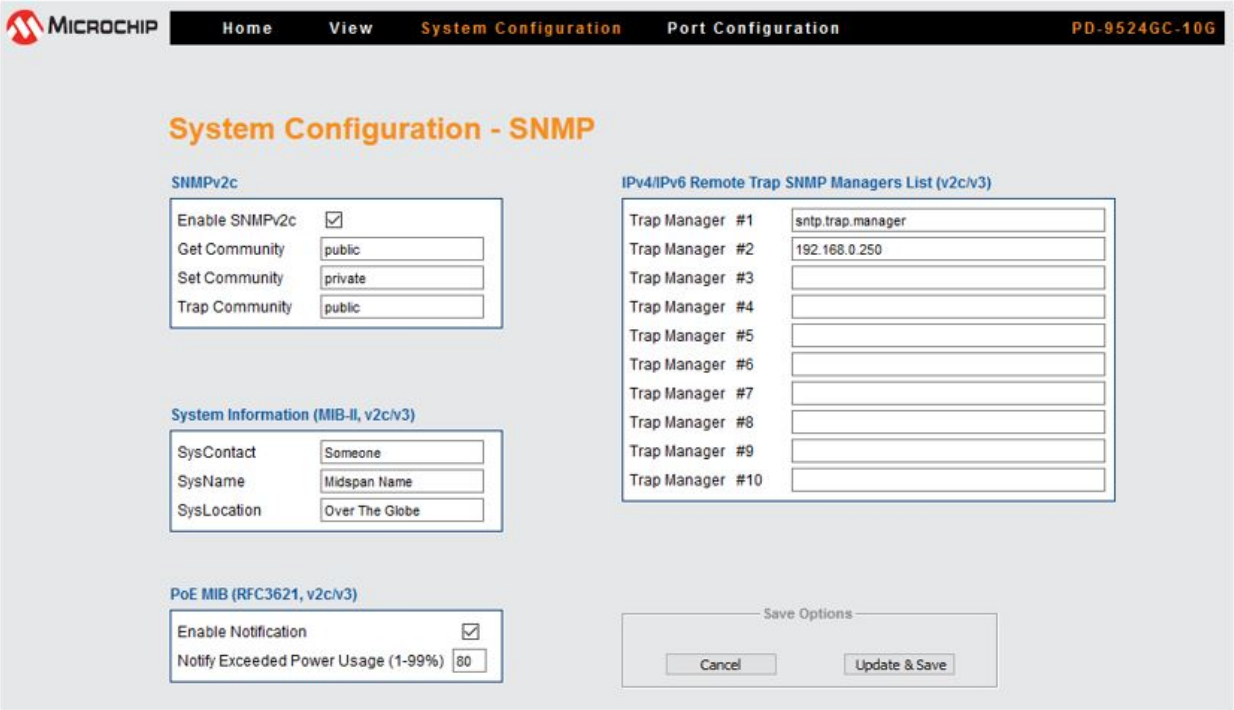
- Set each individual PoE port maximum power.
- Read each individual port current power.
- Limit entire Midspan maximum power.

The SNMPv3 offers a secured method for accessing the Midspan, both for configuration and monitoring. SNMP network packets might be authenticated by MD5 and encrypted by DES.

The System Configuration SNMP screen enables configuration of SNMP parameters common to both SNMPv1/v2 and SNMPv3 (SNMPv1/2 community string is the only exception). The following parameters can be configured, as shown in Figure 3-35:

- SNMPv1/v2c Community Strings.
- MIB-II System Information.
- Remote Trap SNMPv2c/v3 Managers List.
- RFC3621 PoE MIB partial configuration parameters.

Figure 3-35. System Configuration SNMP Screen



3.3.6.1 SNMPv2c

The SNMPv2c feature enables or disables an SNMP agent to respond to SNMPv1/v2c get/set commands, generated by a remote SNMP Management station, such as HP OpenView, IBM Tivoli, and so on.

Community strings—Get/Set/Trap community strings are SNMP passwords. To enable remote SNMP manager communication with the device, you must configure its community strings to match those of the Midspan. Community Strings window enables configuration of the following parameters:

Figure 3-36. SNMPv2 Window

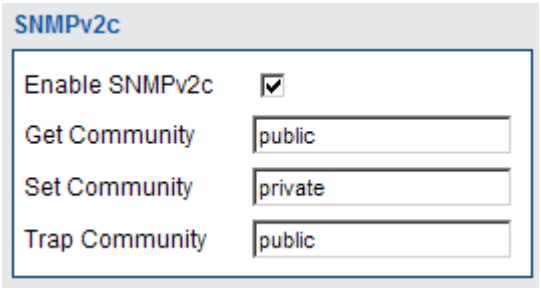


Table 3-8. SNMPv2 Field Details

Field	Description
Enable SNMPv2c	Enable/Disable SNMPv1/v2c agent.
Get community	Password to be used by remote SNMP NMS station for SNMP GET commands.
Set community	Password to be used by remote SNMP NMS station for SNMP SET commands.
Trap community	Each TRAP sent by the Midspan to remote NMS managers contains a Trap community string password. It must match remote SNMP NMS managers password. Otherwise, it is discarded by the SNMP manager.

3.3.6.2 System Information (MIB-II, v2c/v3)

The following table lists the configurations enabled by the System Information window:

Table 3-9. System Information Window

Button/Checkbox	Description
SysContact	SNMP MIB-II 1.3.6.1.2.1.1.4: Textual identification of the contact person for this managed node, joined by information on how to contact this person.
SysName	SNMP MIB-II 1.3.6.1.2.1.1.5: Textual identification of an administratively-assigned name for current managed node.
SysLocation	SNMP MIB-II 1.3.6.1.2.1.1.6: Textual identification of the physical location of current node.

3.3.6.3 PoE MIB (RFC3621, v2c/v3)

The following table lists the configuration of two major RFC3621 PoE MIB parameters simplified by the PoE MIB window:

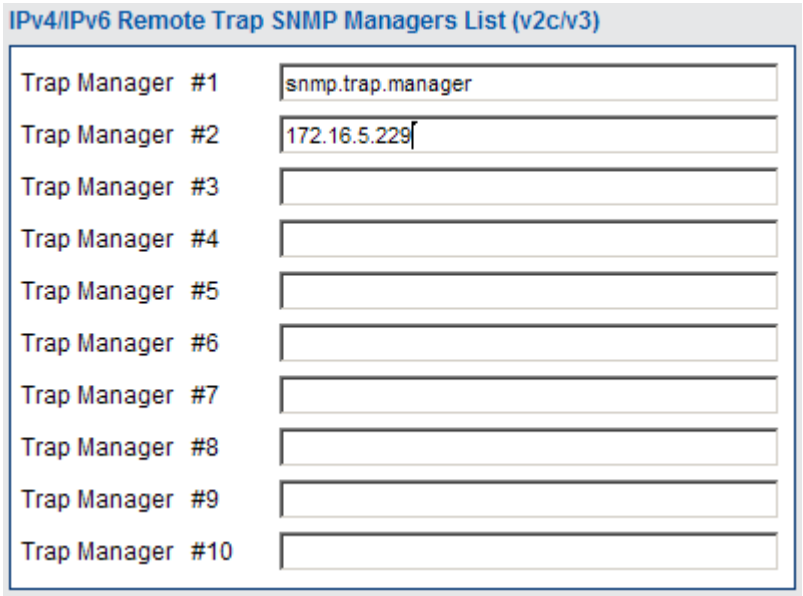
Table 3-10. RFC3621 PoE MIB Parameters

Button/Checkbox	Description
Enable Notification	Allows/Prohibits unit from sending RFC3621 PoE traps (both SNMPv2c and SNMPv3).
Notify Exceeded Power Usage (1%–99%)	If Enable Notification option is checked, Midspan sends a trap whenever total power consumption exceeds xy%.

3.3.6.4 Remote Trap SNMP Managers List

This window enables configuration of up to 10 remote IPv4/IPv6 SNMP managers, as shown in Figure 3-37. When Midspan must send a trap message, the trap is duplicated and sent by the Midspan to all the remote SNMP managers (when both SNMPv2c and SNMPv3 are set, each trap is sent twice, once by SNMPv2c and once by SNMPv3).

Figure 3-37. Remote Trap SNMP Managers List

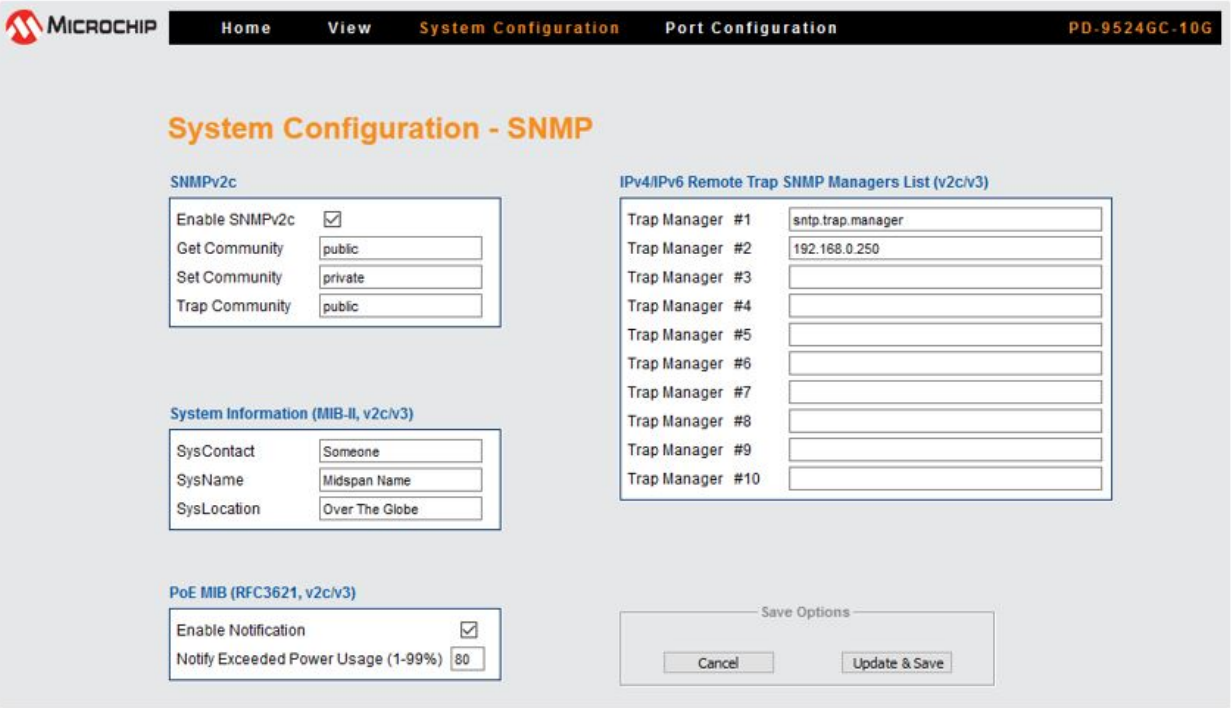


Button	Description
Update & Save	Updates Midspan functionality per the new configuration. All SNMP parameters become effective only after this button has been clicked.
Cancel	Cancels current operation and restores previous values.

3.3.7 System Configuration SNMPv3

The System Configuration SNMPv3 menu (Figure 3-38) enables configuration of three different SNMPv3 user types and notification (trap), which requires similar parameters as any other SNMPv3 user.

Figure 3-38. System Configuration SNMPv3 Screen



- **Enable/Disable SNMPv3**: Enables/disables SNMPv3 agent to respond to SNMPv3 GET/SET messages sent by remote SNMP management station.
  Note: SNMPv3 works independently from SNMPv2c.
- **Guest User**: Enables read only access to the MIB-II System OID tree. It must be used by SNMP managers who prefer not to expose their real username and password to pool the device for "keep alive" reports. A guest user has no authentication or privacy (encryption) ability.
- **View User**: Has read only (GET) access to all SNMP branches but cannot perform any modifications (SET).
  - User Name: SNMPv3 user (mandatory field).
  - Authentication Password (MD5): Applicable when MD5 or MD5+DES are being used.
  - Privacy Password (DES): Applicable only when MD5+DES are being used.
  - Authentication + Encryption: Enables selection of one of the following three security levels:
    - None: SNMPv3 packets are neither authenticated nor encrypted.
    - MD5: SNMPv3 packets are authenticated but not encrypted.
    - MD5+DES: SNMPv3 packets are authenticated and encrypted.
- **Admin User**: Has full reading (GET) and writing (SET) access to all SNMP branches.
  - User Name: SNMPv3 user (mandatory field).
  - Authentication Password (MD5): Applicable when MD5 or MD5+DES are being used.

