User manual – MPH241/242

MPH series video encoders

H.264 / MPEG-4 / MJPEG / MPEG-2 video encoders for PTZ and fixed camera networking applications

MPH241 – 1-ch stand-alone video encoder
MPH242 – 2-ch stand-alone video encoder

SD, HD-SDI (1080p)
Contents

MPH series video encoders introduction ........................................................................................................ 1
MPH series video encoders front and rear panel .......................................................................................... 2-3
Getting started ............................................................................................................................................. 4
  Quick instructions ........................................................................................................................................... 4
  Device’s IP address ......................................................................................................................................... 4
MPH200 series models ................................................................................................................................... 5
Ethernet interface ........................................................................................................................................ 6-7
  Local ports, electrical interfaces ..................................................................................................................... 6
  Power over Ethernet (PoE+) option .................................................................................................................. 6
  Up-link ports, optical interfaces (SFP) ............................................................................................................. 6
  How to unplug or plug-in the SFP transceiver module .................................................................................. 7
  To unplug and plug-in the SFP module, follow these steps ......................................................................... 7
  Some generic notes for successful optical connections ................................................................................ 7
Management interface .................................................................................................................................. 8
  General .......................................................................................................................................................... 8
  WebUI ......................................................................................................................................................... 8
  ONVIF ......................................................................................................................................................... 8
  CLI – command line interface ...................................................................................................................... 8
Web user interface (WebUI) ............................................................................................................................. 9-11
  General ........................................................................................................................................................ 9
  System requirements for WebUI ..................................................................................................................... 9
  Operation ................................................................................................................................................... 9
  Starting WebUI session ................................................................................................................................. 10
  User levels and permissions ......................................................................................................................... 10
  MAIN PAGE ............................................................................................................................................... 11
Event management system .............................................................................................................................. 12-13
  MPH event management system ................................................................................................................. 12
  Event management for video ....................................................................................................................... 13
  Event management for contact closure (digital I/O) ..................................................................................... 13
Configuring video channels ........................................................................................................................... 14-24
  Video connection ....................................................................................................................................... 14
  Video channel configuration .......................................................................................................................... 14
  Video streaming methods ............................................................................................................................. 15
  High-definition serial digital interface (HD-SDI) .......................................................................................... 15
  Media profile (video) .................................................................................................................................. 16
  Video interfaces ......................................................................................................................................... 17
  JPEG snapshot configuration ......................................................................................................................... 18
  Video source and sinks ................................................................................................................................ 19
  Video encoders ......................................................................................................................................... 20
  Video stream multiplication .......................................................................................................................... 23
  Video streaming performance ...................................................................................................................... 24
Configuring audio channels ............................................................................................................................ 27-34
Configuring data channels ............................................................................................................................ 35-39
Configuring contact closure channels ......................................................................................................... 40-42
Event management ....................................................................................................................................... 43-44
Video analytics configurations ......................................................................................................................... 45
Metadata configurations .................................................................................................................................. 46
Network settings ........................................................................................................................................... 47-48
Date & time settings ....................................................................................................................................... 49
Device management ....................................................................................................................................... 50
Services settings ........................................................................................................................................... 51-53
User management .......................................................................................................................................... 54
Configuring ethernet switch ............................................................................................................................ 55-74
Command line interface - CLI ........................................................................................................................ 75-87
MPH200 specifications .................................................................................................................................... 89
Legal declarations .......................................................................................................................................... 90
MPH series video encoders introduction

Stand-alone video encoder with 1 or 2 video inputs, bi-directional data, audio & contact closure channels + Ethernet switch

General

MPH series encoders are ONVIF (Open Network Video Interface Forum) compliant products. This provides wide interoperability with any ONVIF compliant device or system.

Many similarities exist between the MPH series video encoders; the main difference being the number of video channels available and the mechanics. MPH series video encoders are high performance video processing products encoding real time video in mission critical applications for customers in Transportation, City Center Monitoring, and Corporate Security. MPH200 series encoders are temperature-hardened compact size stand-alone video processing products in the MPX platform.

MPH200 series video encoders provides in addition to transparent link of CVBS or HD-SDI video signal up to 1080p resolution (SMTP292M), independently configurable general-purpose bi-directional asynchronous data, bi-directional audio channels and bi-directional contact closure channels. Additionally a layer 2 manageable Ethernet switch is integrated into the encoder. The Ethernet switch comes with four gigabit ports and full-feature layer 2 switching functions such as RSTP, IGMP, QoS and VLAN.

The encoded signal from MPH series encoder can be decoded with MPC/MPX (except H.264) or VMX series HW and/or SW, as well as with industry standard SW players such as Quicktime and VLC. The transmission is accomplished over 10/100/1000BASE-T or 100BASE-FX (SFP) or 1000BASE-X (SFP) network utilizing IP/Ethernet streaming.

MPH series video encoders are equipped with the H.264, MPEG-4, MJPEG and MPEG-2 video encoding engine. The default encoding combination is H.264, MPEG-4 and MJPEG. MPEG-2 is an add-on option, and it should be ordered separately.

The H.264 video encoding engine is compliant with the ISO/IEC 14496-10 (H.264@MP, BP, CBP) standard. The MPEG-4 video encoding engine is compliant with the ISO/IEC14496-2 (MPEG-4@SP/ASP L5) simple profile standard. The MJPEG video encoding engine is compliant with the ISO/IEC 13818-2 (RFC 2435) standard. The MPEG-2 video encoding engine is compliant with the ISO/IEC13818 (MPEG-2 MP@ML) standard.

General-purpose asynchronous data channels are transferred separately from the encoded video signals.

Firmware version

The functionality and operation of the devices described in this manual applies for firmware version 6.0.x.
MPH series video encoders front and rear panel

MPH200 stand-alone encoder (example view from MPH241 device)
MPH200 series video encoders mechanical connections

1. CVBS video input 1, or optional HD-SDI video input (BNC female) and indicator led.
2. CVBS video input 2 (BNC female) for 2-ch versions or Video loop through port for 1-ch versions and indicator led.
3. 16-pin screw terminal block and T indicator led:
   - Data interfaces, EIA RS422/485 (data1), EIA RS232 (data 2) /management interface (CLI) or general purpose serial port.
   - Contact closure interfaces (cc input 1, cc input 2, cc output)
4. Ethernet switch up-link interfaces, 2 x socket for SFP module (GE, see a product catalogue for supported models).
5. Ethernet switch local port interfaces, 2 x 10/100/1000Base-T, RJ-45.
6. Audio interface (10-pin screw terminal block).
7. Power supply connector (2-pin screw terminal block, +12...28 VDC).
   - Reset button: Device software reboot and hard/soft factory defaults restoration (see section Factory reset).
   - Ground: Device ground connection.

<table>
<thead>
<tr>
<th>Led</th>
<th>Colour</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>OFF / Dark</td>
<td>Power off</td>
</tr>
<tr>
<td>M</td>
<td>Yellow</td>
<td>Device starts up</td>
</tr>
<tr>
<td>M</td>
<td>Red</td>
<td>Device self-test failed</td>
</tr>
<tr>
<td>M</td>
<td>Green</td>
<td>Power on / Device is functional</td>
</tr>
<tr>
<td></td>
<td>Blinking Green</td>
<td>Device is being accessed from any interface. Whenever device is accessed from WebUI, CLI or ONVIF interface, led blinks 2s. During software update, LED will blink throughout the firmware image transfer duration.</td>
</tr>
</tbody>
</table>

M - (module/power led) LED indicator operation. This LED indicates power status, factory reset, interface activity.

Factory reset

The factory reset can be done via WebUI, CLI, or using the pinhole reset button on the front panel of device. There are two types of factory resets; Soft factory and Hard factory reset. The Soft factory reset restores all, except IP configuration to the default factory settings. The Hard factory reset restores all settings to default factory settings.

Reset button

The reset pinhole is a button that resets the device to its original default settings. To use this button, insert a stiff wire (such as a straightened paper clip) into the pinhole. If you release the button immediately the device will reboot with current settings. But if you hold the button you can restore the default settings as following table shows.

<table>
<thead>
<tr>
<th>Led</th>
<th>Colour</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>6 x (short) green blinks at boot time</td>
<td>Time window to select Soft factory reset. If reset button is released in this time window, soft factory reset is selected.</td>
</tr>
<tr>
<td>M</td>
<td>2 x (short) red blinks</td>
<td>Soft factory reset shall be applied. Wait until device has fully started (power led green).</td>
</tr>
<tr>
<td>M</td>
<td>24 x yellow blinks at boot time (after the 6 green blinks)</td>
<td>Time window to select Hard factory reset. If reset button is released in this time window, hard factory reset is selected.</td>
</tr>
<tr>
<td>M</td>
<td>4 x (short) red blinks</td>
<td>Hard factory reset shall be applied. Wait until device has fully started (power led green).</td>
</tr>
</tbody>
</table>

Note! If pinhole button is not released within time window, operation will cancelled.
Getting started

Quick instructions

1. Install the temperature hardened stand-alone MPH200 series encoder to the installation location. A +12 VDC supply voltage is provided by a CPS25x series power supply (see example picture beside), or alternately through the LAN cable (CAT5) when using Power over Ethernet (PoE+) technology.

2. Connect all needed signals to their respective connectors on the device’s front panel:
   - HD-SDI / CVBS video signals to the BNC female connector(s).
   - Data and contact closure signals to the screw terminal connector.
   - Audio signal(s) to the screw terminal connector.
   - Ethernet network to Ethernet connectors.

3. Switch on the power and wait until the power led “M” lits green (start-up time approx. 100 secs). This indicates that the device hardware is operating properly and ready for usage.

   **Note!** If led doesn’t lit green, refer to “M- LED indicator” section to know the status of the device.

4. Log on to the device using the IP address assigned by DHCP server, or locally from a Mgmt port (CLI) and then set all necessary settings in the device.

   **Note!** Device uses always two IP-addresses, one for encoder and another for internal switch management. By default device will automatically assign IP addresses via DHCP. If network doesn’t contain DHCP server, then the MPH encoder shall use Zeroconf (link-local) as DHCP fallback (see section below).

Device’s IP address

There are two ways of assigning IP address to the MPH device. The IP address can be automatically assigned via DHCP, or you can set it manually as a static IP address. Factory default IP settings for the device is DHCP enabled.

By default when you have DHCP server in the network, DHCP server assigns an IP address automatically to the MPH encoder. The DHCP server offers an IP address from its address pool when a device is starting up.

If DHCP server is not available device uses zero configuration (link-local address) as DHCP fallback. With Zeroconf protocol MPH chooses an IP address randomly in the IP range from 169.254.0.1 to 169.254.255.254.

Alternatively you can manually assign the IP address, subnet mask and gateway address to the unit.

If there is no DHCP address in the network, the unit chooses randomly an IP address from the private IP range 169.254.0.1 - 169.254.255.254. In this case in order to find the chosen IP address you have two options. You can use Teleste MPH Discovery Tool to browse all the available ONVIF compliment devices in the network, note that your PC IP address should be in the same IP range. Second option is, connecting to the MPH device locally via the serial port and use the CLI (Command Line Interface) to see device IP address.

See section **Network command** to see how to change IP address via CLI.
**MPH200 series models**

One video input (digital HD-SDI or analog CVBS).

Two video inputs (analog CVBS).

MPH241 encoder supports both digital HD (HD-SDI) and analog CVBS video formats.

*For HD-SDI operation the MPH241 needs to have the HD encoding license MLH213 enabled.*
Ethernet interface

Electrical Ethernet connector (RJ-45).

<table>
<thead>
<tr>
<th>Led</th>
<th>Colour</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Green</td>
<td>Link up</td>
</tr>
<tr>
<td></td>
<td>Blinking Green</td>
<td>Traffic</td>
</tr>
<tr>
<td></td>
<td>OFF / Dark</td>
<td>No link</td>
</tr>
<tr>
<td>1</td>
<td>Orange</td>
<td>1000 Mbps</td>
</tr>
<tr>
<td></td>
<td>OFF / Dark</td>
<td>100 Mbps</td>
</tr>
</tbody>
</table>

Ethernet port's led indicator operation (RJ-45 connector).

<table>
<thead>
<tr>
<th>Led</th>
<th>Colour</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFP</td>
<td>Green</td>
<td>Link up</td>
</tr>
<tr>
<td></td>
<td>Blinking Green</td>
<td>Traffic</td>
</tr>
<tr>
<td></td>
<td>OFF / Dark</td>
<td>No link</td>
</tr>
</tbody>
</table>

Ethernet port's led indicator operation (when SFP optical connector).

Ethernet connections

The unit has a built-in 4-port managed Ethernet switch and supports both Fast Ethernet and Gigabit Ethernet connection speeds. Ethernet interface type is either a fixed electrical (copper), or has support for a small form-factor pluggable transceiver (SFP) module. Supported SFP transceivers are specified by Teleste. Please see the latest list of available SFP products.

Local ports, electrical interfaces

Device include two (2) fixed electrical Ethernet connectors. The electrical Ethernet connector type is a RJ-45 female. The interfaces are supporting 10/100/1000Base-T operation (Gigabit Ethernet).

Power over Ethernet (PoE+) option

MPH200 series encoders supports PoE standard (PoE+ 802.3at class 4). This means that the encoders can be powered through the LAN cable without the need of individual power supplies. PoE is available from port number three (3).

Requirements for the use of PoE:

- A Power over Ethernet (PoE) compliant switch or hub.
- MLH251 license activation.

*Note! MPH200 series device PoE port is only used to powered device itself, it not provide output power to other devices.*

Up-link ports, optical interfaces (SFP)

SFP modules for optical Ethernet operation are available with a variety of different types (see the latest list of available SFP products), allowing users to select the suitable module for to provide the required optical reach over the available optical fibre type. The optical connector type is **LC/PC** (single or dual). Ethernet interface speed is 1000BASE-X (Gigabit Ethernet).

When installing the fibre optic cable, do not exceed the minimum bending radius when connecting cable to the system.

Optical Ethernet connection meets class 1 laser safety requirements of IEC 60825-2: 2004 and US department of health services 21 CFR 1040.10 and 1040.11 (1990) when operated within the specified temperature, power supply and duty cycle ranges.
How to unplug or plug-in the SFP transceiver module

If your up-link port requirements change, simply unplug the existing SFP module, and plug-in the new module. **The SFP transceiver modules must be installed before the encoder is powered on.** Installing SFP:

1. Switch off the unit supply voltage.
2. Mount the SFP transceiver to the unit (see bottom instructions).
3. Connect the fibre optic cable(s).
4. Ensure that the remote end of the fibre is already connected to an active switch.
5. Switch on the unit supply voltage.

The SFP transceiver module has a bale-clasp latch that makes easier to install or remove the module. Protect the SFP module by inserting a clean dustplug into the module after you remove the fiber cable. Be sure to clean the optic surfaces of the fiber cable before you plug the cable into another module. When using 2 fibre version SFP, select carefully the correct optical port for TX and RX operation.

To unplug and plug-in the SFP module, follow these steps:

1. Open the bale clasp on the SFP module by pressing the clasp downward until it is in a horizontal position.
2. Use a small flat-blade screwdriver or other long, narrow instrument to push on the hinge pin to unlock the SFP cage latch.
3. Grasp the SFP module by the bale clasp and gently pull it out of the SFP cage.

To plug-in the module:

1. Orient the transceiver with the bale clasp on the bottom, close the bale clasp by pushing it up over the transceiver, then gently insert the transceiver into the port until it clicks into place. **Note! Reboot the device when the SFP is changed.**

Some generic notes for successful optical connections:

- Ensure that the fiber patch cord is damage-free (fiber condition can be easily checked by a visible laser tester)
- Do not exceed the minimum bending radius of the fibre
- Avoid sharp corners on cable shelves and in cable management in overall
- Make sure that correct optical connectors are used
- Open connectors are always secured by dustcaps during maintenance
- Always before mating clean all connectors (wet cleaning by high purity alcohol & drying, or dry cleaning with reel-based lint-free wipes, fiber adapters may require special ferrule end-face cleaning tools)
- Before making any visual inspections ensure that system has been shutdown or no optical power is present
- For fault finding at least a optical power meter is required, a complex fiber cable environment may require use of an OTDR equipment.
General

MPH encoders support web user interface (WebUI), ONVIF configuration interface and command line user interface (CLI) for various configuration purposes.

WebUI

MPH series video encoders can be fully configured using Web user interface (WebUI). You can access the Web user interface via web browser.

ONVIF

MPH series video encoder support ONVIF (Open Network Video Interface Forum) global interface (version 1.02, Profile S).

