NAT-MCH
Ethernet Switch
Configuration Manual
Last Changed FW v2.21.1
Revision v29

The NAT-MCH has been designed by:

N.A.T. GmbH
Konrad-Zuse Platz 9
D-53227 Bonn
Phone: +49 / 228 / 965 864 - 0
Fax: +49 / 228 / 965 864 - 10

Internet: http://www.nateurope.com

Disclaimer

The following documentation, compiled by N.A.T. GmbH (henceforth called N.A.T.), represents the current status of the product's development. The documentation is updated on a regular basis. Any changes which might ensue, including those necessitated by updated specifications, are considered in the latest version of this documentation. N.A.T. is under no obligation to notify any person, organization, or institution of such changes or to make these changes public in any other way.

We must caution you, that this publication could include technical inaccuracies or typographical errors.

N.A.T. offers no warranty, either expressed or implied, for the contents of this documentation or for the product described therein, including but not limited to the warranties of merchantability or the fitness of the product for any specific purpose.

In no event, will N.A.T. be liable for any loss of data or for errors in data utilization or processing resulting from the use of this product or the documentation. In particular, N.A.T. will not be responsible for any direct or indirect damages (including lost profits, lost savings, delays or interruptions in the flow of business activities, including but not limited to, special, incidental, consequential, or other similar damages) arising out of the use of or inability to use this product or the associated documentation, even if N.A.T. or any authorized N.A.T. representative has been advised of the possibility of such damages.

The use of registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations (patent laws, trademark laws, etc.) and therefore free for general use. In no case does N.A.T. guarantee that the information given in this documentation is free of such third-party rights.

This product (and the associated documentation) is governed by the N.A.T. General Conditions, Terms of Delivery and Payment.

Table of Contents

List of Figures

List of Tables

Glossary

µTCA	Micro TCA (= MTCA)
AMC	Advanced Mezzanine Card
ATCA	Advanced Telecom Computing Architecture
BPDU	Bridge Protocol Data Unit
EAPOL	Extensible Authentication Protocol over LAN
I2C	Inter Integrated Circuit, 2 wire serial bus
KCS	Keyboard Controller Style
LAG	Link Aggregation Group
LAG-Master	Port within an aggregation group defined settings for all port of the group
LAN	Local Area Network
LED ID	Light Emitting Diode Identifier
LUN	Logical Unit Number
MAC	Media Access Control address
MCH	µTCA Carrier Hub
NMCH	NAT-MCH
OEM	Original Equipment Manufacturer
Operable Switch	At the current time configurable switch device
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Abbreviations of setting options

AGE TIME	Aging Interval of the MAC-Table
ALIAS	aliases of AMC-Port or additional connection
AMC_PM	Port map of the AMC slots
AUX_PM	Port map of unused ports
BLK_NM	Block Not Mirror packets mode [FLAG]
BRG_PRI	Bridge priority related Spanning Tree Protocol
CPU_1	CPU Port 1 (on the baseboard) (*Table 3-1*)
CPU_PM	Port map of the CPU ports
FLAG	binary value [0|1]
FRT_PM	Port map of the Front panel connections
FRT_1	First front 1GbE uplink port (*Table 3-1*)
FRT_2	Second front 1GbE uplink port (*Table 3-1*)
FRT_3	Third front 1GbE uplink port (*Table 3-1*)
FRT_4	Fourth front 1GbE uplink port (*Table 3-1*)
FWD_DELAY	Forwarding delay: time that is spent in the listening and learning state
GR_MEM_IN	Group Membership Interval of IGMP-Snooping mode in seconds
HELLO_T	Hello Time is a time between each bridge BPDU that is sent on a port
JMB_SIZE	Frame size of Jumbo Ethernet frames
INST_N	RSTP instance ID {INST_0 | INST_1}
ISW_BX	Switch port of the baseboard connected to the XAUI Hub (*Table 3-1*)
ISW_XB	Switch port of the XAUI Hub connected to the baseboard (*Table 3-1*)
ISW_PM	Port map of Inter-Switch connection
LAG_GR	Membership of an aggregation group to provide the Link Aggregation mode

LAG_HM	Hashing Mode of the Link Aggregation
LAG_PM	Propagation Mode of the Link Aggregation [0] –"*Link is Existing*" mode [1] – "*Link has Full Width*" mode
LIST_OF_ALIASES	List of aliases: used AMC-Port and additional connection aliases
MAC_ADDR	MAC Address
MAX_AGE	Max Age maximal time that passes before a bridge port set the info
NON_STP_PORT	FLAG for excluding of a port from the STP mathematic calculation
PONT2POINT	port is connected to a shared LAN or a point-to-point LAN segment
IFF_MODE	Interface mode {SerDes/SGMII/AUTO}
PORT_CPT	Capture port [all used ports]
PORT_NO	Number of port [all used ports]
PORT_PRI	Port priority [0 .. 240] in steps of 16, related RSTP
PORT_PTH_COST	Port path coast [1..200 000 000] or [0]
PRI_1P	802.1p priority [0-7]
PRI_MTAB	priority contained at the MAC-Address table [0-7]
QEUR_IN	Query Interval of IGMP Snooping mode in seconds
SRC_CON	Alias of Source Connection [all used ports]
PM_CON	Propagation Master Connection/Port [all used ports]
TX_QUEUE	Transmit queue [0-4]
UPC_PM	Port map of the Update channels
VLANID	Virtual LAN ID [1-4096]
UPDC_B	Update Channel between 1GbE switches on Base Boards (*Table 3-1*)
UPDC_X	Update Channel between 10GbE switches on XAUI Boards (*Table 3-1*)

1 Introduction

The NAT-MCH is a MicroTCA (µTCA/MTCA) Carrier Hub in the form factor of a single width and single or double height Advanced Mezzanine Card (AMC). It provides the central management and data switching entity for all MicroTCA systems. The NAT-MCH comprises of a base module and numerous optional daughter cards, which can be mounted on the base module. The NAT-MCH is MicroTCA.0 R1.0 compliant and delivers switching and hub functionality for the various system fabrics as defined in the AMC.x standard series, i.e. 1 Gigabit Ethernet, PCI-Express (PCIe), Serial Rapid I/O (SRIO), 10 Gigabit Ethernet (XAUI) or Serial Attached SCSI (SAS). The NAT-MCH can also provide a centralized clock distribution to all AMCs in the system.

2 NAT-MCH Switches

The Gigabit Ethernet option of the NAT-MCH is realized by a Broadcom BCM5396 Ethernet switch, the 10 Gigabit Ethernet option by a Fulcrum FM222X Ethernet switch. These Ethernet switches provide a layer 2, non-blocking, low-latency 1 Gigabit and 10 Gigabit Ethernet packet transfer. They support Port Based VLAN, VLAN 802.1Q protocol, MAC-Security function, Quality of Service 802.1p protocol, Control of Link Status as well as a Port Mirroring control, Jumbo Frame and Link Aggregation mode.

While the 1GbE switch is located on the Base Board of the NAT-MCH the 10 GbE switch is located on an optional extension hub module that can be plugged on the NAT-MCH base. The switches can be connected with each other by a so-called *Inter-Switch Connection,* depending on PCB version.

The 1GbE switch on the baseboard may have one or two Uplinks.

3 Port Switching Concept

The port management in the MicroTCA Systems runs in several steps, controlled by software. This chapter describes the process flow of the port management from physical ports to the AMC-Ports in all details.

3.1 Fabrics and physical Ports

The MicroTCA backplane provides the connectivity among AMCs. The specification defines one to seven *fabric* interfaces per MCH for every AMC. Each fabric consists of the 12 lanes that can be used for different connection types. For example, one lane can provide 1GBE connectivity; four lanes (Fat Pipe) can serve one 10GbE Port of the switch.

The NAT-MCH uses the fabric A1 to A12 for 12x1GbE- and Fat Pipe (four lanes) D1-G1 to D12-G12 for 12x10GbE connections.

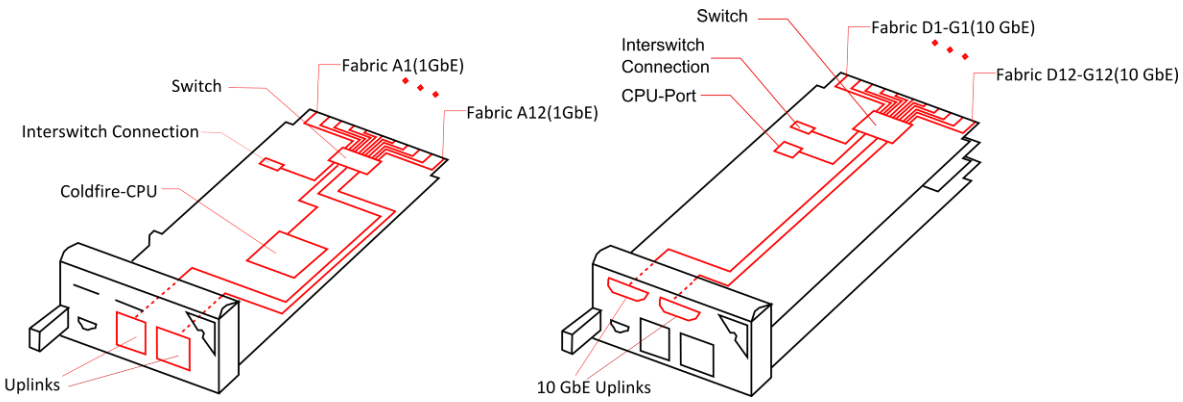


Figure 3-1: NAT-MCH Base V3.x with and without XAUI Hub-Module (simplified)

The BCM5396 supports up to 17x1GbE and the FM222X/FM4000 supports 24x10GbE ports, but depending on the hardware version of the NAT-MCH, not all of these ports might be used: the mapping between physical port of the switch device and fabrics of the NAT-MCH depends on the PCB version. To be independent of the physical port, the firmware provides different mappings of connections for different PCB versions. The mapping process is transparent to the user, to simplify the management of the NAT-MCH.

3.2 AMC Ports and Backplane Interconnect

The specification denotes the ports available at the AMC as AMC-Port [0:20]. The AMC-Ports <0>, <1>, <4>-<11> can be used for the Ethernet connections.

The MicroTCA backplane provides the routing between the MCH fabric and AMC-Port. The backplane routing is variable but defined by the manufacturer at production time. The routing information is stored in the Carrier Point-to-Point Connectivity records that are part of the FRU-Backplane info saved in the backplane EEPROM. To manage Ethernet traffic correctly, the MCH reads the connectivity records at boot time.

The user interface of the NAT-MCH is AMC-Port related. The firmware interprets FRU Info, and then maps the AMC-Ports to the fabrics of the NAT-MCH depending on the p2p records. Therefore, the AMC-Ports are mapped in two following steps:

1. AMC-Port to fabric Lane(s) (depends on p2p record)
2. MCH Fabric to physical port of the switch (depends on PCB version)

NOTE: If the p2p record routes the AMC-Port to the fabric lane(s) that are not supported by the MCH PCB version, the AMC-Port will not be offered to the user in the settings.

3.3 Identifier of AMC Port and Additional Connections

The NAT-MCH orders the notation of the AMC-Ports. The notation contains the connection type, slot number and occupied AMC-Ports:

AMC Slot / AMC-Port(s)

For example, the AMC is in slot <3>; the board is connected with the MCH due the port <0> (1GbE, e.g. fabric A3) and <4>-<7> (10GbE, e.g. fabric D3-G3). Therefore, the port name looks as follows: <AMC3/0> for 1GbE und <AMC3/4-7> for the 10GbE connection.

The NAT-MCH has additional connections that are not part of the fabrics. These are:

- Update channel attached to the second NAT-MCH in redundant environments;
- Connection between the 1GbE- and the 10GbE switch;
- Uplink ports at the front panel of the NAT-MCH that allow interconnecting the system over 1GbE or 10GbE ports to other carriers or to other systems.

These connections are offered in the user settings as well.

The notation of the additional connections contains the connection type and the number (numerical or literal):

Type _ index

Connection Notation	Description	Switch	Port usage on		
			Base Board ≤ V2.1 < V3.0	Base Board ≥ V3.0	XAUI Board V1.2
<FRT_1>	Uplink port **1** at the **fr**on**t** panel	1GbE	used	used	unused
<FRT_2>	Uplink port **2** at the **fr**on**t** panel	1GbE	reserved	optional	unused
<FRT_3>	Uplink port **3** at the **fr**on**t** panel	10 GbE	reserved	unused	optional
<FRT_4>	Uplink port **4** at the **fr**on**t** panel	10GbE	reserved	unused	optional
<UPDC_B>	**Upd**ate **C**hannel between 1GbE switches on **B**ase Boards	1GbE	used	used	reserved
<UPDC_X>	**Upd**ate **C**hannel between 10GbE switches on **X**AUI Boards	10 GbE	unused	unused	used
<ISW_BX>	**I**nter **S**witch **C**onnection from the **B**ase- to the **X**AUI board	1GbE	reserved	used	unused
<ISW_XB>	**I**nter **S**witch **C**onnection from the **X**AUI- to the **B**ase board	10 GbE	unused	unused	used
<CPU_1>	CPU Port 1 (on the base board)	1 GbE	used	used	unused

Table 3-1: NAT-MCH – Additional connections and usage

Table 3-1 indicates additional connections, which are currently used depending on the hardware version of the NAT-MCH Base board and of the NAT-MCH XAUI board.

To avoid entering the port alias string in the console based switch configuration menus also a number has been assigned to each port, which has to be used as "ID" in the configuration menus.

3.4 Configuration Interfaces

Three interfaces can be used to configure the Ethernet switches on the NAT-MCH. The first one is the text based Command Line Interface (CLI) which can either be used via a serial connection at the MCH debug port (DBG) or via a Telnet connection to the board. Furthermore, the switch can be configured via a web-interface, which can be accessed via a standard web-browser. Finally, the switch can be configured via a text based configuration file, which can be edited by the user with a standard text editor on a PC.

3.5 Command Line Interface (CLI)

In order to access the CLI, a VT100 type terminal (19200, 8N1) has to be connected via console cable to the DBG port of the NAT-MCH. For details, please refer to the NAT-MCH User's Manual.

Detailed information about the commands, which need to be entered at the console prompt to call the protocol specific configuration menu, is given in the protocol or feature specific chapters below.

To exit from any menu or any subsequent submenu always press <q>. For help press <h> or <?> or type <help>.

3.6 Web-Interface

The NAT-MCH has an integrated embedded web server, which allows users to view and change configuration parameters of the NAT-MCH.

Before the web server can be used, it has to be enabled via the command line interface. Please refer to the NAT-MCH User's Manual for details. The onboard web server can be accessed with any standard web-browser by entering the IP-address of the NAT-MCH into the browser's address line.

Information about the different configuration web pages can be found in the protocol specific chapters below.

3.7 Text Based Switch Configuration

A text-based configuration file can be used to configure the protocols and features of the Ethernet switch on the NAT-MCH. A set of configuration items has been defined which could be used to set the protocol or feature specific parameters. A general description of these items follows in the next chapters, the protocol or feature specific items and their parameters are explained in the associated chapters below.

To backup the current Ethernet switch settings of a NAT-MCH a text-based configuration file can be generated and downloaded via one of the configuration interfaces. This file then can be adapted with a standard text editor and uploaded again to the NAT-MCH. By this, the configuration of one NAT-MCH can also be "cloned" to other NAT-MCHs.

3.7.1 Text Based Configuration Structure

The text-based configuration is line-oriented; each text line contains exactly one item of the switch configuration. The order of the configuration items in the switch configuration file is irrelevant; however, it is recommended to leave the order unchanged to simplify a review of the configuration file.

Each configuration line starts with the configuration item ID followed by one or more parameters. The configuration item ID and the parameters are separated by a '=' character, the parameters are separated by commas.

For example:

```
eth_802.1q_dflt =    AMC10/0,    100,  5
```

Comments can be added to the configuration by writing a '#' character at the beginning of the line. These lines will be ignored by the software when parsing the configuration file.

Example: `# this is a comment`

The almost all features of the Ethernet switch can be enabled or disabled on user demand by initialization flag item. This is a Boolean value and it can be <0> or <1>. If the initialization flag item of a feature is not set, all other configuration items related to this feature will be ignored and the feature will be disabled. If a configuration item or one of its parameters is not preset, the switch configuration uses default values as specified in the chapters below.

3.7.2 Parameter Data Types

There are three types of the numerical data representation than are used for the parameters in the configuration items:

Type	Prefix	Example	Decimal value
Binary	0b	0b0110	6
Hexadecimal	0x	0xFF	255
Decimal	none	15	15

Table 3-2 : Numerical data representation in the text based switch configuration

4 Device Location of the NAT-MCH

All configurable devices of the NAT-MCH are spread over different mezzanines. The exact position of a device is the so-called *device location*, which consists of three components:

- MCH-ID: reserved for future usage; currently is fixed to '0'
- Mezzanine level: distinguishes the NAT-MCH mezzanine boards; refer to Figure 4-1
- Instance ID: defines the device on the particular mezzanine board

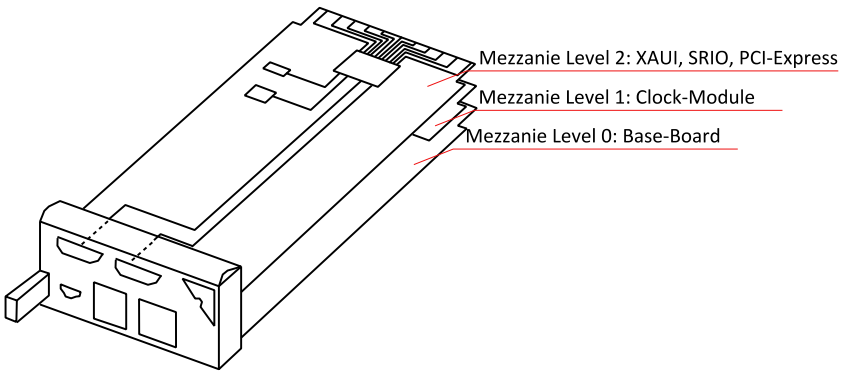


Figure 4-1: NAT_MCH with a Hub-Module

Therefore, the device location is a unique identifier of each configurable device within the NAT-MCH that is used for reference, control and configuration.

4.1 Changing the Switch Device

The Ethernet switches on the NAT-MCH are identified via the device location parameters as described in chapter 4. The user can configure only one of the switches at a time; the currently selected switch is called the *operable switch*. The selection of the operable switch occurs via the CLI and the web interface.

4.1.1 CLI Based Configuration

It is possible to view and change the operable switch device by command line interface.

4.1.1.1 *Menu item: Get Device Location*

This menu item shows the actual switch device:

```
Mezzanine: ........ 2
Instance ID: ...... 0
```

4.1.1.2 *Menu Item: Change Device Location*

This menu item provides a selecting of an operable switch. The information about all initialized switches appears in the console:

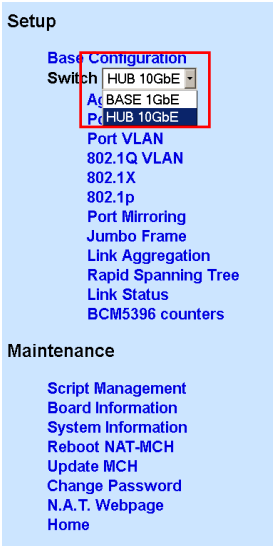
```
ID [1]
Driver: . BCM5396 1Gb(1)
Mezzanine: ........ 0
Instance ID: ...... 0

ID [2]
Driver: . FM222X 10Gb(2)
Mezzanine: ........ 2
Instance ID: ...... 0
```

Please, enter an appropriated ID number to select an operable switch.

4.1.2 Web Based Configuration

The web interface allows the selecting of operable switch via the drop down menu appears on the left of the web browser window:



The current menu item shows the operable switch. To change the operable switch a switch device from the drop down menu has to be selected. The browser refreshes its content automatically afterwards.

Note: please, **refresh** the browser content after power cycling or resetting the NAT-MCH to get the current operable switch and configuration parameters.

4.1.3 Text Based Configuration

All configurable devices on the NAT-MCH can be set up by the Text Based Configuration as well. As described in Chapter 4, three configuration items are required:

- `mch_id` defines MCH
- `mez_id` defines mezzanine level
- `ins_id` defines instance ID

The device location is valid if the configuration items stay sequentially in the order of their arrival. Thereafter, it will be checked, if the device has been initialized for this device location. If the device is referenced correctly, the according configuration part will be parsed and applied. If the device location is not related to Switch Management the searching for the next related device location is to be continued.

5 Default Switch Configuration

This chapter describes the default switch configuration of the NAT-MCH in redundant and non-redundant environments. The Ethernet switch uses a default configuration if the corresponding flag in the MCH-Configuration has not been set.

5.1 Risk of Loops

The NAT-MCH can be operated with up to two Ethernet switches (1-GbE on Base board and 10-GbE on XAUI module). This causes a certain risk of loops in the network attached to the MicroTCA system. Constellations, which can result in network loops, are described in the following sub-chapters.

5.1.1 Loop due to Uplinks

This case needs to be considered with PCBv3.4 (Base) and later or/and XAUI-Hub-Module with Uplink option only: both uplinks at the front panel have been connected with the external switch or hub, as it shown at the next figure:

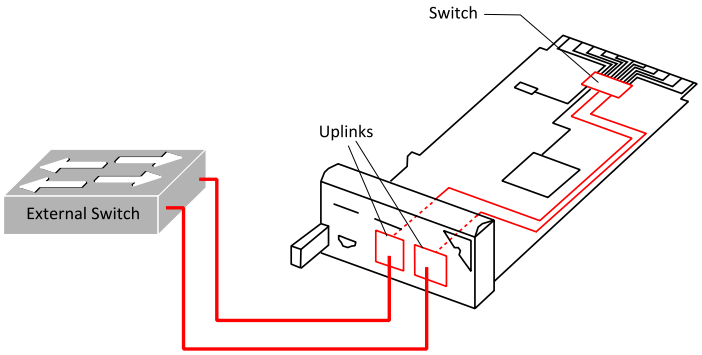


Figure 5-1: Loop due to both uplinks

The Ethernet switch of the Baseboard builds up the loop with the external switch.

5.1.2 Loop due to Update Channel

This case is possible in redundant environment only. The uplinks of different NAT-MCHs are connected with the external switch.

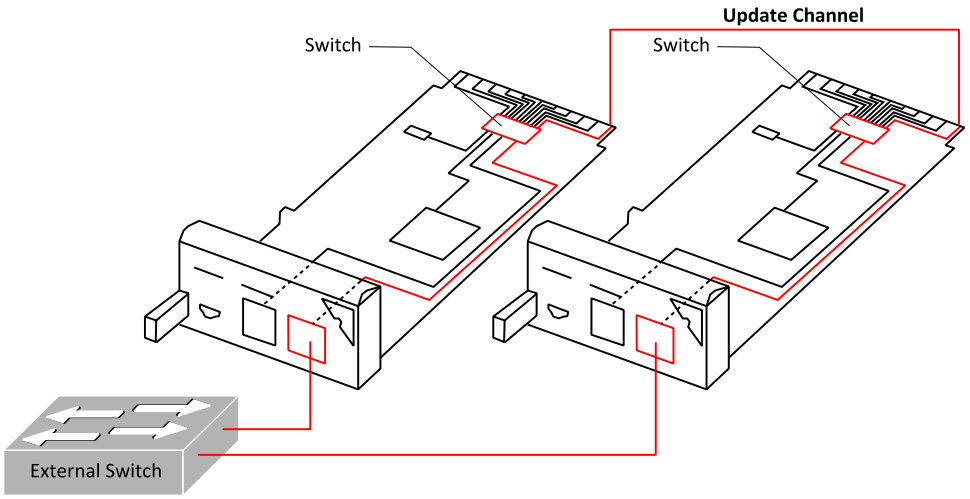


Figure 5-2: Loop due to update channel

The loop accrues via the uplink of one MCH, over the Update Channel and the uplink of a second MCH.

5.1.3 Loop due to Inter-Switch Connection

The loop can be build due to the Inter-Switch connection between MCH Base with 10GbE Hub and external switch over 1-GbE and 10-GbE uplinks:

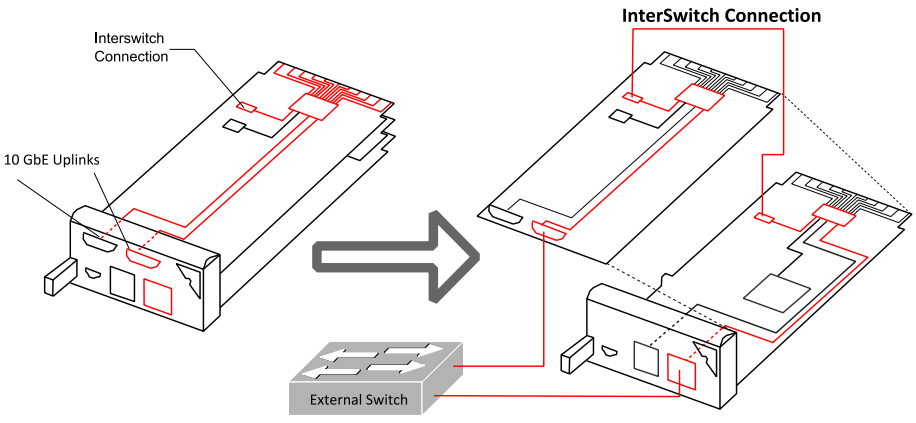


Figure 5-3: Loop due to Inter-Switch connection

The 1-GbEs and 10-GbE switch make the ring connection with the external switch over Ethernet network.

5.2 Loop Avoiding

The default switch configuration serves to avoid the loop in the Ethernet network, if no "Port Enable/Disable" configuration has been loaded.

The case "*Loop due to Uplinks*" can occur in redundant and non-redundant environment. In non-redundant environment, disabling the second uplink port on the switch resolves the loop.

In redundant environments, both front uplink ports of the secondary MCH need to be disabled. If the secondary MCH has a XAUI Hub, all uplinks of this module will be disabled as well.

For resolving a "*Loop due to Inter-Switch Connection*", the Inter-Switch connection is disabled on the 1GbE-Switch.

In reply to summarize the above post, the following ports are disabled by default.

- Primary MCH - `FRT_2, FRT_4, ISW_BX`
- Secondary MCH - `FRT_1, FRT_2, FRT_3, FRT_4, ISW_BX`

5.3 Load User Configurations at System Start

The Ethernet switches of the NAT-MCH support several protocols and features that are described in *Chapter* 6.

The default switch configuration uses only basic switch functionality. If extended or full functionality is needed, particular features need to be activated and set up by the user. After the switch configuration is completed, it has to be saved. The backup process is described in C*hapter* 7.

To load the switch configuration from FLASH memory at system start, the according flag in the MCH configuration should be set. In section "*GbE switch parameter*" the "*configuration source*" is set to `<no configuration> by default`. This flag can be changed in the CLI or web interface of the NAT-MCH.

5.3.1 CLI – load User Configuration at System Start

To set the option in the CLI, enter <mchcfg>:

```
nat> mchcfg
MCH CFG: configuration modes
   [ 0] no action
   [ 1] print complete configuration
   [ 2] reset to defaults
   [ 3] modify MCH global configuration
   [ 4] modify ShM configuration
   [ 5] modify CM configuration
   [ 6] modify SEL configuration
   [ 7] modify GbE switch configuration
   [ 8] modify CLK module configuration
   [10] modify NTP configuration
   [11] modify DHCP configuration
   [ ?] print menu
   [ h] print menu
   [ q] quit and save configuration
```

Choose <7> for <modify GbE switch configuration>:

```
Enter configuration mode (RET=0/0x0): 7
GbE switch parameter:
---------------------
 GbE configuration source:             no configuration

GbE configuration source:
  no configuration:         0
  load from FLASH:          1
```

select 1 to load switch configuration from FLASH.

```
Enter source (RET=0/0x0): 1
```

enter <q> to exit and save MCH-Configuration.

```
Enter configuration mode (RET=0/0x0): q
.......
MCH CFG: configuration updated
```

At the next system start, the NAT-MCH loads the switch configuration from FLASH.