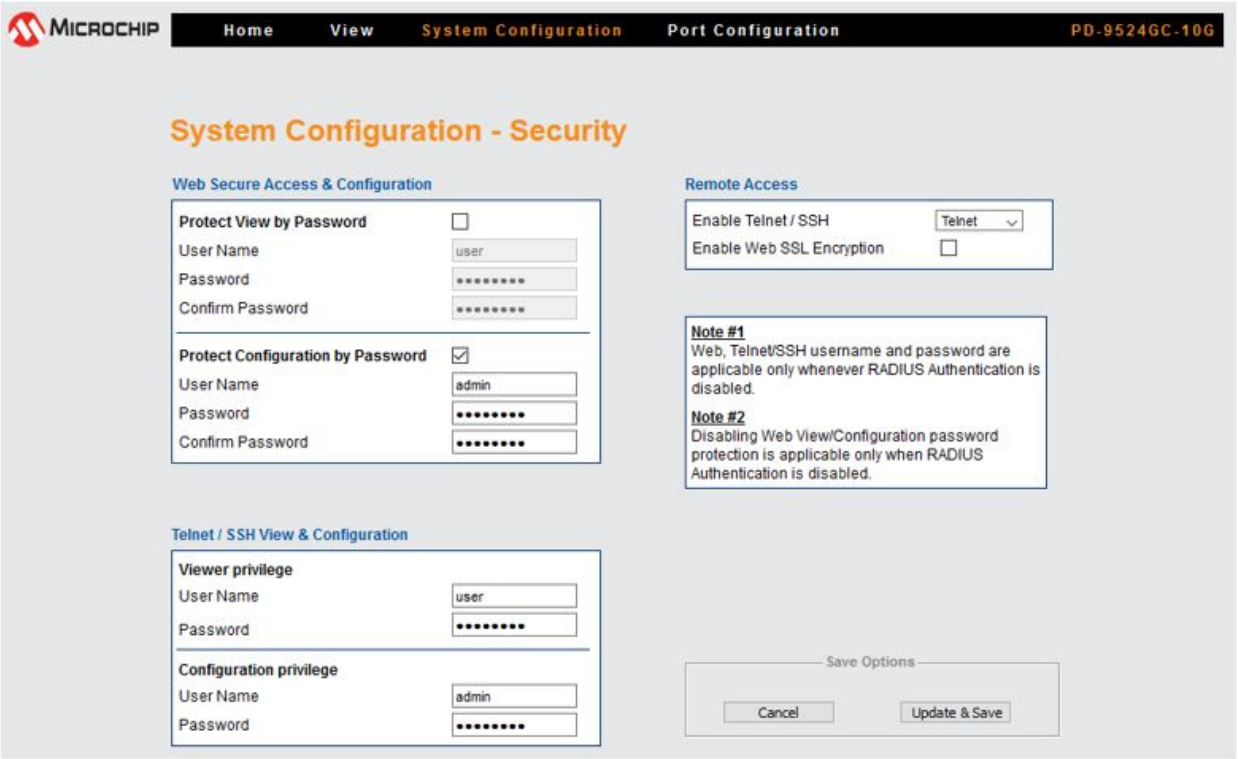
  - Privacy Password (DES): Applicable only when MD5+DES are being used.
  - Authentication + Encryption: Enables selection of one of the following three security levels:
    - None: SNMPv3 packets are not authenticated or encrypted.
    - MD5: SNMPv3 packets are authenticated but not encrypted.
    - MD5+DES: SNMPv3 packets are authenticated and encrypted.
- **Notification Trap**: SNMPv3 trap configuration parameters are identical to SNMPv3 user.
  - User Name: SNMPv3 user (mandatory field).
  - Authentication Password (MD5): Applicable when MD5 or MD5+DES is being used.
  - Privacy Password (DES): Applicable only when MD5+DES is being used.
  - Authentication + Encryption: Enables selection of one of the following three security levels:
    - None: SNMPv3 packets are not authenticated and neither encrypted.
    - MD5: SNMPv3 packets are authenticated but not encrypted.
    - MD5+DES: SNMPv3 packets are authenticated and encrypted.

3.3.8 System Configuration Security

Figure 3-39 shows configuration of the following parameters that are enabled by the System Configuration Security menu:

- Web Secure Access and Configuration
- Telnet/SSH View and Configuration
- Remote Access

Figure 3-39. System Configuration Security Screen



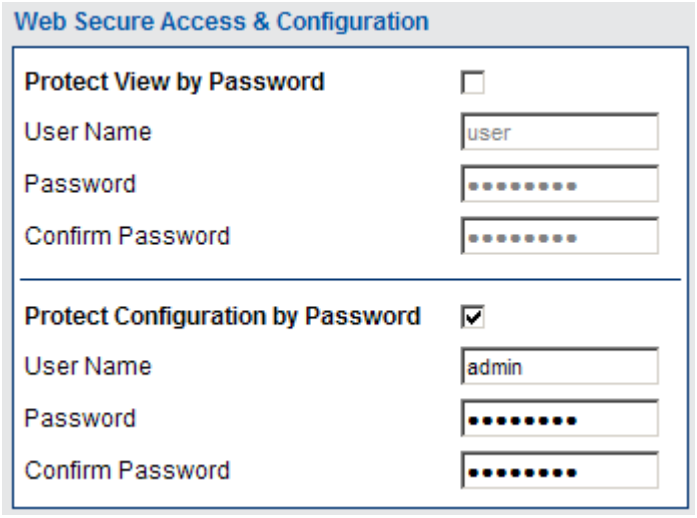
3.3.8.1 Web Secure Access and Configuration

Web pages are divided into the following two sections:

- **View**: View web pages provide status reports and configuration summaries, without being able to change configuration.
- **Configuration**: Configuration web pages (under System Configuration and Port Configuration) enable the user to view and modify the Midspan configuration.

View web pages and Configuration web pages use different passwords. View user name and password provides access only to View web pages, while configuration user name and password provides access both to View and Configuration web pages, as shown in the following figure.

Figure 3-40. Web Secure Access and Configuration Window



Note: Disabling web view/configuration password protection is applicable only when RADIUS authentication is disabled.

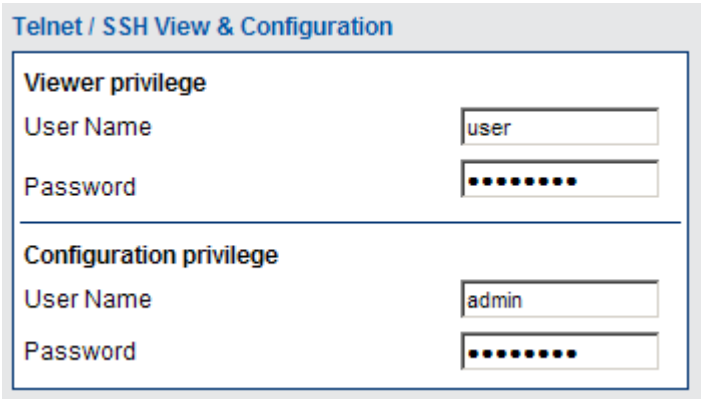
3.3.8.2 Telnet/SSH View and Configuration

The Telnet/SSH remote terminal are always password protected.

The Telnet/SSH menu is divided into Viewer privilege and Configuration privilege submenus (see Figure 3-41).

- **View privilege:** Can view Telnet/SSH text menus, but is rejected when tries to access the Configuration text menus.
- **Configuration privilege:** Can access both View and Configuration text menus.

Figure 3-41. Telnet/SSH View and Configuration Window



Note: Web and Telnet/SSH user name and password are applicable only in cases where RADIUS authentication is disabled.

Figure 3-42. Remote Terminal View Menu Example

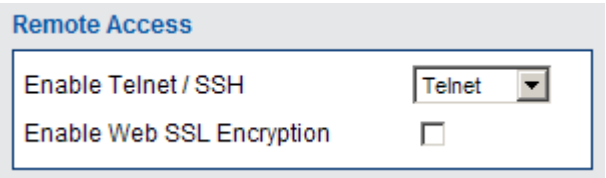
```
      View Menu
-----------------------------
1.  View PoE ports status
2.  View network parameters
3.  View ACL (Access List) filter parameters
4.  View time & system up time
5.  View application & Boot software version


ESC - Return to previous menu
```

Figure 3-43. Remote Terminal Configuration Menu Example

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

3.  Download configuration file from TFTP Server (reset only Manager module)
4.  Upload configuration file to TFTP Server
5.  Download WEB SSL Certificate from TFTP Server (reset only Manager module)
6.  Software update menu

7.  Turn RADIUS,ACL Filter off. Restore all user & password to factory default
8.  Restore unit to factory default (excluding IP configuration)

