Changelog

Version 4.2.98 – March 2018

- Added ARL status
- MediaGateway Remote control revised
- Added SFP port information and new SFP Modules compatibility
- CANGateway Chapter updated
- Removed bootloader update chapter

You can download the latest firmware and documentation for the MediaGateway here:

http://www.technica-engineering.de/en/products/media-gateway/

⚠️ IMPORTANT: Basic software is provided. Additional functionalities can be activated through this email: order@technica-engineering.de
## Contents

**CHangelog** .................................................................................................................. 2

**Contents** ......................................................................................................................... 3

1. **Feature List** .................................................................................................................. 5

2. **Warranty and Safety Information** .................................................................................. 6

3. **Pinning** .......................................................................................................................... 7

   - Power connector (top left) .............................................................................................. 8
   - Switch connectors ........................................................................................................... 9
   - RJ45 Ethernet connectors .............................................................................................. 9
   - SFP slot ........................................................................................................................... 9

4. **Status LEDs and Pushbutton** ....................................................................................... 10

   - LEDs ............................................................................................................................. 10
   - Push button ................................................................................................................... 10

5. **Configuration Website** .............................................................................................. 11

   - Website Home ............................................................................................................... 12
   - System Information Tab ............................................................................................... 12
   - Control Panel Tab ......................................................................................................... 13
   - Media Gateway Feature License Activation .................................................................. 14
   - Switch Status Tab ........................................................................................................ 15
     - Global Configuration ................................................................................................ 15
     - ARL Table status ....................................................................................................... 16
     - Dynamic ARL table .................................................................................................... 17
     - Static ARL table ......................................................................................................... 17
     - Ports ............................................................................................................................ 24

6. **Ethernet CAN Gateway (extra license needed)** .............................................................. 30

   - Basic Settings ............................................................................................................... 30
   - Advanced Settings ....................................................................................................... 30
   - Ethernet CAN Gateway Configuration (UDP mode): ...................................................... 31
   - Ethernet CAN Gateway Configuration (RAW mode): .................................................... 32
   - Ethernet CAN Gateway Sync frames .............................................................................. Error! Bookmark not defined.
   - Structure of a CAN/Ethernet packet .............................................................................. 34
   - Structure of a timestamp packet ..................................................................................... Error! Bookmark not defined.
   - Structure of a UDP packet / RAW frame ........................................................................ 35

7. **802.1AS** ...................................................................................................................... 36

   - Protocol .......................................................................................................................... 36
     - Transport of time-synchronization information ......................................................... 36
     - Propagation delay measurement .................................................................................. 37
   - Using 802.1 AS ............................................................................................................. 38
   - Limitations .................................................................................................................... 39

8. **VLAN Configuration** .................................................................................................... 40

   - VLAN Basics ................................................................................................................ 40
   - Port-Based VLAN .......................................................................................................... 40
   - Single Tagging - IEEE 802.1q (VLAN mode) ................................................................ 41
     - Single Tagging Example .............................................................................................. 42
   - Double Tagging - IEEE 802.1q (VLAN mode) ............................................................... 45
     - Double Tagging Example ......................................................................................... 48

9. **MAC Filtering for Mirroring** ....................................................................................... 50
10. MEDIAGATEWAY REMOTE CONTROL ................................................................. 52
  Reset Device .................................................................................................. 53
  Import Configuration ..................................................................................... 53
  Export Config ................................................................................................. 54
  Dynamic Config ............................................................................................. 54
  Check Status .................................................................................................. 55
  Set WakeUp Line Status ................................................................................ 55
  Get WakeUp Line Status .............................................................................. 55
  Port Enable (OABR) ..................................................................................... 56
  Port Master/Slave (OABR) ........................................................................... 56
  Reset to Default ............................................................................................ 56
  Get System Information ................................................................................ 57

11. HARDWARE VARIANTS .................................................................................. 58
  BroadR-Reach Analog Filter: ........................................................................ 58
  Debug Connector ............................................................................................ 58
  Startup Time .................................................................................................. 59

12. APPLICATION FIRMWARE UPDATE ............................................................ 60

13. FREQUENTLY ASKED QUESTIONS – FAQ .................................................. 62

14. CONTACT ..................................................................................................... ERROR! BOOKMARK NOT DEFINED.
1. Feature List

The Technica Engineering MediaGateway has the following basic features:

**12 Ports** Broadcom BroadR-Reach
100 MBit/s Fullduplex on a single unshielded twisted pair

**3 Ports** Gigabit Ethernet 10/100/1000 BaseTX Fullduplex

**1 Port** Gigabit Ethernet SFP module socket

✓ Broadcom BroadR-Reach Technology
✓ Tyco MQS Connectors for BroadR-Reach and Power Supply
✓ Webserver for easy configuration:
  - Master / Slave
  - Port Mirroring
  - VLAN Tagging
  - Port Status Display
✓ Import and Export of Configurations
✓ WakeUp functionality
✓ CAN, LIN and FlexRay interfaces (requires customer specific software)
✓ Power output for attached devices: \( V_{\text{BAT}} \) max. 1,2 Ampere in total (Fused)
✓ 19 Status LEDs
✓ Possibility to reset to default settings by pushbutton
✓ Robust steel case

<table>
<thead>
<tr>
<th>Feature</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power requirement</td>
<td>7 to 16 Volt DC (nominal 12 Volt DC)</td>
</tr>
<tr>
<td>Power consumption</td>
<td>7 to 12 Watt</td>
</tr>
<tr>
<td>Size</td>
<td>195 x 143 x 33 mm</td>
</tr>
<tr>
<td>Weight</td>
<td>0,77 kg</td>
</tr>
<tr>
<td>International Protection</td>
<td>IP 2 0</td>
</tr>
<tr>
<td>Operating Temperature</td>
<td>-40 to +80 °Celsius</td>
</tr>
</tbody>
</table>
2. Warranty and Safety Information

Before operating the device, read this manual thoroughly and retain it for your reference.
You can download the latest firmware and documentation for the MediaGateway here: http://www.technica-engineering.de/MediaGateway

Use the device only as described in this manual. Use only in dry conditions.
Do not apply power to a damaged device.

Do not open the device. Otherwise warranty will be lost.

This device is designed for engineering purpose only. Special care has to be taken for operation.
Do not use this device in a series production car.
As this device is likely to be used under rough conditions, warranty is limited to 1 year.
Manufacturer liability for damage caused by using the device is excluded.

EG-Konformitätserklärung

gemäß der EG-Richtlinie 2004/108/EG (elektromagnetische Verträglichkeit)
vom 15. Dezember 2004


Hersteller: Technica Engineering
Leopoldstr. 236
80807 München

Bevollmächtigter: Joseba Rodriguez

Beschreibung des Gerätes:
BroadR-Reach Ethernet MediaGateway

Datum der Erklärung: 01.06.2016

Name des Unterzeichners: Joseba Rodriguez

Unterschrift: [Signature]
3. Pinning

The pinning of the ECU connectors is listed on the label on top of the device. The Tyco Electronics (TE) Micro Quad Lock System (MQS) is used.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Part Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tyco, MQS Abdeckkappe</td>
<td>2x9 Pol, black</td>
<td>1-967416-1</td>
</tr>
<tr>
<td></td>
<td>Alternatively</td>
<td>1-1355350-1</td>
</tr>
<tr>
<td>Tyco, MQS Abdeckkappe</td>
<td>2x9 Pol, blue</td>
<td>3-967416-1</td>
</tr>
<tr>
<td>Tyco, MQS Buchsenenge- häuse</td>
<td>2x9 Pol</td>
<td>965778-1</td>
</tr>
<tr>
<td></td>
<td>Alternatively</td>
<td>962108-2</td>
</tr>
<tr>
<td>Tyco crimp contact</td>
<td></td>
<td>928999-1</td>
</tr>
</tbody>
</table>

Note: You can use the official Tyco tool for these crimp contacts. A cheap variant is the crimp tool for “PSK” contacts.
Power connector (top left)

Connector color: **Black**

Power supply for the device is supplied by Pin 1 (12Volt) and Pin 2 (Ground). Requirements for the MediaGateway itself: 12 Volt DC up to 1 Ampere (typical 600mA)

If the 12 Volt camera power output is used, this current is also sourced of Pin 1 and 2.

⚠️ **Warning:** If you apply a voltage higher than 16 Volt, the device **will be damaged**!

A wakeup-line may be connected on pin 7 or 8. The wakeup-line should have the same voltage level as the power supply (12 Volt). A high level on one of these pins wakes up the ECU from sleep mode and keeps it active. If the voltage on this pin drops below approx. 6 Volt for more than about 3 seconds the ECU will enter sleep mode. It will wake up on a high level again. Alternatively the “Prevent sleep” checkbox in the control panel of the website can be enabled.