5.3.2 Web Interface – load user configuration at system start

To change MCH configuration via the web interface, select menu item "Base Configuration" in the navigation frame and find <GbE parameter> on the right side.

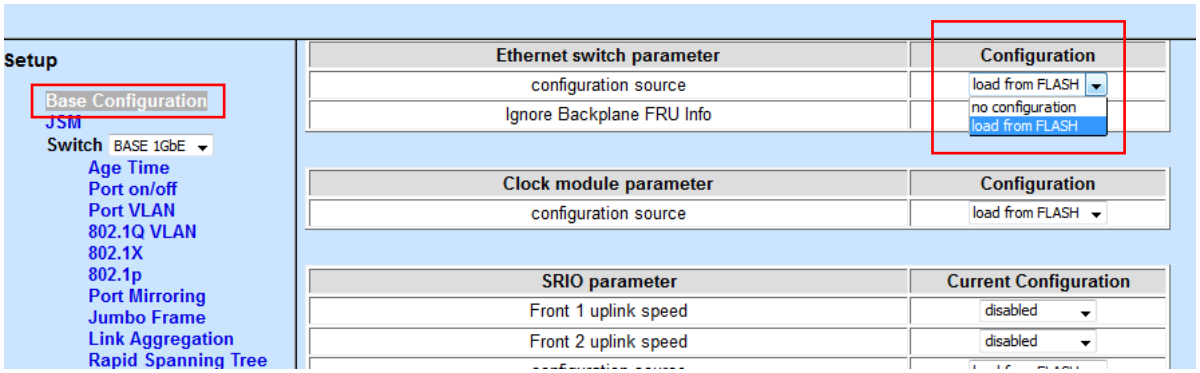


Figure 5-: Change MCH Configuration

Select in the dropdown menu the option <load from FLASH> and confirm the modification with the "Save" button.

At the next system start, the NAT-MCH loads the switch configuration from FLASH.

6 Switch Management

The following chapters describe the switch protocol and feature specific configuration options via the different configuration interfaces. Each chapter contains a short description of the switch protocol or feature followed by a subchapter, which describes the configuration process depending on the used configuration interface.

6.1 Identifier of AMC Port and Additional Connections

6.2 General Settings (Age Time)

This part provides the general settings to control basic functionalities of all NAT-MCH switches. Currently only the Age Time feature is used for this part.

The NAT-MCH switches are configurable for learning the MAC addresses of the packets. The Age Time process periodically removes dynamically learned addresses from the MAC table: the internal switch table is scanned at regular intervals, aging out entries not accessed during previous two aging intervals. The aging intervals are programmable via user interface. Entries that are written via user interface are static; therefore they are not affected by the aging process.

6.2.1 CLI Based Configuration

The `'MAC-Table management'` offers the commands to manipulate the settings related to the MAC table and aging process.

6.2.1.1 *Show Age Time*

This menu item can be used to show the current aging interval of the switch:

```
                AGE TIME
-----------------------------------------
   State: enabled
   Age Time        300 (range [1..1048576])
-----------------------------------------
```

The aging interval is displayed in seconds.

6.2.1.2 *Set Age Time*

This menu item configures an aging interval of table scanning.

```
 AGE TIME
-----------------------------------------
Enter Age time
[0] - disable Age Time functionality
[1..1048576]: Age Time in seconds
```

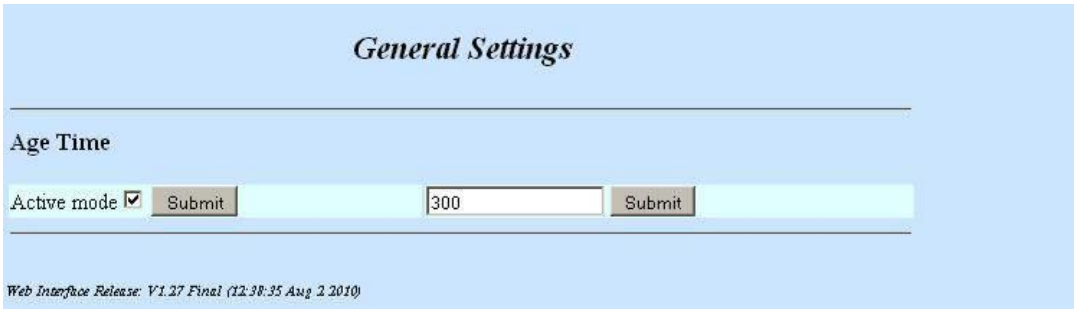
Entering <0> will disable the aging process, any number from <1>-<1048576> sets an aging interval in seconds. To enable the functionality select the <set age time> item again:

```
           AGE TIME
-----------------------------------------
The aging Timeout process is currently disabled!
Possible operation
  [e] - enable Aging Timeout and continue setting
  [x] - quit this menu
```

and confirm it with <e>.

6.2.2 Web Based Configuration

To configure the aging process of the switch select the <General settings> link in the navigation frame of the NAT-MCH website.



Use the <Active mode> checkbox to enable/disable the aging process and the text field to set the aging intervals of table scanning.

6.2.3 Text Based configuration

To configure the Age Time functionality, two configuration items of the text-based configuration have to be used:

```
<eth_mac_ageinit>- Active state of the Age Time functionaly.
<eth_mac_agetime>- Aging interval in seconds.
```

6.2.3.1 *Activate/Deactivate Age Time*

Description:

The <eth_mac_ageinit> configuration item is used to activate/deactivate the aging process. If the configuration item is missing in the configuration file the aging process will be activated by default.

Syntax:

```
eth_mac_ageinit = FLAG;
```

Parameter Description:

The parameters of the <eth_mac_ageinit> configuration item are described in Table 8-16 page 132.

Example:

Activate 802.1Q VLAN mode:

```
eth_mac_ageinit  = 1;
```

The upper configuration item activates the aging process.

6.2.3.2 *Set Aging Interval*

Description:

The <eth_mac_agetime> configuration item determines the aging interval of the table scanning in seconds. If the configuration item is set to "deactivate" or the item is not present at all, other configuration items related with this mode will be ignored.

Syntax:

```
eth_mac_agetime = AGE TIME;
```

Parameter Description:

The parameters of the <eth_mac_agetime > configuration item are described in Table 8-17 page 132.

Example:

Set aging interval parameter:

```
eth_mac_agetime = 30;
```

The upper configuration item sets the aging interval to 30 seconds.

6.3 Enable/Disable Port

This feature is available as a standalone tool since firmware v2.17. It allows the configuring of communication state to *enabled*/*disabled* on particular switch port. The

switch port, which has been set to *disabled*, occurs neither frame transmitting nor frame receiving.

6.3.1 CLI Based Configuration

Please, select submenu `'Port Enable/Disable'` to manipulate the settings of this mode on particular port.

```
[ 0] : no action (unsupported)
[ 1] : show port configuration state
[ 2] : enable/disable port
[ 3] : set default configuration
[ ?] : ?: help
[ h] : h: help
[ q] : q: quit submenu
```

The menu item `<show port configuration state>` show the current state for all switch ports as it follows:

```
|=================================================================|
|                   Enable/Disable State Map                      |
|=================================================================|
|                       AMCs          Front    Up_C   ISw    CPU  |
|                   1  2  3  4  5|     1  2|     B|     B|     1 |
|                   .  .  .  .  .|     .  .|     .|     .|     . |
|-----------------------------------------------------------------|
| AMC        from:  0  0  0  0  0      .  .      .      .      . |
| PORTS        to:  .  .  .  .  .      .  .      .      .      . |
|-----------------------------------------------------------------|
|                   1  1  1  1  1      1  0      1      0      1 |
|=================================================================|
```

To set port mode use the menu item `<enable/disable port>`:

```
Choose Port ID:
 |=================================================================|
 |                   AMCs          Front    Up_C   ISw    CPU  |
 | AMC               1  2  3  4  5|     1  2|     B|     B|     1 |
 | SLOTS             .  .  .  .  .|     .  .|     .|     .|     . |
 |-----------------------------------------------------------------|
 | AMC        from:  0  0  0  0  0      .  .      .      .      . |
 | PORTS        to:  .  .  .  .  .      .  .      .      .      . |
 |-----------------------------------------------------------------|
 |-----------------------------------------------------------------|
 | PORT              0  0  0  0  0      0  0      0      0      1 |
 | ID                1  2  3  4  5      6  7      8      9      0 |
 > (RET=0/0x0):
```

Then enter `<Port ID>` which is to be configured (e.g. `<Port ID>=02` for `AMC2/0` or `<Port ID>=06` for uplink `FRONT1`)

```
[d] - disabled
[e] - enabled
[q] - no change
Enter port state  (RET=e):
```

and finally, select any mode of switch port.

To set default configuration, please use configuration `<set default configuration>`. The default configuration defined to avoid loops described in the chapter *5.1 Risk of Loops.*

6.3.2 Web Based Configuration

To configure a port map select "Port on/off" link in the navigation frame of the NAT-MCH website. In order to enable or to disable a port check or uncheck the checkbox as shown in Figure 6-1.

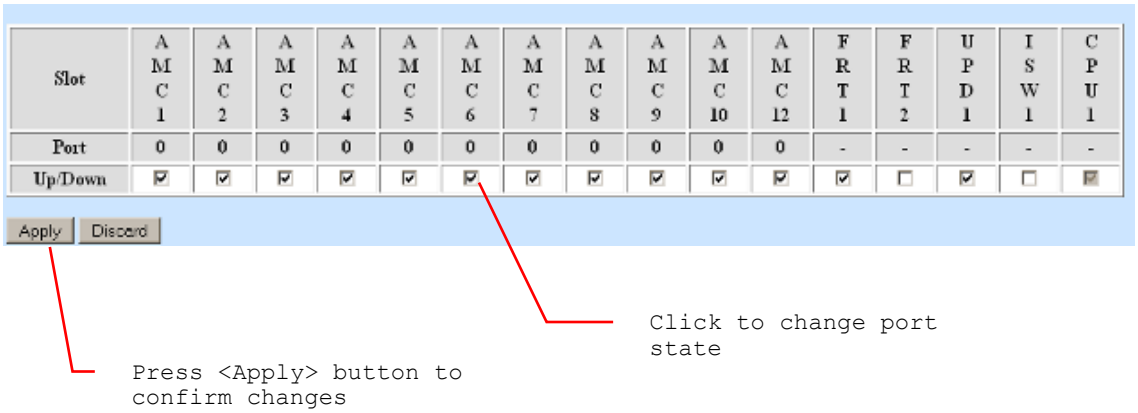


Figure 6-1 : Enable/Disable Port Webpage

6.3.3 Text based Configuration

There are two items to configure enable/disable state of particular switch port:

`<eth_enconn_map>` - main configuration item to configure enable/disable state on particular port.

`<eth_enconn_prim>` - additional configuration item to overrule `<eth_enconn_map>`, if MCH becomes primary role.

Description:

The configuration item `<eth_enconn_map>` is used to specify which connection shall be enabled or disabled. If configuration file does not contain the item, the switch management uses the default configuration.

Syntax:

```
<eth_enconn_map>   =  LIST_OF_ALIASES
```

Parameter Description:

The `eth_enconn_map` configuration item consists of an alias list according to the description in chapter 3.3. The *Table 8-4* describes parameters on *page 125*.

Example:

```
eth_enconn_map   = AMC1/0, AMC2/0, AMC3/0, AMC4/0, AMC5/0, FRT_1, CPU_1
                   LIST_OF_ALIASES
```

The upper example shows that on the current switch the AMC-Ports <AMC1/0>-<AMC5/0> and additional connection, <FRT_1> <CPU_1> are enabled, other connections are disabled.

6.4 Enable/Disable Port on Primary MCH

This feature provides additional setting to "Enable/Disable Port" that is described in previous chapter 6.3. It make available more flexible Ethernet switch configuration in redundant environments. If NAT-MCH becomes primary role, this feature will activated. It overrules setting of "Enable/Disable Port" with previously defined settings.

6.4.1 Text based Configuration

The configuration item `eth_enconn_prim` overrules the setting `eth_enconn_map`, if MCH become primary role.

If configuration file does not contain the item `<eth_enconn_prim>`, the switch management uses item `eth_enconn_prim` to define enable/disable state of a port permanently.

Syntax:

```
<eth_enconn_prim>   =  LIST_OF_ALIASES
```

Parameter Description:

The `eth_enconn_prim` configuration item consists of an alias list according to the description in chapter 3.3. The *Table 8-5* describes parameters on *page 126.*

Example:

```
eth_enconn_prim   = AMC1/0, AMC2/0, AMC3/0, AMC4/0, AMC5/0, FRT_1, CPU_1
                    LIST_OF_ALIASES
```

The upper example shows that on the current switch the AMC-Ports `<AMC1/0>`-`<AMC5/0>` and additional connection, `<FRT_1>` `<CPU_1>` are enabled, other connections are disabled

6.5 Link Propagation

The Link Propagation provides more flexibility to configure Ethernet switch in redundant environments. The feature defines interacting between *propagation master* and *propagation slave*.

The feature propagates a link state of *propagation master* port to "enabled/disabled state" of *propagation slave* port(s). Thus, the functionality lets notify the devices on slave port about link state of master port.

The Link Propagation feature allows usage of a LAG as a *propagation master*. Please take a view on this functionality in the chapter 6.13.3.3 on the page95.

Example:

The front uplink port <FRT_3> of MCH1 is configured as a *propagation master* port. The AMC ports: <AMC1/4-7>, <AMC2/4-7> and <AMC3/4-7> are configured as its *propagation slave*. The set of *propagation master* and its *propagation slave* forms a *propagation chain*.

```
FRT_4-> AMC1/4-7, AMC2/4-7, AMC3/4-7
```

If link state of <FRT_3> is "up", then ports: <AMC1/4-7>, <AMC2/4-7> and <AMC3/4-7> will be set to "enabled". Then AMCs can communicate via <FRT_3>, so long as link of <FRT_3> is up.

If link state of <FRT_3> goes down, then ports: <AMC1/4-7>, <AMC2/4-7> and <AMC3/4-7> will be set to "disabled". Then link states on appropriated ports go to down too. It lets the AMC1, AMC2 and AMC3 know that the communication via <FRT_3> is no more available. In this case, the AMC can make a decision to take another route: e.g. ports <AMC1/8-11>, <AMC2/8-11> and <AMC3/8-11> to communicate via MCH2.

6.5.1 Text based Configuration

The configuration item eth_propag defines a *propagation chain*. It is allowed to define several *propagation chains* on the same device, but the chains may not overlap with each other.

Syntax:

```
<eth_propag>   =  PM_CON, LIST_OF_ALIASES
```

Parameter Description:

The <eth_propag> configuration item consists of an alias list according to the description in chapter 3.3. The *Table 8-6* describes parameters on *page 127*.

Example:

```
eth_propag   = FRT_3,   AMC1/4-7, AMC2/4-7, AMC3/4-7
               PM_CON   LIST_OF_ALIASES

eth_propag   = FRT_4,   AMC4/4-7, AMC5/4-7, AMC6/4-7
               PM_CON   LIST_OF_ALIASES
```

The upper example shows that <FRT_13> is a *propagation master* for <AMC1/4-7>-<AMC2/4-7> and <AMC3/4-7>. The <FRT_14> is a *propagation master* for <AMC4/4-7>-<AMC5/4-7> and <AMC6/4-7>

6.6 Port Based VLAN

Port Based VLAN is used to group certain network stations or networks into Virtual LANs by only allowing the communication between certain switch ports. A Port Based VLAN can be setup by restricting the forwarding of Ethernet frames from one source port to a specific list of destination ports.

6.6.1 CLI Based Configuration

The `'Port Based VLAN menu'` offers the commands to manipulate the settings of the Port Based VLAN mode. To call the menu enter `<vlanp_cfg>` at the prompt.

```
[ 0] : no action (unsupported)
[ 1] : activate port based VLAN
[ 2] : deactivate port based VLAN
[ 3] : set VLAN port map
[ 4] : show VLAN port map
[ 5] : enable/disable port
[ 6] : set default configuration
[ ?] : ?: help
[ h] : h: help
[ q] : q: quit submenu
```

Figure 6-2 : CLI Port Based VLAN menu

The following chapters will explain how to use these submenus.

NOTE: In a redundant MicroTCA system with two MCHs an endless frame loop might occur if the front panel GbE ports of both MCHs are connected to the same network. For this reason, either the VLAN port configuration has to be set to avoid such frame loop, or it must be assured that the front GbE ports are not connected to the same network!

6.6.1.1 *Activate/Deactivate Port Based VLAN*

The configuring of the Port Based VLAN is available, if the protocol mode is set to "enabled". This can be done by choosing the menu item `<activate port based VLAN>` from the configuration menu.

The menu item `<deactivate port based VLAN>` can be used to deactivate the Port Based VLAN protocol again.

6.6.1.2 *Set VLAN Port Map*

With this menu, the forwarding map for one switch port item can be setup and changed. During the configuration process, the user has to enter the source port ID and the list of destination ports to which incoming frames (from the source port) may be forwarded.

The configuration software will display a table of all available ports on the NAT-MCH version. The user has to enter the AMC-Port ID (indicated in the second row of the table) for which the forwarding map should be setup:

```
Choose Port ID:
 |=============================================================================|
 |               AMCs                              Front     Up_C   ISw    CPU   |
 | AMC           0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
 | SLOTS         1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
 |-----------------------------------------------------------------------------|
 | AMC    from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
 | PORTS    to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
 |-----------------------------------------------------------------------------|
 | PORT          0  0  0  0  0  0  0  0  0  1      1  1      1      1      1 |
 | ID            1  2  3  4  5  6  7  8  9  0      1  2      3      4      5 |
 > (RET=0/0x0):
```

After choosing the source port number the user has to decide for each destination port, if forwarding to this port should be allowed:

```
[0] - disable frame forwarding to this port
[1] - enable frame forwarding to this port
```

NOTE: To setup a bi-directional communication path between two switch ports the forwarding map for both (source) ports has to be entered. Please also note that any setting for a particular source port will become effective immediately.

6.6.1.3 *Show VLAN Port Map*

This menu item displays the forwarding map for a specific or all source ports.

```
Choose Port ID:
|=============================================================================|
|                   AMCs                              Front     Up_C   ISw    CPU   |
| AMC               0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
| SLOTS             1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
| AMC        from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
| PORTS        to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
|-----------------------------------------------------------------------------|
|-----------------------------------------------------------------------------|
| PORT              0  0  0  0  0  0  0  0  0  1      1  1      1      1      1 |
| ID                1  2  3  4  5  6  7  8  9  0      1  2      3      4      5 |
 or [a] - for all ports
```

Entering the character <a> will display the forwarding configuration for all available destination ports, entering a specific port number will only display the forwarding map for this port.

```
|=============================================================================|
|                              Forwarding Map(s)                              |
|=============================================================================|
|                   AMCs                              Front     Up_C   ISw    CPU   |
|                   0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
|                   1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
|-----------------------------------------------------------------------------|
| AMC        from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
| PORTS        to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
|-----------------------------------------------------------------------------|
|     S_PORT                                                                  |
|     AMC1/1    :   1  x  1  1  1  1  1  1  1  1      1  d      1      d      1 |
|=============================================================================|
```

The printed table shows the forwarding map for one or all source ports (depending on the selection above). Each line contains the source port ID at the beginning followed by the forwarding map.

The meaning of the characters shown in the forwarding map is as follows:

'x' – no relationship as the source port equals the destination port
'0' – frames are not forwarded to the respective destination port
'1' – frames are forwarded to the respective destination port
'd' – disabled as the respective destination port is existing but turned off

6.6.1.4 *Enable/Disable Port*

This menu item can be used to disable or enable particular switch ports. If a port is disabled no traffic will be received from or transmitted to this port.

Please be aware that turning on or off a port affects its relationship to any destination port. When disabling a port, all port maps that contain an entry for this port as a destination port will have this entry set to <d> for 'disabled'. When enabling a disabled source port the entry in any port map for this particular port as a destination port will be set to <1> for 'frames are forwarded to the respective destination port'.

Please note that any setting for a particular source port will become effective immediately.

The configuration software will display a table of all available ports on the NAT-MCH version. The user has to enter the port number (indicated in the second row of the table) for which the forwarding map should be setup:

```
Choose Port ID:
  |=============================================================================|
  |                    AMCs                                 Front     Up_C   ISw    CPU   |
  | AMC                0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
  | SLOTS              1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
  |-----------------------------------------------------------------------------|
  | AMC        from:   0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
  | PORTS        to:   .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
  |-----------------------------------------------------------------------------|
  | PORT               0  0  0  0  0  0  0  0  0  1      1  1      1      1      1 |
  | ID                 1  2  3  4  5  6  7  8  9  0      1  2      3      4      5 |
> (RET=0/0x0):
```

After entering, the port number the following choices are displayed to either enable the port, disable the port or leave the port state unchanged:

```
    [d] - disabled
    [e] - enabled
    [q] - no change
   Enter port state (RET=0/0x0):
```

NOTE: Disabling the update channel (port number `<UPC_1>`) in a redundant system with two MCHs will seriously affect the functionality of the MicroTCA system, as this will break the communication between the MCHs.

6.6.1.5 *Set Default Configuration*

Choosing this menu item resets the Port Based VLAN settings to default. Forwarding of frames will be enabled for all source ports to all destination ports; all ports will be enabled.

6.6.2 Web Based Configuration

To configure the Port Based VLAN options of the switch select the `<Port VLAN>` link in the navigation frame of the NAT-MCH website.

The Port Based VLAN options can only be changed if the protocol mode has been activated.

6.6.2.1 *Activate/Deactivate Port Based VLAN*

If Port Based VLAN is currently disabled it can be enabled by clicking the <Activate> button.

The Port Based VLAN protocol can be also deactivated at any time by clicking the `<Deactivate>` button.

6.6.2.2 *Set VLAN Port Map*

The Port Based VLAN forwarding maps are presented in form of a table for all ports in the lower part of the configuration webpage as shown in Figure 6-3.

To enable or to disable the forwarding of the Ethernet frames from a source port to a destination port check or uncheck the related checkbox of the forwarding table. To confirm the changes click the `<Apply>` button.

Slot	AMC1	AMC2	AMC3	AMC4	AMC5	AMC6	AMC7	AMC8	AMC9	AMC10	AMC12	FRT1	FRT2	UPD1	ISW1	CPU1
Port	0	0	0	0	0	0	0	0	0	0	0	-	-	-	-	-
AMC1_0	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
AMC2_0	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
AMC3_0	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
AMC4_0	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
AMC5_0	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
AMC6_0	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
AMC7_0	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
AMC8_0	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
AMC9_0	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
AMC10_0	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
AMC12_0	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
FRT_1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
FRT_2	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
UPDC_B	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
ISWC_BX	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
CPU_1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Figure 6-3 : Port Based VLAN Forwarding Maps Webpage

6.6.3 Text based Configuration

There are three configuration items related to the Port Based VLAN protocol.

`eth_pbvlan_init`	Activate/Deactivate Port Based VLAN protocol
`eth_pbvlan_fwcm`	Set port map

6.6.3.1 *Activate/Deactivate Port Based VLAN*

Description:

The configuration item <`eth_pbvlan_init`> is used to activate the Port Based VLAN mode. If the configuration item is missing in the configuration file the Port Based VLAN protocol will be deactivated for default.

Syntax:

```
eth_pbvlan_init   = FLAG;
```

Parameter Description:

The parameters of the `<eth_pbvlan_init>` configuration item are described in Table 8-7 on page 128.

Example:

```
eth_pbvlan_init   = 1;
```

The Port Based VLAN will be activated.

6.6.3.2 *Set VLAN Port Map*

Description:

The `<eth_pbvlan_fwcm>` configuration item is used to specify the forwarding port map for a specific source port.

Syntax:

```
eth_pbvlan_fwcm = SRC_CON, LIST_OF_ALIASES
```

Parameter Description:

The <`eth_pbvlan_fwcm`> configuration item consists of several source aliases and a list of destination aliases, which specify the frame forwarding on connections according to the description in chapter 3.3. Bit values related to reserved ports are ignored and set to the default value. The parameters are described in *Table 8-8* on *page 128*.

Example:

```
eth_pbvlan_fwcm = AMC1/0,     AMC1/0, AMC2/0, AMC3/0, CPU_1
                  SRC_CON     LIST_OF_ALIASES
```

The configuration item sets the forwarding for the source connection assigned to the alias <AMC1/0>. The Ethernet packets will be forwarded to connections: <AMC1/0>, <AMC2/0>, <AMC3/0> and <CPU_1>.

6.7 802.1Q VLAN

The 802.1Q VLAN protocol uses the so-called VLAN tag included in the Ethernet frame for deciding if a frame should be forwarded to a specific switch port or not. Stations within the network are grouped together to one virtual network by using the same VLAN identifier within the Ethernet frame.

The Ethernet switch can be configured to allow the forwarding of VLAN tagged frames only to dedicated ports depending on the VLAN identifier of the received Ethernet frame. This means that a port has to be a member of a VLAN group (identified by the VLAN ID) to allow forwarding of frames containing the VLAN ID to this port. Such ports will be called Membership Ports or Associated Ports in this document.

Furthermore, the switch can be configured to remove the VLAN tag from an Ethernet frame before forwarding the frame to the destination port. This can be configured for each VLAN ID on a per port basis. These ports will been called Untagged Ports in this document.

Incoming frames that do not contain a VLAN tag field are tagged with a default VLAN tag. The default VLAN ID and the default priority within this tag can be set for each port individually.

NOTE: The NAT-MCH cannot process frames that contain a VLAN tag. Therefore, the CPU port always should be marked as Untagged.

The switch is preset to route all frames without a VLAN Tag. This is achieved by setting the default VLAN ID for each port to 1 and adding an VLAN table entry for VLAN ID 1, which allows forwarding these frames to all ports. Furthermore, all ports are marked as untagged ports, so that all incoming frames are forwarded through the switch unchanged.

NOTE: Changing these default VLAN settings might result in unrequested system behavior!

The address-learning mode used by the switch can be configured to either use the MAC address of the Ethernet frame only for the address learning or to use both, the MAC address and the VLAN ID of the Ethernet frame for the address learning.

6.7.1 CLI Based Configuration

The '802.1Q VLAN menu' offers the commands to manipulate the settings related to the 802.1Q VLAN protocol. To call the menu enter <vlanq_cfg> at the prompt.

```
[ 0] : no action (unsupported)
[ 1] : activate 802.1Q VLAN
[ 2] : deactivate 802.1Q VLAN
[ 3] : set learn mode
[ 4] : show learn mode
[ 5] : add/Set VLAN group
[ 6] : remove VLAN group
[ 7] : show all VLAN groups
[ 8] : set default VLAN ID for a port
[ 9] : show port default VLAN IDs
[10] : set default configuration
```

Figure 6-4 : CLI 802.1Q VLAN menu

The following chapters will explain how to use these submenus.

6.7.1.1 *Activate/Deactivate 802.1Q mode*

The 802.1Q VLAN options can only be changed if the protocol mode has been activated. This can be done by choosing the menu item <activate 802.1Q VLAN> from the configuration menu.

The menu item <deactivate 802.1Q VLAN> can be used to deactivate the 802.1Q VLAN protocol again.

NOTE: The 802.1X and 802.1p features require the 802.1Q mode to be activated. Therefore, the 802.1Q VLAN mode cannot be deactivated if one of the features is active.

6.7.1.2 *Set 802.1Q Learn Mode*

This menu item is used to select the address-learning mode of the switch.

The following configuration options can be selected:

```
[1] - use MAC address and VLAN ID for the address resolution
[2] - only use the MAC address for the address resolution
>
```

If option <1> is selected the switch uses the MAC and the VLAN ID of the received Ethernet frame for the address learning. If option <2> is selected, only the MAC address will be used for the address learning.

6.7.1.3 *Show 802.1Q Learn Mode*

This menu item can be used to show the current address learning configuration (refer to chapter 6.7.1.2).

6.7.1.4 *Add/Set VLAN Group*

This menu item can be used to add a new VLAN ID to the VLAN table or to overwrite an already configured VLAN ID.