9.  Reset Manager module
A.  Reset unit

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


ESC - Return to previous menu
```

3.3.8.3 Remote Access

Figure 3-44. Remote Access Window



- **Enable Telnet/SSH/None**: Enables/disables remote IPv4/IPv6 terminal access by Telnet, SSH, or none of them.
- **Enable Web SSL Encryption**: When checked, it enables encryption of web pages between remote web client and an on-board web server.

Note: Due to Web Browser Web pages caching, whenever the Web SSL encryption method (encrypted/non-encrypted) is changed, the Web browser must be closed and re-opened.

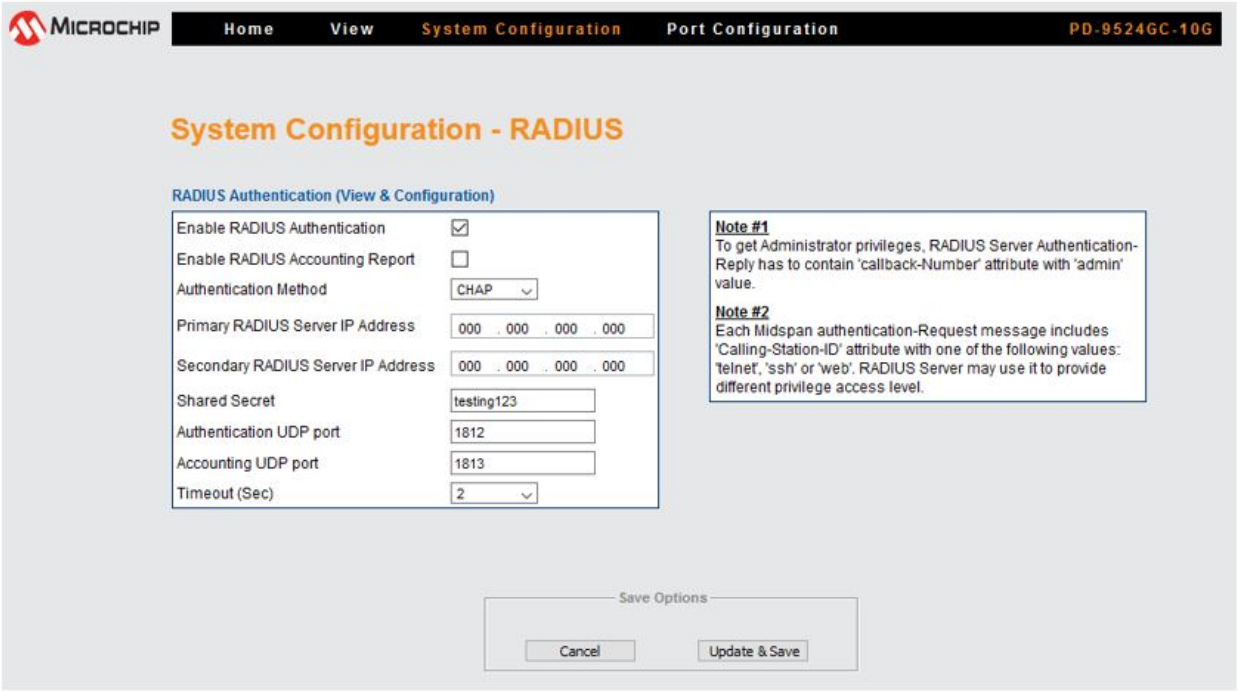
Button	Description
Update & Save	Updates Midspan parameters and saves configuration. All Remote Access parameters become effective only after this button has been clicked.
Cancel	Cancels current operation and restores previous values (when **Update & Save** option is not clicked).

3.3.9 System Configuration-RADIUS

Whenever the IPv4 RADIUS client is enabled (see Figure 3-45), the remote Web/Telnet/SSH user name and password are sent to the RADIUS server for authentication purposes. The RADIUS server can provide the user with a viewer access level, administrator access level, or reject the remote user.

Note: Any invalid activity (for example, user is rejected, user tries to access the configuration section, and so on) is reported to the SysLog server.

Figure 3-45. RADIUS Configuration Screen



- **Enable RADIUS Authentication**: When checked, all remote Telnet/SSH/web users are authenticated by the RADIUS server.
  Note: To deactivate RADIUS if it is enabled while configured incorrectly, connect to Midspan serial port (38400 baud), and select the **Turn RADIUS, ACL Filter off. Restore all user and password to factory default** option from configuration menu.
- **Enable RADIUS Accounting Report**: When enabled (checked), the Midspan sends an accounting report whenever users log in or log out of the remote web/Telnet/SSH occurs.
  Note: The accounting report can be enabled only if RADIUS Authentication is enabled.
- **Authentication Method**: Determines if the remote user, user name, and password are sent to the RADIUS server through PAP or CHAP (more secure).
- **Primary and Secondary RADIUS Server IP Address**: IP address of the RADIUS server. If there is no reply from the primary RADIUS server after three retries, the same authentication request is sent to the backup RADIUS server.
- **Shared Secret**: The same string must be configured both in the RADIUS server and the Midspan RADIUS client.
- **Authentication UDP Port**: Must not be changed, unless a RADIUS server which utilizes UDP port 1645 is used.
- **Accounting UDP Port**: Must not be changed, unless a RADIUS server which utilizes UDP port 1646 is used.
- **Timeout**: Time (in seconds) the Midspan RADIUS client waits for a reply from the RADIUS server before resending a request.
  Note: The Midspan RADIUS client retries up to three times before accessing the backup RADIUS server. For example, if timeout equals to two seconds, the backup server is accessed only after six seconds.

3.3.9.1 Configuring RADIUS Server to Provide Privileged Access to Viewer/Administrator

To get administrator privileges, the RADIUS Server Authentication reply must contain a 'Callback-Number' attribute with an 'admin' value. Failing to do so results in providing viewing access privilege only.

3.3.9.2 How to Differentiate Between Telnet/SSH/Web RADIUS Users

Each Midspan authentication-request message includes a 'Calling-Station-ID' attribute with one of the following values: 'telnet', 'ssh' or 'web'. The RADIUS server might use this attribute to differentiate between Telnet/SSH/Web remote RADIUS users by providing different privilege access levels.

Note: Whenever RADIUS authentication is enabled, Web users are authenticated regardless of whether the Web username and password validation was unchecked (disabled) or not.

3.3.10 System Configuration—Dynamic UPS Power Management

Dynamic UPS power management, as shown in Figure 3-46, enables extending UPS operation time whenever power failure occurs, by monitoring the UPS battery level. Whenever the battery level starts to decline, the Midspan automatically starts shutting down low priority ports to save overall power consumption, which in turn extends the operation of critical PD devices by extending UPS operation time.

Figure 3-46. Dynamic UPS Power Management

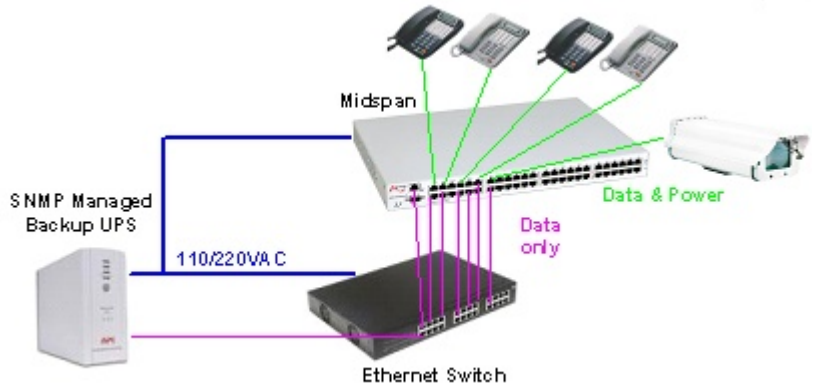
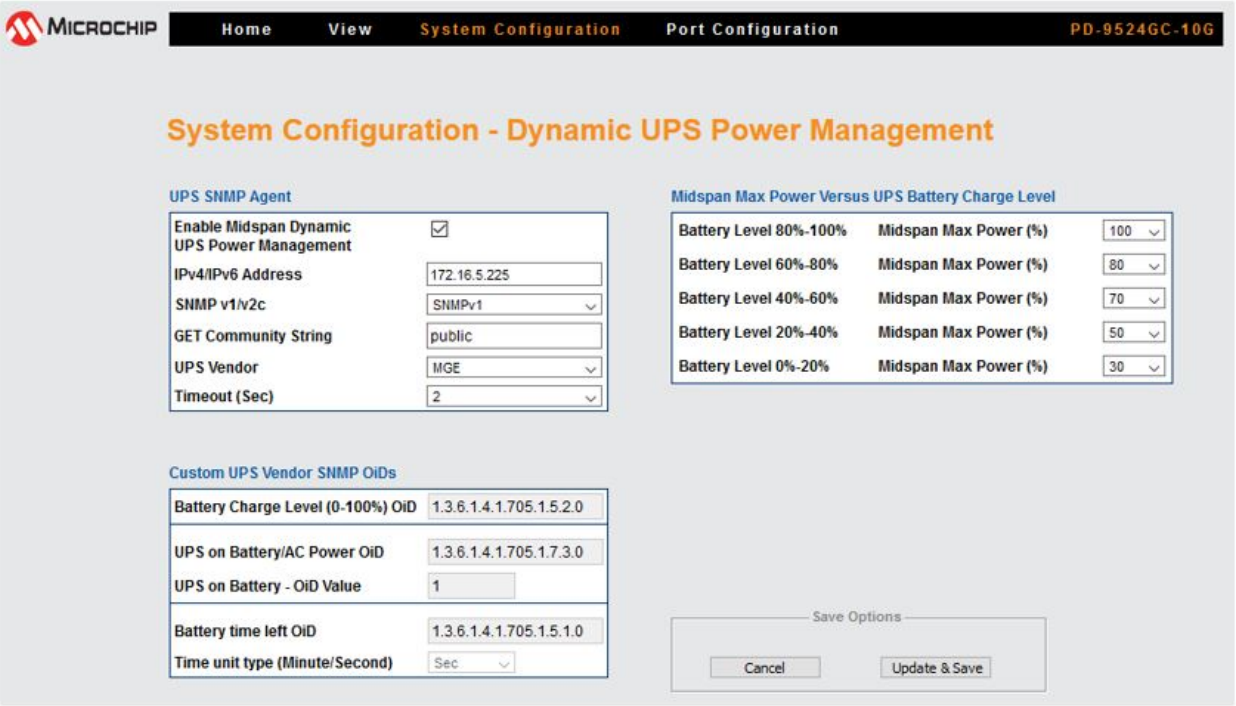


Figure 3-47 shows the following parameters that must be set by the user:

- UPS SNMP Agent network parameters.
- Vendor Specific SNMP parameters.
- Maximum provided power versus UPS battery level.
- When Dynamic UPS Power Management configuration is enabled, the **View > Status** screen provides information related to the UPS status (battery level, UPS operates on AC/Battery, UPS Battery remaining time).

Note: Users must not use SNMP private MIB mainPowerUsageBudget OID to make changes while Dynamic UPS Power Management is enabled.

Figure 3-47. Dynamic UPS Power Management Screen



In a typical Dynamic Power Management configuration, PoE ports priority and power limit must be set. Whenever battery level drops below 80%, 60%, 40%, and so on (main power failure), the Midspan automatically starts to shut down pre-defined low priority PoE ports. This is done to reduce UPS power consumption. The deactivated ports are marked by blinking green LED, which are located on top of each port. The same report can be seen from remote by browsing to the Midspan unit and accessing View System Status Web page.

Note: SysLog reports and SNMP traps are sent per each deactivated PoE port.

3.3.10.1 UPS SNMP Agent

- **Enable Midspan Dynamic UPS Power Management**: Enables/Disables Midspan monitoring of remote UPS over the network by sending IPv4/IPv6 SNMP GET messages.
- **IPv4/IPv6 Address**: IPv4/IPv6 address of the UPS SNMP agent.
- **SNMP Type**: Midspan uses either SNMPv1 or SNMPv2c to communicate with the UPS SNMP agent.
- **GET Community String**: Must be identical to the community string set for the UPS SNMP agent.
- **UPS Vendor**: For APC and MGE UPS vendors, there is no need to define a dedicated SNMP Object's ID to be used to communicate with the UPS. If another vendor is used, select the '*custom'* option, and manually type in the SNMP Object IDs to be used.
  Note: Whenever APC or MGE UPS vendors are selected, the Custom UPS Vendor SNMP OIDs section is dimmed. It is active only whenever the 'custom' option is selected.
- **Timeout**: The time for which the Midspan waits for a reply from the UPS SNMP agent before retrying again.

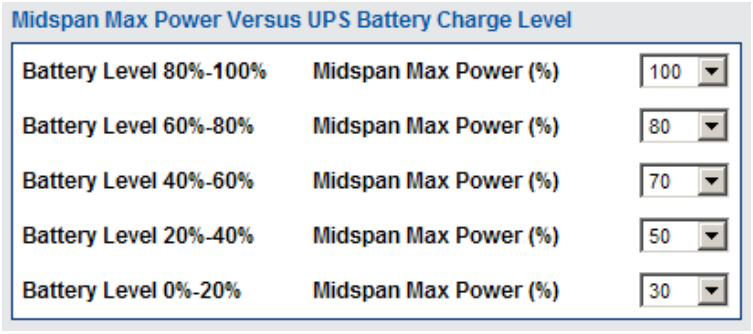
3.3.10.2 Custom UPS Vendor SNMP OIDs

- **Battery charge level (0%–100%) OID**: An SNMP object ID that provides battery charge percentage level (100% = battery fully charged).