CLI – command line interface

MPH series video encoder include a command line interface (CLI) for configuration purposes. The CLI is a text-based interface that allows the user to interact with the operating system by entering commands and optional arguments. CLI is accessible through any terminal emulator application (e.g. Hyper Terminal or PuTTY). The command structure is the same for all session types. A typical CLI usage is to access the device IP address settings. By default the data channel 2 is set for CLI usage. The data channel 2 can be set to normal RS232 data mode with WebUI when needed.

Note! Data 2 channel can be set either general RS232 data transport mode or CLI mode (not simultaneously). The default factory setting is CLI mode (Hard and soft factory reset restores the data channel 2 to the CLI mode).

Local CLI connection

The local CLI session can be establish via data channel 2 by using a serial data connection (RS232) cable (type Teleste CIC506).

Note! Data 2 port must be set to CLI mode.

Remote CLI connection

Over the IP network you can make Telnet or SSH connection to open the command line interface remotely. SSH protocol secures your data session.

Note! Remote CLI is always available through network, even when data 2 is configured for non-CLI usage.

Local management connection (CLI) and management cable (CIC506) pinout (D9 female/screw terminal).
Web user interface (WebUI)

General

The MPH series video encoders can be fully configured using Web user interface (WebUI). You can access the Web user interface via your web browser, e.g. Mozilla Firefox (recommended), Internet Explorer, Apple Safari and Google Chrome. The Secure HTTP (HTTPS, SSL 3.0 or TLS 1.0) feature is supported in MPH encoders.

System requirements for WebUI

- Network connection
- Ethernet cable
- Browser installed (Mozilla Firefox recommended)

Operation

Web user interface consists of several menus and pages. Only one page can be loaded at the same time. You can open a page by clicking the related menu (see picture below).

The Web user interface has the following menu structure:

The information on configuration pages is shown in data fields or boxes. The settings can be changed in the data fields and boxes having white background. The unavailable or read-only options are grayed out. Place the cursor in the desired data field or box and enter a new setting. Settings are entered by ticking a checkbox or clicking on a radio button, by selecting from a pull-down list or by scrolling digits with the help of spin buttons.

Press keyboard’s F5 button to refresh the WebUI page view.

When changing the settings, always click Save button to confirm settings.

By clicking this button on a page you can see more settings.
Starting WebUI session

To create a WebUI session, first enter the device IP address into the web browser’s address bar (see section Device’s IP address). The following LOGIN window appears on the screen. Enter the required username and password (see bottom) in the fields and then click to continue --> Web user interface’s MAIN PAGE appears on the screen.

The Web user interface session to MPH series video encoder is now activated.

Login window with the default username and password (for administrator).

User levels and permissions

The user management supports three different user levels of which each has specific privileges as shown below. The individual usernames, passwords and approved user level can be changed via the WebUI and CLI.

<table>
<thead>
<tr>
<th>Page</th>
<th>Operation</th>
<th>User</th>
<th>Operator</th>
<th>Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main</td>
<td>General Access</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SDP download</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Log download</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Start/Stop</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RTSP link copy</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Video &amp; Audio</td>
<td>General Access</td>
<td>-</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Encoder</td>
<td>Save</td>
<td>-</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cancel</td>
<td>-</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Maintenance</td>
<td>General Access</td>
<td>-</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Backup</td>
<td>-</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restore</td>
<td>-</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reboot device</td>
<td>-</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Soft factory reset</td>
<td>-</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hard factory reset</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software upload</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Software download</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td></td>
<td>License install</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
<tr>
<td>User Management</td>
<td>General Access</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Save</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cancel</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change password</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Ethernet switch</td>
<td>Configuration</td>
<td>-</td>
<td>-</td>
<td></td>
</tr>
</tbody>
</table>
The MAIN PAGE is opened after the WebUI session has been established to the MPH200 series video encoder.

MPH200 encoder contains maximum six (6) encoding profiles, which can be individually configured. On this page you can see each profile’s current status and start/stop their video streaming.

**Type:** Device type (configuration map code)

**Serial Number:** Device serial number

**HW Version:** Device hardware version

**SW Version:** Device firmware version

**Uptime:** Device uptime

**Current time:** Device current time

**Self Test Result:** Device test result

**Current Temperature:** Current ambient temperature

**STATUS**

Here you can see each profile’s current status.

**Type:** Stream type (Video)

**Encoder:** Encoding format (H.264/MJPEG/MPEG-4,MPEG-2)

**Multicast /Unicast:** Video transmission mode (multicast/unicast)

**Target Address:** Multicast: Multicast IP address / multicast group
Unicast: IP address of receiving decoder

**Target Port:** UDP port number

**Camera Status:** Camera status (Ok/No signal)

**Stream Status:** Video stream status (On/Off)

**SDP:** Link to SDP file (Session Description Protocol). The SDP file contains stream parameters that are meant for 3rd party applications (e.g. SW decoders) to open/view the stream. SDP-link requires that video streaming is active.

**Download short term logs:** Debug log file

**Download long term logs:** Debug log file
Event management system

MPH event management system

MPH encoders internally controls events as specified by ONVIF. Events are generated from Digital IO inputs, motion detection, tampering detection and video signal loss and each of those generate event with different Topic. In addition to event topics, events contain data describing the event such as the video interface related, amount of motion and threshold, etc.

The event data is available in the “Message Content filter” box, which is XPath format for matching XML content. Triggering occurs when defined “Topic expression” and “message content filter” matches the internal event.

MPH encoder can trigger actions for **video**, **audio** (only MPH200 series) and **contact closers** (Digital I/O) output. These events are also available for video management system to trigger configurable alarms. You can add multiple event at the same time and each one triggers action.

![Available events for triggering. First choose the required event from the list and then click Add button to select the event -> The event data appears on the Message content filter box.](image)

The list of available events for triggering.

Custom = Modified event for triggering.
Event management for video

For video it can trigger actions such as changing video settings, frame rate, bit rate and video quality for each video profile based on events.

<table>
<thead>
<tr>
<th>Rate Control</th>
<th>VBR</th>
<th>CBR</th>
<th>Capped VBR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate control type</td>
<td>Default 5 frames/s</td>
<td>Triggered 25 frames/s</td>
<td></td>
</tr>
<tr>
<td>Frame rate (1..30fps)</td>
<td>Default 1 frames/s</td>
<td>Triggered 1 frames/s</td>
<td></td>
</tr>
<tr>
<td>Encode Interval (1..30)</td>
<td>Default 5 frames/s</td>
<td>Triggered 25 frames/s</td>
<td></td>
</tr>
<tr>
<td>Effective Frame rate</td>
<td>Default 25 frames</td>
<td>Triggered 25 frames</td>
<td></td>
</tr>
<tr>
<td>GOP length</td>
<td>Default 100 %</td>
<td>Triggered 100 %</td>
<td></td>
</tr>
<tr>
<td>Image quality (1%..100%)</td>
<td>Default 500 kbps</td>
<td>Triggered 2500 kbps</td>
<td></td>
</tr>
<tr>
<td>Bitrate (128..40000)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event subscription (for triggering)</th>
<th>Event subscription (for fallback from triggered state)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signal lost for video 1 and 2</td>
<td>Signal restored for video 1 and 2</td>
</tr>
<tr>
<td>Camera tempered for video source 1 and 2</td>
<td>Temper removed for video source 1 and 2</td>
</tr>
<tr>
<td>Motion detection above the threshold for video 1 and 2</td>
<td>Motion Detection below the threshold for video 1 and 2</td>
</tr>
</tbody>
</table>

Available events for video.

Event management for contact closure (digital I/O)

For contact closure it can trigger actions such as changing output state in case of an event.

<table>
<thead>
<tr>
<th>Output 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common</td>
</tr>
<tr>
<td>Type</td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Idle State</td>
</tr>
<tr>
<td>Mode</td>
</tr>
<tr>
<td>Delay time</td>
</tr>
<tr>
<td>Status</td>
</tr>
<tr>
<td>Logical State</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Event subscription (for triggering)</th>
<th>Event subscription (for fallback from triggered state)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I/O Inputs activation</td>
<td>I/O Inputs deactivation</td>
</tr>
</tbody>
</table>

Available events for contact closure.
Video connection

MPH encoder is available in one and two video input models. One channel model has support for CVBS or HD-SDI video signal, two channel model has support only for CVBS video signal. One channel (CVBS input) model has equipped with additional loop-through output connector. The video connector type is a BNC female. The video input impedance is 75 Ω. The nominal input level is 1 Vpp. Video inputs are equipped with dual colour VIDEO indicator led’s on the front panel. Video port settings can be configured from web user interface (WebUI).

### VIDEO INTERFACES
(Physical video input)

### VIDEO SOURCE CONFIGURATIONS
(Video overlay settings)

### VIDEO ENCODER CONFIGURATIONS
(6 encoding combinations)

### MEDIA PROFILE CONFIGURATIONS
(up to 12 media profiles)

### MAIN PAGE
(Start / Stop video streaming)

### Video channel configuration

MPH is an ONVIF compliant encoder and video channel configuration is designed according to ONVIF standard.

**Note!** Before modifying the configuration of a video profile, make sure that video stream is stopped on the MAIN page (changing only encoding parameters don’t require stopping of the stream).
**Video streaming methods**

Video input is the physical video connector (BCN female) available for video signal. Naturally each video input can be connected to a camera or any other standard video source. The default video input mode is set to PAL/NTSC format (CVBS). MPH241 model has also support for HD-SDI.

**High-definition serial digital interface (HD-SDI)**

MPH241 encoder supports HD-SDI digital video interface. HD-SDI interface is defined by SMPTE 292M standard and allows bitrates up to 1.485 Gbit/s. Progressive input signals are recommended to provide the best picture quality. The HD-SDI support can be enabled with MLH213 license. When changing the video format from CVBS to HD-SDI, the device must reboot. The loop-through port is not available in HD-SDI mode.

<table>
<thead>
<tr>
<th>Input Signal</th>
<th>Output frame/field rates</th>
<th>Resolutions</th>
<th>Coding</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>720p25</td>
<td>1...25fps</td>
<td>1280x720, QCIF, CIF, 4CIF</td>
<td>Progressive</td>
<td>Input signal is progressive, thus deinterlace is not needed neither at encoder or decoder side</td>
</tr>
<tr>
<td>720p30</td>
<td>1...30fps</td>
<td>1920x1080, QCIF, CIF, 4CIF</td>
<td>Field coded</td>
<td>Input signal 1080i is interlaced format containing 60 fields/s. Transmitted video stream is interlaced (field-coded), thus deinterlacing at decoder side is required when display is progressive</td>
</tr>
<tr>
<td>720p60</td>
<td>1...30fps</td>
<td>1920x1080, QCIF, CIF, 4CIF</td>
<td>Progressive</td>
<td>Input signal is progressive, thus deinterlace is not needed neither at encoder or decoder side</td>
</tr>
</tbody>
</table>

Supported HD signal formats and encoding formats.
Media profile (video)

MPH series encoders have a total of six (6) media profiles. Each media profile can be set separately for individual resolution, frame rate, GOP structure and bitrate, within the processing power of the device.

Click “Media Profiles” under the Media Configuration menu. **Media Profile Configurations** page appears on the screen. On this page you can associate virtual video sources with physical video inputs and encoding profiles.

By default this page contains six different media profiles.

**Notes!** It is not possible to change encoding format/resolution and video input settings on this page. Before modifying the profiles the video stream must be stopped on the MAIN page.

[Image of media profile configuration page]

**Profile 1 - Video 1**

**Name:** User defined alias name for media profile (max 63 chars).

- **Video Source Configuration:** Select assigned video source configuration.
- **Video Encoder Configuration:** Select assigned video encoder configuration.
- **PTZ Configuration:** Select assigned PTZ configuration.
- **Metadata Configuration:** Select assigned metadata configuration.
- **Video Analytics Configuration:** Select assigned video analytics configuration.
Video interfaces

Click “Video Interfaces” under the Interface Configuration menu. Video Interfaces page appears on the screen. In this page you can see the number of physical video inputs available and adjust the brightness, contrast and saturation values for them.

### Video status
The colour bar reflects the status of the video. Green colour bar means that there is video signal. Yellow colour bar with text tells that there is no video.

### Screenshot from the current video
Indicates what media profile is using this video interface.

### When monitoring an area for security, there may be certain parts within the camera’s field of view that need to be kept private. Masking is a feature that enables these areas to be concealed from view.

### Brightness, Contrast and Saturation values for the video channel

User can configure the encoder to automatically hide certain areas with a mask, which can be adjusted in terms of its colour.

Mask editor shows a screenshot from camera view and overlays a translucent mask on the image.

**Draw mode:** Masked (highlighted) areas are private areas that are removed (concealed) from camera’s view.

**Brush size:** Select brush size for masking.

**Mask color:** Depending on the brightness of the image snapshot, appropriate mask preview color can be chosen. This color affects the preview on mask editor only and doesn’t reflect on the streaming video.

**VIDEO INTERFACES page.**

MASK EDITOR page contains settings for hiding certain areas from the encoded picture.
Additionally there is a JPEG image capture feature that allows taking JPEG snapshots from the video and storing them into a ftp server. It is also possible view JPEG captures with http.

**Continuous:** Device generates a snapshot at specified interval (period) and sends the images to configured FTP server.

**Triggered:** Snapshots are generated when internal event triggers it. Triggering event can be motion detection, tampering or digital IO event.

%d: The day of the month as a decimal number (range 01...31).
%H: The hour as a decimal number using a 24-hour clock (range 00...23).
%I: The hour as a decimal number using a 12-hour clock (range 01...12).
%m: The month as a decimal number (range 01...12).
%M: The minute as a decimal number (range 00...59).
%S: The second as a decimal number (range 00...60).
%S: The milliseconds as a decimal number (range 0000...9999).
%p: Either “AM” or “PM” according to the given time value, or the corresponding strings for the current locale. Noon is treated as “PM” and midnight as “AM”.
%y: The year as a decimal number without a century (range 00...99).
%Y: The year as a decimal number including the century.
%1: Device hostname (manually conf. or received from DHCP-server).

Snapshot Configuration:

**Upload Mode:** Snapshot generation can operate in two separate modes: Continuous and triggered mode.

**Snapshot Properties:** Keeps the event state unchanged for the defined period for instance if an event has occurred the device starts generating snapshots. After event has occurred, device sends first configured number of images before the event and then continues sending images until defined timeout [ms] elapses.

**Period (in milliseconds):** [200 to 86400000 (1 day)].

**Pre Event Duration:** (in number of snapshots).

**Pre Event Duration:** (in seconds).

**Upload URI:** Defines the remote FTP server address. URI can contain arbitrary directory path and device shall create the directory if it does not yet exist.

**Username:** Set username for server.

**Password:** Set password for server.

**Upload Control Buttons:**

- Start uploading using saved configurations
- Stop uploading using saved configurations
- Test single snapshot upload
- Test upload using saved configurations

**Status of Last Uploaded Snapshot:**

- Snapshot upload not started. Snapshot generation not started.

**Snapshot URI example:**

ttp://192.168.0.247/upload/%1_%2_%Y%m%d/camera1_%H%M%S_%4.jpg expands to:

ttp://192.168.0.247/upload/MPH102-RD00101126_20140424/camera1_183059")_830.jpg

**Trigger Configuration**

See section “Event management system” from page 31 for more details.
Video source and sinks

Click “Video Source and Sinks” under the Media Configuration menu. **Video Source Configurations** page appears on the screen. Video overlay settings can be changed on this page, you can enter a text and time/date on the video.

**Note**! Date and time settings can be changed from Date & Time page.

There are four different virtual video sources available for video inputs. This feature allows you to set four different views with/without video overlay content.

![Source 1 - Plain Video 1](image)

**VIDEO SOURCE CONFIGURATIONS** page.
Click “Video Encoders” under the Media Configuration menu. Video Encoder Configurations page appears on the screen. Video encoding settings can be configured on this page, e.g. select format (MJPEG, MPEG-2, MPEG-4 and H.264), set resolution, bit rate, frame rate and multicast IP/port settings for each profile.

This page contains (by default) six different customizable encoding profiles. This feature allows you to set six different video encoding combinations, each with their own settings.

On this page you can also add multiplied multicast/unicast streams from each encoder.

**Encoder 1 - H.264**

![Encoder 1 - H.264](image)

Click this to see more settings.

**VIDEO ENCODER CONFIGURATIONS page.**

<table>
<thead>
<tr>
<th>Common</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td>User defined alias name for video profile (max 63 chars).</td>
</tr>
<tr>
<td>Resolution:</td>
<td>Video resolution, either digital HD1080 or HD720, or analog D1, Half-D1, 4CIF, 2CIF, CIF or QCIF.</td>
</tr>
</tbody>
</table>
**VBR** (Variable Bit Rate) video aims at constant quality, but as the bit rate fluctuates over time.