👉 **Note:** Ethernet Traffic on any port will prevent sleep mode. Timeout is set to 100 seconds.

The LIN interface on pin 9 can be used to communicate with the Microcontroller by LIN bus. In the default software there is no data transmission specified. This interface may only be used in customer specific software.

The FlexRay interface on pin 17 and 18 can be used to communicate with the Microcontroller by FlexRay bus. In the default software there is no data transmission specified. This interface may only be used in customer specific software.

<table>
<thead>
<tr>
<th>Pin</th>
<th>Function</th>
<th>Pin</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Battery +12 Volt Input</td>
<td>10</td>
<td>Wake Line 3 (Output only)</td>
</tr>
<tr>
<td>2</td>
<td>Ground Input</td>
<td>11</td>
<td>CAN E Plus</td>
</tr>
<tr>
<td>3</td>
<td>CAN C Plus</td>
<td>12</td>
<td>CAN E Minus</td>
</tr>
<tr>
<td>4</td>
<td>CAN C Minus</td>
<td>13</td>
<td>CAN D Plus</td>
</tr>
<tr>
<td>5</td>
<td>CAN A Plus</td>
<td>14</td>
<td>CAN D Minus</td>
</tr>
<tr>
<td>6</td>
<td>CAN A Minus</td>
<td>15</td>
<td>CAN B Plus</td>
</tr>
<tr>
<td>7</td>
<td>Wake Line 2</td>
<td>16</td>
<td>CAN B Minus</td>
</tr>
<tr>
<td>8</td>
<td>Wake Line 1</td>
<td>17</td>
<td>FlexRay Plus</td>
</tr>
<tr>
<td>9</td>
<td>LIN Bus</td>
<td>18</td>
<td>FlexRay Minus</td>
</tr>
</tbody>
</table>

👉 **Note:** CAN interfaces may only be used in customer specific **CAN-Gateway firmware**.
Switch connectors

Connector color: **Blue**

The pins marked with (P) or (N) are used for the BroadR-Reach ports. Four ports are available per switch.
You have to connect the (P) pin to the (P) pin of the periphery device. You have to connect the (N) pin to the (N) pin of the periphery device.

⚠️ **Note:** If you swap these two pins the link LED may be lit on the BroadR-Reach slave side, but no data transmission will be possible.

The pins marked with (+) or (-) are 12 Volt power output pins. The actual voltage level of these pins depends on the supply voltage of the ECU. Be aware that the sum of all 12 power output pairs will deliver a **maximum of 1.2 ampere**. If more current is used the output will temporary switch off. The power output has to be switched on by website configuration (Control panel).

<table>
<thead>
<tr>
<th>Pin</th>
<th>Camera +12 Volt nominal output</th>
<th>Pin</th>
<th>BroadR-Reach Port 3, Positive</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Camera Ground Output</td>
<td>10</td>
<td>BroadR-Reach Port 3, Negative</td>
</tr>
<tr>
<td>2</td>
<td>BroadR-Reach Port 2, Negative</td>
<td>11</td>
<td>Camera Ground Output</td>
</tr>
<tr>
<td>3</td>
<td>BroadR-Reach Port 2, Positive</td>
<td>12</td>
<td>Camera +12 Volt nominal output</td>
</tr>
<tr>
<td>4</td>
<td>n.c.</td>
<td>13</td>
<td>Camera Ground Output</td>
</tr>
<tr>
<td>5</td>
<td>BroadR-Reach Port 1, Positive</td>
<td>14</td>
<td>n.c.</td>
</tr>
<tr>
<td>6</td>
<td>Camera +12 Volt nominal output</td>
<td>15</td>
<td>Camera +12 Volt nominal output</td>
</tr>
<tr>
<td>7</td>
<td>BroadR-Reach Port 1, Negative</td>
<td>16</td>
<td>Camera Ground Output</td>
</tr>
<tr>
<td>8</td>
<td>Camera Ground Output</td>
<td>17</td>
<td>BroadR-Reach Port 0, Negative</td>
</tr>
<tr>
<td>9</td>
<td>Camera Ground Output</td>
<td>18</td>
<td>BroadR-Reach Port 0, Positive</td>
</tr>
</tbody>
</table>

RJ45 Ethernet connectors

There are three RJ45 Standard Ethernet connectors of the front side.

SFP slot

There is one SFP cage for a MiniGBIC module.

The following modules have been tested:
- Edimax Mini GBIC (SFP) LC, 1 Gigabit/s, 1000 Base-SX Module
- SFPEX S1GT-A Mini GBIC (SFP) 10/100/100 MBit RJ45 Module
- BEL SFP-1GBT-05 SFP 10/100/100 MBit RJ45 Module

⚠️ **Note:** New SFP 100Base-T1 and 1000Base-T1 modules are compatible with MediaGateway.

**SFP 1000 Base-T1**

**SFP 100 Base-T1**
4. Status LEDs and Pushbutton

The MediaGateway has several status LEDs at the front side of the case.

**LEDs**

The “Host” LED can toggle at three different speeds:

- Slow toggle (approx. 0.5 sec) during normal operation to show that the microcontroller is running in normal mode.
- Fast toggle (approx. 0.1 sec) when the microcontroller is in bootloader mode. The bootloader mode is used for firmware update only (see below in this manual). You cannot access the website when the device is in bootloader mode.
- When the device is in Bootloader-Update Mode the LED toggles with moderate frequency (approx. 0.25 sec).

The port status LEDs Switch 1 to 3 and Port 3 to 0 monitors the link status of the corresponding port. The LEDs are lit when there is BroadR-Reach link detected. They begin to blink when there is data traffic on this link.

**Note:** There is an issue when P/N of the bus are swapped. The LED may be on in this case on BroadR-Reach slave side, but there will be no data transmission possible.

The built-in LEDs in RJ45 connector shows the status of the gigabit ports. The left (orange LED) is lit by a link-up. The right (yellow) will blink on data traffic.

**Push button**

The *Pushbutton* on the left side of the case will reset all settings to factory default.

Pressing this button down for 5–6 seconds with a pen when the Host Led is blinking normally:

- IP Address will be reset to default (192.168.0.49)
- All settings will be lost.

**Note:** If the device is blocked and all LEDs are lit, device must be sent to Technica Engineering.

**Note:** MAC Address will not be changed.
5. Configuration Website

You can access the configuration website with a standard web browser by connecting your PC to a RJ45 connector.

The default IP address of the device is 192.168.0.49 and subnet mask 255.255.255.0

Note: If IP address has been changed, you can reset it to default as described in this manual.

For example, set the configuration PC to IP address 192.168.0.100 and subnet mask to 255.255.255.0
Website Home

Warning: If there is a lot of broadcast traffic on the switch, the host microcontroller may be jammed. You cannot access the website in this case. Please use VLAN configuration to forward only relevant messages to the microcontroller.

With the first access to the website you will get the home screen. Please select one of the tabs for further configuration.

System Information Tab

On the tab „System Information“ some status information about the device is displayed. You can check the version number of the application firmware and the bootloader or the unique MAC address of the device. The version number registers of the switch and phy chips are displayed for information only.

Up to version 4.1.12 it also shows the UUID that the user will need to activate extra features. You can see which functionality is Unlocked.

The MAC address should be the same as on the label on the bottom of the device.

You can change the IP address of the host microcontroller (Webserver) here. If you want to use multiple devices in one network, you must configure a unique IP address for each device here.

Note: If you forgot your IP address you can reset it to default as described in chapter 4.
Control Panel Tab

<table>
<thead>
<tr>
<th>System Information</th>
<th>Control Panel</th>
<th>CAN Functions</th>
<th>Switch Status</th>
<th>Contact</th>
</tr>
</thead>
</table>

**Control Panel**

<table>
<thead>
<tr>
<th></th>
<th>Restart target</th>
<th>Configuration</th>
<th>Enable camera power</th>
<th>Prevent sleep</th>
<th>Diagnose Service</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Restart</td>
<td>Default</td>
<td>On/Off</td>
<td>On/Off</td>
<td>Off</td>
</tr>
</tbody>
</table>

**MediaGateway Feature License Activation**

<table>
<thead>
<tr>
<th>MediaGateway features</th>
<th>Activation key</th>
<th>Remove extra features</th>
</tr>
</thead>
<tbody>
<tr>
<td>CANGateway</td>
<td></td>
<td>Remove</td>
</tr>
</tbody>
</table>

On the „**Control Panel**“ tab you can:

- **Restart target**: Software reset. Configuration will NOT be lost.
- **Configuration**: It shows the current configuration name.
- **Export**: Save the stored configuration from MediaGateway into user’s PC.
- **Import**: User can import or export the configuration settings of the device to a file (*.cfg) on a computer connected to the RJ45 Port. A restart is needed to apply the new configuration.
- **Default**: You can reset the configuration settings to default. All the configuration stored will be revert to its defaults values. IP address will be not modified.
- **Enable camera power**: The camera power output pins are disabled by default. To activate them, this checkbox should be checked.
- **Prevent sleep**: If you do not want to use a Wakeup line, you can enable the “Prevent sleep” checkbox (default). This will keep the device running without entering the sleep mode. If this option is disabled, the device will restart if no ethernet activity is detected within 60 seconds.
- **Diagnostic service**: If you enable “Diagnose Service” functionality, MediaGateway will send periodically status information about its state. For example, transmitted and dropped frame counters, link quality, etc.. More details about the format of these frames see the Fibex File (and .pdf description) in the firmware release files.
MediaGateway Feature License Activation

In order to activate extra features (CAN Gateway, FlexRay Gateway, BMW Extra Functions), the user should contact us at order@technica-engineering.de to order an activation key.