- **UPS on battery/AC OID**: SNMP object ID that reports if the UPS operates on an AC/battery.
- **UPS on battery OID value**: Used by the Midspan to properly interpret UPS on AC/Battery returned value.
  Note: Any other returned value is considered as if the UPS works on AC.
- **Battery time left OID**: An SNMP object ID that provides the amount of UPS battery time remaining.
- **Time unit type (minute/second)**: Selected time units (seconds, minutes, or time ticks) for the Timeout parameter.

3.3.10.3 Midspan Max Power vs. UPS Battery Charge Level

- For each 20% drop in battery level, users might limit the maximum power allocated by the Mid span, as shown in the following figure. 100% power applies to Midspan maximum power when operated on AC.

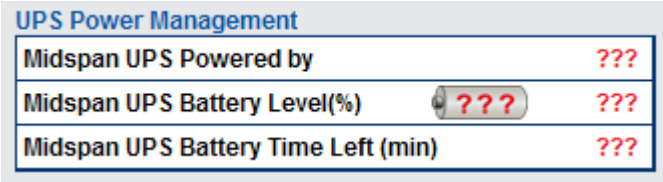
Figure 3-48. Midspan Enforced Maximum Power Levels



Notes:

1. The user must make sure that the Midspan and the Ethernet switch are connected to an AC power source through UPS.
2. After configuring, the user must verify that the Midspan communicates with the UPS over the network. This is performed through the **View > Status** page; the UPS Power Management window appears on the screen with the relevant UPS information.
3. If UPS-Midspan communication fails, the screen below with '???' marks appear, as shown in the following figure.

Figure 3-49. UPS-Midspan Communication Failure

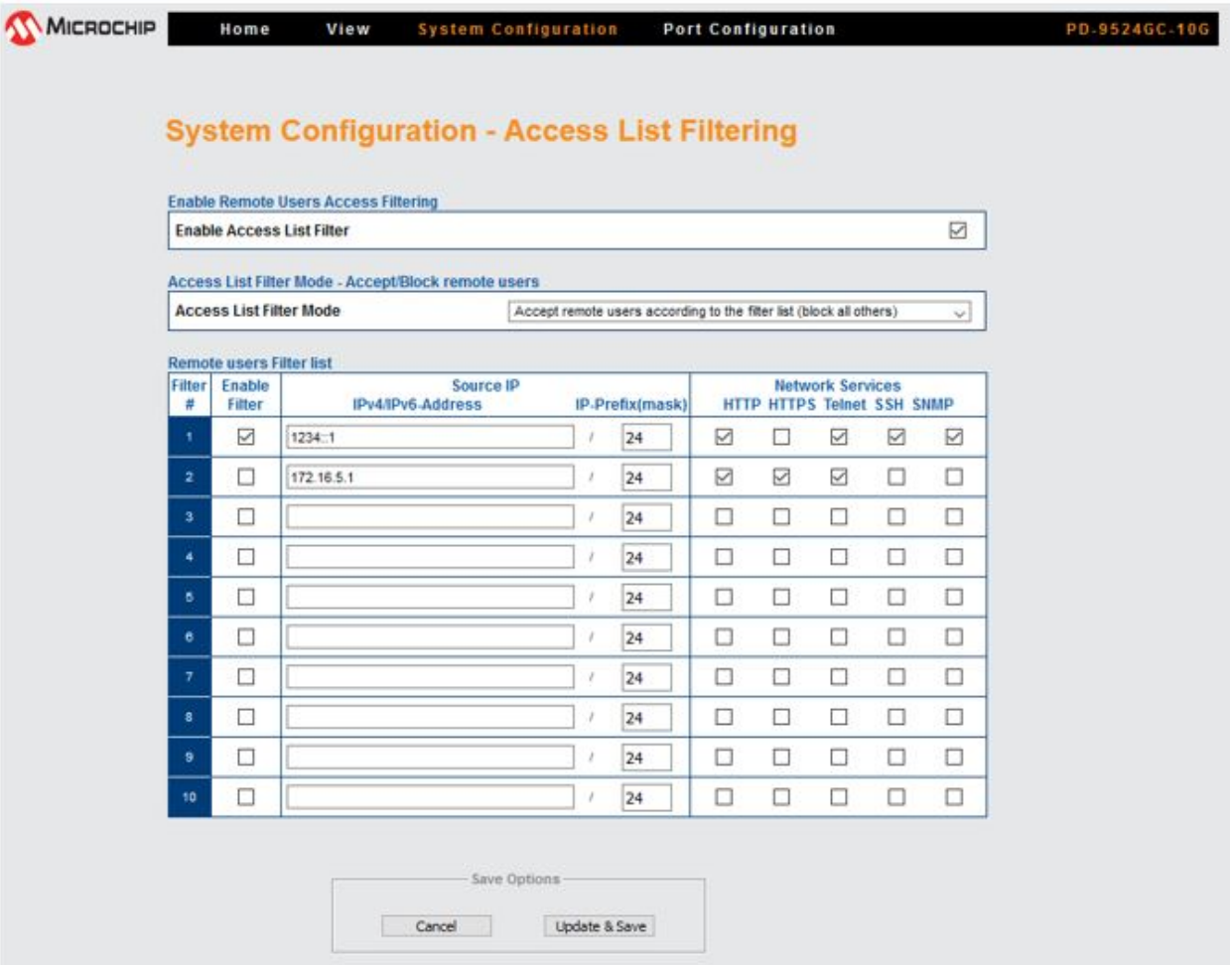


3.3.11 System Configuration-Access List Filter

ACL filter enables configuring which remote networks or even remote users can manage the Midspan over the network.

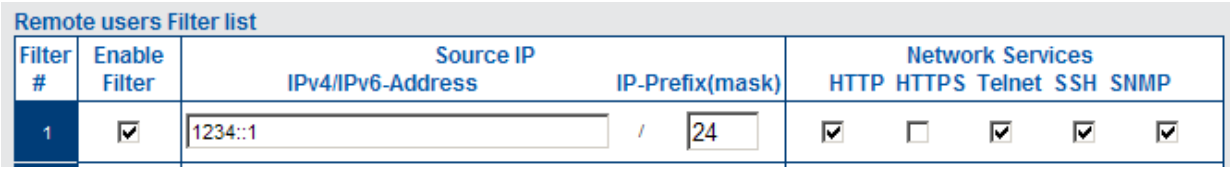
Note: The ACL filter filters (block/forward) only HTTP/HTTPS/Telnet/SSH/SNMP traffic. All other network traffic as DHCP, Ping, ARP, and so on, is handled the same regardless if the ACL filter is enabled or disabled.

Figure 3-50. Access List Filtering



- **Enable Access Filter**: Enable/Disable Access List Filter functionality
- **Access List Filter Mode**:
  - Accept remote users according to the filter list (block all others): Accepts only remote users, which comply with one or more ACL filters. All other remote users are blocked.
  - Block remote users according to the filter list (allow all others): Accepts all remote users excluding the remote users which comply with one or more ACL filters.
- **Remote Users Filter List**:

  Figure 3-51. Access List Filtering



  A user can configure up to ten ACL filters. The IPv4/IPv6 -Address, plus IP-Prefix (mask), controls the size of the IP network which is affected by these filter settings. IP-Prefix is equivalent to IP-Mask. For example, IP-Prefix 24 = 255.255.255.0, IP-Prefix 16 = 255.255.0.0.

Each filter can be configured to affect one or more of the following network protocols:

- HTTP
- HTTPS
- Telnet

- SSH
- SNMP

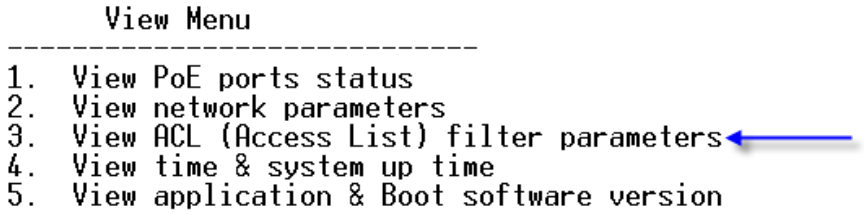
The filter configuration does not affect any other network traffic.

Field	Description
Enable Filter	Enable/Disable one out of ten ACL filters.
Source IP: IP-Address	IPv4/IPv6-Address or IPv4/IPv6-Net to be affected by this ACL filter.
Source IP: IP-Prefix	IPv4-Prefix (1–32) or IPv6-Prefix (1–128) controls the range of VIPs that are affected by this filter setting. Example: 32 (255.255.255.255) = Single IP address 24 (255.255.255.0) = 256 IP address
Network Services: HTTP	Enable/Disable ACL filter from filtering remote user HTTP (Web) access.
Network Services: HTTPS	Enable/Disable ACL filter from filtering remote user HTTPS (Web) access.
Network Services: Telnet	Enable/Disable ACL filter from filtering remote user Telnet access.
Network Services: SSH	Enable/Disable ACL filter from filtering remote user SSH (secure Telnet) access.
Network Services: SNMP	Enable/Disable ACL filter from filtering remote user SNMPv1-v3 access.

3.3.11.1 ACL Filter Statistics

The ACL statistics can be accessed through the View menu. The View menu is accessible by serial/Telnet/SSH interface, as shown in the following figure.

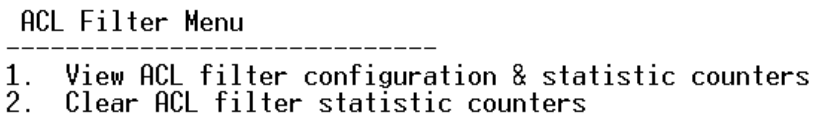
Figure 3-52. View ACL Filter Parameters from View Menu



ACL filter menu options are as follows:

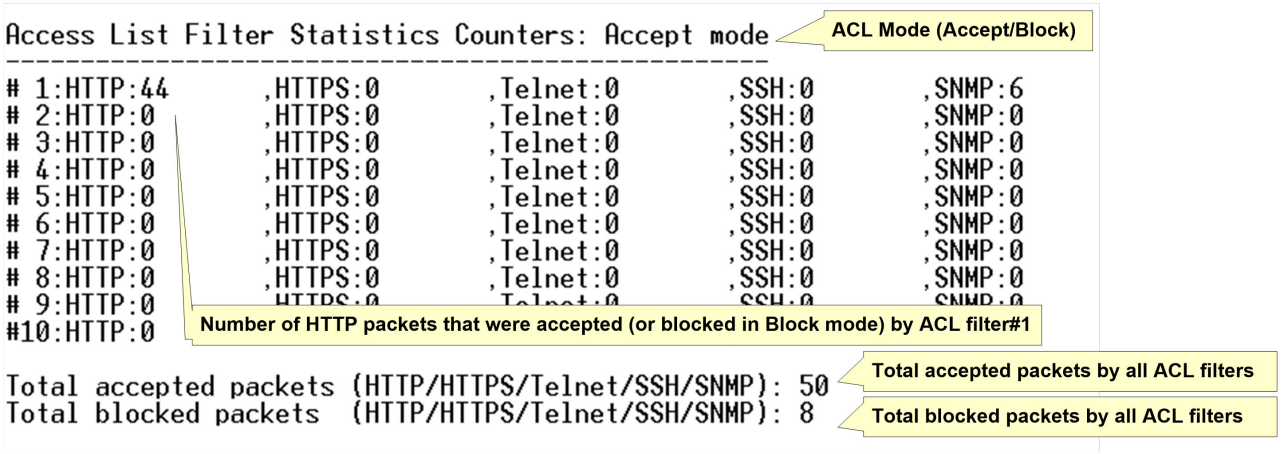
- View ACL filter configuration & statistic counters: Displays ACL filter statistics counters.
- Clear ACL filter statistic counters: Clears ACL filter statistics counters.

Figure 3-53. View ACL Filter Parameters



ACL statistics offers easy ACL configuration verification by reporting how many packets are accepted (or blocked in Block mode) by each ACL filter and by which network protocol (HTTP, HTTPS, Telnet, SSH, or SNMP).

Figure 3-54. View ACL Filter Statistics Counters



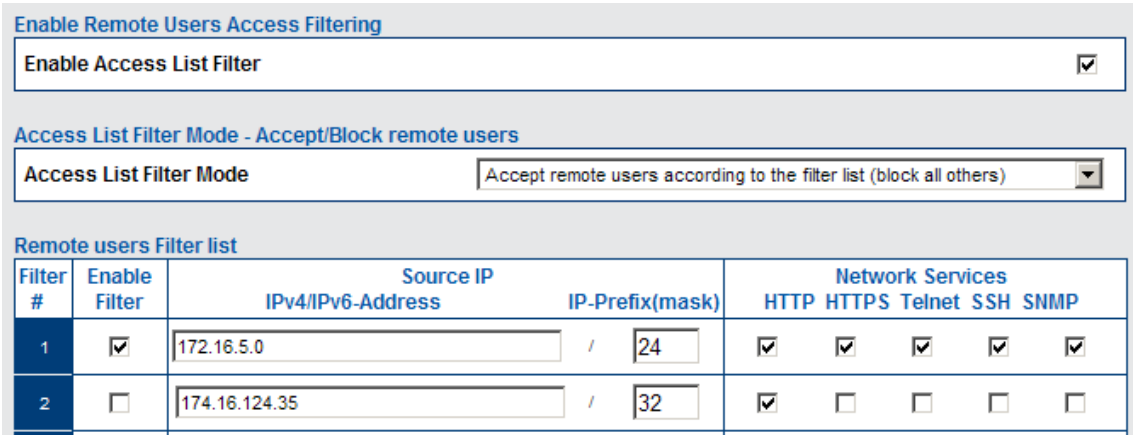
3.3.11.2 ACL Filter Configuration Example

Following are the ACL filter example filtering requirements:

- Enable the Midspan to be fully managed only from IP-network 172.16.5.0-172.16.5.255.
- Limit remote user with IP 174.16.124.35 to manage the Midspan only by HTTP (Web) Solution:

The following figure shows the required settings for complying with the preceding ACL filter requirements.

Figure 3-55. ACL Filter Configuration Example



Notes: If Midspan network connectivity is lost due to incorrect ACL filter configuration, connect to Midspan through serial port (38400 baud) and select one of the following options from the configuration menu:

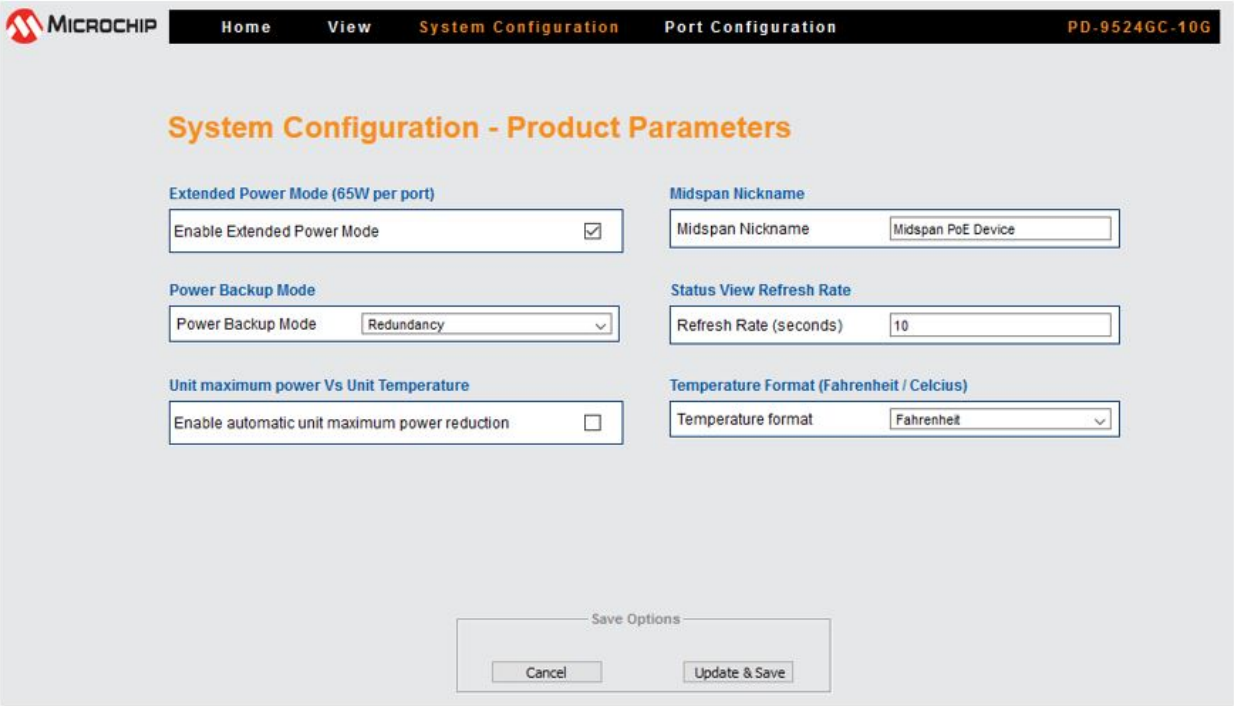
- Turn RADIUS and ACL filter off. Restore all users and passwords to factory default—turn off ACL without changing unit configuration.
- Restore the unit to factory default. Keep IP configuration unchanged—turn off ACL filter as part of restoring the unit to factory default configuration (without modifying IP configuration).

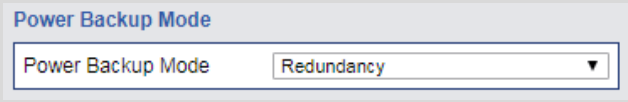
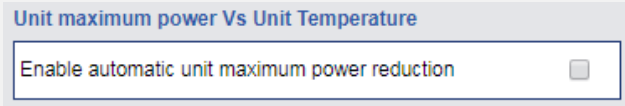
3.3.11.3 System Configuration-Product Parameters

Figure 3-56 shows the following product parameters set by the user:

- Extended Power Mode
- Power Backup Mode
- Unit maximum power versus Unit Temperature
- Midspan Nickname
- Status View Refresh Rate
- Temperature Format (Fahrenheit/Celsius)

Figure 3-56. System Configuration Product Parameters Screen



Button	Description
	Extends PD classification maximum power beyond 2 x 802.3AF+AT+BT (for example, 90W to 92.5W).
	External Power Backup mode: • Redundancy: In this mode, the external power source backs up the internal power supply of the Midspan. If the internal power supply fails to operate, the external source picks up the full load and all the ports continue to function normally. • Maximum Power: In this mode, the external power source offers additional power on top of the power delivered by the internal power supply. For example, if the PD-9624GC Midspan uses a 950W internal power supply, and an external power source is connected in Max Power mode (another PD-9624GC Midspan), the user-available power is 1900W (950W internal + 950W external).