First, the VLAN ID that should be configured has to be entered (e.g. VLAN ID 156):

```
Enter VLAN ID (RET=0/0x0): 156
```

Then the port membership map for this VLAN ID has to be entered for all ports.

```
Enter port membership for this VLAN ID:
[0] - disable forwarding for this port
[1] - enable forwarding for this port
```

If frames with the corresponding VLAN ID should be forwarded to the port, enter <1>, otherwise enter <0> for the port.

After the port membership had been entered for each used port, the untagging map has to be entered:

```
Enter untagging map for this VLAN ID:
[0] - disable untagging for this port
[1] - enable untagging for this port
```

If the VLAN tag should be removed from the frame before it is forwarded to the destination port, enter <1>, otherwise enter <0> for the port.

6.7.1.5 *Remove VLAN Group*

This menu item can be used to remove a VLAN ID from the VLAN table.

The VLAN ID that should be removed has to be entered (e.g. VLAN ID 156):

```
Enter VLAN ID (RET=1/0x1): 156
```

6.7.1.6 *Show all VLAN Groups*

This menu item can be used to show all currently configured VLAN IDs.

The VLAN table will be printed on the console as shown in Figure 6-5.

```
VLAN (RET=0/0x0): 7
 |=============================================================================|
 |                              VLAN Table                                     |
 |=============================================================================|
 |                  AMCs                                 Front    Up_C  ISw  CPU  |
 |                  0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
 |                  1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
 |-----------------------------------------------------------------------------|
 | AMC        from: 0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
 | PORTS        to: .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
 |-----------------------------------------------------------------------------|
 | VLAN                                                                        |
 | 0001 m       :  1  1  1  1  1  1  1  1  1  1      1  d      1      d      1 |
 |      u       :  1  1  1  1  1  1  1  1  1  1      1  d      1      d      1 |
 |-----------------------------------------------------------------------------|
 | 0002 m       :  1  1  0  0  0  0  0  0  0  0      1  d      0      d      0 |
 |      u       :  1  1  0  0  0  0  0  0  0  0      1  d      0      d      0 |
 |-----------------------------------------------------------------------------|
```

Figure 6-5 : IEEE 802.1Q VLAN table example

The first column shows the VLAN ID of the VLAN Group entry. The line marked with a 'm' at the beginning shows the Membership Port map which indicates to which ports a frame containing the VLAN ID may be forwarded. The line marked with a `'u'` at the beginning contains the Untagged Port map, which indicates if the VLAN ID should be removed from the Ethernet frame before it is forwarded to this port.

6.7.1.7 *Set Port Default VLAN Tag*

This menu item can be used to assign a default VLAN ID to a specific switch port.

First, the switch port number has to be entered:

```
Choose Port ID:
 |=============================================================================|
 |                  AMCs                                 Front    Up_C  ISw  CPU  |
 | AMC              0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
 | SLOTS            1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
 |-----------------------------------------------------------------------------|
 | AMC        from: 0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
 | PORTS        to: .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
 |-----------------------------------------------------------------------------|
 | PORT             0  0  0  0  0  0  0  0  0  1      1  1      1      1      1 |
 | ID               1  2  3  4  5  6  7  8  9  0      1  2      3      4      5 |
> (RET=0/0x0):
```

Then the default VLAN ID has to be entered:

```
Enter VLAN ID (RET=164/0xa4): 76
```

and finally the VLAN priority:

```
Enter VLAN Priority[0-7] (RET=0/0x0): 3
```

In this example the default VLAN ID 76 and the VLAN priority 3 will be assigned to the port <AMC 2>, means all incoming Ethernet frames received on port <AMC 2> which do not contain a VLAN tag will be tagged by the switch using the VLAN ID 76 and VLAN priority 3.

6.7.1.8 *Show Port Default VLAN IDs*

This menu can be used to display the current default VLAN ID and VLAN priority assigned to the switch ports.

The settings will be printed on the console as shown in Figure 6-6. The first column contains the switch port number, the second column the default VLAN ID and the third column the default VLAN priority.

```
|============================================|
|***        PORT DEFAULT VLAN IDs          ***|
|============================================|
| port id       VLAN ID           PRI        |
|--------------------------------------------|
|  AMC_01          0001           00         |
|  AMC_02          0001           00         |
|  AMC_03          0001           00         |
|  AMC_04          0001           00         |
|  AMC_05          0001           00         |
|  AMC_06          0001           00         |
|  AMC_07          0001           00         |
|  AMC_08          0001           00         |
|  AMC_09          0001           00         |
|  AMC_10          0001           00         |
|  AMC_11          0001           00         |
|  AMC_12          0001           00         |
|  FRNT_1          0001           00         |
|  UP_C_1          0001           00         |
|  CPU__1          0001           00         |
|============================================|
```

Figure 6-6 : 802.1Q port default VLAN ID example

6.7.2 Web Based configuration

To configure the 802.1Q VLAN protocol options of the switch select the <802.1Q VLAN> link in the navigation frame of the NAT-MCH website.

The 802.1Q VLAN options can only be changed if the protocol mode has been activated.

6.7.2.1 *Activate/Deactivate 802.1Q VLAN*

If 802.1Q VLAN is currently disabled it can be enabled by clicking the <Activate> button.

The 802.1Q VLAN protocol can be deactivated by clicking the <Deactivate> button.

NOTE: The 802.1X and 802.1p features require the 802.1Q mode to be activated. Therefore, the 802.1Q VLAN mode cannot be deactivated if one of the features is active.

6.7.2.2 *802.1Q VLAN menu*

If 802.1Q VLAN mode is activated, the menu as shown in Figure 6-7 will be presented on the webpage. The menu offers diverse tools to configure the 802.1Q VLAN. The configuration options will be explained in the following chapters.

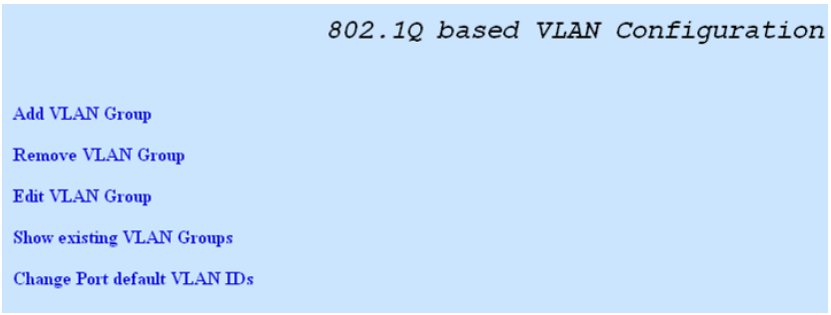


Figure 6-7 : 802.1Q VLAN Web-Menu

6.7.2.3 *Add VLAN Group*

Figure 6-8- shows the "Add VLAN Group" webpage, which can be used to add new VLAN groups to the VLAN table.

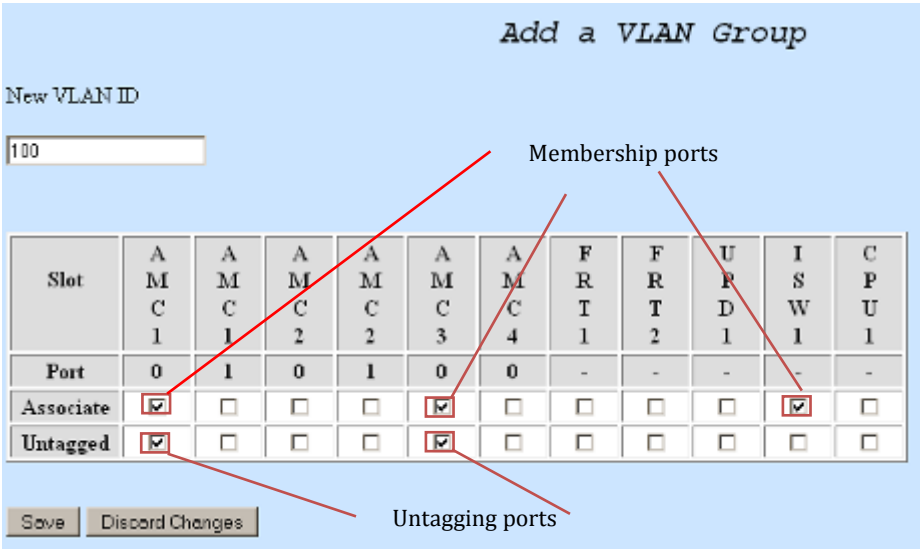


Figure 6-8 : Add VLAN Group webpage

To add a new entry to the VLAN table the VLAN ID has to be entered into the field "New VLAN ID" first. This value must be within a range from 1 to 4094.

After this, the Membership Ports have to be selected by setting the checkboxes in the row named "associate". If the checkbox is set, the port will be a member of that VLAN group, if it is not set the port is not a member of the VLAN group.

The row named "untagged" determines if the VLAN tag shall be removed from the Ethernet frame (means untagged) before it is sent on the destination port. If the checkbox of a port is set the frames directed to this port will be untagged, if not, the frames will routed unchanged.

The VLAN group will be added to the VLAN table after the "Save" button on the webpage has been clicked. By clicking the "Discard Changes" button, the entered information will be neglected.

6.7.2.4 *Remove VLAN Group*

Figure 6-9 shows the "Remove VLAN Group" webpage, which can be used to remove existing VLAN groups from the VLAN table.

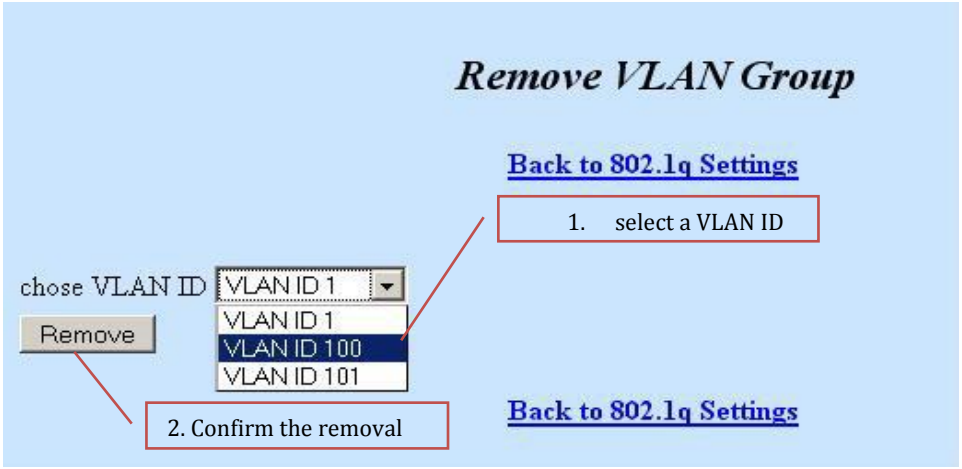


Figure 6-9 : Remove VLAN Group webpage

The currently configured VLAN IDs can be selected via the "choose VLAN ID" dropdown menu. To remove a VLAN ID from the VLAN table select the VLAN ID in the dropdown menu and click the "Remove" button.

6.7.2.5 *Edit VLAN Group*

Existing VLAN groups can be changed via the "Edit VLAN Group" webpage.

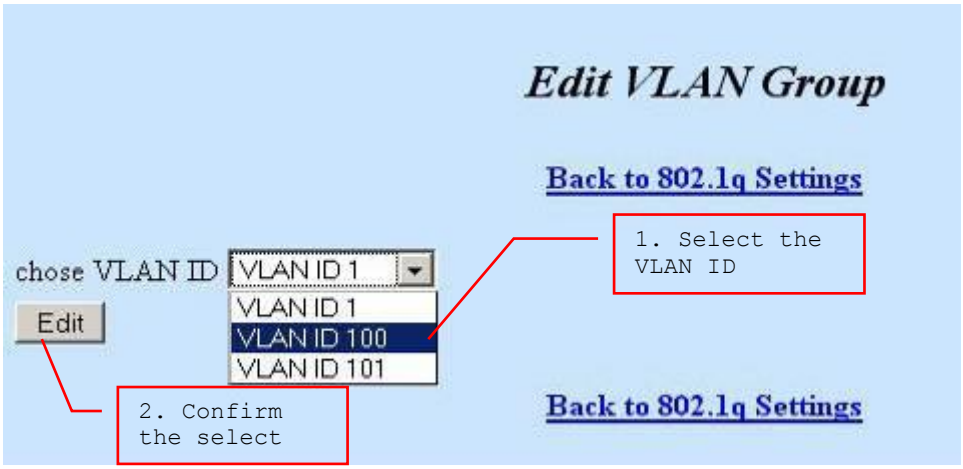
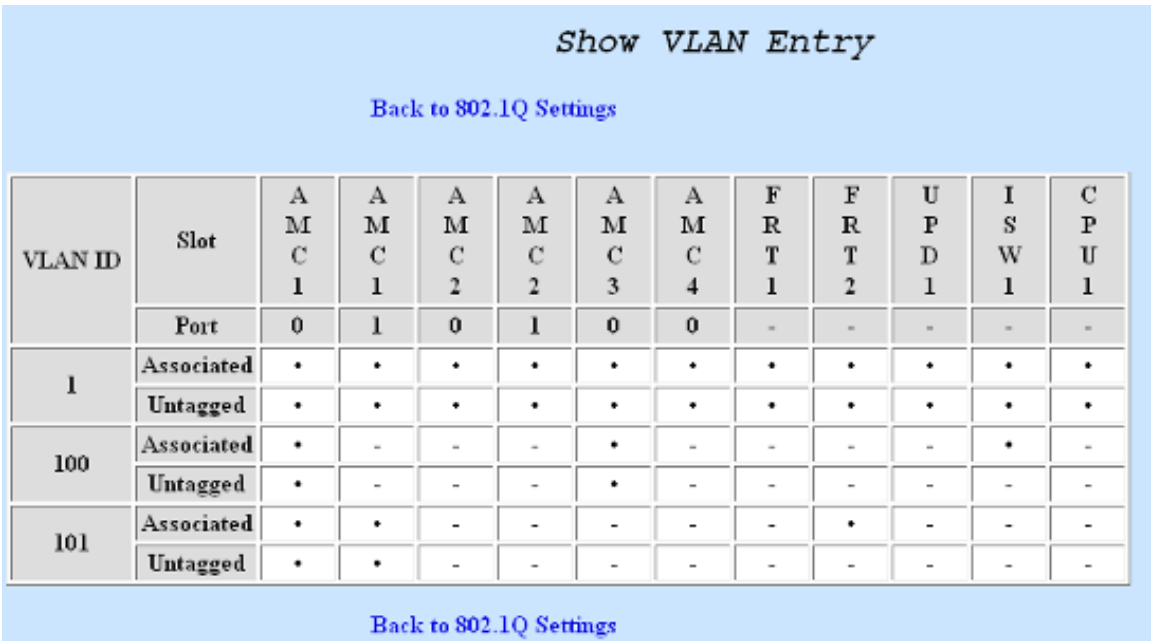


Figure 6-10: Edit VLAN-group

First, the VLAN ID of the group that should be changed has to be selected from the dropdown menu. After clicking the <Edit>-button the VLAN-group can be changed, as described in chapter 6.7.2.3.

6.7.2.6 *Show Existing VLAN Group*

To show the existing VLAN groups choose the "Show existing VLAN Group" webpage from the configuration menu page. The existing VLAN-Table entries will be listed as show in Figure 6-14.



VLAN ID	Slot	AMC1	AMC1	AMC2	AMC2	AMC3	AMC4	FRT1	FRT2	UPD1	ISW1	CPU1
	Port	0	1	0	1	0	0	-	-	-	-	-
1	Associated	•	•	•	•	•	•	•	•	•	•	•
	Untagged	•	•	•	•	•	•	•	•	•	•	•
100	Associated	•	-	-	-	•	-	-	-	-	•	-
	Untagged	•	-	-	-	•	-	-	-	-	-	-
101	Associated	•	•	-	-	-	-	-	•	-	-	-
	Untagged	•	•	-	-	-	-	-	-	-	-	-

Figure 6-11: Show existing VLAN group

Switch ports marked with a dot are members of the VLAN group. Ports marked with hyphen are not members of the group.

6.7.2.7 *Set Port Default VLAN Tag*

This page can be used to display and change default VLAN ID assignment to the switch ports.

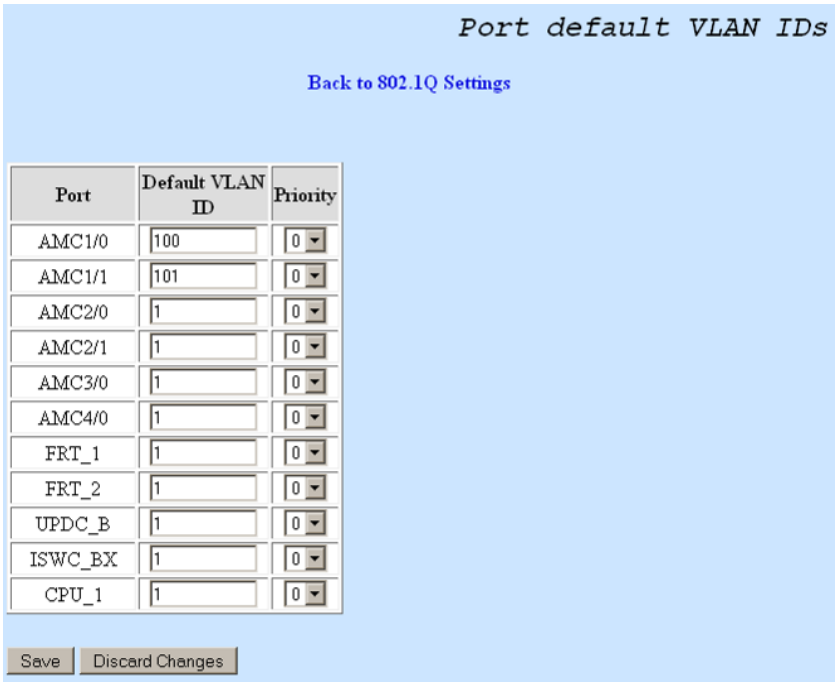


Figure 6-12 : Change Port Default VLAN ID

To assign a default VLAN ID to a certain port, enter the VLAN ID to the column `<Default VLAN ID>` and press the button `<Save>` to confirm a change.

6.7.3 Text Based configuration

To configure the 802.1Q VLAN protocol five configuration items of the text-based configuration have to be used:

`eth_802.1q_init` Activation/Deactivation flag for 802.1Q VLAN mode
`eth_802.1q_lrn` Hash key generation mode
`eth_802.1q_m_cm` Port Membership map of the VLAN group
`eth_802.1q_u_cm` Port Untagging map of the VLAN group
`eth_802.1q_tag` Port default VLAN-Tag

6.7.3.1 *Activate/Deactivate 802.1Q VLAN*

Description:

The `<eth_802.1q_init>` configuration item determines if the 802.1Q VLAN mode should be activated or deactivated. If the configuration item is set to `"deactivate"` or the item is not present at all, other configuration items related to this mode will be ignored.

Syntax:

```
eth_802.1q_init  = FLAG;
```

Parameter Description:

The parameters of the `<eth_802.1q_init>` configuration item are described in the Table 8-9 page 129.

Example:

Activate 802.1Q VLAN mode:

```
eth_802.1q_init  = 1;
```

The upper configuration item activates 802.1Q VLAN mode.

6.7.3.2 *Learn Mode*

Description:

The <`eth_802.1q_lrn`> configuration item can be used to change the hash key generation algorithm of the Ethernet switch.

Syntax:

```
eth_802.1q_lrn   = FLAG;
```

Parameter Description:

The Parameters of `<eth_802.1q_lrn>` *config item* are described in *the Table 8-10* page *129.*

Example:

```
eth_802.1q_lrn   = 0;
```

The configuration item sets the hash key generation algorithm for the MAC-Table entries to the mode:

```
Use only the MAC-Address to generate the hash key
```

6.7.3.3 *Add VLAN Group*

Description:

The configuration items <eth_802.1q_m_cm> and <eth_802.1q_u_cm> can be used to add a VLAN group to the VLAN-Table.

eth_802.1q_m_cm – Port Membership map
eth_802.1q_u_cm – Port Untagging map

NOTE: If one of the configuration items of a VLAN group is missing, it will be substituted by the default values as defined in *Table 8-11* and *Table 8-12*.

Syntax:

Each of the configuration items has seven parameters. The first parameter specifies the VLAN ID of the VLAN group. The other parameters specify the port maps for the VLAN group.

```
eth_802.1q_m_cm = VLANID, LIST_OF_ALIASES
eth_802.1q_u_cm = VLANID, LIST_OF_ALIASES
```

Parameter Description:

The parameters of the <eth_802.1q_m_cm> and <eth_802.1q_u_cm> configuration items are described in *Table* 8-11 *on* page 130 and *Table* 8-12 on page *130.*

Syntax:

Add VLAN group with ID 3.

```
eth_802.1q_m_cm = 0003,  AMC1/0, AMC2/0, AMC3/0
eth_802.1q_u_cm = 0003,  AMC1/0, AMC2/0
```

The upper example shows the configuration items for adding an entry assigned VLAN ID <0003>. The entry allows the forwarding of Ethernet packets with the VLAN-Tag containing VLAN ID <0003> to the all VLAN member ports AMC1/0, AMC2/0, AMC3/0 (see <eth_802.1q_m_cm>) and the removal of VLAN-Tag on ports AMC1/0, AMC2/0 (see <eth_802.1q_u_cm>) by transmitting.

6.7.3.4 *Set Port Default VLAN Tag*

Description:

The configuration item `<eth_802.1q_dflt>` can be used to set the default VLAN ID and default VLAN-Priority of a certain connection. Incoming frames that do not contain a VLAN Tag will be tagged using these default values.

Syntax:

```
eth_802.1q_dflt = ALIAS, VLANID, PRI_1P
```

Parameter Description:

The Parameters of the `<eth_802.1q_tag>` configuration item are described in the *page 130.*

Example:

Set default VLAN tag for AMC Port `<AMC1/0>` using VLAN ID `<1>` and priority `<7>`.

```
eth_802.1q_tag  = AMC1/0,  0001,  7
```

The upper configuration item sets default VLAN tag for AMC-Port `<AMC1/0>` using VLAN ID `<1>` (see VLANID) with the priority `<0>` (see PRI_1P) for all incoming Ethernet frames.

6.7.4 VLAN Tunneling for Update Channel

The redundancy mode of NAT-MCH is procurable due to periodical updates that primary MCH sends to secondary MCH via Ethernet. To isolate update communication from regular traffic, the NAT-MCHs use special VLAN group named *Update*.

The NAT-MCH firmware creates Update group with VLAN ID 4093 automatically on activation of 802.1Q VLAN mode.

VLAN ID	Slot	AMC1	AMC2	AMC3	AMC4	AMC5	AMC6	AMC7	AMC8	AMC9	AMC10	AMC11	AMC12	FRT1	FRT2	UPDB	ISWB	CPU1
	Port	0	0	0	0	0	0	0	0	0	0	0	0	-	-	-	-	-
1	Associated	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
	Untagged	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•
100	Associated	•	-	-	-	•	-	-	-	-	-	-	-	•	-	-	-	-
	Untagged	•	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
UPDATE	Associated	-	-	-	-	-	-	-	-	-	-	-	-	-	-	•	-	•
	Untagged	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	•

Figure 6-13: 802.1Q VLAN group for Update Cannel

The user interface prohibits any editing of this group.

6.8 802.1X Port-Based Security

IEEE 802.1X defines a port-based authentication protocol. It provides authentication of devices attached to a switch port and supports authentication process for all frames based on matching of source MAC address and VLAN ID of an incoming frame and existing information at the MAC table of the switch.

In 802.1X also the source MAC address only can be used for authentication, because the IEEE standard does define this explicitly. Therefore, the decision about which parameters to be used is left to the switch manufacturer. The Ethernet switch on the baseboard uses for the authentication the MAC address and the VLAN ID while the XAUI switch on the hub module only uses the MAC address. The user interface takes care about these differences and only offers the parameters needed for the specific switch device.

The 802.1X protocol can be activated on a per port basis. MAC addresses that should be authenticated must be written into the MAC table of the switch.

6.8.1 CLI based Configuration

The `'802.1X menu'` offers the commands to manipulate the settings of the 802.1s security mode. To call the menu enter `<vlanx_cfg>` at the prompt.

6.8.1.1 *Activate/Deactivate 802.1X Mode*

The 802.1X protocol options can only be changed if the mode has been activated. This can be done by choosing the menu item `"activate 802.1X"` from the submenu.

The 802.1X protocol can be deactivated by choosing the menu item `"deactivate 802.1X"`.

NOTE: The 802.1X feature can only operate if the 802.1Q feature is activated.

6.8.1.2 *Set Frame Dropping Mode*

The switch can be configured to route or drop special frames such as Bridge Protocol Data Units (BPDU) and Extensible Authentication Protocol over LAN (EAPOL) frames. Two modes can be configured on the NAT-MCH related to these special frames:

- Drop frame if source MAC misses in the MAC table, and the frame is not a IEEE Standard 802.1X special frame
- Drop frames that are not IEEE Standard 802.1X special frames

These modes can be set in the `<set/read dropping mode>` menu item.

```
Mode: drop frames if MAC SA misses
Change to 'drop all frames without special frames'?
[0]-no; [1]-yes (RET=0/0x0):
```

When chosen, the current mode setting is shown and the user is asked if the mode should be changed. To change the mode enter `<1>` - for `'yes'` or enter `<0>` - for `'no'`.

6.8.1.3 *Add 802.1X Entry*

The authentication process for every frame is based on matching of the source MAC address and the VLAN ID of an incoming frame with an existing 802.1X entry in the address table of the switch. To write such an 802.1X entry, select the `<write 802.1X entry>` menu item.

First, the MAC address has to be specified in the following format:

```
Enter MAC(xx:xx:xx:xx:xx:xx):
00:E0:4C:75:6B:DE
```

Then the VLAN ID has to be entered (depending on the switch device):

```
Enter VLAN ID: (RET=0/0x0): 0007
```

Finally, the switch port number has to be chosen to which the MAC address belongs:

```
Choose Port ID:
 |=============================================================================|
 |               AMCs                                Front     Up_C   ISw    CPU   |
 | AMC           0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
 | SLOTS         1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
 |-----------------------------------------------------------------------------|
 | AMC    from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
 | PORTS    to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
 |-----------------------------------------------------------------------------|
 | PORT          0  0  0  0  0  0  0  0  0  1      1  1      1      1      1 |
 | ID            1  2  3  4  5  6  7  8  9  0      1  2      3      4      5 |
or [a] - for All ports
 > (RET=0/0x0):
```

6.8.1.4 *Delete 802.1X Entry*

To delete an 802.1X entry from the address table, choose the menu item `<delete 802.1X entry>` and enter the MAC address of the entry in the following format:

```
Enter MAC(xx:xx:xx:xx:xx:xx):
00:E0:4C:75:6B:DE
```

Then enter the VLAN ID:

```
Enter VLAN ID (1..4094): 0007
```

If the 802.1X entry was found it can be deleted:

```
|=============================================================|
|        MAC        | VID  |PRI|Age|Static| Ports            |
|-------------------------------------------------------------|
| 00:E0:4C:75:6B:DE | 0007 | 0 | 0 |  1   | 0x0002(-------)  |
|=============================================================|
 End of Search
Delete?
[1] -'no'; [2] - 'yes' (RET=0/0x0):
```

Figure 6-14: example of menu item „Delete 802.1X entry

Enter `<2>` to delete the 802.1X entry or `<1>` to cancel the operation.

6.8.1.5 *Delete all Entries*

This menu item can be used to delete all existing 802.1X entries. To delete all entries enter <y>, to cancel the operation enter <n>.

6.8.1.6 *Show all 802.1X Entries*

This menu item can be used to show all 802.1X entries.

```
=========================================================
|        MAC         | VID  |PRI|Static|       Port      |
|-------------------------------------------------------|
| 00:03:04:05:06:07 | 0100 | 0 |  1   | AMC_01( 802.1X) |
=========================================================
 End of Search
802.1X (RET=0/0x0):
```

Figure 6-15: example of the menu item „Show all 802.1X entries“

6.8.1.7 *Set 802.1X Ports*

With this menu item, the 802.1X mode can be activated or deactivated for any port of the NAT-MCH separately.