User must provide de UUID code in the order of purchase.

Technica-Engineering will provide an Activation code for the desired feature. Received activation code must be entered in control panel.

Next picture shows how to unlock CAN Gateway feature after receiving the activation code:

1. Select the feature: CANGateway
2. Insert the code
3. Save configuration and restart the device.
Switch Status Tab

The main configuration of the switch is done in the „Switch Status“ tab. Here you can configure details about each port and get some status information about the ports and switch states.

On the left side of the page you can see an overview of all available ports. A blue bar at the side of a port label indicates an active link (On the Cascade SFP port there is no link indication).

Global Configuration

In global configuration, user can change global settings affecting all three switches inside MediaGateway.

- **IEEE 802.1q (VLAN) mode**: Activates port based Single VLAN.
- **Double Tagging**: If IEEE 802.1q (VLAN) mode is activated, it is possible to work with double tagging.
- **Double Tagging TPID**: On Board Switches uses an old non-standard 802.1QinQ 0x9100 ether type (TPID) for double tagged frames. New 802.1QinQ standard uses TPID 0x88A8.
ARL Table status

When you click on the “Switch 1..3” witch label the entries of the **Address Resolution Table** in selected switch will be displayed.

ARL Table shows the following information:
MAC addresses, VLAN ID, Forward port, Age Bit and Static bit

In next example we see that **Switch 1** has two ARL Entries:
1) MAC Address 00:50:C2:E4:34:E5 is present on **port 4** using VLAN ID 0x049.
2) MAC Address 00:24:9B:06:7B:97 is present on **port 5** using VLAN ID 0x049

**Note:** When **IEEE 802.1q (VLAN) mode** is disabled, VLAN will be 0x000.

![Switch Status Diagram](image)

**Note:** By default, the MediaGateway is using Dynamic ARL Table.
Dynamic ARL table

By default, dynamic ARL mode is active on all three internal switches. It means that the information collected from received unicast packets are learned or stored for the future purpose of forwarding frames addressed to the receiving port.

For a received frame, it learns received MAC source address, VLAN ID (if not present VLAN ID = 0x00) and it creates an entry. This entry is dynamic, so it will be active for 300 seconds. After 300 seconds, if no further frames matching this entry are received, the entry will be aged (aged_bit = 0) and removed from the forwarding table. New learning will be necessary.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>Received Source MAC Address</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>VLAN ID associated with the MAC Address</td>
</tr>
<tr>
<td>Fwd port</td>
<td>Port associated with the MAC Addr</td>
</tr>
<tr>
<td>Age bit</td>
<td>1 = Entry has been learned or accessed since last aging process 0 = Entry has not been accessed since last aging process.</td>
</tr>
<tr>
<td>Static bit</td>
<td>Entry has not been learned and cannot expire.</td>
</tr>
</tbody>
</table>

Static ARL table

The MediaGateway permits to each internal switch to use a dynamic or a static ARL table. In ARL Static Table mode the entries do not automatically learn MAC addresses or port associations and are not age out by the automatic internal aging process.

Changing the functional mode of a switch.

To change the functional mode of the switch, the following steps should be performed:

1. Select Switch Status tab.
2. Select the switch in which you want to modify the ARL Table.

3. In the table, which will appear on the right side, user can select Dynamic or Static mode.
Configuring the ARL table of a switch

To add new ARL entries the user must change the *Functional mode* to *Static* followed by selecting *Edit Table* option. The steps are described below.

After performing the steps above the configuration options will appear. Here the user can add data manually, import configurations and reset the ARL table.
Adding a unicast
Frames containing a unicast destination address are assigned a forwarding field corresponding to a single port. Adding manually an entry of this type shall be performed as following:

After restart the data entered shall be displayed in the **Address Resolution Table** of the switch.

*Note:* The last bit of first byte of a MAC of a unicast shall be 0. Ex: FE:FF:FF:FF:FF

Adding a multicast
Frames containing a multicast destination address are assigned a forwarding field corresponding to multiple ports specified in a port map. If no matching ARL entry is found, the packet is flooded to all appropriate ports.

After restart the data entered shall be displayed in the **Address Resolution Table** of the switch.

*Note:* The last bit of first byte of a MAC of a **multicast** shall be 1. Ex: F9:FF:FF:FF:FF
Importing configuration

The user can import a configuration file of type JSON which contains the desired setup:

Export configuration

To export a configuration to a file of type JSON the illustrated steps shall be performed:
Configuration file format

Below it is illustrated a valid configuration JSON file:

```json
{
    "urlEntry": {
        "unicast": {
            "urlMAC": "A8:70:44:00:00:00",
            "vid": "0",
            "port": "4",
            "age": "0",
            "staticBit": "1"
        },
        "multicast": {
            "urlMAC": "B8:70:44:00:00:00",
            "vid": "0",
            "port": ["1", "2", "3", "4"],
            "age": "0",
            "staticBit": "1"
        }
    }
}
```
Reset switch configuration

If needed, the user can erase all the changes applied to a switch as follows:
Ports

The MediaGateway has 4 kinds of ports. A total of 21 configurable ports.

- P4 and P8 are internal Ports which are used to connect the switches with a gigabit link.
- The Microcontroller is connected with a 100 MBit/s link to Switch-1 Port 4 (P4 CPU).
- Switch-3 P8 is an extension gigabit port for the right RJ45 port. For every port, following fields are common.

<table>
<thead>
<tr>
<th>Port Name</th>
<th>Description label will give a better information. (Config-PC, Datalogger, CAM-1, etc.)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default VLAN ID</td>
<td>Port will use this identifier per default</td>
</tr>
<tr>
<td>VLAN membership</td>
<td>Port will be member of this list of VLANs</td>
</tr>
<tr>
<td>VLANs to untag</td>
<td>Port will untag packet</td>
</tr>
<tr>
<td>Egress VID remarking</td>
<td>Port can modify the inner/outer VLAN at egress.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TX Octets</th>
<th>Tx octets status counter for the outgoing bytes of this port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rx Octets</td>
<td>Rx octets status counter for the incoming bytes of this port.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Inner VLAN IDs:</th>
<th>Port will drop packets with single tag specified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source IP</td>
<td>Port will drop packets with specified source IP address</td>
</tr>
<tr>
<td>Destination IP</td>
<td>Port will drop packets with specified destination IP address</td>
</tr>
</tbody>
</table>

Some other fields are port dependent and will be discussed in following sections.

Note: More information about VLANs will be described in chapter 6.
Besides the common fields to all ports, Ethernet ports allows the user to select link speed.

- **Mirroring**: The “Mirroring” feature of a current port copies all incoming traffic from the checked port (BroadR-Reach or internal port) to this “capture” port.

  Note: Only one port per switch can be the “capture” port! If another port (internal P4 or P8) is using mirroring, Ethernet port cannot use mirroring.

- **Speed**: It is possible to set the speed of an Ethernet port through auto-negotiation. Following table shows the available options:

<table>
<thead>
<tr>
<th>Auto-negotiation all Capable</th>
<th>Duplex and Speed auto-detection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto – Only 10 Mbps Capable</td>
<td>Duplex auto-detection – 10 Mbps</td>
</tr>
<tr>
<td>Auto – Only 100 Mbps Capable</td>
<td>Duplex auto-detection – 100 Mbps adv.</td>
</tr>
<tr>
<td>Auto – Only 1000 Mbps Capable</td>
<td>Duplex auto-detection – 1000 Mbps adv.</td>
</tr>
</tbody>
</table>

- **Detected speed**: Show result of link negotiation. Speed and half/full duplex.
Besides the common fields to all ports, BroadR-Reach ports allows the user to:

- **Enable port**: With this checkbox the BroadR-Reach ports can be enabled or disabled completely.