**CBR** (Constant Bit Rate) video fluctuates in quality, while its multiplexing behaviour is easy to predict. Because in unconstrained VBR video the bit rate fluctuation might be too large, **capped VBR** video is proposed as an alternative. Capped VBR video aims at a constant quality, but when in certain intervals this requires a too high bit rate, the bit rate is limited (i.e., capped) in order to support more video flows on the links, at the expense of a quality reduction.

---

**Trigger Configuration**

See section “Event management system” from page 60 for more details.

---

**Note!** Only even port numbers can be used for RTP, and then the following odd port number shall be used for RTCP (RFC 1889).

---

VIDEO ENCODER CONFIGURATIONS page.
Here you see how the media profile is assigned to a video source.

There are three options; Every frame = IP, Every second frame = IBP, Every third frame = IBBP.

MPEG-2 GOP format.

Simple Profile (SP) is recommended only for decoder compatibility. Interlacing toolsets are not used.

Advanced Simple Profile (ASP) Level 5 enables Macroblock-Adaptive Frame/Field Coding (MBAFF) which offers better image quality and better compression ratio with interlaced video signal. Recommended choice when interlaced stream is selected (D1 and Half-D1 resolutions).

Baseline Profile (BP) Level 3 is recommended only for decoder compatibility. Interlacing toolsets are not used.

Main Profile (MP) Level supports field encoding which offers better image quality and better compression ratio with interlaced video signal. Recommended choice when interlaced stream is selected (D1 and Half-D1 resolutions).

Defines video bitrate mode. There are three options available, variable bitrate (VBR), constant bitrate (CBR) or capped VBR. Rate control is a trade off between quality fluctuations and bit rate variability.

Defines video frame rate (adjustable 1...30fps for PAL/NTSC).

Defines encoding frame interval; for instance when encoding interval is 1, all frames are encoded, value 2 means, every second frame is encoded.

GOP length: GOP is a group of successive pictures within an encoded video stream. Each coded video stream consists of successive GOPs. From the pictures contained in it, the visible frames are generated. For instance if you 25 FPS video stream, GOP= 25 means one I-frame per full frame. GOP = 13 means two I-frames per full frame. GOP = 5 means 5 I-frames, 20 p-frames per second

Encoded video image quality, can adjust in VBR or capped VBR mode.

Encoded video bitrate, 128Kbps...15Mbps.

Enables or disables the trigger feature.

Keeps the event state unchanged for the defined period for instance if an event clears quickly, it does not change its state for the defined timeout, recommended 5 seconds.

Select the event type.

The topic expression of the event.

Event description, filter and values.

Timeout for RTSP session

Destination IP address.

Multicast: Multicast IP address / multicast group. This multicast IP address has to be same at both encoder and corresponding decoders.

Unicast: IP address of receiving decoder.

UDP port number (0...65536). This number has to be same at both encoder and decoder pairs. Use even port numbers only.

Time-To-Live for video packets = number of hops that a packet is permitted to travel before being discarded by a router (0...255).

Video streaming will automatically start after reboot. Changing autostart does not immediately start or stop streams.
Video stream multiplication

Each video encoding profile can be assigned with five (5) different destination addresses (primary stream and additional streams). These addresses can be freely set to unicast, multicast or a combination of these. In addition there is a tick box that enables to filter out P-frames from each output stream for low frame rate applications. This approach provides for a very cost efficient dual streaming in situations where the low frame rate stream is a direct subset of the higher frame rate stream. In practise this means that the number of I-frames is the common nominator. As an example, one MPH241 unit can stream (unicast or multicast) 2 x D1@25fps for monitoring and 4 x 2CIF@3fps (unicast or multicast) for recording simultaneously. The precondition is, the number of I-frames per second in the primary stream should match to frame rate of the low frame rate stream. In the example above the I-frame interval of the primary stream would need to be 8 (GOP = IPPPPPPPiPPPPPPPPPiPP…) generating 3 I-frames per second thus resulting in 3fps stream when P-frames are filtered out. The use of multiple destination addresses up to a certain degree doesn’t load the MPU; however one should take into account that the aggregate bit rate of all output streams does not exceed the capacity of the 100Mbps interface.

Quality of Service (DSCP)(0...63): (Differentiated Services Code Point) field lets you set bits in the stream IP header allowing a network device to apply rules such as how the packet is forwarded in the network and QoS (Quality of service) management.

Transmission mode: All frames is the default option and enables the encoder to pass (stream) all frames (I and P frames). I frames enables encoder to send only I-frames, meaning filtering all P frames. Paused = pause streaming.

Container: RTP (Real-time Transport Protocol), SRTP (Secure Real-time Transport Protocol) or TS (MPEG transport stream).

Note! Only even port numbers can be used for RTP, and then the following odd port number shall be used for RTCP (RFC 1889).
Video streaming performance

The following performance table shows the performance of MPH200 devices in encoding and streaming video signal per video input simultaneously.

Total video sessions = original video stream + multiplied streams.

SRTP (Secure Real-time Transport Protocol) = encrypted RTP stream.

De-interlacing is done by choosing right profile.

| Configurations for single input in two channel encoder (NTSC/PAL) | Encoder 1 | Encoder 2 | Encoder 3 | Encoder 4 | De-interl | Privacy zone masking | Motion detection | Tampering | Text overlay | Total sessions | SRTP sessions | Audio |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| D1 30fps | 4CIF 30fps | 30fps | Yes | 40 chars | 3 | 3 | 1XAAC stereo |
| 6Mbps | 6Mbps | | | | | | | |
| D1 30fps | 4CIF 15fps | 15fps | Yes | QCIF 5fps | Yes | 40 chars | 3 | 3 | 1XAAC stereo |
| 6Mbps | 6Mbps | | | | | | | |
| D1 30fps | 2CIF 30fps | Yes | QCIF 5fps | Yes | 40 chars | 3 | 3 | 1XAAC stereo |
| 6Mbps | 3Mbps | | | | | | | |
| CIF 30fps | CIF 30fps | CIF 30fps | CIF 30fps | CIF 30fps | 40 chars | 4 | 4 | 1XAAC stereo |
| 1.5Mbps | 1.5Mbps | 1.5Mbps | 1.5Mbps | 1.5Mbps | | | | |

<table>
<thead>
<tr>
<th>Configurations for single input in single channel encoder (NTSC/PAL)</th>
<th>Encoder 1</th>
<th>Encoder 2</th>
<th>Encoder 3</th>
<th>Encoder 4</th>
<th>De-interl</th>
<th>Privacy zone masking</th>
<th>Motion detection</th>
<th>Tampering</th>
<th>Text overlay</th>
<th>Total sessions</th>
<th>SRTP sessions</th>
<th>Audio</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1 30fps</td>
<td>D1 30fps</td>
<td>4CIF 30fps</td>
<td>4CIF 30fps</td>
<td>30fps</td>
<td>Yes</td>
<td>QCIF 5fps</td>
<td>Yes</td>
<td>40 chars</td>
<td>8</td>
<td>4</td>
<td>1XAAC stereo</td>
<td></td>
</tr>
<tr>
<td>6Mbps</td>
<td>6Mbps</td>
<td>6Mbps</td>
<td>6Mbps</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1080p 30fps</td>
<td>20Mbps</td>
<td>Yes</td>
<td>QCIF 5fps</td>
<td>Yes</td>
<td>40 chars</td>
<td>2</td>
<td>1</td>
<td>1XAAC stereo</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>720p 30fps</td>
<td>10Mbps</td>
<td>Yes</td>
<td>QCIF 5fps</td>
<td>Yes</td>
<td>40 chars</td>
<td>4</td>
<td>2</td>
<td>1XAAC stereo</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Available video streaming performance for MPH200 series encoders.

**Note!** Video traffic could overload Fast Ethernet throughput depending on number of streams/bitrate combination. Be sure that the configuration does not exceed Fast Ethernet port throughput.
**Recommended bitrates for H.264 encoding.**

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Min*</th>
<th>Max</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1</td>
<td>1900</td>
<td>1900</td>
<td>5500</td>
</tr>
<tr>
<td>4CIF</td>
<td>1900</td>
<td>1900</td>
<td>5500</td>
</tr>
<tr>
<td>Half D1</td>
<td>1000</td>
<td>1000</td>
<td>3000</td>
</tr>
<tr>
<td>2CIF</td>
<td>1000</td>
<td>1000</td>
<td>3000</td>
</tr>
<tr>
<td>CIF</td>
<td>500</td>
<td>500</td>
<td>1700</td>
</tr>
<tr>
<td>QCIF</td>
<td>150</td>
<td>150</td>
<td>500</td>
</tr>
</tbody>
</table>

*Note! Minimum (Min) values may be smaller without any picture quality degradation.*

**Recommended bitrates for MPEG-4 encoding.**

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Min*</th>
<th>Max</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1</td>
<td>2200</td>
<td>2200</td>
<td>6000</td>
</tr>
<tr>
<td>4CIF</td>
<td>2200</td>
<td>2200</td>
<td>6000</td>
</tr>
<tr>
<td>Half D1</td>
<td>1200</td>
<td>1200</td>
<td>3200</td>
</tr>
<tr>
<td>2CIF</td>
<td>1200</td>
<td>1200</td>
<td>3200</td>
</tr>
<tr>
<td>CIF</td>
<td>600</td>
<td>600</td>
<td>2000</td>
</tr>
<tr>
<td>QCIF</td>
<td>200</td>
<td>200</td>
<td>600</td>
</tr>
</tbody>
</table>

**Recommended bitrates for MJPEG encoding.**

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Min*</th>
<th>Max</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1</td>
<td>6000</td>
<td>6000</td>
<td>12000</td>
</tr>
<tr>
<td>4CIF</td>
<td>6000</td>
<td>6000</td>
<td>12000</td>
</tr>
<tr>
<td>Half D1</td>
<td>3000</td>
<td>3000</td>
<td>6000</td>
</tr>
<tr>
<td>2CIF</td>
<td>3000</td>
<td>3000</td>
<td>6000</td>
</tr>
<tr>
<td>CIF</td>
<td>2000</td>
<td>2000</td>
<td>4500</td>
</tr>
<tr>
<td>QCIF</td>
<td>600</td>
<td>600</td>
<td>1300</td>
</tr>
</tbody>
</table>

**Recommended bitrates for MPEG-2 encoding.**

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Min*</th>
<th>Max</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>D1</td>
<td>2500</td>
<td>2500</td>
<td>6000</td>
</tr>
<tr>
<td>4CIF</td>
<td>2500</td>
<td>2500</td>
<td>6000</td>
</tr>
<tr>
<td>Half D1</td>
<td>1300</td>
<td>1300</td>
<td>3500</td>
</tr>
<tr>
<td>2CIF</td>
<td>1300</td>
<td>1300</td>
<td>3500</td>
</tr>
<tr>
<td>CIF</td>
<td>700</td>
<td>700</td>
<td>2500</td>
</tr>
<tr>
<td>QCIF</td>
<td>200</td>
<td>200</td>
<td>600</td>
</tr>
</tbody>
</table>

**Recommended bitrates for HD video encoding.**

<table>
<thead>
<tr>
<th>Resolution</th>
<th>Min*</th>
<th>Max</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>H.264</td>
<td>4...5</td>
<td>4.6..5.8</td>
<td>8...10</td>
</tr>
<tr>
<td>MPEG-4</td>
<td>4.6..5.8</td>
<td>8...10</td>
<td>21.5...24</td>
</tr>
<tr>
<td>MPEG-2</td>
<td>8...10</td>
<td>21...24</td>
<td>31.5...37.8</td>
</tr>
<tr>
<td>MJPEG</td>
<td>12.6...15.8</td>
<td>21...24</td>
<td>31.5...37.8</td>
</tr>
</tbody>
</table>
Recommended GOP sizes for H.264 encoding. 

<table>
<thead>
<tr>
<th>Rate Control Mode</th>
<th>GOP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Min</td>
</tr>
<tr>
<td>CBR</td>
<td>7</td>
</tr>
<tr>
<td>Capped VBR</td>
<td>7</td>
</tr>
<tr>
<td>VBR</td>
<td>7</td>
</tr>
</tbody>
</table>

Recommended GOP sizes for MPEG-4 encoding. 

<table>
<thead>
<tr>
<th>Rate Control Mode</th>
<th>GOP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Min</td>
</tr>
<tr>
<td>CBR</td>
<td>7</td>
</tr>
<tr>
<td>Capped VBR</td>
<td>7</td>
</tr>
<tr>
<td>VBR</td>
<td>7</td>
</tr>
</tbody>
</table>

Recommended GOP sizes for MPEG-2 encoding. 

<table>
<thead>
<tr>
<th>Rate Control Mode</th>
<th>GOP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Min</td>
</tr>
<tr>
<td>CBR</td>
<td>7</td>
</tr>
<tr>
<td>Capped VBR</td>
<td>7</td>
</tr>
<tr>
<td>VBR</td>
<td>7</td>
</tr>
</tbody>
</table>

Field Encoding | Not available | Not available | H.264 Base Profile (BP) Level 3
Deinterlacer | x | One field used |
Field Encoding | na | na | x |
Deinterlacer | x | One field used |
Field Encoding | x | x |
Deinterlacer | x | One field used |
MBAFF | x | x |
Deinterlacer | x | One field used |
Field Encoding | x | x |
Deinterlacer | x | One field used |
Type field value | 0 |
Type specific field values | 0 | 1 & 2 | 0 | 1 & 2 | 0 |

Supported interlace coding tools for the MPH video encoders.
Configuring audio channels

**Audio connection**

MPH200 encoder supports two bi-directional audio channels, which can be used for one stereo audio or two mono audio purposes. The audio interface supports both balanced (both channels separately) and unbalanced wiring. Audio input impedance is 6.6 kΩ in unbalanced mode and 13 kΩ in balanced mode. The device is capable of driving 0.707 Vrms (single-ended output) / 1.414 Vrms (differential output) into a 10 kΩ load. The audio channels operates independently, i.e. despite the absence of all video signals.

*Note! Physical audio interface is shared between audio interfaces, so audio interface mode (balanced/unbalanced) and sampling rate configured to each used audio encoder and decoder configuration must be equal.*

Normally audio is transmitted and received in separate RTP streams. However, if video stream is using transport stream (TS), audio packets can be encapsulated inside the same video stream. Note that if audio packets are encapsulated inside the video stream, MPH audio decoder cannot decode it. Audio settings can be configured from web user interface (WebUI).

<table>
<thead>
<tr>
<th>Pin</th>
<th>Balanced signal</th>
<th>Unbalanced signal</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Audio in -</td>
<td>GND for Audio 1 in</td>
</tr>
<tr>
<td>2</td>
<td>Audio in +</td>
<td>Audio 1 in</td>
</tr>
<tr>
<td>3</td>
<td>GND (shield)</td>
<td>GND</td>
</tr>
<tr>
<td>4</td>
<td>Audio out +</td>
<td>Audio 2 out</td>
</tr>
<tr>
<td>5</td>
<td>Audio out -</td>
<td>GND for Audio 2 out</td>
</tr>
</tbody>
</table>

Audio connector’s pinout.

**Audio channel configuration**

MPH is an ONVIF compliant device and audio channel encoder configuration is designed according to ONVIF standard. Audio decoder is designed similarly but is not according to ONVIF standard.

*Note! Before adding the audio configuration to a video profile, make sure that video stream is stopped on the MAIN page.*
Adding audio encoder to media profile:
1. Add to media profile (Media Configuration/Media Profiles) desired audio source configuration. Choose “Mono Audio In 1”, “Mono Audio In 2”, “Stereo Audio In”.
2. Add to media profile desired audio encoder configuration (Media Configuration/Audio Encoders). Choices are “Audio Encoder - AAC-LC” and “Audio Encoder – G.711”.

Adding audio decoder to media profile:
3. Add to media profile (Media Configuration/Media Profiles) desired audio source configuration. Choose “Mono Audio In 1”, “Mono Audio In 2”, “Stereo Audio In”.
4. Add to media profile desired audio encoder configuration (Media Configuration/Audio Decoders). Choices are “Audio Encoder - AAC-LC” and “Audio Encoder – G.711”.

Audio configuration flowchart.
1. Audio interfaces

Click “Audio Interfaces” under the Interface Configuration menu. Audio Interfaces page appears on the screen. In this page you can see the number of physical audio inputs available and choose audio input mode (balanced or unbalanced).