	Enables the Midspan to automatically lower the maximum power that can be provided by the unit whenever internal unit temperature becomes too high (typically due to improper cooling).

.....continued

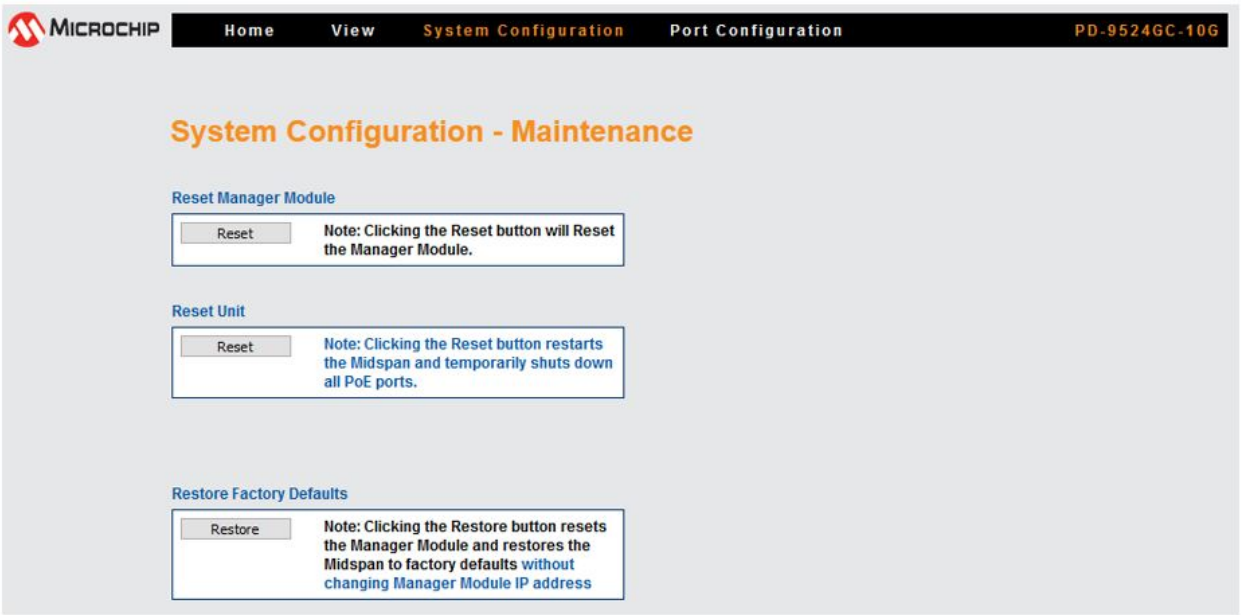
Button	Description
Midspan Nickname Midspan Nickname: Midspan PoE Device	Assists network managers to identify a Midspan by assigning a unique name for each Midspan device. Midspan nickname is displayed when browsing to **View > Status** web page, or accessing the Midspan by Serial/Telnet/SSH.
Status View Refresh Rate Refresh Rate (seconds): 10	Sets the View System Status web page refresh rate.
Temperature Format (Fahrenheit / Celcius) Temperature format: Fahrenheit	Reports the Midspan temperature in View System Status web page in Fahrenheit or Celsius.
Update & Save	Updates Midspan product-based parameters. **Note:** All product parameters become effective only after clicking this button.
Cancel	Cancels current operation and restores previous values.

3.3.12 System Configuration-Maintenance

The System Configuration-Maintenance screen offers the following options:

- Reset Manager Module
- Reset Unit
- Restoring Factory Defaults

Figure 3-57. System Configuration Maintenance Screen



Button/Checkbox	Description
Reset Manager Module Reset **Note: Clicking the Reset button will Reset the Manager Module.**	Resets only the Manager module without affecting Midspan PoE ports.
Reset Unit Reset **Note: Clicking the Reset button restarts the Midspan and temporarily shuts down all PoE ports.**	Resets the entire unit. All active PoE ports momentarily stop providing power to PoE devices (configuration is not changed).
Restore Factory Defaults Restore **Note: Clicking the Restore button resets the Manager Module and restores the Midspan to factory defaults without changing Manager Module IP address**	Restore most of Midspan's parameters to their default value (IP is not changed).

3.4 Port Configuration Screen

The Port Configuration menu enables the following (see Figure 3-58):

- **Port Configuration Enable/Disable**: Provides a quick access to enable/disable one or more PoE ports.
- **Port Configuration Detailed**: Enables detailed configuration of various PoE port values such as priority, allocated power, and port/PD description.
- **Port Configuration—Weekly Schedule**: Enables the user to configure weekly scheduled ports activation/deactivation.

Figure 3-58. Port Configuration Screen

3.4.1 Port Configuration-Enable/Disable

All ports or individual ports can be enabled or disabled in one action.

Disabled ports are marked with a red cross on the RJ45 port. For more information, see section 3.3.2.1 Ports Status Panel.

Figure 3-59. Port Configuration Enable/Disable Screen

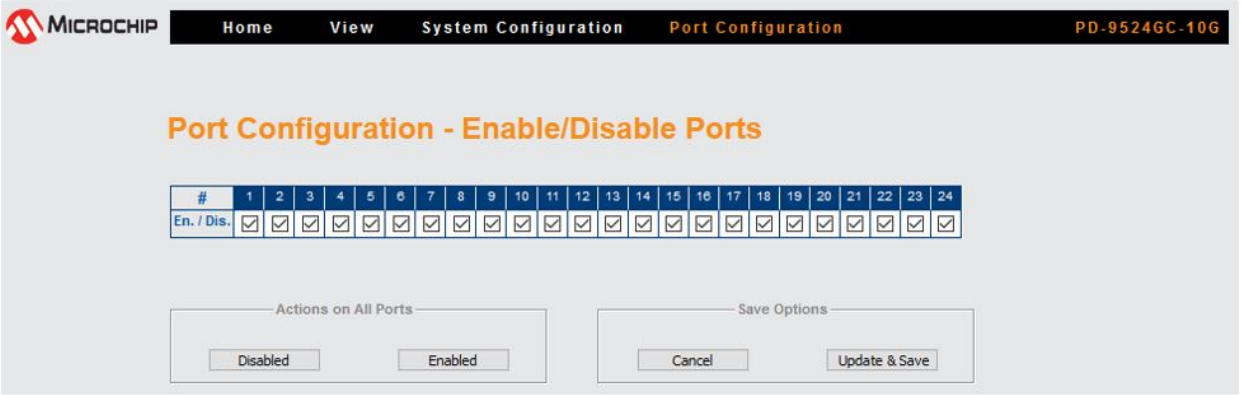
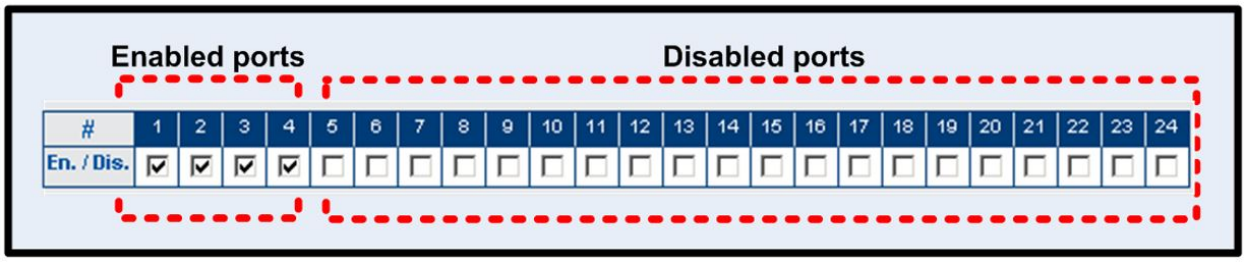
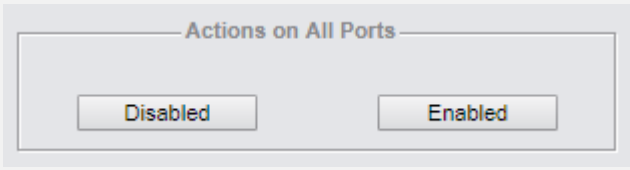
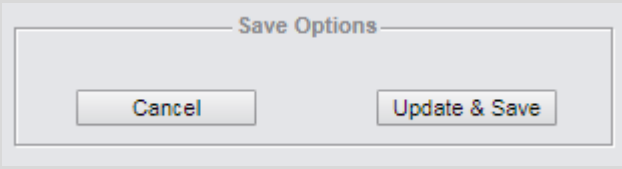


Figure 3-60. Enabled/Disabled Ports in Port Configuration



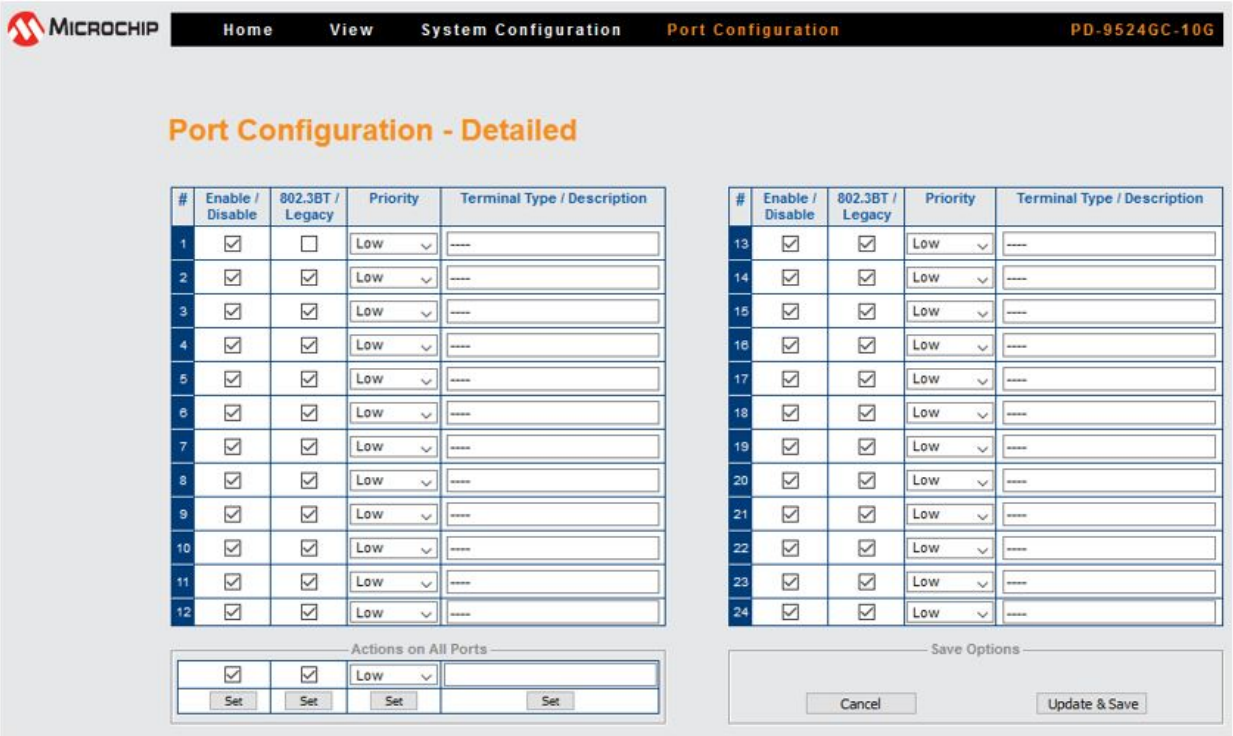
Button/Checkbox	Description
	**Enabled**: Enables all ports. **Disabled**: Disables all ports. **Note:** Only web page is affected.
	**Cancel**: Cancels current operation and restores previous values in cases where Update & Save is not clicked. **Update & Save**: Activates new setting and saves the updated configuration in cases where Midspan restarts.

3.4.2 Port Configuration-Detailed

The Port Configuration-Detailed screen controls individual ports and sets-up parameters as follows:

- Enable/Disable individual PoE ports.
- Power only IEEE 802.3bt (including af/at) compliant PDs or in addition legacy BT PDs, which may not be fully IEEE 802.3bt compliant.
- Priority—low/high/critical. High priority ports are powered first, and remain powered if unit power supply cannot deliver full power to all PDs.
- Add port description for easy orientation when powering multiple PDs.

Figure 3-61. Port Configuration Detailed Screen



To simplify the configuration of multiple ports, each parameter can be set by pressing a single button (SET), thereby applying the selected values to all ports (action on all ports). See Actions on All Ports area on the lower left part of the web page, see Figure 3-61.

3.4.2.1 Ports Enable/Disable

Ports activation or deactivation is performed by the user according to actual requirements. Each PoE port can be switched to Enable or Disable state.

3.4.2.2 IEEE 802.3bt/Legacy

Each PoE port can be switched to IEEE 802.3bt supports also AF/AT or 802.3bt + Legacy.

3.4.2.3 Setting Priority

The user can assign priorities to desired PDs if the Midspan is operating with a limited source of power. Priority selection is performed from the drop-down menu, located on the Priority column. The following three priority states are available:

- Critical
- High
- Low (default)

The Midspan allocates all available power to the PDs, according to the PoE ports sequential number, starting from port #1 up to port #24. Critical ports are powered first, followed by High Priority ports. Low priority ports are powered last. A blinking LED indicates that a port is not powered due to lack of power.

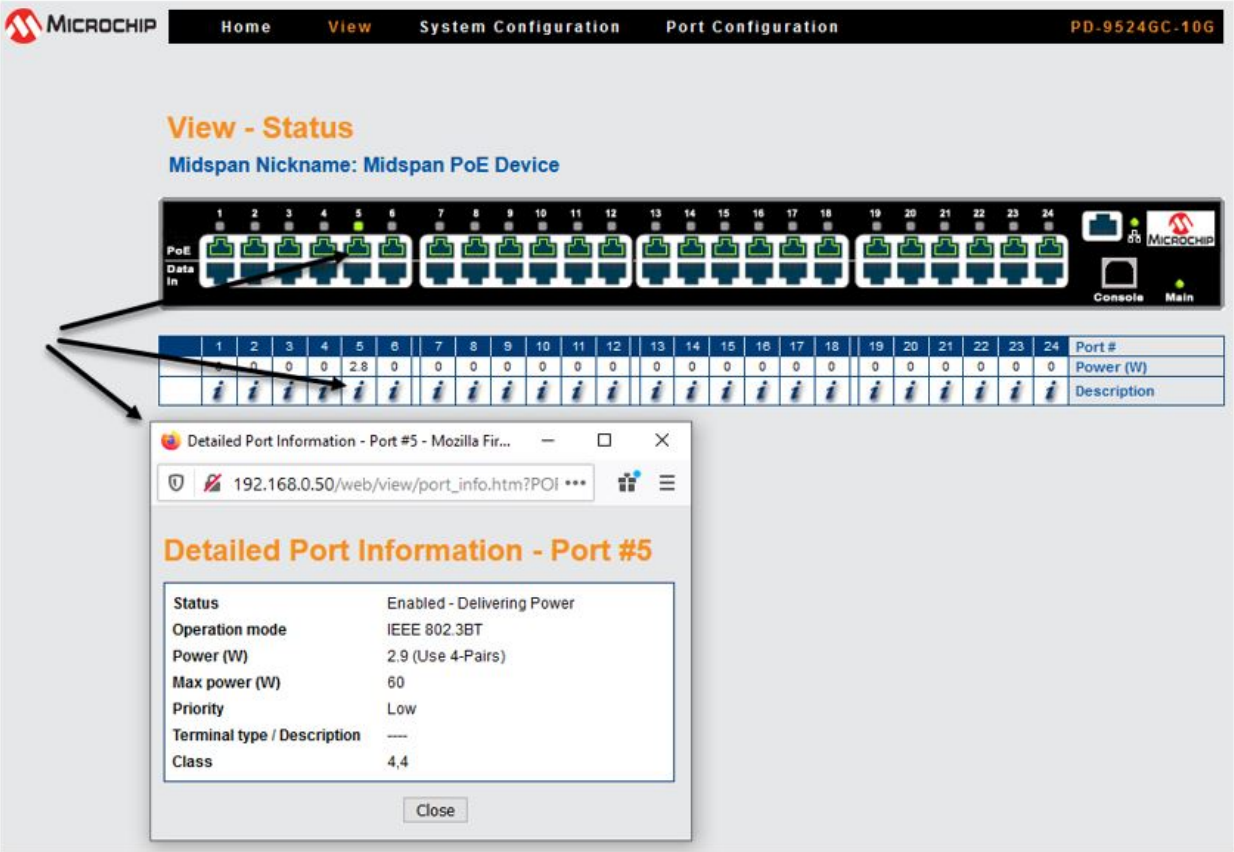
3.4.2.4 Terminal Type/Description

In this column, the operator can enter any free text such as terminal location, name of user, telephone number, and so on, representing the corresponding port.

Note: The column has no effect on power itself and it functions as an assistance tool for the IT manager.

Pressing on the RJ45 icon or the **i** icon causes detailed Port Information web page to appear, showing Terminal Type name, and additional information, as shown in the following figure.

Figure 3-62. Detailed Port Information



3.4.3 Port Configuration-Weekly Schedule

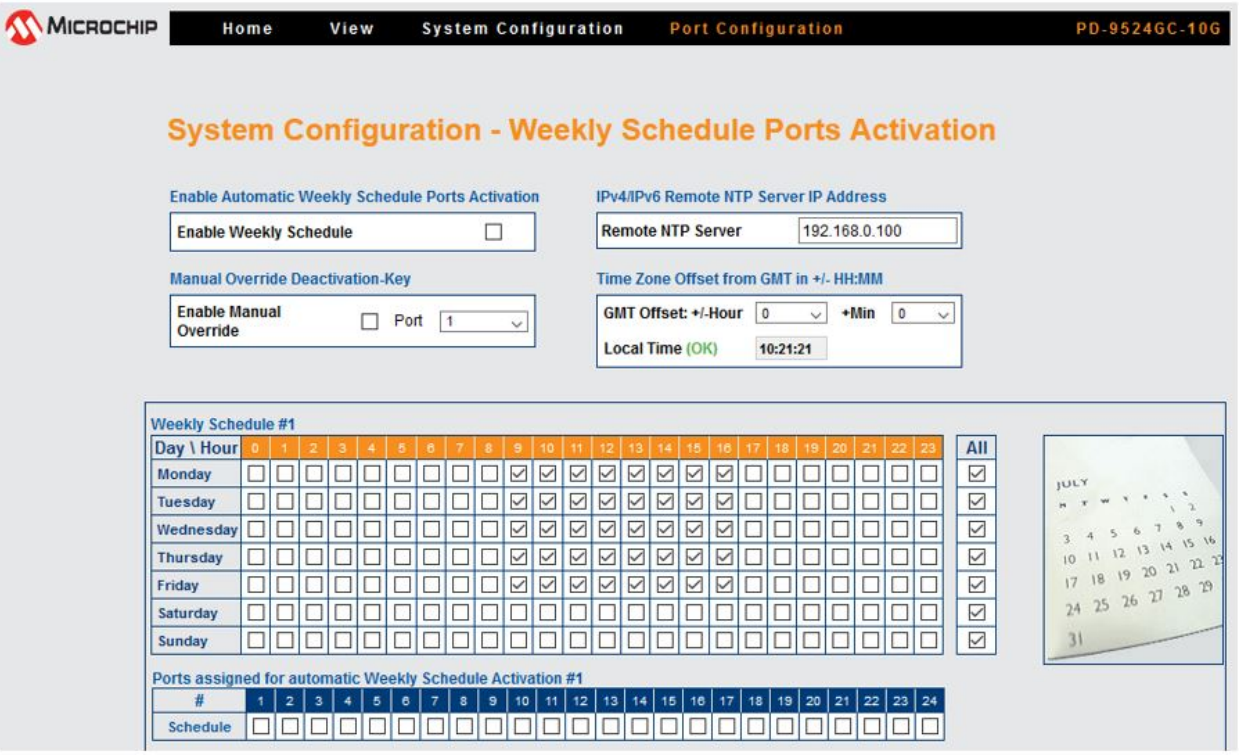
The Weekly Schedule feature (see Figure 3-63) performs an automatic activation/deactivation of PoE ports based on a weekly activation matrix (24x7). Activation/Deactivation of PoE ports might be required to save power saving during weekends, for security reasons (for example, turns off wireless access points during weekends, disconnect unused IP Phones, or reduce power consumption), or even to reset periodically various PoE PD devices.

Four 24 x 7 weekly schedules schemes are available. Each 24x7 scheme manages its own PoE ports, which enables different PoE ports to be turned on or off on different days and hours.
Note: If the same PoE port is assigned to be managed by two different 24x7 schemes, it is turned on whenever the port becomes enabled by one of the 24x7 weekly schedule scheme.

Perform the following steps prior to using this feature:

- Set the NTP server IP address.
- Set the GMT local time offset.
- Update at least one out of four 24x7 hours matrixes to match specific requirements.
- Assign the Midspan PoE ports to be automatically turned ON or OFF.
- Assign the PoE ports that provide power continuously.

Figure 3-63. Port Configuration-Weekly Schedule



Notes:

- For the Weekly Schedule feature to work properly, the Midspan must have access to an NTP server.
- Upon updating the weekly schedule NTP configuration by pressing the **Update & Save** button, wait for a few seconds, refresh the web page, and then verify that the green OK indication appears alongside the local time section (that is, GMT has been properly acquired).

3.4.3.1 Weekly Schedule Ports Activation

- **Enable Weekly Schedule**: Enables/Disables the Weekly Schedule feature.
- **Enable Manual Override**: Enables/Disables the manual override key and selects the port assigned as an override key.
- **Remote NTP Server**: Remote NTP server IP address.
- **GMT Offset**: User configured GMT offset
- **Ports On/Off Weekly Schedule**: 24x7 checkbox matrix. Midspan provides power only during the selected (checked) hours.
  Note: To simplify the configuration of the 24x7 matrix, all 24 ports can be checked for a specific day by checking one of the 'ALL' checkboxes.
- **Ports Assigned for Automatic Weekly Schedule Activation**: Selection of the ports to be activated/ deactivated automatically by the Weekly Schedule feature.
  Note: Disabled ports cannot be assigned for the Weekly Schedule, even if selected by the user.

Table 3-11. Weekly Schedule Icons Reported by View-Status Web Page

Icon/Image Type	Description
	PoE port was Enabled by weekly schedule functionality.
	PoE port was Disabled by weekly schedule functionality.
	PoE port was assigned to act as deactivation key.

4. Power Backup and Power Management

The 12, 24-port Midspan series can be connected to a secondary 12, 24-port Midspan series for power backup redundancy or deliver combined power exceeding the power capabilities of each stand along power supply power capabilities.

Note: The same internal power supply unit must be installed in both units.

Figure 4-1. Secondary Midspan Power Backup

SNMP RFC3621 MIB and private MIB Object IDs, which apply to unit power supply capabilities or total power consumption, are reported as if the two Midspans are one. The following table lists the affected SNMP Object IDs.

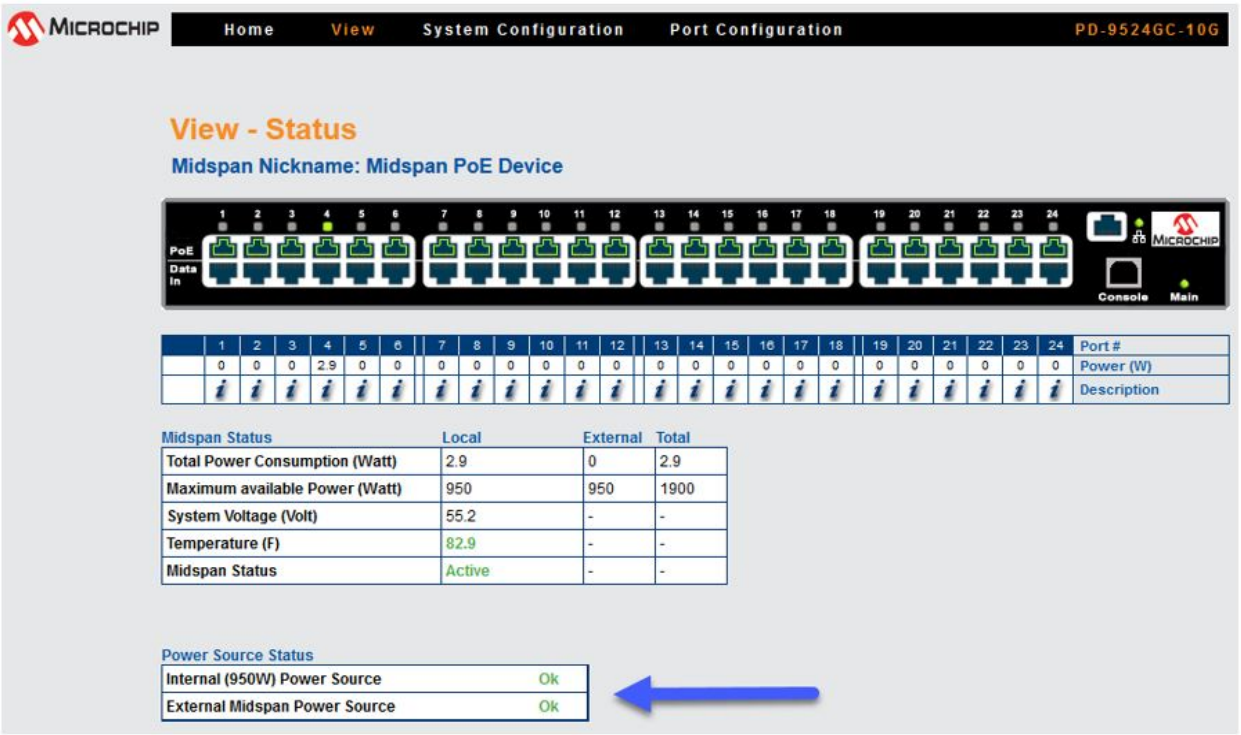
Table 4-1. SNMP Object IDs Affected by Midspan Power Backup Mode Connection

SNMP Object ID	Power Backup Mode
pethMainPsePower (RFC3621)	450W/950W (power backup mode = Redundant). 900W/1900W (power backup mode = Maximum power).
pethMainPseOperStatus (RFC3621)	Fault if there is power failure (Midspan is powered by the second Mid span).
pethMainPseConsumptionPower (RFC3621)	Total power consumption of both the Midspans.
pethMainPseUsageThreshold (RFC3621)	Sends a trap when power consumption of both the Midspans exceeds xy% out of pethMainPsePower OID (total available power by both the Midspans) power.
mainPowerUsageBudget (private MIB)	Changing power usage budget (%) in one Midspan changes it in another Mid span too.
mainPSE_MaxPower (private MIB)	Total maximum power of both the Midspans after it was reduced by pethMainPseUsageThreshold (%).

4.1 Viewing the Power Source Status

View the external power source status (Ok/Fail) and power source type (Midspan) in the View-Status web page, as shown in the following figure. See section 3.3 View Menu for details on the View-Status Screen.

Figure 4-2. Power Source Status



4.2 Dual 95xxGC, 96xxGC, PD95xx-10GC, PD96xx10GC Midspan Power Backup Midspan Power Backup

Connecting a Midspan to a second Midspan provides power backup by enabling the first Midspan to be powered by its internal power source or from the second Midspan power source. Two power backup modes are available: Redundancy and Maximum Power. Power-Shift feature enables shifting power from one Midspan to another when one Midspan requires more power and the second Midspan has spare unused power.

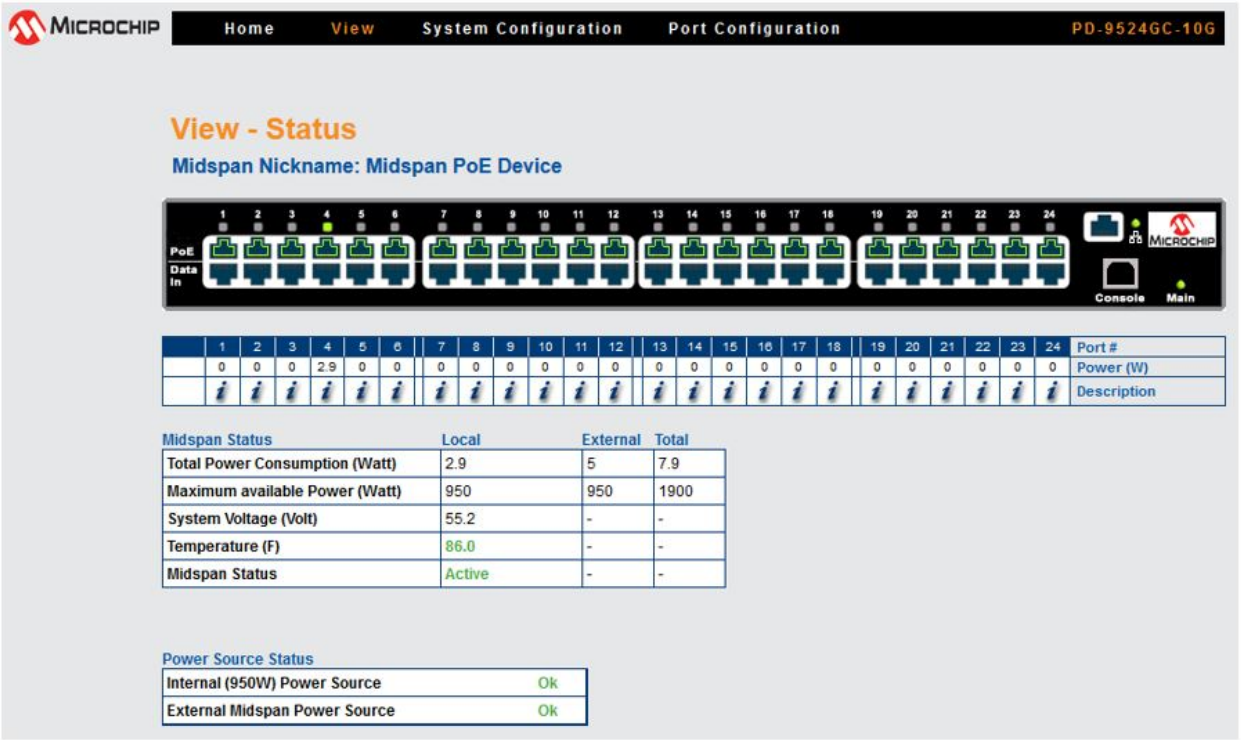
- **Redundancy**: A single Midspan internal power source must power both Midspans if a power failure occurs in one of the Midspan units. The power sum of both the Midspans cannot exceed 450W/950W. Each Midspan's initial maximum power is set to 450/2 = 225W or 950/2 = 475W (the maximum power might change during normal operation).
- **Maximum Power**: The first Midspan power source capabilities are added to second Midspan's internal power source capabilities. Two Midspans having a 450W power supply can provide 900W, while two Midspans having a 950W power supply can provide up to 1900W.

Notes:

- Changing Power-Backup mode in one of the Midspans causes the second Midspan Power-Backup mode to be changed to the same power backup mode.
- If two standalone Midspans are configured to different Power-Backup modes, then after being connected, both the Midspans switch to Redundant power-backup mode.

4.2.1 Midspan to Midspan Power Shift

Figure 4-3. View-Status Window (Power Shift Display)



When two Midspans powers backup each other, two additional rows are added to the View-Status web page. The first additional row displays the extended Midspan power consumption and maximum power. The second row reports total power consumption and total maximum power.

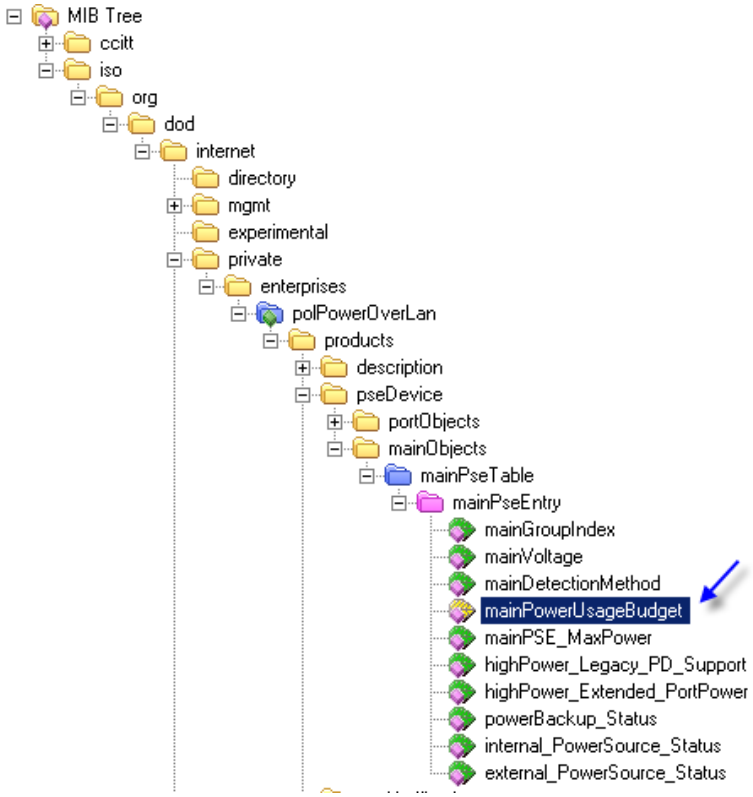
Figure 4-3 shows two PD-9624GC Midspans backing up each other, while in Redundancy Power-Backup mode. The total power of both the Midspans is limited to 950W (due to the Redundant mode configuration). Local Midspan maximum power is reduced by the Midspan power manager to 179W, while external Midspan maximum power is increased to 251W.

4.2.2 Changing Power Limit (%) by SNMP

Midspan maximum power can be limited by SNMP private MIB OID mainPowerUsageBudget (see Figure 4-4) or by Midspan itself whenever Dynamic UPS Power Management is enabled.

Power shift between two Midspans pauses whenever the power limit (%) is less than 100% and resumes automatically whenever the power limit is restored back to 100%.
Note: Changing power limit (%) in one of the Midspans automatically changes power limit on the second Midspan to same value.

Figure 4-4. Midspan Power Limit by SNMP



4.2.3 Activating Dynamic UPS Power Management

The Dynamic UPS Power Management feature must be configured only on a single Midspan when two Midspans power backup each other. When the configured Midspan detects a UPS power failure (UPS switched to battery), it modifies power limit % as per the user configuration. A power limit value on the second Midspan automatically follows a power limit value of the Midspan which monitors the UPS over SNMP.

Note: Do not change by SNMP private MIB mainPowerUsageBudget OID while Dynamic UPS Power Management is enabled.

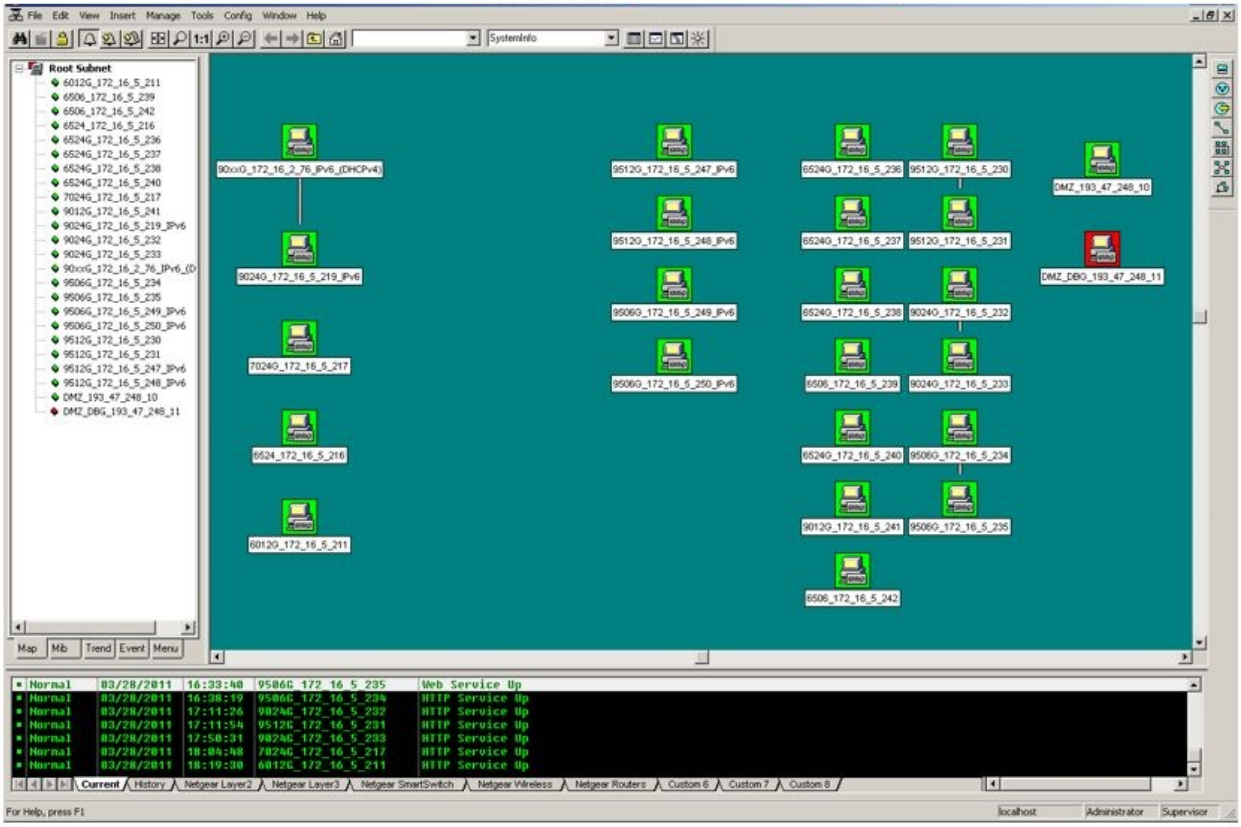
4.2.4 Power Failure and Invalid Midspan to Midspan Power Backup Connection Report

- **Power failure**: If a power failure occurs in one Midspan unit, then an SNMP trap (see SNMP private MIB) and SysLog message is sent to the SNMP Manager and SysLog manager, and an error message appears in View-Status web page. Another SNMP and SysLog message is sent when the power is restored.