  ⚠️ **Note**: If port is disabled and cable is still connected, LED status for this port will be lit but no data is sent or received. Webpage will show no blue bar for this port.

- **BroadR-Reach mode**: On each BroadR-Reach link there has to be one master and one slave device.

  Please set the “BroadR-Reach mode” to the opposite of what the device is set you have connected to this port.

- **Output level**: The “Output Level” is the amplitude level of the BroadR-Reach signal. You can set Full level (Fullout = default) or half amplitude.

  ⚠️ **Note**: Both devices of one BroadR-Reach link have to use the same level. Otherwise you will get an instable link. FullOut Level is always recommended.

- **Link Quality**: The “link quality” is an indicator about the signal integrity of the BroadR-Reach link on this port.

  \[1 = \text{Poor}, \quad 5 = \text{Excellent}\]
BroadR-Reach Test Modes

For BroadR-Reach Ports it is possible to set a BroadR-Reach Physical Layer Test Mode. There are five test modes defined in the BroadR-Reach Specification to check the compliance of a port.

⚠️ **Warning**: When a test mode has been selected there is no communication possible for this port.

⚠️ **Important**: In case of BroadR-Reach Master, it is mandatory to restart the Switch to recover link.

📝 **Note**: For compliance testing an oscilloscope with special test software is necessary.
**SFP Port**

Up to HW version 2.6, it is possible to read and configure some parameters for connected SFP Modules.

![Diagram of SFP Port configurations](image)

Besides the common fields to all ports, SFP ports allows the user to select which module is connected.

- **SFP option:** You have the choice of different modules.
  1. The SFP Port can be set to “Fiber” if you care using a SFP MiniGBIC Fiber module.
  2. Use “RJ45” for copper modules.
  3. Use HSD for old MediaSwitches which have an HSD connector instead of an SFP slot.
4. The SFP module is not part of standard delivery.

✓ The SFPEX 10/100/1000 Modules have been tested in this device.

✓ The Bel SFP-1GBT-05 Copper Modules 10/100/1000Base-T have been tested in this device.

The Edimax Mini GBIC (SFP) LC, 1Gigabit/s, 1000 Base-SX Modules have been tested in this device.

**Note:** New SFP 100Base-T1 and 1000Base-T1 modules are compatible with MediaGateway.

**SFP 100Base-T1**

**SFP 1000Base-T1**
6. Ethernet CAN Gateway (extra license needed)

The Ethernet CAN gateway can be configured using a web page. Its properties can be set on the “CAN Functions” page. The following picture shows the available settings.

CAN Gateway settings can be set as Basic or Advance mode.

Basic settings
Most common configuration. Gateway between Ethernet and CAN frames and vice versa. User is only able to configure MAC destination addresses for Ethernet outgoing frames.

**Note:** Basic mode is recommended when using together with ANDi Tool software.

Advanced settings
In advanced settings all configuration parameters are available for the users. There are four modes of communications (UDP, RAW, Speed RAW and Extrem RAW). The switching between them is done using the radio button Communication Mode.

User can use CAN Parameters table to set CAN Channel speed and set a list of CAN IDs to be filtered.

- **Speed:** CAN channel speed can be set to: 125 Kbps, 500 Kbps or 1000 Kbps.
- **CAN ID Filtering:** Can be activated for each channel independently.
- **Can Listen-Only Mode:** This is used for logging without sending ACK on CAN bus.
Ethernet CAN Gateway Configuration (UDP mode):

Here the Ethernet CAN gateway can be configured by setting target IP Address and the port of the UDP packets. Non-valid entries will not be accepted and will be replaced by default values. If either the target IP address or the port has the default value set, the Ethernet CAN Gateway will be disabled.

**Eth-CAN Gateway Functions Panel**

**Ethernet CAN Gateway Mode**

<table>
<thead>
<tr>
<th>Communication mode</th>
<th>UDP</th>
<th>RAW</th>
<th>Speed RAW</th>
<th>Extrem RAW</th>
</tr>
</thead>
</table>

**CAN Parameters**

<table>
<thead>
<tr>
<th></th>
<th>CAN A</th>
<th>CAN B</th>
<th>CAN C</th>
<th>CAN D</th>
<th>CAN E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>500 Kbps</td>
<td>500 Kbps</td>
<td>500 Kbps</td>
<td>500 Kbps</td>
<td>500 Kbps</td>
</tr>
<tr>
<td>CANID Filtering</td>
<td>Filter: [ ]</td>
<td>Filter: [ ]</td>
<td>Filter: [ ]</td>
<td>Filter: [ ]</td>
<td>Filter: [ ]</td>
</tr>
</tbody>
</table>

**CAN IDs for CAN A**

001, 002, 003

**CAN IDs for CAN B**

004, 001, 005

**Ethernet to CAN: Incoming configurable parameters**

<table>
<thead>
<tr>
<th>rxPort</th>
<th>1024</th>
</tr>
</thead>
</table>

**CAN to Ethernet: Outgoing configurable parameters**

| Destination IP address | 102.166.0.55 |

- **Destination IP address**
  
  Here the target IP address for the UDP packets can be entered in dot-decimal notation. The default IP address is 255.255.255.255.

- **rxPort**
  
  MediaGateway will listen for UDP-CAN packets on selected UDP port. Please select a non-reserved port number.
  
  Received CAN messages will be send to destination IP and destination port set on rxPort.
Ethernet CAN Gateway Configuration (RAW mode):

Here the Ethernet CAN gateway can be configured by setting target MAC Address and the EtherType of the RAW packets. Non-valid entries will not be accepted and will be replaced by default values. If either the target MAC address or the EtherType has the default value set, the Ethernet CAN Gateway will be disabled.

**Eth-CAN Gateway Functions Panel**

**Ethernet CAN Gateway Mode**

<table>
<thead>
<tr>
<th>Communication mode</th>
<th>UDP</th>
<th>RAW</th>
<th>Speed RAW</th>
<th>Extrem RAW</th>
</tr>
</thead>
</table>

**CAN Parameters**

<table>
<thead>
<tr>
<th></th>
<th>CAN A</th>
<th>CAN B</th>
<th>CAN C</th>
<th>CAN D</th>
<th>CAN E</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speed</td>
<td>500 Kbps</td>
<td>500 Kbps</td>
<td>500 Kbps</td>
<td>500 Kbps</td>
<td>500 Kbps</td>
</tr>
<tr>
<td>CANID Filtering</td>
<td>Filter:</td>
<td>Filter:</td>
<td>Filter:</td>
<td>Filter:</td>
<td>Filter:</td>
</tr>
</tbody>
</table>

**Ethernet to CAN: Incoming configurable parameters**

- **EtherType (hex)**: 0x00

**CAN to Ethernet: Outgoing configurable parameters**

- **Target MAC address**: 00:11:22:33:44:55
- **EtherType (hex)**: 0x00

- **Target MAC Address**: Target MAC address must respect the usual format (a sequence of six hexadecimal numbers having two bytes size each, separated by a two points delimiter) xx:xx:xx:xx:xx:xx. Note that entering Broadcast MAC address “0xFFFFFFFFFFFF” as Target MAC address will cause sending time stamps frames to be disabled.

- **EtherType**: EtherType is a two bytes hexadecimal number. EtherType field can accept any value between 0 and FFFF.
6.1 Ethernet CAN Gateway Configuration (Speed and Extreme RAW)

- Speed RAW is faster as normal RAW. Incoming Ethernet-RAW frames are fixed to Ethernet Type: 0x1886

- Extreme RAW is the fastest mode. It is only accepting RAW Frames with EthernetType 0x1887
Structure of a CAN/Ethernet packet

The following picture shows the structure of a CAN packet that is sent as a UDP packet/RAW frame.