The mode can either be set for all ports at once or for one specific port.

```
  |=================================================================|
  |              Set security function ports                        |
  |=================================================================|
    Choose switch port ID:
P |=============================================================================|
O |         AMC SLOTS       |    Fr_PHY   |Upd_C|    ISw      |     CPU     |
R | 0 0 0 0 0 0 0 0 0 1 1 1 | 0 0 . . . . | 0 . | 0 . . . . . | 0 . . . . . |
T | 1 2 3 4 5 6 7 8 9 0 1 2 | 1 2 . . . . | 1 . | 1 . . . . . | 1 . . . . . |
  |-----------------------------------------------------------------------------|
I | 0 0 0 0 0 0 0 0 0 0 1 1 | 1 1 . . . . | 1 . | 2 . . . . . | 2 . . . . . |
D | 0 1 2 3 4 5 6 7 8 9 0 1 | 2 3 . . . . | 8 . | 0 . . . . . | 6 . . . . . |
or [a] - for All ports
     > (RET=a):
```

Figure 6-16 : example of the menu item „Set 802.1X ports“

If the 802.1X mode should only be activated for one specific port, enter the number of this port, otherwise enter <a> to set the mode for each used port:

The security mode can either be enabled by entering <1> or disabled by entering <0>.

```
[0] - disable security function for this port
[1] - enable security function for this port
```

6.8.1.8 *Show 802.1X Ports*

With this menu item, the 802.1X states of all ports are shown.

```
|=========================================================|
|                802.1X Security Port Map                 |
|=========================================================|
|                  AMC SLOTS           Fr_PHY  Upd_C   CPU |
|           0 0 0 0 0 0 0 0 0 0 1 1 1     0      0        0 |
|           1 2 3 4 5 6 7 8 9 0 1 2 3     1      1        1 |
|---------------------------------------------------------- |
|           1 0 0 0 0 0 0 0 0 0 0 0 0     0      0        0 |
|=========================================================|
```

Figure 6-17 : example of the menu item „Show 802.1X ports“

<0> indicates that the 802.1X mode is deactivated for that port, <1> indicates that it is activated.

6.8.2 Web Based Configuration

To configure 802.1X protocol via the web interface, click the <802.1X> link at the navigation part of the browser window.

6.8.2.1 *Activate/Deactivate 802.1X Mode*

The 802.1X protocol can be activated and deactivated via the web interface by clicking the <Activate> button (refer to Figure 6-18). The 802.1Q VLAN mode has to be enabled before the 802.1X mode can be activated.

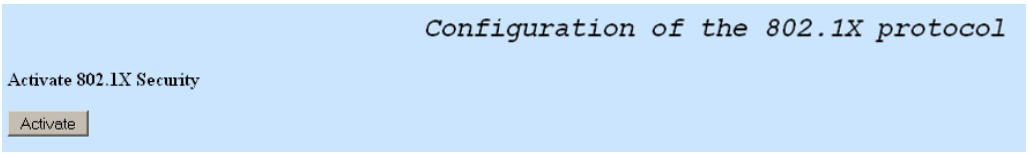


Figure 6-18 : Activate 802.1X

After the 802.1X protocol has been activated, the configuration menu will be displayed on the web page as shown in Figure 6-19.

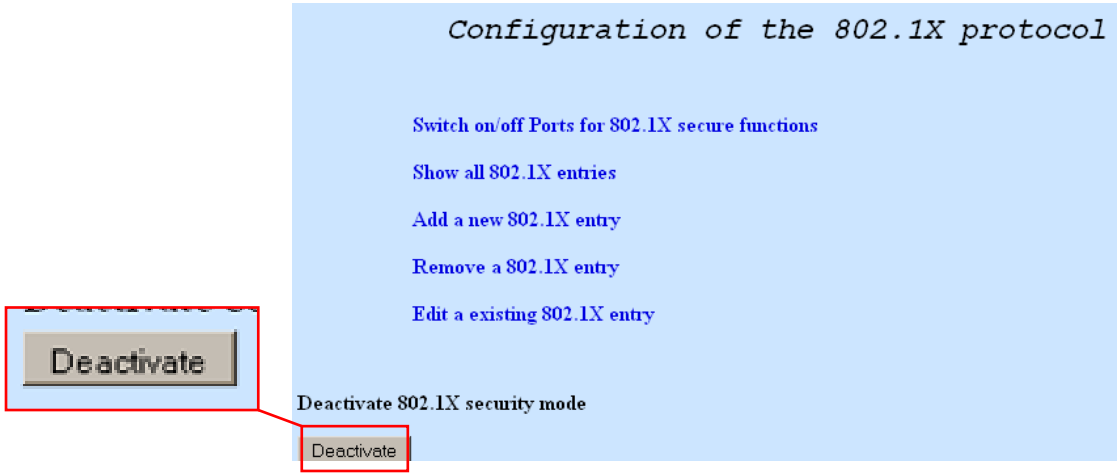


Figure 6-19 : 802.1X Menu

To deactivate the 802.1X protocol, press the <Deactivate> button on the bottom of the webpage.

6.8.2.2 *Set 802.1X Ports*

To enable the security function on a certain port, choose the <Switch on/off ports for security function> link as shown in Figure 6-19.

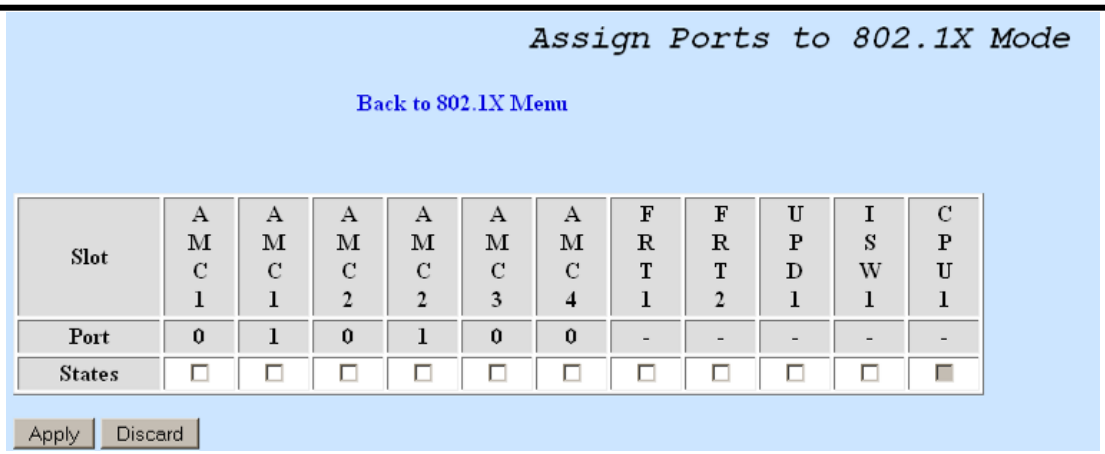


Figure 6-20 : 802.1X secure ports

To enable the 802.1X function on a specific port the checkbox in the column "On" has to be set for that port. The changes will be applied after pressing the <Save> button or discarded when pressing the <Discard Changes> button.

6.8.2.3 *Show all 802.1X Entries*

To view all 802.1X related MAC table entries click on the <Show all 802.1X entries> link in the configuration menu. The entries present in the MAC table are displayed as shown in **Figure 6-21**.

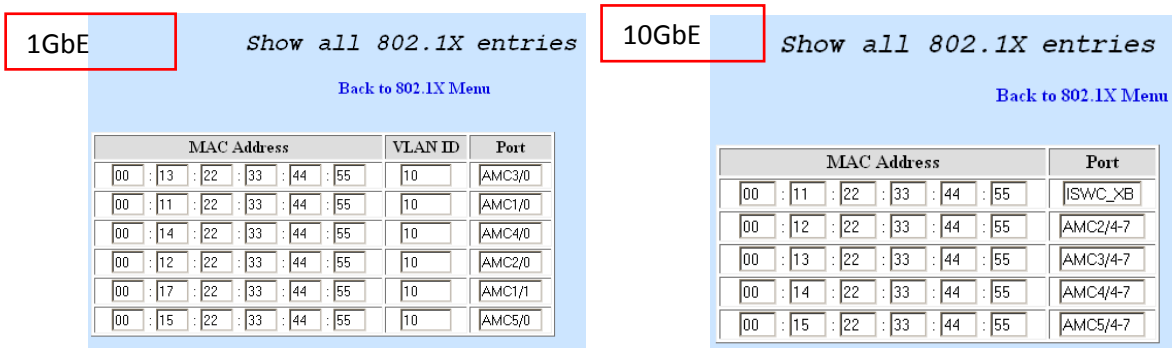


Figure 6-21 : Show all 802.1X Entries

6.8.2.4 *Add 802.1X Entry*

To authenticate a station in the Ethernet switch, its MAC address has to be added to the MAC table. This can be done via the <Add a new 802.1X entry> webpage in the 802.1X configuration menu as shown in Figure 6-19.

There are three parameters that have to be set to add a new 802.1X entry to the MAC table (refer to Figure 6-22). The MAC address (unicast address) of the station that should be authenticated has to be entered in the row "Mac Address". After that, the VLAN ID of the VLAN group the station belongs to has to be entered in the row "VLAN ID". Finally the switch port, the station is connected to, has to be selected via the radio buttons.

The entry will be added after pressing the <Save> button on the web page.

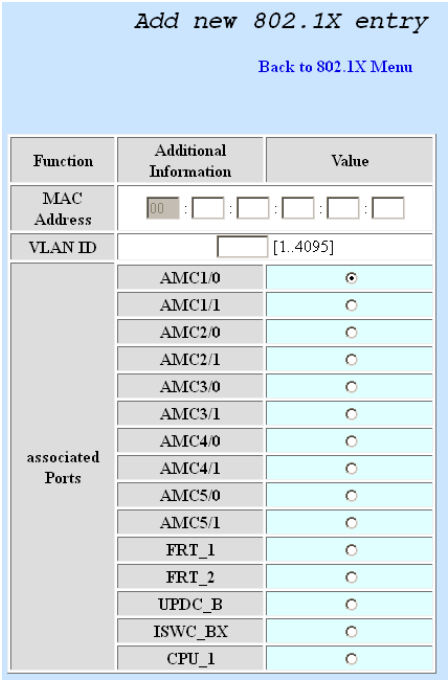


Figure 6-22 : Add new 802.1X Entry

6.8.2.5 *Remove 802.1X Entry*

To delete an 802.1X entry via the web interface choose the menu item <remove a 802.1X entry> at 802.1X configuration menu as shown in Figure 6-19.

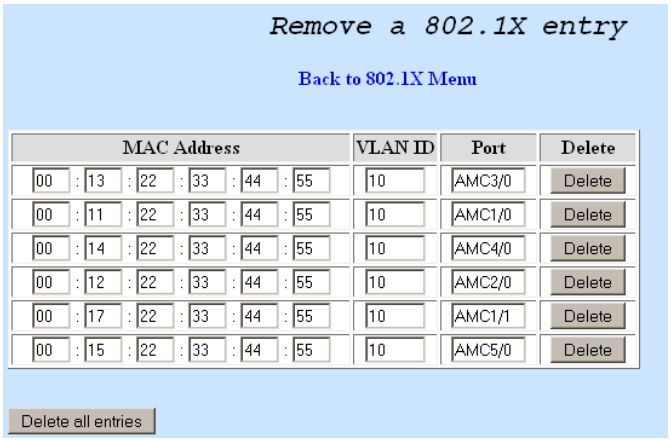


Figure 6-23 : Remove 802.1X entry

To delete one specific entry from the MAC table press the <Delete> button at the end of the row of the table entry. To remove all 802.1X entries, press the button <Delete all entries> button at the bottom of the webpage.

6.8.2.6 *Edit 802.1X Entries*

Already existing 802.1X entries can be changed via the `<Edit existing 802.1V entries>` menu item.

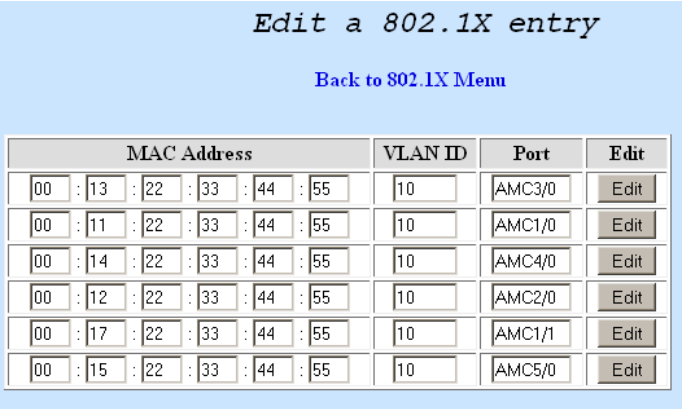


Figure 6-24 : Edit 802.1X Entry

To change an 802.1X entry press the `<Edit>` button in the table and update the parameters as described in *Chapter 6.8.1.3*.

6.8.3 Text Based Configuration

There are four types of configuration items, which are used, to configure the 802.1X mode:

```
eth_802.1X_ini      - 802.1X activation/deactivation
eth_802.1X_dm       - dropping mode
eth_802.1x_cm       - port map for 802.1X mode
eth_mac_ent_con     - MAC-Table entry for 802.1X mode
```

6.8.3.1 *Activate/Deactivate 802.1X Mode*

Description:

The <eth_802.1X_ini> configuration item determines if the 802.1X mode should be activated or deactivated. If the configuration item is set to "deactivate" or the item is not present at all, other configuration items related to this mode will be ignored.

Syntax:

```
eth_802.1X_ini  =  FLAG;
```

Parameter Description:

The parameters of the <eth_802.1X_ini> configuration item are described in Table 8-18 on page 133.

Example:

```
eth_802.1X_ini  = 1;
```

The upper example activates the 802.1X Security mode.

6.8.3.2 *Set Frame Dropping Mode*

Description:

The <eth_802.1X_dm> configuration item can be used to determine which frames types shall be dropped.

Syntax:

```
eth_802.1X_dm  = FLAG
```

Parameter Description:

The parameters of the <eth_802.1X_dm> configuration item are described in *Table* 8-19 page *133.*

Example:

```
eth_802.1X_dm  = 0
```

The configuration item allows the dropping of Ethernet frames if the source MAC misses in the MAC table and the frame is not an IEEE Standard 802.1X special frame.

6.8.3.3 *Set 802.1X Ports*

Description:

The 802.1X security mode can be activated at any connection by means of the `<eth_802.1x_cm>` configuration item.

Syntax:

```
eth_802.1x_cm  =LIST_OF_ALIASES
```

Parameter Description:

The parameters of `<eth_802.1x_cm>` configuration item are described in *Table 8-20* page *134.*

Example:

```
eth_802.1x_cm  =  AMC1/0, AMC2/0, AMC3/0, AMC4/0, AMC5/0
```

The example shows the activating of 801.2X port security mode at the connections `<AMC1/0>`, `<AMC2/0>`, `<AMC3/0>`, `<AMC4/0>` and `<AMC5/0>`.

6.8.3.4 *Add 802.1X Entry*

Description:

This configuration can be used to add 802.1X entries to the MAC table.

Syntax:

```
eth_mac_ent_con  = MAC_ADDR, VLANID, PRI_MTAB, ALIAS
```

Parameter Description:

The parameters of `<eth_mac_ent_con>` configuration item are described in Table 8-15 page *132.*

Example:

Add 802.1X entry for MAC `00:40:42:22:33:44` with VLAN ID `<100>`, priority `<0>` on port `<AMC1/0>`.

```
eth_mac_ent_con  = 00:40:42:22:33:44, 0100, 00, AMC1/0
```

6.9 Quality of Service

The Quality of Service (QoS) feature provides up to four internal queues per port to support four different traffic priorities. These priorities can be set in such a way that high priority traffic experiences less delay in the switch under congested condition than does low-priority traffic.

The switch can assign packets to one of the four egress transmit queues, according to information in the IEEE Standard 802.1p. The priority of the transmit queues raises with the queue's number so that queue number 0 has the lowest priority and queue 3 has the highest priority.

The IEEE Standard 802.1p feature is enabled on a port-by-port basis. When using the IEEE Standard 802.1p priority mechanism, the incoming packet is examined for the presence of a valid IEEE Standard 802.1p priority tag. If the tag is present, the packet is assigned a remapped IEEE Standard 802.1p priority based on a priority ID mapping. The priority ID from the IEEE Standard 802.1p priority tag can be mapped to one of four transmit queues.

6.9.1 CLI Based Configuration

The `'Quality of service menu'` offers the commands to manipulate the settings of the Quality of Service feature. To call the menu enter `<qos_cfg>` at the prompt.

6.9.1.1 *Show Priority ID Mapping"*

To show the priority mapping of a specific port enter the port number:

```
Choose Port ID:
 |=============================================================================|
 |               AMCs                                Front     Up_C   ISw    CPU   |
 | AMC           0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
 | SLOTS         1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
 |-----------------------------------------------------------------------------|
 | AMC    from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
 | PORTS    to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
 |-----------------------------------------------------------------------------|
 | PORT          0  0  0  0  0  0  0  0  0  1      1  1      1      1      1 |
 | ID            1  2  3  4  5  6  7  8  9  0      1  2      3      4      5 |
or [a] - for All ports
```

The current priority mapping for this port will be shown.

```
*****************************************
            Priority Mapping port: 1
*****************************************
pri_id: 0 tx_queue: 3
pri_id: 1 tx_queue: 3
pri_id: 2 tx_queue: 3
pri_id: 3 tx_queue: 3
pri_id: 4 tx_queue: 3
pri_id: 5 tx_queue: 3
pri_id: 6 tx_queue: 3
pri_id: 7 tx_queue: 3
```

Figure 6-25 : Quality of Service priority mapping

6.9.1.2 *Set Priority ID Mapping*

To change the priority mapping of a specific port first enter the port number:

```
     Choose switch port ID:
Choose Port ID:
 |=============================================================================|
 |               AMCs                              Front     Up_C   ISw    CPU   |
 | AMC           0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
 | SLOTS         1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
 |-----------------------------------------------------------------------------|
 | AMC    from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
 | PORTS    to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
 |-----------------------------------------------------------------------------|
 | PORT          0  0  0  0  0  0  0  0  0  1      1  1      1      1      1 |
 | ID            1  2  3  4  5  6  7  8  9  0      1  2      3      4      5 |
or [a] - for All ports
```

The current priority mapping for this port will be shown.

```
*****************************************
            Priority Mapping port: 1
*****************************************
pri_id: 0 tx_queue: 3
pri_id: 1 tx_queue: 3
pri_id: 2 tx_queue: 3
pri_id: 3 tx_queue: 3
pri_id: 4 tx_queue: 3
pri_id: 5 tx_queue: 3
pri_id: 6 tx_queue: 3
pri_id: 7 tx_queue: 3
```

Now the priority ID of the IEEE 802.1p standard has to be entered:

```
Enter priority id(0 - 7):  (RET=0/0x0): 1
```

Finally the transmit queue number for this priority ID has to be chosen:

```
Enter TX Queue(0 - 3):  (RET=0/0x0): 1
tx_queue: 1
```

After this the new priority mapping is printed:

```
****************************************
            Priority Mapping port: 1
****************************************
pri_id: 0 tx_queue: 3
pri_id: 1 tx_queue: 1
pri_id: 2 tx_queue: 3
pri_id: 3 tx_queue: 3
pri_id: 4 tx_queue: 3
pri_id: 5 tx_queue: 3
pri_id: 6 tx_queue: 3
pri_id: 7 tx_queue: 3
```

Note: The 802.1P mode has to be activated for a specific port in the `'802.1p submenu'`.

6.9.1.3 *Set Default QoS Configuration*

With this menu item, the current setting can be replaced by the default QoS configuration.

```
[1] - Reset general QoS setting only
[2] - Reset general all QoS setting
[q] - Qiut
```

In order to reset only general QoS settings enter `<1>`. In this case, all priority IDs for all MCH ports will be remapped to transmission queue 0 (lowest priority).

To reset all QoS settings (also 802.1p settings) enter `<2>`. In this case, all priority IDs for all MCH ports will be remapped to transmission queue 0 and the state of 802.1p ports will be set to `<0>` (disabled state).

6.9.2 Web Based Configuration

As the general Quality of Service options and the settings to support 802.1p have been placed on one webpage, please refer to chapter 6.10.2 for a detailed description.

6.9.3 Text Based Configuration

There is only one configuration item to set the general Quality of Service options:

`<eth_qos_cm>` - set priority mapping

6.9.3.1 *Set Priority ID Mapping*

Description:

It is possible to configure a mapping between a VLAN –Priority and internal transmit queue for a certain port. This can be done via the `<eth_qos_cm>` configuration item.

Syntax:

```
eth_qos_cm  = ALIAS, PRI_1P, TX_QUEUE
```

Parameter Description:

The parameters of the `<eth_qos_cm>` configuration item are described in *Table 8-21* on page *135.*

Syntax:

```
eth_qos_cm  = AMC1/0,  01,  03
```

The upper example accords the transmit queue 3(`TX_QUEUE`) to 802.1p priority 1 (see `PRI_1P`) on the AMC-Port `<AMC1/0>`.

6.10 802.1p Quality of Service

6.10.1 CLI Based Configuration

This submenu offers the following commands to manipulate the parameters of the 802.1p mode. To call the menu enter <qos1p_cfg> at the prompt.

```
[ 0] : no action (unsupported)
[ 1] : activate 802.1p mode
[ 2] : deactivate 802.1p mode
[ 3] : 802.1p port
[ ?] : ?: help
[ h] : h: help
[ q] : q: quit submenu
```

6.10.1.1 *Activate/Deactivate 802.1p Mode*

The 802.1p configuration options can only be changed if the 802.1Q mode and the 802.1p mode have been activated. This can be done by choosing the menu item <activate 802.1p mode>.

NOTE: The 802.1p feature can only operate if the 802.1Q mode is activated.

If activating the 802.1p mode the user will be asked if the 802.1Q (if deactivated) should also be activated.

```
802.1Q is deactivated. 802.1p need 802.1Q activated.
Should the 802.1Q mode be deactivated?
```

The 802.1p mode can be deactivated by choosing the menu item <deactivate 802.1p mode>.

6.10.1.2 *Set 802.1p Ports*

This menu item activates or deactivates the 802.1p protocol on a per port basis.

Enter the port number whose state should be changed:

```
Choose Port ID:
 |=============================================================================|
 |               AMCs                                Front     Up_C   ISw    CPU   |
 | AMC           0  0  0  0  0  0  0  0  0  0|      0  0|      0|      0|      0 |
 | SLOTS         1  1  2  2  3  3  4  4  5  5|      1  2|      1|      1|      1 |
 |-----------------------------------------------------------------------------|
 | AMC    from:  0  1  0  1  0  1  0  1  0  1      .  .      .       .       . |
 | PORTS    to:  .  .  .  .  .  .  .  .  .  .      .  .      .       .       . |
 |-----------------------------------------------------------------------------|
 | PORT          0  0  0  0  0  0  0  0  0  1      1  1      1       1       1 |
 | ID            1  2  3  4  5  6  7  8  9  0      1  2      3       4       5 |
or [a] - for All ports
     > (RET=a):
```

Then the 802.1p state can be set to <on> or <off>:

```
[0] - 802.1p off
[1] - 802.1p on.
```

6.10.2 Web Based Configuration

To call the Quality of Service webpage select the <802.1p> link at the navigation part of the browser window.

6.10.2.1 *Activate/Deactivate 802.1p Mode*

To activate the 802.1p mode click the <Activate> button on the 802.1p configuration webpage. To deactivate the mode use the <Deactivate> button.

6.10.2.2 *Set Priority ID Mapping*

To configure the mapping between the VLAN-Priority and the TX-Queue for a port follow the link <Switch on/off Ports and set priority ID mapping for 802.1p QoS> on the configuration webpage (See Figure 6-26).

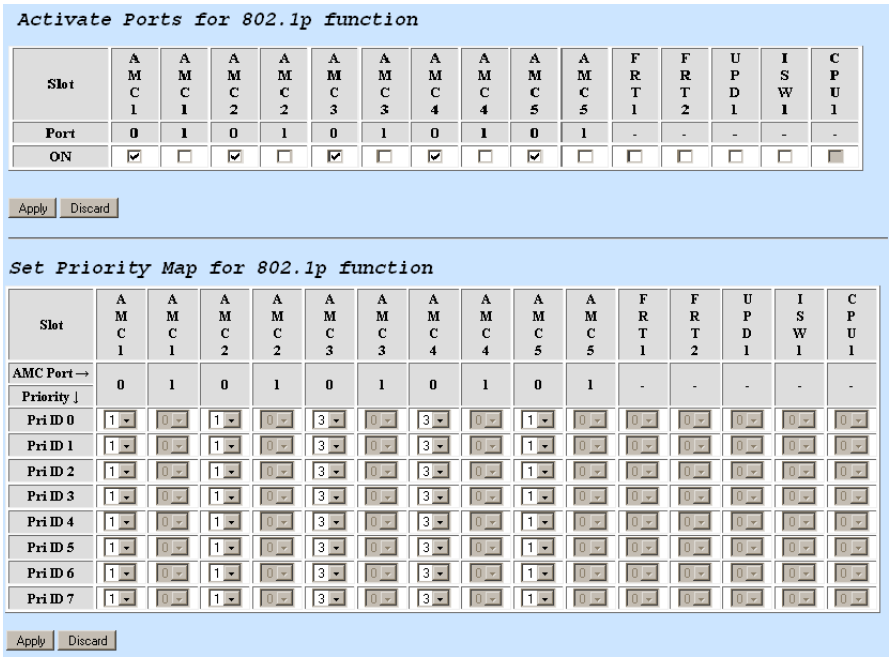


Figure 6-26 : Web based 802.1p Mapping

Before the priority ID mapping can be changed for a specific port the 802.1p mode has to be activated for that port via the table on the top of the page. To activate the 802.1 mode for a port set the checkbox for that port and press the <Apply> button.

The checkbox columns related to the port in the lower table will be activated and can be used to assign the used TX-Queue for a specific priority. To confirm the changes press the <Apply> button below the table.

6.10.3 Text Based Configuration

There are two configuration items available to configure the 802.1p mode.

`eth_802.1p_ini` – Activate/Deactivate 802.1p mode
`eth_802.1p_cm` – Set priority ID mapping

6.10.3.1 *Activate/Deactivate 802.1p Mode*

Description:

The `eth_802.1p_ini` configuration item can be used to activate the 802.1p mode. If this configuration item is set to "`deactivated`" or if the item is not present in the configuration file, all further configuration items related to 802.1p mode will be ignored.

Syntax:

```
eth_802.1p_ini  = FLAG
```

Parameter Description:

The parameters of the `<eth_802.1p_ini>` configuration item are described in *Table 8-22* on page 136.

Example:

Activate 802.1p mode.

```
eth_802.1p_ini  = 1
```

6.10.3.2 *Set 802.1p Ports*

Description:

The configuration item `<eth_802.1p_cm>` defines on which port(s) 802.1p mode is activated.

Syntax:

```
eth_802.1p_cm  = LIST_OF_ALIASES
```

Parameter Description:

The parameters of the `<eth_802.1p_cm>` configuration item are described in *Table* 8-23 on page*136.*

Example:

```
eth_802.1p_cm = AMC1/0, AMC2/0
```

The upper configuration item activates 802.1p priority at the ports `<AMC1/0>` and `<AMC2/0>`.

6.11 Port Mirroring

The Port Mirroring feature can be used to monitor the incoming (ingress) and/or outgoing (egress) traffic for specific ports. The traffic of the monitored ports will be directed to one switch port, the so-called mirror capture port.

Via so-called filtering rules it can be defined if the traffic of a port shall be mirrored and what kind of traffic will be mirrored in detail (ingress and/or egress). The mirror filtering rules consist of two filtering masks:

- <Port Mask for Ingress Traffic>
- <Port Mask for Egress Traffic>

Both filtering masks can be configured via the following menus and via text based configuration.