  Note: Main power LED blinks when Midspan is being powered by external Midspan due to internal power supply failure (no AC power).
- **Invalid connection**: The following actions occur when a Midspan having a 950W power supply is connected to another Midspan (earlier Midspan models were non-IEEE 802.3bt compliant) using internally 430W power supply:
  - Both Midspans reduce maximum power to 41W, which must stop power to most of the PoE PD devices.
  - A Midspan message reporting invalid configuration by sending SNMP Trap and Slog message.
  - An error message appears on the **View > Status** web page.
  - A repeating error message appears on Terminal/Telnet/SSH screen.

5. SNMP Monitoring and Configuration

The following figure shows that the multiple Midspan devices management can be performed by using third-party standard network management tools, such as HP Openview, IBM Tivoli, or SNMPc.

Figure 5-1. SNMPc Network Management Tool



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

5.1 Enabling Midspan SNMP

The Midspan manager module supports SNMPv1, SNMPv2c, and SNMPv3.

Perform the following steps to use the SNMP:

1. Browse to the System Configuration SNMP or SNMPv3 web page and verify that either one of them is enabled.
   - For SNMPv2c, browse to the System Configuration SNMP web page. Make sure that the community strings match your SNMP manager configuration.
   - For SNMPv3, browse to System Configuration SNMPv3 web page and make sure that the username, authentication, privacy password, and encryption method match user's SNMP manager configuration.
2. Browse to the SNMP Web page. Enable PoE MIB traps and set remote manager IP address in the trap list.

5.2 SNMP MIBs

Several MIBs are supported by Midspan SNMP manager.

- **RFC3621**: PoE MIB which provides various management capabilities.

Note: RFC3621 MIB is written for IEEE 802.3af/at and not all the SNMP OIDs comply with PoE-BT. For example, only classes 0–4 can be reported although PoE-BT support classes 0–8.

- **Private MIB**: Enhance PoE functionality beyond RFC3621 PoE MIB.
- **RFC1213**: MIB2 which provides general IPv4 network statistics and information on the device being managed.
- Various SNMPv3 MI's, such as RFC3413, RFC3414, and RFC3415.

5.3 RFC3621 PoE MIB

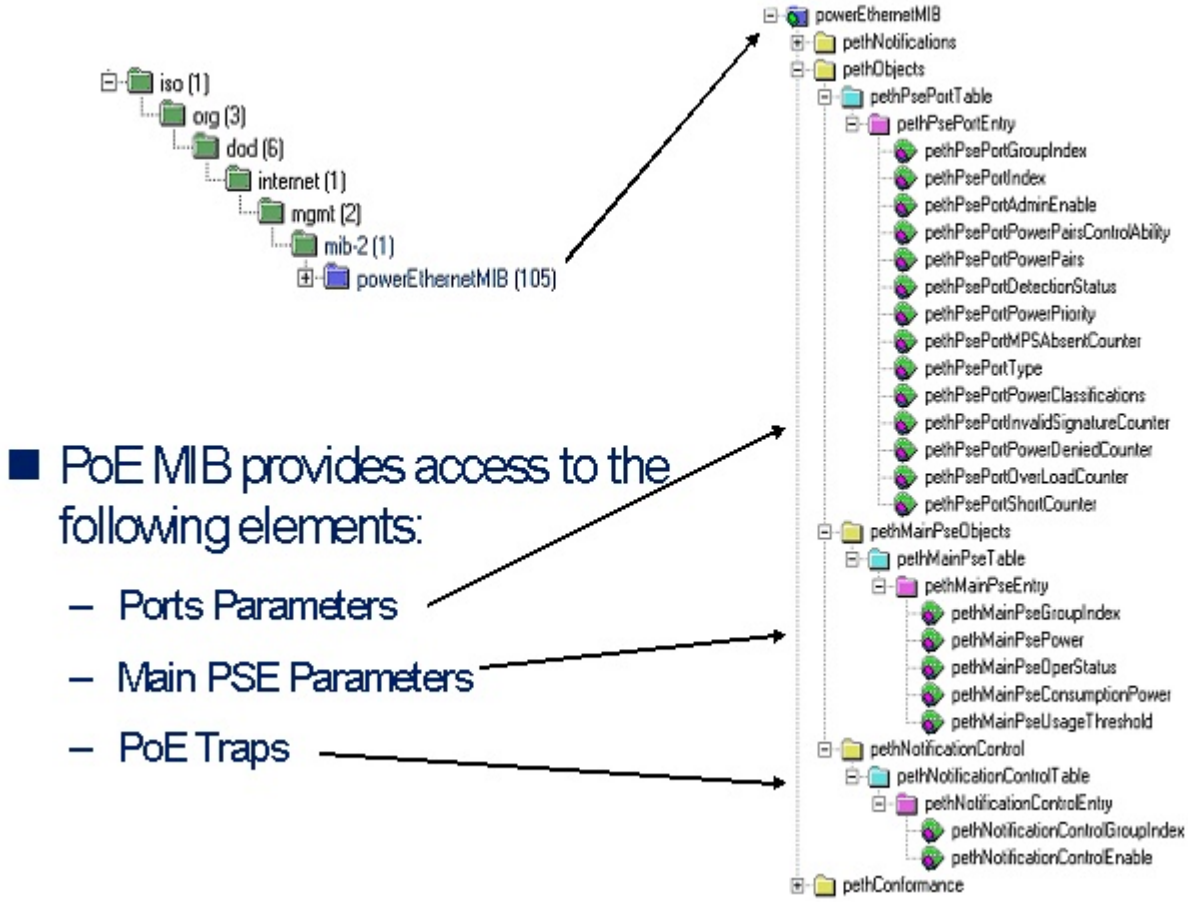
FC3621 PoE MIB is located under the 1.3.6.1.2.1.105 SNMP MIB tree.

Note: For a detailed RFC3621 PoE MIB description, see Microchip's *Technical Note–132*, which describes the PoE MIB functionality.

Figure 5-2 shows how MIB is divided into three sections:

- The first section deals with PoE ports and provides functionality as Enable/Disable, read port status, class, and so on. Each OID is accessed as a two-dimensional array table.
- The second section deals with power source, which is responsible to provide power to a group of PoE ports. It enables reading total power consumption, power supply status, and so on.
- The third section enables/disables PoE traps to be sent to remote SNMP managers.

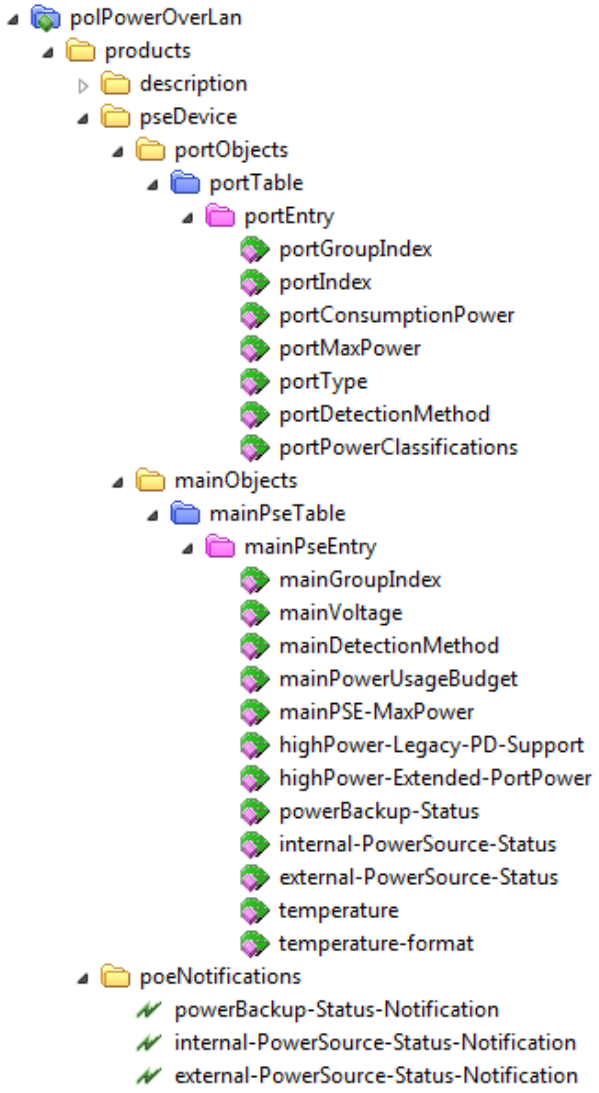
Figure 5-2. MIB Tree Structure



5.4 Private MIB

Midspan's private MIB extend RFC3621 PoE MIB with the following additional management functionalities:

Figure 5-3. MIBs Management Functionalities



5.4.1 Port Parameters

- **portConsumptionPower**: Readout of each individual port's power consumption.
- **portMaxPower**: Readout of maximum power that the PD device might consume based on PD class.
- **portType**: Report that power will be provided for all four pairs.
- **portDetectionMethod**: Read/Write PD detection mode—IEEE 802.3bt (include AF+AT) or Legacy, that is, non-fully IEEE 802.3bt compliant devices.
- **portPowerClassifications**: Read PD device class (0–8).

5.4.2 System Parameters

- Resolves MIB-II SysobjID description.
- **mainVoltage**: Read power supply voltage.
- **mainDetectionMethod**: Not applicable.

- **mainPowerUsageBudget**: Read/write Midspan power budget percentage (%). For example, setting to 50% for Midspan with 950W capacity, limits Midspan power to 475W.
  Notes:
  - Power budget limitation is canceled if the Midspan manager module is restarted or the Midspan is turned off and on.
  - Midspan power budget cannot be set below 10%.
- **ainPSE-MaxPower**: Read maximum power the unit may provide after taking into consideration *mainPowerUsageBudget* percentage.
- **highPower-Legacy-PD-Support**: Not applicable.
- **highPower-Extended-PortPower**: Read/Write extended class power. When enabled, PD might consume slightly more power beyond IDEEE 802.3bt specification. For example, class 8—up to 92.5W instead of 90W.
- **powerBackup-Status**: Report power backup type—stand-alone/second Midspan/Invalid power backup device.
- **internal-PowerSource-Status**: Report internal power source status.
- **external-PowerSource-Status**: Report external power source status.
- **temperature**: Midspan temperature.
- **temperature-format**: Midspan temperature format—Celsius/Fahrenheit.

6. Software Upgrade

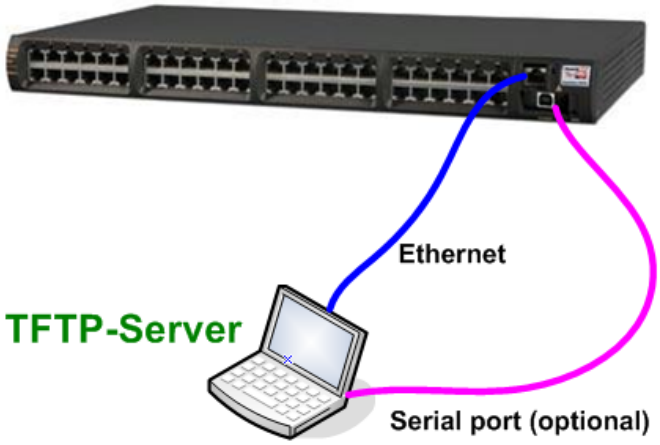
The following sections describe how to upgrade the system software.

6.1 Software upgrade types

There are two types of software upgrades associated with the PoE Midspan:

- **Midspan Manager Module Software**: Updates Midspan management application (including all web pages) that provide remote network management capabilities.
- **Midspan Firmware**: Update the firmware that manages PoE Power ports (rarely required).

Figure 6-1. System Software Architecture



6.2 Midspan Manager Module Software Upgrade

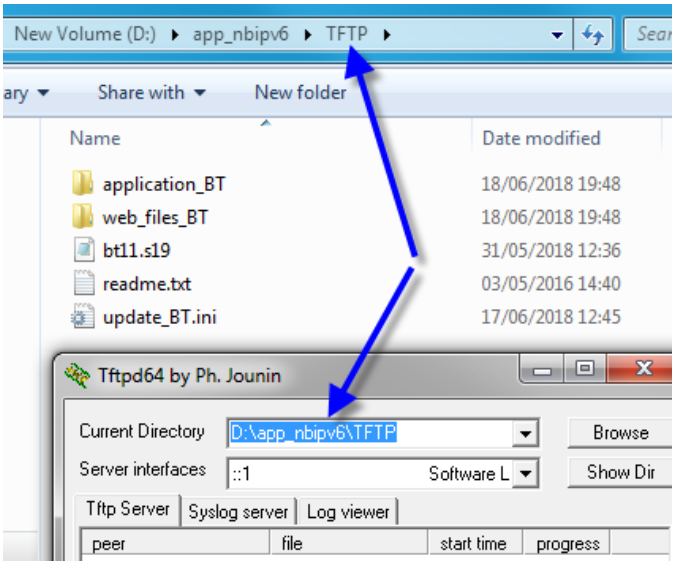
6.2.1 Upgrading to Latest Software Version (version 1.xx)

The latest version of the Microchip Midspan Network Management software is available on Microchip's Software Library.

6.2.2 Checklist Prior to Performing Software Update

- Access the unit by Telnet or serial connection.
- For serial communication over USB, install the USB virtual COM driver. For the USB driver CP210x, visit the manufacturer website www.silabs.com.
- Verify network connectivity by trying to browse or ping the Midspan unit.
- Run TFTP server on the computer, which has the latest Midspan network Manager Module software version.
- Verify that the firewall is turned off or enable firewall UDP port 69.
- Unzip the network Management Module software and place it in the root folder of the TFTP server, as shown in Figure 6-2.

Figure 6-2. TFTP Server Root Folder Setting



Note: Active PoE ports are not affected by software update (no intermediate power failure to PD devices).

6.2.3 Performing Software Update

Perform the following steps to update the software:

1. Ensure that the TFTP Server is running and the appropriate files are copied to TFTP Server root folder.
2. Connect to the Midspan unit by Telnet/SSH or serial interface, using HyperTerminal or any other serial communication software (38400 baud, 1 stop bit, or flow control off). Press **ESC** to access the main menu.