<table>
<thead>
<tr>
<th>B0</th>
<th>B1</th>
<th>B2</th>
<th>B3</th>
<th>B4</th>
<th>B5</th>
<th>B6</th>
<th>B7</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>version</td>
<td>CAN Channel</td>
<td>ID</td>
<td>ID</td>
<td>ID</td>
<td>ID</td>
<td>ID type</td>
</tr>
<tr>
<td>8</td>
<td>DLC</td>
<td>D0</td>
<td>D1</td>
<td>D2</td>
<td>D3</td>
<td>D4</td>
<td>D5</td>
</tr>
<tr>
<td>16</td>
<td>D7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>version</td>
<td>uint8</td>
<td>Version of the CAN/Ethernet Packet type. It is always 1 for this type of CAN/Ethernet packet.</td>
</tr>
<tr>
<td>CAN channel</td>
<td>uint8</td>
<td>Number between 1 and 4 for the channel CAN of this packet.</td>
</tr>
<tr>
<td>ID</td>
<td>uint32</td>
<td>CAN ID for base or extended frame format.</td>
</tr>
<tr>
<td>ID type</td>
<td>uint8</td>
<td>0 for 11 Bit standard ID, 1 for 29 Bit extended ID</td>
</tr>
<tr>
<td>frame type</td>
<td>uint8</td>
<td>0 for CAN data frame, 1 for CAN remote transmission request</td>
</tr>
<tr>
<td>DLC</td>
<td>uint8</td>
<td>Payload length of the CAN packet.</td>
</tr>
<tr>
<td>D0 ... D7</td>
<td>1 to 8 x uint8</td>
<td>Payload</td>
</tr>
</tbody>
</table>
Structure of a UDP packet / RAW frame:

- CAN packet packed in a UDP packet:

<table>
<thead>
<tr>
<th>Ethernet Header (14 Bytes)</th>
<th>IP Header (20 Bytes)</th>
<th>UDP Header (8 Bytes)</th>
<th>Payload (CAN packet) (17 Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Destination IP Address (4 Bytes)</td>
<td>Destination Port (2 Bytes)</td>
<td></td>
</tr>
</tbody>
</table>

**UDP Packet size=59**

- CAN packet packed in RAW frame:

| Destination MAC (6 Bytes) | Source MAC (6 Bytes) | EtherType (2 Bytes) | Payload (CAN packet) (17 Bytes) |

**RAW Frame Size=31**

Note: Fields in red color are settable through the website (Ethernet CAN Gateway Configuration).
7. 802.1AS

This chapter explains the current support of the MediaGateway for 802.1AS protocol.

802.1AS is a protocol used between two or more devices to synchronize all of them through an Ethernet communication. This synchronization allows two or more devices (one master and one or multiple slaves) to transmit/receive time-critical information as audio or video through a physical link and assures that all the devices will handle the same time reference to encode/decode correctly the information.

This special software allows to maintain the synchronization between the 802.1AS connected devices, receiving, modifying and creating new corrected packets for the 802.1AS protocol, correcting so the possible delays generated for the routing through the Switch and the propagation delays of the cables.

Protocol

The software allows MediaGateway to be converted in a time-aware system bridge, which implements the transport of time-synchronization information and also the mechanism for the measurement of the propagation delay.

Transport of time-synchronization information

For the reference case where this communication is established only between two devices, „Time-aware system i-1“ configured as 802.1as master and „Time-aware system i+1“ configured as slave, the ports of the MG („Time-aware system i“) implements additionally then the respective opposite sides of the communication, one slave port and one master port, as shown in the next image.

The time-synchronization information contained on the Sync and Follow Up messages sent by the „Time-aware system i-1“ is redirected and only received by the MediaGateway processor. These packets are decoded and the relevant information extracted. The extracted information is used later to generate, together with the information extracted from the propagation delay algorithm, the new corrected Sync and Follow Up messages that will be sent to the „Time-aware system i+1“. In the new generated packets, a field called “correction field” will be changed and this parameter will be used on reception side to adjust the reference time of the system considering the delay of the switch and the delay in the path „Time-aware system i-1“ to „Time-aware system i“.
Propagation delay measurement

For the correction adjust of the time reference transmitted by the Sync and Follow Up Packets, the delay between the initiator of the protocol „Time-aware system i-1“ and the first slave port of the MediaGateway „Time-aware system i“, should be measured.

\[
D = \frac{f_{12} + f_{21}}{2} = \frac{(t_4 - t_3) - (t_3 - t_2)}{2}
\]

The measures of the propagation delay are performed by each attached link of an 802.1as communications, it means each side of the link will generate and response to these packets, called Pdelay_Request, Pdelay_Response and Pdelay_Response_Follow_Up.
Using 802.1 AS

MediaGateways allows the user to configure through the webpage six different bridges. Each of them offers two possibilities: BridgeX_Master or BridgeX_Slave.

Each Broad-R Reach port can set as:

1. **Disabled**: Port will not take part of any 802.1AS traffic.
2. **BridgeX_Slave**: Only one per BridgeX. It will receive 802.1AS traffic from an external master.
3. **BridgeX_Master**: Port will send 802.1AS traffic coming from its BridgeX_Slave.

![Diagram of MediaGateway configuration](image)

**Note**: Only one port in each bridge can receive the information of one attached 802.1AS Master. This means that only one port of this MediaGateway BridgeX should be configured as a BridgeX_Slave, but more than one port of the same BridgeX can be configured as BridgeX_Master, allowing so a distribution of the time reference 1 to N (with all the devices of the bridge sharing the same time reference, with N limited to 3).

4. **Master_802.1AS**: Port will work as 802.1AS Master Clock.

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.30102400</td>
<td>Technica:08:00</td>
<td>LLDP_Multicast</td>
<td>PTPv2</td>
<td>68</td>
<td>Path_Delay_Req</td>
</tr>
<tr>
<td>0.30185700</td>
<td>Technica:09:00</td>
<td>LLDP_Multicast</td>
<td>PTPv2</td>
<td>60</td>
<td>Sync Message</td>
</tr>
</tbody>
</table>

Traffic capture of a Master Clock

**Warning**: Redirection of 802.1AS packets to processor are not following normal use of VLANs.
Limitations

Due the need of working constantly with a high precision timestamping’s and the huge number of packets pro 802.1AS OABR port that should be received and transmitted by the microcontroller of the MediaGateway there are some limitations that the user has to know before start to use it.

- The implementation allows only the use of the 802.1AS in the 12 x OABR Ports of the MediaGateway, due technical reasons the use of the protocol 802.1AS on the Ethernet Ports is not possible.

- A Bridge should be formed by at least one port configured as Bridge_Slave (Connected with 802.1AS Master) and up to 3 Ports configured as Bridge_Master (Connected with 802.1AS Slave). It means the next possibilities pro Bridge are allowed: 1BS:1BM, 1BS:2BM and 1BS:3BM.

- For a correct synchronization, all ports that forms one Bridge (2 to 4 ports) should be connected to the same Broadcom Ethernet Switch.
  
  o Broadcom Ethernet Switch 1: OABR Ports 0 to 3
  o Broadcom Ethernet Switch 2: OABR Ports 4 to 7
  o Broadcom Ethernet Switch 3: OABR Ports 8 to 11

- For the use of the 802.1AS Bridge functionality of the MG, the configuration of the MediaGateway should use double VLAN with unidirectional VLANs.

- For 802.1AS should not be used together with traffic injection. This means that no Ethernet Test Tools should generate traffic and routed using a MediaGateway while 802.1AS is being used.

- Announcement packages from best master clock (BMC) algorithm are not corrected or forwarded. They should not be present on automotive as there is only one Master Clock.

⚠️ Important: When 802.1AS is activated, there some parameters should be taken into account:

1. It is mandatory to set Egress Remarking of port P4 (CPU) as Normalized / Normalized.

2. The implementation won’t be functional using bidirectional VLANs. 802.1AS packets are automatically forwarded to CPU port and destination ports. It is mandatory to use Double Tagging for the processor to be able to send the corrected packet into correct destination port.
8. VLAN Configuration

This chapter describes the Virtual Local Area Network (VLAN) feature supported by internal switches present in the device. MediaGateway provides flexible VLAN configuration for each ingress (receiving) port.

Note: It is not possible to cover all of possible combinations that VLAN feature provides. It will be explained as accurate as possible with a couple of uses cases.

VLAN Basics

A Virtual LAN (VLAN) is a logical switched LAN formed by segmenting physical Local Area Networks (LANs).

Separating a switched LAN into one or more VLANs provides multiple advantages:

1. Multicast and Broadcast packages flood are limited only to the required segments to save LAN bandwidth.
2. Provides security. LAN traffic is restricted only to its specific segment.
3. Eases management by logically grouping ports across multiples switches.

VLAN work in the same was as physical LANs. Source device sends a packet to an end station or network device inside the same VLAN.

The MediaGateway allows the user to create Virtual Local Area Networks (VLANs), in order to separate traffic of different sources and providing a better general performance.

Port-Based VLAN

MediaGateway uses port-based VLAN. This feature partitions the switching ports into a virtual private domain designated on a per-port basis. Data switching outside of the port private domain is not allowed.

The port-based VLAN feature works as a filter, rejecting all the traffic destined to non-private domain ports.

Once a packet is received, MediaGateway’s switch tries to identify the VLAN for the received packet. A port based VLAN determines the membership of a data frame by examining the configuration of the port that received the transmission or reading a portion of the data frame’s tag header. A four-byte field in the header is used to identify the VLAN. This VLAN identification indicates what VLAN the frame belongs to. If the frame has no tag header, the switch checks the VLAN setting of the port that received the frame. If the switch has been configured for port based VLAN support, it assigns the port’s VLAN identification to the new frame.
Single Tagging - IEEE 802.1q (VLAN) mode

When the “IEEE 802.1q (VLAN) mode” is enabled, it is possible to can up to 4096 VLANs (Virtual Local Area Network) for routing the traffic through the switch.