NOTE: The switch might not be able to forward all traffic to the mirror capture port if the traffic on the mirrored ports is higher than the data rate of the capture port.

6.11.1 CLI Based Configuration

The 'Port Mirroring menu' offers the commands to manipulate the settings of the Port Mirroring feature. To call the menu enter <mirr_cfg> at the prompt.

6.11.1.1 *Activate/Deactivate Port Mirroring*

The Port Mirroring options can only be changed if the mode has been activated. This can be done by choosing the menu item <activate port mirroring>. It can be deactivated again by choosing the menu item <deactivate port mirroring>.

6.11.1.2 *Set Capture port*

This menu item sets the general Port Mirroring options.

First, a capture port ID has to be specified:

```
Choose Port ID:
 |=============================================================================|
 |               AMCs                              Front     Up_C   ISw    CPU   |
 | AMC           0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
 | SLOTS         1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
 |-----------------------------------------------------------------------------|
 | AMC    from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
 | PORTS    to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
 |-----------------------------------------------------------------------------|
 | PORT          0  0  0  0  0  0  0  0  0  1      1  1      1      1      1 |
 | ID            1  2  3  4  5  6  7  8  9  0      1  2      3      4      5 |
or [a] - for All ports
     |>(RET=1/0x0): 0
```

6.11.1.3 *Set Default Configuration*

With this menu item, the current Port Mirroring settings can be replaced by the default Port Mirroring configuration.

6.11.1.4 *Set Monitored Ports (Ingress Traffic)*

The ingress mirror rule defines the ports of which the ingress traffic will mirrored to the capture port. The mirroring can either be set for all ports or for one specific port.

```
Choose Port ID:
 |=============================================================================|
 |               AMCs                              Front     Up_C   ISw    CPU   |
 | AMC           0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
 | SLOTS         1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
 |-----------------------------------------------------------------------------|
 | AMC    from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
 | PORTS    to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
 |-----------------------------------------------------------------------------|
 | PORT          0  0  0  0  0  0  0  0  0  1      1  1      1      1      1 |
 | ID            1  2  3  4  5  6  7  8  9  0      1  2      3      4      5 |
 or [a] - for All ports
 > (RET=a):
```

If the state of the mirroring mode should only be changed for one specific port, enter the port ID, otherwise enter <a> to set the mode for each used port. To enable the ingress mirroring, enter <1> for the specific port, to disable mirroring enter <0>:

```
[0] - don't monitor this port
[1] - monitor this port
```

6.11.1.5 *Set Monitored Ports (Egress Traffic)*

The egress mirror rule defines the ports of which the egress traffic will mirrored to the capture port. The mirroring can either be set for all ports or for one specific port.

```
Choose Port ID:
 |=========================================================================|
 |               AMCs                              Front     Up_C   ISw    CPU   |
 | AMC           0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
 | SLOTS         1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
 |-------------------------------------------------------------------------|
 | AMC    from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
 | PORTS    to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
 |-------------------------------------------------------------------------|
 | PORT          0  0  0  0  0  0  0  0  0  1      1  1      1      1      1 |
 | ID            1  2  3  4  5  6  7  8  9  0      1  2      3      4      5 |
  or [a] - for All ports
  > (RET=a):
```

If the state of the mirroring mode should only be changed for one specific port, enter the port ID, otherwise enter <a> to set the mode for each used port. To enable the egress mirroring, enter <1> for a specific port, to disable mirroring enter <0>:

```
[0] - don't monitor this port
[1] - monitor this port
```

6.11.1.6 *Show Port Mirroring Configuration*

If Port Mirroring mode has been activated, the current configuration can be shown via the `<show port mirroring configuration>` menu item:

```
Mirroring mode:.................. enabled
Capture port ID:..................  FRT_1

 Receive ports that are monitored
 [0]-not monitored, [1]-monitored


|=============================================================================|
|                         Ingress Mirror Port Map                             |
|=============================================================================|
|               AMCs                                Front     Up_C   ISw    CPU   |
| AMC           0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
| SLOTS         1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
|-----------------------------------------------------------------------------|
| AMC    from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
| PORTS    to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
|-----------------------------------------------------------------------------|
|               0  0  0  0  0  0  0  0  0  0      0  1      0      0      0 |
|=============================================================================|

      Transmit ports that are monitored
      [0]-not monitored, [1]-monitored
|=============================================================================|
|                         Egress Mirror Port Map                              |
|=============================================================================|
|               AMCs                                Front     Up_C   ISw    CPU   |
| AMC           0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
| SLOTS         1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
|-----------------------------------------------------------------------------|
| AMC    from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
| PORTS    to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
|-----------------------------------------------------------------------------|
|               0  0  0  0  0  0  0  0  0  0      0  0      0      0      0 |
|=============================================================================|
```

6.11.2 Web Based Configuration

To call the Port Mirroring web page select the <Port Mirroring> link at the navigation part of the browser window.

6.11.2.1 *Activate/Deactivate Port Mirroring Mode*

To activate the Port Mirroring mode click the <Activate> button on the Port Mirroring configuration web page. To deactivate the mode use the <Deactivate> button on the web page.

6.11.2.2 *Set Ingress and Egress Port Mirroring*

If the Port Mirroring mode has been enabled, the following form will be shown (*Figure 6-27*). To configure the functionality, the capture port has to be defined. It can be selected by the <Capture port> drop down menu. The shortcuts of the port names are described in chapter 3.

To enable/disable the mirroring on the certain port(s) use the according checkboxes. The row of the checkboxes defines the mirroring type. The <Ingress> row defines the mirroring of the inbound traffic; the <Egress> row controls the outbound traffic. To confirm the settings press the button <Apply> or <Discard> to cancel.

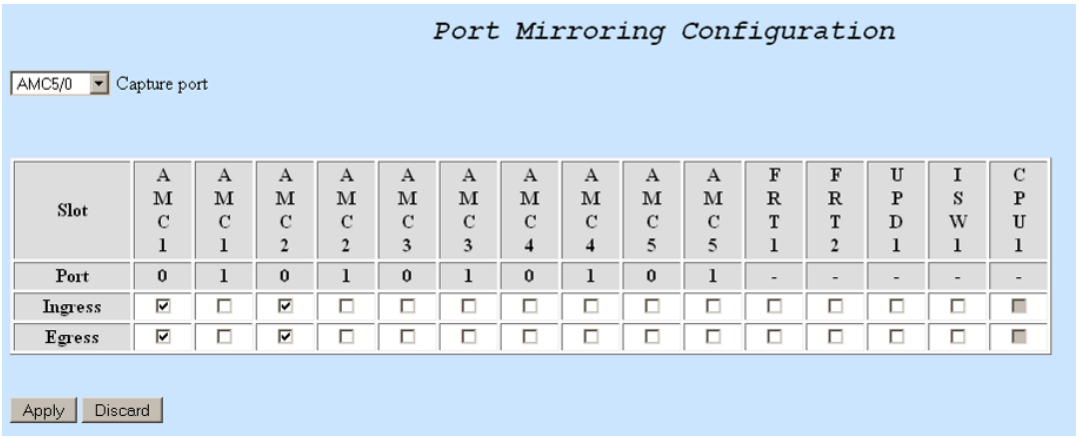


Figure 6-27: Port-Mirroring settings over web interface

The upper example (*Figure 6-27*) provides the mirroring of inbound traffic on the ports <AMC_1> und <AMC_2>.

6.11.3 Text Based Configuration

There are four configuration items available to configure Port Mirroring mode.

`eth_mirr_ini` – Activate/Deactivate Port Mirroring
`eth_mirr_capt` – General settings of Port Mirroring
`eth_mirr_icm` – Ingress traffic mirroring rule
`eth_mirr_ecm` – Egress traffic mirroring rule

6.11.3.1 *Activate/Deactivate Port Mirroring*

Description:

The `eth_mirr_ini` configuration item can be used to activate the Port Mirroring feature. If this configuration item is set to `"deactivated"` or if the item is not present in the configuration file, all further configuration items related to Port Mirroring will be ignored.

Syntax:

```
eth_mirr_ini  = FLAG
```

Parameter Description:

The parameters of the `<eth_mirr_ini>` configuration item are described in *Table 8-24* on page *137.*

Example:

Activate port mirroring:

```
eth_mirr_ini  = 1
```

6.11.3.2 *Set Capture port*

Description:

The configuration item `<eth_mirr_capt>` can be used to specify the mirroring capture port and if non-mirror traffic to this port shall be allowed.

Syntax:

```
eth_mirr_capt  = PORT_CPT
```

Parameter Description:

The parameters of the `<eth_mirr_capt>` configuration item are described in *Table 8-25* on page *137*.

Example:

```
eth_mirr_capt   = FRT_1
```

The example shows a configuration item that sets the port `FRT_1` as a capture port.

6.11.3.3 *Set Monitored Ports (Ingress Traffic)*

Description:

The `<eth_mirr_icm>` configuration item can be used to set the ingress mirroring rule.

Syntax:

```
eth_mirr_icm  = LIST_OF_ALIASES
```

Parameter Description:

The parameters of <eth_mirr_icm> configuration item are described in *Table 8-26* page *137.*

Example:

```
eth_mirr_icm  = AMC2/0, AMC3/0
```

The upper configuration item allows the mirroring of ingress traffic at the ports <AMC2/0> and <AMC3/0>.

6.11.3.4 *Set Monitored Ports (Egress Traffic)*

Description:

The <eth_mirr_ecm> configuration item can be used to set the egress-mirroring rule.

Syntax:

```
eth_mirr_ecm  = LIST_OF_ALIASES
```

Parameter Description:

The parameters of the <eth_mirr_ecm> configuration item are described in *Table* 8-27 on page *138.*

Syntax:

```
eth_mirr_ecm  = AMC12/0
```

The upper configuration item allows the mirroring of egress traffic at the port <AMC12/0>.

6.12 Jumbo Frame Forwarding

The Ethernet switches can receive and transmit Ethernet frames of extended length on ports linked on 1 Gigabit and 10 Gigabit speed. Referred to as Jumbo Frames, these packets may be longer than 1518 byte (when untagged). The maximum supported frame size ranges from 9kB to 16kB and can be different depending on the switch device type. This feature can be enabled on each port individually.

NOTE: Jumbo frames consume larger blocks of Gigabit switch buffer memory. Thus it is strongly recommended, to set a port to Jumbo enable mode only if necessary and - to ensure system performance – not to enable more than two ports of the Gigabit switch simultaneously.

6.12.1 CLI Based Configuration

6.12.1.1 *Activate/Deactivate Jumbo Frame Forwarding Mode*

The Jumbo Frames Forwarding options can only be changed if the mode has been activated. This can be done by choosing the menu item `<activate jumbo mode>`. The Jumbo Frame Forwarding can be deactivated again by choosing the menu item `<deactivate jumbo mode>`.

6.12.1.2 *Set Jumbo Ports*

The Jumbo Frame Forwarding mode can either be set for all ports or for one specific port.

```
Choose Port ID:
 |=========================================================================|
 |               AMCs                              Front     Up_C   ISw    CPU   |
 | AMC           0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
 | SLOTS         1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
 |-------------------------------------------------------------------------|
 | AMC    from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
 | PORTS    to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
 |-------------------------------------------------------------------------|
 | PORT          0  0  0  0  0  0  0  0  0  1      1  1      1      1      1 |
 | ID            1  2  3  4  5  6  7  8  9  0      1  2      3      4      5 |
  or [a] - for All ports
  > (RET=a):
```

If the state of the Jumbo Frame Forwarding mode shall only be changed for one specific port, enter the port ID, otherwise enter `<a>` to set the mode for each used port. As different switches support different Jumbo sizes, the information about possible options is given as follows:

```
-----------------------------------------
 The switch supports the following
 JUMBO frame sizes:
-----------------------------------------
  Size   | Size ID
 --------|--------
   OFF   |   0
    9K   |   9
   -----|---
   10K   |  10
 --------|--------
```

NOTE: Currently, NAT-MCH does not support Jumbo frames on CPU port.

Use the "`Size ID`" to set the necessary Jumbo state for the certain port.

6.12.2 Web Based Configuration

To call the Jumbo Frame page select the <Jumbo Frame> link at the navigation part of the browser window.

6.12.2.1 *Activate/Deactivate Jumbo Frame Mode*

To activate the Jumbo Frame mode click the <Activate> button on the jumbo frame configuration web page. To deactivate the mode use the <Deactivate> button on the web page.

6.12.2.2 *Set Jumbo Frame Mode on Port*

If the Jumbo Frame mode has been enabled, the functionality can be activated on the certain port of the switch.

To configure the Jumbo Frames transmission on the certain port(s) use the according checkboxes as it is shown on the *Figure 6-28*. To confirm the settings press the button <Apply>, <Discard> to cancel, <Deactivate> to disable Jumbo frame functionality.

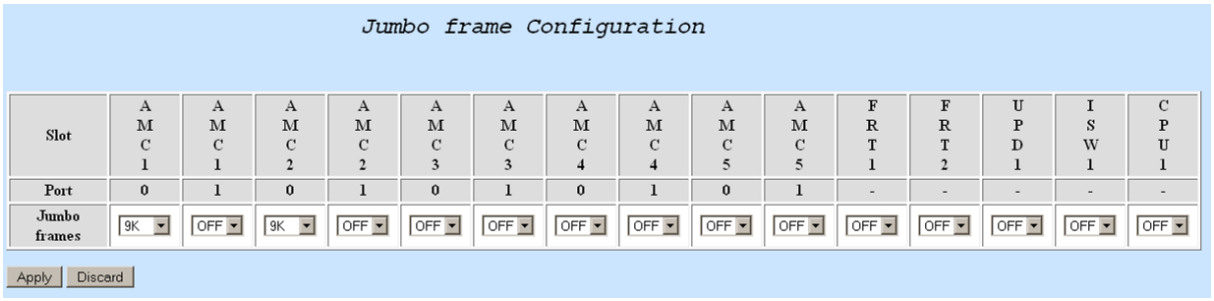


Figure 6-28: Jumbo Frame settings over web interface

The upper example enables the Jumbo Frame transmission on the port <AMC1/0> and <AMC2/0>.

6.12.3 Text Based Configuration

There are two configuration items available to configure the Jumbo Frame mode.

`eth_jumbo_ini` – Activates/Deactivates Jumbo mode
`eth_jumbo_size` – Defines the frame size

6.12.3.1 *Activate/Deactivate Jumbo Frame Mode*

Description:

The <`eth_jumbo_ini`> configuration item can be used to activate the Jumbo Frame Forwarding. If this configuration item is set to "`deactivated`" or if the item is not present in the configuration file, all further configuration items related to the Jumbo Frame mode will be ignored.

Syntax:

```
eth_jumbo_ini = FLAG
```

Parameter Description:

The parameters of the <`eth_jumbo_ini`> configuration item are described in *chapter 8.12* on the page *139.*

Example:

Activate Jumbo Frame Forwarding:

```
eth_jumbo_ini = 1
```

6.12.3.2 *Set the frame size*

Description:

The configuration item <`eth_jumbo_size`> defines the frame size on the port.

Syntax:

```
eth_jumbo_size = ALIAS, JMB_SIZE
```

Parameter Description:

The parameters of the <`eth_jumbo_size`> configuration item are described in *chapter 139* on the page *139.*

Example:

```
eth_jumbo_size = 5,10;
```

The upper configuration item activates Jumbo mode at the port `AMC 6` and sets the maximal frame size to `10K`.

```
eth_jumbo_size =  6,  0;
```

The upper configuration item deactivates Jumbo mode at the port `AMC  7` and sets the normal maximal frame size.

6.13 Link Aggregation

The Link Aggregation feature allows more than one port to be grouped together as a single link connection between two switch devices. This increases the effective bandwidth through a link and provides redundancy. The switch used on the NAT-MCH allows up to four aggregation groups, with each group consisting of two to eight physical ports. There are no restrictions in the membership in any aggregation group, like as sequential order of link ports. However, the ports within a Link Aggregation group cannot overlap the ports of another group. By performing a dynamic hashing algorithm based on the MAC addresses, each packet destined to the aggregation group is forwarded to one of the valid ports within this group. This allows a seamless, automatic redundancy scheme. The hashing function can be performed either on the MAC Destination Address (DA), MAC Source Address (SA) or the mixed Destination/Source Address (DA/SA), depending on the user's choice.

The protocol configuration of the ports within an aggregation group has to be the same for all ports. This is handled by the MCH-Software as described in the following example:

For instance, port < AMC1/0> and < AMC5/1> are enabled for frame checking in the 802.1X configuration:

```
|=============================================================================|
|                              802.1X Security Port Map                       |
|=============================================================================|
|               AMCs                                Front     Up_C   ISw    CPU   |
| AMC           0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
| SLOTS         1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
|-----------------------------------------------------------------------------|
| AMC    from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
| PORTS    to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
|-----------------------------------------------------------------------------|
|               1  0  0  0  0  0  0  0  0  1     0  0       0      0 ..   0 |
|=============================================================================|
```

Now the Link Aggregation mode is activated and the ports <AMC1/0>, <AMC2/0> and <AMC2/1> are added to the aggregation group <3>. In this case, three ports of the same aggregation group have different 802.1X related settings. The MCH-Software handles this in the following way:

1. Determine the Link Aggregation Master Port (LAG-Master). The LAG-Master is the port within an aggregation group, which is located on the leftmost position within the aggregation membership vector. This port defines the setting for all ports of the group. In this example, the LAG-Master is the port <AMC 1> for the aggregation group <3>.

2. Apply the setting of the LAG-Master to all ports within the aggregation group. In this example, the states of the ports <AMC 3> and <AMC 4> will be changed automatically from the state <0> to <1>. As a result, the configuration of the 802.1X ports will be changed as follows:

```
|=========================================================================|
|                              802.1X Security Port Map                   |
|=========================================================================|
|              AMCs                              Front     Up_C   ISw    CPU   |
| AMC          0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
| SLOTS        1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
|-------------------------------------------------------------------------|
| AMC    from: 0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
| PORTS    to: .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
|-------------------------------------------------------------------------|
| LAG Gr.      3  .  3  3  .  .  .  .  .  .      .  .      .      .      . |
|=========================================================================|
|              1  0  1  1  0  0  0  0  0  1     0  0       0      0 ..   0 |
```

The row <LAG Gr.> shows, which ports are member of which aggregation group.

6.13.1 CLI Based Configuration

The '(submenu) Link Aggregation' offers the commands to manipulate the settings of the Link Aggregation mode.

6.13.1.1 *Activate/Deactivate Link Aggregation Mode*

The options of the Link Aggregation can only be changed if the mode has been enabled. This can be done by choosing the menu item <enable link aggregation> from the submenu.

The Link Aggregation mode can be disabled by choosing the menu item <disable link aggregation>.

6.13.1.2 *Set Hashing Mode*

With this menu item, the hashing mode can be configured to route outbound frames within the aggregation group. To set the required hashing mode, choose the dialog item <set hashing mode>.

Then select a hashing mode (page 90)

```
        [1] - DA^SA
        [2] - DA
        [3] - SA
    Enter hashing mode > (RET=0/0x0)
```

and press <Enter>; the change will be assumed.

6.13.1.3 *Set Members of an Aggregation Group*

As previously described, the switch allows up to four aggregation groups. With this dialog item, the aggregation groups can be customized.

As a first step, the aggregation group has to be chosen.

```
    Enter Group ID [0-3]
```

Then the ports have to entered that should be added to the aggregation group.

```
Choose Port ID:
 |=============================================================================|
 |               AMCs                                Front     Up_C   ISw    CPU   |
 | AMC           0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
 | SLOTS         1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
 |-----------------------------------------------------------------------------|
 | AMC    from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
 | PORTS    to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
 |-----------------------------------------------------------------------------|
 | PORT          0  0  0  0  0  0  0  0  0  1      1  1      1      1      1 |
 | ID            1  2  3  4  5  6  7  8  9  0      1  2      3      4      5 |
  or [a] - for All ports
  > (RET=a):
```

If only one specific port is to be added/removed, enter the port ID, otherwise enter <a> to set the membership state for each port. To add a port to an aggregation group, enter <1>, and otherwise enter <0> for removal:

6.13.1.4 *Show Configuration*

With this menu item, the memberships of all aggregation groups are shown.

```
                  THE LINK AGGREGATION CONFIGURATION

  Hashing mode: ... DA^SA
 |=============================================================================|
 |                              Link Aggreration Groups                        |
 |=============================================================================|
 |               AMCs                                Front     Up_C   ISw    CPU   |
 | AMC           0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
 | SLOTS         1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
 |-----------------------------------------------------------------------------|
 | AMC    from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
 | PORTS    to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
 |-----------------------------------------------------------------------------|
 |Group ID                                                                     |
 |     0    :    0  0  0  0  0  0  1  1  0  0      0  1      0 .    0      0 |
 |-----------------------------------------------------------------------------|
 |     1    :    0  0  0  0  0  0  0  0  0  0      0  0      0      0      0 |
 |-----------------------------------------------------------------------------|
 |     2    :    0  0  0  0  0  0  0  0  0  0      0  0      0      0      0 |
 |-----------------------------------------------------------------------------|
 |     3    :    0  0  0  0  0  0  0  0  0  0      0  0      0      0      0 |
 |=============================================================================|
```

6.13.1.5 *Set default configuration*

Choosing this menu item resets the Link Aggregation settings to default, means all ports will be removed from all membership groups. To set the default configuration of Link Aggregation, select dialog item <set default configuration>.

6.13.2 Web Based Configuration

To call the Link Aggregation page select the <Link Aggregation> link at the navigation part of the browser window.

6.13.2.1 *Activate/Deactivate Link Aggregation Mode*

To activate the Link Aggregation mode click the <Activate> button on the Link Aggregation web page. To deactivate the mode use the <Deactivate> button on the web page.

6.13.2.2 *Set Hashing Mode and Members of Aggregation Group*

If the Link Aggregation mode has been enabled, ports can be combined to an aggregation group. Up to four aggregations group can be set as it is shown at the *Figure 6-2*.

At first, the hashing mode has to be set: one of three hashing modes can be selected by the drop down menu.

To aggregate the port to the group use the checkboxes of the required ports at one of four groups. To confirm the settings press the button <Apply> or <Discard> to cancel.

The button <Deactivate> is used to disable the Link Aggregation mode and to deny the access to the feature settings.

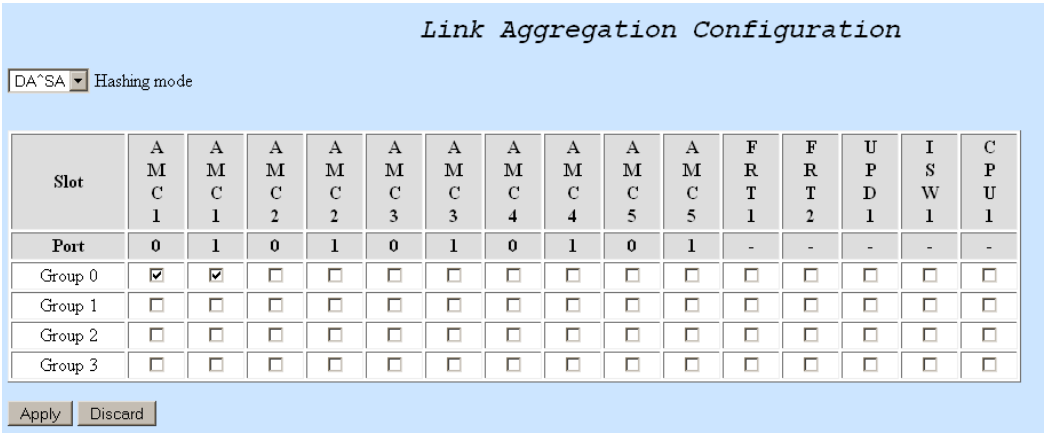
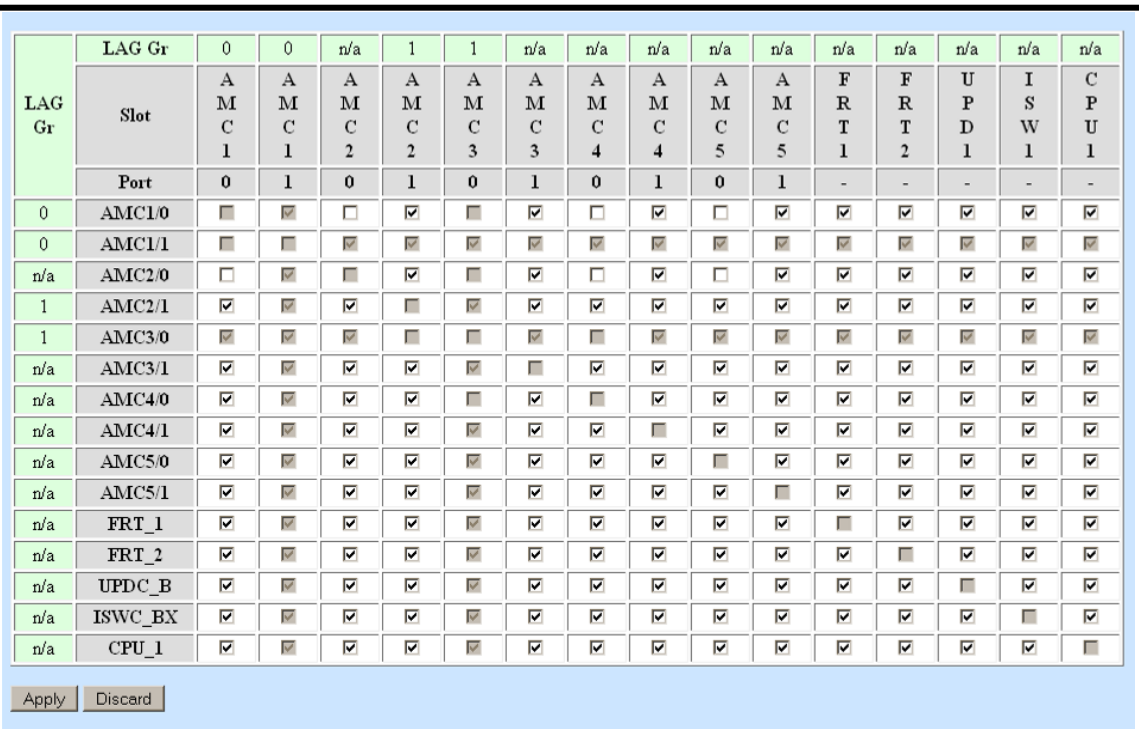


Figure 6-29: Link Aggregation settings over web interface

The upper example combines the port <AMC1/0> and <AMC1/1> to the link aggregation group <0>.

6.13.2.3 *Additional Link Aggregation Information*

The Link Aggregation has effect on all port related settings for all protocols. For this reason, the information about the port assignment to the aggregation group is present at all other features if the Link Aggregation mode is enabled. The following figure shows the web interface of the Port Based VLAN in case the Link Aggregation mode has been activated.



LAG Gr	LAG Gr	0	0	n/a	1	1	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
	Slot	AMC1	AMC1	AMC2	AMC2	AMC3	AMC3	AMC4	AMC4	AMC5	AMC5	FRT1	FRT2	UPD1	ISW1	CPU1
	Port	0	1	0	1	0	1	0	1	0	1	-	-	-	-	-
0	AMC1/0	☐	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	☑	☑	☑	☑
0	AMC1/1	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
n/a	AMC2/0	☐	☑	☐	☑	☐	☑	☐	☑	☐	☑	☑	☑	☑	☑	☑
1	AMC2/1	☑	☑	☑	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
1	AMC3/0	☑	☑	☑	☐	☐	☑	☐	☑	☑	☑	☑	☑	☑	☑	☑
n/a	AMC3/1	☑	☑	☑	☑	☑	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑
n/a	AMC4/0	☑	☑	☑	☑	☐	☑	☐	☑	☑	☑	☑	☑	☑	☑	☑
n/a	AMC4/1	☑	☑	☑	☑	☑	☑	☑	☐	☑	☑	☑	☑	☑	☑	☑
n/a	AMC5/0	☑	☑	☑	☑	☑	☑	☑	☑	☐	☑	☑	☑	☑	☑	☑
n/a	AMC5/1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☑	☑	☑	☑	☑
n/a	FRT_1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☑	☑	☑	☑
n/a	FRT_2	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☑	☑	☑
n/a	UPDC_B	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☑	☑
n/a	ISWC_BX	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐	☑
n/a	CPU_1	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☐

Apply Discard

Figure 6-30: addition information over web interface

As shown in the figure above all settings of the slave ports within the aggregation group are indicated as inactive. The values of these inactive settings change automatically if the value of the master port is modified.