<table>
<thead>
<tr>
<th>COMMON</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common</strong></td>
</tr>
<tr>
<td>Options</td>
</tr>
<tr>
<td>Mode</td>
</tr>
</tbody>
</table>

Audio interface mode selection. Affects both input and output connection.

<table>
<thead>
<tr>
<th>PHYSICAL SOURCES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AudioSourceStereoInterface1</strong></td>
</tr>
<tr>
<td><strong>Status</strong></td>
</tr>
<tr>
<td>Channels</td>
</tr>
<tr>
<td>Sample rate</td>
</tr>
<tr>
<td><strong>Usage</strong></td>
</tr>
<tr>
<td>Profiles</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PHYSICAL SINKS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AudioSinkStereoInterface1</strong></td>
</tr>
<tr>
<td><strong>Status</strong></td>
</tr>
<tr>
<td>Channels</td>
</tr>
<tr>
<td>Sample rate</td>
</tr>
<tr>
<td><strong>Usage</strong></td>
</tr>
<tr>
<td>Profiles</td>
</tr>
</tbody>
</table>
2. Audio source and sinks

Click “Audio Sources” under the Media Configuration menu. **Audio Source & Sink Configurations** page appears on the screen. You can rename the audio settings name but by default the name describes the physical port location in connector, e.g. “Mono Audio In 1 (pins 1, 2)”. 

![Audio Source-Stereo](image)

<table>
<thead>
<tr>
<th>Common</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>AudioSource-Stereo</td>
</tr>
<tr>
<td>Audio source</td>
<td>AudioSourceStereoInterface1</td>
</tr>
<tr>
<td>Usage Profiles</td>
<td>Not used in any profile</td>
</tr>
</tbody>
</table>

![Audio Source-MonoLeft](image)

<table>
<thead>
<tr>
<th>Common</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>AudioSource-MonoLeft</td>
</tr>
<tr>
<td>Audio source</td>
<td>AudioSourceStereoInterface1</td>
</tr>
<tr>
<td>Usage Profiles</td>
<td>Not used in any profile</td>
</tr>
</tbody>
</table>

![Audio Source-MonoRight](image)

<table>
<thead>
<tr>
<th>Common</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>AudioSource-MonoRight</td>
</tr>
<tr>
<td>Audio source</td>
<td>AudioSourceStereoInterface1</td>
</tr>
<tr>
<td>Usage Profiles</td>
<td>Not used in any profile</td>
</tr>
</tbody>
</table>

![Audio Sink-Stereo](image)

<table>
<thead>
<tr>
<th>Common</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>AudioSink-Stereo</td>
</tr>
<tr>
<td>Audio sink</td>
<td>AudioSinkStereoInterface1</td>
</tr>
<tr>
<td>Usage Profiles</td>
<td>Not used in any profile</td>
</tr>
</tbody>
</table>

![Audio Sink-MonoLeft](image)

<table>
<thead>
<tr>
<th>Common</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>AudioSink-MonoLeft</td>
</tr>
<tr>
<td>Audio sink</td>
<td>AudioSinkStereoInterface1</td>
</tr>
<tr>
<td>Usage Profiles</td>
<td>Not used in any profile</td>
</tr>
</tbody>
</table>

![Audio Sink-MonoRight](image)

<table>
<thead>
<tr>
<th>Common</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>AudioSink-MonoRight</td>
</tr>
<tr>
<td>Audio sink</td>
<td>AudioSinkStereoInterface1</td>
</tr>
<tr>
<td>Usage Profiles</td>
<td>Not used in any profile</td>
</tr>
</tbody>
</table>
3. Audio encoders

Click “Audio Encoders” under the Media Configuration menu. **Audio Encoder Configurations** page appears on the screen. Audio encoding settings can be configured on this page, e.g. select format: G.711 (uLaw), G.726 (ADPCM), AAC-LC or HE-AAC, set samplerate, bit rate, format and multicast IP/port settings for each profile.

This page contains (by default) four different customizable encoding profiles. This feature allows you to set four different audio encoding combinations, each with their own settings.

On this page you can also add multiplied multicast/unicast streams from each encoder.

**Audio Encoder Configuration - 1**

**Common**

- **Name**: User defined alias name for audio profile (max 63 chars).
- **Format**: Audio format, either G.711, G.726, AAC-LC or HE-AAC.
**Note!** Samplerate value has to be same at both encoder and corresponding decoders.

**Note!** Only even port numbers can be used for RTP, and then the following odd port number shall be used for RTCP (RFC 1889).

**Trigger Configuration**
See section “Event management system” from page 60 for more details.

AUDI0 ENCODER CONFIGURATIONS page.

**Usage**
Profiles: Here you see how the media profile is assigned to a audio source.

**Rate control**
Samplerate: Defines audio codecs samplerate value (8/16/32/44.1 or 48 KHz). Setting a higher samplerate value improves audio file quality and increases its size.

Bitrate: Defines encoded audio bitrate (8..288 kbps). The higher the rate is, the better the quality of sound is. However this also increases the file size.

**Container**: RTP (Real-time Transport Protocol) or TS (MPEG transport stream).

**RTSP Options**: Session timeout: Timeout for RTSP session.
Enable or disables the trigger feature. Keeps the event state unchanged for the defined period for instance if an event clears quickly, it does not change its state for the defined timeout, recommended 5 seconds.

Event subscription (for triggering):
- Events: Select the event type
- Topic Expr: The topic expression of the event
- Message content filter: Event description, filter and values

Streaming Configuration:
- Destination address: Destination IP address. Multicast: Multicast IP address / multicast group. This multicast IP address has to be same at both encoder and corresponding decoders. Unicast: IP address of receiving decoder.
- Destination port: UDP port number (0...65536). This number has to be same at both encoder and decoder pairs. Port number needs to be even, as next odd port is always used for RTCP traffic.
- TTL (Time To Live): Time-To-Live for video packets = number of hops that a packet is permitted to travel before being discarded by a router (0...255).
- Auto start: Audio streaming will automatically start after reboot. Changing autostart does not immediately start or stop streams.
- Quality of Service (DSCP): (Differentiated Services Code Point) field lets you set bits in the stream IP header allowing a network device to apply rules such as how the packet is forwarded in the network and QoS (Quality of service) management.
- Transmission mode: Default = Normal audio transmission mode:
  - Active: Audio is transmitted.
  - Paused: Audio encoder is ready but paused (no packets transmitted).
  - Triggered = Audio is configured with triggering feature:
    - Active: Audio is transmitted.
    - Paused: Audio encoder is ready but paused (no packets transmitted).
Audio stream multiplication

Each audio encoding profile can be assigned with five (5) different destination addresses (primary stream and additional streams). These addresses can be freely set to unicast, multicast or a combination of these.

The use of multiple destination addresses up to a certain degree doesn’t load the MPU; however one should take into account that the aggregate bit rate of all output streams does not exceed the capacity of the 100Mbps interface.

**Stream multiplication**: Destination IP address. **Multicast**: Multicast IP address / multicast group. This multicast IP address has to be same at both encoder and corresponding decoders. **Unicast**: IP address of receiving decoder. UDP port number (0...65536). This number has to be same at both encoder and decoder pairs.

**Destination address**: Destination port

**Quality of Service (DSCP/DiffServ)**: Differentiated Services Code Point field lets you set bits in the stream IP header allowing a network device to apply rules such as how the packet is forwarded in the network and QoS (Quality of service) management.

**Transmission mode**: **Active**: Audio is transmitted. **Paused**: Audio encoder is ready but paused (no packets transmitted). **Add new copy**: Adds new copy from stream.
Configuring data channels

**Data connections**

The MPH200 encoder provides two independent bi-directional data channels. Supported data modes for data channel 1 are RS422, RS485-2w and RS485-4w. Data channel 2 is fixed for RS232 mode only. Data port settings can be configured from web user interface (WebUI) or Command Line Interface (CLI).

Data channel 1 is fully configurable and supports RS422, RS485 2-wire and RS485 4-wire modes. ONVIF PTZ service is only available from data channel 1, whereas data channel 2 is used either for RS232 data mode or command-line interface usage. Both channels support tunneling protocol and can be connected to the PTZ controller application.

The default factory settings are:
- Data channel 1: **RS485-2w**
- Data channel 2: mode is set to **CLI** (Command Line Interface) usage

<table>
<thead>
<tr>
<th>Pin</th>
<th>Signal</th>
<th>RS232</th>
<th>RS422</th>
<th>RS485-2w</th>
<th>RS485-4w</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data 1</td>
<td>OUT +</td>
<td>OUT +</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>OUT -</td>
<td>OUT -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>IN +</td>
<td>IN/OUT +</td>
<td>IN +</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>IN -</td>
<td>IN/OUT -</td>
<td>IN -</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>GROUND</td>
<td>GROUND</td>
<td>GROUND</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Data 2</td>
<td>TX</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>RX</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>GROUND</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Data connector’s pinout and supported data types.

<table>
<thead>
<tr>
<th>Led</th>
<th>Colour</th>
<th>Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>T</td>
<td>Green</td>
<td>Active Connection. Terminal server TCP connection is established.</td>
</tr>
<tr>
<td></td>
<td>Blinking Green</td>
<td>On stream.</td>
</tr>
<tr>
<td></td>
<td>OFF / Dark</td>
<td>No stream.</td>
</tr>
</tbody>
</table>

T - (terminal server) Led indicator operation. This LED indicates the status of Terminal server activity on RS422/485 port.

<table>
<thead>
<tr>
<th>Data 1</th>
<th>Data 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnelling protocol</td>
<td>x</td>
</tr>
<tr>
<td>ONVIF PTZ protocol</td>
<td>x</td>
</tr>
<tr>
<td>RS232</td>
<td>x</td>
</tr>
<tr>
<td>RS422, RS485</td>
<td>x</td>
</tr>
<tr>
<td>Command line interface</td>
<td>x</td>
</tr>
</tbody>
</table>

MPH unit provides two data channels for PTZ cameras on Terminal server page.
RS485-2w data connection diagram. A 2-wire RS485 network is implemented as a half-duplex system using single twisted-pair cabling. This means that data can flow in both directions but only in one direction at a time.

RS422 / RS485-4w data connection diagram. A 4-wire RS485 network can be implemented as a full-duplex system using two twisted-pair buses where each bus is used for each direction of transmission.

Data type descriptions

RS232 is an unbalanced data format (i.e. the signal wire working against a reference – ground). Simplex RS232 requires two connections (signal and ground). Full-duplex RS232 requires three connections (signal TX, signal RX and ground).

RS422 is a balanced data format. Simplex RS422 requires three data connections (+/- and ground). Full-duplex RS422 requires five data connections (in+/in-, out+/out- and ground).

RS485 is used for full-multipoint communications where multiple transceiver devices may be connected to a single twisted-pair signal cable. Most RS485 systems use a Master/Slave architecture, where each Slave unit has a unique address and responds only to packets addressed to that unit. Packets are generated by the Master (e.g. CCTV controller keyboard), which periodically ‘polls’ all connected Slave units (e.g. CCTV camera receiver units). The Slave unit that has been addressed then sends the appropriate reply packet back to the Master. Slave units have no means of initiating communication without the risk of a collision so they need to be assigned the ‘right to transmit’ by the Master (by polling). RS485 exists in two versions, 2-wire and 4-wire.

Data termination and biasing

Termination is used to match impedance of a node to the impedance of the transmission line being used. When impedance are mismatched, the transmitted signal is not completely absorbed by the load and a portion is reflected back into the transmission line. If the source, transmission line and load impedance are equal these reflections are eliminated.

Biasing -> the lines will be biased to known voltages and nodes will not interpret the noise from undriven lines as actual data; without biasing resistors, the data lines float in such a way that electrical noise sensitivity is greatest when all device stations are silent or unpowered.

Data mode | Input termination options
---|---
RS232 | None
RS422 | Line termination (120 Ω)
RS485 - 2w | No term (with failsafe)
| Hard bias (forced 680 Ω line biasing)
| Line termination (120 Ω)
RS485 - 4w | No term (with failsafe)
| Hard bias (forced 680 Ω line biasing)
| Line termination (120 Ω)

Data input termination options for data channels. Data termination connects 120 Ω between pins. Hard bias connects 680 Ω (+input) to +5V and GND (- input).
An analog PTZ camera can be controlled remotely over an IP network via the MPH encoder’s serial port (RS-232/422/485). MPH encoders support two ways to control PTZ camera, ONVIF PTZ service and transparent RS-data tunneling.

Click “Terminal Server” under the Interface Configuration menu. Terminal Server - Data Ports page appears on the screen. Data port settings can be changed on this page.

**Data 1 & 2 (WebUI)**

**Common**
- **Name**: User defined alias name for data interface (max 64 chars)
- **Mode**: Data connection protocol towards the external device, options are RS422, RS485 2-wire and RS485 4-wire (Data 1) and RS232 (Data 2)
- **Baud rate**: Data channel connection speed (range 600…230 400 bps)
- **Data bits**: Number of data bits. Options are 5, 6, 7, 8 & 9
- **Parity**: A data-checking technique, which uses an extra bit, Options are Even, Odd & N (None)
- **Stop bits**: Options are 1 or 2
- **Termination**: Enabled/disabled (Data 1). The default setting is enabled.
- **Biasing**: Enabled/disabled (Data 1). The default setting is disabled.

**Usage Model**
- **Mode**: Data usage mode. By MPH encoder you can control PTZ cameras via two protocols, Tunnelling Protocol and OnVIF.
Data port mode can be set to the tunneling protocol usage from the Terminal Server page.

**Tunneling Protocol**

Tunnelling Protocol enables you to establish point to point connection between encoder, decoder and management system. There are three options, TCP server, TCP client and UDP multicast.

### Tunneling Configuration

<table>
<thead>
<tr>
<th>Protocol</th>
<th>TCP Server - Listens at</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Port</td>
<td>16360</td>
</tr>
<tr>
<td>Status</td>
<td>Tunneling Inactive</td>
</tr>
</tbody>
</table>

**State**

- **Data counter**
  - Rx: 0 bytes
  - Tx: 0 bytes

**Note**

In order to have correct channel status information, you can check the followings:

- Device address is configured correctly in PTZ nodes page.
- Serial Port configuration : connection mode (RS-485 4-wire, etc), Baud rate, and parity. in terminal server page.
- PTZ configuration is added to a media profile. PTZ configuration “PTZ1” by default is added to media Profile 1.

**Data counter**

Data port’s traffic counter.
ONVIF PTZ service

ONVIF PTZ service lets you control the camera from ONVIF client application. ONVIF PTZ service is available from data channel 1. It means that MPH converts ONVIF PTZ commands to Pelco D commands and transmits that to the camera via Data channel 1.

In order to activate the ONVIF PTZ protocol, data port mode must be first set to the ONVIF PTZ service usage from the Terminal Server page.

**Step-by-step flowchart how to configure ONVIF PTZ data 1 channel in the MPH encoder.**

1. **Terminal Service**
   (enable ONVIF PTZ on DATA 1)

2. **PTZ Node**
   (set a bus address for camera)

3. **PTZ Configurations**
   (set limitations for PTZ operations)

4. **Media Profile**
   (PTZ configurations assignment)

2. Next on the PTZ Nodes page you need to set a Bus address for the camera, you can have two cameras using the same Data port with different bus addresses.

3. Then on the PTZ configurations page you can set limitations for PTZ operations. For each PTZ node you can limit speed, pan, tilt and zoom.

4. Finally on the Media profiles page you need to assign the PTZ configuration to the media profile where the camera is connected to.
Configuring contact closure channels

**Contact closure loop (CCL) connection**

The MPH200 series video encoders provide two inputs and one contact closure output channel line.

**Contact closure inputs**

There are two different CC input connection types. First one is for a normal short circuit which is called “dry contact closure”. Dry contact closure enables you to switch ON & OFF input signals between connector’s contact pins (internal power source). Second type is called “Optoisolated” current loop input signals (logical 0 = 0.0VDC...+1.4VDC and logical 1 = +2.2VDC...+30.0VDC) between contact pins (external power source). Input pins nominal current consumption is 3 mA.

**Contact closure output**

CC output is a normal relay on/off - output signal (30V / 0.6A) between connector’s contact pins.

*Note! If voltage output is needed from output, do not use Vcc (10mA) pin for it. Instead use external voltage source or device power supply for it. See an example connection bottom.*
Device generates events from changes in digital input states. Events are used internally to trigger configuration changes in video encoding or provided for ONVIF clients through metadata streams and ONVIF notification interfaces (Real Time Notification Interface and Base Notification Interface).