Note: This is a global option applying to all three switches.

Warning: Expert knowledge is needed to use these VLAN settings! Only use these settings if you have understood the VLAN process.

Difference between a normal Ethernet and a Single tagged VLAN frame is represented as it follows:

<table>
<thead>
<tr>
<th>VLAN Frame</th>
<th>Ethernet Frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>Untag</td>
<td></td>
</tr>
<tr>
<td>Single Tag</td>
<td></td>
</tr>
</tbody>
</table>

**TPID** = Tag Protocol Identifier, EtherType.
A value of 0x8100 indicates that the frame has VLAN 802.1q information.

**VID** = Vlan Identifier.
A value indicating to which VLAN domain belongs the packet.
View of the Port Configuration with Single Tagging activated:

Once **IEEE 802.1q (VLAN) mode** is enabled, several fields common to all ports will be available:

- **Default VLAN ID**: User can set the default VLAN identifier for this port.

  Note: Untagged frames received to this port will be tagged with its Default VLAN ID. If user does not set a Default VLAN ID, frames will be tagged with ID=1 at ingress.

- **VLAN Membership**: Setting a “VLAN membership” ID makes the port a member in the given virtual LAN. The switch will route (“forward”) packets which are tagged with one of these IDs to this port.

- **VLAN to untag**: Packets matching this list of VLAN IDs will be untagged at egress (“outgoing”).

- **Drop ingress packets with:**
  - **inner VLAN IDs**: Packets matching this list of VLAN IDs will be dropped. This fields may be filled with comma or space separated lists of numbers (VLAN IDs). The VLAN IDs are entered in 3 digit hexadecimal format. Valid numbers range from 001 to FFF.
Single Tagging Example

If user needs to analyze traffic between a Camera and ICAM to a “stand alone” datalogger or a computer using a Traffic analyzer, following setup can meet this purpose.

User wants to:
1. Set VLAN for accessing to MediaGateway’s webpage.
2. Set VLAN between ports BR-S1-P3 and BR-S1-P1 and redirect it to Log Device at S2-P5.

Setting VLAN for MediaGateway’s webpage.
   a. For PC-Config port (S1-P5) we set a both VLAN and a VLAN Membership to 0x49

Warning: As our computer is not using VLAN, we untag packets.

b. For CPU port, we set the same VLAN as in PC-Config.

Warning: MediaGateway’s CPU is not using VLANs. Make sure you untag the frames.
2. Setting VLAN between ports BR-S1-P3 and BR-S1-P1 and redirect it to Log Device at S2- P5.

It is supposed that the devices (Camera and iCAM) are working with VLAN ID=0x80. Now we are going to create a VLAN with ID 0x80 between ports BR-S1-P3 and BR-S1-P1.

a. Create a VLAN with ID 0x80. Ports BroadR-Reach 1 and 3 will be members.

b. Datalogging is on Switch2 – Port5. User has to do a Mirroring from Ports P3 and P1 to obtain a copy of traffic flow to P8.

Note: Mirroring copies only traffic inside the same VLAN Membership.

c. On port P4 from Switch-2, the membership 0x80 must be added. At this moment all the packets from ports P3 and P1 from the Switch 1 will be visible through P4. Last step is forwarding all the traffic to the Datalogger port S2-P5.
Double Tagging - IEEE 802.1q (VLAN) mode

Media Gateway supports *Double tagging*. This feature can be enabled at the global configuration.

![Switch Status Diagram](image)

**Note:** This is a global option applying to all three switches.

This feature allows to use a second tag “Outer Tag” besides the Single tag “Inner Tag”. This extra tag (Double tag) provides an addition layer of tagging to the existing IEEE 802.1Q VLAN. When the double-tagging feature is enabled, users can expect two VLAN tags in a frame.

### VLAN Frame

<table>
<thead>
<tr>
<th>Destination MAC</th>
<th>Source MAC</th>
<th>TPID</th>
<th>EtherType</th>
<th>Size</th>
<th>Payload</th>
<th>CRC / FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Untag</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Ethernet Frame

<table>
<thead>
<tr>
<th>Destination MAC</th>
<th>Source MAC</th>
<th>802.1Q Header</th>
<th>EtherType</th>
<th>Size</th>
<th>Payload</th>
<th>CRC / FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Tag</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Destination MAC</th>
<th>Source MAC</th>
<th>802.1Q Header</th>
<th>EtherType</th>
<th>Size</th>
<th>Payload</th>
<th>CRC / FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Double Tag</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**TPID** = Tag Protocol Identifier, EtherType.
A value of 0x9100 indicates that the frame has double tag information.

**Outer VID** = Tag close to Source MAC is the ISP tag (Outer Tag).

**Inner VID** = Tag following is the Customer tag (Inner Tag).
With enabled “Double tagging” for each port, user can set now the following parameters for VLAN settings. Following picture shows in green the available fields for *Double tagging*.

**Default VLAN ID**: User can set the default VLAN identifier for this port.

- **Note**: Untagged frames received to this port will be tagged with its Default VLAN ID. In case of

**VLAN Membership**: Setting a “VLAN membership” ID makes the port a member in the given virtual LAN. The switch will route (“forward”) packets which are tagged with one of these IDs to this port.

**VLAN to untag**: Packets matching this list of VLAN IDs will be untagged at egress (“outgoing”).

- **Note**: This option is not available if “*Double tagging*” is activated.

**Drop ingress packets with inner VLAN IDs**: Packets matching this list of VLAN IDs will be dropped.
If double tagging is active the “Normalization” process takes place on all ingress packets on all ports. The normalization process modifies all incoming packets with one or zero VLAN tags so that every packet has two VLAN tags afterwards. Every packet that flows through the switch is double tagged.

Three different cases of normalization are possible:

1. **Packet is received with two VLAN tags** (double tagged)
   - The packet will be left unchanged
   - The packet will be forwarded if the packet VLAN is matching its Outer VLAN membership.

2. **Packet is received with one VLAN tag** (a single tagged packet with a so called customer tag /inner tag)
   - A second tag (also called ISP /outer tag) with TPID 0x9100 will be added with configured with the “Default VLAN” ID for this port to the packet during normalization.

3. **A packet is received without any VLAN tags**
   - In this case, the normalization process adds two VLAN tags, the inner tag with TPID 0x8100 and the outer tag with TPID 0x9100. Both tags will hold the “Default VLAN” ID of this port.
   - With double tagging enabled, only the **outer** tag (the one with TPID 0x9100) is relevant for frame forwarding, i.e. the “VLAN membership” refers to the outer tag.
   - TPID = Tag Protocol Identifier, EtherType
   - A value of 0x8100 indicates that the frame has VLAN 802.1q information.
   - A value of 0x9100 indicates that the frame has QinQ (Double Tagging).

With “Egress VID remarking” (available if double tagging is enabled only) you can specify, how to modify the packets before they are sent on this port.

Three options are available for inner and outer VLAN tag:

1. **“As received”** means the tag shall left unchanged as the packet was received from its ingress port.
   - If this tag was there before normalization it shall be sent with the same value.
   - If no tag was there on ingress it shall be sent without this tag.

2. **“Normalized”** means that the tag shall be sent as the internally normalized VLAN tag (Default VID of the receiving port).

3. **“Remove”** indicates that this tag shall be removed before the packet is transmitted.
Double Tagging Example

The scenario of this use-case is:

- Up to six BroadR-Reach cameras should be connected to their dedicated ports on one central ICAM ECU.
- Each camera stream must not influence the other camera streams.
- Mirroring of all the camera data streams to the “Datalogger” gigabit Ethernet port has to be possible.

 ısı: By default all series cameras are configured as a BroadR-Reach Master and FullOut.

The BroadR-Reach cameras used for series production send their Ethernet packets with a VLAN tag (inner Tag) to identify the “type” of traffic transported in it (e.g. video- or control-data).

With double tagging a VLAN “outer-tag” will be added to each data packet. After all data is stored on the datalogger hard disk drive, the information “On which connection has the packet been received?” can be derived from the ID number of the “outer tag”.

Each Ethernet packet recorded by the data-logger has an inner VLAN tag (with TPID 0x8100) showing the type of traffic and an outer VLAN tag (with TPID 0x9100) containing information about the ingress port. Packets sent from the camera to the ECU (and vice versa) will show up unchanged on the outgoing BroadR-Reach port with only one VLAN tag. The switch is “transparent” for this connection.