6.13.3 Text Based Configuration

There are three configuration items available to configure the Link Aggregation mode.

`eth_lag_ini` – Activate/Deactivate the Link Aggregation mode
`eth_lag_hash` – Hashing of the Link Aggregation
`eth_lag_gr_cm` – Port-Membership of the certain aggregation group
– Port-Membership of the certain aggregation group

6.13.3.1 *Activate/Deactivate Link Aggregation Mode*

Description:

The <`eth_lag_ini`> configuration item can be used to activate the Link Aggregation mode. If this configuration item is set to "`deactivated`" or if the item is not present in the configuration file, all further configuration items related to the Link Aggregation will be ignored.

Syntax:

```
eth_lag_ini  = FLAG
```

Parameter Description:

The parameters of the <`eth_lag_ini`> configuration item are described in *the Table 8-30* on the *page 140*.

6.13.3.2 *Set Hashing Mode*

Description:

The configuration item <`eth_lag_hash`> defines the hashing mode to route the outbound frames wihtin an aggregation group.

Syntax:

```
eth_lag_hash  = LAG_HM
```

Parameter Description:

The parameters of the <`eth_lag_hash`> configuration item are described in Table 8-31 on the page 140.

Example:

```
eth_lag_hash   = 1
```

This configuration forces the switch to generate the hash key based on the destination address of frames routed to the ports that are member of an aggregation group.

6.13.3.3 *Set Link Propagation Mode on LAG (HUB-XAUI FM4000 only)*

The Propagation Link Mode on LAG specifies a mode for the *Link Propagation*, if a LAG represents a *propagation master*. There are two modes available:

- *Link is Existing*
- *Link has Full Width*

The mode defines what link status of LAG triggers the *Link Propagation*.

The "*Link is Existing*" mode does not trigger the Link Propagation functionality so long as LAG has a link. *propagation slave* port(s) become(s) "disabled" when all ports inside of LAG (*propagation master*) lost the links. As soon as any port inside of LAG becomes a link again, all slave port of appropriated *propagation chain* becomes an "enabled" state.

The "*Link has Full Width*" mode keeps *propagation slave* port(s) on "enabled" state so long as a link of a LAG has a full width. *propagation slave* port(s) become(s) "disabled", when one or more ports inside of LAG (*propagation master*) lost the links. As soon as all port inside of LAG have a link again, slave port of appropriated *propagation chain* becomes an "enabled" state.

Please use the "*Link has Full Width*" mode very carefully, because the reducing of link with on LAG triggers the Link Propagation and sets *propagation slave* port(s) to "disabled", but the LAG has still a link and can forward packets!

Description:

The configuration item `<eth_lag_propag>` defines a mode for Link Propagation mode if propagation master is a LAG (for all such *propagation chains*).

Syntax:

```
eth_lag_propag = LAG_PM
```

Parameter Description:

Table 8-33 on the *page 141* describes the parameters of the `<eth_lag_propag>` configuration item are described in *Table 8-33* on the *page 141.*

Example:

```
eth_lag_propag   = 0
```

This configuration item sets the "*Link is Existing*" mode for all *propagation chains* if *propagation master* is represented by an aggregation group.

6.13.3.4 *Set Member of Aggregation Group*

Description:

The `<eth_lag_gr_cm>` configuration item is used to specify the forwarding port map for a specific source port.

Syntax:

```
eth_lag_gr_cm  = LAG_GR, LIST_OF_ALIASES
```

Parameter Description:

The <eth_lag_gr_cm> configuration item consists of an aggregation group ID and six parameters, which specify the port membership according to the description in chapter *Table* 8-32*.* Bit values related to reserved ports are ignored and set to the default value. The parameters are described in *Table* 8-32 on the page *141.*

Example:

```
eth_lag_gr_cm = 0,   <FRT_1>, <FRT_2>
eth_lag_gr_cm = 1,   <AMC1/0>, <AMC2/0>
```

This configuration assigns <FRT_1> and <FRT_2> to the aggregation group <0> and <AMC1/0> and <AMC2/0> to the group <1>. The switch handles the ports <FRT_1>, <FRT_2> and <AMC1/0>, <AMC/0> as two single link connections.

6.14 Rapid Spanning Tree Protocol

The *Spanning Tree Protocol* (STP) is a network protocol that provides a loop avoiding network topology for any bridged Ethernet LAN. The basic function of STP is to prevent bridge loops and ensuing broadcast radiation. Spanning tree also allows a network design to use redundant links to provide backup paths, if an active link fails.

The *Rapid Spanning Tree Protocol* (RSTP) provides significantly faster spanning tree convergence after a topology change. RSTP was designed to be backwards-compatible with standard STP.

To ensure that each bridge has enough information about another, the bridges use special messages called *Bridge Protocol Data Units* (BPDUs) to exchange information about bridge IDs, root path costs etc. A bridge shares BPDUs via Ethernet frames that contain the reserved MAC address 01:80:C2:00:00:00 in the destination field.

The firmware supports a user interface for the RSTP with Multi-Instance and Single-Instance functionalities. Therefore, you can configure particular RSTP instances via the command line or the web interface and backup your settings.

6.14.1 Single-Instance Mode: “Ignore VLAN ID”

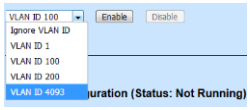
The NAT-MCH provides “*VLAN ignore*” option. In this case, the 802.1Q VLAN is irrelevant for a switch configuration. Please, enable this option to make no difference what VLAN information contains in a BPDU frame. In this case, all received frame have to be processed by the same RSTP Instance. The selecting of this mode make a using of another RSTP unavailable.

6.14.2 Multi-Instance Mode

The NAT-MCH supports up to two RSTP instances on the Base-MCH. Because a RSTP instance runs on a VLAN Group, add first *802.1Q VLAN* groups for the future RSTP instances (e.g. Group 100 and Group 200). To make your MCH available over the new VLAN, add, "Default VLAN Tag" on the CPU port too (e.g. to VLAN 100).

NOTE:
Please, note that the BPDU frames from your external switch must contain a VLAN tag. The absence of the VLAN information corrupts communication between switches. If your external switch sends the BPDU frames without a VLAN Tag, you have to add it at the receiving side on the MCH (see *6.7.2.7*).

NOTE:
Please, **does not select** VLAN 4093 (VLAN tunnel) to initialize new RSTP instance. It is currently available for selecting, but will be removed with next NAT-MCH firmware released.



The selecting of this VLAN Group could lead to unpredictable results!

6.14.3 Instance Membership

The user has to add switch port to RSTP instance from assigned VLAN group. These ports form *instance membership*. The instance membership represents switch ports that take an active part in protocol convergence and conversation.

The user interface of RSTP forbids overlapping between memberships of different instances, although 802.1Q VLAN allows it. This way, the ports are protected from duplicated controlling of two different RSTP instances.

6.14.4 CLI Based Configuration

The `'(submenu) RSTP'` offers the commands to manipulate the settings of the Rapid Spanning Tree mode.

6.14.4.1 *Activate/Deactivate Spanning Tree Protocol*

The options of the Rapid Spanning Tree can only be changed if the mode has been enabled. This can be done by choosing

Please, use the menu item `<enable RSTP>` to enable new RSTP instance. Then enter VLAN group ID or “VLAN Ignore” option, bridge priority and member ports of new RSTP instance.

The RSTP instance can be disabled by choosing the menu item `<disable RSTP>`.

After the activation, the bridge and port are initialized with default configuration. The bridge exchanges information, computes the current topology and avoids loops. To define the reaction on network topology changing, the bridge and port configuration has to be set manually.

6.14.4.2 *Configure Bridge Parameters*

With this menu item, the main parameters of the bridge can be configured for the Rapid Spanning Tree Protocol.

Enter the `<configure bridge>` and select appropriated VLAN group. Then set *Bridge Priority*. from 0 to 61440 in steps of 4096; if the step is not exactly 4096, it will be rounded automatically.

The *Hello Time* has to be entered, which means the time between each bridge BPDU that is sent to a port. This time is set to 2 seconds (sec) by default, but it can be tuned in a range between 1 and 2 sec.

NOTE: This parameter should be changed if mandatory only.

The Max Age value needs to be set: the Max Age timer controls the maximal time that passes before a bridge port saves its configuration BPDU information. This time is 15 sec by default, but can be tuned in a range between 6 and 40 sec.

The Forward Delay value needs to be entered. It defines the time that is spent in the listening and learning state. This time is equal to 15 sec by default, but can be varied between 4 and 30 sec.

Finally, the dialog requests an instance membership (see *page 99*). It is recommended to set port automatically:

```
RSTP Member Port:
   [y] - port is RSTP member
   [n] - port isn't RSTP member
AMC1/0[y]/[n]>(RET=y)
```

The instance membership can be defined in the submenu Attach Port.

6.14.4.3 *Configure Port Parameters*

At first, enter VLAN ID of RSTP instance and the port ID, which is to be configured:

```
Choose Port ID:
|=============================================================================|
|                AMCs                              Front     Up_C   ISw    CPU   |
| AMC            0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
| SLOTS          1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
|-----------------------------------------------------------------------------|
| AMC     from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
| PORTS     to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
|-----------------------------------------------------------------------------|
|-----------------------------------------------------------------------------|
| PORT           0  0  0  0  0  0  0  0  0  1      1  1      1      1      1 |
| ID             1  2  3  4  5  6  7  8  9  0      1  2      3      4      5 |
> (RET=0/0x0): 5
```

Then the Port Priority and Path Cost have to be configured:

```
Enter <Port Priority>[0..240] in steps of 16 (RET=128/0x80): 0
Enter admin Port <Path Cost> [1..200 000 000] (RET=0/0x0): 1
```

Both parameters are used to determine the current state of the interface and can effect current LAN topology.

Path Cost: This parameter assigns how the *local switch* elects the root port. Cost is cumulative throughout the STP domain, the higher cost is the less preferred.

Port Priority: This parameter affects how the *downstream switch* elects its root port. This is only significant locally between the two directly connected switches, higher priority is less preferred.

AdminPointToPointMAC specifies whether this port is connected to a shared LAN segment or a point-to-point LAN segment. A point-to-point LAN segment is connected to exactly one other bridge, typically with a direct cable in between. Only point-to-point links and edge ports can rapid transition to forwarding state.

If this field is set to Auto, the switch automatically detects whether the port is connected to a shared link or a point-to-point link. Ports operating in half duplex are set to False, and ports operating in full duplex are set to True. However, the type of link can be set manually; options are:

- `ForceTrue` - Defines the port as connected to a point-to-point link.
- `ForceFalse` - Defines the port as connected to a shared LAN segment.
- `Auto` - Automatically detects whether the port is connected to a shared link or a point-to-point link.

```
Enter <adminPointToPointMAC>
  [t] - ForceTrue
  [f] - ForceFalse
  [a] - Auto
>  (RET=a): a
```

AdminEdgePort specifies whether this port is an edge port or a non-edge port. An edge port is not connected to any other bridge. Only edge ports and point-to-point links can rapid transition to forwarding state; options are:

- True - Defines the port as an edge port.
- False- Defines the port as a non-edge port.

```
Enter adminEdgePort
  [t] - True
  [f] - False
Enter <adminEdgePort>  (RET=t):
```

The Admin Non STP – Status indicates whether the port includes the STP mathematic calculation.

- True- Port does not include feature
- False- Port includes feature

```
STP Enter <admin non stp>  (RET=f):
```

6.14.4.4 *Attach Port*

With this menu item, the user can add/remove particular port to/from instance membership:

```
Choose Port ID:
|=============================================================================|
|                AMCs                          Front     Up_C   ISw    CPU    |
| AMC            0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
| SLOTS          1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
|-----------------------------------------------------------------------------|
| AMC     from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
| PORTS     to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
|-----------------------------------------------------------------------------|
|-----------------------------------------------------------------------------|
| PORT           0  0  0  0  0  0  0  0  0  1      1  1      1      1      1 |
| ID             1  2  3  4  5  6  7  8  9  0      1  2      3      4      5 |
> (RET=0/0x0): 5
[d] - disabled RSTP
[e] - enabled RSTP
[q] - no change
Enter port state (RET=e):
```

This utility is designed for software diagnostic purpose, it shall be changed if necessary only.

6.14.4.5 *Show Brief*

This submenu item shows all settings of the bridge and of the all port instance.

```
Bridge Configuration:
......Bridge Priority:....32768
......Hello Time:.........2
......Max Age:............20
......Forwarding delay:...15

Port Configuration: AMC1/0(ID=0)
      Port Priority:.........128
      Path Cost:.............0
      adminPointToPointMAC:..Auto
      admin_non_stp:.........false

Port Configuration: AMC1/1(ID=1)
      Port Priority:.........128
      Path Cost:.............0
      adminPointToPointMAC:..Auto
      admin_non_stp:.........false
```

etc…

6.14.4.6 *Show Instance Status*

This submenu item shows current state of RSTP state machine on particular RSTP instance:

```
=== State machine: VLAN 100 ===
BrId:
     prio             -  61436
     addr             -  00 40 42 0b 10 e8

BrTimes:
     MessageAge       -  0
…
rootPrio :
     root_bridge
         prio         -  61436
         addr         -  00 40 42 0b 10 e8
     root_path_cost   -  0
…
    port_name          -  UPDC_B
    port_id            -  256
    role               -  DisabledPort
    selectedRole       -  DisabledPort
    forward/forwarding -  0/0
    learn/learning     -  0/0
    proposed/proposing -  0/0
    adminPCost         -  20000
    operPCost          -  20000
    operSpeed          -  1000
….
```

This utility can be use to check the RSTP configuration of NAT-MCH relating another networking hardware.

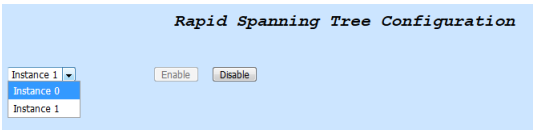
6.14.4.7 *Show Port States*

This submenu item shows the current Spanning Tree State of all ports summarized in the table as it follows:

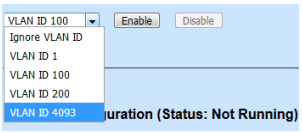
```
|=============================================================================|
|                              STP Port State                                 |
|=============================================================================|
|                   AMCs                                Front     Up_C   ISw    CPU   |
|                   0  0  0  0  0  0  0  0  0  0|     0  0|     0|     0|     0 |
|                   1  1  2  2  3  3  4  4  5  5|     1  2|     1|     1|     1 |
|-----------------------------------------------------------------------------|
| AMC        from:  0  1  0  1  0  1  0  1  0  1      .  .      .      .      . |
| PORTS        to:  .  .  .  .  .  .  .  .  .  .      .  .      .      .      . |
|-----------------------------------------------------------------------------|
|log 100            X  X  X  X  F  F  D  D  X  X      F  d      F      d      X |
|log 200            F  D  D  D  X  X  X  X  X  X      F  d      F      d      X |
|physical           F  D  D  D  F  D  D  D  N  N      F  d      F      d      N |
|=============================================================================|
  Legend:
     [N]- NON STP
     [D]- DISCARDING
     [d]- DISABLED
     [L]- LEARNING
     [F]- FORWARDING
     [X]- Not Instance Member
```

6.14.5 Web Based Configuration

To call the Rapid Spanning Tree Protocol Settings page select the <RSTP> link at the navigation part of the browser window. Then select RSTP instance (0 or 1) that is to be enabled.



Finally, chose appropriated VLAN group or "Ignore VLAN ID" option.



NOTE:
Please, **does not select** VLAN 4093 (VLAN tunnel) to initialize new RSTP instance. It is currently available for selecting, but will be removed with next NAT-MCH firmware released.
The selecting of this VLAN Group could lead to unpredictable results!

The protocol configuration consists of two parts "Bridge Configuration" and "Port Configuration".

6.14.5.1 *Bridge Configuration*

The upper part provides the configuration applied for generally switch configuration: Bridge Priority, Hello Time, Max Age, and Forwarding Delay and initialization of BPDU Filtering (*Chapter 6.15*).

6.14.5.2 *Port Configuration*

The second part (bottom) defines configuration of ports that from Instance Membership. The ports that are not from appropriated VLAN group are shown grayed with the text "Not in VLAN" and can not be attached to RSTP instance. The web interface offers for other ports following options:

- Instance Membership
- Port Priority
- Port Path Cost
- PointToPointMAC
- AdminEdgePort
- BPDU Filtering

that are applicable on the particular port.

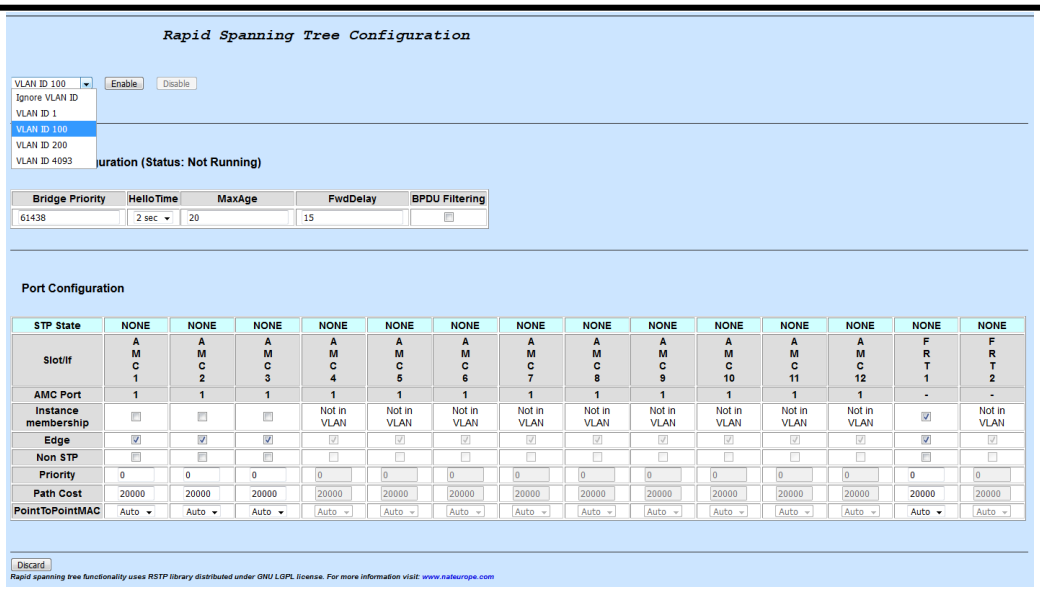


Figure 6-31: Rapid Spanning Tree - Settings

To confirm the settings press the button `<Apply>` or `<Discard>` to cancel not applied changes. To disable the protocol instance, use the button `<Deactivate>`.

6.14.6 Text Based Configuration

There are three configuration items available to configure the Rapid Spanning Tree Protocol settings.

`eth_rstp_ini`	– Activate/Deactivate the RSTP on particular instance
`eth_rstp_vid`	- Set assignment of RSTP instance to VLAN group
`eth_rstp_bridge`	– Bridge configuration for the Rapid Spanning Tree Protocol
`eth_rstp_port_e`	– Port configuration for the Rapid Spanning Tree Protocol

6.14.6.1 *Activate/Deactivate Rapid Spanning Tree Protocol*

Description:

The `'eth_rstp_ini'` configuration item can be used to activate the Rapid Spanning Tree Protocol on particular instance. If this configuration item is set to `"deactivated"` or if the item is not present in the configuration file, all further configuration items related to the RSTP will be ignored.

Syntax:

```
eth_rstp_ini  = INST_N, FLAG
```

Parameter Description:

The parameters represent Instance ID {0|1} and Initialization Flag {enabled:0|disabled:1}. The parameters of the <`eth_rstp_ini`> configuration item are described in *Table 8-34* on page *142*.

6.14.6.2 *Assign to VLAN group*

Description:

The `'eth_rstp_vid'` configuration item assigns an instance of Rapid Spanning Tree Protocol to particular VLAN group. If this configuration item `'eth_rstp_ini'` is set to `"enabled"`, but `'eth_rstp_vid'` is absent, than it could lead to unpredictable results.

Syntax:

```
eth_rstp_vid    =   INST_N,     VLANID
```

Parameter Description:

The parameters represent Instance ID {0|1} and assigned VLAN group. The `<0> of VLANID` represents option "Ignore VLAN"(see page 98) The parameters of the <`eth_rstp_vid`> configuration item are described in *Table 8-34* on page *142*.

6.14.6.3 *Set Bridge Configuration*

Description:

The `<eth_rstp_bridge>` configuration item is used to specify the generic Bridge configuration of the Rapid STP.

Syntax:

```
eth_rstp_bridge = INST_N, BRG_PRI, HELLO_T, MAX_AGE, FWD_DELAY
```

Parameter Description:

The parameters represent Bridge Priority, Hello Time, Max Age and Forward Delay Time

The <eth_rstp_bridge> configuration item contains four parameters: Bridge Priority, Hello Time, Max Age and Forward Delay Time, which specify the RSTP Brodge options according to the description in chapter 6.14.4.2. Bit values related to reserved ports are ignored and set to the default value. The Parameters are described in *Table 8-36* on the *page 142.*

Example:

```
eth_rstp_bridge = INST_0 32768, 2, 20, 15
```

This configuration item sets Bridge Priority to 32768, the Hello Time to 2 seconds, Max Age to 20 seconds and Forwarding delay to 15 seconds on a bridge for RSTP "instance 0".

6.14.6.4 *Set Port Configuration*

Description:

The <eth_rstp_port_e> configuration item adds particular port from assigned VLAN group to instance membership and defines configuration relating the Rapid STP. If the ALIAS is not a port from assigned VLAN group or already used by another instance, then the <eth_rstp_port_e> configuration item will be ignored.

Syntax:

```
eth_rstp_port_e = INST_N, ALIAS, PORT_PRI, PORT_PTH_COST, PONT2POINT,
NON_STP_PORT
```

Parameter Description:

The <eth_rstp_bridge> configuration item consists of a part alias and five parameters, which specify the port configuration according to the description in *chapter 6.14.4.3*. Bit values related to reserved ports are ignored and set to the default value. The Parameters are described in Table 8-37 on the *page 143.*

Example:

```
eth_rstp_port_e =   INST_0,      FRT_1,  000,  000020000,  Auto,  1,  0
```

This configuration item sets for the connection FRT_1 Port Priority to 0, the Port Path Cost to 20000, share LAN or Pont2Point to Auto and the port is included to STP calculation for RSTP "instance 0".

6.15 BPDU Filtering

BPDU filtering is a feature that extends the functionality of Rapid Spanning Tree Protocol. It is a software module, which provides the blocking of any RSTP BPDU on particular port. If the BPDU filtering is enabled, the outgoing and incoming BPDUs will not be transmitted and the incoming BPDUs will not be process by RSTP Stack.

6.15.1 Web Based Configuration

The configuration of the BPDU filtering can be set in the RSTP menu. To configure the filter, enable the feature at first. Therefore, select the checkbox “BPDU Filtering” in the “Bridge configuration” section and press the button “Apply” to confirm the act.

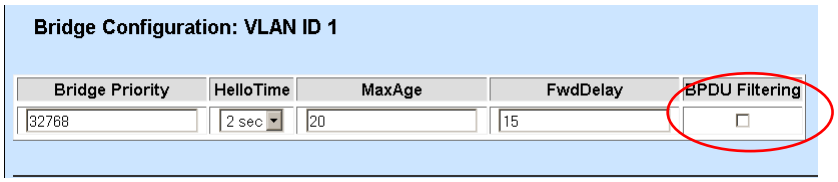
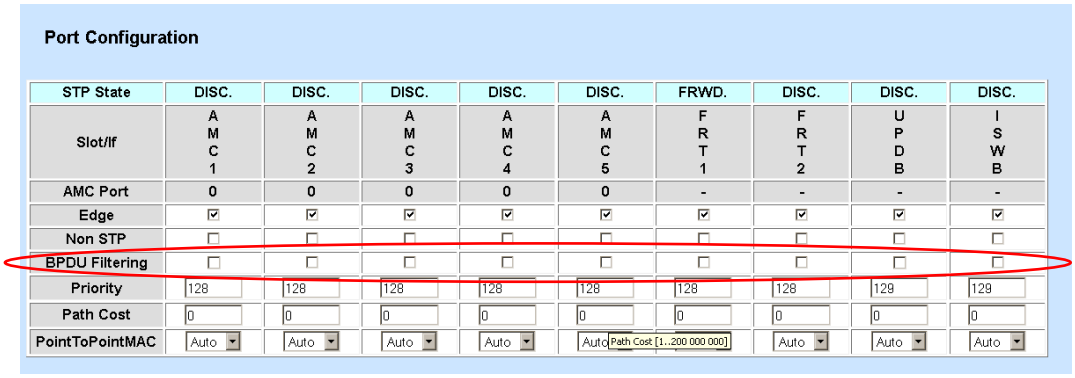


Figure 6-32: enable BPDU filtering

Then the port related settings become accessible and appear in the “Port configuration” section.



If the “BPDU filtering” has not been enabled in the “Bridge configuration”, the port related settings of the feature have been hidden.

6.15.2 Text Based Configuration

The “BPDU filtering” is represented as a stand-along feature by the text-based configuration.

6.15.2.1 *Activate/Deactivate BPDU Filtering*

Description:

The <eth_txfilt_ini> configuration item can be used to activate the BPDU Filtering. If this configuration item is set to “deactivated” or if the item is not present in the

configuration file, all further configuration items related to the BPDU Filtering will be ignored.

Syntax:

```
eth_txfilt_ini  = FLAG
```

Parameter Description:

The parameters of the <eth_txfilt_ini> configuration item are described in *Table 8-38* on page 144.

6.15.2.2 *Set BPDU Filtering on Port*

Description:

The configuration item <eth_txfilt_cm> is used to define connections that apply the BPDU Filtering.

Syntax:

```
eth_txfilt_cm   =  LIST_OF_ALIASES
```

Parameter Description:

The <eth_txfilt_cm> configuration item consists of an alias list. If connection has been presented in the list, the BPDU Filtering has been enabled on it. The parameters are described in *page 144*.

Example:

```
eth_txfilt_cm   = AMC1/0, AMC2/0, AMC3/0, AMC4/0, AMC5/0, FRT_1, CPU_1
```

6.16 IGMP Snooping for IGMP V1V2 on IPV4

(The IGMP Snooping functionality is only available for the 10 GbE Hub-Module equipped with a FM4000 chip.)

***I**nternet **G**roup **M**anagement **P**rotocol Snooping* is the process of capturing IGMP packets from the network. This feature allows a NAT-MCH to observe communication between hosts and routers in terms of IGMP management packets. By listening to these conversation the NAT-MCH calculates a port membership associated to IP multicast streams. In this respect, the NAT-MCH forwards IP multicast data stream only to these ports which are interested in the multicast stream.

The NAT-MCH processes IGMP Management frames only on selected VLAN. Therefore, 802.1Q VLAN has to be setup first. For each VLAN present, the IGMP Snooping can be activated to capture IGMP management frames for this VLAN (VLAN *Trap*).

The NAT-MCH can operate in "Querier" or "Non-Querier" mode. If Querier mode is enabled a General Query can be sent on all active non-router ports in order to reduce network convergence time.

6.16.1 CLI Based Configuration

The `'(submenu) IGMP'` offers commands to manipulate the settings of the IGMP Snooping mode.

6.16.1.1 *Activate/Deactivate IGMP Snooping*

To enable IGMP Snooping choose the menu item `<enable IGMP Snooping>` from the submenu.

To disable IGMP Snooping choose the menu item `<disable IGMP Snooping>`.

After the activation of IGMP Snooping, the default settings for IGMP will be set. These settings can be changed manually in terms of `<IGMP general settings>` and `<configure VLAN Trap>` items.