Click “Digital I/O” under the Interface Configuration menu. Contact Closure / Inputs & Outputs page appears on the screen. Contact closure settings can be changed on this page.

**Contact closure input 1 & 2**

- **Common**
  - **Name**: User defined alias name for contact closure interface (max 64 chars)
  - **Input filter**: Monitors how many state changes happen (from close to open or vice versa) during the time frame given by “Filter Time” parameter. If during this time frame CC input state changes more than once, the input state is set as “unstable”.
  - **Filtering time**: Time frame for “Input Filter” (100...2000 ms).
  - **Logical State**: The default state for CC input (open/closed).
  - **Time of last change**: Shows the time when the last cc state was changed.
  - **Change counter**: Shows the total number of state changes that has been registered by a given input CC.

- **Tunneling Protocol**
  - **Protocol**: IP connection type. There are three options: “TCP Client - Connects to”, “TCP Server - Listens at” and “UDP multicast - Sends to”.
  - **Address**:
    - **Port**: UDP port number (0...65535). This number has to be same at both encoder and decoder pairs.
  - **Connection status**: Shows connection status. The status can be active, disabled or no connection.
**Bistable** – After changing the state, the relay remains in this state.

**Monostable** – After changing the state, the relay returns to its idle state after the specified time.

**Note!** When Contact closure tunneling is used, Bistable mode is only applicable. Monostable mode is applicable when relay output is controlled by ONVIF commands from ONVIF client.

| **Common** | **Type** | DigitalOutput |
| **Name** | Output 1 |
| **Idle State** | Open (Closed) |
| **Mode** | Monostable, Bistable |
| **Delay time** | 30000 ms |
| **Status** | Open (Inactive) |

| **Logical State** | 0 |
| **State Source** | ONVIF Commands Only (Device Management Service), Tunneling Protocol, ONVIF Message Filter |

| **Tunneling Protocol** | **Protocol** | TCP Server - Listeners at |
| **Address** | 0.0.0.0 |
| **Port** | 16000 |
| **Connection status** | No Connection |

| **Event Subscription (For Active State)** | **Event** | Signal lost for Video1 |
| **Topic Expression** | Add | Replace |
| **Message Content Filter** | |

| **Event Subscription (For Idle State)** | **Event** | Signal lost for Video1 |
| **Topic Expression** | Add | Replace |
| **Message Content Filter** | |

### Contact closure output

CC output can be controlled either with ONVIF Commands (SetRelay-OutputState) or by receiving state using tunneling protocol.

- **User defined alias name for contact closure interface (max 64 chars)**
- **User defined default standby mode for contact closure output pins.**
  - **Open** means that the output relay is open in inactive mode.
  - **Close** means the output relay is closed in inactive mode.
  - **Mode**: Contact closure output state mode, either Monostable or Bistable.
  - **Delay time**: Time period in monostable mode when state changes back to the idle state.

- **Current CC output state.**

**Tunneling protocol**

- **There are three connection types.** Point-to-point (Client/server) based connection which is done by TCP client/server protocol. If the encoder is set to be TCP Server, then the decoder or management system must be set to TCP Client, or vice versa. In UDP multicast mode, you can control multiple devices and connection can be point to multipoint.

- **Address**: Destination IP address
- **Port**: UDP port number (0...65535). This number has to be same at both encoder and decoder pairs

**Connection status**: Current CC connection status

---

**Trigger Configuration**

See section "Event management system" from page 60 for more details.
### Triggering

MPH internally controls events as specified by ONVIF. Events are generated from digital IO inputs, motion detection, tampering detection and video signal loss and each of those generate event with different topic.

### Operation

MPH can trigger actions for video, audio and contact closers output. These events are also available for video management system to trigger configurable alarms. You can add multiples event at the same time and each one triggers action.

#### Following events are available:

<table>
<thead>
<tr>
<th>Event</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signal lost for video 1 and 2</td>
<td>Signal restored for video 1 and 2</td>
</tr>
<tr>
<td>I/O Inputs activation</td>
<td>I/O Inputs deactivation</td>
</tr>
<tr>
<td>Motion Detection above the threshold for video 1 and 2</td>
<td>Motion Detection below the threshold for video 1 and 2</td>
</tr>
<tr>
<td>Camera tampered</td>
<td>Camera tamper removed</td>
</tr>
</tbody>
</table>

In addition to event topics, events contain data describing the event such as the video interface related, amount of motion and threshold, etc.

The event data is available in the “Message Content filter” box, which is XPath format for matching XML content. Triggering occurs when defined “Topic expression” and “message content filter” matches the internal event.
Video triggering

For video the triggering can trigger actions such as changing video settings, frame rate, bit rate and video quality for each video profile based on events.

Audio triggering

For audio the triggering can activate or deactivate audio transmission.

Contact Closure triggering

For contact closure (digital I/O) the triggering changes the output state in case of an event.

An example from Video Encoder Configurations page shows: The video bit rate and frame rate change when an event triggered.

An example from Audio Encoder Configurations page shows: Audio stream is paused in normal mode but when an event triggered, it starts streaming.

An example from Digital I/O page.
Click “Video Analytics” under the Media Configuration menu. **Video Analytics Configurations** page appears on the screen. Video Analytics settings can be configured on this page. All the parameters can be configured dynamically i.e. when video analytics configuration is active.

### Common
- **Type:** Adaptive motion detection.
- **Name:** User defined name for video analytics configuration object (max 64 chars).

### Usage
- **Profiles:** It shows the media profile which the video analytic is associated with.

### Parameters
- **Engine Cfg Name:** User defined name for video analytics engine configuration (max 64 chars).
- **Sensitivity:** Motion detection algorithm sensitivity. Range is 1-100%
- **Learning rate:** Motion detection algorithm learning rate.
- **Mask:** When monitoring an area for security, there may be certain parts within the camera’s field of view that need to be kept private. Masking is a feature that enables these areas to be concealed from view.

### Rules
- **Type:** Motion detection threshold.
- **Name:** User defined name for rule (max 64 chars).
- **Threshold (0%..100%):** Threshold percentage to trigger rule. Range is 0-100%
- **Messages:** User can add/remove rules (maximum of 5 rules are supported per configuration).

---

**Note:** Video Analytics configuration is activated if the configuration is included in at least one of the profiles. **Profile does not need to be activated when configuring video analytics settings.**
Metadata is a data channel and one of the Onvif features which can carry events, PTZ status, and/or video analytics data for network video devices.

**Metadata configurations**

- **Common**
  - **Name**: User defined alias name for metadata configuration (max 64 chars).
  - **Analytics**
    - **Scene Description**: Enable/disable scene description. When enabled, adds video analytics results from each analyzed frame to metadata. With motion detection this includes amount of motion detected and defined threshold level.
  - **PTZ Status**
    - **Status**: Enable/disable PTZ control status.
    - **Position**: Enable/disable PTZ camera position.
  - **Event Subscription**
    - **Topics**: Event subscription defines which events are included to metadata stream.
    - **Message content filter**: Event subscription message content filter.
  - **Multicast Configuration**
    - **Destination address**: You can set a multicast address and port number for a Metadata stream, the multicast address can be the same as video stream multicast address but with different port number.
    - **Destination port**: Destination port
    - **Time To Live (TTL) (1..255)**: Multicast Time-To-Live for metadata packets.
    - **Auto start**: If enabled, metadata streaming starts automatically after reboot (does not immediately start or stop streams).
    - **Quality of Service (DSCP)**: Defines QoS class in differentiated services (DiffServ) traffic management. DSCP/DiffServ (Differentiated Services Code Point) is a field in the IP headers that affects the priority of packet in the network per hop basis.

**Note!** Parameters cannot be changed when streaming is active.

**Metadata Configurations**

- Click "Metadata" under the Media Configuration menu. **Metadata Configurations** page appears on the screen. You can add a metadata configuration to an existing media profile, adding a metadata configuration to a profile means that streams using that profile contain metadata. Four metadata configurations are supported. In addition to video analytics information, metadata can transmit PTZ camera status and position to the Onvif client. Carrying other events such as “loss of video signal” is done by metadata channel. Metadata transmits video analytics information like motion detection over RTP stream in XML format. Currently MPH transmits motion detection information, PTZ camera status (feedback) and video loss event over metadata channel.

**Note!** Only even port numbers can be used for RTP, and then the following odd port number shall be used for RTCP (RFC 1889).
Click “Network” under the Media Configuration menu. Ethernet Interface & Network Settings pages appears on the screen. Device’s network settings can be changed on these pages.

**Ethernet Interface**

**Common**
- **Type**: Device’s Ethernet Interface type.
- **Module**: Shows the status of SFP module.
- **Link status**: Shows the current link status and connection type.
- **Ethernet MAC**: MAC address of the device.

**Link Level Configuration**
- **Mode**: You can select the connection mode, Auto negotiation or fixed rate.
- **MTU (1000 to 1500)**: You can adjust the maximum transmission unit based on your connection type, default value is 1492 bytes. The MTU range is from 68 to 1500.

**IPv4 Configuration**
- **Enable IPv4**: IPv4 enabled (change not supported).
- **IP address resolution**: You can set a static IP address for the unit (in case of static IP the user can set IP address, subnet mask and gateway address) or select DHCP mode to obtain IP address automatically. When you enable ZeroConf protocol, the device will set an IP address randomly to itself if it fails to find the DHCP server after few trials.
- **IP address**: IP address of the device.
- **Netmask**: Netmask address of the device.
- **Gateway**: Gateway address for router definition.
Network settings

Hostname Configuration

Hostname: User defined hostname for device (max 64 chars). If the DHCP server is configured to assign a hostname to the unit, it will be used, and will be shown here.

Note! Underline is not allowed, use only marks A...Z, a...z, 0...9 and – (dash)

Domain Name Server Configuration

DNS configuration mode: Static Mode or DHCP Mode. In Static NTP mode you can set up to 3 NTP servers, change the priority by moving the servers up and down and no needed servers can be deleted. The server on the top of the list has the highest priority and decreases down the list. In DHCP mode all controls are disabled and the priority is assigned by the DHCP server.

Search domains: Searches the given DNS domain (e.g. teleste.com) for lookup an IP address; you can add up to three domain names. You can change the DNS domains’ priority by moving them up and down. The top of the list has the highest priority.

DNS servers: Sends name resolution query to then given DNS servers, you can add up to three DNS sever. You can change the DNS servers’ priority by moving them up and down. The one on the top of the list has the highest priority.

Network Time Protocol (NTP) Configuration

NTP configuration mode: If you select DHCP server to control DNS and NTP settings, the manually entered DNS and NTP servers will be discarded.

NTP servers: You can add up to three NTP servers for time synchronisation. You can change the NTP servers’ priority by moving them up and down. The one on the top of the list has the highest priority.
Click “Date & Time” under the Administration menu. **Date & Time Settings** page appears on the screen. Device’s Date & Time settings can be changed on this page. This page also shows the system time and the local time calculated using the time zone set on the device.

- **Local Time**
  - **Time zone**: Selected time zone. Defines how conversion from system time (UTC) to local time is done. For user the local time is shown, for example in video text overlay timestamps. Conversion also takes daylight saving time into account.
  - **Local time**: Shows local time.
  - **System time**: Shows system time (always in GMT).

- **Time Source**
  - **Mode**: Source for the clock, either manual or NTP synchronized.
  - **NTP info**: Status: NTP status (synchronization OK, No NTP servers configured).
  - **Current NTP servers**: Shows configured NTP servers IP address.
  - **Manual time**: Shows system time set manually.
  - **Set UTC time**: Set UTC time manually.

- **Time & Date Format**
  - **Date**: Select date format type.
  - **Time**: Select time format type.

**Notes!** If month is entered as 14, the date will change to February of the next year and if date is entered as 32, the date will change to the 1st of the next month if the number of days in the current month is 31.

The date and time entered in the boxes has to match the format specified. If the required date is 1st Jan 2011, it has to be entered as 01/01/2011 and not as 1/1/2011. The latter setting will throw up an error when saved.
Device management

Configuration Backup
- **Backup:** Click Backup to store the current configuration to a file.
- **Restore:** Click Browse to find/select the stored configuration file to the device and then click Restore & Reboot to save the configuration file to the device. Device restarts automatically after pressing this button.

Device control
- **Reboot Device:** Click Reboot device to restart the device.
- **Soft Factory Reset:** Click Soft Factory Reset to make a soft factory reset to the device -> restores all, except IP configuration to the default factory settings.
- **Hard Factory Reset:** Click Hard Factory Reset to make a hard factory reset to the device -> restores all settings to default factory settings.

Software update
- **Current software:** Shows device’s current firmware version.
- **Upload:** Click Browse to find/select the new firmware file to the device and then click Upload & Reboot to upload the firmware file to the device. Device restarts automatically after pressing this button.
- **Download from URL:** Click Download & Reboot to upload the new firmware file from user specified server (TFTP, FTP and HTTP) to the device. An example of FTP URL: "ftp://FTP_SERVER_IP/MPH-x-x.x.xx-x.bin". Device restarts automatically after pressing this button.

License management
- **Device serial number:** Shows device serial number.
- **License status:** Shows current licence status.
- **Current license:** Shows device’s current licence(s).
- **Install license:** Copy a licence code here and then click Install & Reboot to take the license to use. Device restarts automatically after pressing this button.

License features:
Services

<table>
<thead>
<tr>
<th>Network Services</th>
<th>Services Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP enabled</td>
<td>HTTP is always enabled.</td>
</tr>
<tr>
<td>HTTP port</td>
<td>Port 80 is used always.</td>
</tr>
<tr>
<td>HTTPS enabled</td>
<td>Enable/disable HTTPS.</td>
</tr>
<tr>
<td>HTTPS port</td>
<td>Configure HTTPS server port.</td>
</tr>
<tr>
<td>RTSP enabled</td>
<td>Enable/disable RTSP (Real time streaming protocol) server.</td>
</tr>
<tr>
<td>RTSP port</td>
<td>Configure RTSP server port.</td>
</tr>
<tr>
<td>TLS 1.0</td>
<td>Enable/Disable Transport Layer Security protocol 1.0 (RFC 2246).</td>
</tr>
<tr>
<td>TLS 1.2</td>
<td>Enable/Disable Transport Layer Security protocol 1.2 (RFC 5246).</td>
</tr>
<tr>
<td>HTTP Digest Authentication</td>
<td>Enable/Disable HTTP digest access authentication (RFC 2069).</td>
</tr>
<tr>
<td>Enabled</td>
<td>Note! When is enabled, authentication is mandatory for all profile based JPEG snapshot download.</td>
</tr>
<tr>
<td>Multicast TTL</td>
<td>Multicast Time-To-Live for SAP packets (1...255).</td>
</tr>
<tr>
<td>Announcement interval</td>
<td>SAP timing in seconds (1...999). Retransmit time of SAP-packet. This time has to be same at both encoder and decoder pairs.</td>
</tr>
</tbody>
</table>
**Administrative scope:** Range of multicast IP addresses advertised with SAP. When the stream multicast address is within the SAP scope, end of the scope is used. Otherwise default SAP-address 224.2.127.254 is used. Default SAP-scope is 239.0.0.0 - 239.255.255.255.

**Device Discovery**

WS-Discovery enabled: This enables ONVIF device discovery feature.

---

**Simple Network Management Protocol (SNMP)**

SNMP v2c enabled: Enables SNMP v2c protocol. Requires licence MLH371 installation. Activation disables ONVIF.

Read community: Specifies the read only community (public or private).

Write community: Specifies the write community (public or private).

Trap destination 1...4: Trap Destination defines the IP address of an agent receiving traps.

---

**Syslog**

Syslog is a standard for computer data logging. By using syslog you can collect messages sent from MPH on the syslog sever.

Server: Shows syslog server IP address. If this field is left blank then remote logging is disabled.

---

**Resource Reservation Protocol (RSVP)**

RSVP enabled: This enables RSVP feature (RFC 2205).

Message Interval: Defines RSVP message interval.

---

**RSVP logs**

Shows RSVP Logs.
RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key. The public key for the RSA algorithm are generated by MPH key generator and appears in the “Current RSA Public Key” box.

Video stream encryption and authentication

**Secure RTP (SRTP)** MPH200 series supports video stream encryption and authentication, it adds authentication information to video elementary stream. It allows verifying the exact encoder has encoded the video stream and video is authentic. Authentication is done by a hardware chip in the device called trusted platform module (TPM). TPM is a hardware chip in devices that securely holds RSA key and generates RSA-signatures by it. You can have a certification (x509) for TPM RSA key pairs (e.g. signed by Teleste) mapped to the serial number of the MPH encoder, showing that particular device encoded the video. So any recording can be traced back to exact MPH unit.