```
 Main Menu - [Midspan PoE Device]
-----------------------------------
1.  View menu
2.  Configuration & maintenance menu
3.  Ping remote host


E.  Exit to debug information screen
```

3. Select Configuration and Maintenance menu (2). The following screen appears:

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

3.  Download configuration file from TFTP Server (reset only Manager module)
4.  Upload configuration file to TFTP Server
5.  Download WEB SSL Certificate from TFTP Server (reset only Manager module)
6.  Software update menu

7.  Turn RADIUS,ACL Filter off. Restore all user & password to factory default
8.  Restore unit to factory default (excluding IP configuration)

9.  Reset Manager module
A.  Reset unit

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


ESC - Return to previous menu
```

4. Select the Software Update Menu. Type the appropriate TFTP server's IP address; the following screen appears:

```
  Software Update Menu
--------------------------------
1.  Update Midspan Manager module software (reset only Manager module)
2.  Update Midspan firmware (reset unit)


ESC - Return to previous menu
```

5. Select the Update Midspan Manager Module Software option.
   The software update starts by loading various files from TFTP server. At the end of the software update, the Network Management module resets without affecting working PoE ports. Wait for the software power up to finish, browse to the unit (or connect by serial), and verify that the software version number matches the software version that has been upgraded.

7. Troubleshooting

The following table lists the symptom and resolution sequence to assist in the troubleshooting of operating problems. If the steps given do not solve the problem, call the local dealer for further assistance.

Table 7-1. Troubleshooting Guide

Symptom	Corrective Steps
AC LED does not illuminate (green).	1. Check your power source. 2. Ensure that a proper Ethernet cable is used.
Midspan Ethernet LINK LED is OFF.	If a network card (NIC) is connected directly to the Midspan's RJ45 connector, use a crossed Ethernet cable.
Midspan Ethernet LINK LED is on and no ping reply.	1. Midspan is shipped with the default IP 192.168.0.50. Change your network card IP to 192.168.0.40 and try to ping again. 2. Connect to Midspan serial communication port and set Midspan IP to the same IP network as your host computer. 3. If one Mid span is switched with another at a fast speed (both with default IP 192.168.0.50), then erase the IP address from the host ARP table by opening DOS window and typing arp–d 192.168.0.50.
Midspan can be 'pinged' from a local Host but when trying to use the Midspan Ping utility, there is no reply.	1. Try to turn OFF the host firewall. 2. If ping is OK, 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 Midspan Ping utility to ping the host that is running the TFTP server application. 2. Turn off the firewall, or enable UDP port 69. 3. Verify that the appropriate update files package is copied to the TFTP server root folder.
Unit cannot be accessed through Telnet.	Use a web browser to view the System Configuration-Security screen and make sure that Telnet is selected under the Remote Access area, in the Enable Telnet/SSH list.
When accessing the unit by Telnet, Telnet session is terminated each time the Configuration option is pressed.	Log-on to Telnet through the administrator user name and password option and not through the viewer user name and password.
Log-on to unit through Telnet is okay but Telnet session is terminated after a while.	Telnet session is terminated if no key is pressed and no activity takes place for more than three minutes.
No SNMP TRAP events are received.	1. Use a web browser to view **System Configuration > Security** web page and verify that the SNMP checkbox is selected. 2. Check the **System Configuration > SNMP** web page and verify that the remote SNMP manager IP matches, and the trap community string matches the Remote SNMP manager trap configuration. 3. Turn of the firewall on the SNMP manager station or allow UDP port 162 to pass through it.

.....continued

Symptom	Corrective Steps
SysLog Server IP was set properly, but log messages are not received.	Turn OFF the host firewall or allow UDP port 514 to pass through it.
When using a web browser and accessing View-Status web page, all ports are illuminated red and a question mark appears.	If Midspan does not provide power to PoE PDs, try to update the internal firmware. If the problem persists, contact technical support.
Weekly schedule was properly configured but PoE ports do not turn on/off in accordance with the weekly schedule scheme.	1. Verify that the NTP Server IP address is configured properly 2. Verify that the Time Zone Offset on the GMT window displays “OK”. 3. Verify your company’s firewall does not block outgoing or incoming NTP packets (UDP Port 123).
In cases where UPS operates on battery, Midspan does not turn off low priority ports.	1. Browse to View-Status web page and verify that the UPS Power Management window does not display “???” in any one of the fields. If “???” appears, verify that the UPS Dynamic Management parameters are properly configured. 2. Verify that the Midspan SNMP configuration (SNMPv1 or SNMPv2) matches UPS SNMP agent capabilities.

8. Support

8.1 Technical Support

For technical support, visit the Microchip Technical Support Portal.

8.2 Management Software

For more information, see the PowerView Pro software that is available on Microchip's Software Library.

9. Revision History

Revision	Date	Description
A	06/2021	Initial revision

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip design partner program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Product Change Notification Service

Microchip's product change notification service helps keep customers current on Microchip products. Subscribers will receive email notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods being used in attempts to breach the code protection features of the Microchip devices. We believe that these methods require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Attempts to breach these code protection features, most likely, cannot be accomplished without violating Microchip's intellectual property rights.
- Microchip is willing to work with any customer who is concerned about the integrity of its code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable." Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Trademarks

ISBN: 978-1-5224-8382-3

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: www.microchip.com/support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Australia - Sydney** Tel: 61-2-9868-6733 **China - Beijing** Tel: 86-10-8569-7000 **China - Chengdu** Tel: 86-28-8665-5511 **China - Chongqing** Tel: 86-23-8980-9588 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 **China - Hong Kong SAR** Tel: 852-2943-5100 **China - Nanjing** Tel: 86-25-8473-2460 **China - Qingdao** Tel: 86-532-8502-7355 **China - Shanghai** Tel: 86-21-3326-8000 **China - Shenyang** Tel: 86-24-2334-2829 **China - Shenzhen** Tel: 86-755-8864-2200 **China - Suzhou** Tel: 86-186-6233-1526 **China - Wuhan** Tel: 86-27-5980-5300 **China - Xian** Tel: 86-29-8833-7252 **China - Xiamen** Tel: 86-592-2388138 **China - Zhuhai** Tel: 86-756-3210040	**India - Bangalore** Tel: 91-80-3090-4444 **India - New Delhi** Tel: 91-11-4160-8631 **India - Pune** Tel: 91-20-4121-0141 **Japan - Osaka** Tel: 81-6-6152-7160 **Japan - Tokyo** Tel: 81-3-6880- 3770 **Korea - Daegu** Tel: 82-53-744-4301 **Korea - Seoul** Tel: 82-2-554-7200 **Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906 **Malaysia - Penang** Tel: 60-4-227-8870 **Philippines - Manila** Tel: 63-2-634-9065 **Singapore** Tel: 65-6334-8870 **Taiwan - Hsin Chu** Tel: 886-3-577-8366 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 **Thailand - Bangkok** Tel: 66-2-694-1351 **Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4485-5910 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-72400 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-72884388 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820