6.16.1.2 *IGMP general settings*

If the IGMP Snooping has been enabled this menu item allows configuring the `<Querier mode>`, `<Query interval>` and `<Group Membership Interval>`. These parameters will be prompted as follows:

```
Should be Querier Mode enabled?
[y]-yes, [n]- no(RET=n)>
```

To select `<Querier mode>` of the NAT-MCH enter `<y>` to enable Querier or `<n>` set it as a `<Non-Querier>`.

```
The following parameters are used to calculate internal timer update.
Change the default settings If you are really sure.
Enter Query Interval in sec. (RET=125/0x7d):>125
Enter Query Interval in sec. (RET=320/0x140):>320
```

6.16.1.3 *Configure VLAN Trap*

The NAT-MCH processes IGMP Management frames only for the selected VLANs. In this menu item, the VLAN Trap state can be configured to <enable trap> or to <disable trap>. The chosen VLAN must be configured via the 802.1Q VLAN setting first:

```
Enter VLAN ID[1 - 4094] (RET=1/0x1):>10
Should be this VLAN an IGMP member?
[y]-yes, [n]- no (RET=y):>y
```

Enter <y> to configure VLAN for <enable trap> or <n> for <disable trap>.

6.16.2 Web Based Configuration

To call the IGMP Snooping Settings page select the <IGMP Snooping> link at the navigation part of the browser window and activate it if mode is down.

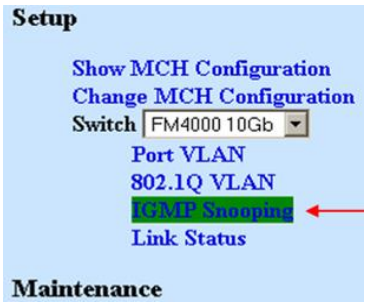


Figure 6-33: IGMP Snooping - Submenu

The protocol configuration consists of two parts "Summary Settings" and "VLAN Traps". The upper part provides the configuration applied for general switch configuration: Group membership Interval, Group Query Interval and Querier Mode. The Summary settings must be submitted explicit by press the button "Submit".

There are VLANs to select in the bottom part of menu. The IGMP Snooping can be activated to capture IGMP management frames on particular VLANs (VLAN *Trap*).To add a VLAN to the VLAN Trap choose it in the dropdown menu list and submit selection with the button "Add".

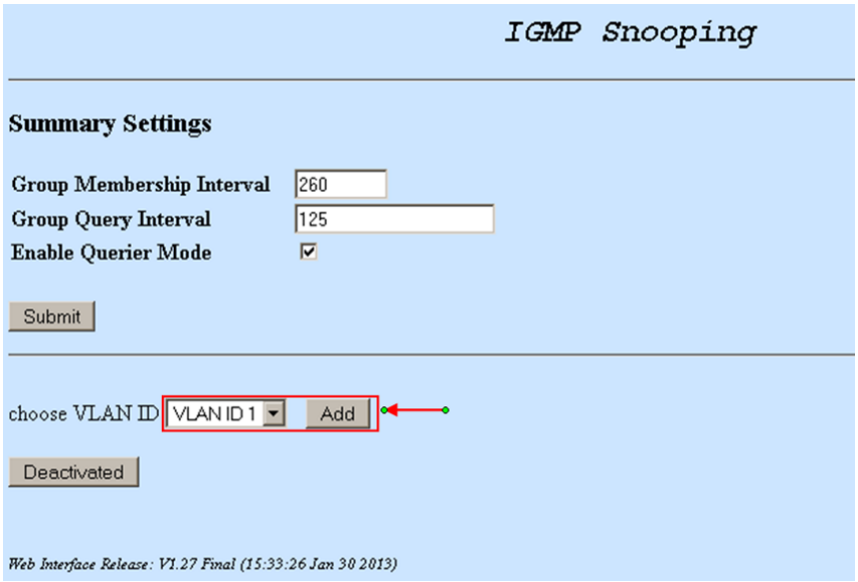


Figure 6-34: IGMP Snooping - Add VLAN Trap

Each VLAN can be removed from the VLAN Trap anytime, by press the button "Remove" for the corresponding VLAN.

Figure 6-35: IGMP Snooping - Remove VLAN Trap

All settings will be accepted at the running time.

6.16.3 Text Based Configuration

There are five configuration items available to configure the IGMP mode.

`eth_igmps_ini` – Activates/Deactivates IGMP Snooping
`eth_igmps_qf` – Defines Querier/Non-Querier mode
`eth_igmps_qi` - Defines Query Interval for internal timers
`eth_igmps_gmi` - Defines Group Membership Interval for internal timers
`eth_igmps_vlan` - Defines VLAN (one per item) as related to IGMP Snooping

6.16.3.1 *Activate/Deactivate IGMP Snooping*

Description:

The <`eth_igmps_ini`> configuration item can be used to enable/disable IGMP Snooping mode. If this configuration item is set to "`deactivated`" or if the item is not present in the configuration file, all further configuration items related to IGMP Snooping will be ignored.

Syntax:

```
eth_igmps_ini = FLAG
```

Parameter Description:

The parameters of the <eth_igmps_ini> configuration item are described in *Table 8-40* on page *145.*

Example:

Activate IGMP Snooping mode:

```
eth_igmps_ini = 1
```

6.16.3.2 *Querier mode*

Description:

The <eth_igmps_qf> configuration item can be used to enable/disable Querier mode for IGMP Snooping mode.

Syntax:

```
eth_igmps_qf = FLAG
```

Parameter description:

The parameters of the <eth_igmps_qf> configuration item are described in *Table 8-41* on page *145.*

Example:

Activate Querier mode for IGMP Snooping:

```
eth_igmps_qf = 1
```

Set NAT-MCH to Non-Querier mode:

```
eth_igmps_qf = 0
```

6.16.3.3 *Query Interval*

Description:

The <eth_igmps_qi> configuration item can be used to Set Query Interval for IGMP Snooping mode.

Syntax:

```
eth_igmps_qf = QEUR_IN
```

Parameter description:

The parameters of the <eth_igmps_qi> configuration item are described in *Table 8-42* on page *145.*

Example:

Set Query Interval at internal timer to 125 seconds:

```
eth_igmps_qi = 125
```

6.16.3.4 *Group Membership Interval*

Description:

The <eth_igmps_gmi> configuration item can be used to Set Group Membership Interval for IGMP Snooping mode.

Syntax:

```
eth_igmps_gmi = GR_MEM_IN
```

Parameter description:

The parameters of the <eth_igmps_gmi> configuration item are described in on page *146.*

Example:

Set Group membership Interval at internal timer to 320 seconds:

```
eth_igmps_gmi = 320
```

6.16.3.5 *Add/Remove VLAN to/from IGMP Snooping*

Description:

The <eth_igmps_vlan> can be used to set one VLAN Group per configuration item for IGMP Snooping mode. More than one item can be present for the same switch device. The chosen VLAN must be configured via the 802.1Q VLAN setting first.

Syntax:

```
eth_igmps_vlan = VLANID
```

Parameter description:

The parameters of the <eth_igmps_vlan> configuration item are described in *Table 8-44* on page *146.*

Example:

Set the VLANs: 10, 20 and 30 as active for IGMP Snooping

```
eth_igmps_vlan = 10
eth_igmps_vlan = 20
eth_igmps_vlan = 30
```

6.17 Pause Frame Processing

The PAUSE frame is a mechanism for temporarily stopping the transmission of data on Ethernet family computer networks. An overwhelmed network node can send a pause frame, which halts the transmission of the sender for a specified period.

This frame was defined by the IEEE 802.3x standard. The IEEE 802.3 PAUSE frame is a special frame, which contains a single pause interval applicable to all traffic classes. It is identified by Ethertype =8808 and destination MAC address 01-80-c2-00-00-01.

A Pause Frames have not to be forwarded by Ethernet switch, but The 10 GbE Switch (FM4000) has the capacity to react to reception of PAUSE frames and can to be configured to process them.

If an “overwhelmed node” sends a pause frame, then the switch stops transmitting of all frames to the “overwhelmed node”, but the regular frames have not to be dropped. All frames are stored in the internal queues of the switch. If pause time is elapsed, the switch resumes the frames transmitting from internal queues. Thereby, other communicating partners do not notice, that an “overwhelmed node” has sent PAUSE frames in the meantime.

If Pause Frames hold a frame transmitting for a long time, then internal switch queues are going full. To prevent it, a switch can send PAUSE frames on the other port(s) to reduce ingress traffic on the switch. In this respect, FM4000 switch monitors memory usage for ingress traffic on particular port.

6.17.1 Web Based Configuration

The configuring interface defines the limits in number of segments that each Rx Queue can use before starting or stopping sending PAUSE frames.

- Pause is activated when the number of segments is above this *On Limit*.
- Pause is deactivated when the number of segments is below or equal to this *Off Limit*.

The hardware assumes that the ON Limit is greater than the OFF Limit. The value may range from 0 to 8191.

The *Pause Resend Time* defines the number of bit-times before the switch resends the PAUSE ON frame in units of 512 bit-times. The value may range from 0 to 65535

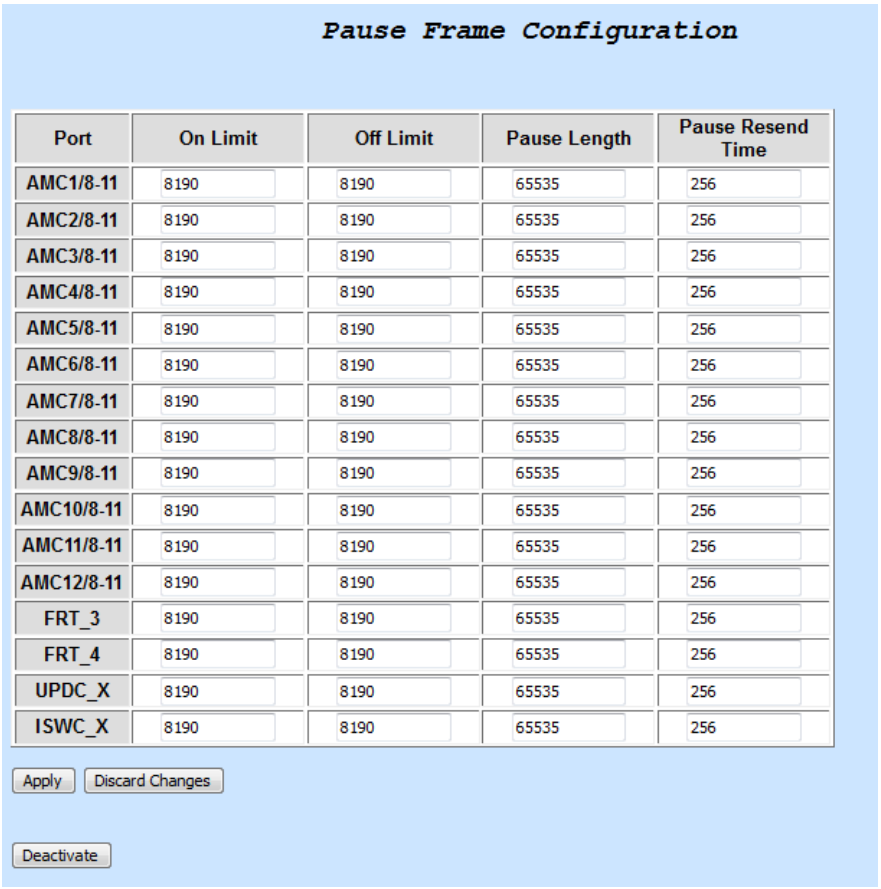


Figure 6-36: Pause Frame Processing

The *Pause Length* defines the number of bit-times that the link partner needs to pause in units of 512 bit-times. The value may range from 0 to 65535 (specify zero to disable PAUSE). The default value is 65535.

6.18 Interface mode - SerDes/SGMII (Base MCH GbE)

The Ethernet (GbE) switch on the Base Board of the NAT-MCH is integrated with 1.25G-SerDes/SGMII port interfaces for connecting to AMCs. Those AMC port can be configured in SGMII or SerDes mode. The SGMII interface pins are shared with the SerDes interface pins. There are three options available SerDes, SGMII and Auto-Detection.

The SerDes interface operates via 1000BASE-X and complies with IEEE Standard 802.3.

The SGMII interface transmits and receives serial data differentially at 1.25 Gbit/s. Transmit data timing is recovered from the incoming data signal, and the attached link partner does the same.

To detect the interface mode automatically, the link partner exchange control information, when establishing a link. Upon receiving proper acknowledgement, the Ethernet switch of Base-MCH completes auto-negotiation and returns to normal data mode.

6.18.1 Web Based Configuration

The configuration of Interface mode can be set in the “SerDes/SGMII” menu.

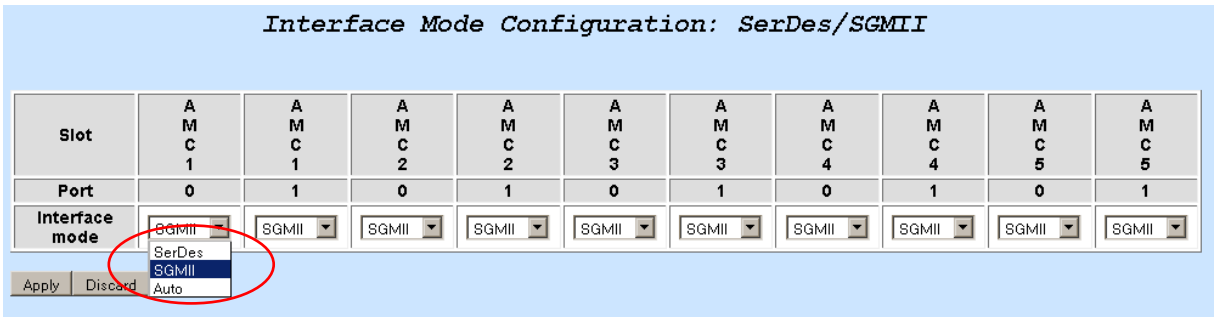


Figure 6-37: Interface mode SerDes/SGMII on AMC Backplane Ports

Therefore, select the dropdown menu on particular ports to select one of three available options SerDes, SGMII or Auto. Then press button “Apply” to confirm the act.

6.18.2 Text Based Configuration

There is one configuration item available to configure the Interface mode on particular port.

`eth_sgmii_imode` – Interface mode on particular port

Syntax:

```
eth_sgmii_imode= ALIAS, IFF_MODE
```

Parameter Description:

The <eth_sgmii_imode> configuration item consists of a part alias and one parameter, which specify the port configuration according to the description in *chapter 6.17*. The Parameters are summered in Table 8-45 on the *page 147.*

Example:

```
eth_sgmii_imode = AMC1/0, serdes
eth_sgmii_imode = AMC2/0, sgmii
…
eth_sgmii_imode = AMC7/0, auto
…
```

Those configuration items set for the interface mode of connection AMC1/0 to SerDes, AMC2/0 to SGMII and connection AMC7/0 to Auto-Detection.

6.19 Switch Counters (Base MCH GbE)

The web interface make available three types of counters for Ethernet (GbE) switch on the baseboard:

- Bit Error (BER) Counter
- Checksum Error (CRC) Counter
- Received Packets (RCV) Counter

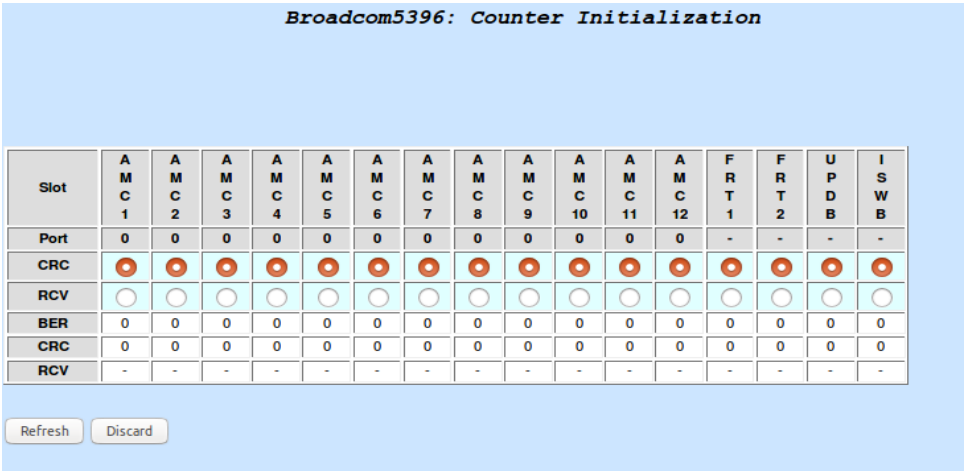


Figure 6-38: Switch Counters (Base MCH GbE)

BER Counter is always enabled: It counts if invalid code groups are detect. The counter may to be increased if MCH is starting or if AMC has been hold from reset. If all carrier components are already running, the BER Counter should stay unchanged. Otherwise, the increase of a port value can indicate a hardware complication with a system component.

The CRC/ RCV counters cannot run simultaneously. One of two counters has to be selected by user. CRC shows number of frames with detected CRC Error. RCV counter shows number of received Ethernet frames.

7 Script Management Backup Settings

7.1 Script Management – Web interface (FW V2.16 and later)

The web interface offers a comfortable menu for the management of the switch configuration. To enter the menu, select the `<Script Management>` link at the navigation part of the browser window.

Then the settings management menu appears on the right side of the browser window as follows:

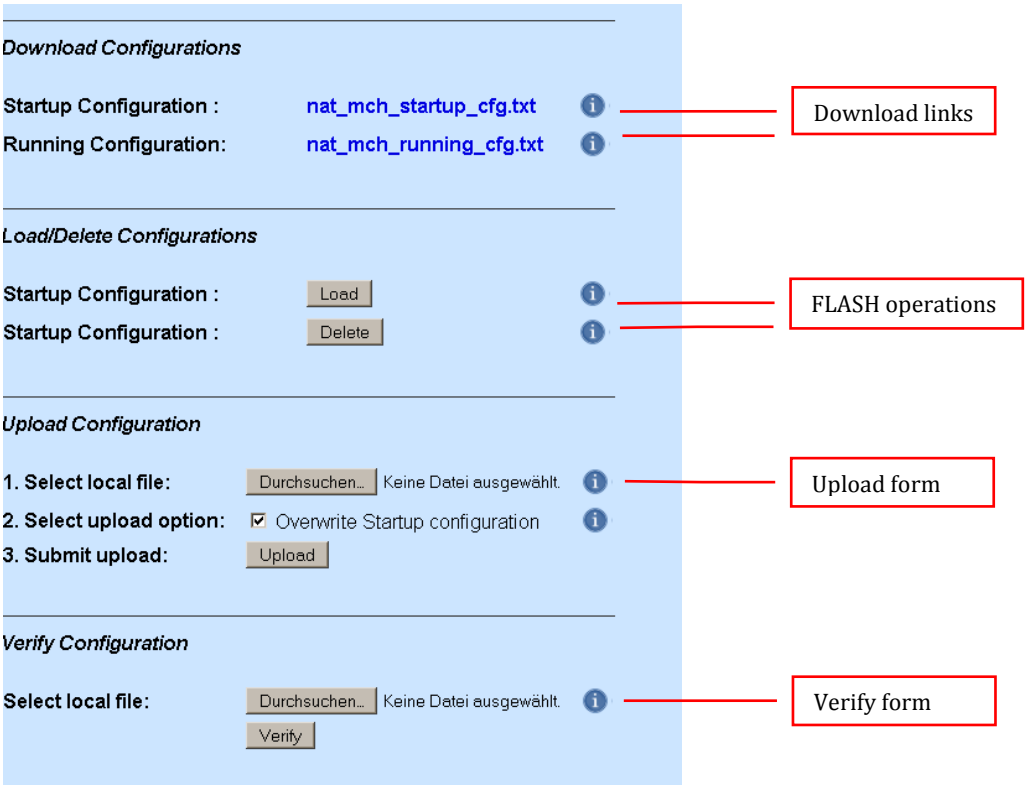


Figure 7-1: Script Management menu

7.1.1 Download the Switch Configuration

Because the Startup configuration can be modified by user in the runtime, the Running configuration originates from it. Both configurations can be downloaded in the "Script Management "menu as shown in *Figure 7-1*.

7.1.2 Save Running Configuration

New running configuration of switch can be simply saved to FLASH. To save it permanently, press the button <Save> and wait a little until the operation has been confirmed. Therefore, a new switch configuration will not be lost after NAT-MCH reboot.

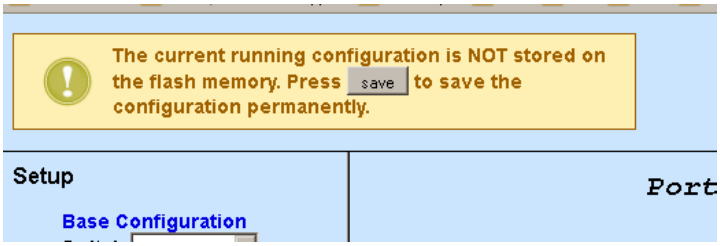


Figure 7-2: save switch configuration

7.1.3 Load/Delete Startup Configuration

The Startup switch configuration can be loaded applied by user manually.

The feature is very useful, if the board has been misconfigured in the runtime. Please, press the button <Load> to overwrite nonconforming-Running configuration by the Startup configuration.

To load the default switch configuration on startup, the startup configuration must be removed from FLASH. Please, press the button <Delete> and wait until the operation has been completed.

7.1.4 Upload the Switch Configuration

The web interface offers the upload of the switch configuration via web browser.

To upload the switch configuration, press at first the button <Browse> to select the path of the file, then press the button <Upload>.

If the option "Overwrite Startup" is not selected the local file will be applied for the Running Configuration only. Selecting this option overwrites the Startup Configuration on FLASH memory.

8 Description Tables of the Text Based Configuration

8.1 Device Location

Table 8-1: <mch_id> configuration item (page 23, 25)

This configuration item specifies the MCH that that shall be selected for the further configuration (see the chapter 4)		
Parameter No.	**Parameter description**	**Default value**
1	MCH ID 0 – Currently only one MCH is supported	0

Table 8-2: <mez_id> configuration item (page 23, 25)

The configuration item defines mezzanine level (see the chapter 4)		
Parameter No.	**Parameter description**	**Default value**
1	Mezzanine level[0..2]: - Base Board - Clock Module - Hub Module	none

Table 8-3: <ins_id> configuration item (page 23, 25)

The configuration item defines instance ID on mezzanine level (see the chapter 4)		
Parameter No.	**Parameter description**	**Default value**
1	Instance ID [0..7]: First Device Second Device …	none

8.2 Port Enable/Disable

Table 8-4: `<eth_enconn_map>` configuration item (page 33)

This configuration item disables/enables AMC Ports and additional connections. If a connection is disabled no traffic will be received from or transmitted to this port from switch.

Parameter No.	Parameter description	Example
1	LIST_OF_ALIASES: alias list of active connections	1GbE Switch: AMC1/0, AMC1/1, AMC2/0, AMC2/1, AMC3/0, AMC3/1, AMC4/0, AMC4/1, AMC5/0, AMC5/1, FRT_1, FRT_2, UPDC_B, ISW_BX, CPU_1

8.3 Enable/Disable Port on Primary MCH

Table 8-5: <eth_enconn_prim> configuration item (page 37)

This configuration item provides overruling of <eth_enconn_map> setting, if MCH becomes primary. If a connection is disabled, then no traffic will be received from or transmitted to this port from switch.

Parameter No.	Parameter description	Example
1	LIST_OF_ALIASES: alias list of active connections	1GbE Switch: AMC1/0, AMC1/1, AMC2/0, AMC2/1, AMC3/0, AMC3/1, AMC4/0, AMC4/1, AMC5/0, AMC5/1, FRT_1, FRT_2, UPDC_B, ISW_BX, CPU_1

8.4 Link Propagation

Table 8-6: <eth_propag> configuration item (page 38)

The configuration item specifies the link propagation from master port to list of slave ports.		
Parameter No.	**Parameter description**	**Example**
1	ALIAS: alias of propagation master port	10GbE Switch: `FRT_3`

	LIST_OF_ALIASES: alias list of propagation slave ports	10GbE Switch:
		`AMC1/4-11,`
		`AMC2/4-11,`
		`AMC3/4-11,`
		`AMC4/4-11,`
		`AMC5/4-11,`
		`AMC6/4-11,`
		`AMC7/4-11,`
		`AMC8/4-11`

8.5 Port Bsed VLAN Configuration

Table 8-7: `<eth_pbvlan_init>` configuration item (page45)

This configuration item enables the Port Based VLAN mode.		
Parameter No.	**Parameter description**	**Default value**
1	Port Based VLAN initialization flag 0 - Port Based VLAN is deactivated 1 - Port Based VLAN is activated	0

Table 8-8 : `<eth_pbvlan_fwcm>` configuration item (page 45)

The configuration item specifies the connection list map for a specific source port.		
Parameter No.	**Parameter description**	**Example**
1	source ALIAS: alias of some source connection	1GbE Switch: AMC1/0
2	LIST_OF_ALIASES: alias list of destination connections	1GbE Switch: `AMC1/0, AMC1/1, AMC2/0, AMC2/1, AMC3/0, AMC3/1, AMC4/0, AMC4/1, AMC5/0, AMC5/1, FRT_1, FRT_2, UPDC_B, ISW_BX, CPU_1`

8.6 802.1Q VLAN Configuration

Table 8-9: `<eth_802.1q_init>` configuration item (page 57)

The configuration item determines if the 802.1Q VLAN mode should be activated or deactivated.		
Parameter No.	**Parameter description**	**Default value**
1	802.1Q VLAN initialization flag 0 - 802.1Q VLAN is deactivated 1 - 802.1Q VLAN is activated	0

Table 8-10: `<eth_802.1q_lrn>` configuration item (page 57)

The configuration item can be used to change the hash key generation algorithm of the Ethernet switch		
Parameter No.	**Parameter description**	**Default value**
1	The Mode of the MAC-Entry-Resolution flag 0 – The MAC-Address is used to generate the hash key for the MAC-Table entry. 1 – The MAC-Address and VLAN ID are used to generate the hash key for the MAC-Table entry.	1

Table 8-11: `<eth_802.1q_m_cm>` configuration item (page 58)

The configuration item defines the connections assigned to the VLAN group of the VLAN-Table; those provides the forwarding of the VLAN frames.

Parameter No.	Parameter description	Example
1	VLAN ID `[1-4094]` of VLAN-Entry	10
2	LIST_OF_ALIASES: alias list of connection have to be assigned to the VLAN membership	1GbE Switch: `AMC1/0, AMC1/1, AMC2/0, AMC2/1, AMC3/0, AMC3/1, AMC4/0, AMC4/1, AMC5/0, AMC5/1, FRT_1, FRT_2, UPDC_B, ISW_BX, CPU_1`

Table 8-12: `<eth_802.1q_u_cm>` configuration item (page 58)

The configuration item defines the ports on which the VLAN Tag must be removed from frames by transmit.

Parameter No.	Parameter description	Default value
1	VLAN ID[1-4094] of VLAN-Entry	10
2	LIST_OF_ALIASES: alias list of connection to define VLAN Untagging on Particular Port	1GbE Switch: `AMC1/0, AMC1/1, AMC2/0, AMC2/1, AMC3/0, AMC3/1, AMC4/0, AMC4/1, AMC5/0, AMC5/1, FRT_1, FRT_2, UPDC_B, ISW_BX, CPU_1`

Table 8-13: `<eth_802.1q_dflt>` configuration item (page 59)

This configuration item specifies the VLAN-Tag is to be added to the untagged Ethernet frame at the certain connection.

Parameter No.	Parameter description	Example
1	ALIAS of connection, on which all ingress frame have to be tagged	`AMC1/0`
2	Default VLAN ID[1-4094]	`100`
3	VLAN priority[0-7]	`7`

Table 8-14: `<eth_802.1q_tag>` configuration item (V2.9 and earlier)

This configuration item specifies the VLAN-Tag, which is to be added to the untagged Ethernet frame at the certain port.