- **Enable**: Enables/disables SRTP feature.
- **SRTP Master Key**: A single “master key” can provide keying material for encryption and integrity protection for both SRTP and SRTCP streams.

**Video Stream Authentication** Video stream authentication is based on secure RSA private key stored safely on Trusted Platform Module (TPM). SRTP uses 2048bit RSA mode encryption for authentication. RSA delivers a higher level of security strength compared to other algorithms.

- **Enable**: Enables/disables video stream authentication feature.
- **Key generation**: Generates RSA key.
- **Current RSA Public Key**: Shows generated RSA public key.
Click "User management" under the Administration menu. **User management** page appears on the screen. This page allows you modify user settings.

**Users**

- Shows device user accounts. All user accounts are protected by a user name and a password. Administrator user can create and remove user.
- **Username**: Set username for user.
- **Password**: Set password for user.
- **User Level**: Select user level for user.

**Functionality / Allowed users**

Shows permissions for different users.
Configuring ethernet switch

MPH200 has two fixed (3 &4) and two SFP (1 & 2) Ethernet ports.

MPH200 switch’s internal connection.

Switch introduction and features

MPH200 has a built-in four port tri-speed Ethernet Switch with two integrated copper transceivers and two SFP ports. Switch is a fully managed field hardened stand-alone Gigabit Ethernet switch for video networking applications. The product is designed for use in harsh environment applications.

MPH200 Ethernet Switch provides non-blocking wire-speed performance. It can operate as either a VLAN-aware switch or a VLAN-unaware switch. It can forward frames at Layer 2, based on information from layer 2 and layer 3. All memory is included on-chip, because each port has its own shared memory of 20 kilobytes for frame storage. This section gives an overview of the functionality and features of the switch.

MPH200 Ethernet Switch supports IGMP snooping, VLAN, network redundancy, SNMP management, port configuration, port alarms, QoS (layer 2 and 3) and port mirroring. Switch supports both command line interface (CLI) and WEB User Interface (WebUI).

Auto-negotiation

MPH200 Ethernet Switch supports twisted pair auto-negotiation, as defined in IEEE Std 802.3-2002 clause 28. The purpose of auto negotiation is to allow a device to advertise modes of operation. The auto negotiation function provides the means to exchange information between two devices that share a point-to-point link segment, and to automatically configure both devices to take maximum advantage of their abilities. Auto negotiation is performed totally within the physical layers during link initiation, without any additional overhead to either the MAC or higher protocol layers. Auto negotiation allows the ports to do the following:

- Advertise their abilities
- Acknowledge receipt and understanding of the common modes of operation that both devices share
- Reject the use of operational modes that are not shared by both devices
- Configure each port for the highest-level operational mode that both ports can support.

Auto MDI/MDI-X function

The device automatically detects whether the cable connected to an RJ-45 port is crossed or straight through, when auto-negotiation is enabled. Standard wiring for end stations is Media-Dependent Interface (MDI) and the standard wiring for hubs and switches is known as Media-Dependent Interface with Crossover (MDIX).

QoS – quality of service

Various classifications and prioritizations are supported in order to enable Quality of Service for real time applications. The switch supports four QoS classes. On each port, an enhanced categorizer assigns priorities based on information taken from Layer 2 and Layer 3.
The categorizer analyzes all received frames. It assigns each frame to one of four QoS classes based on:

1. Port-based priority
2. User priority in the VLAN tag header (IEEE Std 802.1p)
3. Differentiated Services Code Point (DSCP/DiffServ) from the IP-header (IPv4 and IPv6 supported)

Based on the priority assigned by the categorizer, higher priority frames take precedence over lower priority frames during forwarding through the switching engine. In case of congestion, the lowest priority traffic is dropped before higher priority frames. In addition, the higher priority frames are able to overtake the lower priority frames in the queue, thereby minimizing latency for expedited data.

**Congestion control**

The ingress and egress directions on all ports can be configured to manage network congestion independently, either by dropping frames or by flow control pause frame signalling. Flow control is guaranteed no dropping for frame sizes up to about 4 kilobytes. Asymmetric flow control is supported for both the ingress and egress direction. Software can set up individual high and low thresholds for each FIFO. These thresholds control the starting and stopping of pause signalling. The internal FIFOs have enough memory to handle flow control on short-haul, full-duplex lines without using excessive pause signalling. The switch generates flow control pause frames, when necessary, to ensure that frames are never dropped. In half-duplex mode, flow control is supported through back pressure. In drop mode, the switch handles congestion situations by dropping frames intelligently according to bandwidth allocations, frame priorities, and available buffer capacity. The MPH premium switch features both strict priority-based forwarding and weighted fairness forwarding, with guaranteed bandwidth allocation for the different QoS classes.

**MAC address learning**

When a frame is received, the source MAC address is looked up in the MAC address table. If the address is not registered, and it is not a multicast address, a new entry is created. If necessary, an entry is discarded to make room for the new one based on a “least recently used” algorithm. MPH200 Ethernet Switch is capable of looking up and adding all incoming entries to the MAC table at maximum load, which is known as “wire-speed learning”.

**IP multicast**

MPH200 Ethernet Switch provides enhanced support for IP Multicast by allowing up to 8192 programmable multicast groups to co-exist in the MAC table. This, in combination with IGMP snooping enables applications such as digital video distribution.

**IGMP snooping**

The Internet Group Management Protocol (IGMP) lets host and routers share information about multicast group memberships. IGMP snooping is a switch feature that monitors the exchange of IGMP messages and copies them to the CPU for further processing. The overall purpose of IGMP-snooping is to limit the forwarding of multicast frames to only ports that are a member of the multicast group.
Flooding storm control

MPH200 Ethernet Switch features a flooding control system for constraining undesired behavior caused by, for example, loops in the network or denial-of-service attacks.

SNMP – simple network management protocol

MPH200 Ethernet Switch supports SNMPv2c. SNMP enables network administrators and control engineers to manage network performance, find and solve network problems, and plan for network growth. One feature of SNMP is that the SNMP agent (in this case a MPH200 switch) can send SNMP traps to one or more SNMP Hosts. SNMP traps mean system alarms such as a port link loss or a port enabled for port alarms or the switch temperature exceeding a predefined threshold.

Flow control

Flow control can be enabled or disabled on a per-port basis from the command line interface or from the WEB interface. If flow control is enabled for a port the associated PHY will be set to advertise support of “Symmetric Pause”, but not “Asymmetric Pause”. If the station connected to the port also supports “Symmetric Pause”, flow control will be enabled on the switch port. Watermarks are set to hard-coded values. Different values are used depending on whether flow control is enabled or not and on current speed.

Ageing

To prevent that an automatically learned MAC address of a station that has been detached will remain in the MAC address table permanently, the ageing function in the switch is activated on a regular basis. The period for doing the ageing function is determined by the ageing time parameter. Given the ageing mechanism in the switch, the period must be half the value of the ageing time parameter in order to make the ageing time parameter comply with IEEE 802.1D. For instance, if the ageing time parameter is 300 seconds, the period must be 150 seconds to ensure that an unused MAC address will not remain in the MAC address table for more than 300 seconds. The ageing time parameter can be set from the command line interface. Default value is 300 seconds. Setting the ageing time parameter to 0 disables the ageing function.

VLAN support

VLANs are collections of switching ports that comprise a single broadcast domain. Packets are classified as belonging to a VLAN based on either the VLAN tag or based on a combination of the ingress port and packet contents. Packets sharing common attributes can be grouped in the same VLAN.

STP – spanning tree protocol

802.1d Spanning tree is a standard Layer 2 switch requirement that allows bridges to automatically prevent and resolve L2 forwarding loops. Switches exchange configuration messages using specifically formatted frames and selectively enable and disable forwarding on ports.
**RSTP – rapid spanning tree protocol**

Spanning Tree can take 30...60 seconds for each host to decide whether its ports are actively forwarding traffic. Rapid Spanning Tree (RSTP) detects uses of network topologies to enable faster convergence, without creating forwarding loops.

**Port mirroring**

Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from a monitored port to a monitoring port. Users specify which target port receives copies of all traffic passing through a specified source port.

**Link aggregation (trunking)**

MPH200 Ethernet Switch supports ingress and egress port aggregation in accordance with IEEE Std 802.3ad. Any number of ports can be aggregated into any number of groups. Frames are distributed among the aggregated ports by an advanced frame distribution function, which, through configuration, can use the following information:

- Source and destination MAC addresses
- Source and destination IP addresses
- TCP/UDP port numbers for IPv4 packets
- Flow label for IPv6 packet
- Pseudo-randomization.

**LACP – link aggregation control protocol**

LACP uses peer exchanges across links to determine, on an ongoing basis, the aggregation capability of various links, and continuously provides the maximum level of aggregation capability achievable between a given pair of systems. LACP automatically determines, configures, binds and monitors the port binding within the system.

**802.1X – port-based network access control**

The port-based network access standard IEEE Std 802.1X provides a framework to implement port authentication where only authenticated ports have access to the network. Ports are initially in an unauthorized state where normal frame forwarding for the port is disabled. The port only accepts special authentication frames. Upon authorization, the network services become enabled for the port, and normal frame forwarding is possible. The authentication is initiated by extensible authentication protocol over LAN (EAPOL) frames, which are identified by the unique bridge group address 01-80-C2-00-00-03.
Web user interface

You can manage the switch via Web User Interface (WebUI). Following options are available:

**Configuration**
- Set port speed
- Configure simple port-based VLAN
- Enable/disable flow control
- Storm Control Configuration
- Configure RSTP parameters
- Configure QoS
- Configure and monitor IGMP snooping

**Monitoring**
- Read and clear port statistics
- Monitor LACP status
- Monitor RSTP status
- Monitor IGMP status

How to access the Ethernet Switch

In order to access the Ethernet switch you need to assign an IP address to the switch from encoder WebUI. By default both encoder and ethernet switch IP addresses are assigned automatically from DHCP server. The IP address should be in the same IP range as encoder is set.

To assign the static IP address, click “Network” under the Administration menu. NETWORK SETTINGS page appears on the screen. In the “IPv4 Configuration For Switch” session you can set the IP address, netmask and gateway address.

The default setting is DHCP enabled.
Click “Ethernet Switch” under the Administration menu. The Ethernet Switch settings / System Configuration page appears on the screen.

**System Configuration**

- **Mac address:** Device mac address
- **Active IP Address:** Valid IP address
- **Active Subnet Mask:** Valid subnet mask
- **Active Gateway:** Valid gateway address
- **DHCP Server:** Netmask address for subnet definition
- **Lease Time Left:** The time how long the DHCP server will lease the IP address to the device using it
Port configuration

Enable Jumbo Frames: Allows you to enable Jumbo (giant) frames which are bigger than the standard frame size (1518 bytes of payload).

PERFECT_REACH/Power Saving Mode: PerfectReach is an intelligent algorithm, it detects the presence of a shorter cable and then adaptively lowers the power level, saving energy for links shorter than the full 100 meters of cable length specified by IEEE standards.

Drop frames after excessive collisions: Allows the switch to drop the frame if it has exceeded the maximum of 16 retransmissions in the collision mechanism.
Virtual LANs (VLANs) – introduction

VLANs are logical partitions of the physical LAN. VLANs are collections of switching ports that comprise a single broadcast domain. Packets are classified as belonging to a VLAN based on either the VLAN tag or based on a combination of the ingress port and packet contents. Packets sharing common attributes can be grouped in the same VLAN.

You can use VLANs to:

- Increase network performance
- Increase internal network security
- Create separate broadcast domains

If the network has adequate performance and security for your current needs, it is recommended that you leave the VLAN settings in the default configuration. The default configuration is as follows:

- All ports are members of VLAN 1
- The switch management interface is on VLAN 1 (this cannot be changed)
- All ports have a Port VLAN ID (PVID) of 1
- All ports can send and receive both VLAN-tagged and untagged packets (i.e. they are “hybrid” ports)

In the default configuration, any port is able to send traffic to any other port and a PC connected to any port will be able to reach the management interface. Broadcast traffic, for example, will be flooded to all ports on the switch.

VLAN page lets you to configure VLANs per port. The switch can be configured as either VLAN unaware, behaving transparently toward VLAN-tagged frames, or as VLAN aware, where VLAN information is used in the forwarding decision. The switch can maintain 16 VLANs.

For a VLAN-aware (enabled) switch, untagged frames are classified to a port specific, configurable VLAN identifier (PVID). Frames that already have a VLAN tag when they are received, they will be classified to the VID within the tag header in the frame.

VLAN-awareness (tagging or untagging frames) can be configured on a per-port basis. Each port can be configured to a set of ports to which it can forward and thereby facilitate port-based VLANs. By defaults, all ports can forward to all other ports.

Packet type

PCs should be connected to ports with Packet Type set to All. PCs cannot, in general, send or receive tagged packets. Switches should be connected to each other with Packet Type set to Tagged.

If the Packet Type is set to All, the port can accept incoming tagged and untagged packets. Untagged packets will be associated with the VLAN identified by the PVID. Tagged packets will be dropped unless the port is a member of the VLAN identified by the VLAN tag in the packet. Outgoing packets will be tagged unless the packet’s VLAN ID is the same as the PVID.

If the Packet Type is set to Tagged, the port will drop untagged packets and will only send and receive tagged packets. Tagged packets will be dropped unless the port is a member of the VLAN identified by the VLAN tag in the packet. The PVID has no effect in this case.
### Ingress VLAN classification

The switch always classifies incoming frames to a VLAN. In the VLAN-unaware mode, this classification does not influence the forwarding of the frame, whereas in the VLAN-aware mode, then classification is used to make forwarding decisions. If VLAN tags are available in a frame, the VLAN classification is always based on the outer tag in the frame.

### Egress VLAN handling

The switch egress port decides which frames to transmit tagged and which frames to transmit untagged. The following shows how the tagging or untagging is performed at the egress port:

**Do not tag frames**: This applies when switch is running as VLAN-unaware mode or when the port is VLAN-aware but configured as an access port.

**Tag all frames**: This applies when the port is configured as a trunk port.

**Tag all frames except those with a specific VID**: This applies when the port configured as hybrid port, frames with a specific VID won’t be tagged.

### VLAN IDs

VLAN ID number can be any number from 2 to 3290, or from 3293 to 4094. (VLAN ID 1 is reserved for the default VLAN, which is used for untagged frames received on the interface. VLAN IDs 3291...3292 are reserved and cannot be used.) To create a VLAN, enter the ID number and click Add VLAN.

- VLAN 1 is a special VLAN; it cannot be deleted and, if there is a possibility that a port could become isolated, the Web User Interface will add the port to VLAN 1.
- You can add up to 16 VLANs to the configuration of the switch. Each VLAN must be given a VLAN ID in the range 1...4094.
- A port can be a member of up to 16 VLANs.
- All packets travelling through the switch are associated with one and only one VLAN.
- If a port is not a member of a VLAN, it cannot send or receive packets associated with that VLAN.
- A tagged packet carries its VLAN ID in the payload of the packet.
- An untagged packet, received on a port with Packet Type set to All, is associated with the VLAN identified by the PVID.

### Port VLAN ID – PVID

PVID is the VLAN ID that is associated with untagged, ingress packets. It is not possible to remove a port from VLAN 1 unless its PVID has been changed to something other than 1.

Outgoing packets are tagged unless the packet’s VLAN ID is the same as the PVID. When the PVID is set to “None,” all outgoing packets are tagged (trunk port).
Port segmentation (VLAN) configuration

VLAN ID: Sets VLAN ID (identification of the VLAN).
VLAN Configuration List: Adds the VLAN specified in the VLAN ID field to the VLAN Configuration list.

VLAN setup

Click “Modify” button on the VLANs page. VLAN Setup page appears on the screen.

Port: Shows available ports.
Member: Adds the VLAN specified in the VLAN ID field to the VLAN Configuration list.
VLAN per port configuration

Click “Port Config” button on the VLANs page. VLAN Per Port Configuration page appears on the screen. This page allows you to configure the VLAN parameters for individual ports.