Note: For BR-Ports, Egress VID Remark will be set. Inner: As received. Outer: Remove
The “Datalogger” gigabit Ethernet port and the internal ports (P4, P8) connecting the three switches are configured so that all incoming BroadR-Reach packets will be mirrored to the data-logging port, regardless of the address resolution learning mechanism of the switches (“promiscuous mode”). To achieve this, suitable mirror maps are defined as well as the VLAN Memberships of the BR-Ports for the internal ports (S1-P8 and S3-P4) and the data-logging port (S2-P5).

The gigabit Ethernet port “Config-PC” shares a private VLAN (ID 0x049) with port S1-P4 to be able to reach the internal CPU of the MediaSwitch for configuration and status-monitoring. All outgoing packets on the “Config-PC” port will be untagged (all VLAN tags removed) for usage with a standard desktop PC.

Note: There is a pre-configured port-based forward map that avoids packet-forwarding from ports other than the “Config-PC” port to the CPU port (S1-P4). This rule is intended to prevent flooding the CPU with useless packets and prevent loops. This implies that the integrated webserver of the MediaSwitch is reachable via the port “Config-PC” only.
9. MAC Filtering for mirroring

This new feature allows the user to filter undesired packets arriving from several sources to be mirrored to a Datalogger.

**Note:** This feature is only available on Ethernet Ports (S1-P5, S2-P5, S3-P5, S3-P8)

By default, no port has Mirror activated, so this feature won’t be active by default

If the user wants to mirror traffic from several sources but does not need all of them to be mirrored, this options allows to “filter” undesired MAC sources.

Next example will clarify how MAC Filtering for mirroring ports is working:

1. **Mirroring is active and MAC filtering disabled**

   In this case, all devices will be mirrored on S1-P5 as usual in normal mirroring.
2. Mirroring is active and MAC filtering activated for Broadcast packets

In this case, all devices will be mirrored on S1-P5 as usual in normal mirroring but packets with destination MAC FF:FF:FF:FF:FF which the user does not need to analyze will not reach the port S1-P5.

Note: MAC filtering will not affect the normal forwarding behavior of the Switch. Dropped packets at mirroring port will still reach its destination.
10. MediaGateway Remote Control

From firmware version 4.1.23, it is possible to configure and change some values of the MediaGateway through SOME/IP messages.

Currently there are some methods implemented:

1. Restart device
2. Import Configuration
3. Export Configuration
4. Import Dynamic Configuration
5. Check Status
6. Wake Up Line Trigger
7. Wake Up Line Sense
8. Port Enable
9. Port Master/Slave
10. Reset to Defaults
11.

To use one of the previous, user should be send an SOME/IP packet over UDP to the MediaGateway.

UDP Packet should be sent to:
IP destination: MediaGateway IP
UDP Port: 30491

This SOME/IP packet contains 16 bytes of header. The bytes description of following table refers only the SOME/IP header (16 bytes after UDP layer) and payload.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PAYLOAD [variable size]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: 192.168.0.150:30491 (depending on Computers IP)
Destination: 192.168.0.49:30491 (depending on MediaGateways current IP)
ServiceID: 0x0124
MethodID: 0x0001 (depending on users requested method)
Length: 0x08 + sizeof(payload)
Request: 0x00000000
Interface version: 0x1
Protocol version: 0x1
Message Type: 0x0
SessionID: 0x0000 ClientID: 0x0000
Payload: (if necessary)
The fields of a SOME/IP request (message from user to MediaGateway) differs only on:
- Method ID
- Length (depending on used payload)
- Payload

**Reset device**
This method performs a complete device reset. Configuration after a device restart will loaded from flash.

**Method ID: 0x0001**

a) **REQUEST:** Method ID has to be set to 0x0001. No payload needed.

```
Internet Protocol Version 4, Src: 192.168.0.150 (192.168.0.150), Dist: 192.168.0.49 (192.168.0.49)
SOME/IP Protocol, Service ID: 0x0024, Method ID: 0x0001, Length: 8, Session ID: 0x0000
Message ID: 0x01240001
Service ID: 0x0124 (debugservice/mediaswitch)
Method ID: 0x0001
Length: 8
Session ID: 0x0000
```

b) **RESPONSE:** This method returns a SOME/IP Message with Return Code 0x00 (OK) before restarting.

**Import configuration**
Same behavior as Import button from Webpage. It will store the load configuration into the flash
New settings will be applied at next device restart.

**Method ID: 0x0002**

a) **REQUEST:** Payload of this message is the configuration file as HEX stream.

   ![Image](image)

   **Note:** Length field should be adjusted

b) **RESPONSE:** This method returns a SOME/IP Message with Return Code 0x00 (OK)
Export Config

Same behavior as Export button from Webpage. Response message from MediaGateway will contain the CFG file in its payload as HEX stream.

Method ID: 0x0003

a) REQUEST: Method ID has to be set to 0x0003. No payload needed.

b) RESPONSE: This method returns a SOME/IP Message with Return Code 0x00 (OK)

```plaintext
Internet Protocol Version 4, Src: 192.168.0.49 (192.168.0.40), Dst: 192.168.0.150
SOME/IP Protocol, Service ID: 0x0124, Method ID: 0x0003, Session ID: 0x0000, Service ID: 0x0124 (DebugServiceMediaSwitch)
Method ID: 0x0003
Payload: 0x0000
```

Note: Payload of this message is the configuration file as HEX stream.

Dynamic Config

It is useful for automation of tests which different configurations are needed.
This method loads a configuration and applies it with “fast restart”. No complete reset is needed.
When Dynamic Configuration is applied and running, Host LED will blink faster as in normal operation.
This Dynamic Configuration will run until next device restart or new load dynamic configuration.

Note: At a device restart, current configuration stored in flash will be applied.

Method ID: 0x0004

a) REQUEST: Same as Import Configuration Method. Method ID has to be set to 0x0004

b) RESPONSE: Same as Import Configuration Method.
Check Status
This method will response with the current status of the device. Current status can be:

Normal Mode: When current configuration is loaded from flash.
Dynamic Mode: When current configuration is loaded dynamically. In dynamic mode, Host LED will blink a little faster.

Method ID: 0x0005

a) RESPONSE: This method returns a SOME/IP Message with Return Code 0x00 (OK). The response payload will contain: Normal Operation or Dynamic Operation

<table>
<thead>
<tr>
<th>Payload</th>
<th>Byte[0]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>0x01</td>
</tr>
<tr>
<td>Info</td>
<td>Normal</td>
</tr>
</tbody>
</table>

Set WakeUp Line Status
This method provide users the possibility of driving the wakeup line to high or low level. Two wake up lines are available in the MediaGateway

Method ID: 0x0006

a) REQUEST: Method ID has to be set to 0x0006. Payload will have to contain the pair values {wakeup line, line status}
If user want to set WakeUp Lines to High, the payload should contain these two bytes:

<table>
<thead>
<tr>
<th>Payload</th>
<th>Byte 0 (line select)</th>
<th>Byte 1 (line new status)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>0x01</td>
<td>0x00</td>
</tr>
<tr>
<td>Info</td>
<td>WakeUp Line 1 or 2</td>
<td>Low or High</td>
</tr>
</tbody>
</table>

b) RESPONSE: This method returns a SOME/IP Message with Return Code 0x00 (OK) if values passed are correct. Otherwise it will return Code 0x01 (NOT_OK)

Get WakeUp Line Status
This method returns the state of the selected wake up line.

Method ID: 0x0007

a) REQUEST: Method ID has to be set to 0x0007. **No payload needed.**

b) RESPONSE: This method returns a SOME/IP Message with Return Code 0x00 (OK) and its payload will contain the current status of both WakeUp Lines

<table>
<thead>
<tr>
<th>Payload</th>
<th>Byte[0] (Status Line 1)</th>
<th>Byte[1] (Status Line 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>0x00</td>
<td>0x00</td>
</tr>
<tr>
<td>Info</td>
<td>Low or High</td>
<td>Low or High</td>
</tr>
</tbody>
</table>
Port Enable (OABR)
It allows the user to enable or disable selected BroadR-Reach ports.

Method ID: 0x0008

a) REQUEST: Method ID has to be set to 0x0008. First byte will select the desired port. Valid range is 0 to 11. (0x00 to 0x0B in hexadecimal)

<table>
<thead>
<tr>
<th>Payload</th>
<th>Byte[0]</th>
<th>Byte[1]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>0x00 to 0x0B</td>
<td>0x00 or 0x01</td>
</tr>
<tr>
<td>Info</td>
<td>BR Port select</td>
<td>Disable</td>
</tr>
</tbody>
</table>

b) RESPONSE: This method returns a SOME/IP Message with Return Code 0x00 (OK)

Port Master/Slave (OABR)
It allows the user to set selected BroadR-Reach ports in Master or Slave Mode. This method it is useful in cases where user does not know which mode is using the DUT (Device under Test)

Method ID: 0x0009

a) REQUEST: Method ID has to be set to 0x0009. First byte selects the desired port. Valid range is 0 to 11. (0x00 to 0x0B in hexadecimal) Second byte refers to new OABR mode for selected port. Slave or Master.