Parameter No.	Parameter description	Default value
1	Port ID where default VLAN-Tag has to be set.	All used ports
2	Default VLAN ID[1-4094]	1
3	VLAN priority[0-7]	0

8.7 MAC Table

Table 8-15: `<eth_mac_ent_con>` configuration item page (page 69)

The configuration item adds the entry to the MAC Address Table to provide the static routing of frames and to support the 802.1X port security mode.		
Parameter No.	**Parameter description**	**Example**
1	6.8.3.4-Address: `[xx:xx:xx:xx:xx:xx]`	`00:01:02:03:04:05`
2	VLAN ID `[1-4094]`	`100`
3	Priority `[0-7]`	`7`
4	ALIAS of connection on which the frame with previously mentioned source -Address has been received and permitted to route	`AMC6/0`

Table 8-16: `<eth_mac_ageinit>` configuration item page (page 33)

The configuration item defines Age Time initialized state.		
Parameter No.	**Parameter description**	**Default value**
1	Age Time initialization flag 0 – aging process is deactivated 1 - aging process is activated	1

Table 8-17: `<eth_mac_agetime>` configuration item page (page 33)

The configuration item determines activated or deactivated Age Time(in seconds) of the dynamical learned MAC Table entry.		
Parameter No.	**Parameter description**	**Default value**
1	Aging interval in seconds AGE TIME [1..<depends on the switch device>]	300

8.8 802.1X Configuration

Table 8-18: `<eth_802.1X_ini>` configuration item (page 68)

The configuration item provides the access for using the 802.1X port security functionalities		
Parameter No.	**Parameter description**	**Default value**
1	802.1X initialization flag 0 - 802.1X Port Security is deactivated 1 - 802.1Q Port Security is activated	0

Table 8-19: `<eth_802.1X_dm>` configuration item (page 68)

The configuration item sets the dropping mode by frame checking		
Parameter No.	**Parameter description**	**Default value**
1	The Drop mode flag 0 - Drop frame if source MAC misses in the MAC table, and the frame is not a IEEE Standard 802.1X special frame 1 - Drop frames that are not IEEE Standard 802.1X special frames	0

Table 8-20: `<eth_802.1x_cm>` configuration item (page 69)

The configuration items defines connections on which the 802.1X mode is enabled

Parameter No.	Parameter description	Default value
1	LIST_OF_ALIASES of connections on which the 802.1X mode is enabled	1GbE Switch: `AMC1/0, AMC1/1, AMC2/0, AMC2/1, AMC3/0, AMC3/1, AMC4/0, AMC4/1, AMC5/0, AMC5/1, FRT_1, FRT_2, UPDC_B, ISW_BX, CPU_1`

8.9 Quality of Service Configuration

Table 8-21: `<eth_qos_cm>` configuration item (page 73)

The configuration item configures a mapping between a VLAN –Priority and internal transmit queue for a certain connection		
Parameter No.	**Parameter description**	**Example**
1	ALIAS of connection on which the mapping between VLAN priority and internal transmit queue has to be defined.	none
2	Priority (0-7) at VLAN Tag of Ethernet Frame	none
3	Egress Queue (0-3)	0

8.10 802.1p Quality of Service Configuration

Table 8-22: `<eth_802.1p_ini>` configuration item (page 76)

The configuration item can be used to activate the 802.1p mode		
Parameter No.	**Parameter description**	**Default value**
1	Quality of Service- 802.1p initialization flag 0 - 802.1p QoS is deactivated 1 - 802.1p QoS is activated	0

Table 8-23: `<eth_802.1p_cm>` configuration item (page 77)

The configuration item defines on which port(s) 802.1p mode is activated		
Parameter No.	**Parameter description**	**Default value**
1	LIST_OF_ALIASES of connections on those the 802.1X mode is enabled	1GbE Switch: `AMC1/0, AMC1/1, AMC2/0, AMC2/1, AMC3/0, AMC3/1, AMC4/0, AMC4/1, AMC5/0, AMC5/1, FRT_1, FRT_2, UPDC_B, ISW_BX, CPU_1`

8.11 Port Mirroring Configuration

Table 8-24: `<eth_mirr_ini>` configuration item (page 83)

The configuration item can be used to activate the port mirroring feature		
Parameter No.	**Parameter description**	**Default value**
1	Port Mirroring initialization flag 0 - Port Mirroring is deactivated 1 - Port Mirroring is activated	0

Table 8-25: `<eth_mirr_capt>` configuration item (page 83)

The configuration item defines the capture port		
Parameter No.	**Parameter description**	**Default value**
1	`PORT_CPT` capture port	`FRT_1`

Table 8-26: `<eth_mirr_icm>` configuration item (page 83)

The configuration item defines the port(s) on which all **ingress** frames must be mirrored to the capture port.		
Parameter No.	**Parameter description**	**Default value**

1	LIST_OF_ALIASES of connections on those all **ingress** frames must be mirrored to the capture port `PORT_CPT`.	1GbE Switch:
		
		`AMC1/0, AMC1/1,`
		`AMC2/0, AMC2/1,`
		`AMC3/0, AMC3/1,`
		`AMC4/0, AMC4/1,`
		`AMC5/0, AMC5/1,`
		`FRT_1, FRT_2,`
		`UPDC_B, ISW_BX,`

Table 8-27: `<eth_mirr_ecm>` configuration item (page 84)

The configuration item defines the port(s) on which all **egress** frames must be mirrored to the capture port		
Parameter No.	**Parameter description**	**Default value**

1	LIST_OF_ALIASES of connections on those all **ingress** frames must be mirrored to the capture port `PORT_CPT`.	1GbE Switch:
		
		`AMC1/0, AMC1/1,`
		`AMC2/0, AMC2/1,`
		`AMC3/0, AMC3/1,`
		`AMC4/0, AMC4/1,`
		`AMC5/0, AMC5/1,`
		`FRT_1, FRT_2,`
		`UPDC_B, ISW_BX,`

8.12 Jumbo frame Configuration

Table 8-28: `<eth_jumbo_ini>` configuration item (page 88)

The configuration item can enable or disable the access to the Jumbo frame functionality.

Parameter No.	Parameter description	Default value
1	Jumbo mode initialization flag 0 - Jumbo mode is deactivated 1 - Jumbo mode is activated	0

Table 8-29: `<eth_jumbo_size>` configuration item (page 85)

The configuration item defines the Jumbo Frame functionality on the port.

Parameter No.	Parameter description	Default value
1	Port ID where Jumbo functionality is to be set	0
2	The frame size (Kbyte) `[0,9,...,16]`	0

8.13 Link Aggregation Configuration

Table 8-30: `<eth_lag_ini>` configuration item (page 95)

The configuration item can enable or disable the Link Aggregation mode.		
Parameter No.	**Parameter description**	**Default value**
1	Link Aggregation initialization flag 0 - aggregation mode is deactivated 1 - aggregation mode is activated	0

Table 8-31: `<eth_lag_hash>` configuration item (pages 90, 95)

The configuration item specifies the hash key generation method to provide the routing of the frames within the Aggregation Group		
Parameter No.	**Parameter description**	**Default value**
1	Hashing mode provide the routing of outbound frames inside of an Aggregation Group. The setting takes effect for all Aggregation Groups. 0 – The hash key will be generated based on the Destination and Source MAC Addresses of the processed frame. 1 – The hash key will be generated based on the Destination MAC Addresses of the processed frame. 0 – The hash key will be generated based on the Source MAC Addresses of the processed frame.	0

Table 8-32 : <eth_lag_gr_cm> configuration item (pages 90, 91)

This configuration item defines ports are assigned to the specific aggregation group.		
Parameter No.	**Parameter description**	**Default value**
1	ID of an aggregation group [0-3]	Each used ports
2	LIST_OF_ALIASES of connections are assigned to the aggregation group	none

Table 8-33 : <eth_lag_propag> configuration item (pages 95)

This configuration item defines Link Propagation mode if *propagation master* is a LAG.		
Parameter No.	**Parameter description**	**Default value**
1	ID of an aggregation group [0-3]	Each used ports
2	LIST_OF_ALIASES of connections are assigned to the aggregation group	none

8.14 Rapid Spanning Tree Protocol

Table 8-34: `<eth_rstp_ini>` configuration item (page 107)

The configuration item can enable or disable the Rapid Spanning Tree Configuration.		
Parameter No.	**Parameter description**	**Default value**
1.	INST_N RSTP instance ID	{INST_0 | INST_1}
2.	Protocol initialization flag 0 - Rapid Spanning Tree mode is deactivated 1 - Rapid Spanning Tree mode is activated	0

Table 8-35: `<eth_rstp_vid>` configuration item (page 107)

The configuration item assigns VLAN group to RSTP instance.		
Parameter No.	**Parameter description**	**Default value/Range**
1.	INST_N RSTP instance ID	{INST_0 | INST_1}
2.	Assigned VLAN group 0 – "Ignore VLAN ID" option 1-4092 Rapid Spanning Tree mode is activated	0-4092

Table 8-36: `<eth_rstp_bridge>` configuration item (pages 107)

This configuration item defines generic Rapid STP configuration .of the Bridge.		
Parameter No.	**Parameter description**	**Default value**
1.	INST_N RSTP instance ID	{INST_0 | INST_1}
2.	BRG_PRI: Bridge Priority	61336-61339
3.	HELLO_T: Hello Time	2
4.	MAX_AGE: Max Age	20
5.	FWD_DELAY: Forwarding Delay	15

Table 8-37: `<eth_rstp_port_e>` configuration item (pages 108)

This configuration item attaches port to Instance Membership in RSTP instance.		
Parameter No.	**Parameter description**	**Default value**
1.	INST_N RSTP instance ID	{INST_0 | INST_1}
2.	ALIAS of connection	none
3.	PORT_PRI: Port Priority `[0..240]` steps 16	128
4.	PORT_PTH_COST: Port Path Cost `[1..200 000 000]`	1
5.	PONT2POINT: adminPointToPointMAC `[True|False|Auto]`	Auto
6.	NON_STP_PORT: admin_non_stp `[0..1]`	0

8.15 BPDU Filtering

Table 8-38: `<eth_txfilt_ini>` configuration item (page 109)

The configuration item can enable or disable BPDU Filtering Configuration.		
Parameter No.	**Parameter description**	**Default value**
1	Feature initialization flag 0 - BPDU Filtering mode is deactivated 1 - BPDU Filtering mode is activated	0

Table 8-39: `<eth_txfilt_cm>` configuration item (page 110)

The configuration items defines connections on which the BPDU Filtering mode is enabled		
Parameter No.	**Parameter description**	**Default value**
1	LIST_OF_ALIASES of connections on which the BPDU Filtering mode is enabled	1GbE Switch: `AMC1/0, AMC1/1, AMC2/0, AMC2/1, AMC3/0, AMC3/1, AMC4/0, AMC4/1, AMC5/0, AMC5/1, FRT_1, FRT_2, UPDC_B, ISW_BX, CPU_1`

8.16 IGMP Snooping

Table 8-40: `<eth_igmps_ini>` configuration item (page 114)

The configuration item can enable or disable IGMP Snooping Configuration.		
Parameter No.	**Parameter description**	**Default value**
1	Protocol initialization flag 0 – IGMP Snooping mode is deactivated 1 - IGMP Snooping mode is activated	0

Table 8-41: `<eth_igmps_qf>` configuration item (page 115)

The configuration item can set Querier mode of the NAT-MCH.		
Parameter No.	**Parameter description**	**Default value**
1	Querier mode 0 – Non-Querier mode 1 - Querier mode is enabled	0

Table 8-42: `<eth_igmps_qi>` configuration item (page 115)

The configuration item can set Query Interval for IGMP Snooping mode.		
Parameter No.	**Parameter description**	**Default value**
1	Querier mode in seconds	125

Table 8-43: `< eth_igmps_gmi>` configuration item (page116)

The configuration item can set Group Membership Interval for IGMP Snooping mode.		
Parameter No.	**Parameter description**	**Default value**
1	Group Membership Interval in seconds	320

Table 8-44: `<eth_igmps_vlan>` configuration item (page 116)

The configuration item can set a VLAN group as active for the IGMP Snooping		
Parameter No.	**Parameter description**	**Default value**
1	VLANID [0 .. 4095]	none

8.17 Interface mode SerDes/SGMII

Table 8-45: `<eth_sgmii_imode>` configuration item (pages 119)

This configuration item defines Rapid STP configuration .of the Port.		
Parameter No.	**Parameter description**	**Default value**
1	ALIAS of AMC connection	none
4	Interface mode `[SerDes|SGMII|Auto]`	SerDes

9 XAUI Packet Counters -

The FM222x switch of Fulcrum Microsystems inc. supports a few counters to maintain the statistic of packet traffic. All counters are listed in thirteen groups. Furthermore, most counters have one *additional parameter* such as port ID, VCNT field ID or Trigger ID. Each counter in a group is mutually exclusive. The description of packet counters are shown in chapter *9.1 XAUI - Packet Counter Description*

9.1 XAUI - Packet Counter Description

Table 9-1 : Group 1 Counters - RX Packet Counters per Type [0..24]

Name	Description
RxUcast	Unicast frames received. (Note: oversize and undersize frames with good or bad CRC are counted. Proper size frames with bad CRC are not counted; they are counted as RxFCSErrors.)
RxBcast	Valid broadcast frames received (good frames only).
RxMcast	Valid multicast frames received (good frames only, does not include broadcast or pause frames).
RxPause	Valid received pause frames
RxFCSErrors	Received frames of proper size but CRC error, and integral number of octets.
RxSymbolErrors	Received frames of proper size, but with symbol error.

Table 9-2: Group 2 Counters - RX Packet Counters per Size [0..24]

Name	Description
RxMinto63	Received frames of < 64 octets that are not error frames because the min. frame size is set below the Ethernet minimum (good and bad frames counted).
Rx64	Received frames of 64 octets (good and bad frames counted).
Rx65to127	Received frames of 65 to 127 octets (good and bad frames counted).
Rx128to255	Received frames of 128 to 255 octets (good and bad frames counted).
Rx256to511	Received frames of 256 to 511 octets (good and bad frames counted).
Rx512to1023	Received frames of 512 to 1023 octets (good and bad frames counted).
Rx1024to1522	Received frames of 1024 to 1522 octets (good and bad frames counted).
Rx1523to2047	Received frames of 1523 to 2047 octets (good and bad frames counted).
Rx2048to4095	Received frames of 2048 to 4095 octets (good and bad frames counted).
Rx4096to8191	Received frames of 4096 to 8191 octets (good and bad frames counted).
Rx8191to10239	Received frames of 8192 to 10239 octets (good and bad frames counted).
Rx10240toMax	Received frames of 10240 to MaxFrame octets. Note: Maxframe is configurable. This counter will only be activated if MaxFrame is > 10240. That is it is the count of non-error frames above 10240. In any case, Fulcrum strongly recommends against sending packets above 10240 octets, as the Ethernet CRC is no longer valid.
RxFragments	Received frames smaller than Min Sized Frame octets with either a CRC or alignment error.
RxUndersized	Received frames smaller than the minimum frame size but otherwise well formed with a good CRC
RxJabbers	Received frames greater than MaxFrame octets and alignment error and good or bad CRC. This counter is only 16 bits

RxOversized	Received frames greater than MaxFrame octets . This counter includes oversized well formed packets as well oversized packets with a bad CRC or an alignment problem. The software must read the counter STAT_RX_JABBER[Jabber Count] in the EPL to detect how many of the oversized frames were actually malformed packets. NOTE: If the frame is counted here, it is not counted in a bin counter RxXXXXtoYYYY even if it fits in that bin

Table 9-3: Group 3 Counters - RX Octet Counters [0..24]

Name	Description
RxGoodOctets	Received octets on good packets
RxBadOctets	Received octets on bad packets. Note: total received octets is the sum of RxGoodOctets and RxBadOctets.

Table 9-4: Group 4 Counters - RX Packet Counters per Priority [0..24]

Name	Description
RxP0	Received frames of priority 0
RxP1	Received frames of priority 1
RxP2	Received frames of priority 2.
RxP3	Received frames of priority 3
RxP4	Received frames of priority 4
RxP5	Received frames of priority 5.
RxP6	Received frames of priority 6.
RxP7	Received frames of priority 7.

Table 9-5: Group 5 Counters - RX Octet Counters per Priority [0..24]

Name	Description
RxOctetsP0	Received octets on Priority 0
RxOctetsP1	Received octets on Priority 1.
RxOctetsP2	Received octets on Priority 2.
RxOctetsP3	Received octets on Priority 3.
RxOctetsP4	Received octets on Priority 4
RxOctetsP5	Received octets on Priority 5
RxOctetsP6	Received octets on Priority 6.
RxOctetsP7	Received octets on Priority 7

Table 9-6: Group 6 Counters - RX Packet Counters per Flow [0..24]

Name	Description
FIDForwarded	Number of frames that were forwarded normally, either unicast or multicast, as a result of a lookup of a valid entry in the MAC address table, or a broadcast. Note: This counter does not count mirrored frames.
FloodForwarded	Number of good unicast addressed frames that were flooded because the destination is unknown, or an unregistered multicast.
TriggerMirrored	Number of good frames that were mirrored. Note: Total number of normally forwarded packets = FIDForwarded + FloodForwarded + TriggerMirrored (note that trapped frames are not subject to triggers, so are not mirrored). This counter is only incremented if flooding is enabled in the switch
STPDrops	Number of frames that were dropped because either the ingress or egress port is not in the forwarding spanning tree state, resulting in a frame drop on ingress.
ReservedTraps	Number of frames that are trapped to the CPU and not forwarded normally, as a result of any of the three specific trap functions:
BroadcastDrops	Number of frames that were dropped with DA=0xFFFFFFFFFFFF because storm control is enabled.
SecurityViolationDrops	Number of frames that are dropped or trapped because they are considered a security violation.
VLANTagDrops	Number of frames discarded because the frames were untagged, and drop untagged is configured, or the frames were tagged, and drop tagged is configured.
VLANIngressBVDrops	Number of frames dropped for an ingress VLAN boundary violation. Note: This only applies to 802.1Q, because in port-based VLAN there is no such thing as an ingress violation.
VLANEgressBVDrops	Number of frames dropped for an egress VLAN boundary violation. This does not mean the number of ports filtered by the VLAN membership list in a multicast or flood; it means the destination address

	corresponds to a port that is not (or no longer) in the VLAN membership list, so the frame was dropped and not forwarded.
TriggerRedirAndDrops	Number of frames that were dropped or redirected because they caused a user defined trigger to fire.
DLFDrops	Number of frames that were discarded because there was a destination lookup failure and flooding is not enabled in the switch. Note: This counter is incremented for unicast & multicast
CMRxDrops	Number of frames dropped for exceeding the RX shared watermark.

Table 9-7: Group 7 Counters - TX Packet Counters per Type [0..24]

Name	Description
TxUnicast	Unicast frames transmitted, possibly with incorrect FCS due to cut-through. (Note: undersized frames that have been padded to the min size (MAC_CFG_2[PadMinSize]=1) are counted.)
TxBroadcast	Broadcast frames transmitted, possibly with incorrect FCS due to cut-through.
TxMulticast	Multicast frames transmitted, possibly with incorrect FCS due to cut-through.
TxPause	Transmitted pause frames and valid FCS. This counter is a 32 bit counter only
TxFCSErrors	Transmitted frames with FCS errors. (Note: undersized frames that have been padded to the min size (MAC_CFG_2[PadMinSize]=1) are not counted even though they have a forcedbad CRC.). This counter is a 32 bit counter only.
TxErrorDrops	The number of frames that were marked on ingress as erroneous (either due to an FCS or PHY error, or due to under/over size problems) which the switch element actually managed to discard. Frames marked as erroneous on ingress which were transmitted (due to cutthrough) will not be included in this counter.
TxTimeoutDrops	A frame in a TX queue was dropped as a result of a time out.

Table 9-8: Group 8 Counters - TX Packet Counters per Size [0..24]

Name	Description
TxMinto63	Transmitted frames of min. frame size to 63 octets. This counter is for non-error frames that are less than 64 octets because the min. frame size is set below 64 octets in the MAC, or error frames that the switch transmitted anyway because MAC_CFG_2[Min Frame Discard] was not set (includes bad frames)
Tx64	Transmitted frames of 64 octets. (includes bad frames)
Tx65to127	Transmitted frames of 65 to 127 octets (includes bad frames)
Tx128to255	Transmitted frames of 128 to 255 octets (includes bad frames)
Tx256to511	Transmitted frames of 256 to 511 octets (includes bad frames)
Tx512to1023	Transmitted frames of 512 to 1023 octets (includes bad frames)
Tx1024to1522	Transmitted frames of 1024 to 1522 octets (includes bad frames)
Tx1523to2047	Transmitted frames of 1522 to 2047 octets (includes bad frames)
Tx2048to4095	Transmitted frames of 2048 to 4095 octets (includes bad frames)
Tx4096to8191	Transmitted frames of 4096 to 8191 octets (includes bad frames)
Tx8192to10239	Transmitted frames of 8192 to 10239 octets (includes bad frames)
Tx10240toMax	Transmitted frames of 10240 to MaxFrame octets (includes bad frames). This counter will only be activated if Maxframe is >10240. That is it is the count of non-error frames above 10240. However, Fulcrum strongly recommends not sending packets above 10240, as the Ethernet CRC is not long enough.

Table 9-9: Group 9 Counters - TX Octet Counters [1..24]

Name	Description
TxOctets	Transmitted octets including CRC but excluding preambles and inter-frame characters.

Table 9-10: Group 10 Counters - Congestion Management Counters

Name	Description
CMTxDrops[0..24]	Count of frames dropped for congestion management from TX port 0.
CMGlobalLowDrops	Count of frames dropped for congestion management from the global low PWD watermark.
CMGlobalHighDrops	Count of frames dropped from the global high PWD watermark.
CMGlobalPrivilegeDrops	Count of frames dropped from the global privilege watermark.

Table 9-11: Group 11 Counters - VLAN Octet Counters [0..31]

Name	Description
VLANUnicastOctets[i]	Unicast octets received on VLAN[i]
VLANXcastOctets[i]	Broadcast and multicast octets received on VLAN[i].

Table 9-12: Group 12 Counters - VLAN Packet Counters [0..31]

Name	Description
VLANUnicast[i]	Unicast frames received on VLAN[i]
VLANXcast[i]	Broadcast and multicast frames received on VLAN[i]

Table 9-13: Group 13 Counters - Trigger Counters [0..16]

Name	Description
TrigCount[i]	Number of times trigger “I” was taken, where0 ≤ i ≤ 15
TrigCount[16]	No trigger was taken.

10 Document's History

Version	Date	Description	Author
1.0	30.08.2007	Initial version;	HK
1.1	21.09.2007	Added note about Port Based VLAN configuration and frame loops;	WW
1.2	26.09.2007	Added description of the 802.1Q VLAN configuration menu;	WW
1.3	03.03.2008	Added description of 802.1X and 802.1p protocol configuration;	AL/WW
1.4	28.03.2008	Added description of the port mirroring configuration;	AL
1.5	10.06.2008	Added activate/deactivate mode and set default configuration for each feature	AL/WW
1.6	03.12.2008	Changed the document's structure; Added description of web interface; Added description of the text based configuration;	AL
1.7	04.08.2009	Added note about the Jumbo frame mode;	AL
1.8	27.07.2009	Fixed the forwarding map in Chapter 6.6.3.2; Added description of the Link Aggregation mode;	AL
1.9	30.07.2009	Added the cross references and short descriptions to the chapter "Description tables of the text based configuration"	AL
1.10	12.08.2009	Added descriptions of the web interface for the Port Mirroring, Jumbo Frame und Link Aggregation modes.	

	19.08.2009	Changed the chapter headlines for the consistent by the chapter naming.	
1.11	11.02.2010	Added description about the 10 GbE switch	AL
	11.02.2010	Added description about device location	AL
	11.02.2010	Adapted the Jumbo frame description for the changed configuration process	AL
1.12	27.04.2010	Text correction: Chapter 5.1, 5.1.1.2, 5.1.3	AL
	15.05.2010	Added chapter 9, 9.1, 9.1.1, 9.2, 9.2.1, 9.2.2 und 9.2.3	AL
1.13	02.05.2010	Added chapter 6 “General settings (Age Time)”	AL
	01.04.2011	Changed name of chapter “Switch Port Numbering” to “Port switching concept” Added parts: “*Fabrics and physical Ports*”, “*AMC Ports and Backplane Interconnect*” and “*Identifier of AMC Port and Additional Connections*”	
	06.04.2011	Added chapter “Default Switch Configuration”	
1.14	23.12.2011	Added Rapid Spanning Tree Protocol to the chapter 6 and chapter 8	AL
1.15	11.12.2012	Fixed table : MCH - Base Board Mapping <Front 2 > to physical <port 13>	AL
1.15	11.12.2012	Added description for the IGMP Snooping mode	AL
1.16	31.01.2013	Added Web-Interface description for the IGMP Snooping mode	AL
1.16	31.1.2013	All additional ports changed to reference on text marks.	AL
1.16	31.1.2013	Changed address of the N.A.T. Headquarters	AL

1.17	16.05.2013	Updated chapter "Script Management – Web interface"	
1.18	19.05.2013	Phone and fax updated, words updated	
	13.11.2013	Reworked, typo correction	SE
1.19	11.08.2014	Chapter "Backup Settings" renamed to "Switch Management"	AL
	19.01.2015	Chapter "Switch Management" updated for FW V2.16	AL
	20.02.2015	Added Chapter 6.12 "BPDU Filtering"	AL
20	08.04.2015	Changed version numbering	AL
	08.04.2015	Removed chapters "Port Maps (v2.9 and earlier)" and "Port Maps, Connection List and Backward Compatibility"- are not related to FWv2.17	
	08.04.2015	Added chapter "Enable/Disable Port"	AL
	09.04.2015	The Chapter *"XAUI - Packet Counter Description"* has been made as a standalone part	AL
	09.04.2015	Remove part *"Driver Level"*- supported regular by switch management	AL
	10.04.2015	Updated description tables in chapters *8.9 Port Mirroring Configuration* and *8.10 Jumbo frame Configuration*	AL
	10.04.2015	Removed all chapters are not related FW v2.17	AL
	24.10.2016	Added chapter 6.16 *Switch Counters (Base MCH GbE)*	AL
	25.10.2016	Added chapter 6.12.1.6 *Show Instance Status* Chapter 6.12 *Rapid Spanning Tree Protocol* reworked for because of RSTP multi instance feature.	AL
Rev23	14.06.2017	Added chapter "Pause Frame Processing"	AL

Rev24	24.08.2017	Updated document information for NAT-MCH firmware V2.19.2	AL
Rev25	15.09.2017	Updated Chapter “5.3.2 Web Interface – load user configuration at system start “ Updated document information for NAT-MCH firmware V2.19.3	AL
Rev26	11.12.2017	Current released FW version replaced by Last Changed FW version	
Rev 27	10.04.2018	Fixed some style mistakes at chapter 4.1 Changing the Switch Device	AL
	04.05.2018	Added chapter “VLAN Tunneling for Update Channel”	AL
Rev 28	12.07.2018	Added a note about Jumbo frame on CPU port	AL
	28.08.2018	Removed description for script configuration items <eth_qos_map> and <eth_pbvlan_encm> Removed chapter "Backward Compatibility" of "Enable/Disable Port" -> "Text based Configuration". Added description for script configuration item <eth_enconn_prim>	AL
	30.08.2018	Added chapter 6.3 “Enable/Disable Port on Primary MCH”	AL
	30.10.2018	Added description table 8.3 “Enable/Disable Port on Primary MCH	AL
		Added chapter 6.5 “Link Propagation”	AL
		Added description table 8.3 “Link Propagation”	AL
	31.10.2018	Added subchapter 6.13.3.3 “Set Propagation Mode” of chapter 6 “Link Aggregation”	AL
		Removed reference to old configuration item in chapter 6.6.3	AL

Rev29	02.08.2019	Added description of script item <eth_rstp_vid>	AL
	05.08.2019	Added description for Instance Membership of RSTP.	AL
	05.08.2019	Adjusted for new script item name <eth_rstp_port_e> indeed <eth_rstp_port>	AL