<table>
<thead>
<tr>
<th>Port</th>
<th>VLAN aware Enabled</th>
<th>Ingress Filtering Enabled</th>
<th>Packet Type</th>
<th>Pvid</th>
</tr>
</thead>
<tbody>
<tr>
<td>SFP(Top)</td>
<td></td>
<td></td>
<td>All Tagged Only</td>
<td>1</td>
</tr>
<tr>
<td>Internal</td>
<td></td>
<td></td>
<td>All Tagged Only</td>
<td>1</td>
</tr>
<tr>
<td>SFP(Down)</td>
<td></td>
<td></td>
<td>All Tagged Only</td>
<td>1</td>
</tr>
<tr>
<td>RJ45(Top)</td>
<td></td>
<td></td>
<td>All Tagged Only</td>
<td>1</td>
</tr>
<tr>
<td>RJ45(Crown)</td>
<td></td>
<td></td>
<td>All Tagged Only</td>
<td>1</td>
</tr>
</tbody>
</table>

VLAN aware Enabled: VLAN aware ports are able to use VLAN tagged frames to determine the destination of the frame. Click to enable or disable VLAN awareness mode for this port. (Default: Disabled).

Ingress Filtering Enabled: If enabled, incoming frames for VLANs which do not include this ingress port as a member will be discarded. (Default: Disabled).

Packet Type: Set a port’s handling of tagged and untagged packets. (Default: All).

Pvid: Set the Port VLAN ID. (Default: 1).
Aggregation – introduction

Link aggregation (trunking) allows any number of ports to be grouped together automatically using Link Aggregation Control Protocol (LACP), or manually, to form an ultra-high-bandwidth connection to the network backbone, which helps prevent traffic bottlenecks. MPH200 Ethernet Switch supports LACP.

Link aggregation (IEEE Std 802.3ad) describes a way of aggregating multiple links together to form what appears to be a single link. The goals are to increase bandwidth and to reduce the risk of link failures. Link aggregation groups can be defined statically.

The system provides up to four link aggregated groups. Aggregated links may be defined, each with up to four member ports, to form a single link aggregated group. Link aggregated groups provide:
- Fault tolerance protection from physical link disruption
- Higher bandwidth connections
- Improved bandwidth granularity
- High bandwidth server connectivity
- Link aggregated group is composed of ports with the same speed, set to full-duplex operation.

The software will automatically detect that a link has gone down and then reassign packet distribution on the other links in the group.

MPH200 Ethernet Switch supports ingress and egress port aggregation in accordance with IEEE Std 802.3ad. Any number of ports can be aggregated into any number of groups. Frames are distributed among the aggregated ports by an advanced frame distribution function, which, through configuration, can use the following information:
- Source and destination MAC addresses
- Source and destination IP addresses
- TCP/UDP port numbers for IPv4 packets
- Flow label for IPv6 packet
- Pseudo-randomization

**Note**! If port mirroring is enabled and mirrors frames to a port in an aggregation group, all mirrored frames go to the mirror port without reflecting the other ports in the aggregation group.

Aggregation configuration

Click “Aggregation” menu under the configuration heading. **Aggregation/Trunking Configuration** page appears on the screen.

**Group \ Port:** Ethernet port number.
**Normal / Group1-4:** Click the tick-box of the port you would like to add to the link aggregation groups (LAGs).
LACP – introduction

Link Aggregation Control Protocol (LACP) is part of the IEEE specification 802.3ad. LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on the switch as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the switch and the other device will negotiate a trunk link between them.

A Gigabit Ethernet port channel balances the traffic load across the links by reducing part of the binary pattern formed from the addresses in the frame to a numerical value that selects one of the links in the channel. Bundled ports equally inherit the logical MAC addresses on the port channel interface.

LACP supports the automatic creation of Gigabit Ethernet port channels by exchanging LACP packets between ports. It learns the capabilities of port groups dynamically and informs the other ports. Once LACP identifies correctly matched Ethernet links, it facilitates grouping the links into a Gigabit Ethernet port channel.

LACP configuration

Click “LACP” menu under the configuration heading. LACP Port Configuration page appears on the screen.

Protocol Enabled: Allows LACP to be enabled or disabled. When the box is checked, Key Value (0..255, 0 means auto-generated key). Used to determine the link aggregation group membership, and to identify this device to other switches during negotiations.
Spanning tree (STP/RSTP) – introduction

The Spanning Tree Algorithm (STA) can be used to detect and avoid network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

The spanning tree algorithms supported by this switch include these versions:
- **STP** – Spanning Tree Protocol (IEEE 802.1D).
  STP is a standard Layer 2 switch requirement that allows bridges to automatically prevent and resolve L2 forwarding loops. Switches exchange configuration messages using specifically formatted frames and selectively enable and disable forwarding on ports.
- **RSTP** – Rapid Spanning Tree Protocol (IEEE 802.1w).
  RTP can take 30-60 seconds for each host to decide whether its ports are actively forwarding traffic. Rapid Spanning Tree (RSTP) detects network topologies to achieve faster convergence, without creating forwarding loops.

Click “RSTP” under the Configuration menu. **RSTP System Configuration** page appears on the screen. The page is composed of two tables:
- **RSTP System Configuration** - Configure global system settings.
- **RSTP Port Configuration** - Setup port related settings.

### System Priority:
This parameter configures the spanning tree priority globally for this switch. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Number between 0..61440 in increments of 4096. Therefore, there are 16 distinct values.

### Hello Time:
Interval (in seconds) at which the root device transmits a configuration message (BPDU frame). Number between 1...10 (default is 2).

### Max Age:
The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. That also means the maximum life time for a BPDU frame. Number between 6...40 (default is 20).

### Forward Delay:
The maximum time (in seconds) the root device will wait before changing states (i.e., discarding to learning to forwarding). Number between 4...30 (default is 15).

### Force version:
Set and show the RSTP protocol to use.
Normal = use RSTP,
Compatible = compatible with STP.
Protocol Enabled: Click on the tick-box to enable/disable the RSTP protocol for the port.

Edge: Expect the port to be an edge port (linking to an end station) or a link to another STP device.

Path Cost: This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. Set the RSTP pathcost on the port. Number between 0...200000000.

802.1X – introduction

The 802.1X (IEEE 802.1X) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication.

802.1X configuration

Click “802.1X” under the Configuration menu. 802.1X Configuration page appears on the screen.

Mode: Indicates if 802.1X protocol is globally enabled or disabled on the switch.

RADIUS IP: Sets the RADIUS server IP address.

RADIUS UDP Port: Sets the UDP port to the use for the external RADIUS server.

RADIUS Secret: Sets the text string used for encryption between the switch and the RADIUS server.
Port: The port number.

Admin State: Sets the authentication mode to one of the following options:
- **Auto**: Requires a 802.1X-aware client to be authorized by the authentication server. Clients that are not 802.1X-aware will be denied access.
- **Force-Authorized**: Forces the port to grant access to all clients, either 802.1X-aware or otherwise.
- **Force-Unauthorized**: Forces the port to deny access to all clients, either 802.1X-aware or otherwise.

Port State: The state of the port.
- **Re-Authenticate**: Schedules a reauthentication to whenever the quiet-period of the port runs out.
- **Force-Reinitialize**: Bypasses the quiet-period of the port and enables immediate reauthentication regardless of the status for the quiet-period.

Statistics: Displays 802.1X statistics. Statistics can be viewed on a per-port basis.
- **Authenticator counters**: General statistics for authenticator.
- **Backend Authenticator counters**: General statistics for RADIUS server.
- **802.1X MIB counters**: MIB module defined for 802.1X.

Select the port that you want to view:
IGMP – Introduction

The Internet Group Management Protocol (IGMP) lets host and routers share information about multicast group memberships. IGMP snooping monitors IGMP service requests passing between multicast clients and servers, and dynamically configures the ports which need to receive the multicast traffic.

MPH200 Ethernet Switch provides enhanced support for IP Multicast by allowing up to 8192 programmable multicast groups to co-exist in the MAC table. This, in combination with IGMP snooping where IPMC membership information is passed on to the CPU, enables applications such as digital video distribution. Source specific multicast (SSM) is not supported.

IGMP configuration

Click “IGMP Snooping” under the Configuration menu. IGMP Configuration page appears on the screen. This page enables customers to setup the configuration of IGMP. The page is composed of two tables:

- **IGMP Snooping Configuration** – Configure global system settings
- **IGMP Snooping VLAN Configuration** – Configure VLAN related settings

<table>
<thead>
<tr>
<th>Configuration</th>
<th>System</th>
<th>Ports</th>
<th>VLANs</th>
<th>Aggregation</th>
<th>LACP</th>
<th>RSTP</th>
<th>802.1X</th>
<th>IGMP Snooping</th>
<th>Mirroring</th>
<th>Quality of Service</th>
<th>Storm Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring</td>
<td>Statistics Overview</td>
<td>Detailed Statistics</td>
<td>LACP Status</td>
<td>RSTP Status</td>
<td>IGMP Status</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**IGMP Enabled:** Enables/disables IGMP support on the switch. When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic.

**Router Ports:** Enable Router Port if it is leading towards the IGMP querier (switch or router having IGMP querying function enabled).

**Unregistered IPMC Flooding enabled:** Enabling this will make the switch flood the unregistered (not joined) multicast to all ports and disabling will make the switch forward unregistered multicast traffic to the router ports only.

**VLAN ID:** The VLAN ID. It can not be changed.

**IGMP Snooping Enabled:** Enables/disables IGMP snooping on a VLAN. When enabled, the port will monitor network traffic to determine which hosts want to receive the multicast traffic.

**IGMP Querying Enabled:** Enables/disables IGMP querier on the VLAN. When enabled, the port can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic.
Quality of service (QoS) – introduction

QoS configuration enables the switch to use resources more efficiently to ensure high-quality performance for critical applications. QoS is a mechanism which is used to prioritize certain traffic as it is moves through the switch. Traffic can be classified as High, Medium, Normal or Low priority. This switch features both strict priority-based and weighted round-robin (WRR) forwarding, with guaranteed bandwidth allocation for the different QOS classes.

QoS configuration

Click “Quality of Service” under the Configuration menu. QoS Configuration page appears on the screen.

Queue Mode: The Queue Mode can be selected by ticking the radio button:
- **Strict**: Higher priority frames take precedence over lower priority frames during forwarding. In case of congestion, the lowest priority traffic is dropped before higher priority frames. Head-of-queue blocking maybe encountered by using this mode.
- **WRR**: In this mode, all priorities can be guaranteed a share of the bandwidth when the system is overloaded. The bandwidth sharing percentage can be adjusted by specifying the four QOS class with different ratio in WRR Weight, which appears after WRR is enabled in Queue Mode.

**Note**: WRR is selectable only when Jumbo Frame is disabled in Ports / Settings.

QoS Mode: The QoS Mode can be selected using the QoS Mode drop-down list:
- **QoS Disabled**: QoS is turned off and all packets have equal priority.
- **802.1p**: Packets are prioritized using the content of the VLAN-tag.
- **DSCP/DiffServ**: Packets are prioritized using the DSCP/DiffServ (Differentiated Services Code Point) value.

**Note**: Only one QoS mode can be active at one time. It is not possible, for example, to prioritise traffic using the DSCP/DiffServ and 802.1p.
802.1p configuration

The 802.1p field is held within the VLAN-tag of a packet. The field is three bits long so can hold eight values; 0...7 inclusive. When QoS Mode is set to 802.1p, the 802.1p Configuration table appears which allows a priority to be set for each of the eight values.

You can use the Priority drop-down list to quickly set the values in the 802.1p Configuration table. Select Low to set all values to low priority, Normal to set all values to normal priority, Medium to set all values to medium priority, or select High to set all values to high priority. Use Custom if you want to set each value individually.

Note: Because end-stations, like PCs, are not usually VLAN aware, they do not create VLAN-tagged frames. As a result, this method of prioritization is not ideal when there are a lot of PCs connected to the switch.

DSCP configuration

DSCP (DiffServ/Differentiated Services Code Point) is a six bit field that is contained within an IP (TCP or UDP) header. Six bits allows the DSCP field to take any value in the range 0...63 inclusive. When QoS Mode is set to DSCP, the DSCP Configuration table appears which allows a priority to be set for each of the DSCP values.

You can use the Priority drop-down list to quickly set the values in the DSCP Configuration table. Select Low to set all values to low priority, Normal to set all values to normal priority, Medium to set all values to medium priority, or select High to set all values to high priority. Use Custom if you want to set each value individually.
Storm control – introduction

This page allows you to set up a threshold for incoming broadcast and multicast packets. Too many incoming packets can severely cripple the switch and network performance. Rate limiting protects the switch and network by keeping the amount of data passing through the ports to a safe limit. The use of VLANs and Trunks to partition ports and network devices into separate groups can also keep the network from unnecessary traffic by restricting the packet destination. The same setting is applied to all the ports on the switch.

Storm control configuration

Click “Storm Control” under the Configuration menu. Storm Control Configuration page appears on the screen.

List the type of traffic which can be rate limited, including Broadcast, Multicast and Flooded unicast frames.

The Rate field is set by a single drop-down list. The same threshold is applied to every port on the switch. When the threshold is exceeded, packets are dropped, irrespective of the flow-control settings.
Command line interface - CLI

General

The MPH series video encoder unit includes a command line interface (CLI) for configuration purposes. The CLI is a screen interface that allows the user to interact with the operating system by entering commands and optional arguments.

The MPH supports CLI over UART (RS-232), Telnet and SSH.

CLI is accessed through any terminal emulator application. The command structure is the same for all session types.

Note! PuTTY is a free and open source terminal emulator application which can act as a client for the SSH, Telnet, rlogin, and raw TCP computing protocols and as a serial console client. Tera Term has comparable features to PuTTY. Hyper Terminal is not included in Windows Vista or later.

The CLI can be accessed in the following ways:

- Serial data connection (RS232), via Data 2 port, with a serial connection cable.
- TCP/IP connection, via active Ethernet port.

System requirements for CLI

Connection through Data 1 port locally (UART):

* PC equipped with terminal emulator application supporting VT100 / 102 or ANSI protocols, e.g. Hyper Terminal, PuTTY or Tera Term.
* RS232-cable (type Teleste CIC506)

Connection through Ethernet port remotely (Telnet/SSH):

* PC equipped with terminal emulator application supporting Secure Shell (SSH) network protocol, e.g. PuTTY or Tera Term.
* Ethernet-connection
This chapter describes how to connect to CLI locally (via serial cable) using Putty terminal emulator application.

1. Start the Putty terminal emulator application. Wait until the following “Putty Configuration” window appears on the screen.
2. Select Serial category to continue. The following “Options controlling local serial lines” window appears on the screen.
3. Choose COM port where the serial (RS232) cable is connected, e.g. COM4 port and then set here the values as described in table beside. Click Open to continue. The blank “COM4 - PuTTY” window appears on the screen.
4. To activate the terminal connection first press Enter --> “MPH241-f login:” appears on the screen (MPH name depends on device in question).
5. Enter the required user name and the password (admin/admin for administrator). The MPH Hyper Terminal window appears on the screen. The terminal connection to MPH series video encoder device is now completed and you can now use the CLI commands to management the device.

The terminal connection can be terminated by selecting File/Exit, Alt+F4 or clicking x on the right upper corner of Hyper Terminal window.
Connection methods - TCP/IP

This chapter describes how to connect to CLI via TCP/IP connection using Putty terminal emulator application. The same menus that are displayed on a local terminal are instantly available over an IP network.

1. Start the PuTTY application. Wait until the following “PuTTY Configuration” window appears on the screen:

PuTTY application view (Windows XP).

2. Enter the device IP address into the “Host Name (or IP address)” address bar and click to continue.

The following “PuTTY” window appears on the screen:

Telnet program view.

3. Enter the required user name and the password. The following “172.16.200.5 - PuTTY” window appears on the screen:

The CLI connection to MPH series video encoder is now completed and you can now use the CLI commands to management the device. The CLI connection can be terminated by entering command exit.
Detailed descriptions of CLI commands

CLI lets you enter several commands. To execute a command, press enter after typing command. By entering “Help” command you get a list of all available commands. To get more information about how to use a specific command you can enter “Help + specific command”. Ctrl+C is the interrupt key and returns user to the prompt.

Note! letters can be typed either lowercase or uppercase.

Main menu

Enter the help command to view a CLI main menu:

```
**************************************
| Main menu                          |
| **************************************
| datetime                | sub menu        |
| devmgmt                 | sub menu        |
| ethswitch               | sub menu        |
| network                 | sub menu        |
| up                      |                 |
| help                    |                 |
| exit                    |                 |
```

Datetime command

Enter the datetime command to view datetime menu:

```
**************************************
| datetime menu               |
| **************************************
| setutc                      |
| up                          |
| help                        |
| exit                        |
```

Use the setutc command to change device date and time settings.

```
setutc <-src=time_src> [<-date=date_str>] [<-time=time_str>]
```

Description:
Sets UTC date and time parameters. If no arguments are passed, the command will display current date and time

<time_src>: manual/ntp
If manual mode is selected, then date and time should be provided

<[date_str]>: Date in DD/MM/YYYY format

<[time_str]>: Time in HH:MM:SS 24 hour format
**Devmgmt command**

Enter the **devmgmt** command to view devmgmt menu:

```
.devmgmt menu
  reboot
  softfactoryreset
  hardfactoryreset
  licenseupdate
  swversion
  swud
  getconf
  putconf
  up
  help
  exit
```

Available CLI commands in **devmgmt** menu. These commands allows you to manage device, as make factory resets, update firmware and save/restore device settings.