<table>
<thead>
<tr>
<th>Payload</th>
<th>Byte[0]</th>
<th>Byte[1]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>0x00 to 0x0B</td>
<td>0x00 or 0x01</td>
</tr>
<tr>
<td>Info</td>
<td>BR Port select</td>
<td>0x00</td>
</tr>
<tr>
<td></td>
<td>Slave</td>
<td>Master</td>
</tr>
</tbody>
</table>

b) RESPONSE: This method returns a SOME/IP Message with Return Code 0x00 (OK)

Reset to default
It performs a reset configuration to default values and device restarts.

Method ID: 0x0010

a) REQUEST: Method ID has to be set to 0x0010. No payload needed.

b) RESPONSE: This method returns a SOME/IP Message with Return Code 0x00 (OK) before restarting.
Get System Information

This method returns device information and its active licenses.

Method ID: 0x0011

a) **REQUEST:** Method ID must be set to 0x0011. **No payload needed.**

c) **RESPONSE:** This method returns a SOME/IP Message with Return Code 0x00 (OK) and its payload will contain the following parameters

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>0x02</td>
<td>0x06</td>
<td>0x040262</td>
<td>0x00</td>
<td>0x01</td>
<td>0x00</td>
</tr>
<tr>
<td>Info</td>
<td>HW version high</td>
<td>HW version low</td>
<td>SW version</td>
<td>Basic BMW</td>
<td>CAN</td>
<td>FlexRay</td>
</tr>
</tbody>
</table>

The response is showed above, is showing the information shown on System Information Page

- **Hardware version:** Media Gateway 2.6
- **Application Software version:** 4.2.08
- **Bootloader version:** 3.3.0
- **Repository ID:** 5575c07
- **BMW Extra Functions:** Disabled
- **CAN Gateway Function:** Unlock
- **FlexRay Gateway Function:** Disabled
11. Hardware Variants

Different versions of the MediaGateway have been built. Here some information about hardware variants. The HW version is stated on the label on the bottom of the case.

**BroadR-Reach Analog Filter:**
All filter versions are compatible with each other.

Hardware Version 2.0 and above have the following filter for all BroadR-Reach ports:

L32 and L35 are placement options.
In Version 2.0 and 2.1 the CMC L32 is not fixed.
In Version 2.2 and above the CMC L35 is not fixed.

**Debug connector**
There is a debug connector on the Tyco Connector side of the case. This small connector is only for customer service purpose.

⚠️ **Warning:** Do not connect anything to this port.
Startup Time

The startup time on the device has been greatly reduced in firmware version 3.7. It is dependent of the used hardware version.

MediaSwitch (all Versions), MediaGateway Version up to 2.1:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PowerUp and Processor Boot time:</strong></td>
<td>65 ms</td>
</tr>
<tr>
<td><strong>Configuration time depending on complexity:</strong></td>
<td>173 ms</td>
</tr>
<tr>
<td><strong>BroadR-Reach LinkUp time:</strong></td>
<td>20-130 ms</td>
</tr>
</tbody>
</table>

MediaGateway Version since 2.1a:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>PowerUp and Processor Boot time:</strong></td>
<td>65 ms</td>
</tr>
<tr>
<td><strong>Configuration time depending on complexity:</strong></td>
<td>47-55 ms</td>
</tr>
<tr>
<td><strong>BroadR-Reach LinkUp time:</strong></td>
<td>20-130 ms</td>
</tr>
</tbody>
</table>

ี้ **Note:** On the RJ45 gigabit ports the Linkup time is about 3 to 4 seconds. This is because of IEEE Auto Negotiation which must be done in gigabit mode.
12. Application Firmware Update

You can download the latest firmware and documentation for the MediaGateway here:
http://www.technica-engineering.de/MediaGateway

The application firmware of the device may be updated by the following process:

⚠️ **Warning:** Never downgrade the bootloader or application to a former version. This could cause serious problems.

⚠️ **Note:** If you update the application the bootloader should also be updated to the latest version.

⚠️ **Warning:** Not following this instruction may cause erroneous states of the device. You will have to send it back to Technica Engineering for repair. Technica Engineering may charge support fees for this service.

⚠️ **Warning:** Only upgrade to the latest firmware. Do not downgrade to old releases. Otherwise it may happen that you cannot access the device anymore because old firmware does not support new hardware.

⚠️ **Note:** You need to have administration privileges on a Windows PC to be able to do the firmware update on the MediaGateway.

1. Power up the device by a stable 12 Volt DC power supply. Do **not** switch off the powersupply during the update process.

2. It is recommended to connect the Wake-up line (Pin 8 of the black MQS connector) to 12 Volt of the same power supply to make sure the ECU is awake during update.

3. Connect a Windows PC with a RJ45 cable directly to the left RJ45 Port of the MediaGateway and make sure there is a link. Do not connect a switch in between.

4. Disconnect all other Ethernet, CAN, FlexRay, LIN and BroadR-Reach links from the MediaGateway.

5. **Disable the Firewall** of the Windows PC. Set the network device of the PC to the same subnet as the MediaGateway. (For example 192.168.0.100 and 255.255.0.0)

6. Check that your firmware package you received from Technica Engineering contains the following files:
   - redtool.exe
   - EthernetSwitch.crc.srec

   You will need to have java installed on your PC.

7. Check that the “Host” LED toggles slowly (so the device is running in application mode).

8. Check that you can access the website at 192.168.0.49 (or whatever the IP address of the MediaGateway is).
9. Open a DOS-Box and execute the following command to enter bootloader mode:

```
redtool.exe -t 192.168.0.49 -e
```

Option –t specifies the IP Address of the MediaGateway. Option –e restarts the MediaGateway and starts it in bootloader mode.

Note: The Host LED is blinking fast when in bootloader mode.

10. In the DOS-Box execute the following command:

```
redtool.exe -t 192.168.0.49 -f EthernetSwitch.crc.srec -r
```

Option –t specifies the IP Address of the MediaGateway. Option –f specifies the new firmware file. Option –r activates the application mode after successful update.

Note: during the update process the Host LED will stop to blink. This is a normal condition. Do not reset the device! The update process will last about one minute. When the update is finished the Host LED will toggle slowly again.

11. You can re-activate your Windows firewall after successful update.
13. Frequently Asked Questions – FAQ

Q: **What is the delay time for Ethernet packets through the switch?**
A: The propagation delay of the switch depends on the load. The switch works collision free. So buffers are used to solve collisions. These buffers delay packets for some time and cause delay jitter. On high load these times rise exponential. On normal load the delay should be about 0.3 ms. But if the packed passes all 3 switches it may sum up to about 1 ms.

Q: **Is AVB supported?**
A: Currently Audio Video Bridging is not supported. Only automotive 802.1AS time synchronization protocol is implement.

Q: **What to do to get CAN, FlexRay and LIN supported?**
A: In the standard firmware edition these interfaces are not supported. Please contact the sales of Technica Engineering GmbH to get information about advanced software features.

Q: **When I use the MediaGateway in my test setup, I cannot access the configuration website anymore.**
A: The host microcontroller is jammed by mislead packets. Please use a valid VLAN configuration and avoid too much broadcast packets.

Q: **After a firmware update the host LED is still blinking fast. What to do?**
A: The firmware update failed, and the host is still in bootloader mode. Please restart the device and try to update the application again as described in this manual.

Q: **All LEDs on the front of the MediaGateway are lit permanently?**
A: The host microcontroller is not running. Maybe a firmware update has failed. Please send the device to Technica Engineering GmbH for service.

Q: **I have problems with the website user interface.**
A: The website is tested with Firefox and Internet Explorer. Firefox is preferred. Chrome is not supported.

Q: **I have problems with firmware update. TFTP Timeout error is appearing.**
A: It is known that some Ethernet-USB adapters are having problems with Update procedure. Try to connect your MediaGateway directly ton your integrated LAN Adapter.
14. **Contact**

![Technica Engineering Logo]

In the „Contact Tab“ information is displayed how to contact us if you need service.

If you have any questions regarding this product please or you want to obtain a new license, you can contact us at:

**Technica Engineering GmbH**  
LeopoldStr 236  
80807 München Germany  

Fax: +49-89-34290265  
info@technica-engineering.de  
www.technica-engineering.de