Entering **help reboot** displays information about the reboot command:

```
reboot
Description:
Reboot the device.
```

Entering **help softfactoryreset** displays information about the softfactoryreset command:

```
softfactoryreset
Description:
Soft factory resets the device. Specific configurations will be reset to factory defaults. The device will reboot on this command.
```

Entering **help hardfactoryreset** displays information about the hardfactoryreset command:

```
hardfactoryreset
Description:
Hard factory resets the device. All configurations will be reset to factory defaults. The device will reboot on this command.
```
Enter the `licenseupdate` command to activate a new licence to the device.

`licenseupdate <license_key>`

**Description:**
Update product license key. The license key will be validated against device serial number before updating. The device will reboot after successfully updating the license key. If the license key is not provided, this command will print the current license key.

`<license_key>`: Product license key string. If this string is not provided, current license key will be displayed.

**Example:**
`licenseupdate MPH-1A-B1CGAX-XXAXXXOX-XXXXXXXX,HL00000000,0,EJPK0J-XLJAYA-172CA2`

Enter the `swversion` command to view the current firmware version of the device.

`swversion`

**Description:**
Prints the current software version.

Enter the `swud` command to change device’s firmware.

`swud <tftp link>`

**Description:**
Downloads software image from tftp and update. Device will reboot once the software image is downloaded successfully.

`<tftp link>`: String of up to 128 characters with `tftp://<ip_address>/software_image` format.

**Example:**
`swud tftp://192.168.36.148/tvelightimage.bin`

Enter the `getconf` command to download stored configuration from a TFTP server.

`getconf <ip=server_ip> <file=config_file_name>`

**Description:**
Download configuration file from TFTP server and restore configurations. Device will reboot once the file is downloaded successfully.

**Example:**
`getconf -ip=192.168.36.148 -file=tve.cfg`

Enter the `putconf` command to upload the current configuration to a TFTP server.

`putconf <ip=server_ip> <file=config_file_name>`

**Description:**
Upload configuration file to TFTP server for backup. The file name can be chosen by the user.

**Example:**
`putconf -ip=192.168.36.148 -file=tve.cfg`

Use the `licenseupdate` command to activate a new licence to the device.

Use the `swversion` command to view the current firmware version of the device.

Use the `swud` command to change device’s firmware.

Use the `getconf` command to download stored configuration from a TFTP server.

Use the `putconf` command to upload the current configuration to a TFTP server.
Ethswitch command

CLI lets you manage device’s internal Ethernet switch. Enter the **ethswitch** command to view ethswitch menu:

```
ethswitch menu

help

Commands at top level:

- System  - System commands
- Console  - Console commands
- Port     - Port commands
- MAC      - MAC commands
- VLAN     - VLAN commands
- Aggr     - Aggregation commands
- LACP     - IEEE 802.3ad Link Aggregation commands
- RSTP     - IEEE 802.1w Rapid Spanning Tree commands
- User Group  - User Group commands
- QoS      - QoS commands
- Mirror   - Mirror commands
- IP       - IP commands
- Dot1x    - Dot1x commands
- IGMP     - IGMP Snooping commands
- Debug    - Debug commands

>ENDOFCMD
```

These commands allows you to manage Ethernet Switch settings. To get more information about how to use a specific CLI command on the menu, enter help + command, for example: **port help** displays all commands at port level.

Use the **help** command to see information on a command (usage: enter “help + the specified command”, for example: **help help** displays information from help command.)
**System command**
Enter the *system* command to go to **System** level:

- Commands at System level:
  - System Configuration [all]
  - System Restore Default [keepIP]
  - System Name [<name>]
  - System Reboot
  - System SNMP [enable|disable]
  - System Trap [<IP Address>]
  - System Readcommunity [<community string>]
  - System Writecommunity [<community string>]
  - System Trapcommunity [<community string>]
  - System Power Saving [full|up|down|disable]

**Console command**
Enter the *console* command to go to **Console** level:

- Commands at Console level:
  - Console Configuration
  - Console Password [<password>]
  - Console Timeout [<timeout>]
  - Console Prompt [<prompt string>]

**Port command**
Enter the *port* command to go to **Port** level:

- Commands at Port level:
  - Port Configuration [<portlist>]
  - Port Mode [<portlist>] [mode]
  - Port Flow Control [<portlist>] [enable|disable]
  - Port State [<portlist>] [enable|disable]
  - Port MaxFrame [<portlist>] [framesize|reset]
  - Port Statistics [<portlist>] [clear]
  - Port Excessive Collisions Drop [enable|disable]
  - Port VeriPHY [<portlist>] [full|anomaly|termination]
MAC command
Enter the mac command to go to MAC level:

```
Commands at MAC level:
MAC Configuration
MAC Add <macaddress> <portlist>|none [<vid>]
MAC Delete <macaddress> [<vid>]
MAC Lookup <macaddress> [<vid>]
MAC Table <vidlist>
MAC Flush
MAC Agetime [<agetime>]
```

VLAN command
Enter the vlan command to go to VLAN level:

```
Commands at VLAN level:
VLAN Configuration [<portlist>]
VLAN Add <vidlist> [<portlist>]
VLAN Delete <vidlist>
VLAN Lookup <vidlist>
VLAN Aware [<portlist>] [enable|disable]
VLAN PVID [<portlist>] [<vid>|none]
VLAN Frame Type [<portlist>] [all|tagged]
VLAN Ingress Filtering [<portlist>] [enable|disable]
```

Aggr command
Enter the aggr command to go to Aggr level:

```
Commands at Aggr level:
Aggr Configuration
Aggr Add <portlist>
Aggr Delete <portlist>
Aggr Lookup <portlist>
Aggr Mode [smac|dmac|xor]
```
LACP command
Enter the `lacp` command to go to system level:

Commands at LACP level:
- LACP Configuration [<portlist>]
- LACP Mode [<portlist>] [enable|disable]
- LACP Key [<portlist>] [<key>|auto]
- LACP Status
- LACP Statistics

RSTP command
Enter the `rstp` command to go to console level:

Commands at RSTP level:
- RSTP Configuration [<portlist>]
- RSTP sysprio [<sysprio>]
- RSTP hellotime [<secs>]
- RSTP maxage [<hops>]
- RSTP fwddelay [<secs>]
- RSTP version [normal|compat]
- RSTP Mode [<portlist>] [enable|disable]
- RSTP Aggr [enable|disable]
- RSTP Edge [<portlist>] [enable|disable]
- RSTP Pathcost [<portlist>] [<pathcost>|auto]
- RSTP mcheck <portlist>
- RSTP Status
- RSTP Statistics

User Group command
Enter the `user group` command to go to system level:

Commands at User Group level:
- User Group Configuration
- User Group Add <grouplist> [<portlist>]
- User Group Delete <grouplist>
- User Group Lookup <grouplist>
QoS command
Enter the qos command to go to console level:

Commands at QoS level:
QoS Configuration [<portlist>]
QoS Mode [<portlist>] [tag|port|difserv]
QoS Default [<portlist>] [<class>]
QoS Tagprio [<portlist>] [tagprio<list>] [<class>]
QoS DiffServ [<dscpno>] [<class>]
QoS Userprio [<portlist>] [tagprio]
QoS Storm Control [traffic type] [enable|disable] [rate]

<class> range: low|normal|medium|high
<traffic type>: Broadcast|Multicast|Flood Unicast

Mirror command
Enter the mirror command to go to system level:

Commands at Mirror level:
Mirror Configuration
Mirror Port [<port>]
Mirror Source [<portlist>] [enable|disable]

IP command
Enter the ip command to go to console level:

Commands at IP level:
IP Configuration
IP Status
IP Setup [ipaddress] [ipmask] [ipgateway] [vid]
IP Mode [enable|disable]
IP Ping [-n <count>] [-w <timeout>] <ipaddress>
IP Arp
IP Dhcp [enable|disable]
IP tftp [enable|disable]
IP tftpget server-ip filename
IP tftpput config|image|backup server-ip filename
**Dot1x command**

Enter the **dot1x** command to go to system level:

- **Commands at Dot1x level:**
  - Dot1x Configuration
  - Dot1x Mode [enable|disable]
  - Dot1x State [portlist] [Auto|ForceAuthorized|ForceUnauthorized]
  - Dot1x Server [<IP Address>]
  - Dot1x UDP Port [<value>]
  - Dot1x Secret [Shared Secret]
  - Dot1x Statistics [portlist]
  - Dot1x Reauthenticate [portlist] [now]
  - Dot1x Parameters [parameter] [value]

**IGMP command**

Enter the **igmp** command to go to console level:

- **Commands at IGMP level:**
  - IGMP Configuration
  - IGMP Status
  - IGMP Groups vidlist
  - IGMP Mode [enable|disable]
  - IGMP State vidlist [enable|disable]
  - IGMP Querier vidlist [enable|disable]
  - IGMP Router ports portlist [enable|disable]
  - IGMP Unregistered Flood [enable|disable]

**Debug command**

Enter the **debug** command to go to system level:

- **Commands at Debug level:**
  - Debug Read Register block subblock address
  - Debug Write Register block subblock address value
  - Debug PHY Read portlist [address] [page]
  - Debug PHY Write portlist address value [page]
  - Debug Loopback [int|ext]
Network command

Enter the **network** command to view network menu:

```
**************************************
| network menu                      |
| **************************************
<p>| linkstatus                        |
| linklevel                         |
| ip                                |
| hostname                          |
| dns                               |
| ntp                               |
| up                                |
| help                              |</p>
<table>
<thead>
<tr>
<th>exit</th>
</tr>
</thead>
</table>
```

Use CLI commands in **network** menu to configure device IP settings.

Entering **help linkstatus** displays information about the linkstatus command:

```
linkstatus
Description:
Displays network interface and link status
```

Entering **help linklevel** displays information about the linklevel command:

```
linklevel [<mode=mode_str>] [<mtusize=mtu_size>]
Description:
Sets the link mode and/or mtu size.
mode_str: Can be one of the following:
  auto    : Auto negotiation
  100FD   : 100 mbps full duplex
  100HD   : 100 mbps half duplex
mtu_size: MTU size in bytes (Valid range: 64 to 1500)
If no arguments are passed, the command will display current configuration
```

Entering **help ip** displays information about the ip command:

```
ip <-mode=ip_mode> [<<addr=ip_addr>]> [<<mask=subnet>>] [<<gate=gateway>>]
Description:
Sets the IP mode. Also sets IP address, subnet and gateway in case of static IP mode only
If no arguments are passed, the command will display the current configuration.

<ip_mode>: static / dhcp
If manual mode is selected, then ip address, subnet mask and gate way also should be provided

[<ip_addr>]: IP address
[<subnet>]: Subnet mask
[<gateway>]: Default gateway
```

An example how to change device IP address, subnet and gateway:
```
network
ip -mode=static -addr=172.31.252.13 -mask=255.255.0.0 -gate=172.31.2.1
```

Caution: If ip address is changed, you might have to login using new IP address. Change in IP address might make the device in-accessible from your network if configured to a different subnet.
Use the **hostname** command to set a hostname to the device.

**hostname [hostname_string]**

Description:
Sets the hostname. If no arguments are passed, the command will display current configuration

[<hostname_string>]: Hostname upto 32 characters (without special characters or spaces)

Use the **dns** command to set DNS parameters to the device.

**dns <mode=dns_mode>[/<domain=search_domains>][/<servers=dns_servers>]**

Description:
Sets DNS parameters. If no arguments are passed, the command will display current configuration

[dns_mode]: manual/dhcp
If manual mode is selected, search domains and dns servers should be provided
Dhcp mode is available only if 'ip mode' is set to DHCP.
Otherwise only manual mode is available.

[<search_domains>]: Comma seperated list of search domains in decreasing order of priority (Upto 3 search domains are supported)

[<dns_servers>]: Comma seperated list of dns servers in decreasing order of priority (Upto 3 search dns servers are supported)

Use the **swud** command to change device's firmware.

Entering **help hostname** displays information about the hostname command:

Entering **help dns** displays information about the dns command:

Entering **help ntp** displays information about the ntp command:

Entering **help hostname** displays information about the hostname command:

**ntp <mode=ntp_mode> [/<servers=ntp_servers>]**

Description:
Sets NTP parameters. If no arguments are passed, the command will display current configuration

[ntp_mode]: manual/dhcp
If manual mode is selected, ntp server list should be provided
Dhcp mode is available only if 'ip mode' is set to DHCP.
Otherwise only manual mode is available.

[<ntp_servers>]: Comma seperated list of ntp servers in decreasing order of priority (Upto 3 search ntp servers are supported)
### MPH200 specifications

<table>
<thead>
<tr>
<th>Video</th>
<th>MPH241</th>
<th>MPH242</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVBS video input</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>HD-SDI video input</td>
<td>1*</td>
<td>-</td>
</tr>
<tr>
<td>Encoding channels</td>
<td>up to 4 or 1 HD*</td>
<td>up to 4</td>
</tr>
<tr>
<td>Total streams</td>
<td>up to 8 or 1 HD*</td>
<td>up to 6</td>
</tr>
<tr>
<td>Coding</td>
<td>H.264/MJPEG/MPEG-4/MPEG-2*</td>
<td>QCIF/CIF/2CIF/4CIF, ¾D1/D1/720p*/1080i*</td>
</tr>
<tr>
<td>Resolution</td>
<td>QCIF/CIF/2CIF/4CIF, ¾D1/D1</td>
<td>QCIF/CIF/2CIF/4CIF, ¾D1/D1</td>
</tr>
<tr>
<td>Frame rate (fps)</td>
<td>1...25 PAL, 1...30 NTSC</td>
<td></td>
</tr>
<tr>
<td>Max. Performance (25/30 fps)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H.264, MJPEG, MPEG-4*, MPEG-2*</td>
<td>4 x 4CIF/D1 or 1 x 720p/1080p* or 1 x 720p + 1 x 4CIF/D1*</td>
<td>2 x 4CIF/D1 (per video input)</td>
</tr>
</tbody>
</table>

### ONVIF
- Yes

### SNMP*
- Yes

### Motion detection
- Yes

### Camera tampering
- Yes

### Text overlay
- Yes

### SAP
- Yes (Session Announcement Protocol)

### NTP
- Yes (Network Time Protocol)

### RTSP
- Yes (Real Time Streaming Protocol)

### Data channels
- 2

### Standard
- Data 1: RS422/485, Data 2: RS232

### Audio channels
- 2

### Coding
- G.711. G.726, AAC-LC, AAC-HE*

### Contact closures
- 2 in, 1 out

### Ethernet ports
- 4

### VLAN
- 16 ids

### Multicast
- IGMP v1, v2

### Link redundancy
- STP/RSTP

### Protocols
- RTP, UDP, TCP, IP, HTTP, DHCP, SSH, Telnet, DHCP, DNS, ZeroConf, ICMP, ARP, QoS

### SFP support*
- Yes

### Management
- WebUI / SNMP / CLI (password protected user groups with different user levels, CLI via serial or SSH connection)

### Size (H x W x D)
- 25.2 x 130 x 254

### Operating temperature
- -34...+74 °C (-29...+165 °F)

### Power consumption
- 13 W

### Power Over Ethernet
- PoE+, 802.11at, 15W (class 4)

* = option
Legal declarations

Copyright © 2014 Teleste Corporation. All rights reserved.

TELESTE is a registered trademark of Teleste Corporation. Other product and service marks are property of their respective owners.

This document is protected by copyright laws. Unauthorized distribution or reproduction of this document is strictly prohibited.

Teleste reserves the right to make changes to any of the products described in this document without notice and all specifications are subject to change without notice. Current product specifications are stated in the latest versions of detailed product specifications.

To the maximum extent permitted by applicable law, under no circumstances shall Teleste be responsible for any loss of data or income or any special, incidental, consequential or indirect damages howsoever caused.

The contents of this document are provided “as is”. Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose, are made in relation to the accuracy, reliability or contents of this document.

Teleste reserves the right to revise this document or withdraw it at any time without notice.

Teleste Corporation
P.O. Box 323
FI-20101 Turku
Street address: Telestenkatu 1, 20660 Littoinen
FINLAND
www.teleste.com